โครงการป้องกันความปลอดภัยข้อมูลคอมพิวเตอร์ ครั้งที่ 22

THE 22TH CYBER DEFENSE INITIATIVE CONFERENCE (CDIC2023)
หลักสูตร ALL-IN ONE CYBERSECURITY

22 - 24 JANUARY 2024

จัดทำโดย
นายพิชัยชาญ กาญจนศร
นักวิชาการคอมพิวเตอร์ปฏิบัติการ
สำนักตรวจสอบระบบสารสนเทศ

แบบฟอร์มสรุปองค์ความรู้

(สำหรับการฝึกอบรมภายนอก ร่วมประชุม สัมมนา ศึกษาดูงานในประเทศและต่างประเทศ)

โครงการป้องกันความปลอดภัยข้อมูลคอมพิวเตอร์ ครั้งที่ 22

The 22th Cyber Defense Initiative Conference (CDIC2023)

หลักสูตร All-In One Cybersecurity

วันที่ ๒๒ - ๒๔ มกราคม ๒๕๖๗

ณ โรงแรมบลิสตัน สุวรรณ พาร์ควิว

ผู้เข้าร่วมอบรม/ผู้จัดทำ

นายพิชัยชาญ กาญจนศร นักวิชาการคอมพิวเตอร์ปฏิบัติการ

สำนักตรวจสอบระบบสารสนเทศ

SADI
STATE AUDIT DEVELOPMENT INSTITUTE
สถาบันพัฒนาการตรวจเงินแผ่นดิน

1. วัตถุประสงค์ เป้าหมาย หรือสิ่งที่คาดว่าจะได้รับของโครงการ

สร้างความรู้ความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์ อธิบายประเภทของภัยคุกคาม แนวโน้ม และผลกระทบที่เกิดขึ้นได้ พัฒนาทักษะในการป้องกันภัยคุกคามทางไซเบอร์ โดยนำเอาความรู้ไปปรับใช้เพื่อปฏิบัติงานด้านการตรวจสอบระบบสารสนเทศเพื่อส่งผลให้จำนวนเหตุการณ์ Cybersecurity ลดลง และสร้างความตระหนักรู้เกี่ยวกับความสำคัญของ Cybersecurity ให้พร้อมที่จะปฏิบัติตามแนวทางปฏิบัติที่ดีที่สุดเมื่อเกิดภัยคุกคามทางไซเบอร์

2. เนื้อหาสาระสำคัญที่ได้เรียนรู้ หรือได้รับประสบการณ์

ได้รู้เกี่ยวกับ

1. Cybersecurity

- ภัยคุกคามทางไซเบอร์ ประเภท แนวโน้ม และผลกระทบ
- แนวทางปฏิบัติที่ดีที่สุดในการป้องกันภัยคุกคามทางไซเบอร์
- เทคโนโลยี Cybersecurity ที่ใช้ในการป้องกันภัยคุกคาม
- กฎระเบียบและข้อบังคับเกี่ยวกับ Cybersecurity

2. Incident Response

- กระบวนการ Incident Response
- บทบาท หน้าที่ และความรับผิดชอบของทีม Incident Response
- เครื่องมือและเทคนิคที่ใช้ในการตอบสนองต่อเหตุการณ์
- การฝึกซ้อมและทดสอบแผน Incident Response

3. Tools & Technologies

- เครื่องมือและเทคโนโลยี Cybersecurity ต่างๆ
- การใช้งานและการกำหนดค่าเครื่องมือ
- การวิเคราะห์และตรวจสอบข้อมูล
- การจัดการและตอบสนองต่อเหตุการณ์

4. Case Studies

- กรณีศึกษาเหตุการณ์ Cybersecurity ที่เกิดขึ้นจริง

- บทเรียนที่เรียนรู้จากเหตุการณ์
- วิธีการป้องกันไม่ให้เกิดเหตุการณ์ซ้ำ

3. ประโยชน์ที่ได้รับ

3.1 <u>ประโยชน์ต่อตนเอง</u>

ได้เพิ่มพูนความรู้และทักษะด้าน Cybersecurity ได้เข้าใจภัยคุกคามทางไซเบอร์ ประเภท แนวโน้ม และผลกระทบ ในปัจจุบัน และเรียนรู้แนวทางปฏิบัติที่ดีที่สุดในการป้องกันภัยคุกคาม เทคโนโลยี Cybersecurity ที่ใช้ในการป้องกันภัย รวมถึงรู้กฎระเบียบและข้อบังคับเกี่ยวกับ Cybersecurity

3.2 <u>ประโยชน์ต่อหน่วยงาน</u>

สามารถนำเอาความรู้ที่ได้ไปเป็นพื้นฐานในการตรวจสอบระบบสารสนเทศได้อย่างมีประสิทธิภาพ ใช้เครื่องมือและเทคนิคในการตรวจสอบได้อย่างถูกต้อง ในด้าน Cybersecurity ทำให้เข้าใจความเสี่ยงด้าน Cybersecurity ของหน่วยรับตรวจ และประเมินความเสี่ยง

3.3 <u>การประยุกต์ใช้ในสำนักงานการตรวจเงินแผ่นดิน</u>

สามารถนำเอาความรู้ที่ได้มาประเมินความเสี่ยงด้าน Cybersecurity ของสำนักงานการตรวจเงินแผ่นดินได้ เพื่อออกแบบมาตรการควบคุมภายในเพื่อลดความเสี่ยงได้อย่างมีประสิทธิภาพ ป้องกันความเสียหายจากภัยคุกคามทางไซเบอร์ ลดค่าใช้จ่ายในการแก้ไขปัญหา และเพิ่มประสิทธิภาพในการทำงาน

4. แนวทาง หรือแนวคิดในการนำองค์ความรู้ ประสบการณ์ที่ได้รับไปประยุกต์ใช้ในการปฏิบัติงานจริง

นำความรู้เกี่ยวกับภัยคุกคาม แนวโน้ม และเทคนิคการโจมตีมาปรับใช้ในการออกแบบโปรแกรมตรวจสอบ, พัฒนา checklists การตรวจสอบที่ครอบคลุมประเด็น Cybersecurity ที่สำคัญ นำเสนอผลการตรวจสอบและข้อเสนอแนะต่อหน่วยรับตรวจ ในการออกแบบและ implement มาตรการควบคุม Cybersecurity

5. ข้อเสนอแนะในการส่งบุคลากรเข้าร่วมการฝึกอบรม สัมมนา ศึกษาดูงาน

เป็นโครงการอบรมที่เน้นเกี่ยวกับภัยคุกคามด้าน Cybersecurity ซึ่งจะกล่าวแค่ในภาพรวม ไม่ได้ลงลึกไปด้านเทคนิคจริงๆ ทำให้ไม่ต้องมีพื้นฐานคอมมากๆ ก็เรียนได้ แต่ส่วนใหญ่คำศัพท์ที่ใช้ เป็นคำศัพท์เฉพาะทางเยอะมาก บุคลากรที่เข้าร่วมอบรม อย่างน้อยควรมีความรู้ทางในวงการ Cybersecurity อยู่บ้าง

6. ในภาพรวมของหลักสูตรท่านเห็นว่าควรจัดส่งบุคลากรเข้าอบรมในครั้งถัดไปหรือไม่

หลักสูตรครอบคลุมเนื้อหาเกี่ยวกับภัยคุกคามทางไซเบอร์ แนวโน้ม เทคโนโลยี และแนวทางปฏิบัติที่ดีที่สุด ซึ่งมีความสำคัญต่อการปฏิบัติงาน IT Audit ในปัจจุบัน และรูปแบบการอบรมผสมผสานการบรรยาย การฝึกปฏิบัติ และการศึกษากรณีศึกษา ช่วยให้ผู้เข้าอบรมเข้าใจเนื้อหาและสามารถนำไปประยุกต์ใช้ได้ ดังนั้นจึงเห็นควรอย่างยิ่งในการจัดส่งบุคลากรเข้าอบรมในครั้งถัดไป

7. ภาพกิจกรรม ภาพงาน เอกสารประกอบ (ถ้ามี)

.....

รายงานเรื่อง

โครงการป้องกันความปลอดภัยข้อมูลคอมพิวเตอร์ ครั้งที่ 22

The 22th Cyber Defense Initiative Conference (CDIC2023)

หลักสูตร

All-In One Cybersecurity

จัดทำโดย

นายพิชัยชาญ กาญจนศร นักวิชาการคอมพิวเตอร์ปฏิบัติการ

สำนักตรวจสอบระบบสารสนเทศ

สารบัญ

ภัยคุกคามความปลอดภัยทางไซเบอร์ (Cybersecurity Threat)

คำศัพท์เกี่ยวกับความปลอดภัยทางไซเบอร์

- **Intrusion Detection** (การตรวจจับการบุกรุก) : กระบวนการและวิธีการวิเคราะห์ข้อมูลจากเครือข่ายและระบบสารสนเทศเพื่อพิจารณาว่ามีการละเมิดความปลอดภัยหรือการละเมิดความปลอดภัยเกิดขึ้นหรือไม่
- **Exploit** : การโจมตีโดยอาศัยบั๊กของซอฟแวร์ (โจมตีในสิ่งที่โปรแกรมไม่ได้ถูกออกแบบไว้)
- **Breach** (การละเมิด) : เหตุการณ์ใดๆ ที่ส่งผลให้เกิดการเข้าถึงข้อมูล แอปพลิเคชัน บริการ เครือข่าย หรืออุปกรณ์โดยไม่ได้รับอนุญาต โดยการเลี่ยงผ่านการควบคุมความปลอดภัยพื้นฐาน แล้วโอนถ่ายข้อมูลจากที่นึง ไปสู่ที่นึง (ต้องได้ข้อมูลไปด้วย)
- **Malware** (มัลแวร์) : คำทั่วไปที่อธิบายถึงซอฟต์แวร์ที่เป็นอันตรายทุกประเภท ซึ่งออกแบบมาเพื่อสร้างความหายนะให้กับคอมพิวเตอร์ ได้แก่ viruses, trojans, worms และ ransomware เป็นต้น
- **Ransomware** (แรนซัมแวร์) : มัลแวร์ประเภทหนึ่งที่จงใจป้องกันไม่ให้ผู้ใช้งานเข้าถึงไฟล์บนคอมพิวเตอร์ ซึ่งเป็นการเอาข้อมูลของผู้ใช้งานเป็นตัวประกัน โดยทั่วไปจะเข้ารหัสไฟล์และขอให้จ่ายค่าไถ่เพื่อถอดรหัสหรือกู้คืน
- **Bot / Botnet** : ประเภทของซอฟต์แวร์แอปพลิเคชันหรือสคริปต์ที่ทำงานตามคำสั่ง ช่วยให้ผู้โจมตีสามารถควบคุมคอมพิวเตอร์ที่ได้รับผลกระทบจากระยะไกลได้อย่างสมบูรณ์
- **Distributed Denial of Service (DDoS)** : รูปแบบหนึ่งของการโจมตีทางไซเบอร์ โดยเป็นการโจมตีที่มีจุดมุ่งหมายเพื่อทำให้บริการต่างๆ เช่น เว็บไซต์ไม่สามารถใช้งานได้โดยการ "flooding" ด้วยการรับส่งข้อมูลที่เป็นอันตรายหรือข้อมูลจากหลายแหล่ง (มักเป็นบอตเน็ต)
- **Phishing / Spear Phishing** : เทคนิคที่แฮกเกอร์ใช้เพื่อขโมยข้อมูลที่ละเอียดอ่อน ตัวอย่างเช่น การใช้ข้อความอีเมลที่ออกแบบมาเพื่อหลอกให้ผู้อื่นเปิดเผยข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นความลับ เช่น รหัสผ่านและข้อมูลบัญชีธนาคาร

สิ่งที่ Threat Actor (ผู้คุกคาม) สนใจ

ผู้คุกคามต้องการข้อมูลและความลับ เพื่อขู่กรรโชกเงินจากองค์กร สิ่งที่ผู้คุกคามต้องการมักจะเป็น

- ชื่อผู้ใช้และรหัสผ่าน สามารถเอาไปยกระดับสิทธิ์ของตัวเองให้สูงขึ้น
- เอกสารบริษัทที่มีความละเอียดอ่อน
- ข้อมูลด้านสุขภาพที่ได้รับการคุ้มครอง (PHI)
- ข้อมูลบัตรเครดิตและข้อมูลธนาคาร
- เทคโนโลยีควบคุมการส่งออก
- ทรัพย์สินทางปัญญาและเอกสารทางเทคโนโลยีที่ละเอียดอ่อน
- ข้อมูลที่ระบุตัวตนส่วนบุคคล (PII)
- รายชื่อผู้ติดต่อ (อีเมล สมุดโทรศัพท์ ฯลฯ)
- อีเมลที่เป็นความลับ

ความเสี่ยงด้านความปลอดภัยทางอินเทอร์เน็ต

- System Compromised (การโจมตีในลักษณะยึดเครื่องหรือครอบครองระบบ)
- Identity Theft (การขโมยข้อมูลประจำตัว)
- Social Engineering Attack (การหลอกลวง ล่อหลอกผู้อื่น ใช้หลักการพื้นฐานทางจิตวิทยาให้เหยื่อเปิดเผยข้อมูล เช่น การหลอกโทรหา)
- Data Leakage (ข้อมูลรั่วไหล)
- Web Defacement (การโจมตีเว็บไซต์เพื่อเปลี่ยนแปลงข้อมูลที่เผยแพร่หน้าเว็บ)
- Malware Infection (APT) การโจมตีโดยฝังตัวในระบบระยะยาว และหลบเลี่ยงการตรวจจับได้ดี
- Denial of Service (การโจมตีโดยมีจุดมุ่งหมายทำให้ระบบไม่สามารถให้บริการได้)

Scanning & Vulnerability Assessment (การสแกนและประเมินความเสี่ยง)

- เป็นกระบวนการระบุและประเมินช่องโหว่ในระบบคอมพิวเตอร์หรือเครือข่าย
- ช่วยให้สามารถระบุและแก้ไขช่องโหว่ก่อนที่จะถูกผู้โจมตีทางไซเบอร์ใช้ประโยชน์

ประเภทของ Threat Actor (ผู้คุกคาม)

- Script kiddies : แฮกเกอร์สมัครเล่น ที่ยังไม่ได้เชี่ยวชาญเรื่องคอมพิวเตอร์ มักจะหาไวรัสจากคนที่เคยทำไว้อยู่แล้ว มาปล่อย เพื่อเล่นสนุก หรือลองของ
- Malicious insiders : บุคคลภายในที่ประสงค์ร้าย อาจเป็นพนักงานหรือบุคคลที่มีสิทธิ์เข้าถึงข้อมูลหรือระบบภายในองค์กร อาจใช้ข้อมูลหรือระบบภายในเพื่อแสวงหาผลประโยชน์ส่วนตัว แก้แค้น หรือสร้างความเสียหายต่อองค์กร
- Hacktivists : มักโจมตีระบบคอมพิวเตอร์หรือเครือข่ายเพื่อแสดงจุดยืนทางการเมือง สังคม หรือศาสนา มักไม่มุ่งหวังผลประโยชน์ทางการเงิน แต่ต้องการสร้างความตระหนักรู้หรือสร้างความเสียหายต่อชื่อเสียงขององค์กรเป้าหมาย
- Cyberterrorists : มุ่งหวังสร้างความหวาดกลัว สร้างความเสียหาย หรือขัดขวางโครงสร้างพื้นฐานสำคัญ มักใช้การโจมตีทางไซเบอร์เพื่อบรรลุเป้าหมายทางการเมืองหรือศาสนา
- State Sponsor : รัฐบาลหรือหน่วยงานของรัฐที่สนับสนุนการโจมตีทางไซเบอร์ มักมุ่งเป้าไปที่รัฐบาลหรือองค์กรในต่างประเทศ เพื่อขโมยข้อมูล ขัดขวางการทำงาน หรือสร้างความเสียหายต่อชื่อเสียง
- CyberWarrior : เป็นบุคคลที่มีทักษะสูง มักทำงานให้กับรัฐบาลหรือหน่วยงานด้านความมั่นคง มักมีหน้าที่โจมตีระบบคอมพิวเตอร์หรือเครือข่ายของศัตรู ปกป้องระบบของตนเอง และรวบรวมข้อมูลข่าวกรอง

มัลแวร์ (Malware)

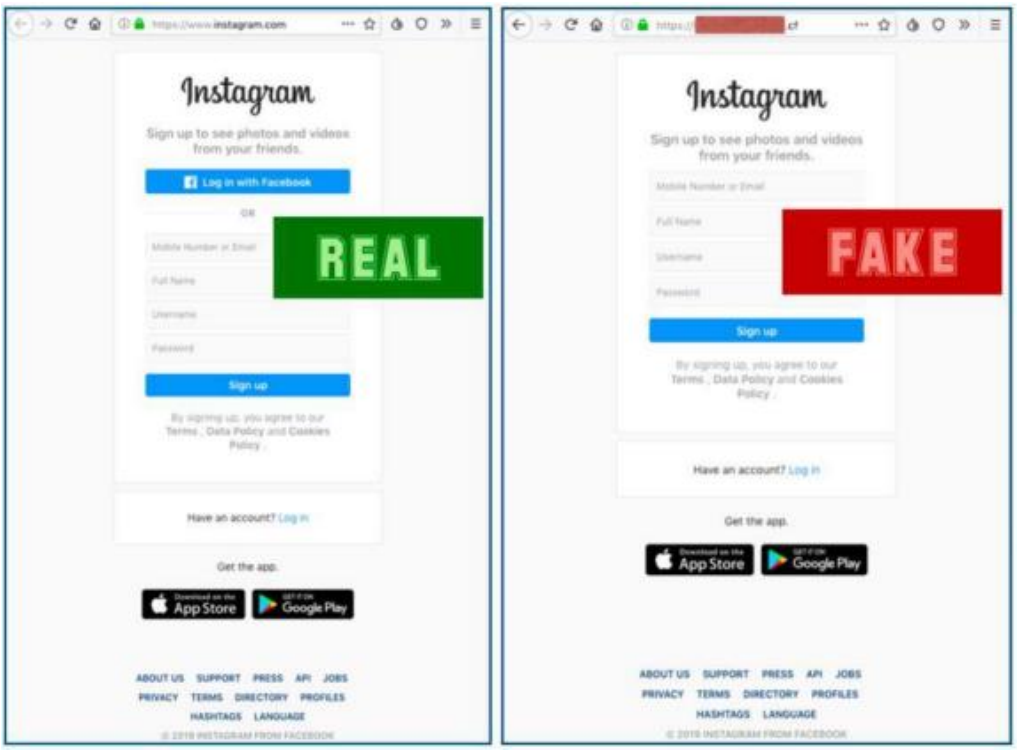
- ซอฟต์แวร์ที่ออกแบบมาเพื่อสร้างความเสียหายหรือขโมยข้อมูล
- มีหลายประเภท เช่น
    - **Keylogger:** บันทึกการกดแป้นพิมพ์เพื่อขโมยรหัสผ่านและข้อมูลส่วนตัว
    - **Trojan:** แฝงตัวมาในโปรแกรมอื่นเพื่อหลอกล่อผู้ใช้ให้ติดตั้ง
    - **Botnet:** กลุ่มคอมพิวเตอร์ที่ถูกติดมัลแวร์และถูกควบคุมโดยแฮ็กเกอร์
    - **Rootkit:** ซ่อนตัวอยู่ในระบบปฏิบัติการเพื่อควบคุมคอมพิวเตอร์
    - **Ransomware:** เข้ารหัสข้อมูลและเรียกค่าไถ่เพื่อปลดล็อก
    - **Adware:** แสดงโฆษณาที่ไม่ต้องการบนคอมพิวเตอร์
    - **Spyware:** ขโมยข้อมูลส่วนตัวจากคอมพิวเตอร์
- **การ Cracking Password:** การพยายามเดาหรือใช้เทคนิคต่างๆ เพื่อค้นหารหัสผ่าน
- **การดักจับข้อมูล (Sniffing):** การดักจับข้อมูลที่ส่งผ่านเครือข่าย โดยมักใช้เครื่องมือดักจับข้อมูล (packet sniffer)

- **การใช้ช่องโหว่ (Exploitation):** การใช้ช่องโหว่ในระบบคอมพิวเตอร์หรือซอฟต์แวร์เพื่อเข้าถึงหรือควบคุมระบบ
    - **Buffer Overflow:** การเขียนข้อมูลจำนวนมากเกินไปยังบัฟเฟอร์ (buffer) ในโปรแกรม ทำให้โปรแกรมทำงานผิดปกติและอาจถูกผู้โจมตีใช้ประโยชน์
- **การโจมตีทางไกล (Remote Exploitation):** การโจมตีระบบคอมพิวเตอร์จากระยะไกลผ่านทางเครือข่าย
    - **การโจมตีภายใน (Local Exploitation):** การโจมตีระบบคอมพิวเตอร์โดยใช้สิทธิ์การเข้าถึงที่มีอยู่ภายในระบบนั้น
    - **การโจมตีฝั่ง Client (Client-side Exploitation):** การโจมตีระบบคอมพิวเตอร์ผ่านทางเบราว์เซอร์หรือโปรแกรมอื่นๆ ของผู้ใช้
    - **การโจมตีฝั่ง Server (Server-side Exploitation):** การโจมตีระบบคอมพิวเตอร์ที่เป็นเซิร์ฟเวอร์
- **การโจมตีปฏิเสธบริการ (Denial of Service) และ การโจมตีปฏิเสธบริการแบบกระจาย (Distributed Denial of Service):**
    - **การโจมตีปฏิเสธบริการ (DoS):** การโจมตีที่ทำให้ระบบคอมพิวเตอร์หรือเครือข่ายไม่สามารถให้บริการแก่ผู้ใช้งานที่ถูกต้อง โดยมักทำโดยการส่งข้อมูลจำนวนมากไปยังระบบจนเกิดการ overload
    - **การโจมตีปฏิเสธบริการแบบกระจาย (DDoS):** การโจมตี DoS ที่ใช้คอมพิวเตอร์จำนวนมากโจมตีระบบเป้าหมายพร้อมกัน ทำให้การป้องกันยากขึ้น

ประเภทของวิศวกรรมทางสังคม (Social Engineering)

วิศวกรรมทางสังคม (Social Engineering) คือ เทคนิคการหลอกลวงทางจิตวิทยาเพื่อโน้มน้าวให้เหยื่อเปิดเผยข้อมูลส่วนตัวหรือดำเนินการบางอย่างที่เป็นอันตรายต่อตนเองหรือองค์กร ต่อไปนี้คือประเภทต่างๆ ของวิศวกรรมทางสังคม:

- **Spoofing (การสวมรอย):** การปลอมแปลงข้อมูลเพื่อให้ดูเหมือนเป็นบุคคลหรือองค์กรที่น่าเชื่อถือ เช่น การปลอมแปลงอีเมล เบอร์โทรศัพท์ หรือเว็บไซต์
- **Impersonation (การปลอมตัว):** การแอบอ้างเป็นบุคคลอื่นเพื่อหลอกลวงเหยื่อ เช่น การโทรศัพท์ปลอมเป็นเจ้าหน้าที่ธนาคาร
- **Hoax (ข่าวลวง):** การเผยแพร่ข้อมูลเท็จเพื่อสร้างความตื่นตระหนกหรือหลอกลวงเหยื่อ เช่น การส่งต่ออีเมลปลอมเกี่ยวกับไวรัสคอมพิวเตอร์
- **Phishing (ฟิชชิ่ง):** การส่งอีเมล SMS หรือข้อความปลอมแปลงที่เลียนแบบองค์กรที่น่าเชื่อถือ เพื่อหลอกให้เหยื่อเปิดเผยข้อมูลส่วนตัว เช่น รหัสผ่านหรือข้อมูลบัญชีธนาคาร



Phishing Page : การปลอมหน้าเว็บที่มีความหน้าเชื่อถือแล้วดักขโมยรหัสผ่านเมื่อผู้ใช้งานใส่รหัสผ่าน

- **Vishing (วิชชิ่ง):** การโทรศัพท์ปลอมเป็นองค์กรที่น่าเชื่อถือเพื่อหลอกให้เหยื่อเปิดเผยข้อมูลส่วนตัว เช่น Phishing
- **Whaling (วาฬลิง):** เป็น Phishing ที่มุ่งเป้าไปยังบุคคลระดับสูงในองค์กร เช่น CEO หรือ CFO
- **URL hijacking/typo squatting (การแอบอ้าง URL / การวางเพย์ URL):** การสร้าง URL ที่คล้ายคลึงกับเว็บไซต์ที่น่าเชื่อถือเพื่อหลอกให้เหยื่อเข้าสู่เว็บไซต์ปลอม
- **Spam and spim (สแปมและสปิม):** การส่งข้อความที่ไม่ต้องการจำนวนมากผ่านทางอีเมล (spam) หรือข้อความมือถือ (spim) เพื่อโฆษณา หลอกลวง หรือแพร่กระจายมัลแวร์

- **Shoulder surfing (การแอบมอง):** การแอบมองข้อมูลบนหน้าจอคอมพิวเตอร์หรือเอกสารของผู้อื่น
- **Dumpster diving (การคุ้ยถังขยะ):** การค้นหาข้อมูลที่ทิ้งแล้ว เช่น เอกสาร บิล หรือแผ่นซีดี เพื่อขโมยข้อมูลส่วนตัว
- **Tailgating (การติดตามเข้า):** การติดตามบุคคลที่ได้รับอนุญาตเข้าไปยังพื้นที่ที่มีการควบคุมการเข้าออก

กระบวนการโจมตีทางไซเบอร์ (Cyber Attack Methodology)

Cyber Kill Chain เป็นกรอบแนวคิดที่แบ่งกระบวนการโจมตีทางไซเบอร์ออกเป็น 7 ขั้นตอน เพื่อช่วยให้องค์กรสามารถป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามได้ดียิ่งขึ้น

1. **Reconnaissance (การรวบรวมข้อมูล):**
    - ผู้โจมตีทำการค้นคว้า ค้นหา และเลือกเป้าหมาย
    - อาจรวมถึงการรวบรวมข้อมูลเกี่ยวกับเครือข่าย บุคลากร และระบบขององค์กร
2. **Weaponization (การสร้างอาวุธ):**
    - ผู้โจมตีสร้างเครื่องมือโจมตี (payload) ที่เหมาะสมกับเป้าหมาย
    - อาจรวมถึงการผสมผสานมัลแวร์เข้ากับช่องโหว่ในโปรแกรมที่เปราะบาง
3. **Delivery (การส่งมอบอาวุธ):**
    - ผู้โจมตีส่งมอบเครื่องมือโจมตีไปยังเป้าหมาย
    - อาจใช้ช่องทางต่างๆ เช่น อีเมล์ เว็บไซต์ หรืออุปกรณ์ USB
4. **Exploitation (การใช้ช่องโหว่):**
    - เมื่อส่งมอบไปแล้ว โค้ดของเครื่องมือโจมตีจะทำงาน โดยใช้ช่องโหว่ในแอปพลิเคชันหรือระบบเปราะบาง
5. **Installation (การติดตั้ง):**
    - เครื่องมือโจมตีติดตั้ง backdoor ไว้บนระบบเป้าหมาย
    - ช่วยให้ผู้โจมตีสามารถเข้าถึงระบบได้อย่างต่อเนื่อง
6. **Command & Control (การควบคุมและสั่งการ):**
    - เซิร์ฟเวอร์ภายนอกติดต่อกับเครื่องมือโจมตี
    - ช่วยให้ผู้โจมตีสามารถควบคุมระบบเป้าหมายจากระยะไกล
7. **Actions on Objective (การดำเนินการตามวัตถุประสงค์):**
    - ผู้โจมตีดำเนินการตามวัตถุประสงค์ของการโจมตี
    - อาจรวมถึงการขโมยข้อมูล ทำลายข้อมูล หรือโจมตีระบบอื่นๆ ต่อไป

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Enterprise

เป็นฐานข้อมูลสาธารณะที่รวบรวมเทคนิค ยุทธวิธี และความรู้เชิงพฤติกรรมของผู้โจมตีทางไซเบอร์ ซึ่งเป็นหน่วยงานวิจัยเทคโนโลยีของอเมริกา สามารถใช้ฐานข้อมูลนี้เพื่อประเมินความเสี่ยง ปรับปรุงระบบป้องกัน และพัฒนากลยุทธ์ในการรับมือกับภัยคุกคาม โดยสามารถเข้าได้ที่ลิงก์: https://attack.mitre.org/

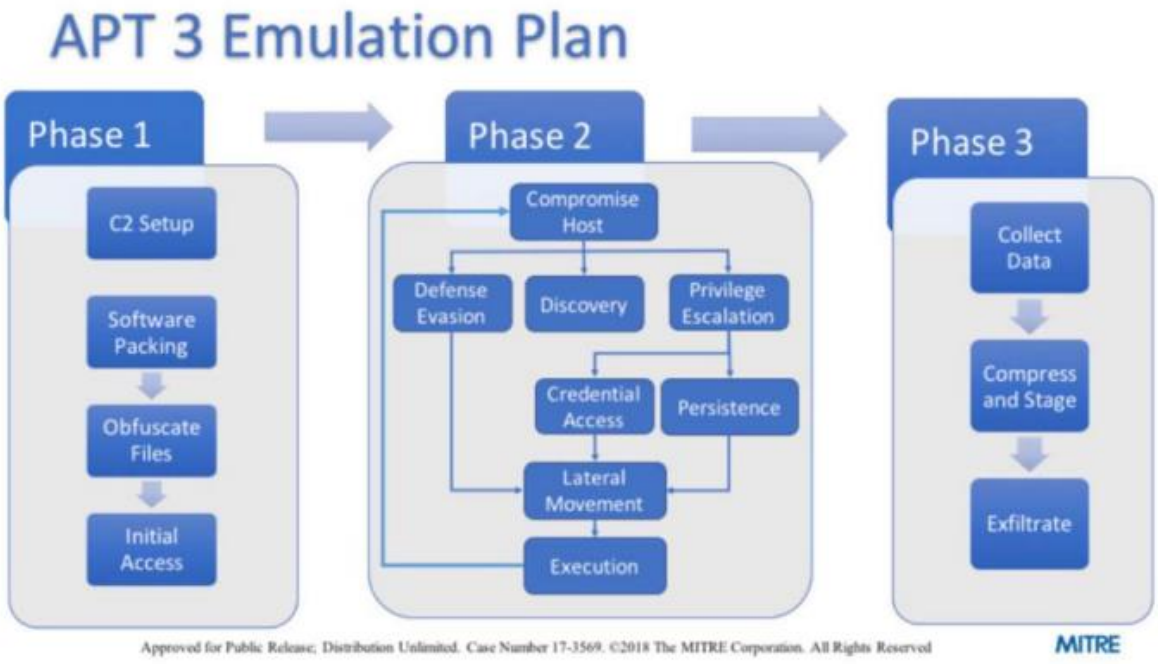
- MITRE ATT&CK Enterprise Tactics

ID	Name	Description
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

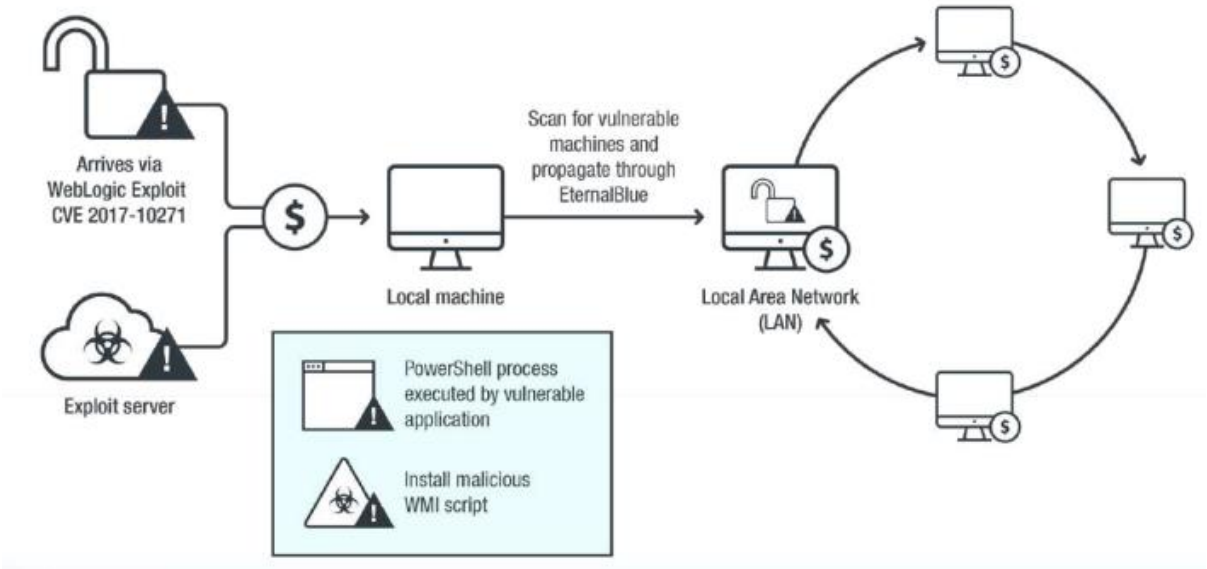
- MITRE ATT&CK Techniques

ID	Name	Description
T1156	.bash_profile and .bashrc	`~/.bash_profile` and `~/.bashrc` are executed in a user's context when a new shell opens or when a user logs in so that their environment is set correctly. `~/.bash_profile` is executed for login shells and `~/.bashrc` is executed for interactive non-login shells. This means that when a user logs in (via username and password) to the console (either locally or remotely via something like SSH), `~/.bash_profile` is executed before the initial command prompt is returned to the user. After that, every time a new shell is opened, `~/.bashrc` is executed. This allows users more fine grained control over when they want certain commands executed.
T1015	Accessibility Features	Windows contains accessibility features that may be launched with a key combination before a user has logged in (for example, when the user is on the Windows logon screen). An adversary can modify the way these programs are launched to get a command prompt or backdoor without logging in to the system.
T1098	Account Manipulation	Account manipulation may aid adversaries in maintaining access to credentials and certain permission levels within an environment. Manipulation could consist of modifying permissions, modifying credentials, adding or changing permission groups, modifying account settings, or modifying how authentication is performed. These actions could also include account activity designed to subvert security policies, such as performing iterative password updates to subvert password duration policies and preserve the life of compromised credentials. In order to create or manipulate accounts, the adversary must already have sufficient permissions on systems or the domain.
T1182	AppCert DLLs	Dynamic-link libraries (DLLs) that are specified in the AppCertDLLs value in the Registry key `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager` are loaded into every process that calls the ubiquitously used application programming interface (API) functions CreateProcess, CreateProcessAsUser, CreateProcessWithLoginW, CreateProcessWithTokenW, or WinExec.

- Adversary Emulation Plans



- ตัวอย่าง APT (Advanced ,Persistent ,Threat) ฝังตัวระยะยาวที่ระบบ ซึ่งส่วนใหญ่มักเจาะระบบเจอเครื่องสิทธิ์ต่ำก่อน แล้วขยายผลไปยังสิทธิ์สูง ส่วนใหญ่ตามสถิติ มักฝังตัวไม่ต่ำกว่า 6 เดือน



ภาพรวมความปลอดภัยไซเบอร์ (Overview Cybersecurity)

วัตถุประสงค์ด้านความปลอดภัย (Security Objectives)

- **ความลับ (Confidentiality):** การจำกัดการเข้าถึงข้อมูลและการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต รวมถึงวิธีการปกป้องข้อมูลส่วนบุคคลและข้อมูลความลับ
- **ความถูกต้องสมบูรณ์ (Integrity):** ป้องกันการแก้ไขหรือทำลายข้อมูลโดยไม่เหมาะสม รวมถึงการรับรองความถูกต้องและความน่าเชื่อถือของข้อมูล
- **ความพร้อมใช้งาน (Availability):** การรับประกันการเข้าถึงและใช้ข้อมูลได้อย่างทันเวลาและเชื่อถือได้

หลักการปฏิบัติตามความปลอดภัย (Security Implementation Principles)

- **ความลับ, ความถูกต้องสมบูรณ์, ความพร้อมใช้งาน (CIA):** หลักการพื้นฐานสามประการของความปลอดภัยทางไซเบอร์
- **การรับรู้ความจำเป็น (Need-to-know):** ผู้ใช้ควรได้รับอนุญาตเข้าถึงข้อมูล (หรือระบบ) เฉพาะที่จำเป็นสำหรับการปฏิบัติหน้าที่เท่านั้น
- **สิทธิ์การเข้าถึงขั้นต่ำสุด (Least privilege):** ผู้ใช้ควรได้รับสิทธิ์การเข้าถึงที่เพียงพอสำหรับการทำงานเท่านั้น
- **การแบ่งแยกหน้าที่ (Separation of duties):**
    - บุคคลใดคนหนึ่งไม่ควรมีหน้าที่รับผิดชอบดำเนินการทั้งหมดตั้งแต่ต้นจนจบ สำหรับข้อมูลที่ละเอียดอ่อน มีค่า หรือสำคัญ
    - บุคคลใดคนหนึ่งไม่ควรมีหน้าที่อนุมัติงานของตนเอง

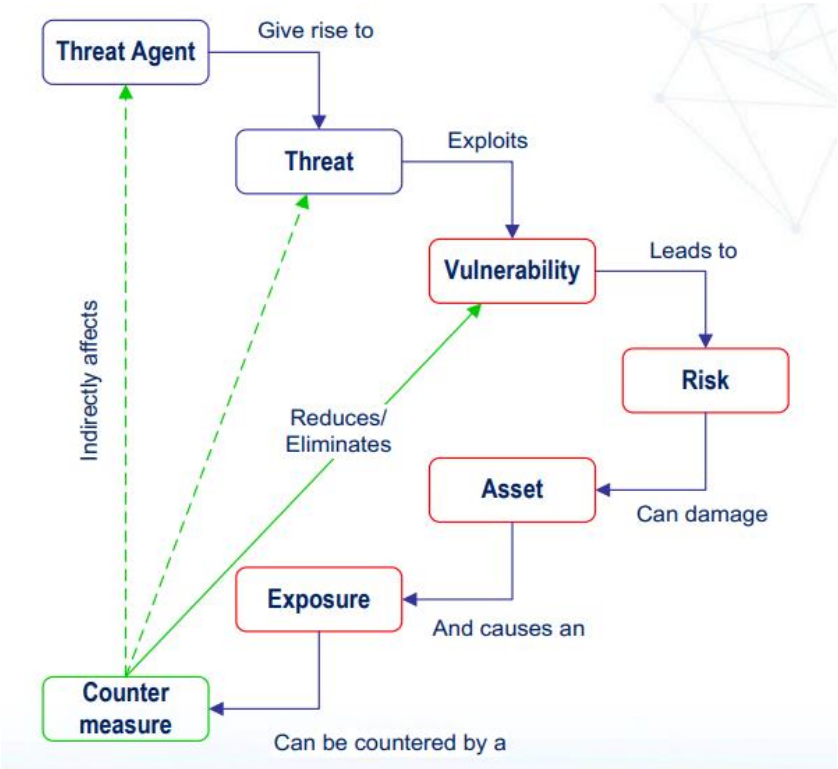
แนวทางปฏิบัติที่ดีด้านความปลอดภัย (Security Best Practices)

- **โดเมนความปลอดภัย (Security Domain)** : ขอบเขตของระบบ ข้อมูล หรือทรัพย์สินที่ต้องได้รับการปกป้อง
- **การแบ่งส่วน (Compartmentalization)** : การแบ่งข้อมูลออกเป็นส่วนย่อย ๆ เพื่อจำกัดการเข้าถึงข้อมูล เฉพาะผู้ที่ได้รับอนุญาตเท่านั้นที่จะเข้าถึงข้อมูลที่เกี่ยวข้อง
- **การรับรู้เท่าที่จำเป็น (Need-to-know)** : การอนุญาตให้บุคคลเข้าถึงข้อมูลเฉพาะที่จำเป็นสำหรับการปฏิบัติหน้าที่เท่านั้น
- **สิทธิ์การเข้าถึงขั้นต่ำ (Least privilege)** : การกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบให้แก่บุคคลน้อยที่สุดเท่าที่จำเป็น

- **การแบ่งแยกหน้าที่ (Separation of duties)** : การแบ่งแยกหน้าที่ที่เกี่ยวข้องกับความปลอดภัยออกจากกัน เช่น การอนุมัติ การเบิกจ่าย และการบันทึกข้อมูล ไม่ควรให้บุคคลเดียวทำหน้าที่เหล่านี้ทั้งหมด
- **การหมุนเวียนงาน (Job rotation)** : การหมุนเวียนบุคลากรไปทำหน้าที่ต่าง ๆ เพื่อป้องกันการทุจริตร่วมกัน (collusion)
    - **เพื่อลดความเสี่ยงจากการทุจริตร่วมกัน (To reduce risk of collusion)**
    - **เพื่อให้แน่ใจว่าไม่มีจุดอ่อนเพียงจุดเดียว (To ensure no single point of failure)**
- **การบังคับพักร้อน (Mandatory vacation)** : การกำหนดให้พนักงานที่มีหน้าที่สำคัญลาพักร้อนเพื่อป้องกันการทุจริตและให้ผู้อื่นสามารถตรวจสอบบันทึกได้

ความสัมพันธ์ระหว่างภัยคุกคาม และมาตรการรับมือ

- **ตัวการภัยคุกคาม (Threat Agent)** : บุคคลหรือระบบที่อาจใช้ช่องโหว่เพื่อก่ออันตราย
- **ภัยคุกคาม (Threat)** : อันตรายใด ๆ ที่อาจเกิดขึ้นกับวงจรชีวิตของข้อมูล (information life cycle)
- **ช่องโหว่ (Vulnerability)** : จุดอ่อนหรือข้อบกพร่องของระบบที่อาจถูกตัวการภัยคุกคามใช้โจมตี
- **ความเสี่ยง (Risk)** : โอกาสที่ตัวการภัยคุกคามจะใช้ประโยชน์จากช่องโหว่ที่พบ
- **การเปิดเผย (Exposure)** : เหตุการณ์ที่ข้อมูลหรือระบบถูกบุกรุกโดยตัวการภัยคุกคาม
- **มาตรการรับมือ / การป้องกัน (Countermeasure / safeguard)** : แนวทางการป้องกัน ทั้งทางด้านการบริหาร การดำเนินงาน หรือการกำหนดกฎเกณฑ์ เพื่อลดความเสี่ยงที่อาจเกิดขึ้น



การควบคุมความปลอดภัย (Security Controls)

การควบคุมความปลอดภัย คือ มาตรการป้องกันทั้งทางการจัดการ ปฏิบัติการ และเทคนิคที่ใช้ภายในระบบสารสนเทศขององค์กร เพื่อปกป้อง **ความลับ** (confidentiality) **ความถูกต้อง** (integrity) และ **ความพร้อมใช้งาน** (availability) ของระบบและข้อมูล

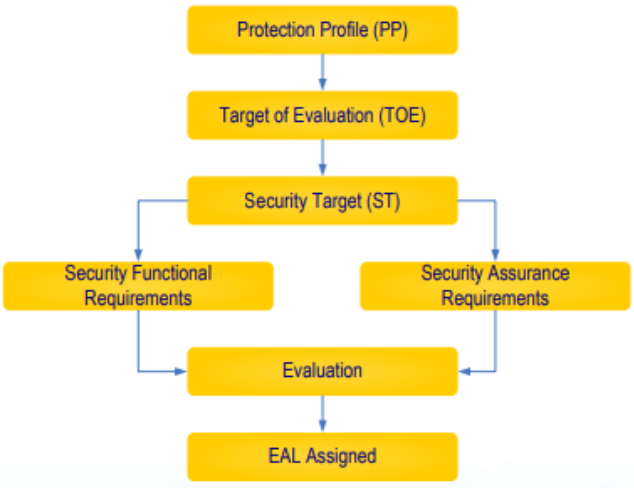
ประเภทของการควบคุมความปลอดภัย

1. **การควบคุมทางการจัดการ (Management (Administrative) Controls)**: เป็นนโยบาย มาตรฐาน กระบวนการ ขั้นตอน และแนวทางที่กำหนดท่าทีด้านความปลอดภัยขององค์กร พวกเขากำหนดโดย **ฝ่ายบริหารระดับสูงและระดับกลาง**
    - ตัวอย่าง: นโยบายความปลอดภัยด้านข้อมูล ขั้นตอนการจัดประเภทข้อมูล นโยบายการควบคุมการเข้าถึง แผนการกู้คืนภัยพิบัติ
2. **การควบคุมเชิงปฏิบัติการ (และกายภาพ) (Operational (and Physical) Controls)**: เน้นที่การปฏิบัติตามการควบคุมทางการจัดการ การฝึกอบรมความตระหนักด้านความปลอดภัย และมาตรการรักษาความปลอดภัยทางกายภาพ
    - **ความปลอดภัยเชิงปฏิบัติการ (Operational Security)**:
        - การนำนโยบายและขั้นตอนไปปฏิบัติ
        - การให้การศึกษาและอบรมด้านความปลอดภัยแก่บุคลากร
    - **ผู้ให้บริการ**:
        - การประกันความปลอดภัยสารสนเทศ (IA)
        - ความปลอดภัยของโปรแกรม
        - ความปลอดภัยของบุคลากร
        - การควบคุมเอกสาร (หรือการจัดการการกำหนดค่า - CM)
        - ทรัพยากรบุคคล (HR)
        - การเงิน
    - **ความปลอดภัยทางกายภาพ (Physical Security)**:
        - สิ่งกีดขวางทางกายภาพ เช่น ประตู กำแพง รั้ว และม่าน
    - **ผู้ให้บริการ**:
        - เจ้าหน้าความปลอดภัยสถานที่ (FSO)
        - เจ้าหน้ารักษาความปลอดภัย
        - สุนัขรักษาความปลอดภัย

3. **การควบคุมเชิงเทคนิค (Technical (Logical) Controls)**: เป็นมาตรการทางเทคนิคที่บังคับใช้การควบคุมความปลอดภัยที่กำหนดไว้ในหมวดหมู่การจัดการและการปฏิบัติการ พวกเขาเน้นการควบคุมการเข้าถึง การระบุตัวตน การอนุญาต ความลับ ความถูกต้อง ความพร้อมใช้งาน และการยืนยันตัวตน
    - ตัวอย่าง: รายการควบคุมการเข้าถึง (ACLs), ไฟร์วอลล์, การเข้ารหัส, ระบบตรวจจับและป้องกันการบุกรุก (IDS/IPS), โซลูชันการสำรองข้อมูลและกู้คืน

CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
	Planning	PL
	System and Services Acquisition	SA
	Security Assessment and Authorization	CA
	Program Management	**PM**
Operational	Personnel Security	PS
	Physical and Environmental Protection	PE
	Contingency Planning	CP
	Configuration Management	CM
	Maintenance	MA
	System and Information Integrity	SI
	Media Protection	MP
	Incident Response	IR
	Awareness and Training	AT
Technical	Identification and Authentication	IA
	Access Control	AC
	Audit and Accountability	AU
	System and Communications Protection	SC

หมวดหมู่ของการควบคุมความปลอดภัย



แนวคิดข้อกำหนดด้านความปลอดภัยและเกณฑ์ทั่วไป (ISO/IEC 15408)

ประเภทของการควบคุมความปลอดภัย (Types of Security Controls)

1. การควบคุมเชิงนโยบาย (Directive Controls) (บางครั้งเรียกว่า การควบคุมทางการจัดการ (administrative controls)) มุ่งแนะนำพนักงานเกี่ยวกับพฤติกรรมที่คาดหวังจากพวกเขาเมื่อมีปฏิสัมพันธ์หรือใช้ระบบสารสนเทศขององค์กร

2. การควบคุมเชิงป้องกัน (Preventive Controls)

- รวมถึงมาตรการทางกายภาพ การบริหาร และเทคนิคที่มุ่งป้องกันการกระทำที่ละเมิดนโยบายหรือเพิ่มความเสี่ยงต่อทรัพยากรระบบ
- ตัวอย่าง:
    - การควบคุมการเข้าถึง (access control)
    - ไฟร์วอลล์ (firewalls)
    - การเข้ารหัสข้อมูล (data encryption)
    - การสำรองข้อมูล (data backup)

3. การควบคุมเชิงตรวจสอบ (Detective Controls)

- เกี่ยวข้องกับการใช้แนวทาง กระบวนการ และเครื่องมือเพื่อระบุและอาจตอบสนองต่อการละเมิดความปลอดภัย
- ตัวอย่าง:
    - ระบบตรวจจับการบุกรุก (intrusion detection systems - IDS)
    - การตรวจสอบบันทึกกิจกรรม (log monitoring)
    - การทดสอบช่องโหว่ (vulnerability assessments)

4. การควบคุมเชิงแก้ไข (Corrective Controls)

- รวมถึงมาตรการทางกายภาพ การบริหาร และเทคนิคที่ออกแบบมาเพื่อตอบสนองต่อการตรวจพบเหตุการณ์ เพื่อลดหรือขจัดโอกาสที่เหตุการณ์ที่ไม่พึงประสงค์จะเกิดขึ้นซ้ำ
- ตัวอย่าง:
    - การฟื้นฟูระบบ (system recovery)
    - การกำหนดบทลงโทษ (disciplinary actions)
    - การปรับปรุงนโยบายความปลอดภัย (security policy updates)

5. การควบคุมเชิงกู้คืน (Recovery Controls)

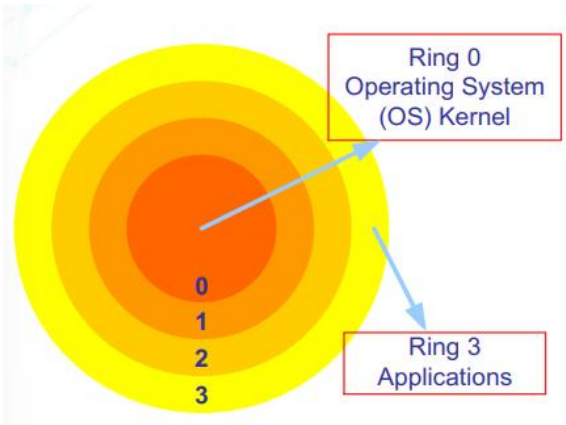
- เมื่อเกิดเหตุการณ์ที่ส่งผลต่อความสมบูรณ์หรือความพร้อมใช้งาน การดำเนินการควบคุมการกู้คืนเป็นสิ่งจำเป็นเพื่อกู้คืนระบบหรือการดำเนินงานกลับสู่สถานะการทำงานปกติ
- ตัวอย่าง:
    - การกู้คืนข้อมูล (data recovery)
    - การเปลี่ยนรหัสผ่าน (password resets)
    - การปิดใช้งานบัญชีผู้ใช้ (user account disablement)

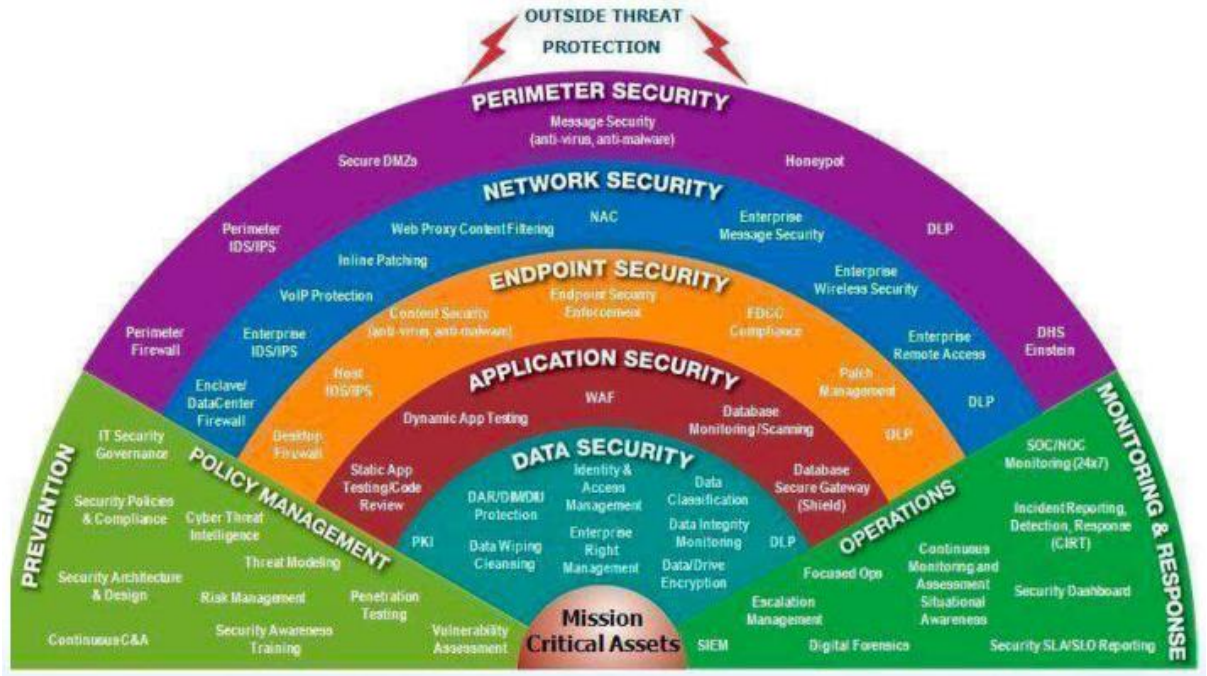
แนวทางการป้องกันเชิงลึก (Defense-in-Depth Model) - วงแหวนแห่งการป้องกัน

โมเดลการป้องกันเชิงลึก (Defense-in-Depth Model) เป็นแนวทางการรักษาความปลอดภัยที่ใช้หลายชั้นการป้องกัน เพื่อปกป้องระบบจากการโจมตี แนวคิดคือการสร้างอุปสรรคหลายชั้น โดยแต่ละชั้นมีความเข้มของการเข้าถึงข้อมูลแตกต่างกัน

หลักการสำคัญ:

- **หมายเลขของวงแหวน** กำหนด **ระดับการเข้าถึง**
- **โปรแกรม** สามารถเข้าถึง **ข้อมูล** ที่อยู่ใน **วงแหวนเดียวกัน** หรือ **วงแหวนที่มีสิทธิ์น้อยกว่า** เท่านั้น
- **โปรแกรม** สามารถเรียกใช้ **บริการ** ที่อยู่ใน **วงแหวนเดียวกัน** หรือ **วงแหวนที่มีสิทธิ์มากกว่า** ได้
- **วงแหวน 0** ประกอบด้วย **ฟังก์ชันเคอร์เนล** ของระบบปฏิบัติการ
- **วงแหวน 1** ประกอบด้วย **ระบบปฏิบัติการ**
- **วงแหวน 2** ประกอบด้วย **ยูทิลิตี้ของระบบปฏิบัติการ**
- **วงแหวน 3** ประกอบด้วย **แอปพลิเคชัน**





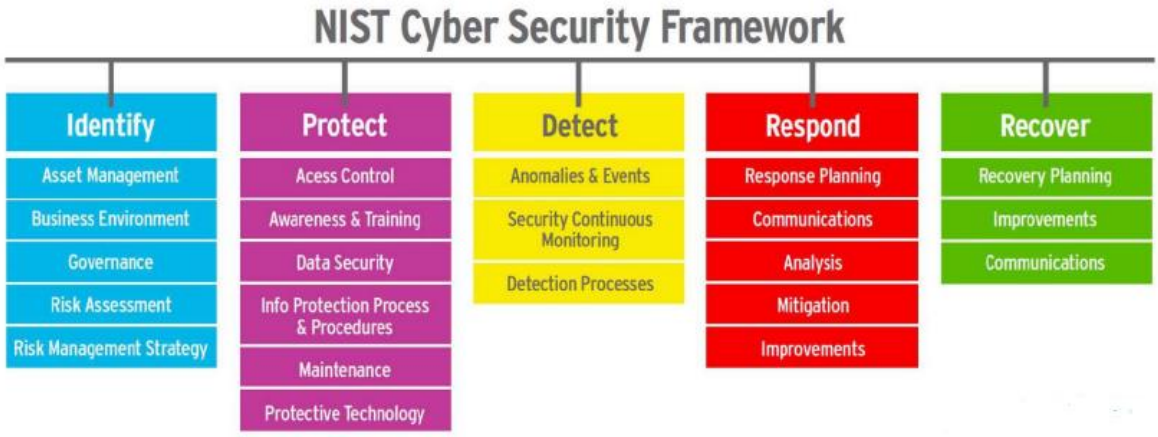
ธรรมาภิบาลด้านความปลอดภัยสารสนเทศ (Information Security Governance)

เป็นกรอบการทำงานที่ช่วยให้องค์กรจัดการความเสี่ยงด้านความปลอดภัยสารสนเทศอย่างมีประสิทธิภาพ ประกอบด้วยองค์ประกอบสำคัญดังนี้:

- **นโยบาย (Policy):** คำสั่งจากฝ่ายบริหารที่กำหนดความคาดหวัง (เป้าหมายและวัตถุประสงค์) และมอบหมายบทบาทและความรับผิดชอบ
- **มาตรฐาน (Standards):** กิจกรรม บทบาท และกฎเกณฑ์เฉพาะด้านที่กำหนดไว้ให้ปฏิบัติตามอย่างเคร่งครัด
- **กระบวนการและขั้นตอน (Process & Procedure):** คำแนะนำทีละขั้นตอนสำหรับการปฏิบัติ
- **แนวทาง (Guideline):** คำแนะนำ กรอบการทำงาน หรือข้อเสนอแนะทั่วไปเพื่อเสริมกระบวนการหรือขั้นตอน

Trends in Cybersecurity (แนวโน้มความปลอดภัยทางไซเบอร์)

พัฒนามาจาก NIST ซึ่งเป็นหน่วยงานที่ดูเรื่องมาตรฐานความปลอดภัยของอเมริการ ซึ่งมี Framework อยู่ 5 ฟังก์ชั่น ได้แก่ Identity Protect Detect Respond และ Recover



การฝึกอบรมและการศึกษาความปลอดภัยทางไซเบอร์

(Cybersecurity Training & Education)

การศึกษา การฝึกอบรม และการสร้างความตระหนักด้านความปลอดภัย (SETA)

SETA เป็นแนวทางการสร้างความรู้ความเข้าใจด้านความปลอดภัยสารสนเทศสำหรับพนักงานองค์กร ประกอบด้วย 3 ระดับ ดังนี้:

- **การสร้างความตระหนัก (Awareness):** บทสรุปและเอกสารประกอบการปฐมนิเทศ เพื่อแจ้งและเตือนพนักงานเกี่ยวกับภาระรับผิดชอบด้านความปลอดภัยของตนเองและความคาดหวังของฝ่ายบริหาร
- **การฝึกอบรม (Training):** หลักสูตรและเอกสารประกอบการฝึกอบรม เพื่อมอบทักษะที่จำเป็นแก่พนักงานในการปฏิบัติหน้าที่
- **การศึกษา (Education):** หลักสูตรและเอกสารประกอบการศึกษา เพื่อมอบทักษะการตัดสินใจและการจัดการที่จำเป็นแก่พนักงาน เพื่อยกระดับความสามารถในการเลื่อนตำแหน่งและความคล่องตัว

National Initiative for Cybersecurity Education (NICE)

NICE เป็นส่วนหนึ่งของ **โครงการริเริ่มด้านความมั่นคงปลอดภัยไซเบอร์ระดับชาติอย่างครอบคลุม (CNCI)** ซึ่งเป็นความร่วมมือระหว่างภาครัฐและภาคเอกชนในการสร้าง **กรอบการฝึกอบรมและการศึกษา** สำหรับ **บุคลากรด้านความมั่นคงปลอดภัยไซเบอร์**

NICE กำหนดชุดทักษะความสามารถที่จำเป็นสำหรับบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ โดยแบ่งออกเป็น 7 กลุ่มดังนี้:

1. Securely Provision (การจัดเตรียมอย่างปลอดภัย): ความเชี่ยวชาญด้านการออกแบบ แนวคิด และการสร้างระบบไอทีที่ปลอดภัย

2. Operate and Maintain (การดำเนินงานและบำรุงรักษา): ความรับผิดชอบในการสนับสนุน บริหาร และดูแลรักษา เพื่อให้ระบบไอทีทำงานอย่างมีประสิทธิภาพ ปลอดภัย

3. Protect and Defend (การป้องกันและปกป้อง): ความเชี่ยวชาญในการระบุ วิเคราะห์ และลดทอนภัยคุกคามต่อระบบไอทีและเครือข่าย

4. Investigate (การสืบสวน): ความเชี่ยวชาญในการสืบสวนเหตุการณ์หรืออาชญากรรมทางไซเบอร์ที่เกิดขึ้นภายในระบบไอทีและเครือข่าย

5. Operate and Collect (การดำเนินงานและรวบรวม): ความเชี่ยวชาญพิเศษ (ส่วนใหญ่เป็นความลับ) ในการรวบรวมข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อนำไปใช้พัฒนาข่าวกรอง

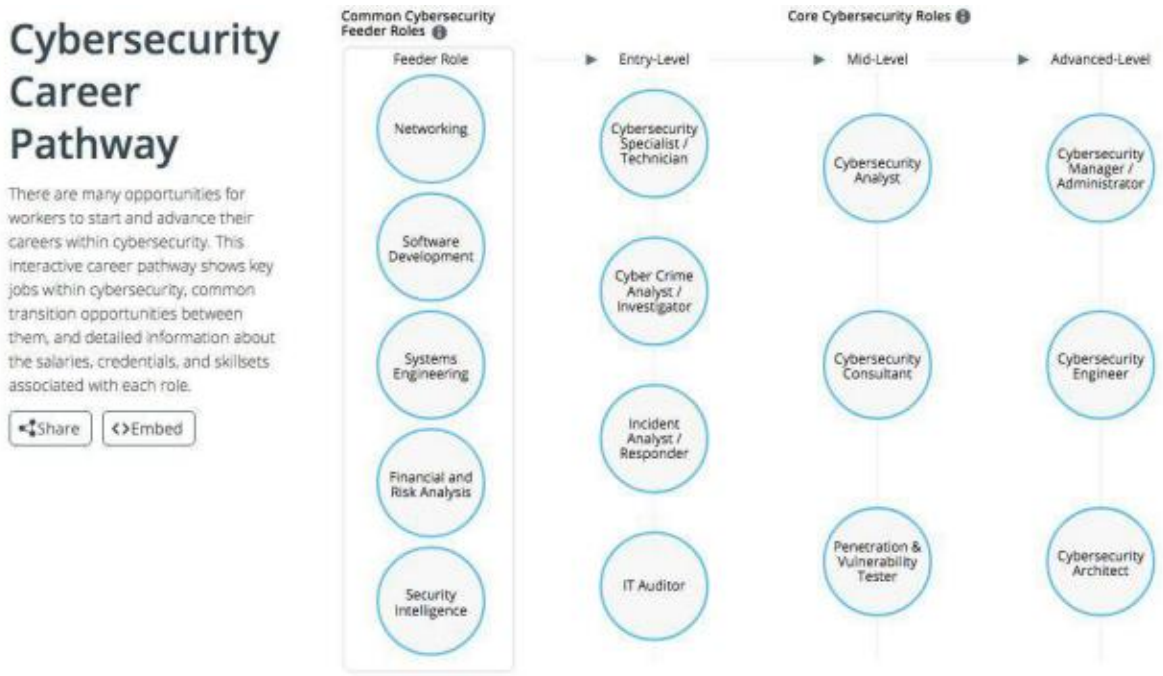
6. Analyze (การวิเคราะห์): ความเชี่ยวชาญพิเศษ (ส่วนใหญ่เป็นความลับ) ในการตรวจสอบและประเมินข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ที่ได้รับ

7. Support (การสนับสนุน): ให้การสนับสนุนที่สำคัญเพื่อให้บุคลากรอื่น ๆ สามารถปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ

บทบาทของ กรอบการทำงาน NICE ด้านความมั่นคงปลอดภัยไซเบอร์

- **Analyze (วิเคราะห์):** ประเมินข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ที่ได้รับอย่างละเอียดเพื่อประเมินประโยชน์ในการใช้เป็นข่าวกรอง
- **Collect and Operate (รวบรวมและดำเนินงาน):** ดำเนินการปฏิบัติการหลอกลวงและปฏิเสธการให้บริการที่เฉพาะทาง รวมถึงรวบรวมข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจนำไปใช้พัฒนาข่าวกรอง
- **Investigate (สืบสวน):** สืบสวนเหตุการณ์หรืออาชญากรรมทางไซเบอร์ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ (IT) เครือข่าย และหลักฐานดิจิทัล
- **Operate and Maintain (ดำเนินงานและบำรุงรักษา):** ให้การสนับสนุน บริหาร และดูแลรักษาเพื่อให้ระบบเทคโนโลยีสารสนเทศ (IT) ทำงานอย่างมีประสิทธิภาพ ปลอดภัย

- **Oversee and Govern (กำกับดูแล):** ให้การนำ แนวทาง บริหาร จัดการ และพัฒนา เพื่อให้องค์กรสามารถดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ
- **Protect and Defend (ป้องกันและปกป้อง):** ระบุ วิเคราะห์ และลดทอนภัยคุกคามต่อระบบเทคโนโลยีสารสนเทศ (IT) ภายในและ/หรือเครือข่าย
- **Securely Provision (จัดเตรียมอย่างปลอดภัย):** ออกแบบ แนวคิด จัดหา และ/หรือสร้างระบบเทคโนโลยีสารสนเทศ (IT) ที่ปลอดภัย โดยรับผิดชอบด้านการพัฒนาระบบและ/หรือเครือข่าย



Cybersecurity Career Pathway (เส้นทางอาชีพการรักษาความปลอดภัยทางไซเบอร์)

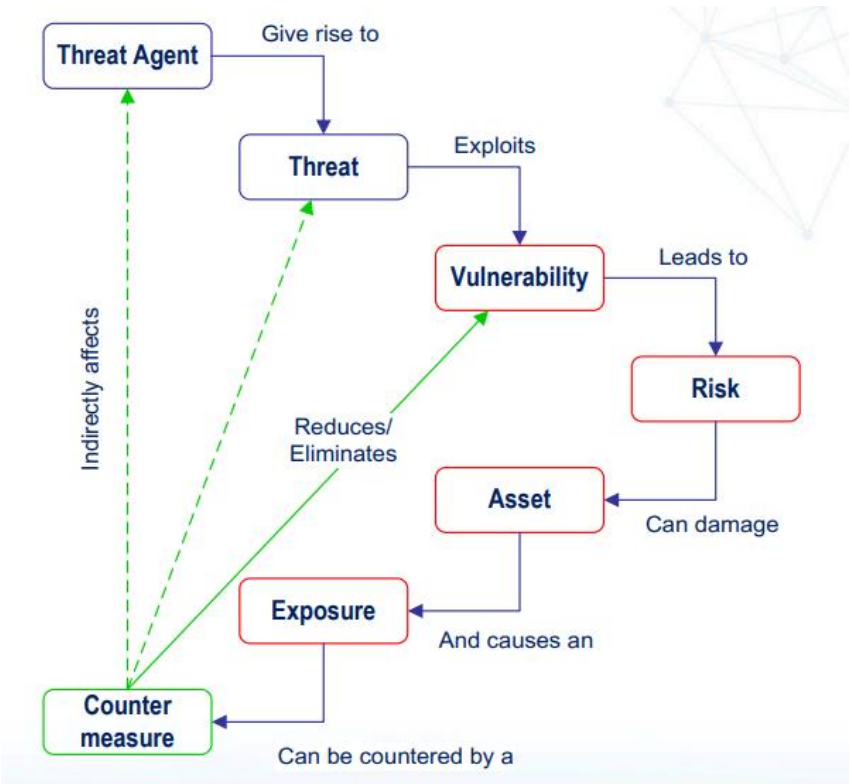
การจัดการความเสี่ยง (Risk Management)

ความหมายของความเสี่ยง (Risk)

- เป้าหมายหลักของกระบวนการจัดการความเสี่ยงขององค์กรคือการปกป้ององค์กรและความสามารถในการปฏิบัติภารกิจ ไม่ใช่แค่ทรัพย์สินด้านไอทีเท่านั้น
- ความเสี่ยงเป็นผลมาจากความน่าจะเป็นที่แหล่งที่มาของภัยคุกคามใช้ช่องโหว่ที่อาจเกิดขึ้น และผลกระทบที่เกิดขึ้นจากเหตุการณ์ไม่พึงประสงค์นั้นต่อองค์กร

ความสัมพันธ์ระหว่าง ภัยคุกคาม ความเสี่ยง และ การป้องกัน

- **ตัวการคุกคาม (Threat Agent):** สิ่งที่อาจใช้ช่องโหว่
- **ภัยคุกคาม (Threat):** อันตรายใด ๆ ที่อาจเกิดขึ้นกับวงจรชีวิตของข้อมูล
- **ช่องโหว่ (Vulnerability):** จุดอ่อนหรือข้อบกพร่องที่อาจเปิดโอกาสให้กับตัวการคุกคาม
- **ความเสี่ยง (Risk):** ความน่าจะเป็นที่ตัวการคุกคามจะใช้ประโยชน์จากช่องโหว่ที่ค้นพบ
- **การเผยแพร่ (Exposure):** ตัวอย่างของการถูกโจมตีโดยตัวการคุกคาม
- **มาตรการป้องกัน/การป้องกัน (Countermeasure / safeguard):** การลดหย่อนความเสี่ยงที่อาจเกิดขึ้นด้วยวิธีการทางการบริหาร การปฏิบัติงาน หรือวิธีการทางตรรกะ



คำจำกัดความในการจัดการความเสี่ยง

- **ทรัพย์สิน (Asset):** สิ่งที่มีค่าต่อองค์กร เช่น ข้อมูล บุคลากร ระบบ เทคโนโลยี
- **แหล่งที่มาของภัยคุกคาม (Threat-source):** แหล่งที่มาของภัยคุกคาม เช่น อาชญากรรมทางไซเบอร์ ภัยธรรมชาติ
- **ตัวการคุกคาม (Threat Agent):** หน่วยงาน บุคคล หรือระบบที่อาจเป็นภัยคุกคาม
- **ภัยคุกคาม (Threat):** อันตรายใด ๆ ที่อาจเกิดขึ้นกับทรัพย์สิน
- **การเผยแพร่ (Exposure):** ตัวอย่างของการถูกโจมตีโดยตัวการคุกคาม
- **ช่องโหว่ (Vulnerability):** จุดอ่อนหรือข้อบกพร่องในระบบหรือกระบวนการ
- **ความน่าจะเป็น (Likelihood):** โอกาสที่ภัยคุกคามจะเกิดขึ้น
- **การโจมตี (Attack):** การกระทำที่มุ่งหวังที่จะใช้ประโยชน์จากช่องโหว่
- **การควบคุม (Controls):** วิธีการลดความเสี่ยง เช่น นโยบาย ขั้นตอนการทำงาน
- **มาตรการป้องกัน (Countermeasures):** วิธีการลดความเสี่ยง เช่น การเข้ารหัสข้อมูล การติดตั้งไฟร์วอลล์
- **การป้องกัน (Safeguards):** วิธีการลดความเสี่ยง เช่น การสำรองข้อมูล การฝึกอบรมพนักงาน
- **ความเสี่ยงทั้งหมด (Total Risk):** ความเสี่ยงก่อนที่จะมีการนำมาตรการป้องกันใด ๆ
- **ความเสี่ยงคงเหลือ (Residual Risk):** ความเสี่ยงที่ยังคงอยู่หลังจากนำมาตรการป้องกันมาใช้แล้ว

ประโยชน์ของการวิเคราะห์ความเสี่ยง (Benefits of Risk Analysis)

- **ช่วยให้การกำหนดนโยบายและการจัดสรรทรัพยากรมีจุดเน้น:** ช่วยให้การกำหนดนโยบายด้านความปลอดภัยและการจัดสรรทรัพยากรด้านความปลอดภัยไปยังพื้นที่ที่มีความเสี่ยงสูง
- **ระบุพื้นที่ที่มีความต้องการด้านความเสี่ยงเฉพาะเจาะจง:** ช่วยในการระบุส่วนต่างๆ ขององค์กรที่มีความเสี่ยงเฉพาะเจาะจง
- **เป็นแนวทางในการบริหารงบประมาณ:** ช่วยในการตัดสินใจว่าควรจัดสรรงบประมาณด้านความปลอดภัยไปยังส่วนใดมากน้อยเพียงใด
- **ช่วยสนับสนุน:**
    - **กระบวนการดำเนินธุรกิจอย่างต่อเนื่อง (Business continuity process):** ช่วยในการวางแผนและเตรียมพร้อมรับมือกับเหตุการณ์ไม่คาดคิดที่จะส่งผลกระทบต่อการดำเนินธุรกิจ
    - **การตัดสินใจด้านประกันภัยและความรับผิด:** ช่วยในการตัดสินใจเกี่ยวกับการเลือกประเภทของประกันภัยและการบริหารจัดการความรับผิด
    - **การสร้างความชอบธรรมให้กับโปรแกรมการสร้างความตระหนักด้านความปลอดภัย:** ช่วยสนับสนุนเหตุผลในการจัดอบรมหรือรณรงค์ให้พนักงานมีความตระหนักด้านความปลอดภัย

ภัยคุกคามรูปแบบใหม่ (Emerging Threats Vectors) ที่องค์กรควรเตรียมรับมือ ได้แก่:

- **เทคโนโลยีใหม่:**
    - **IoT (Internet of Things):** อุปกรณ์ต่างๆ ที่เชื่อมต่ออินเตอร์เน็ต เช่น เครื่องใช้ไฟฟ้าภายในบ้าน
    - **คอมพิวเตอร์ควอนตัม (Quantum Computing):** คอมพิวเตอร์ที่มีความสามารถในการประมวลผลขั้นสูง
    - **เทคโนโลยีบล็อกเชน (Blockchain Technology):** เทคโนโลยีการจัดเก็บข้อมูลแบบกระจายศูนย์ อาจถูกโจมตีเพื่อเปลี่ยนแปลงข้อมูล
- **การเปลี่ยนแปลงกฎระเบียบและกฎหมาย:** กฎหมายใหม่ๆ ที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ
- **การเปลี่ยนแปลงแนวทางการดำเนินธุรกิจ:** วิธีการทำงานรูปแบบใหม่ๆ
- **การเปลี่ยนแปลงวัฒนธรรมหรือสภาพแวดล้อม:** วัฒนธรรมการทำงานจากระยะไกล การใช้โซเชียลมีเดีย
- **การใช้เทคโนโลยีโดยไม่ได้รับอนุญาต:**
    - **เทคโนโลยีไร้สาย (Wireless technologies):** การเชื่อมต่อ Wi-Fi ที่ไม่ปลอดภัย
    - **โมเด็มเถื่อน (Rogue modems):** การติดตั้งโมเด็มอินเตอร์เน็ตโดยไม่ได้รับอนุญาต
    - **เครื่องช่วยดิจิทัลส่วนบุคคล (PDAs):** การนำอุปกรณ์ส่วนตัวมาใช้ทำงาน
    - **ซอฟต์แวร์ที่ไม่ได้รับอนุญาต (Unlicensed software):** การใช้ซอฟต์แวร์เถื่อน

แหล่งที่มาในการระบุภัยคุกคาม (Sources to Identify Threats)

องค์กรสามารถระบุภัยคุกคามได้จากแหล่งข้อมูลต่างๆ ดังนี้:

- **ผู้ใช้ (Users):** ผู้ใช้ภายในองค์กรอาจรายงานช่องโหว่ที่พบเจอ
- **ผู้ดูแลระบบ (System Administrators):** ผู้ดูแลระบบมักพบเจอช่องโหว่ในระหว่างการทำงาน
- **เจ้าหน้าที่รักษาความปลอดภัย (Security Officers):** เจ้าหน้าที่รักษาความปลอดภัยมีหน้าที่ในการประเมินและติดตามภัยคุกคาม
- **ผู้ตรวจสอบ (Auditors):** ผลการตรวจสอบภายในองค์กรอาจช่วยระบุช่องโหว่
- **ฝ่ายปฏิบัติการ (Operations):** ฝ่ายปฏิบัติการอาจพบเจอเหตุการณ์ที่เกี่ยวข้องกับภัยคุกคาม
- **บันทึกสถานที่ (Facility Records):** บันทึกเกี่ยวกับสถานที่ เช่น กล้องวงจรปิด อาจช่วยในการระบุภัยคุกคาม
- **บันทึกชุมชนและรัฐบาล (Community and Government Records)**
- **การแจ้งเตือนผู้ขาย/ผู้ให้บริการรักษาความปลอดภัย (Vendor/Security Provider Alerts)**

ปัจจัยสำคัญในการวิเคราะห์ความเสี่ยง (Risk Analysis Key Factors)

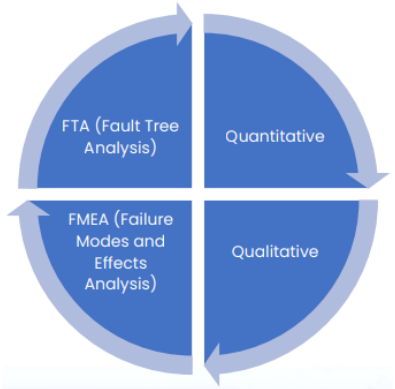
- **การสนับสนุนจากฝ่ายบริหาร (Management support):** ฝ่ายบริหารต้องให้การสนับสนุนทรัพยากรต่างๆ ที่จำเป็นสำหรับการวิเคราะห์ความเสี่ยง
- **การจัดตั้งทีม (Establish team):** ควรจัดตั้งทีมงานที่มีความรู้ความสามารถด้านความปลอดภัยสารสนเทศ
- **สมาชิกในทีม (Team members):** สมาชิกในทีมควรมีผู้เชี่ยวชาญจากหลายด้าน เช่น IT, ความปลอดภัยสารสนเทศ และธุรกิจ
- **ระบบอัตโนมัติ (Automation):** การใช้เครื่องมืออัตโนมัติสามารถช่วยลดเวลาและเพิ่มประสิทธิภาพในการวิเคราะห์ความเสี่ยง

การประเมินความปลอดภัยเบื้องต้น (Preliminary Security Evaluation)

เป็นขั้นตอนเริ่มต้นของกระบวนการวิเคราะห์ความเสี่ยง ประกอบด้วย:

- **ระบุช่องโหว่ (Identify vulnerabilities):** ค้นหาจุดอ่อนของระบบที่อาจถูกโจมตี
- **ทบทวนมาตรการรักษาความปลอดภัยที่มีอยู่ (Review existing security measures):** ประเมินมาตรการรักษาความปลอดภัยที่องค์กรใช้ในปัจจุบัน
- **บันทึกผลการประเมิน (Document findings):** บันทึกผลการประเมินช่องโหว่และมาตรการรักษาความปลอดภัย
- **ขออนุมัติจากฝ่ายบริหาร (Obtain management review and approval):** นำเสนอผลการประเมินความเสี่ยงเบื้องต้นและขออนุมัติจากฝ่ายบริหาร

ประเภทของการวิเคราะห์ความเสี่ยง (Risk Analysis Types)



- **การวิเคราะห์ต้นไม้ความผิดพลาด (FTA - Fault Tree Analysis):** วิธีนี้นำเสนอความสัมพันธ์ของเหตุการณ์ต่างๆ ที่อาจนำไปสู่ความล้มเหลวของระบบ
- **การวิเคราะห์เชิงปริมาณ (Quantitative):** วิธีนี้ใช้ตัวเลขและข้อมูลเชิงสถิติในการประเมินความเสี่ยง
- **การวิเคราะห์เชิงคุณภาพ (Qualitative):** วิธีนี้ใช้การพิจารณาจากประสบการณ์ ความเห็น และข้อมูลเชิงคุณภาพในการประเมินความเสี่ยง
- **การวิเคราะห์รูปแบบและผลกระทบจากความล้มเหลว (FMEA - Failure Modes and Effects Analysis):** วิธีนี้นำมาใช้ในการระบุรูปแบบความล้มเหลวที่อาจเกิดขึ้น ผลกระทบ และวิธีการป้องกัน

วิธีการประเมินความเสี่ยง (Risk Assessment Methods) มี 2 แบบ ดังนี้:

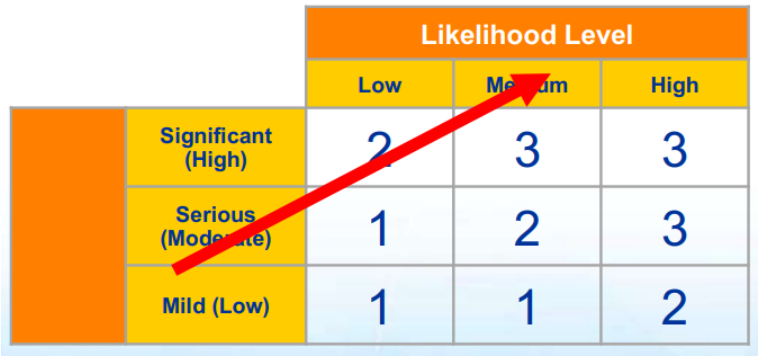
1. การประเมินความเสี่ยงเชิงปริมาณ (Quantitative):

- **ความสูญเสียเฉลี่ยประจำปี (Annualized Lost Expectancy - ALE):** คำนวณโดยสูตร ALE = SLE x ARO
    - **ความสูญเสียเฉลี่ยต่อเหตุการณ์ (Single Loss Expectancy - SLE):** มูลค่าความสูญเสียที่เกิดขึ้นจากเหตุการณ์ภัยคุกคาม 1 ครั้ง (SLE = AV x EF)
        - **มูลค่าทรัพย์สิน (Asset Value - AV):** มูลค่าทางการเงินของทรัพย์สินสารสนเทศ
        - **ปัจจัยความสูญเสีย (Exposure Factor - EF):** เปอร์เซ็นต์ความสูญเสียที่เกิดขึ้นจากภัยคุกคามนั้น
    - **อัตราการเกิดเหตุการณ์ประจำปี (Annualized Rate of Occurrence - ARO):** ความถี่ที่คาดว่าภัยคุกคามจะเกิดขึ้นภายใน 1 ปี

2. การประเมินความเสี่ยงเชิงคุณภาพ (Qualitative):

- **การพิจารณาความน่าจะเป็น (Likelihood Determination):** พิจารณาจาก
    - แรงจูงใจและความสามารถของตัวการคุกคาม
    - ลักษณะของช่องโหว่
    - การมีอยู่และประสิทธิภาพของมาตรการป้องกันที่มีอยู่
- **การวิเคราะห์ผลกระทบ (Impact Analysis):** พิจารณาผลกระทบต่อ 3 ด้าน (CIA)
    - **ความลับ (Confidentiality):** ข้อมูลรั่วไหลหรือไม่
    - **ความถูกต้องสมบูรณ์ (Integrity):** ข้อมูลถูกเปลี่ยนแปลงหรือไม่
    - **ความพร้อมใช้งาน (Availability):** สามารถเข้าถึงข้อมูลได้หรือไม่

- **ภารกิจของระบบ (System mission):** กระบวนการที่ระบบไอทีดำเนินการ
- **ความสำคัญของระบบและข้อมูล (System and data criticality):** คุณค่าหรือความสำคัญของระบบต่อองค์กร
- **ความอ่อนไหวของระบบและข้อมูล (System and data sensitivity):** ความเสี่ยงต่อการโจมตีของระบบและข้อมูล



		Likelihood Level		
		Low	Medium	High
	Significant (High)	2	3	3
	Serious (Moderate)	1	2	3
	Mild (Low)	1	1	2

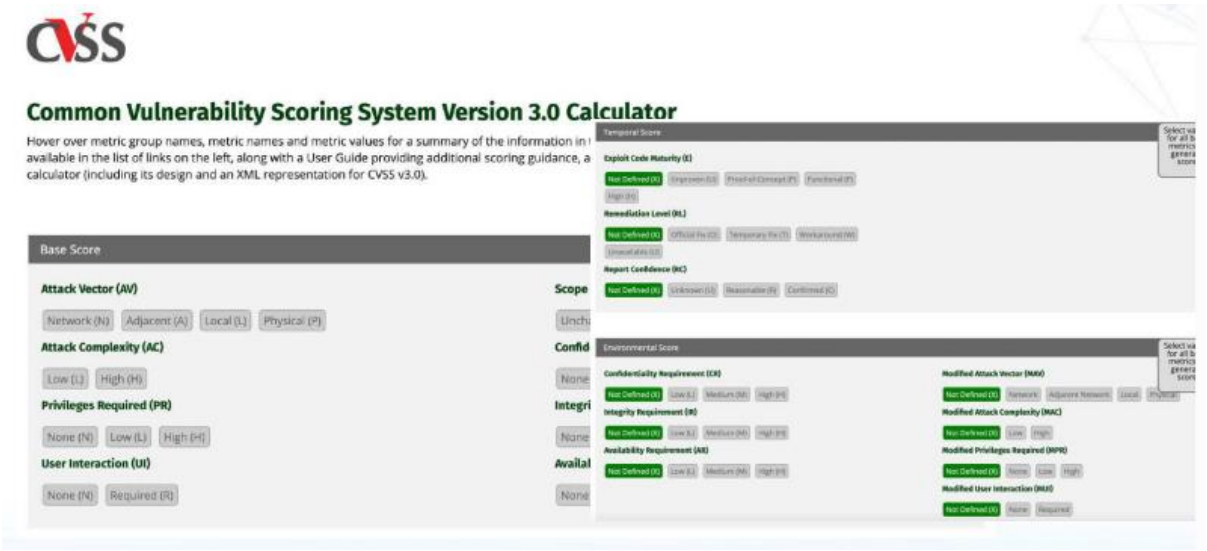
เครื่องมือประเมินความเสี่ยง Risk Assessment Tools

- ระดับความเสี่ยง Risk Levels (AS/NZ 4360 Standard)

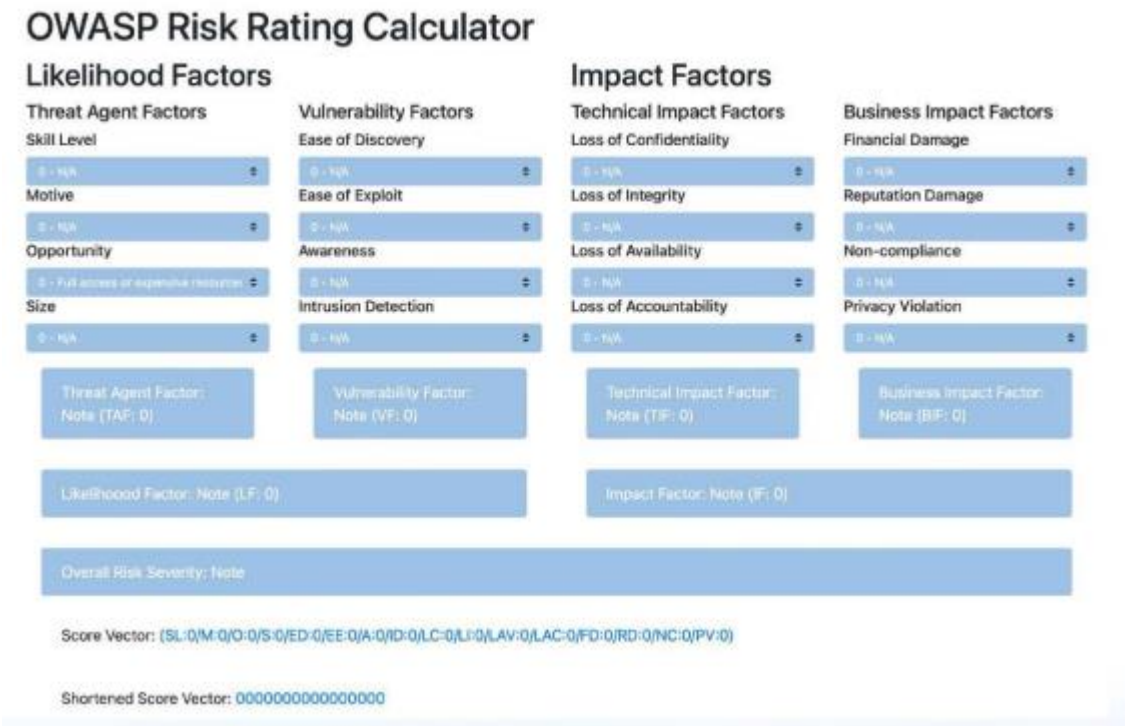
	Consequence:				
	Insignificant	*Minor*	*Moderate*	*Major*	*Catastrophic*
Likelihood:	*1*	*2*	*3*	*4*	*5*
A (almost certain)	H	H	E	E	E
B (likely)	M	H	H	E	E
C (possible)	L	M	H	E	E
D (unlikely)	L	L	M	H	E
E (rare)	L	L	M	H	H

E	Extreme Risk: Immediate action required to mitigate the risk or decide to not proceed
H	High Risk: Action should be taken to compensate for the risk
M	Moderate Risk: Action should be taken to monitor the risk
L	Low Risk: Routine acceptance of the risk

- CVSS Version 3



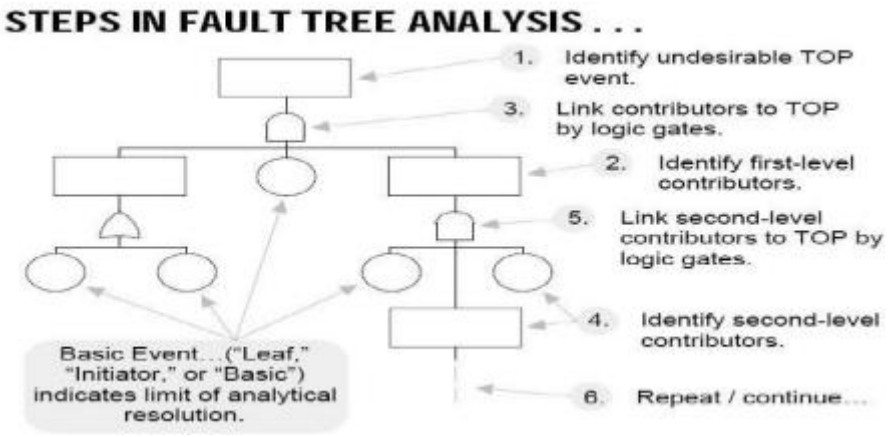
- OWASP Risk Rating



วิธีการวิเคราะห์ความเสี่ยงเพิ่มเติม (Other Risk Analysis Methods)

นอกจากวิธีการวิเคราะห์ความเสี่ยงที่กล่าวไปข้างต้นแล้ว ยังมีวิธีการอื่น ๆ ที่ใช้ในอุตสาหกรรมต่างๆ ได้แก่:

- **การวิเคราะห์รูปแบบและผลกระทบจากความล้มเหลว (FMEA - Failure Modes and Effects Analysis) :**
    - **ใช้ใน:** อุตสาหกรรมการผลิต
    - **วัตถุประสงค์:** ระบุรูปแบบความล้มเหลวที่อาจเกิดขึ้น ผลกระทบ และวิธีการป้องกัน
- **การวิเคราะห์ต้นไม้ความผิดพลาด (FTA - Fault Tree Analysis) :**
    - **ใช้ใน:** ระบบความปลอดภัยและการออกแบบ
    - **วัตถุประสงค์:** วิเคราะห์ความสัมพันธ์ของเหตุการณ์ต่างๆ ที่อาจนำไปสู่ความล้มเหลวของระบบ



ตัวเลือกในการลดความเสี่ยง (Risk Mitigation Options)

เมื่อระบุความเสี่ยงแล้ว องค์กรสามารถเลือกวิธีการลดความเสี่ยงได้ ดังนี้:

- **ยอมรับ (Acceptance):** ยอมรับความเสี่ยงและผลกระทบที่อาจเกิดขึ้น
- **ลดความเสี่ยง (Reduction):** นำมาตรการควบคุมต่างๆ มาใช้เพื่อลดความเสี่ยง
- **โอนความเสี่ยง (Transference):** โอนความเสี่ยงไปยังบริษัทประกันภัย
- **หลีกเลี่ยงความเสี่ยง (Avoidance):** หลีกเลี่ยงกิจกรรมที่ก่อให้เกิดความเสี่ยง

การปกป้องข้อมูลส่วนบุคคลและความเป็นส่วนตัว

(Data Protection and Privacy)

ภัยคุกคามต่อความเป็นส่วนตัวของข้อมูล (Data Privacy Threat)

- **มัลแวร์ (Malware):**
    - **แรนซัมแวร์ (Ransomware):** โปรแกรมที่เข้ารหัสข้อมูลในเครื่องผู้ใช้งานและเรียกค่าไถ่เพื่อปลดล็อก
    - **ม้าโทรจัน (Trojan Horse):** โปรแกรมที่แฝงมาในโปรแกรมอื่นเพื่อแอบทำอันตราย
    - **สปายแวร์ (Spyware) และคีย์ล็อกเกอร์ (Keylogger):** โปรแกรมที่แอบเก็บข้อมูลการใช้งานของผู้ใช้ เช่น รหัสผ่าน
- **การโจมตีขโมยข้อมูลออกนอกระบบ (Data Exfiltration attack):**
    - **ตัวอย่าง:**
        - การขโมยข้อมูลการสมัครงานจากเว็บไซต์
        - การขโมยรหัสผ่านที่ถูกเข้ารหัส (hashed password) จากเว็บไซต์
        - การใช้ข้อมูลรับรองปลอม (credential stuffing) เพื่อโจมตีเว็บไซต์ธนาคาร
- **การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต (Unauthorized Access):** ผู้ที่ไม่ได้รับอนุญาตเข้าถึงข้อมูลส่วนบุคคล
- **ความเสี่ยงจากบุคคล (Human Risk):**
    - **การนำข้อมูลธุรกิจออกไปโดยพนักงานเก่า:** พนักงานเก่านำข้อมูลธุรกิจออกไปหลังจากลาออก
    - **การส่งข้อมูลไปยังบุคคลที่สามโดยไม่ตั้งใจ:** ส่งข้อมูลไปยังบุคคลที่สามที่ไว้ใจโดยไม่ตั้งใจ
- **ความผิดพลาดของบุคคล (Human Mistaken):**
    - **การส่งข้อมูลส่วนบุคคลที่ละเอียดอ่อนทางไปรษณีย์โดยผิดพลาด:** ส่งข้อมูลส่วนบุคคลที่ละเอียดอ่อนทางไปรษณีย์โดยไม่ได้ตั้งใจ
- **การโจมตีทางวิศวกรรมสังคม (Social Engineering attack):**
    - **การขโมยข้อมูลประจำตัว (Identity theft):** แอบอ้างเป็นผู้อื่นเพื่อขโมยข้อมูลส่วนบุคคล
    - **การขโมยข้อมูลผ่านอีเมล (Email exfiltration):** หลอกล่อให้เหยื่อเปิดเผยข้อมูลส่วนบุคคลผ่านทางอีเมล
    - **การปลอมแปลงตัวตน (Impersonation):** แอบอ้างเป็นบุคคลหรียญองกรอื่นเพื่อหลอกลวง

ข้อมูลที่ถูกขโมย (Stolen Data)

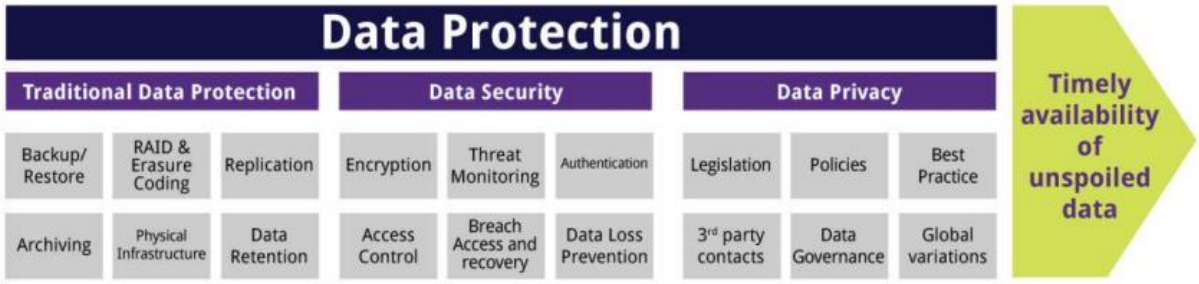
- ข้อมูลที่ถูกขโมยซึ่งมีข้อมูลส่วนบุคคลที่เข้ารหัส
- ข้อมูลที่ถูกขโมยซึ่งมีข้อมูลส่วนบุคคลที่ไม่ได้เข้ารหัส
- แฟ้มเอกสารกระดาษที่มีข้อมูลส่วนบุคคลที่ละเอียดอ่อน

ภาพรวมการปกป้องข้อมูล (Overview Data Protection)

ความเป็นส่วนตัวของข้อมูลคืออะไร และมีความสำคัญอย่างไร? (What Is Data Privacy and Why Is it Important?)

- **ความเป็นส่วนตัวของข้อมูล** คือ แนวทางปฏิบัติในการจัดเก็บและใช้งานข้อมูล โดยพิจารณาจากความละเอียดอ่อนและความสำคัญของข้อมูล โดยทั่วไปแล้ว ความเป็นส่วนตัวของข้อมูลจะถูกนำไปใช้กับข้อมูลสุขภาพส่วนบุคคล (PHI) และข้อมูลที่สามารถระบุตัวตนได้ (PII) ซึ่งรวมถึง ข้อมูลทางการเงิน , บันทึกทางการแพทย์, หมายเลขประกันสังคมหรือเลขประจำตัวประชาชน, ชื่อ, วันเกิด และข้อมูลการติดต่อ
- **กฎระเบียบการปกป้องข้อมูล** กำหนดวิธีการจัดเก็บ, ส่งต่อ, และใช้ข้อมูลบางประเภท ข้อมูลส่วนบุคคลนั้นครอบคลุมข้อมูลต่างๆ เช่น ชื่อ, รูปภาพ, ที่อยู่อีเมล, ข้อมูลบัญชีธนาคาร, ที่อยู่ IP ของคอมพิวเตอร์ส่วนบุคคล และข้อมูลชีวภาพ

การคุ้มครองข้อมูลทั้งสามประเภท (The Three Categories of Data Protection)



เทคโนโลยีการปกป้องข้อมูล (Data Protection Technologies)

- **การค้นหาข้อมูล (Data discovery):** การระบุว่าข้อมูลใดบ้างที่องค์กรมีอยู่
- **ระบบป้องกันการรั่วไหลของข้อมูล (Data loss prevention - DLP):** ระบบที่ช่วยป้องกันการสูญหายของข้อมูลที่สำคัญ
- **การจัดเก็บข้อมูลที่มีระบบป้องกันข้อมูลในตัว (Storage with built-in data protection):** การจัดเก็บข้อมูลในระบบที่มีฟีเจอร์การรักษาความปลอดภัยในตัว
- **การสำรองข้อมูล (Backup):** การสร้างสำเนาของข้อมูลไว้เพื่อกู้คืนกรณีข้อมูลสูญหาย
- **การสร้างจุดกู้คืน (Snapshots):** การบันทึกสถานะของข้อมูล ณ เวลาใดเวลาหนึ่ง เพื่อกู้คืนข้อมูลย้อนกลับไปยังจุดนั้น
- **การจำลองข้อมูล (Replication):** การสร้างสำเนาของข้อมูลไว้ในอีกที่หนึ่ง เพื่อให้สามารถใช้งานได้กรณีระบบหลักขัดข้อง

- **ไฟร์วอลล์ (Firewalls):** ระบบป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต
- **การควบคุมการเข้าถึงข้อมูล (Access Controls):** การกำหนดสิทธิ์ในการเข้าถึงข้อมูล
- **การเข้ารหัสข้อมูล (Encryption):** การเปลี่ยนข้อมูลให้เป็นรหัสเพื่อป้องกันการอ่านโดยไม่ได้รับอนุญาต
- **ระบบป้องกันปลายทาง (Endpoint protection):** ระบบป้องกันอุปกรณ์ต่างๆ เช่น คอมพิวเตอร์และโทรศัพท์มือถือ จากภัยคุกคาม
- **การลบข้อมูล (Data erasure):** การลบข้อมูลอย่างปลอดภัย
- **การกู้คืนระบบหลังภัยพิบัติ (Disaster recovery):** กระบวนการกู้คืนระบบและข้อมูลหลังจากเกิดภัยพิบัติ

แนวคิดการปกป้องข้อมูล (Data Protection) และการรักษาความปลอดภัยข้อมูล (Data Security)

- **ความลับ (Confidentiality):** ปกป้องข้อมูล ข่าวสาร และโปรแกรมจากการเข้าถึงและเปิดเผยโดยไม่ได้รับอนุญาต
- **ความถูกต้องสมบูรณ์ (Integrity):** ข้อมูลทั้งหมดมีความถูกต้อง แม่นยำ และครบถ้วน ทั้งในด้านข้อเท็จจริงและเทคนิค ระหว่างการประมวลผล
- **ความพร้อมใช้งาน (Availability):** Information, data, applications, IT systems และ IT networks พร้อมสำหรับการประมวลผล
- **ความยืดหยุ่น (Resilience):** แสดงถึงลักษณะของความพร้อมใช้งาน และความจุของข้อมูล Information, data, applications, IT systems และ IT networks ในกรณีที่เกิดความผิดปกติ ความล้มเหลว หรือการใช้งานหนัก

การรักษาความลับ (Confidentiality)

- **การควบคุมการเข้าถึง (Access control):**
    - **การระบุตัวตน (Identification):** การพิสูจน์ตัวตนของผู้ขอเข้าถึงข้อมูล
    - **การรับรองความถูกต้อง (Authentication):** การยืนยันว่าผู้ขอเข้าถึงข้อมูลเป็นบุคคลที่ได้รับอนุญาต
    - **การอนุญาต (Authorization):** การกำหนดสิทธิ์ในการเข้าถึงข้อมูล
    - **การรับผิดชอบ (Accountability):** การติดตามและตรวจสอบการเข้าถึงข้อมูล

การรักษาความปลอดภัยทางกายภาพ (Physical security)

- สถานประกอบการและอาคารมีเจ้าหน้ารักษาความปลอดภัยดูแลตลอด 24 ชั่วโมง 7 วันต่อสัปดาห์
- ศูนย์ข้อมูล (data center) รวมถึงฮาร์ดแวร์ เซิร์ฟเวอร์ หรืออุปกรณ์ต่างๆ จะอยู่ในพื้นที่ปลอดภัยที่แยกต่างหากจากสำนักงานทั่วไป
- มีการติดตั้งระบบตรวจสอบการเปิดประตู
- มีการทำสัญญารับบริการระบบเฝ้าระวัง
- มีการบันทึกการเข้าถึงข้อมูล
- เจ้าหน้ารักษาความปลอดภัยทำการตรวจสอบเอกสารประจำตัว
- อนุญาตให้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้นเข้าถึงข้อมูล หลังจากการตรวจสอบและยืนยันตัวตน

การควบคุมการเข้าถึง (Access Control)

การควบคุมการเข้าถึงเป็นกระบวนการสำคัญในการปกป้องข้อมูล โดยมุ่งเน้นที่การอนุญาตให้บุคคลที่ได้รับอนุญาตเท่านั้นเข้าถึงข้อมูลที่จำเป็น หลักการสำคัญของการควบคุมการเข้าถึง ได้แก่

- **การอนุญาตการเข้าถึงข้อมูล (Access authorization):** อนุญาตการเข้าถึงข้อมูลตามขั้นตอนที่กำหนดไว้ โดยพิจารณาจากความจำเป็นและหน้าที่ความรับผิดชอบ
- **ความปลอดภัยของรหัสผ่าน (Password security):** มีมาตรการรักษาความปลอดภัยของรหัสผ่าน เช่น กำหนดความยาว ความซับซ้อน และวิธีการเก็บรักษาที่ปลอดภัย
- **หลักการ "จำเป็นต้องรู้" และ "จำเป็นต้องทำ" (Need-to-know and need-to-do):** อนุญาตการเข้าถึงข้อมูลเฉพาะบุคคลที่จำเป็นต้องรู้และต้องใช้ข้อมูลนั้นในการปฏิบัติงานเท่านั้น
- **บัญชีผู้ดูแลระบบ (Administrator accounts):** ใช้บัญชีผู้ดูแลระบบสำหรับกิจกรรมที่ได้รับอนุญาตอย่างเคร่งครัดเท่านั้น
- **การเปลี่ยนแปลงสถานะการจ้างงาน (Change of employment):** มีกฎระเบียบสำหรับการจัดการสิทธิ์การเข้าถึงข้อมูลของพนักงานที่ลาออกหรือเปลี่ยนงาน
- **การตรวจจับความพยายามเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต (Unauthorized access detection):** มีระบบตรวจจับความพยายามเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และดำเนินการสืบสวนตามความเหมาะสม

การบันทึกการเข้าถึง (Logging of access)

- **บันทึกการเข้าถึงระบบ (System access logs):** บันทึกการเข้าถึงระบบประมวลผลข้อมูลและเวิร์คสเตชัน เพื่อตรวจสอบการใช้งาน
- **การเข้าถึงระบบทางไกล (Remote access logs):** บันทึกการเข้าถึงระบบทางไกลผ่านเกตเวย์ VPN
- **การอนุญาต/เปลี่ยนแปลงสิทธิ์การเข้าถึง (Access authorization logs):** บันทึกการอนุญาตหรือเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูล
- **การประเมินบันทึก (Log evaluation):** ประเมินบันทึกการเข้าถึงข้อมูล เพื่อตรวจสอบความผิดปกติอย่างสม่ำเสมอ

การจัดเก็บข้อมูลอย่างปลอดภัย (Secure Data Storage)

- **อุปกรณ์จัดเก็บข้อมูลที่เข้ารหัส (Encrypted data storage devices):** ใช้ฮาร์ดดิสก์หรืออุปกรณ์จัดเก็บข้อมูลอื่น ๆ ที่เข้ารหัสข้อมูลเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
- **การควบคุมการจัดเก็บอุปกรณ์จัดเก็บข้อมูล (Safekeeping of data storage devices):** ควบคุมการจัดเก็บอุปกรณ์จัดเก็บข้อมูลอย่างปลอดภัย
- **การทำลายอุปกรณ์จัดเก็บข้อมูล (Data storage device destruction):** เมื่อไม่ต้องการใช้อุปกรณ์จัดเก็บข้อมูลอีกต่อไป ต้องทำลายข้อมูลอย่างปลอดภัยแทนการนำไปซ่อม
- **การอนุญาตการนำอุปกรณ์จัดเก็บข้อมูลออก (Authorized data storage device removal):** กำหนดบุคคลที่ได้รับอนุญาตให้นำอุปกรณ์จัดเก็บข้อมูลออกจากสถานที่
- **การเข้ารหัสฮาร์ดไดรฟ์ (Hard drive encryption):** เข้ารหัสฮาร์ดไดรฟ์ด้วยฮาร์ดแวร์เพื่อเพิ่มความปลอดภัย

ความถูกต้องสมบูรณ์ (Integrity)

หมายถึง การรักษาความถูกต้อง แม่นยำ และครบถ้วนของข้อมูลตลอดกระบวนการ

- ข้อกำหนดเกี่ยวกับการรับส่งข้อมูลทางอิเล็กทรอนิกส์ (Regulation concerning electronic transfer)
    - **การใช้เครือข่ายภายนอก**: อนุญาตให้ใช้เฉพาะเครือข่ายภายนอกที่ปลอดภัย เช่น VPN หรือ leased line
    - **ไฟร์วอลล์ (Firewall):** มีระบบไฟร์วอลล์เพื่อป้องกันการเชื่อมต่อกับระบบไอทีที่ไม่ได้รับอนุญาต

    - **การเข้ารหัสข้อมูล (Data encryption):** มีตัวเลือกในการเข้ารหัสข้อมูลก่อนส่ง (เช่น S-MIME, PGP) และใช้โปรโตคอลที่รองรับการเข้ารหัสขณะส่ง (เช่น SSL, TLS)
    - **การรับรองความถูกต้องของอีเมล (Email authentication):** ใช้การลงลายมือชื่อดิจิทัล (digital signature) เพื่อรับรองความถูกต้องของผู้ส่งอีเมล
- ข้อกำหนดเกี่ยวกับการจัดเก็บข้อมูลบนอุปกรณ์เคลื่อนย้าย (Regulation concerning storage on removable media) เช่น แฟลชไดร์ฟ ฮาร์ดดิสก์แบบพกพา
- ข้อกำหนดเกี่ยวกับการขนยอุปกรณ์จัดเก็บข้อมูล (Regulations concerning the transportation of data storage devices) เช่น ฮาร์ดดิสก์ เทปสำรองข้อมูล
- ข้อกำหนดเกี่ยวกับการกำจัดอุปกรณ์จัดเก็บข้อมูล (Regulations concerning the disposal of data storage devices)

ความพร้อมใช้งานและความยืดหยุ่น/ความสามารถในการกู้คืน (Availability and resilience/recoverability)

- **การสร้างและเก็บรักษาข้อมูลสำรอง (Creation and safekeeping of backups):** มีการสำรองข้อมูลอย่างสม่ำเสมอและเก็บรักษาข้อมูลสำรองไว้ในสถานที่ปลอดภัย
- **การรักษาความปลอดภัยของการดำเนินงานประจำวัน (Safeguarding of day-to-day operations):** มีมาตรการป้องกันความเสี่ยงที่อาจส่งผลกระทบต่อการดำเนินงานประจำวัน
- **ความยืดหยุ่น (Resilience - Operational availability):** ระบบไอทีสามารถใช้งานได้แม้เกิดเหตุการณ์ไม่คาดคิด เช่น ไฟฟ้าดับ
- **ระบบไฟฟ้าสำรอง (Uninterruptible power supply - UPS):** มีระบบไฟฟ้าสำรองกรณีไฟฟ้าดับ
- **ระบบป้องกันอัคคีภัย (Fire protection):** มีระบบป้องกันอัคคีภัยในสถานที่เก็บรักษาข้อมูล
- **ระบบปรับอากาศ (Air-Conditioning):** มีระบบปรับอากาศเพื่อควบคุมอุณหภูมิในสถานที่เก็บรักษาข้อมูล
- **การเชื่อมต่ออินเทอร์เน็ต (Internet connection):** มีการสำรองระบบอินเทอร์เน็ตเพื่อป้องกันกรณีการเชื่อมต่อหลักขัดข้อง
- **แผนการสำรองข้อมูล (Data Backup Operation):** มีแผนการสำรองข้อมูลที่ชัดเจน
- **การบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management - BCM):** มีกระบวนการบริหารจัดการความต่อเนื่องทางธุรกิจเพื่อให้ธุรกิจสามารถดำเนินงานได้แม้เกิดภัยพิบัติ

ความปลอดภัยโครงสร้างพื้นฐาน (Infrastructure Security)

คือ การรักษาความปลอดภัยของระบบเครือข่าย ฮาร์ดแวร์ และซอฟต์แวร์ที่เป็นพื้นฐานในการทำงานขององค์กร

การรักษาความปลอดภัยอุปกรณ์เครือข่าย (Security of Network Equipment)

- **การซิงโครไนส์เวลา (Time synchronization):**
  - ใช้แหล่งที่มาของเวลามากกว่าหนึ่งแหล่ง
  - ใช้ NTP (Network Time Protocol) สำหรับอุปกรณ์เลเยอร์ 3 ทั้งหมดเพื่อซิงโครไนส์เวลา
  - ใช้การรับรองความถูกต้องของ NTP ระหว่างไคลเอ็นต์ เซิร์ฟเวอร์ และเพียร์ เพื่อให้แน่ใจว่าเวลามีการซิงโครไนส์กับเซิร์ฟเวอร์ที่ได้รับอนุญาตเท่านั้น
- **การบันทึกเหตุการณ์ (Event Logging):**
  - กำหนด ACL (Access Control List) สำคัญเพื่อบันทึกการละเมิดการเข้าถึง
  - ตัวอย่าง: การละเมิดการสวมรอย, ความพยายามเข้าถึงพอร์ตคอนโซล, การละเมิดตัวกรองเราเตอร์, ICMP, HTTP, SNMP ฯลฯ
- **การควบคุมการเข้าถึงทางกายภาพ (Physical Access Control):**
  - พอร์ตการเข้าถึงเฉพาะสำหรับการจัดการ
    - พอร์ตคอนโซล, พอร์ตเสริม, พอร์ต VTY (Virtual TTY)
  - I/F (Interface) การตรวจสอบเฉพาะสำหรับ SNMP
    - ใช้ SNMPv3 หรือ SNMPv2c, ไม่มี community string เริ่มต้น
    - สำหรับ SNMPv2c ให้ถือว่า community string เป็น "รหัสผ่าน"
- **การควบคุมการเข้าถึงทางตรรกะ (Logical Access Control):**
  - ตั้งค่ารหัสผ่านและระดับสิทธิ์
  - นำระบบ AAA (Authentication, Authorization & Accountability) มาใช้
  - ใช้วิธีการรับรองความถูกต้องและอนุญาตแบบรวมศูนย์: TACACS+ หรือ RADIUS

ไฟร์วอลล์ (Firewalls)

เป็นระบบรักษาความปลอดภัยเครือข่าย ทำหน้าที่ควบคุมการรับส่งข้อมูลระหว่างเครือข่ายภายในกับเครือข่ายภายนอก ช่วยป้องกันการโจมตีและการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

ไฟร์วอลล์มีหลายประเภท ดังนี้:

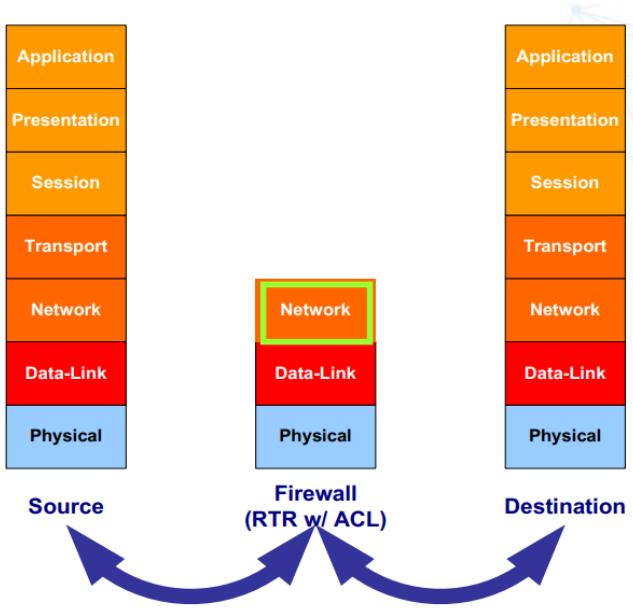
- **ไฟร์วอลล์กรองแพ็กเก็ต (Packet-filtering firewall):**
    - ตรวจสอบข้อมูลส่วนหัว (header) ของแพ็กเก็ตข้อมูลเท่านั้น เช่น ที่อยู่ IP ต้นทางและปลายทาง พอร์ตต้นทางและปลายทาง
    - ไม่สามารถตรวจสอบข้อมูลภายในแพ็กเก็ต (Layer 4-7)
    - ดังนั้น จึงไม่สามารถป้องกันการโจมตีที่มุ่งเป้าไปยังแอปพลิเคชันเฉพาะเจาะจงได้
- **ไฟร์วอลล์พร็อกซี่ (Proxy firewall):**
    - ทำหน้าที่เป็นตัวกลางในการรับส่งข้อมูลระหว่างไคลเอ็นต์และเซิร์ฟเวอร์
    - รองรับโปรโตคอล IP ที่เลือกไว้ (เช่น DNS, Finger, FTP, HTTP, LDAP, NNTP, SMTP, Telnet)
    - สำหรับโปรโตคอลมัลติคาสต์ (PIM, IGMP ฯลฯ) ต้องสร้างอุโมง (TUNNEL) ผ่านไฟร์วอลล์
    - ข้อจำกัด:
        - ใช้ทรัพยากรค่อนข้างเยอะ
        - ไม่รองรับทุกโปรโตคอล
- **ไฟร์วอลล์ตรวจสอบสถานะ (Stateful inspection firewall):**
    - ตรวจสอบทั้งส่วนหัวและข้อมูลภายในแพ็กเก็ต (Layer 4)
    - ทำงานได้เร็วกว่าไฟร์วอลล์พร็อกซี่และมีความยืดหยุ่นมากกว่า เนื่องจากตรวจสอบโปรโตคอล TCP/IP ไม่ใช่แค่ข้อมูลภายใน
    - ไม่ได้เขียนทับทุกแพ็กเก็ตข้อมูล และไม่สื่อสารแทนเซิร์ฟเวอร์ของแอปพลิเคชัน
- **ไฟร์วอลล์ไฮบริด (Hybrid Firewalls):**
    - เป็นการผสมผสานเทคโนโลยีของไฟร์วอลล์ประเภทต่างๆ เข้าด้วยกัน
- **ไฟร์วอลล์พร็อกซี่ระดับวงจร (Circuit-level proxy firewall):**
    - ใช้โปรโตคอล SOCKS (RFC 1928) สร้างวงจรการสื่อสารที่ปลอดภัยระหว่างไคลเอ็นต์และเซิร์ฟเวอร์
    - ไม่จำเป็นต้องรู้จักบริการเครือข่าย (ไม่สามารถควบคุมแอปพลิเคชันเฉพาะเจาะจงได้)
    - รองรับการรับรองความถูกต้องของผู้ใช้
- **ไฟร์วอลล์พร็อกซี่แอปพลิเคชัน (Application proxy firewall):**
    - เป็นการผสมผสานระหว่างไฟร์วอลล์พร็อกซี่และไฟร์วอลล์ตรวจสอบสถานะ

- ต้องใช้พร็อกซี่ที่แตกต่างกันสำหรับแต่ละบริการ
- รองรับการรับรองความถูกต้องของผู้ใช้สำหรับแต่ละบริการที่รองรับ
- ตัวอย่าง: Checkpoint Firewall-1 NG

ไฟร์วอลล์กรองแพ็กเก็ต (Packet-filtering firewalls)

ไฟร์วอลล์กรองแพ็กเก็ต (Packet-filtering firewall) หรือที่เรียกว่า ACL ของเราเตอร์ ทำหน้าที่ตรวจสอบส่วนหัว (header) ของแพ็กเก็ตข้อมูลที่เข้าออกเครือข่าย

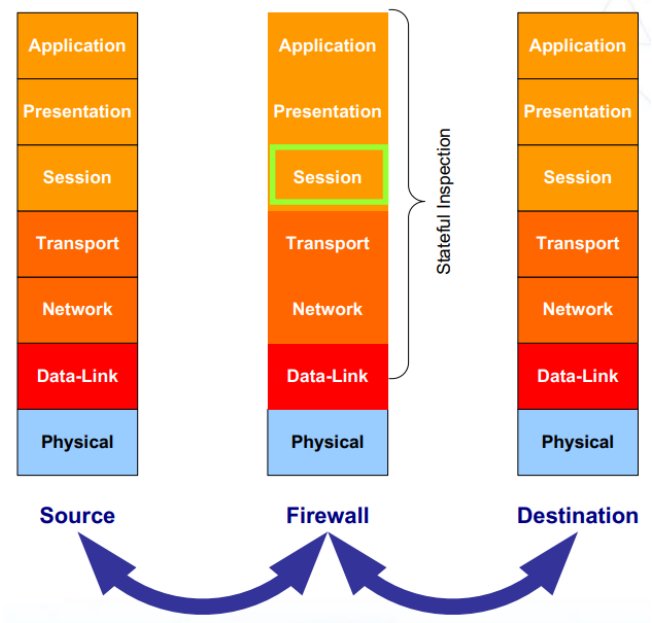
- **นโยบายการทำงานของไฟร์วอลล์ (Firewall Policy):** ปฏิเสธตามค่าเริ่มต้น อนุญาตเป็นข้อยกเว้น (Deny by default, Permit by exception)
  - คือ บล็อกการรับส่งข้อมูลทั้งหมดไว้ก่อน
  - ต้องสร้างกฎ (rule) เพื่ออนุญาตการรับส่งข้อมูลที่ต้องการเท่านั้น
- **วิเคราะห์การไหลของข้อมูล (Data-flow):** วิศวกรรักษาความปลอดภัยเครือข่ายต้องเข้าใจการไหลของข้อมูล เช่น ต้นทาง ปลายทาง โพรโตคอล และวิธีการกำหนดเส้นทาง เพื่อที่จะสามารถกำหนดกฎการกรอง IP ได้อย่างถูกต้อง
  - จำเป็นต้องรู้ทั้งการรับเข้า (Inbound) และการส่งออก (Outbound)
- **ปิดใช้งานโปรโตคอลและบริการที่ไม่จำเป็น (Disable all unnecessary protocols & services):** อนุญาตเฉพาะโปรโตคอลและบริการที่จำเป็นเท่านั้นเพื่อลดช่องโหว่



ไฟร์วอลล์ตรวจสอบสถานะ (Stateful inspection firewalls)

ไฟร์วอลล์ตรวจสอบสถานะ (Stateful inspection firewall) จะตรวจสอบทั้งส่วนหัวและข้อมูลภายในแพ็กเก็ต (Layer 4)

- **รองรับบริการที่ใช้ TCP/IP ทั้งหมด รวมถึง UDP (บางรุ่น):** รองรับการตรวจสอบบริการต่างๆ ที่ใช้ TCP/IP
- **ตรวจสอบสถานะของแพ็กเก็ต (Tracks state of packets):** ติดตามสถานะการเชื่อมต่อของแต่ละแพ็กเก็ต ทำให้ทำงานได้รวดเร็วและมีประสิทธิภาพสูง
- **อนุญาตการเชื่อมต่อ TCP/IP โดยตรงระหว่างโฮสต์ภายในและไคลเอ็นต์ภายนอก (Direct TCP/IP sessions):** อนุญาตให้คอมพิวเตอร์ภายในเครือข่ายติดต่อกับคอมพิวเตอร์ภายนอกได้โดยตรง
- **ไม่รองรับการรับรองความถูกต้องของผู้ใช้ (No user authentication):** ไม่ได้มีการตรวจสอบสิทธิ์ของผู้ใช้

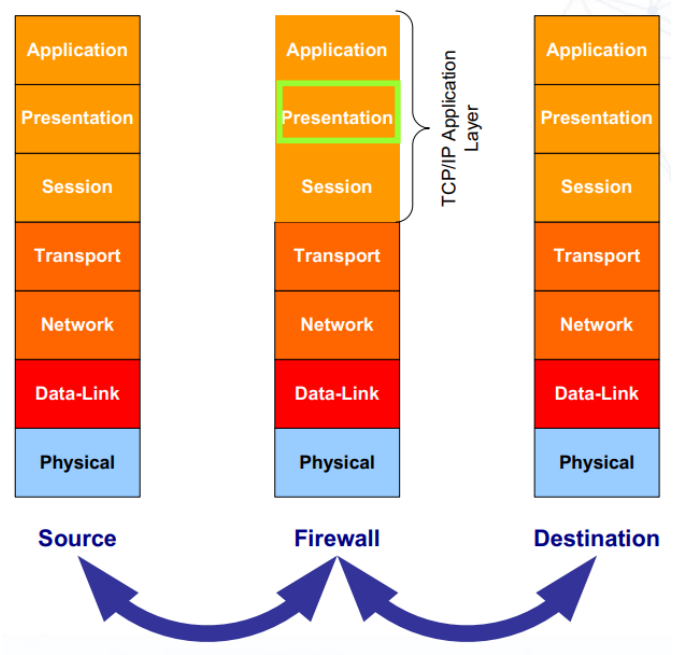


ไฟร์วอลล์พร็อกซี่ (Proxy firewalls)

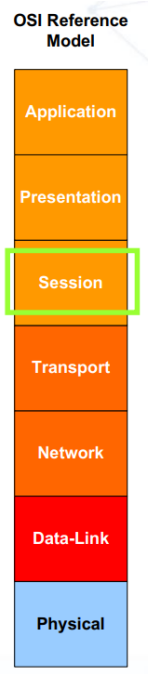
ไฟร์วอลล์พร็อกซี่ ทำหน้าที่เป็นตัวกลางในการรับส่งข้อมูลระหว่างไคลเอ็นต์ภายในและเซิร์ฟเวอร์ภายนอก

- **ไม่อนุญาตให้มีการเชื่อมต่อโดยตรงระหว่างโฮสต์คอมพิวเตอร์ภายในและภายนอก (No direct connections):** คอมพิวเตอร์ภายในเครือข่ายจะไม่สามารถติดต่อกับคอมพิวเตอร์ภายนอกโดยตรง ต้องติดต่อผ่านไฟร์วอลล์พร็อกซี่เท่านั้น

- **วิเคราะห์คำสั่งของแอปพลิเคชันภายในข้อมูล (Analyze application commands):** สามารถวิเคราะห์คำสั่งของแอปพลิเคชันที่อยู่ภายในแพ็กเก็ตข้อมูลได้
- **รองรับการรับรองความถูกต้องระดับผู้ใช้ (User-level authentications):** สามารถตรวจสอบสิทธิ์ของผู้ใช้ได้
- **บันทึกข้อมูลการรับส่งข้อมูล (Traffic logs):** สามารถบันทึกข้อมูลการรับส่งข้อมูลและกิจกรรมของผู้ใช้ได้อย่างละเอียด



นโยบายการทำงานของไฟร์วอลล์ (Firewall Policy)

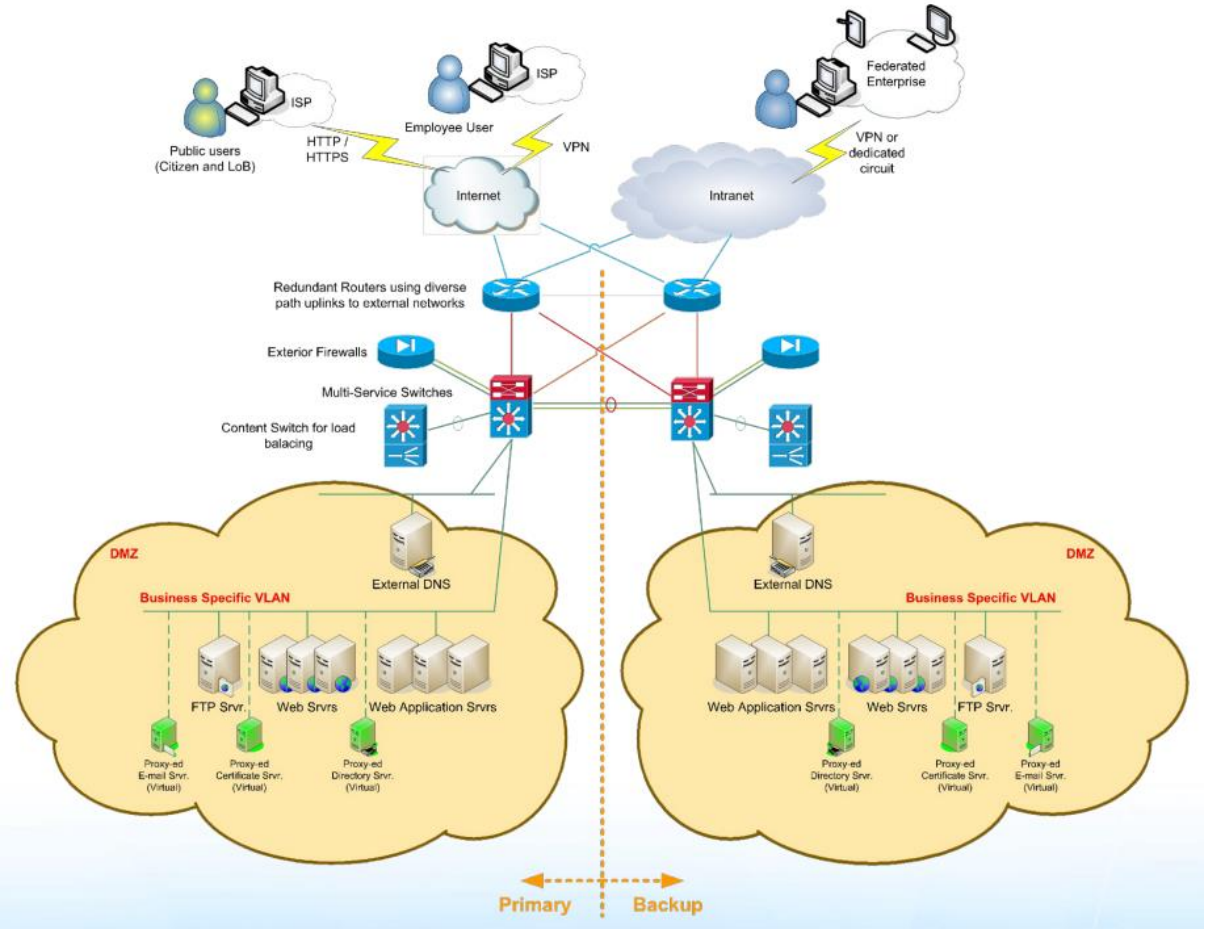


โดยทั่วไป ไฟร์วอลล์จะมีการทำงาน 3 รูปแบบ:

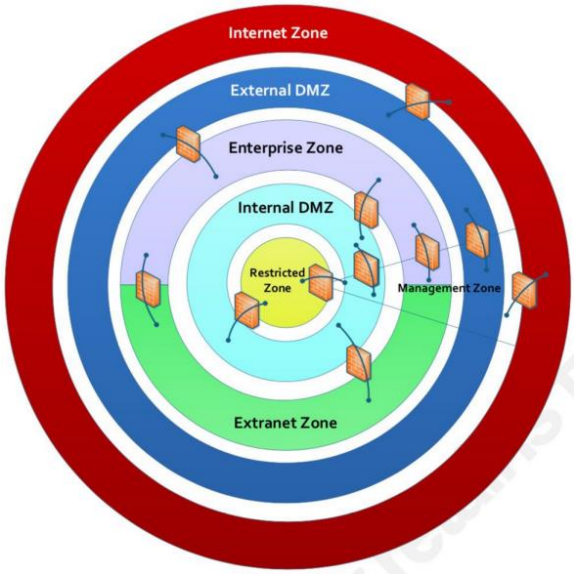
- **อนุญาต (Accept):** อนุญาตให้แพ็กเก็ตข้อมูลผ่านตามกฎที่กำหนดไว้
- **ยกเลิก (Drop):** ยกเลิกการรับส่งข้อมูล โดยไม่แจ้งข้อผิดพลาดกลับไปยังผู้ส่ง (เหมือนกับ "หลุมดำ")
- **ปฏิเสธ (Reject):** ยกเลิกการรับส่งข้อมูล และแจ้งข้อผิดพลาดกลับไปยังผู้ส่ง (มีการบันทึก Log)

การออกแบบเครือข่ายกับไฟร์วอลล์ (Network Design with Firewalls)

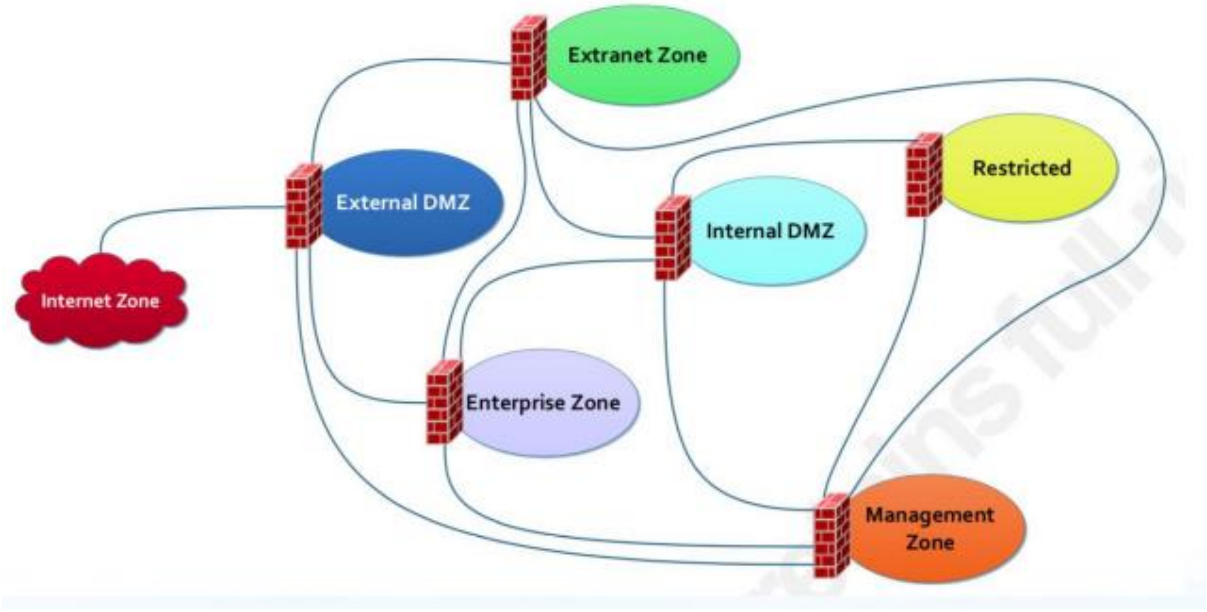
การออกแบบเครือข่ายให้ปลอดภัย โดยแบ่งเป็นโซน (Zone) ต่างๆ และใช้ไฟร์วอลล์ในการควบคุมการรับส่งข้อมูลระหว่างโซน



โซนความปลอดภัยของเครือข่าย (Network Security Zones)



- **Internet Zone - ไม่น่าเชื่อถือ (No Trust):** มักประกอบด้วยอินเทอร์เน็ต เครือข่ายโทรศัพท์สลับสาธารณะ (PSTN) และเครือข่ายแกนหลักสาธารณะของผู้ให้บริการอินเทอร์เน็ต (ISP)
- **External DMZ - ความน่าเชื่อถือต่ำ (Low Trust):**
    - สำหรับระบบที่จำเป็นต้องเชื่อมต่อกับอินเตอร์เน็ต
    - โซนนี้ทำหน้าเป็นพร็อกซี่ ควบคุมการเข้าถึงระหว่างระบบในโซนองค์กร (Enterprise Zone) และอินเตอร์เน็ต
        - Web servers ภายนอก
        - E-mail gateways
        - FTP servers
        - Web proxy servers
        - Remote access services
- **Enterprise Zone - ความน่าเชื่อถือปานกลาง (Medium Trust):**
    - สำหรับระบบของผู้ใช้ทั่วไป เช่น คอมพิวเตอร์ เครื่องพิมพ์ และโทรศัพท์ VoIP
    - ระบบรักษาความปลอดภัยของอุปกรณ์ (Endpoint protection) เป็นสิ่งสำคัญของโซนนี้ในการป้องกันมัลแวร์ต่างๆ
- **Extranet Zone - ความน่าเชื่อถือปานกลาง (Medium Trust):**
    - สำหรับการเชื่อมต่อกับบุคคลที่สามที่ไม่ได้อยู่ในองก์กรณ์เรา แต่เป็นพันธมิตรทางธุรกิจ (3rd party) ที่เราต้องเชื่อมต่อด้วย
    - อาจเป็นการขยายของโซนองค์กรที่เพิ่มขึ้นมา
    - ควรมีการตรวจสอบและกรองปริมาณข้อมูลที่รับส่งระหว่าง Enterprise Zone และ Extranet Zone เพื่ออนุญาตเฉพาะการรับส่งข้อมูลที่ได้รับอนุมัติแล้วเท่านั้น
- **Internal DMZ - ความน่าเชื่อถือสูง (High Trust):**
    - ควบคุมการเข้าถึงระหว่างระบบใน Enterprise/Extranet Zones และ Restricted Zone
    - เซิร์ฟเวอร์ภายในขององค์กรมักจะอยู่ในโซนนี้
    - ผู้ใช้จะต้องได้รับอนุญาตก่อนจึงจะเข้าถึงข้อมูลที่เก็บอยู่ในโซนที่เข้มงวด
- **Management Zone - ความน่าเชื่อถือสูงสุด (Highest Trust):** สำหรับระบบดูแลจัดการและระบบตรวจสอบ เช่น performance servers, configuration management servers, log management servers
- **Restricted Zone - ความน่าเชื่อถือสูงสุด (Highest Trust):** สำหรับระบบที่ต้องการความปลอดภัยสูงสุด



เว็บแอปพลิเคชันไฟร์วอลล์ (Web Application Firewall: WAF) คืออะไร

เว็บแอปพลิเคชันไฟร์วอลล์ (WAF) คือ ซอฟต์แวร์หรือฮาร์ดแวร์ที่ช่วยปกป้องเว็บแอปพลิเคชันของเราจากภัยคุกคามและการโจมตีต่างๆ

- WAF จะวิเคราะห์การป้องกันเว็บแอปพลิเคชันที่เลเยอร์แอปพลิเคชัน (Layer 7) ซึ่งรวมถึงการติดต่อ HTTP และ HTTPS ของเว็บแอปพลิเคชันของเรา XML/SOAP และเว็บเซอร์วิส
- WAF สามารถตรวจจับและป้องกันภัยคุกคามยอดนิยม 10 อันดับ (OWASP Top Ten Threats)
- WAF บางตัวสามารถเรียนรู้เกี่ยวกับเว็บแอปพลิเคชันที่มันปกป้องอยู่ได้

WAF แตกต่างจากระบบป้องกันความปลอดภัยอื่นอย่างไร

- **ไฟร์วอลล์แบบดั้งเดิม (รุ่นแรก):**
    - เน้นการตรวจสอบสถานะ (Stateful inspection) และการทำงานเป็นพร็อกซี่ (Proxy)
    - มีประสิทธิภาพในการตรวจสอบการรับส่งข้อมูลขาออก (Outbound) และอินเทอร์เน็ต
    - แต่มีประสิทธิภาพในการป้องกันเว็บเซิร์ฟเวอร์ขาเข้า (Inbound) ค่อนข้างต่ำ
- **Next Generation Firewalls (NGFW):**
    - เน้นการตรวจสอบลายเซ็นของข้อมูลประเภทแอปพลิเคชัน ซึ่งทำงานได้ดีสำหรับการรับส่งข้อมูลขาออก (Outbound) และอินเทอร์เน็ต
    - แต่มีประสิทธิภาพในการป้องกันเว็บเซิร์ฟเวอร์ขาเข้า (Inbound) ค่อนข้างต่ำ

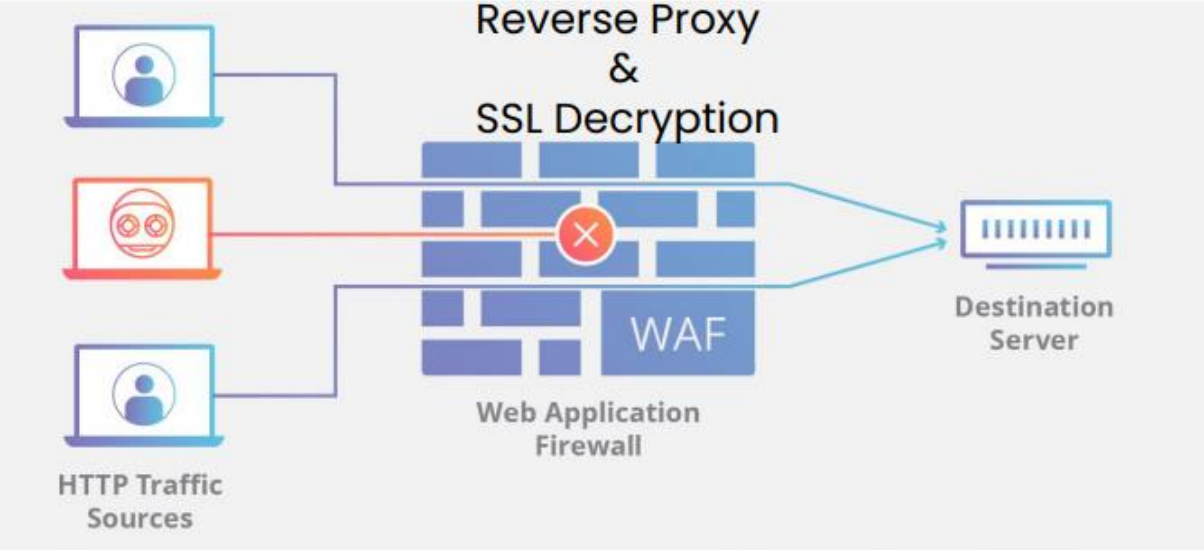
- **ระบบตรวจจับและป้องกันการบุกรุกเครือข่าย (Network IDS/IPS):**
    - รองรับการตรวจสอบเครือข่ายที่หลากหลาย เช่น TCP/IP
    - เน้นการตรวจสอบแบบกว้างๆ
    - มักใช้การขยายฐานข้อมูลลายเซ็นเพื่อให้เข้าใจ HTTP ได้ดียิ่งขึ้น
    - ส่วนใหญ่ใช้การตรวจจับจากลายเซ็น
    - ไม่สามารถรับรู้ผู้ใช้หรือเซสชัน

คุณสมบัติหลักของเว็บแอปพลิเคชันไฟร์วอลล์ (WAF)

- รองรับโปรโตคอล HTTP
- รองรับ XML/SOAP
- ป้องกันการหลีกเลี่ยงการตรวจจับ (Anti-evasion)
- การถอดรหัสและตรวจสอบ SSL
- การถอดรหัสและการกำหนดเส้นทางให้เป็นมาตรฐาน (Path)
- Signatures
    - การโจมตีทั่วไป (การท่องเว็บไดเรกทอรี, เว็บสคริปต์ CGI, เว็บสคริปต์ PHP)
    - ช่องโหว่ที่ทราบของเว็บแอปพลิเคชัน (ช่องโหว่ของเว็บแอปพลิเคชันที่กำหนดโดย CVE, วิ Wikis, phpmyexplorer)
- เครื่องมือการกำหนดนโยบาย (Policy engine)
- การแจ้งเตือนและการตรวจสอบ (Alert / Auditing)

ปัญหาเกี่ยวกับการรักษาความปลอดภัยของเว็บแอปพลิเคชันไฟร์วอลล์ (WAF)

- ความซับซ้อนที่เพิ่มขึ้นของโครงสร้างพื้นฐานด้านไอที (Yet-another-proxy argument)
- ประสิทธิภาพของเว็บแอปพลิเคชัน
- ค่าผิดพลาดเชิงบวก (False positives)
- การแก้ไขปัญหาที่ซับซ้อนมากขึ้น
- ผลกระทบที่อาจเกิดขึ้นกับเว็บแอปพลิเคชันหาก WAF ยุติการทำงานของเซสชันแอปพลิเคชัน
- คุ้มค่ากับต้นทุนหรือไม่ (Cost-effectiveness)



การวางตำแหน่งไฟร์วอลล์บนเว็บแอปพลิเคชันโดยทั่วไป

ระบบตรวจจับและป้องกันการบุกรุก

(Intrusion Detection and Prevention System)

ระบบตรวจจับและป้องกันการบุกรุกเป็นระบบรักษาความปลอดภัยเครือข่ายที่มี 2 ประเภทหลักๆ ได้แก่

- **ระบบตรวจจับการบุกรุก (Intrusion Detection System: IDS):** เป็นระบบแบบ "passive"
    - ทำหน้าที่ตรวจจับการโจมตีและการละเมิดความปลอดภัยอื่นๆ
    - ตรวจจับและรับมือกับสัญญาณเบื้องต้นของการโจมตี (เช่น การสแกนหาช่องโหว่)
    - บันทึกข้อมูลเกี่ยวกับภัยคุกคาม เพื่อช่วยในการวินิจฉัย กู้คืนระบบ และแก้ไขปัญหาการบุกรุกที่ไม่ได้รับอนุญาต
- **ระบบป้องกันการบุกรุก (Intrusion Prevention System: IPS):** เป็นระบบแบบ "in-line"
    - มีคุณสมบัติเหมือนกับระบบ N-IDS (Network Intrusion Detection System) และเพิ่มเติมด้วย
    - วิเคราะห์ "พฤติกรรม" ของเครือข่ายเพื่อป้องกันความเสียหายเพิ่มเติม

วิธีการตรวจจับของระบบ IDS/IPS

- **ระบบ N-IDS (และ Host-IDS):** ใช้เทคนิค "ตามฐานข้อมูล" (signature-based) ในการตรวจจับการบุกรุก
    - ใช้ฐานข้อมูลของการโจมตีและช่องโหว่ที่รู้จักกันดีเรียกว่า signatures
    - ประสิทธิภาพขึ้นอยู่กับการอัพเดทฐานข้อมูลลายเซ็น
    - การปรับแต่งระบบอาจทำได้ยาก เนื่องจากอาจมีการแจ้งเตือนผิดพลาด (false positives) และการมองข้ามพฤติกรรมปกติที่อาจเข้าใจผิดเป็นการโจมตี
- **ระบบ N-IPS:** ใช้เทคนิค "ตามพฤติกรรม" (behavior-based) ในการตรวจจับและป้องกันการบุกรุก
    - เรียนรู้พฤติกรรมปกติของเครือข่ายหรือโฮสต์
    - แจ้งเตือนเมื่อมีพฤติกรรมเบี่ยงเบนไปจากปกติ เช่น แพ็กเก็ตที่ผิดรูปแบบ การใช้ทรัพยากรเครือข่ายที่ผิดปกติ หรือการใช้หน่วยความจำผิดปกติ

ระบบตรวจจับการบุกรุกเครือข่าย (Network-based Intrusion Detection System: N-IDS)

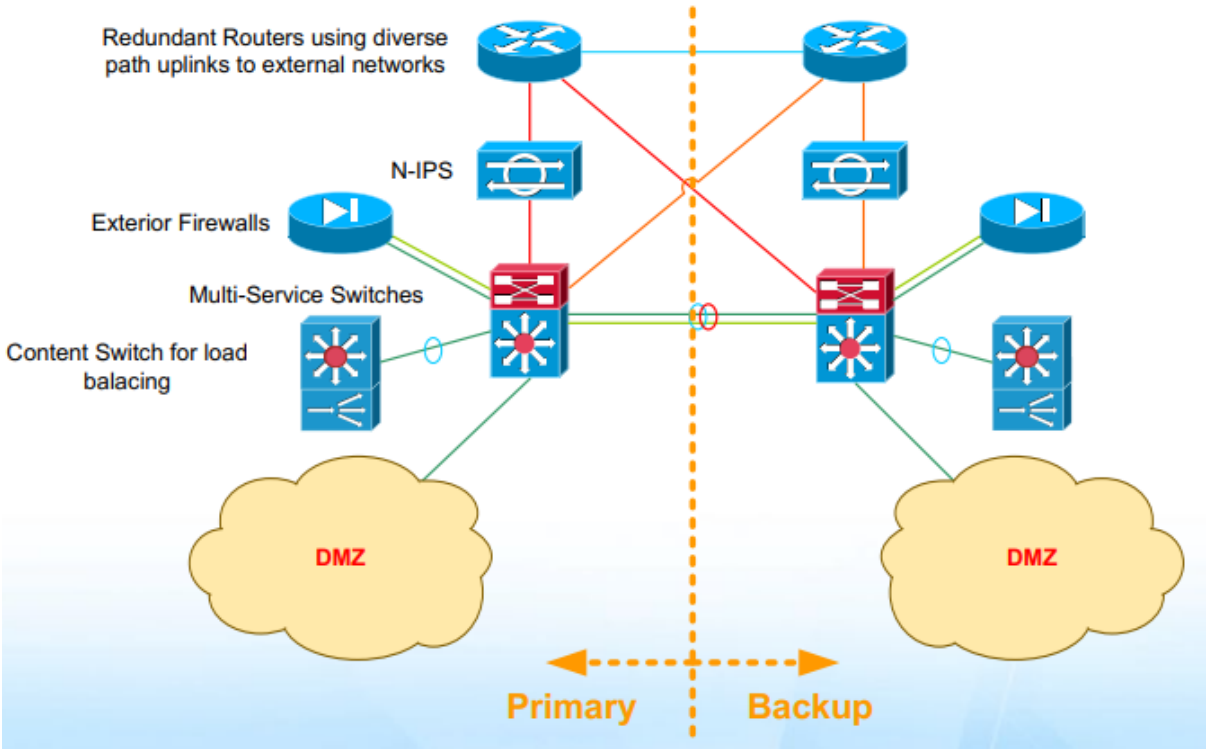
ระบบตรวจจับการบุกรุกเครือข่าย (N-IDS) เป็นระบบรักษาความปลอดภัยแบบ "passive" ที่ทำหน้าที่ตรวจจับพฤติกรรมน่าสงสัยบนเครือข่าย

- **การติดตั้ง N-IDS:** มี 2 วิธีในการติดตั้ง N-IDS เพื่อดักฟังข้อมูลบนเครือข่าย
    - Network TAP: เป็นอุปกรณ์ที่ทำหน้าที่สำเนาข้อมูลเครือข่ายทั้งหมดบนพอร์ตที่เชื่อมต่อ
    - VLAN Port Spanning on L2 switch: เป็นการกำหนดให้ switch คัดลอกข้อมูลจาก Port ต้นทางไปยัง Port ปลายทางที่ติดตั้ง N-IDS
- **การทำงานของ N-IDS:** N-IDS ประกอบด้วย 2 ส่วนหลัก
    - Sensor (Pre-processor): ทำหน้าที่รวบรวมและประมวลผลแพ็กเก็ตข้อมูลที่ดักฟังได้
    - Event Collector/Analyzer: ทำหน้าที่เก็บรวบรวม Event จาก Sensor ทั้งหมด มาวิเคราะห์และแสดงรูปแบบของการโจมตี
    - Sensor จะทำการเปรียบเทียบแพ็กเก็ตข้อมูลกับฐานข้อมูลลายเซ็น (Signatures) ของการโจมตีที่มักจะรู้จักบ่อยๆอยู่แล้ว
    - ฐานข้อมูลลายเซ็นนี้จึงจำเป็นต้องได้รับการอัพเดทอยู่เสมอเพื่อประสิทธิภาพในการตรวจจับ

ระบบป้องกันการบุกรุกเครือข่าย (Network-based Intrusion Prevention System: N-IPS)

ระบบป้องกันการบุกรุกเครือข่าย (N-IPS) เป็นระบบรักษาความปลอดภัยแบบ "in-line" ที่ทำหน้าที่ตรวจจับและป้องกันการโจมตีได้ทันที

- **การทำงานของ N-IPS:** N-IPS จะตรวจสอบการรับส่งข้อมูลบนเครือข่ายหลัก
    - สามารถบล็อกการรับส่งข้อมูลที่ไม่พึงประสงค์หรือเป็นอันตรายได้โดยอัตโนมัติ
    - ข้อควรระวัง: ระบบ N-IPS อาจบล็อกการรับส่งข้อมูลปกติขององค์กรได้ ดังนั้นควรติดตั้งระบบ N-IPS ระหว่างเราเตอร์ขอบเครือข่าย (Edge Router) กับไฟร์วอลล์ด้านนอก



ความปลอดภัยของระบบคลาวด์ (Cloud Security)

ระบบคลาวด์ (Cloud Computing) เปรียบเหมือนการใช้คอมพิวเตอร์เป็นแบบสาธารณูปโภค เป็นยุคใหม่ของการใช้คอมพิวเตอร์ เทคโนโลยีที่ทำให้ระบบคลาวด์เกิดขึ้นได้แก่

- **กฎของมัวร์ (Moore's Law):** การที่จำนวนทรานซิสเตอร์บนวงจรอัดรวม (IC) จะเพิ่มขึ้นเป็นสองเท่าทุกๆ 2 ปี ส่งผลให้คอมพิวเตอร์มีประสิทธิภาพมากขึ้นและราคาถูกลง
- **การเชื่อมต่ออันทรงพลัง (Hyperconnectivity):** การเชื่อมต่ออินเตอร์เน็ตความเร็วสูงที่เข้าถึงได้ง่าย
- **สถาปัตยกรรมแบบบริการเชิงบริการ (Service-Oriented Architecture: SOA):** รูปแบบการออกแบบซอฟต์แวร์ที่แยกแต่ละส่วนออกเป็นบริการย่อยๆ ที่สามารถนำมาประกอบกันได้อย่างยืดหยุ่น
- **การประหยัดขนาด (Provider scale):** ผู้ให้บริการระบบคลาวด์มีศูนย์ข้อมูลขนาดใหญ่ ทำให้สามารถให้บริการได้อย่างคุ้มค่า

คุณสมบัติสำคัญของระบบคลาวด์

- **ยืดหยุ่นและตามความต้องการ (Elastic & on-demand):** ผู้ใช้สามารถปรับขนาดการใช้งานของระบบคลาวด์ได้ตามความต้องการ
- **มีผู้ใช้หลายราย (Multi-tenancy):** ระบบคลาวด์เดียวสามารถให้บริการแก่ผู้ใช้หลายรายได้ในเวลาเดียวกัน
- **คิดค่าบริการตามการใช้งาน (Metered service):** ผู้ใช้จ่ายค่าบริการตามจริงตามที่ใช้งาน

รูปแบบการให้บริการระบบคลาวด์

- **ระบบคลาวด์สาธารณะ (Public Cloud):**
    - ให้บริการโดยผู้ให้บริการภายนอก (Third-party provider)
    - ใครก็ตามสามารถใช้งานได้ผ่านอินเตอร์เน็ตสาธารณะ
    - มีจุดเด่นที่ความรวดเร็วในการปรับขนาดและความสะดวกในการใช้งาน
- **ระบบคลาวด์ส่วนบุคคล (Private Cloud):**
    - ให้บริการแก่ผู้ใช้ที่ได้รับอนุญาตเท่านั้น
    - อาจเชื่อมต่อผ่านอินเตอร์เน็ตหรือเครือข่ายภายในองค์กร
    - มีจุดเด่นด้านความปลอดภัยที่สามารถควบคุมได้มากกว่า
    - แต่ยังคงต้องมีทีมงานดูแลระบบเหมือนกับการมีศูนย์ข้อมูลเอง

- **ระบบคลาวด์ผสม (Hybrid Cloud):**
    - เป็นการผสมผสานระหว่างระบบคลาวด์สาธารณะและระบบคลาวด์ส่วนบุคคล
    - ความรับผิดชอบด้านความปลอดภัยแบ่งตามการใช้งาน
    - ช่วยให้สามารถควบคุมข้อมูลและกระบวนการสำคัญได้อย่างเคร่งครัด

Cloud Security Alliance (CSA)

Cloud Security Alliance (CSA) เป็นองค์กรไม่แสวงหาผลกำไรระดับโลก

- มีสมาชิกบุคคลกว่า 23,000 คน สมาชิกองค์กร 100 แห่ง และสาขา 50 แห่งทั่วโลก
- มุ่งเน้นการสร้างแนวทางปฏิบัติที่ดีที่สุดและระบบนิเวศน์ระบบคลาวด์ที่น่าเชื่อถือ
- มีแนวคิด Agile เน้นการพัฒนาผลงานวิจัยประยุกต์อย่างรวดเร็ว

ภารกิจหลักของ CSA

- **GRC: บริหารจัดการความเสี่ยง (Risk Management) ควบคู่ไปกับการปฏิบัติตามข้อกำหนด (Compliance):**
  มุ่งเน้นการสร้างสมดุลระหว่างการปฏิบัติตามกฎระเบียบและการบริหารจัดการความเสี่ยง
- **Reference models: การสร้างโมเดลอ้างอิงโดยใช้มาตรฐานที่มีอยู่**: การสร้างโมเดลโดยอาศัยมาตรฐานที่มีอยู่แล้วเพื่อให้เกิดประสิทธิภาพ
- **Identity: พื้นฐานสำคัญของระบบเศรษฐกิจคลาวด์ที่ใช้งานได้**: เน้นย้ำความสำคัญของระบบ Identity Management ที่เป็นพื้นฐานสำคัญ
- **ส่งเสริมการทำงานร่วมกัน (Interoperability):** สนับสนุนการทำงานร่วมกันระหว่างระบบและเทคโนโลยีต่างๆ
- **ส่งเสริมนวัตกรรม (Innovation):** สนับสนุนการสร้างสรรค์เทคโนโลยีและแนวคิดใหม่ๆ
- **ผลักดันนโยบายสาธารณะที่รอบคอบ (Prudent public policy):** ผลักดันให้มีการกำหนดนโยบายภาครัฐที่เหมาะสมกับเทคโนโลยีคลาวด์

ปัญหาความปลอดภัยของระบบคลาวด์ในปัจจุบัน

ข้อมูลจากผลวิจัย Top Threats ของ CSA ชี้ให้เห็นถึงปัญหาความปลอดภัยที่สำคัญ ดังนี้

- **ความน่าเชื่อถือ (Trust):** การขาดความโปร่งใสจากผู้ให้บริการส่งผลต่อการบริหารจัดการ ความเสี่ยง และการปฏิบัติตามข้อกำหนด
- **ข้อมูล (Data):** ความเสี่ยงต่อการรั่วไหล สูญหาย หรือถูกจัดเก็บในพื้นที่ที่ไม่ปลอดภัย
- **ซอฟต์แวร์ระบบคลาวด์ที่ไม่ปลอดภัย**
- **การใช้บริการคลาวด์ในทางที่ผิด**
- **การยึด account หรือ service**
- **ภัยจากภายในองค์กร**
- **การโจมตีระบบคลาวด์โดยเฉพาะ**

คู่มือการรักษาความปลอดภัยระบบคลาวด์จาก CSA

- Popular best practices for securing cloud computing
- Flagship research project
- V2.1 released 12/2009
- V4 released 07/2017
- wiki.cloudsecurityalliance.org/guidance

การรักษาความปลอดภัยของอุปกรณ์ปลายทาง (Endpoint Security)

การรักษาความปลอดภัยของอุปกรณ์ปลายทาง คือ การป้องกันอุปกรณ์ต่างๆ ที่เชื่อมต่อกับเครือข่าย เช่น คอมพิวเตอร์ แล็ปท็อป มือถือ ไม่ให้ถูกโจมตีหรือใช้งานในทางที่ผิด

การควบคุมรักษาความปลอดภัยของเซิร์ฟเวอร์ (เน้นการรักษาความปลอดภัยของเครือข่าย)

- **การรักษาความปลอดภัยระบบปฏิบัติการ (Securing Core OS):** ทำการตั้งค่าระบบปฏิบัติการให้มีความปลอดภัย เช่น การตั้งค่ารหัสผ่านที่แข็งแรง การปิดใช้งานฟีเจอร์ที่ไม่จำเป็น
- **การอัพเดทระบบรักษาความปลอดภัย (Security Update):** ติดตั้งการอัพเดทระบบปฏิบัติการและโปรแกรมต่างๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่
- **จำกัดฟังก์ชันการทำงานของบริการ (Be specific on service functions):**
    - ติดตั้งและเปิดใช้งานเฉพาะบริการที่จำเป็นเท่านั้น
    - เพื่อลดช่องโหว่ที่อาจเกิดจากการติดตั้งบริการที่ไม่จำเป็น
- **ลดช่องโหว่ด้วยการโฟกัสที่ฟังก์ชันการทำงานเดียว (Focus on a single function):**
    - ตัวอย่างเช่น
        - เว็บเซิร์ฟเวอร์: ควรอนุญาตให้ให้บริการหน้าเว็บไซต์เท่านั้น
        - DNS Server: ควรอนุญาตให้ให้บริการ DNS เท่านั้น
        - E-mail Server: ควรอนุญาตให้ให้บริการอีเมลเท่านั้น
        - DB Server: ควรอนุญาตให้ให้บริการฐานข้อมูลเท่านั้น
- **ติดตั้งระบบตรวจจับการบุกรุกโฮสต์ (Host-IDS) และรักษาความปลอดภัยของโปรแกรมของบุคคลภายนอก (Secure 3rd Party Application):**
    - ติดตั้งระบบตรวจจับการบุกรุกโฮสต์เพื่อตรวจสอบกิจกรรมที่ผิดปกติบนอุปกรณ์
    - ดูแลความปลอดภัยของโปรแกรมที่ติดตั้งเพิ่มเติมจากผู้ผลิตอื่น
- **บังคับใช้การจัดการการเปลี่ยนแปลง (CM: Change Management) และการควบคุมการเปลี่ยนแปลง (Change Control):** มีกระบวนการอนุมัติก่อนการเปลี่ยนแปลงระบบต่างๆ เพื่อลดความเสี่ยง
- **ติดตั้งโปรแกรม Antivirus:** เพื่อช่วยสแกนหาและกำจัดไวรัส
- **ปิดใช้งานกระบวนการ/บริการที่ไม่ได้ใช้งาน (Disable all processes/services not in use):** ปิดใช้งานกระบวนการและบริการที่ไม่จำเป็นเพื่อลดช่องโหว่
- **บังคับใช้การควบคุมการเข้าถึงอย่างเคร่งครัด (Enforce strict access control):** อนุญาตให้เข้าถึงระบบเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

Microsoft Windows Security

การโจมตีที่ Microsoft มักจะเจอบ่อยๆ และต้องออกเครื่องมือมาใช้ในการรักษาความปลอดภัย

Attack	Windows 10 protection
Extraction of domain accounts NTLM hashes	Credential Guard
Extraction of local accounts NTLM hashes	**Still possible**
Extraction of clear-text domain passwords for running sessions	Windows 8.1 removed clear-text
Extraction of clear-text local passwords	Windows 8.1 removed clear-text
Extraction of secrets through DMA	Credential Guard (VT-d / IOMMU)
Pass-the-Hash on domain accounts	Credential Guard
Overpass-the-hash	Credential Guard
Pass-the-ticket (TGS)	**Still possible**
Bootkit	Secure Boot (UEFI)
Rootkit loaded before anti-malware solution	ELAM[1] and Device Guard
Malware and unauthorized applications	Device Guard (or AppLocker)
Tampering with whitelisting solution	Device Guard
Tampering with whitelisting ruleset	Device Guard signed ruleset

แนวทางการรักษาความปลอดภัยอื่นๆ

- **DISA STIGs (DISA Security Technical Implementation Guides):** คู่มือความปลอดภัยจากสำนักงานความมั่นคงด้านระบบสารสนเทศของกระทรวงกลาโหมสหรัฐอเมริกา (US Department of Defense)
- **NSA IA Guidance (National Security Agency Information Assurance Guidance):** แนวทางการรักษาความปลอดภัยสารสนเทศจากสำนักงานความมั่นคงแห่งชาติสหรัฐอเมริกา (National Security Agency)
- **The CIS Benchmarks (Center for Internet Security Benchmarks):** ค่ามาตรฐานการตั้งค่าความปลอดภัยจากศูนย์กลางด้านความมั่นคงอินเทอร์เน็ต (Center for Internet Security)

ค่ามาตรฐานความปลอดภัยสำหรับ Member Server

- **การปรับแต่งและใช้งานเทมเพลต:** ปรับแต่งค่าต่างๆ ภายในเทมเพลตให้เหมาะสมกับความต้องการ แล้วนำไปใช้กับ Member Server ทั้งหมด
- **ตัวอย่างค่ามาตรฐานภายในเทมเพลต:**
    - Audit Policy (นโยบายการตรวจสอบระบบ)
    - User Rights Assignment (การกำหนดสิทธิ์ผู้ใช้งาน)
    - Security Options (ตัวเลือกความปลอดภัย)
    - Event Log (บันทึกกิจกรรมระบบ)
    - System Services (บริการระบบ)

การใช้งานเทมเพลตความปลอดภัย

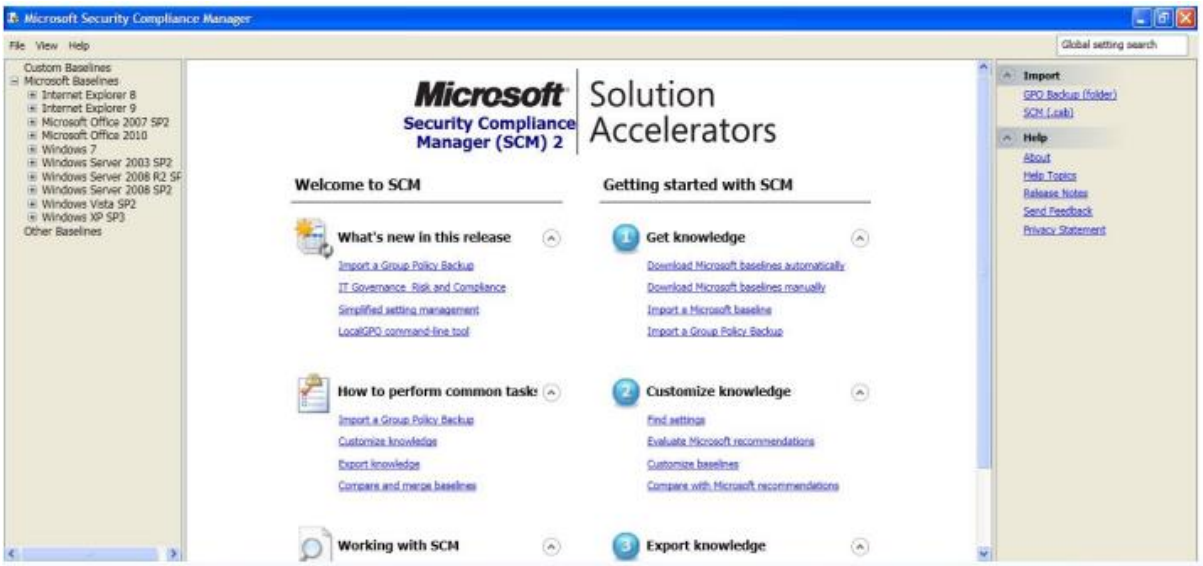
- **ทดสอบก่อนใช้งานจริง:** ควรทดสอบการตั้งค่าความปลอดภัยด้วยเทมเพลตก่อนนำไปใช้จริง
- **วิเคราะห์การตั้งค่าเป็นระยะ:** ควรวิเคราะห์การตั้งค่าความปลอดภัยเป็นระยะๆ ด้วยเครื่องมือ
    - Security Configuration and Analysis snap-in
    - Scripting (Secedit.exe)
- **วิธีการใช้งานเทมเพลต:**
    - Group Policy (Active Directory): สำหรับการตั้งค่าเทมเพลตภายในโดเมน Active Directory
    - Security Configuration and Analysis snap-in: เครื่องมือสำหรับการตั้งค่าและวิเคราะห์ความปลอดภัย
    - Scripting (Secedit.exe): ใช้ Script เพื่อตั้งค่าความปลอดภัยผ่านคำสั่ง

แนวทางปฏิบัติที่ดีสำหรับการใช้เทมเพลตความปลอดภัย

- ตรวจสอบและปรับแต่งค่าต่างๆ ภายในเทมเพลตก่อนใช้งานจริง
- ใช้เครื่องมือวิเคราะห์การตั้งค่าความปลอดภัยก่อนใช้งาน
- ทดสอบเทมเพลตอย่างละเอียดก่อนใช้งานจริง
- จัดเก็บเทมเพลตความปลอดภัยไว้ในสถานที่ที่ปลอดภัย

Security Compliance Manager (เครื่องมือจัดการความปลอดภัย)

- **การจัดการแบบรวมศูนย์และคลังค่ามาตรฐาน:** เครื่องมือ Security Compliance Manager ช่วยในการจัดการค่ามาตรฐานความปลอดภัยต่างๆ แบบรวมศูนย์
- **การปรับแต่งค่ามาตรฐาน:** สามารถปรับแต่งค่ามาตรฐานความปลอดภัยให้เหมาะสมกับความต้องการ
- **การเปรียบเทียบและส่งออกค่ามาตรฐาน:** สามารถเปรียบเทียบค่ามาตรฐานต่างๆ และส่งออกข้อมูลสำหรับการวิเคราะห์
- **การตรวจสอบและยืนยันความสอดคล้องกับค่ามาตรฐาน:** เครื่องมือช่วยในการตรวจสอบว่าระบบปฏิบัติการตั้งค่าความปลอดภัยตามมาตรฐานที่กำหนด



คู่มือการตั้งค่าความปลอดภัย (Security Configuration Guidance)

เกี่ยวกับคู่มือการตั้งค่าความปลอดภัยสำหรับระบบปฏิบัติการ Microsoft Windows ควรดูคู่มือที่จัดทำโดยหน่วยงานต่างๆ ดังนี้

- Microsoft
- Center for Internet Security (CIS)
- National Security Agency (NSA)
- Defense Information Systems Agency (DISA)
- National Institute of Standards and Technology (NIST)

หมายเหตุ: การตั้งค่าตามค่าความปลอดภัยสูงสุดในบางคู่มือ อาจส่งผลต่อการใช้งานของระบบ ดังนั้นควรทดสอบอย่างละเอียดก่อนนำไปใช้จริง

ดูรายละเอียดเพิ่มเติมได้ที่: http://support.microsoft.com/default.aspx?scid=kb;en-us;885409

คู่มือการตั้งค่าความปลอดภัย โดยเพิ่มความแข็งแกร่ง (Hardening Guides)

- **การเพิ่มความแข็งแกร่งระบบปฏิบัติการ (Operating System Hardening)**
    - คู่มือความปลอดภัยสำหรับ Windows Server (Windows Server Security Guide)
        - รวมถึงข้อมูลการเพิ่มความแข็งแกร่งให้เว็บเซิร์ฟเวอร์
- **การเพิ่มความแข็งแกร่งของ Mail Server**
    - คู่มือการเพิ่มความแข็งแกร่งของ Microsoft Exchange Server
- **การเพิ่มความแข็งแกร่งของฐานข้อมูล (Database Hardening)**
    - คุณสมบัติความปลอดภัยและแนวทางปฏิบัติที่ดีสำหรับ SQL Server

การเพิ่มความแข็งแกร่งตามบทบาทของ Server (Hardening Server Roles)

เอกสารแนะนำแนวทางการเพิ่มความแข็งแกร่งตามบทบาทของ Server (Server Roles) โดยทั่วไปแล้วเซิร์ฟเวอร์แต่ละตัวจะมีบทบาทเดียว แต่หากจำเป็นต้องรวมบทบาทเข้าด้วยกัน สามารถปรับแต่งรูปแบบความปลอดภัย เพื่อกำหนดค่าบริการและตัวเลือกความปลอดภัยที่เหมาะสม

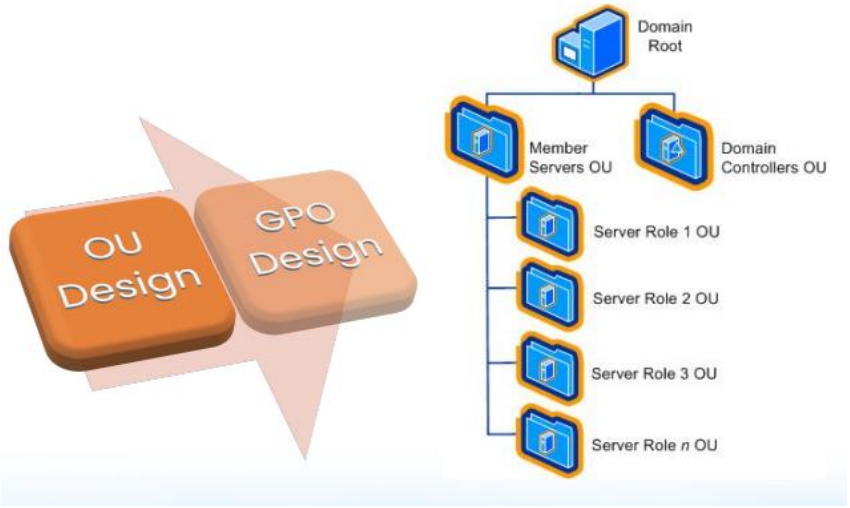
บทบาทของ Windows Server (Windows Server Security Guide) ได้แก่

- ตัวควบคุมโดเมน (Domain controllers)
- เซิร์ฟเวอร์โครงสร้างพื้นฐาน (Infrastructure servers)
- เซิร์ฟเวอร์ไฟล์ (File servers)
- เซิร์ฟเวอร์พิมพ์ (Print servers)
- เซิร์ฟเวอร์บริการสารสนเทศบนอินเทอร์เน็ต (Internet Information Services: IIS)
- เซิร์ฟเวอร์บริการการรับรองความถูกต้องบนอินเทอร์เน็ต (Internet Authentication Services: IAS)
- เซิร์ฟเวอร์บริการใบรับรอง (Certificate Services)
- Bastion Host (เซิร์ฟเวอร์สำหรับป้องกันการโจมตีเครือข่าย)

การใช้ Active Directory เพื่อเพิ่มความปลอดภัย

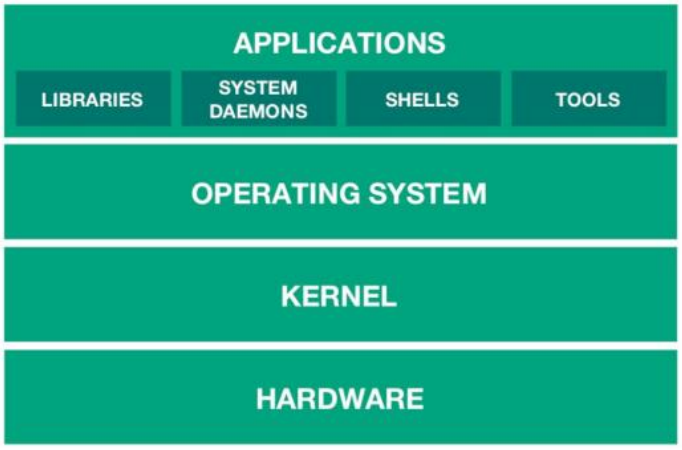
เอกสารแนะนำการใช้ Active Directory เพื่อเพิ่มความปลอดภัย ดังนี้

- ออกแบบโครงสร้าง OU (Organizational Unit) โดยคำนึงถึงความปลอดภัยของไคลเอ็นต์
- ออกแบบลำดับชั้นของ OU เพื่อแยกวัตถุผู้ใช้และคอมพิวเตอร์ตามบทบาท
- ใช้นโยบายกลุ่ม (Group Policy) กับการตั้งค่าความปลอดภัยที่เหมาะสมสำหรับบทบาทของคอมพิวเตอร์แต่ละเครื่อง

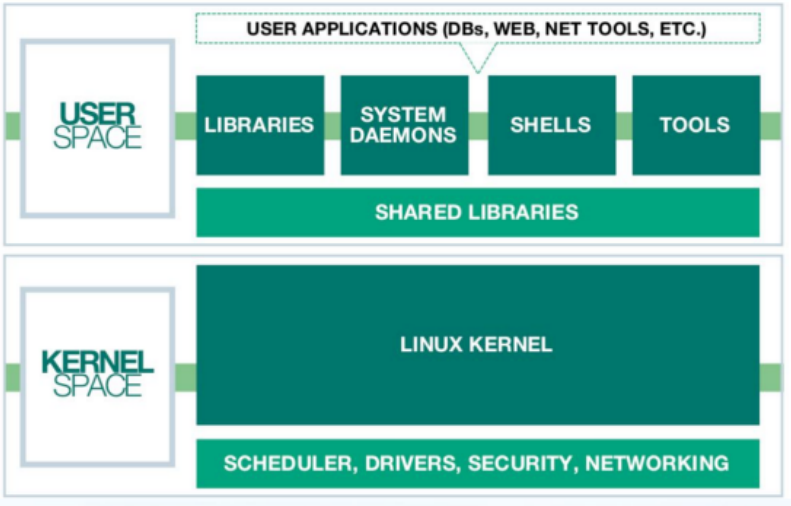


Linux security

โครงสร้างระบบปฏิบัติการ



พื้นที่ Kernel และพื้นที่ User



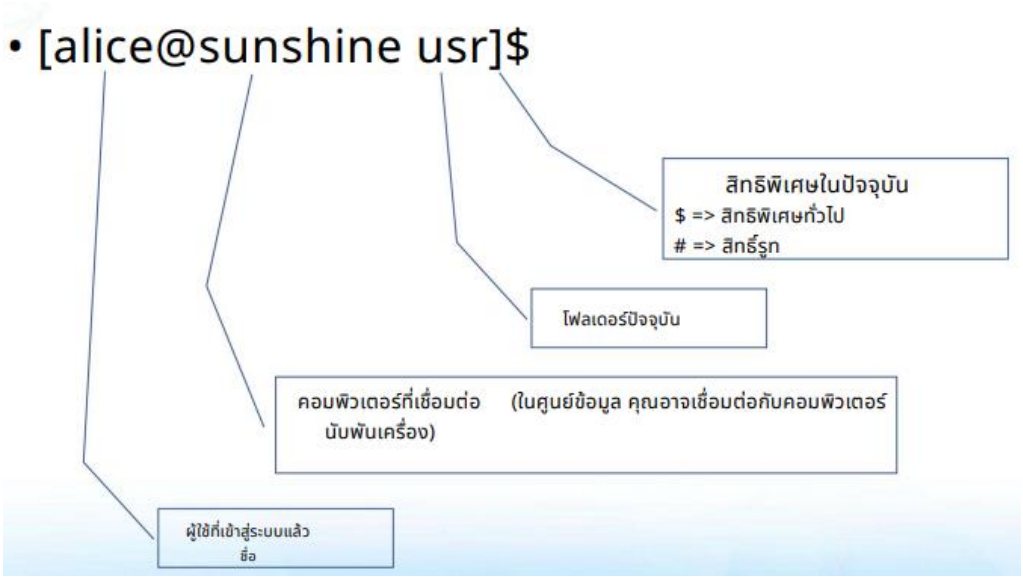
Shell

- Shell เป็นอินเทอร์เฟซหลักสำหรับผู้ดูแลระบบ (System Administrator)
- ช่วยให้เข้าถึงโครงสร้างของระบบปฏิบัติการโดยตรง (Direct access to OS structures)
- คำสั่งภายใน Shell มักใช้ภาษาอังกฤษง่ายๆ (Plain English)
- Shell เหมาะสำหรับการทำงานบนระบบเครือข่ายที่มีแบนด์วิธจำกัด
- รองรับการเขียนสคริปต์ (Scripting) เพื่อทำงานอัตโนมัติ

เปรียบเทียบ Shell กับระบบปฏิบัติการอื่นๆ

- **Windows:** PowerShell ทำหน้าที่คล้ายกับ Shell ใน Linux แต่เป็นโปรแกรมแยกต่างหาก
    - เพิ่งถูกนำมาใช้ในระบบปฏิบัติการ Windows 7 และ Windows Server 2008
- **Unix:** Shell พร้อมใช้งานตั้งแต่เริ่มต้นระบบ (Ready on OS start-up)
    - สามารถเข้าถึงเปลือกของระบบ Unix ได้ง่ายจากระบบ Windows

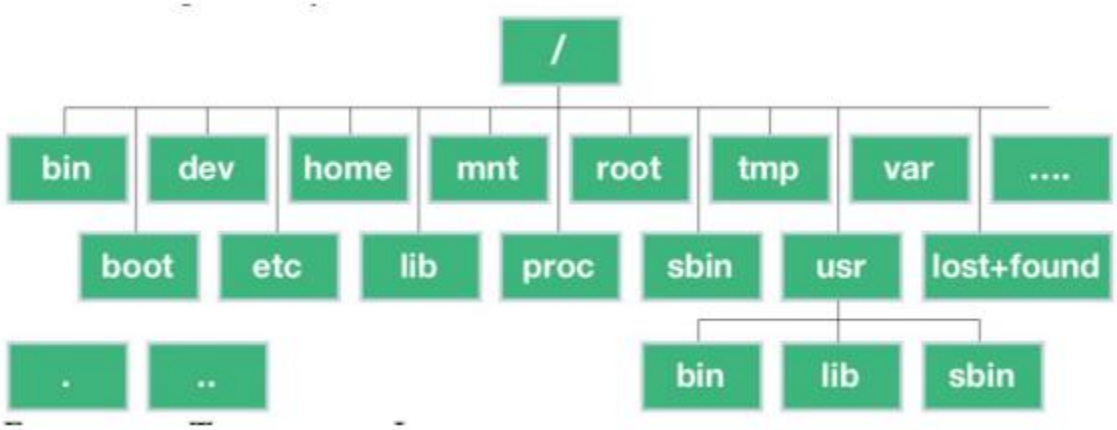
การเข้า Bash prompt



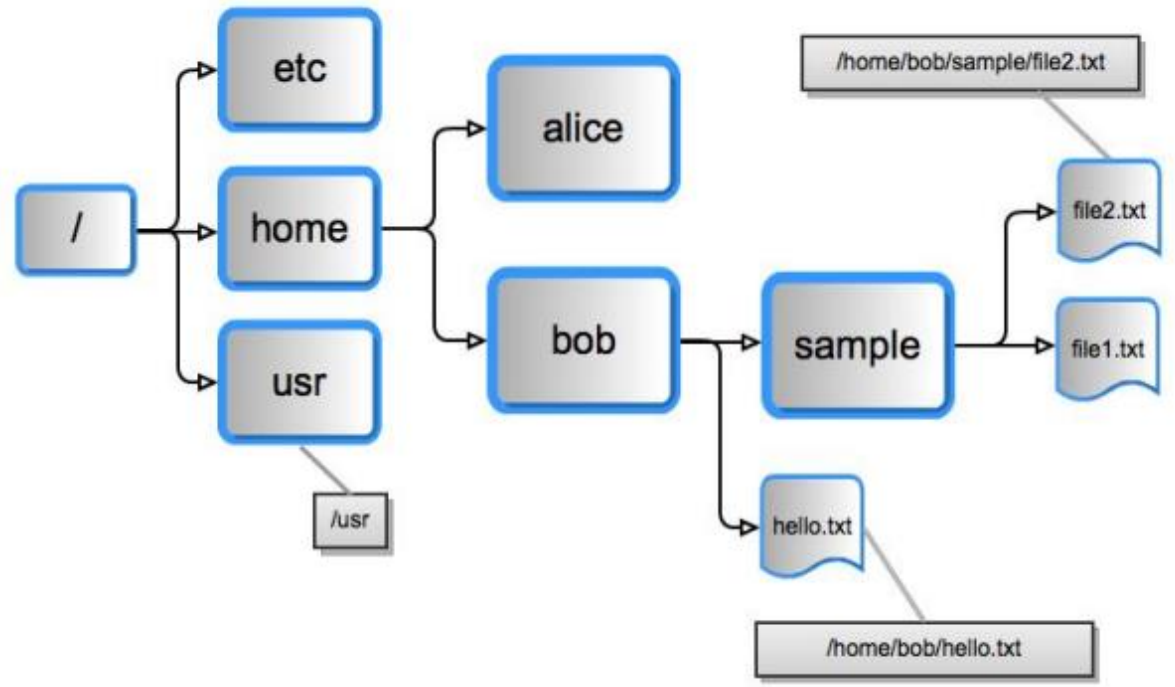
การดำเนินงานทั่วไป

- **การนำทางไฟล์ (File navigation):** ค้นหาและเปิดไฟล์ที่ต้องการภายในระบบ
- **การจัดการไฟล์ (File management):** สร้างไฟล์ ย้าย ลบ เปลี่ยนชื่อไฟล์
- **การดูและแก้ไขเนื้อหาของไฟล์ (File content viewing and editing):** ใช้คำสั่งเพื่อแสดงหรือแก้ไขข้อมูลภายในไฟล์
- **การค้นหา (Search):** ค้นหาไฟล์หรือข้อมูลตามชื่อหรือเนื้อหา
- **การควบคุมการเข้าถึงข้อมูล (Access control):** กำหนดสิทธิ์การเข้าถึงไฟล์และข้อมูลต่างๆ เพื่อความปลอดภัย
- **การจัดการผู้ใช้ (User management):** สร้าง บล็อค หรือลบผู้ใช้งาน
- **รายการควบคุมการเข้าถึง (Access control lists - ACLs):** รายการที่กำหนดสิทธิ์การเข้าถึงไฟล์และข้อมูลสำหรับผู้ใช้และกลุ่มผู้ใช้ต่างๆ
- **การกำหนดสิทธิ์การเข้าถึงไฟล์ (File permissions):** กำหนดสิทธิ์การอ่านเขียนสำหรับเจ้าของไฟล์ กลุ่มผู้ใช้ และผู้ใช้ทั่วไป
- **การติดตั้งและอัพเดทซอฟต์แวร์ (Software installation and updates):** ติดตั้งและอัพเดทโปรแกรมต่างๆ ภายในระบบ

Linux File Directory



File system navigation



Linux เป็นระบบปฏิบัติการที่ได้รับความนิยมมากขึ้น เนื่องจากความสามารถหลากหลาย แต่ฟีเจอร์ต่างๆ เหล่านี้ก็หมายถึงพื้นที่ที่อาจถูกโจมตีได้มากเช่นกัน ถึงกระนั้นเราก็สามารถสร้างระบบ Linux ที่มีความปลอดภัยสูง

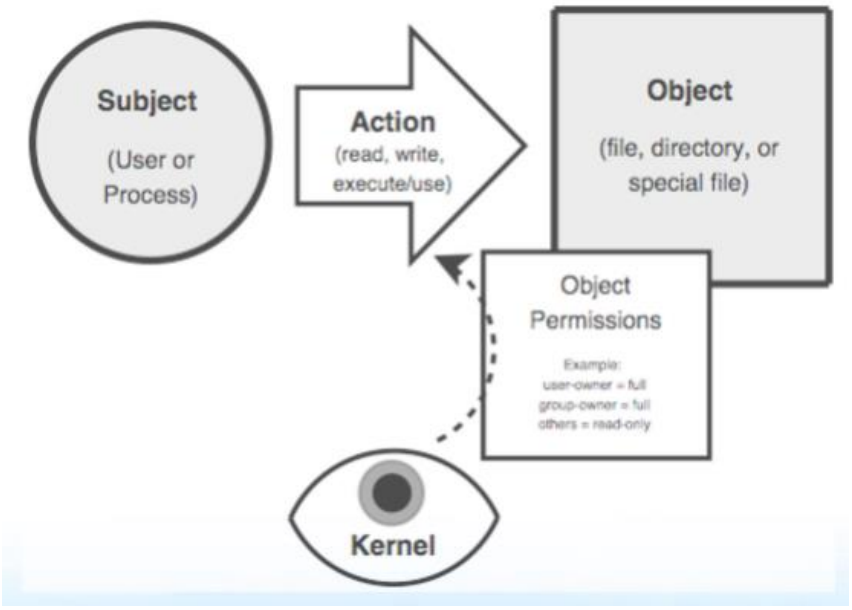
โมเดลความปลอดภัยของ Linux

โมเดลความปลอดภัยแบบดั้งเดิมของ Linux คือ:

- บัญชีผู้ใช้หรือกระบวนการที่มีสิทธิ์ "root" สามารถทำอะไรก็ได้
- บัญชีผู้ใช้แบบอื่นๆ จะมีสิทธิ์ในการกระทำสิ่งต่างๆ น้อยกว่ามาก

ดังนั้น เป้าหมายของผู้โจมตีระบบมักจะเป็นการดึงสิทธิ์ "root" มาใช้

แม้ว่าจะมีความเสี่ยง แต่เราก็สามารถใช้งานระบบ Linux ได้อย่างปลอดภัย สิ่งสำคัญจึงอยู่ที่การใช้ระบบการควบคุมการเข้าถึงตามความต้องการ (Discretionary Access Controls: DAC)



ในระบบยูนิกซ์ (UNIX) ทุกสิ่งถือเป็นไฟล์ ยกเว้นเพียงสองอย่าง ดังนี้

- **บัญชีผู้ใช้ (user):** แสดงถึงบุคคลที่สามารถใช้งานไฟล์ได้ บัญชีผู้ใช้ไม่เพียงแค่สำหรับคนจริง แต่ยังรวมถึงกระบวนการ (process) ของระบบด้วย
- **กลุ่ม (group):** คือรายชื่อของบัญชีผู้ใช้ ผู้ใช้จะมีกลุ่มหลัก (main group) ที่สังกัดอยู่ และอาจเป็นสมาชิกของกลุ่มอื่นๆ ได้อีกด้วย
- ข้อมูลของผู้ใช้จะถูกเก็บไว้ในไฟล์ **/etc/passwd** ตัวอย่างเช่น

maestro:x:200:100:Maestro Edward Hizzersands:/home/maestro:/bin/bash

- รายละเอียดเพิ่มเติมของกลุ่มจะถูกเก็บไว้ในไฟล์ **/etc/group** ตัวอย่างเช่น

conductors:x:100:
pianists:x:102:maestro,volodya

- เราสามารถจัดการและแก้ไขการเป็นสมาชิกกลุ่มของผู้ใช้ด้วยคำสั่ง useradd, usermod, userdel

สิทธิ์การเข้าถึงไฟล์ (File Permissions)

- ไฟล์ในระบบ Linux มีเจ้าของสองคน คือ เจ้าของผู้ใช้ (user) และเจ้าของกลุ่ม (group)
- เจ้าของแต่ละคนจะมีชุดสิทธิ์การเข้าถึงไฟล์ที่แตกต่างกัน
- นอกจากนี้ยังมีสิทธิ์การเข้าถึงของ "ผู้อื่น" (other) อีกหนึ่งชุด
- สิทธิ์การเข้าถึงประกอบด้วย การอ่าน (read) เขียน (write) และรัน (execute) โดยแบ่งตามลำดับเจ้าของผู้ใช้/เจ้าของกลุ่ม/ผู้อื่น
- ตัวอย่างเช่น

-rw-rw-r-- 1 maestro user 35414 Mar 25 01:38 baton.txt

- เราสามารถตั้งค่าสิทธิ์การเข้าถึงไฟล์ได้ด้วยคำสั่ง chmod

สิทธิ์การเข้าถึงไดเรกทอรี (Directory Permissions)

- **อ่าน (read):** อ่านรายการไฟล์ภายในไดเรกทอรี
- **เขียน (write):** สร้างหรือลบไฟล์ภายในไดเรกทอรี
- **รัน (execute):** ใช้สิ่งต่างๆ ภายในไดเรกทอรี หรือเปลี่ยนไดเรกทอรี ทำงานเป็นไดเรกทอรีนี้
- ตัวอย่างเช่น

$ chmod g+rx extreme_casseroles # เพิ่มสิทธิ์อ่าน (read) และรัน (execute) ให้กับกลุ่ม
$ ls -l extreme_casseroles # แสดงรายละเอียดของไดเรกทอรี extreme_casseroles
drwxr-x--- 8 biff drummers 288 Mar 25 01:38 extreme_casseroles

- ในตัวอย่างข้างต้น ไดเรกทอรี extreme_casseroles จะมีสิทธิ์ดังนี้
    - เจ้าของ (owner): อ่าน (read), เขียน (write), รัน (execute)
    - กลุ่ม (group): อ่าน (read), รัน (execute)
    - ผู้อื่น (other): ไม่มีสิทธิ์

Sticky Bit

- เดิมทีใช้สำหรับล็อคไฟล์ไว้ในหน่วยความจำ (memory)
- ปัจจุบัน ใช้กับไดเรกทอรีเพื่อจำกัดสิทธิ์ในการลบไฟล์
    - ไฟล์หรือไดเรกทอรีที่ตั้งค่า Sticky Bit จะอนุญาตให้ลบได้เฉพาะเจ้าของเท่านั้น
    - ผู้ใช้คนอื่นๆ จะไม่สามารถลบไฟล์ได้ แม้จะมีสิทธิ์เขียน (write) ก็ตาม
- ใช้คำสั่ง chmod พร้อมแฟล็ก +t เพื่อตั้งค่า Sticky Bit ตัวอย่างเช่น

chmod +t extreme_casseroles

- รายละเอียดของไดเรกทอรีจะแสดงตัวอักษร t หรือ T เพื่อบอกว่ามีการตั้งค่า Sticky Bit ตัวอย่างเช่น drwxrwx--T 8 biff drummers 288 Mar 25 01:38 extreme_casseroles

- Sticky Bit มีผลเฉพาะกับไดเรกทอรีที่ตั้งค่าเท่านั้น ไม่ส่งผลกับไดเรกทอรีลูก (child directories)

SetUID และ SetGID

- **SetUID:**
    - เป็นการตั้งค่าให้โปรแกรมรันโดยใช้สิทธิ์ของเจ้าของไฟล์นั้น
    - ไม่ว่าใครจะเรียกใช้โปรแกรมนี้ก็ตาม
- **SetGID:**
    - เป็นการตั้งค่าให้โปรแกรมรันโดยใช้กลุ่มของเจ้าของไฟล์นั้น
    - ไม่ว่าใครจะเรียกใช้โปรแกรมนี้ก็ตาม
- " run as " มีความหมายเดียวกับ " run with same privileges as "
- การตั้งค่า SetUID และ SetGID บนไฟล์ที่เป็นของผู้ใช้ root หรือบัญชีผู้ใช้/กลุ่มที่มีสิทธิ์พิเศษ **มีความเสี่ยงสูง**
- ใช้ได้กับไฟล์ที่รันได้ (executable files) เท่านั้น ไม่สามารถใช้กับสคริปต์ shell

SetGID กับไดเรกทอรี

- SetUID ไม่มีผลต่อไดเรกทอรี
- SetGID มีผลต่อไดเรกทอรี:
    - ไฟล์ใดๆ ที่สร้างขึ้นภายในไดเรกทอรีที่ตั้งค่า SetGID จะได้รับกลุ่มเดียวกับไดเรกทอรีนั้นโดยอัตโนมัติ
- **มีประโยชน์หากผู้ใช้อยู่ในกลุ่มอื่นและสร้างไฟล์เป็นประจำเพื่อแชร์กับสมาชิกคนอื่นๆ** โดยไม่ต้องเปลี่ยนกลุ่มของไฟล์เหล่านั้นทีละไฟล์

เคอร์เนล (Kernel) vs พื้นที่ผู้ใช้ (User Space)

- **เคอร์เนล (Kernel):** หมายถึงหน่วยความจำที่ใช้โดยเคอร์เนลของ Linux และโมดูลที่โหลดได้ (เช่น ไดรเวอร์อุปกรณ์)
- **พื้นที่ผู้ใช้ (User Space):** หมายถึงหน่วยความจำที่ใช้โดยโปรแกรมอื่นๆ ทั้งหมด

เนื่องจากเคอร์เนลเป็นตัวบังคับใช้ระบบการควบคุมการเข้าถึงตามความต้องการ (Discretionary Access Control: DAC) และความปลอดภัยของ Linux ดังนั้นจึงมีความสำคัญอย่างยิ่งที่จะแยกเคอร์เนลออกจากพื้นที่ผู้ใช้

- ด้วยเหตุนี้ เคอร์เนลจึงไม่ถูกสลับไปยังดิสก์ (ไม่ถูกเขียนทับลงบนดิสก์)
- เฉพาะผู้ใช้ root เท่านั้นที่มีสิทธิ์โหลดและยกเลิกการโหลดโมดูลของเคอร์เนล

ช่องโหว่ของโปรแกรม SetUID Root

- โปรแกรม SetUID Root เป็นโปรแกรมที่รันโดยใช้สิทธิ์ของผู้ใช้ root
    - ไม่ว่าใครจะเรียกใช้โปรแกรมนี้ก็ตาม
- โปรแกรมเหล่านี้มักถูกใช้เพื่อให้ผู้ใช้ที่ไม่มีสิทธิ์สามารถเข้าถึงทรัพยากรที่มีสิทธิ์พิเศษได้
- จำเป็นต้องเขียนโปรแกรมเหล่านี้ด้วยความระมัดระวังอย่างยิ่ง
- ช่องโหว่ของโปรแกรมเหล่านี้สามารถเกิดขึ้นได้จากบั๊กของซอฟต์แวร์
    - อาจทำให้ผู้ใช้ที่ไม่มีสิทธิ์สามารถใช้โปรแกรมเหล่านี้เพื่อดึงสิทธิ์ของผู้ใช้ root มาใช้โดยไม่ได้รับอนุญาต
- ปัจจุบัน ตัวแจกแจง Linux ส่วนใหญ่ได้ลดการใช้โปรแกรม SetUID Root ลง
- ถึงกระนั้น ผู้โจมตีระบบก็ยังคงพยายามสแกนหาโปรแกรมเหล่านี้อยู่

ช่องโหว่ของเว็บ

- ช่องโหว่ของเว็บเป็นช่องโหว่ที่มีจำนวนมากและหลากหลายประเภท
    - เนื่องจากเว็บไซต์มีพื้นที่ที่ถูกโจมตีได้กว้างขวางและมองเห็นได้ง่าย
- เว็บแอปพลิเคชันที่เขียนด้วยภาษาสคริปต์
    - มักจะไม่ค่อยมีปัญหาเรื่องบัฟเฟอร์โอเวอร์โฟลว์ (buffer overflow) แบบดั้งเดิม
    - แต่ก็ยังคงมีความเสี่ยงจากการจัดการอินพุตที่ไม่ดี (poor input-handling)
- เว็บแอปพลิเคชันที่เปิดใช้งานโดยค่าเริ่มต้น (enabled-by-default) มีจำนวนน้อย
- แต่ผู้ใช้มักจะติดตั้งเว็บแอปพลิเคชันที่มีช่องโหว่
    - หรือเขียนเว็บแอปพลิเคชันเองที่มีจุดบกพร่องที่สามารถระบุและโจมตีได้ง่าย

รูทคิท (Rootkits)

- รูทคิท คือ ชุดเครื่องมือที่ผู้โจมตีใช้เพื่อปกปิดร่องรอย ของการบุกรุกระบบ
- หากรูทคิทถูกติดตั้งลงในระบบได้สำเร็จ ก่อนที่จะถูกตรวจพบ เจ้าของระบบแทบจะสูญเสียการควบคุมระบบทั้งหมด

- รูทคิทในยุคแรก มักจะเป็นการดัดแปลงคำสั่งพื้นฐานของระบบ เช่น ls เพื่อ ซ่อนไฟล์ ซ่อนไดเรกทอรี และซ่อนกระบวนการของผู้โจมตี
- รูทคิทในปัจจุบัน มักใช้โมดูลของเคอร์เนลที่โหลดได้ (loadable kernel modules) เพื่อดักจับการเรียกใช้ระบบ (system calls) ภายในเคอร์เนล
    - ทำให้ผู้โจมตีสามารถปกปิดตนเอง จากคำสั่งตรวจสอบระบบทั่วไป
- เราอาจตรวจพบรูทคิทได้ด้วยโปรแกรม chkrootkit
- โดยทั่วไปแล้ว เมื่อพบรูทคิท เราจำเป็นต้องฟอร์แมตและติดตั้งระบบปฏิบัติการใหม่

การเพิ่มความแข็งแกร่งของระบบ Linux (Linux System Hardening)

เนื่องจากระบบ Linux มีประวัติการใช้งานแอปพลิเคชันที่ไม่ได้รับการรักษาความปลอดภัยมานาน ดังนั้น การลดความเสี่ยงด้านความปลอดภัยทั้งในระดับระบบและระดับแอปพลิเคชันจึงเป็นสิ่งที่ควรคำนึงถึง

- **การติดตั้งระบบปฏิบัติการ (OS Installation):**
    - ความปลอดภัยเริ่มต้นตั้งแต่กระบวนการติดตั้งระบบปฏิบัติการ
    - โดยเฉพาะอย่างยิ่ง ควรเลือกติดตั้งเฉพาะซอฟต์แวร์ที่จำเป็นเท่านั้น
    - เพราะแอปพลิเคชันที่ไม่ได้ใช้งาน มักจะถูกละเลย ไม่ได้รับการปรับแต่งเพื่อเพิ่มความแข็งแกร่ง และไม่ได้รับการอัพเดทแพทช์ความปลอดภัย
    - ตัวอย่างซอฟต์แวร์ที่โดยทั่วไปไม่ควรติดตั้ง:
        - X Window System, RPC services, R-services, inetd, SMTP daemons, telnet etc.
- **การกำหนดค่าเบื้องต้นของระบบ (Initial System Software Configuration):**
    - ตั้งค่ารหัสผ่านของผู้ใช้ root
    - สร้างบัญชีผู้ใช้สำหรับใช้งานทั่วไป (non-root user account)
    - ตั้งค่าระดับความปลอดภัยโดยทั่วไปของระบบ
    - เปิดใช้งานไฟร์วอลล์เบื้องต้น
    - เปิดใช้งาน SELinux (Security Enhanced Linux)

การจัดการแพทช์ (Patch Management)

- แอปพลิเคชันเซิร์ฟเวอร์ที่ติดตั้งจำเป็นต้อง:
    - ถูกกำหนดค่าอย่างปลอดภัย
    - ได้รับการอัพเดทแพทช์ความปลอดภัยอย่างสม่ำเสมอ
- การติดตั้งแพทช์อาจไม่สามารถหยุดยั้งช่องโหว่ใหม่ๆ ได้ทัน (patch rat-race)
- ดังนั้น ควรมีเครื่องมือสำหรับดาวน์โหลดและติดตั้งแพทช์ความปลอดภัยโดยอัตโนมัติ
    - ตัวอย่างเช่น up2date, YaST, apt-get
    - หมายเหตุ: ไม่ควรเปิดใช้งานการติดตั้งอัพเดทโดยอัตโนมัติบนระบบที่มีการควบคุมการเปลี่ยนแปลง (change-controlled systems) โดยไม่ได้ทดสอบก่อน

การควบคุมการเข้าถึงเครือข่าย (Network Access Controls)

- อย่างที่เราได้เห็นไปแล้ว เครือข่ายเป็นช่องทางโจมตีที่สำคัญที่ต้องได้รับการป้องกัน
- TCP wrappers เป็นเครื่องมือสำคัญที่ใช้ในการตรวจสอบการเข้าถึงระบบ
    - เดิมทีเป็นโปรแกรม TCP daemon ที่ทำงานร่วมกับ inetd
    - ก่อนที่จะอนุญาตการเชื่อมต่อมายังบริการ จะทำการตรวจสอบดังนี้
        - โฮสต์ที่ขอเชื่อมต่อมีชื่อระบุอย่างชัดเจนอยู่ในไฟล์ hosts.allow หรือไม่ (อนุญาตการเชื่อมต่อ)
        - โฮสต์ที่ขอเชื่อมต่อมีชื่อระบุอย่างชัดเจนอยู่ในไฟล์ hosts.deny หรือไม่ (บล็อกการเชื่อมต่อ)
        - ถ้าโฮสต์ที่ขอเชื่อมต่อไม่อยู่ในรายชื่อทั้งสองไฟล์ (อนุญาตการเชื่อมต่อ)
    - การตรวจสอบจะพิจารณาบริการ ปลายทาง IP และชื่อผู้ใช้
    - ปัจจุบัน TCP wrappers มักจะรวมเป็นส่วนหนึ่งของแอปพลิเคชันที่ใช้ libwrappers
- นอกจากนี้ ยังมี netfilter ซึ่งเป็นกลไกไฟร์วอลล์ภายในเคอร์เนลของ Linux ที่ทรงพลัง
    - พร้อมกับ iptables ซึ่งเป็นโปรแกรมสำหรับตั้งค่า netfilter
- netfilter มีประโยชน์สำหรับทั้งไฟร์วอลล์ เซิร์ฟเวอร์ และเดสก์ท็อป
- การกำหนดค่า netfilter โดยตรงค่อนข้างยุ่งยาก ต้องเรียนรู้เพิ่มเติม แต่มีเครื่องมือสำหรับสร้าง Rule อัตโนมัติ
- สำหรับการใช้งานไฟร์วอลล์ส่วนบุคคล (personal firewall) ทั่วไป มักจะตั้งค่าดังนี้:
    - อนุญาตการขอเข้าถึงบริการที่ระบุเท่านั้น
    - บล็อกการขอเข้าถึงบริการอื่นๆ ทั้งหมด
    - อนุญาตการส่งข้อมูลออก (outbound) ทั้งหมด (จากเครื่องภายใน)
- หากต้องการความปลอดภัยที่สูงขึ้น จำเป็นต้องกำหนดค่าด้วยตัวเอง

Antivirus Software

- ในอดีต ระบบ Linux ไม่ค่อยถูกโจมตีด้วยไวรัส เนื่องจากความนิยมที่น้อยกว่าระบบปฏิบัติการอื่นๆ (มากกว่าที่จะมีความปลอดภัยสูง)
- การติดตั้งแพทช์อย่างรวดเร็วมีประสิทธิภาพพอสมควรในการป้องกันเวิร์ม (worms)
- อย่างไรก็ตาม ไวรัส มักจะอาศัยสิทธิ์ของผู้ใช้ในการแพร่กระจาย
    - ผู้ใช้ที่ไม่ใช่ root จะสร้างความเสียหายได้น้อยกว่า แต่ก็ยังสามารถใช้ทรัพยากรของระบบได้
- ความนิยมที่เพิ่มขึ้นของระบบ Linux ทำให้ช่องโหว่ต่างๆ เริ่มเป็นที่สนใจของผู้โจมตีมากขึ้น
    - ดังนั้น ซอฟต์แวร์ Antivirus จึงมีความสำคัญมากขึ้น
- ปัจจุบันมีโปรแกรม Antivirus สำหรับ Linux ทั้งแบบฟรีและแบบเสียเงิน ตัวอย่างเช่น McAfee, Symantec, Sophos, ClamAV

การจัดการผู้ใช้ (User Management)

- หลักการสำคัญในการรักษาความปลอดภัยของบัญชีผู้ใช้:
    - ต้องใส่ใจในการตั้งค่าสิทธิ์ของไฟล์และไดเรกทอรี
    - ใช้กลุ่มเพื่อแบ่งแยกผู้ใช้ตามหน้าที่ (roles)
    - ใช้สิทธิ์ของผู้ใช้ root อย่างระมัดระวังและเท่าที่จำเป็น
- คำสั่งที่เกี่ยวข้อง: chmod, useradd/mod/del, groupadd/mod/del, passwd, chage
- ข้อมูลผู้ใช้จะถูกเก็บไว้ในไฟล์ /etc/passwd และ /etc/group
- การจัดการกลุ่มที่ผู้ใช้เป็นสมาชิก
- ตั้งค่าอายุของรหัสผ่านให้เหมาะสม: /etc/login.defs

การมอบหมายสิทธิ์ระดับ Root (Root Delegation)

- ในระบบ Linux มีปัญหาที่ว่า "ผู้ใช้ root สามารถทำทุกอย่าง ผู้ใช้ทั่วไปทำได้น้อย"
- คำสั่ง "su" อนุญาตให้ผู้ใช้รันคำสั่งในฐานะผู้ใช้ root
    - สามารถเข้าสู่ root shell หรือรันเพียงคำสั่งเดียว
    - จำเป็นต้องป้อนรหัสผ่านของผู้ใช้ root
    - ซึ่งอาจหมายความว่ามีผู้ใช้หลายคนรู้รหัสผ่านนี้
- SELinux RBAC (Role-Based Access Control) สามารถจำกัดสิทธิ์ของผู้ใช้ root ได้ แต่มีความซับซ้อนสูง
- คำสั่ง "sudo" อนุญาตให้ผู้ใช้รันคำสั่งในฐานะผู้ใช้ root
    - แต่จำเป็นต้องใช้เพียงรหัสผ่านของผู้ใช้เอง ไม่ใช่รหัสผ่านของผู้ใช้ root

    - ไฟล์ /etc/sudoers จะระบุคำสั่งที่อนุญาตให้ใช้กับ sudo
- อีกวิธีหนึ่งคือการตั้งค่าสิทธิ์ของผู้ใช้หรือกลุ่มเพื่ออนุญาตการใช้งาน ซึ่งอาจทำได้ยาก

การบันทึกระบบ (Logging)

- การบันทึกระบบ (Logging) ที่มีประสิทธิภาพ เป็นทรัพยากรที่สำคัญ
- ระบบ Linux ใช้โปรแกรม syslogd หรือ Syslog-NG ในการบันทึกระบบ
    - รับข้อมูลการบันทึกจากแหล่งต่างๆ
    - แบ่งประเภทตามหมวดหมู่ (facility) และความรุนแรง (severity)
    - เขียนข้อความบันทึกไปยังไฟล์บันทึกในเครื่องหรือเครื่องอื่น
- แนะนำให้ใช้ Syslog-NG มากกว่า syslogd เพราะ:
    - รองรับแหล่งที่มาและปลายทางของข้อมูลการบันทึกที่หลากหลาย
    - มี "เครื่องมือจัดการกฎ" (rule engine) ที่ยืดหยุ่นกว่าสำหรับการกำหนดค่า
    - สามารถบันทึกข้อมูลผ่านทาง TCP ซึ่งเข้ารหัสได้
- ควรตรวจสอบและปรับแต่งค่าเริ่มต้นให้เหมาะสม

การจัดการการบันทึกระบบ (Log Management)

- ควรหาจุดสมดุลระหว่างจำนวนไฟล์บันทึกที่ใช้
    - ไฟล์บันทึกขนาดใหญ่จำนวนน้อย อาจทำให้การค้นหาข้อมูลทำได้ยาก
- ควบคุมขนาดของไฟล์บันทึก
    - จำเป็นต้องหมุนเวียนไฟล์บันทึก (rotate log files) และลบสำเนาเก่า
    - โดยทั่วไปจะใช้โปรแกรม logrotate ที่รันโดย cron
    - เพื่อจัดการทั้งไฟล์บันทึกของระบบและแอปพลิเคชัน
- นอกจากนี้ยังต้องกำหนดค่าการบันทึกของแอปพลิเคชันด้วย

ความปลอดภัยของแอปพลิเคชัน (Application Security)

- หัวข้อนี้เป็นหัวข้อที่กว้าง ขึ้นอยู่กับแอปพลิเคชันที่ต้องการรักษาความปลอดภัย
- อย่างไรก็ตาม คุณสมบัติความปลอดภัยหลายอย่างมีการนำไปใช้อย่างคล้ายคลึงกันในแอปพลิเคชันต่างๆ
- ประเด็นที่ควรพิจารณา:
    - การรันแอปพลิเคชันในฐานะผู้ใช้/กลุ่มที่ไม่ได้รับสิทธิ์พิเศษ (unprivileged user/group)

- การรันแอปพลิเคชันภายใน chroot jail
- โมดูลาร์ (modularity)
- การเข้ารหัส (encryption)
- การบันทึกระบบ (logging)

การรันแอปพลิเคชันในฐานะผู้ใช้/กลุ่มที่ไม่ได้รับสิทธิ์พิเศษ (Running As Unprivileged User/Group)

- ทุกกระบวนการ (process) ในระบบจะ "run" ในฐานะผู้ใช้บางคน
- สิ่งสำคัญอย่างยิ่งคือผู้ที่กระทำการ “run” ไม่ควรมีสิทธิ์เป็น root
  - เนื่องจากข้อผิดพลาด (bug) ใดๆ อาจส่งผลกระทบต่อทั้งระบบ
- แอปพลิเคชันอาจต้องการสิทธิ์ของผู้ใช้ root เช่น การผูกกับพอร์ตหมายเลขต่ำ
  - ให้กระบวนการพ่อที่เป็นผู้ใช้ root ดำเนินการฟังก์ชันที่มีสิทธิ์พิเศษ
  - แต่บริการหลักจะรันจากกระบวนการลูกที่ไม่ได้รับสิทธิ์พิเศษ
- ควรใช้ผู้ใช้/กลุ่มเฉพาะสำหรับแอปพลิเคชันนั้นๆ
  - เพื่อให้ง่ายต่อการระบุที่มาของข้อความบันทึก

การรันแอปพลิเคชันภายใน Chroot Jail

- chroot ใช้จำกัดพื้นที่ที่กระบวนการสามารถเข้าถึงได้ภายในระบบไฟล์ (/)
  - โดยการแม็พ (map) เส้นทาง “/” เสมือนไปยังไดเรกทอรีอื่น
- มีประโยชน์สำหรับการรันเดมอน (daemon) ที่ควรจะเข้าถึงได้เฉพาะส่วนใดส่วนหนึ่งของระบบไฟล์เท่านั้น เช่น FTP Server
  - ไดเรกทอรีนอกเหนือจาก chroot jail จะมองไม่เห็นและไม่สามารถเข้าถึงได้เลย
- ช่วยจำกัดผลกระทบกรณีเดมอนถูกโจมตี
- การกำหนดค่า chroot jail ค่อนข้างซับซ้อนและแก้ไขปัญหายาก
  - จำเป็นต้องมีการคัดลอกส่วนประกอบที่จำเป็นของระบบไว้ภายใน chroot jail

โมดูลาร์ (Modularity)

- แอปพลิเคชันที่รันเป็นกระบวนการเดียวขนาดใหญ่และมีวัตถุประสงค์หลายอย่าง มักจะมีปัญหา ดังนี้:
  - ยากแก่การรันในฐานะผู้ใช้ที่ไม่ได้รับสิทธิ์พิเศษ (unprivileged user)
  - ยากแก่การค้นหาและแก้ไขช่องโหว่ความปลอดภัยใน source code

    - ยากแก่การปิดใช้งานฟังก์ชันที่ไม่จำเป็น
- ดังนั้น โมดูลาร์จึงเป็นคุณสมบัติที่สำคัญที่ช่วยลดพื้นที่เสี่ยงต่อการโจมตี (attack surface) ตัวอย่างเช่น postfix เมื่อเทียบกับ sendmail หรือโมดูลของ Apache

การเข้ารหัส (Encryption)

- การส่งข้อมูลเข้าสู่ระบบ การส่งรหัสผ่าน หรือการส่งข้อมูลแอปพลิเคชันผ่านเครือข่ายแบบข้อความธรรมดา (clear text) จะมีความเสี่ยงต่อการถูกดักฟัง (eavesdropping)
- ด้วยเหตุนี้ แอปพลิเคชันเครือข่ายจำนวนมากจึงรองรับการเข้ารหัสเพื่อปกป้องข้อมูลเหล่านี้
    - มักใช้ไลบรารี OpenSSL
- อาจจำเป็นต้องใช้ใบรับรอง X.509 ของตัวเอง
    - สามารถสร้างและลงนามใบรับรองได้ด้วยคำสั่ง openssl
    - สามารถใช้ใบรับรองแบบฟรี แบบที่สร้างเอง หรือแบบเชิงพาณิชย์

การบันทึกระบบ (Logging)

- แอปพลิเคชันส่วนใหญ่สามารถกำหนดค่าให้บันทึกข้อมูลในระดับต่างๆ ได้ (ตั้งแต่ระดับ debug ไปจนถึงไม่บันทึกเลย) จึงจำเป็นต้องตั้งค่าการบันทึกที่เหมาะสม
- ควรตัดสินใจว่าจะใช้ไฟล์บันทึกเฉพาะของแอปพลิเคชันนั้นๆ หรือใช้ระบบบันทึกกลางของระบบ (เช่น syslog)
- ต้องแน่ใจว่ามีการหมุนเวียนไฟล์บันทึก

การควบคุมการเข้าถึงแบบบังคับ (Mandatory Access Controls)

- ระบบ Linux ใช้โมเดลความปลอดภัยแบบ Discretionary Access Control (DAC) ซึ่งผู้ใช้สามารถกำหนดสิทธิ์การเข้าถึงไฟล์และไดเรกทอรีได้เอง
- ในทางกลับกัน Mandatory Access Control (MAC) จะบังคับใช้นโยบายความปลอดภัยระดับโลกกับผู้ใช้ทั้งหมด
    - ผู้ใช้ไม่สามารถตั้งค่าการควบคุมที่อ่อนแอกว่านโยบายที่กำหนด
    - ผู้ดูแลระบบทั่วไปจะไม่สามารถใช้บัญชีที่ไม่มีสิทธิ์ในการเปลี่ยนแปลงนโยบายความปลอดภัยระดับโลก
- แต่ระบบ MAC มีความซับซ้อนในการจัดการ
- ตัวอย่างระบบควบคุมการเข้าถึงแบบบังคับบน Linux:

    - AppArmor ของ Novell’s SuSE Linux:จำกัดกระบวนการเฉพาะ แต่ปล่อยให้ส่วนอื่นๆ ใช้ระบบ DAC
    - SELinux ของ Fedora และ RedHat Enterprise Linux:จำกัดเน็ตเวิร์กเดมอน แต่ปล่อยให้ส่วนอื่นๆ ใช้ระบบ DAC
- โดยทั่วไป SELinux แบบเต็มรูปแบบจะใช้เฉพาะกับเครื่องที่มีความปลอดภัยสูง

SELinux

- SELinux เป็นระบบควบคุมการเข้าถึงแบบบังคับที่ทรงพลัง พัฒนาโดย iNSA สำหรับระบบ Linux
- ระบบ DAC ของ Linux ยังคงทำงานอยู่ แต่ถ้าหากระบบอนุญาตการกระทำนั้น SELinux จะประเมินอีกครั้งตามนโยบายความปลอดภัยของตัวเอง
- "Subject" คือ กระบวนการ (เนื่องจากกระบวนการเหล่านี้รันคำสั่งของผู้ใช้)
- "Action" คือ "สิทธิ์"
- "Object" ไม่ได้หมายถึงแค่ไฟล์และไดเรกทอรีเท่านั้น แต่ยังรวมถึงกระบวนการและทรัพยากรของระบบด้วย
- เพื่อจัดการความซับซ้อน SELinux มีหลักการ:
    - "สิ่งที่ไม่ได้รับอนุญาตอย่างชัดเจน ล้วนถูกปฏิเสธ"
    - ใช้กลุ่มของ Subject, Permission และ Object

บริบทความปลอดภัย (Security Contexts)

- ในระบบ SELinux ทุกๆ Subject และ Object จะถูกควบคุมโดยบริบทความปลอดภัย (security context) ซึ่งประกอบด้วย:
    - user - ผู้ใช้แต่ละคน (ไม่ว่าจะเป็นมนุษย์หรือเดมอน)
        - SELinux มีรายชื่อผู้ใช้ของตัวเอง
        - user label บน Subject จะระบุสิทธิพิเศษของบัญชีนั้น
        - user label บน Object จะระบุเจ้าของ
    - role - เหมือนกลุ่มผู้ใช้ แต่ใช้โดย Subject
        - ผู้ใช้สามารถใช้ได้เพียงแค่ 1 role ใน 1 เวลา
        - สามารถเปลี่ยน role ได้ก็ต่อเมื่อได้รับอนุญาตเท่านั้น
    - domain (type) - แซนด์บ็อกซ์ (sandbox) เป็นการรวมกลุ่ม Subject และ Object ที่สามารถโต้ตอบกันได้
- โมเดลนี้เรียกว่า Type Enforcement (TE)

การตัดสินใจใน SELinux (Decision Making in SELinux)

- มีการตัดสินใจอยู่สองประเภท:
    - การตัดสินใจการเข้าถึง (access decisions)
        - เมื่อ Subject ดำเนินการบางอย่างกับ Object ที่มีอยู่แล้ว หรือสร้างสิ่งใหม่ๆ ในโดเมนที่คาดการณ์ไว้
    - การตัดสินใจการเปลี่ยนผ่าน (transition decisions)
        - การเรียกใช้กระบวนการในโดเมนที่แตกต่างไปจากโดเมนที่ Subject-process กำลังทำงานอยู่
        - การสร้าง Object ในประเภท (โดเมน) ที่แตกต่างจากไดเรกทอรีต้นทาง
- การเปลี่ยนผ่านจะต้องได้รับอนุญาตตามนโยบาย SELinux

การควบคุมการเข้าถึงตามบทบาท (RBAC) และ การรักษาความปลอดภัยหลายระดับ (MLS)

- SELinux ยังผสมผสานการควบคุมการเข้าถึงตามบทบาท (Role-Based Access Control: RBAC)
    - กฎระบุบทบาทที่ผู้ใช้สามารถใช้ได้
    - กฎอื่นๆ ระบุสถานการณ์ที่ผู้ใช้สามารถเปลี่ยนจากบทบาทหนึ่งไปยังอีกบทบาทหนึ่ง
- และการรักษาความปลอดภัยหลายระดับ (Multi-Level Security: MLS) ซึ่งอิงตามโมเดล Bell-LaPadula
    - เกี่ยวข้องกับการจัดการข้อมูลลับ
        - หลักการ "ห้ามอ่านข้อมูลระดับสูงกว่า (no read up)" และ "ห้ามเขียนข้อมูลระดับต่ำกว่า (no write down)"
    - MLS ถูกบังคับใช้ผ่านการติดป้ายกำกับระบบไฟล์

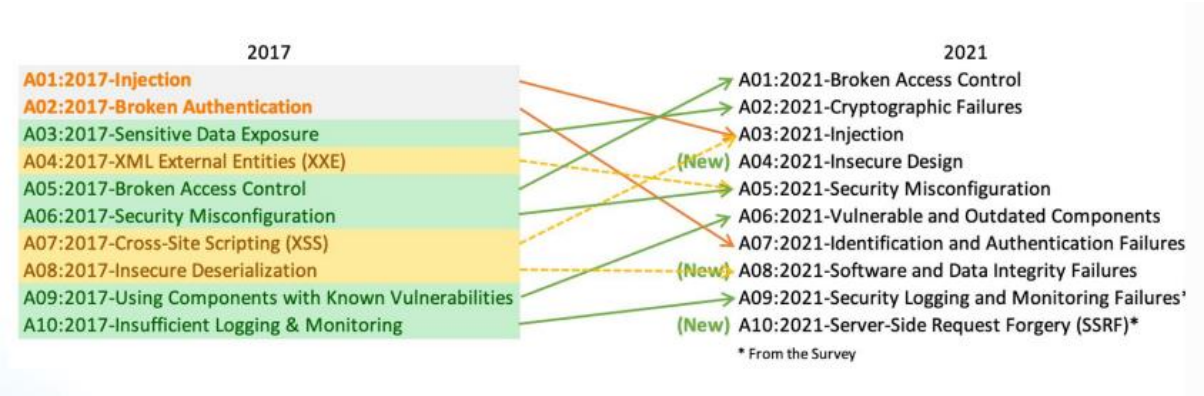
Open Web Application Security Project (OWASP)

มูลนิธิ Open Web Application Security Project (OWASP) เป็นองค์กรไม่แสวงหาผลกำไรที่ทำงานเพื่อยกระดับความปลอดภัยของซอฟต์แวร์ โดยอาศัยโครงการโอเพนซอร์สที่ขับเคลื่อนโดยชุมชน บทบาทประจำภูมิภาคทั่วโลกหลายร้อยแห่ง สมาชิกหลายหมื่นคน และการประชุมด้านการศึกษาและการฝึกอบรมชั้นนำ มูลนิธิ OWASP Foundation เป็นแหล่งความรู้สำหรับนักพัฒนาและนักเทคโนโลยีในการรักษาความปลอดภัยเว็บ

บริการของมูลนิธิ OWASP

- เครื่องมือและทรัพยากร
- ชุมชนและการสร้างเครือข่าย
- การศึกษาและการฝึกอบรม

โครงการ OWASP Top 10



รายการความเสี่ยงด้านเว็บแอปพลิเคชัน 10 อันดับแรกของ OWASP (OWASP Top 10) ปี 2019

รายการ 10 อันดับแรกนี้ ระบุถึงช่องโหว่ที่พบได้บ่อยที่สุดและมีความรุนแรงสูง ซึ่งผู้พัฒนาเว็บแอปพลิเคชันควรใส่ใจเป็นพิเศษ

- **API1:2019 Broken Object Level Authorization (การรับรองสิทธิ์ระดับ Object ที่ไม่ปลอดภัย)**
    - เกิดขึ้นเมื่อระบบไม่สามารถควบคุมการเข้าถึงข้อมูลของผู้ใช้แต่ละคนได้อย่างเหมาะสม
    - ตัวอย่างเช่น ผู้ใช้ A ไม่ควรสามารถเข้าถึงข้อมูลของผู้ใช้ B ได้
- **API2:2019 Broken User Authentication (การรับรองความถูกต้องของผู้ใช้ที่ไม่ปลอดภัย)**
    - เกิดขึ้นเมื่อระบบมีช่องโหว่ในการตรวจสอบว่าผู้ใช้เป็นใคร
    - ตัวอย่างเช่น การใช้รหัสผ่านที่ง่ายเกินไปหรือการจัดเก็บรหัสผ่านแบบไม่เข้ารหัส

- **API3:2019 Excessive Data Exposure (การเปิดเผยข้อมูลมากเกินไป)**
    - เกิดขึ้นเมื่อระบบเผยแพร่ข้อมูลผู้ใช้หรือข้อมูลระบบมากกว่าที่จำเป็น
    - ตัวอย่างเช่น การแสดงหมายเลขประกันสังคมของผู้ใช้ทั้งหมดในผลการค้นหา
- **API4:2019 Lack of Resources & Rate Limiting (การขาดทรัพยากรและการจำกัดอัตราการใช้งาน)**
    - เกิดขึ้นเมื่อระบบไม่สามารถรองรับจำนวนผู้ใช้งานหรือคำขอได้เพียงพอ
    - หรือไม่มีการจำกัดจำนวนครั้งที่ผู้ใช้สามารถกระทำการบางอย่างได้
    - ซึ่งอาจนำไปสู่การโจมตีแบบ Distributed Denial-of-Service (DDoS) ได้
- **API5:2019 Broken Function Level Authorization (การรับรองสิทธิ์ระดับฟังก์ชันที่ไม่ปลอดภัย)**
    - เกิดขึ้นเมื่อระบบไม่สามารถควบคุมว่าผู้ใช้แต่ละคนสามารถใช้ฟังก์ชันใดของระบบได้บ้าง
    - ตัวอย่างเช่น ผู้ใช้ทั่วไปไม่ควรสามารถใช้ฟังก์ชันการดูแลระบบได้
- **API6:2019 Mass Assignment (การกำหนดค่าข้อมูลจำนวนมากพร้อมกัน)**
    - เกิดขึ้นเมื่อระบบอนุญาตให้ผู้ใช้ป้อนข้อมูลลงในฟอร์มทีเดียวหลายช่อง
    - ซึ่งช่องโจมตีอาจใช้ช่องโหว่นี้ในการแฝง script ที่เป็นอันตรายเข้าไปในระบบ
- **API7:2019 Security Misconfiguration (การกำหนดค่าความปลอดภัยที่ผิดพลาด)**
    - เกิดขึ้นเมื่อระบบไม่ได้ถูกกำหนดค่าให้มีความปลอดภัยอย่างเหมาะสม
    - ตัวอย่างเช่น การใช้ค่าเริ่มต้นที่ไม่ปลอดภัยหรือการติดตั้งแพทช์ความปลอดภัยล่าสุด
- **API8:2019 Injection (การโจมตีแบบ Injection)**
    - เกิดขึ้นเมื่อช่องโจมตีแทรกคำสั่งที่ไม่ต้องการลงในข้อมูลที่ส่งไปยังระบบ
    - ตัวอย่างเช่น การโจมตีแบบ SQL Injection ที่ใช้แทรกคำสั่ง SQL เพื่อแอบหาข้อมูลจากฐานข้อมูล
- **API9:2019 Improper Assets Management (การจัดการสินทรัพย์ที่ไม่เหมาะสม)**
    - เกิดขึ้นเมื่อระบบไม่สามารถติดตามหรือควบคุมทรัพย์สินต่างๆ ที่เกี่ยวข้องกับระบบได้อย่างมีประสิทธิภาพ
    - ตัวอย่างเช่น การไม่ทราบว่ามีระบบย่อยไหนบ้างที่เชื่อมต่อกับระบบหลัก
    - หรือการไม่ทราบว่ามีข้อมูลสำคัญใดบ้างที่ถูกจัดเก็บไว้ในระบบ
- **API10:2019 Insufficient Logging & Monitoring (การบันทึกและตรวจสอบระบบที่ไม่เพียงพอ)**
    - เกิดขึ้นเมื่อระบบไม่สามารถบันทึกกิจกรรมของผู้ใช้หรือเหตุการณ์ที่เกิดขึ้นภายในระบบได้อย่างละเอียดเพียงพอ
    - ซึ่งอาจทำให้ยากต่อการตรวจสอบหาสาเหตุของปัญหาหรือการโจมตี

โครงการอื่นๆ ของ OWASP (Other OWASP Projects)

นอกเหนือจากรายการความเสี่ยง 10 อันดับแรกของ OWASP (OWASP Top 10) แล้ว OWASP ยังมีโครงการอื่นๆ ที่มีประโยชน์ ดังนี้

- **OWASP Software Assurance Maturity Model (OWASP SAMM):**
    - เป็นกรอบการทำงานที่ใช้งานง่าย ช่วยให้องค์กรต่างๆ กำหนดและดำเนินกลยุทธ์ด้านความปลอดภัยของแอปพลิเคชัน
    - โดยปรับแต่งให้เหมาะสมกับความเสี่ยงทางธุรกิจที่เฉพาะเจาะจงขององค์กรนั้นๆ
- **OWASP Development Guide (คู่มือการพัฒนาของ OWASP):**
    - เป็นแนวทางปฏิบัติสำหรับการรักษาความปลอดภัยในระดับแอปพลิเคชัน
    - รวมถึงตัวอย่างโค้ด J2EE, ASP.NET และ PHP
- **OWASP Application Security Verification Standard (มาตรฐานการตรวจสอบความปลอดภัยของแอปพลิเคชัน OWASP):**
    - เป็นมาตรฐานสำหรับการดำเนินการตรวจสอบความปลอดภัยในระดับแอปพลิเคชัน
- และอื่นๆ อีกมากมาย

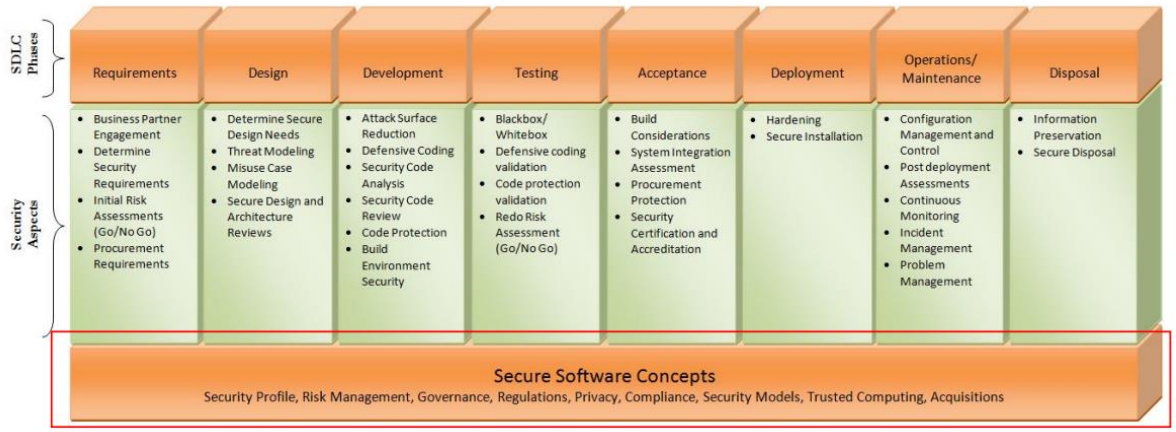
สำหรับรายละเอียดเพิ่มเติมเกี่ยวกับโครงการต่างๆ ของ OWASP สามารถดูได้ที่เว็บไซต์ OWASP: https://owasp.org/projects/

- OWASP ModSecurity Core Rule Set
- OWASP OWTF
- OWASP Risk Assessment Framework
- OWASP SAMM
- OWASP security Knowledge Framework
- OWASP Security Shepherd
- OWASP Top Ten
- OWASP Web Security Testing Guide
- OWASP ZAP
- OWASP Amass
- OWASP Application Security Verification Standard
- OWASP Cheat Sheet Series
- OWASP CSFRGuard
- OWASP Defectdojo
- OWASP Dependency-Check
- OWASP Dependency-Track
- OWASP Juice Shop
- OWASP Mobile Security Testing Guide
- OWASP Mobile Top 10

Secure Software Development Life Cycle

โมเดลการพัฒนาซอฟต์แวร์อย่างปลอดภัย (Secure Software Development Model)

โมเดลนี้เป็นกรอบแนวทางในการพัฒนาซอฟต์แวร์ที่คำนึงถึงความปลอดภัยตั้งแต่เริ่มต้นกระบวนการจนถึงการใช้งานจริง ช่วยลดความเสี่ยงช่องโหว่ด้านความปลอดภัย



ขั้นตอนต่างๆ ในโมเดล

1. **กำหนดความต้องการ (Requirements)**
    - การมีส่วนร่วมของพันธมิตรทางธุรกิจ (Business Partner Engagement)
    - กำหนดความต้องการด้านความปลอดภัย (Determine Security Requirements)
    - ประเมินความเสี่ยงเบื้องต้น (Initial Risk Assessments) เพื่อตัดสินใจเดินหน้าโครงการ (Go/No Go)
    - กำหนดความต้องการสำหรับการจัดซื้อ (Procurement Requirements)
2. **ออกแบบ (Design)**
    - กำหนดความต้องการด้านการออกแบบที่ปลอดภัย (Determine Secure Design Needs)
    - สร้างโมเดลภัยคุกคาม (Threat Modeling)
    - สร้างโมเดลกรณีใช้งานที่ไม่เหมาะสม (Misuse Case Modeling)
    - ทบทวนการออกแบบและสถาปัตยกรรมด้านความปลอดภัย (Secure Design and Architecture Reviews)
3. **พัฒนา (Development)**
    - ลดพื้นที่เสี่ยงต่อการโจมตี (Attack Surface Reduction)
    - การเขียนโค้ดเชิงป้องกัน (Defensive Coding)
    - การวิเคราะห์โค้ดด้านความปลอดภัย (Security Code Analysis)

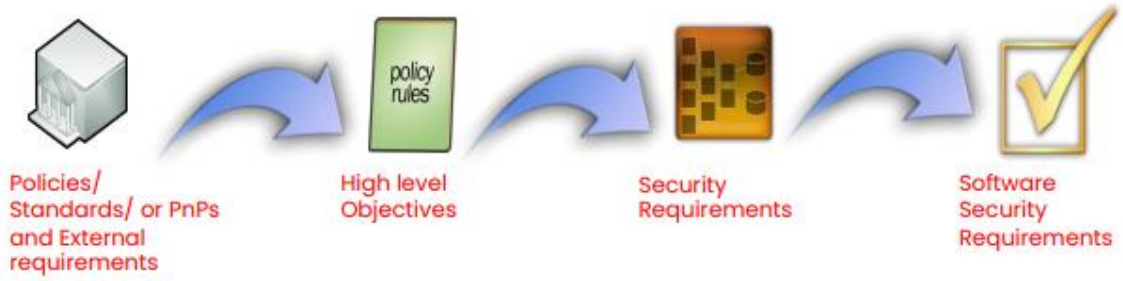
- การทบทวนโค้ดด้านความปลอดภัย (Security Code Review)
- การป้องกันโค้ด (Code Protection)
- สภาพแวดล้อมการบิลด์ (Build Environment)

4. **ทดสอบ (Testing)**
    - ทดสอบแบบกล่องดำ/กล่องขาว (Blackbox/Whitebox Testing)
    - ตรวจสอบการทำงานของการเขียนโค้ดเชิงป้องกัน (Defensive coding validation)
    - ตรวจสอบการทำงานของการป้องกันโค้ด (Code protection validation)
    - ประเมินความเสี่ยงอีกครั้ง (Redo Risk Assessment) เพื่อตัดสินใจเดินหน้าโครงการ (Go/No Go)
5. **การยอมรับ (Acceptance)**
    - พิจารณาการสร้าง (Build Considerations)
    - ประเมินการบูรณาการระบบ (System Integration Assessment)
    - ป้องกันการจัดซื้อ (Procurement Protection)
    - การรับรองและรับรองความถูกต้องด้านความปลอดภัย (Security Certification and Accreditation)
6. **การติดตั้ง (Deployment)**
    - การเสริมความแข็งแกร่งระบบ (Hardening)
    - การติดตั้งอย่างปลอดภัย (Secure Installation)
7. **การดำเนินงาน/การบำรุงรักษา (Operations/Maintenance)**
    - การจัดการและควบคุมการกำหนดค่า (Configuration Management and Control)
    - ประเมินหลังการติดตั้ง (Post deployment Assessments)
    - การตรวจสอบอย่างต่อเนื่อง (Continuous Monitoring)
    - การจัดการเหตุการณ์ (Incident Management)
    - การจัดการปัญหา (Problem Management)
8. **การกำจัด (Disposal)**
    - การเก็บรักษาข้อมูล (Information Preservation)
    - การกำจัดอย่างปลอดภัย (Secure Disposal)

แนวคิดด้านซอฟต์แวร์ความปลอดภัย (Security Software Concepts)

- โพรไฟล์ความปลอดภัย (Security Profile)
- การจัดการความเสี่ยง (Risk Management)
- ธรรมาภิบาล (Governance)
- ข้อบังคับ (Regulations)
- ความเป็นส่วนตัว (Privacy)
- การปฏิบัติตาม (Compliance)
- โมเดลความปลอดภัย (Security Models)
- การประมวลผลที่น่าเชื่อถือ (Trusted Computing)
- การจัดซื้อ (Acquisitions)

การรวบรวมความต้องการ (Requirements Elicitation)



การรวบรวมความต้องการ เป็นกระบวนการระบุ จัดกลุ่ม และกำหนดความต้องการของผู้มีส่วนได้ส่วนเสีย (Stakeholder) ต่างๆ เพื่อนำไปใช้ในการพัฒนาซอฟต์แวร์ ในส่วนนี้จะแยกประเภทความต้องการด้านความปลอดภัย ดังนี้

ความต้องการจากนโยบาย/มาตรฐาน/ระเบียบปฏิบัติภายในองค์กร (Policies/Standards/ or PnPs) และความต้องการภายนอก

- SOX (Sarbanes-Oxley Act): กฎหมายสหรัฐอเมริกาว่าด้วยการปฏิรูปการบัญชีบริษัทมหาชน
- PCI DSS (Payment Card Industry Data Security Standard): มาตรฐานความปลอดภัยข้อมูลสำหรับอุตสาหกรรมบัตรเครดิต
- นโยบายการรับรองความถูกต้อง (Authentication Policy)
- HIPAA (Health Insurance Portability and Accountability Act): กฎหมายสหรัฐอเมริกาว่าด้วยการโอนย้ายและความรับผิดชอบข้อมูลสุขภาพ

เป้าหมายระดับสูง (High level Objectives)

- การรักษาความลับ (Confidentiality): ข้อมูลต้องไม่ถูกเปิดเผยต่อบุคคลที่ไม่ได้รับอนุญาต
- การส่งข้อมูลอย่างปลอดภัย (Secure Transmission): ข้อมูลต้องถูกส่งผ่านเครือข่ายอย่างปลอดภัย
- ความเป็นส่วนตัว (Privacy): ข้อมูลส่วนบุคคลต้องได้รับการคุ้มครอง

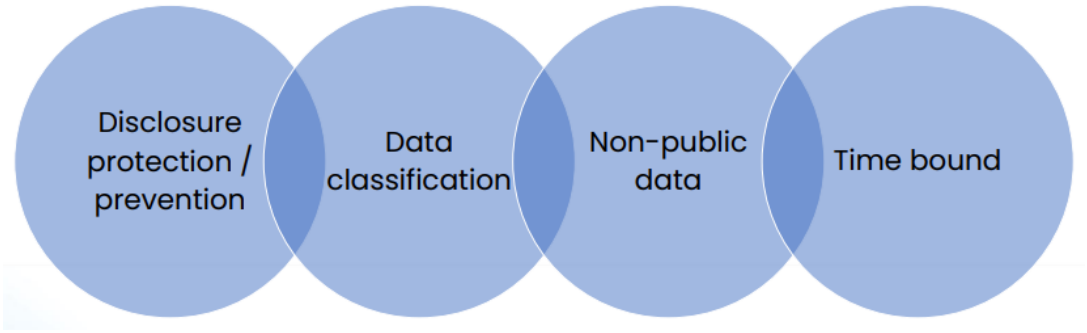
ความต้องการด้านความปลอดภัย (Security Requirements)

- การจัดประเภทและการจัดการข้อมูล (Information Classification & Handling): กำหนดวิธีการจัดประเภทข้อมูลตามความสำคัญและความละเอียดอ่อน
- การจัดการสิทธิ์ (Identity Management): ควบคุมการเข้าถึงข้อมูลของผู้ใช้งาน

ความต้องการด้านความปลอดภัยของซอฟต์แวร์ (Software Security Requirements)

- การตรวจสอบข้อมูลขาเข้า (Input Validation): ระบบต้องตรวจสอบข้อมูลที่ผู้ใช้ป้อนเข้ามาเพื่อป้องกันการโจมตีประเภท Input Validation
- การจัดการสถานการณ์ผิดพลาด (Exception Handling): ระบบต้องมีการจัดการกับสถานการณ์ที่ผิดพลาดอย่างเหมาะสมเพื่อป้องกันการโจมตี
- การเข้ารหัสข้อมูลขาออก (Output Encoding): ระบบต้องเข้ารหัสข้อมูลที่ส่งออกไปเพื่อป้องกันการดักฟังข้อมูล

ความต้องการด้านการรักษาความลับ (Confidentiality Requirements)



- **การป้องกันการเปิดเผยข้อมูล (Disclosure protection / prevention):** ข้อมูลต้องไม่ถูกเปิดเผยต่อบุคคลที่ไม่ได้รับอนุญาต
- **การจัดประเภทข้อมูล (Data classification):** ข้อมูลควรได้รับการจัดประเภทตามความสำคัญและความละเอียดอ่อน
- **ข้อมูลที่ไม่ใช่สาธารณะ (Non-public data):** ระบบต้องปกป้องข้อมูลที่ไม่ใช่ข้อมูลสาธารณะ
- **การกำหนดระยะเวลา (Time bound):** ข้อมูลต้องรักษาความลับเป็นเวลาที่กำหนดไว้

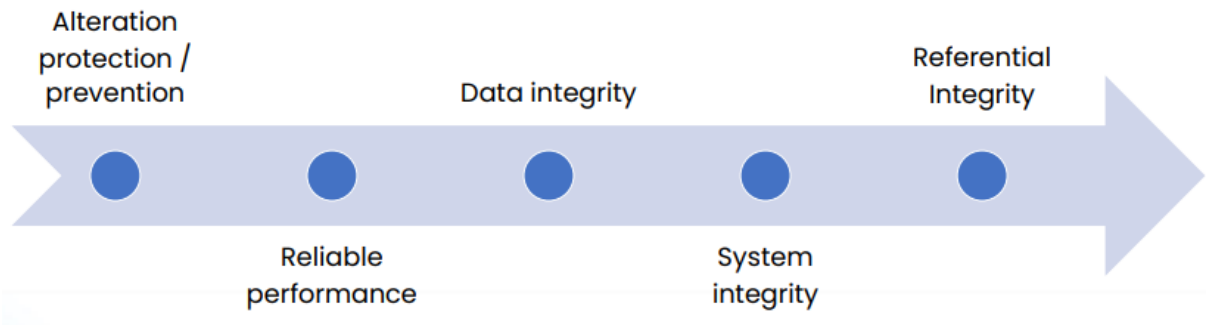
ระดับการรักษาความลับ (Confidentiality Levels)

- **ขณะข้อมูลอยู่นิ่ง (At Rest):** ข้อมูลต้องได้รับการป้องกันขณะที่ไม่ได้ใช้งาน
- **ขณะข้อมูลถูกส่งผ่าน (In Transit):** ข้อมูลต้องได้รับการป้องกันขณะที่ถูกส่งผ่านเครือข่าย
- **ขณะข้อมูลถูกใช้งาน (In Use):** ข้อมูลต้องได้รับการป้องกันขณะที่กำลังถูกใช้งาน

กลไกการรักษาความลับ (Confidentiality Mechanisms)

- **การเข้ารหัสข้อมูล (Encryption):** เปลี่ยนข้อมูลต้นฉบับให้เป็นรหัสเพื่อป้องกันการอ่านโดยไม่ได้รับอนุญาต
- **การสร้างค่าแฮช (Hashing):** สร้างค่าประจำตัว (hash) ของข้อมูลเพื่อตรวจสอบความถูกต้องของข้อมูล
- **การบังข้อมูล (Masking):** ปิดบังส่วนหนึ่งของข้อมูลที่ละเอียดอ่อน เช่น เลขประจำตัวประชาชน

ความต้องการด้านความถูกต้องสมบูรณ์ (Integrity Requirements)



- **การป้องกันการแก้ไขข้อมูล (Alteration protection / prevention):** ข้อมูลต้องปราศจากการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต
- **การทำงานที่เชื่อถือได้ (Reliable performance):** ระบบต้องทำงานได้อย่างถูกต้องและเชื่อถือได้
- **ความถูกต้องของข้อมูล (Data integrity):** ข้อมูลต้องถูกต้อง สมบูรณ์ และไม่ถูกเปลี่ยนแปลง
- **ความถูกต้องของระบบ (System integrity):** ระบบต้องทำงานได้อย่างถูกต้องตามที่ออกแบบ
- **ความสัมพันธ์ข้อมูลต้องถูกต้อง (Referential Integrity):** ความสัมพันธ์ระหว่างข้อมูลต่างๆ ในฐานข้อมูลต้องถูกต้อง

กลไกการรักษาความถูกต้องสมบูรณ์ (Integrity Mechanisms)

- **การตรวจสอบข้อมูลขาเข้า (Input Validation):** ระบบต้องตรวจสอบข้อมูลที่ผู้ใช้ป้อนเข้ามาเพื่อป้องกันการแก้ไขข้อมูล
- **การสร้างค่าแฮช (Hashing):** สร้างค่าประจำตัว (hash) ของข้อมูลเพื่อตรวจสอบความถูกต้องของข้อมูล
- **คุณสมบัติ ACID ของฐานข้อมูล (Database Integrity (ACID))**
    - **Atomicity (ความเป็นหน่วยเดียว):** ธุรกรรมฐานข้อมูลต้องสำเร็จทั้งชุดหรือล้มเหลวทั้งชุด
    - **Consistency (ความสอดคล้อง):** ข้อมูลในฐานข้อมูลต้องอยู่ในสถานะที่ถูกต้องตามกฎเกณฑ์ที่กำหนด
    - **Isolation (ความแยก):** ธุรกรรมฐานข้อมูลแต่ละชุดต้องไม่รบกวนซึ่งกันและกัน
    - **Durability (ความคงอยู่):** เมื่อธุรกรรมฐานข้อมูลสำเร็จแล้ว การเปลี่ยนแปลงข้อมูลจะถูกบันทึกอย่างถาวร

ความต้องการด้านความพร้อมใช้งาน (Availability Requirements)

- **การป้องกันการทำลายข้อมูล (Destruction protection / prevention):** ระบบต้องป้องกันข้อมูลจากการสูญหายหรือถูกทำลาย
- **การป้องกันการโจมตีแบบปฏิเสธการให้บริการ (Denial of Service prevention):** ระบบต้องสามารถให้บริการได้ตามปกติ แม้จะมีผู้พยายามโจมตีแบบปฏิเสธการให้บริการ

การรับรองความถูกต้อง (Authentication) – หลักพื้นฐาน

กระบวนการรับรองความถูกต้อง คือการยืนยันตัวตนของผู้ใช้งานก่อนอนุญาตให้เข้าถึงระบบ หลักพื้นฐานในการออกแบบระบบรับรองความถูกต้องมีดังนี้

- **อย่าสร้างระบบใหม่หากมีระบบที่มีอยู่แล้ว (Don’t reinvent the wheel):** ควรพิจารณาใช้ระบบรับรองความถูกต้องที่มีอยู่แล้ว เช่น ระบบไดเรกทอรีกลาง (Centralized Directory Service) แทนการสร้างระบบใหม่เอง
- **ใช้การรับรองความถูกต้องแบบผสาน (Integrated Authentication) (Kerberos, NTLM) ถ้าเป็นไปได้:** ระบบรับรองความถูกต้องแบบผสานจะอาศัยระบบเครือข่ายที่มีอยู่แล้ว ช่วยลดความยุ่งยากในการจัดการรหัสผ่านของผู้ใช้
- **ใช้ใบรับรองความถูกต้องของไคลเอ็นต์ (Client Certificates) ถ้าเป็นไปได้:** ใบรับรองความถูกต้องของไคลเอ็นต์เป็นวิธีการรับรองความถูกต้องที่ปลอดภัย เหมาะสำหรับการสื่อสารผ่านเครือข่ายสาธารณะ
- **ใช้การรับรองความถูกต้องแบบกำหนดเอง เฉพาะกรณีจำเป็น:** ควรพิจารณาสร้างระบบรับรองความถูกต้องแบบกำหนดเอง เฉพาะกรณีที่ระบบที่มีอยู่แล้วไม่สามารถตอบสนองความต้องการได้

ความต้องการด้านการอนุญาต (Authorization Requirements)

กระบวนการอนุญาต (Authorization) คือการกำหนดสิทธิ์ในการเข้าถึงทรัพยากรของระบบ โดยพิจารณาจากผลลัพธ์ของการรับรองความถูกต้อง (Authentication)

- **การร้องขอการเข้าถึงทรัพยากร (Resource request access):** ระบุทรัพยากรที่ผู้ใช้ต้องการเข้าถึง เช่น ไฟล์ โฟลเดอร์ หรือฐานข้อมูล

- **การอนุญาตให้ดำเนินการบางอย่างได้ (Allowed specific actions):** กำหนดสิทธิ์ว่าผู้ใช้สามารถดำเนินการอะไรกับทรัพยากรได้บ้าง เช่น อ่าน เขียน หรือลบข้อมูล
- **การอนุญาตขึ้นอยู่กับการรับรองความถูกต้อง (Layered on top of authentication):** ระบบจะพิจารณาสิทธิ์ของผู้ใช้จากผลลัพธ์ของการรับรองความถูกต้องเท่านั้น

บันทึกกิจกรรมระบบ (System Logging) - บันทึกอะไร?

ระบบบันทึกกิจกรรม (System Logging) เป็นกระบวนการบันทึกเหตุการณ์ต่างๆ ที่เกิดขึ้นภายในระบบ ข้อมูลเหล่านี้มีประโยชน์สำหรับการตรวจสอบ แก้ไขปัญหา และวิเคราะห์การรักษาความปลอดภัย

คำถามสำคัญคือ ควรบันทึกกิจกรรมอะไรบ้าง ได้แก่

- **ธุรกรรมทางธุรกิจที่สำคัญ (Critical business transactions):**
  เช่น การโอนเงิน การสร้างบัญชีผู้ใช้ใหม่ หรือการอนุมัติการสั่งซื้อ
  เพื่อให้สามารถตรวจสอบเส้นทางการเงิน การใช้งานสิทธิ์ และการเปลี่ยนแปลงข้อมูลสำคัญได้
- **ฟังก์ชันการดูแลระบบ (Administrative functionality):**
  เช่น การสร้างบัญชีผู้ใช้ การแก้ไขสิทธิ์การเข้าถึงข้อมูล หรือการกำหนดค่าระบบ
  เพื่อตรวจสอบการเปลี่ยนแปลงที่เกิดขึ้นภายในระบบ
- **ความพยายามเข้าสู่ระบบ (Authentication attempts):**
  ควรบันทึกความพยายามเข้าสู่ระบบทุกครั้ง รวมถึงกรณีที่เข้าสู่ระบบสำเร็จและไม่สำเร็จ
  เพื่อตรวจสอบการโจมตีแบบ Brute-Force หรือการใช้งานบัญชีผู้ใช้โดยไม่ได้รับอนุญาต

ข้อกำหนดอื่นๆ (Other Requirements)

- **สภาพแวดล้อมการติดตั้ง (Deployment Environment):** เช่น อินเทอร์เน็ต (Internet) อินทราเน็ต (Intranet) เอ็กซ์ทราเน็ต (Extranet) หรือ Demilitarized Zones (DMZs) จะส่งผลต่อการเลือกประเภทของข้อมูลที่ควรบันทึก
- **การเก็บรักษาข้อมูล (Archiving):** ควรมีแผนการสำหรับการเก็บรักษาข้อมูลที่บันทึกไว้ รวมถึงการกำหนดระยะเวลาในการเก็บรักษาข้อมูล
- **การรองรับผู้ใช้งานนานาชาติ (International):** หากระบบรองรับผู้ใช้งานนานาชาติ ควรพิจารณาการบันทึกข้อมูลที่เกี่ยวข้องกับไทม์โซนและการแปลภาษา
- **การจัดซื้อ (Procurement):** ข้อกำหนดจากการจัดซื้อ อาจมีผลต่อการเลือกโซลูชันระบบบันทึกกิจกรรม

ความรู้เบื้องต้นเกี่ยวกับการจัดการเหตุการณ์

(Introduction of Incident Management)

อะไรคือการจัดการเหตุการณ์ (What is Incident Management)?

เหตุการณ์ด้านความปลอดภัยคอมพิวเตอร์ (Computer Security Incident) คือ เหตุการณ์ที่ส่งผลกระทบต่อระบบโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ หรือมีความเสี่ยงที่จะส่งผลกระทบดังกล่าว

เหตุการณ์ (Event) คือ การเกิดขึ้นที่สังเกตได้ภายในระบบหรือเครือข่าย ซึ่งบางครั้งอาจเป็นสัญญาณเบื้องต้นที่บ่งบอกว่ากำลังเกิดเหตุการณ์ด้านความปลอดภัย

ประเภทของเหตุการณ์ (Incident Types)

- **การโจมตีด้วยรหัสประสงค์ร้าย (Malicious code attacks):** เช่น ไวรัส มัลแวร์
- **การเข้าถึงโดยไม่ได้รับอนุญาต (Unauthorized access):**
    - ความพยายามบุกรุก (Attempted intrusion)
    - การสืบลาดตระเวนสืบข้อมูล (Reconnaissance activity)
    - การรุกรานระบบ (System compromise/ intrusion)
- **สูญหาย ถูกโจรกรรมหรือสูญหายของทรัพย์สิน ข้อมูล ฯลฯ (Loss of, theft of or missing assets, data, etc.)**
- **การหยุดชะงักของบริการ (Disruption of service):** ระบบไม่สามารถให้บริการได้ตามปกติ
- **การใช้งานโดยไม่ได้รับอนุญาต/ การใช้ในทางที่ผิด (Unauthorized use / Misuse):** ละเมิดนโยบายการใช้งานระบบ
- **การกระทำผิดกฎหมาย (Illegal activity):** ใช้ระบบเพื่อกระทำผิดกฎหมาย
- **การจารกรรม (Espionage):** ลักขโมยข้อมูลสำคัญ
- **ข่าวลวง (Hoaxes):** ข้อมูลเท็จที่สร้างความเสียหาย

การจัดการเหตุการณ์ คือ การระบุ วิเคราะห์ ตอบสนอง และฟื้นฟูจากเหตุการณ์ด้านความปลอดภัย โดยมีเป้าหมายเพื่อลดความเสียหาย ควบคุมสถานการณ์ และป้องกันเหตุการณ์ที่คล้ายคลึงกันเกิดขึ้นอีก โดยมีเป้าหมายเป็นการกู้คืนการทำงานปกติของระบบอย่างรวดเร็วที่สุด และลดผลกระทบเชิงลบต่อธุรกิจให้น้อยที่สุด

ฟังก์ชันการตอบสนองต่อเหตุการณ์ของ NIST (NIST Incident Response Function)

ฟังก์ชันการตอบสนองต่อเหตุการณ์ของ NIST เป็นกรอบแนวทางที่องค์กรสามารถนำไปประยุกต์ใช้ในการจัดการกับเหตุการณ์ด้านความปลอดภัย โดยแบ่งเป็นขั้นตอนหลัก ดังนี้

1. การวางแผนการตอบสนอง (Response Planning)

- มีแผนการตอบสนองต่อเหตุการณ์ที่ชัดเจน โดยแผนจะถูกนำไปปฏิบัติระหว่างหรือหลังจากเกิดเหตุการณ์
- บุคลากรทุกคนทราบหน้าที่และลำดับการดำเนินการ เมื่อจำเป็นต้องตอบสนองต่อเหตุการณ์

2. การสื่อสาร (Communications)

- รายงานเหตุการณ์ตามเกณฑ์ที่กำหนดไว้
- แบ่งปันข้อมูลตามแผนการตอบสนองต่อเหตุการณ์
- ประสานงานกับผู้มีส่วนได้ส่วนเสียตามแผนการตอบสนองต่อเหตุการณ์
- แบ่งปันข้อมูลกับผู้มีส่วนได้ส่วนนอกองค์กรอย่างสมัครใจ เพื่อให้เกิดการรับรู้สถานการณ์ด้านความปลอดภัยไซเบอร์ร่วมกัน

3. การวิเคราะห์ (Analysis)

- ตรวจสอบการแจ้งเตือนจากระบบตรวจจับภัยคุกคาม
- ประเมินผลกระทบของเหตุการณ์
- ดำเนินการตรวจสอบ forensics เพื่อเก็บรวบรวมหลักฐานทางดิจิทัล
- จัดประเภทเหตุการณ์ตามแผนการตอบสนองต่อเหตุการณ์

4. การลดผลกระทบ (Mitigation)

- ควบคุมเหตุการณ์ไม่ให้แพร่หลาย (Containment)
- บรรเทาผลกระทบของเหตุการณ์ (Mitigation)
- ปรับปรุงช่องโหว่ที่ค้นพบใหม่ หรือ บันทึกเป็นความเสี่ยงที่ยอมรับได้

5. การปรับปรุง (Improvements)

- นำบทเรียนที่ได้จากเหตุการณ์ ไปปรับปรุงแผนการตอบสนองต่อเหตุการณ์
- ปรับปรุงกลยุทธ์การตอบสนองต่อเหตุการณ์ให้ทันสมัย

ทำไมเราจึงจำเป็นต้องมีการจัดการเหตุการณ์ (Why do we need Incident Management)?

- ไม่สามารถป้องกันและคาดการณ์เหตุการณ์ได้ทั้งหมด แม้ว่าจะมีการลดความเสี่ยงแล้วก็ตาม
- เทคโนโลยีใหม่ๆ อาจนำมาซึ่งรูปแบบของภัยคุกคามใหม่ๆ เช่น Zero Days Attacks (การโจมตีช่องโหว่ที่ยังไม่มีการแก้ไข)
- การจัดการเหตุการณ์เป็นกระบวนการที่ซับซ้อน
- เมื่อเกิดเหตุการณ์ ควรมีแผนการที่พร้อมดำเนินการทันที ไม่ใช่เพิ่งมาคิดตอนนั้น

วิธีการจัดการเหตุการณ์ (Incident Handling Methodology)

วิธีกาจัดการเหตุการณ์ (Incident Handling Methodology) คือ ชุดขั้นตอนที่องค์กรใช้ในการระบุ วิเคราะห์ ตอบสนอง และฟื้นฟูจากเหตุการณ์ด้านความปลอดภัย

1. แนวทางการตอบสนองต่อเหตุการณ์ (Incident Response & Handling Methodology)

แนวทางนี้มักแบ่งเป็น 4 ขั้นตอนหลัก ดังนี้

- **การเตรียมความพร้อม (Preparation):** กำหนดแผนการตอบสนองต่อเหตุการณ์ ทีมงาน บทบาท หน้าที่ และกระบวนการต่างๆ
- **การตรวจจับและวิเคราะห์ (Detection & Analysis):** ตรวจจับเหตุการณ์ที่เกิดขึ้น ประเมินผลกระทบ และเก็บรวบรวมข้อมูล
- **การควบคุม ปราบปราม และฟื้นฟู (Containment, Eradication & Recovery):** ควบคุมไม่ให้เหตุการณ์แพร่หลาย กำจัดสาเหตุของเหตุการณ์ และกู้คืนระบบให้กลับสู่สภาวะปกติ
- **กิจกรรมหลังเกิดเหตุการณ์ (Post Incident Activity):** ทบทวนเหตุการณ์ วิเคราะห์ข้อผิดพลาด และปรับปรุงแผนการตอบสนองต่อเหตุการณ์ให้ดียิ่งขึ้น

2. แนวทางแบบ 6 ขั้นตอน (Six Phase Approach)

- **กลยุทธ์การจัดการเหตุการณ์ (Incident Management Strategy):** กำหนดเป้าหมาย นโยบาย และกระบวนการต่างๆ
- **การเตรียมความพร้อม (Preparation)**
- **การระบุ (Identification):** ตรวจจับเหตุการณ์ที่เกิดขึ้น
- **การควบคุม (Containment)**
- **การปราบปราม (Eradication)**
- **การฟื้นฟู (Recovery)**
- **บทเรียนที่ได้รับ (Lessons learned):** ทบทวนเหตุการณ์ วิเคราะห์ข้อผิดพลาด และปรับปรุงแผนการตอบสนองต่อเหตุการณ์ให้ดียิ่งขึ้น

ทั้งสองแนวทางมีความคล้ายคลึงกัน โดยเน้นที่การเตรียมความพร้อม การตอบสนองต่อเหตุการณ์ และการฟื้นฟูระบบ องค์กรสามารถเลือกใช้แนวทางที่เหมาะสมกับขนาดและความซับซ้อนของระบบ

การเตรียมความพร้อมสำหรับการตอบสนองต่อเหตุการณ์ (Incident Response Preparation)

การเตรียมความพร้อมถือเป็นหัวใจสำคัญของการจัดการเหตุการณ์ด้านความปลอดภัย ขั้นตอนการเตรียมความพร้อมมีดังนี้

1. จัดตั้งทีมตอบสนองต่อเหตุการณ์ด้านคอมพิวเตอร์ (Computer Incident Response Team - CIRT)

- แต่งตั้งหัวหน้าทีมที่มีอำนาจในการตัดสินใจและระดมทรัพยากร
- จัดการฝึกอบรมให้กับทั้งทีมบริหารและทีมปฏิบัติการเบื้องต้น

2. จัดทำแผนการตอบสนองต่อเหตุการณ์ (Plan of Action)

- **ภารกิจ (Mission):** กำหนดเป้าหมายของทีม CIRT
- **กลยุทธ์และเป้าหมาย (Strategies and goals):** กำหนดกลยุทธ์และเป้าหมายในการตอบสนองต่อเหตุการณ์
- **การอนุมัติจากฝ่ายบริหาร (Management Approval):** แผนการตอบสนองต่อเหตุการณ์ต้องได้รับการอนุมัติจากฝ่ายบริหาร
- **แนวทางการจัดการเหตุการณ์ (Approach to incidents):** กำหนดแนวทางในการระบุ วิเคราะห์ ตอบสนอง และฟื้นฟูจากเหตุการณ์
- **การสื่อสาร (Communications):** กำหนดช่องทางและวิธีการสื่อสารภายในทีมและภายนอกองค์กร
- **ตัวชี้วัดประสิทธิภาพการตอบสนอง (Metrics for response):** กำหนดตัวชี้วัดประสิทธิภาพในการตอบสนองต่อเหตุการณ์
- **การฝึกอบรมและการทดสอบ (Training and Testing):** จัดการฝึกอบรมทีม CIRT และทดสอบแผนการตอบสนองต่อเหตุการณ์

3. เครื่องมือสำหรับทีม (Team Toolkit)

- **รายชื่อติดต่อ (Contact information):** รายชื่อผู้บริหาร ทีมงาน ผู้ติดต่อจาก Vendor และนโยบายการแจ้งปัญหา
- **ระบบติดตามปัญหา (Issue tracking system):** ระบบสำหรับติดตามสถานะของเหตุการณ์
- **สมาร์ทโฟน (Smartphones):** สำหรับการสื่อสารและการเข้าถึงเว็บไซต์ขณะปฏิบัติงานนอกสถานที่
- **ห้องปฏิบัติการชั่วคราว (War room):** สถานที่สำหรับทีม CIRT ประชุม วิเคราะห์ และแก้ไขปัญหา

- **เครื่องมือสำหรับการตรวจสอบ (Forensic tools):** คอมพิวเตอร์ที่ติดตั้งโปรแกรมสำหรับเก็บรวบรวมหลักฐานทางดิจิทัล
- **อุปกรณ์และความรู้ในการรวบรวมหลักฐาน (Evidence gathering accessories and knowledge):** อุปกรณ์และความรู้ที่จำเป็นสำหรับการเก็บรวบรวมหลักฐานทางดิจิทัล
- **ข้อมูลและแผนผังการกำหนดค่าเครือข่าย (Detailed network configuration data and diagrams access):** สิทธิ์เข้าถึงข้อมูลและแผนผังการกำหนดค่าเครือข่าย

บริการของทีมตอบสนองต่อเหตุการณ์ (Incident Response Team Services)

- พัฒนากระบวนการตอบสนองต่อเหตุการณ์
- ฝึกซ้อมแผนการตอบสนองต่อเหตุการณ์
- การฝึกอบรมและพัฒนาศักยภาพของทีม
- ประเมินความเสี่ยง
- ระบบตรวจจับการบุกรุก
- การให้ความรู้และสร้างความตระหนัก
- ติดตามเทคโนโลยีด้านความปลอดภัย

ทีมตอบสนองต่อเหตุการณ์ด้านคอมพิวเตอร์ (Incident Response Team)

ทีมตอบสนองต่อเหตุการณ์ด้านคอมพิวเตอร์ (Computer Security Incident Response Team - CSIRT) มีหน้าที่ในการระบุ วิเคราะห์ ตอบสนอง และฟื้นฟูจากเหตุการณ์ด้านความปลอดภัย องค์กรสามารถเลือกใช้วิธีการจัดตั้งทีม CSIRT ได้ 3 รูปแบบ ดังนี้

- **ทีมภายในองค์กร (Employees):** องค์กรจัดตั้งทีม CSIRT ด้วยพนักงานภายในองค์กร
- **ทีมผสมผสาน (Partially Outsourced):** องค์กรจัดตั้งทีม CSIRT ด้วยการผสมผสานระหว่างพนักงานภายในองค์กรและทีมจากภายนอก
- **ทีมภายนอกองค์กร (Fully Outsourced):** องค์กรว่าจ้างทีม CSIRT จากภายนอกองค์กร

การเลือกรูปแบบของทีม (Team Model Selection)

ปัจจัยต่างๆ ที่ควรพิจารณาในการเลือก รูปแบบของทีม CSIRT ได้แก่

- **ความจำเป็นในการให้บริการตลอด 24 ชั่วโมง 7 วัน (The Need for 24/7 Availability)**
- **สมาชิกทีมแบบเต็มเวลา (Full-Time Versus Part-Time Team Members)**
- **ขวัญกำลังใจของพนักงาน (Employee Morale):** การให้พนักงานทำงานในทีม CSIRT อาจส่งผลต่อขวัญกำลังใจหรือไม่
- **ต้นทุน (Cost):** องค์กรมีงบประมาณในการจัดตั้งทีม CSIRT มากน้อยแค่ไหน
- **ความเชี่ยวชาญของทีม (Staff Expertise):** องค์กรมีบุคลากรที่มีความเชี่ยวชาญด้านความปลอดภัยเพียงพอหรือไม่
- **โครงสร้างองค์กร (Organizational Structures):** โครงสร้างองค์กรของแต่ละแห่งมีความเหมาะสมกับรูปแบบทีม CSIRT แบบใด

แผนการตอบสนองต่อเหตุการณ์ (Incident Response Plan)

เป็นเอกสารที่กำหนดแนวทางในการระบุ วิเคราะห์ ตอบสนอง และฟื้นฟูจากเหตุการณ์ด้านความปลอดภัยกระบวนการในการจัดทำแผนการตอบสนองต่อเหตุการณ์ มีดังนี้

- **ระบุความต้องการ (Identify):** ระบุความต้องการ ขอบเขต และเป้าหมายของแผน
- **พัฒนาแผน (Develop):** กำหนดขั้นตอน บทบาท หน้าที่ และกระบวนการต่างๆ
- **ตรวจสอบแผน (Verify):** ทดสอบแผนเพื่อตรวจสอบความถูกต้องและประสิทธิภาพ
- **ฝึกซ้อมแผน (Exercise):** ฝึกซ้อมแผนการตอบสนองต่อเหตุการณ์
- **บทเรียนที่ได้รับ (Lesson Learn):** ทบทวนผลการฝึกซ้อม นำข้อผิดพลาดมาปรับปรุงแผนให้ดียิ่งขึ้น

SOSECURE

- ALL IN ONE - CYBERSECURITY

About me
Watcharaphon Wongaphai

- CEO/Founder SOSECURE
- (ISC)²® Announces 2015 Asia-Pacific Information Security Leadership Achievements (ISLA)
- The Hacker TV Show
- Guest Speaker Master Degree “Cybersecurity”
  - Penetration Testing
  - Digital Forensics
  - SOC Operation & Analysis

My Certification

SOSECURE

SANS

ISC2

CISSP® Certified Information Systems Security Professional

SSCP® Systems Security Certified Practitioner

EC-Council

C|EH™ Certified Ethical Hacker

E|CSA™ EC-Council Certified Security Analyst

CompTIA

Microsoft

Microsoft CERTIFIED Trainer

MCSA Microsoft CERTIFIED Solutions Associate

Course Agenda

- Cybersecurity Threat & Attack
- Overview Cybersecurity Framework
- Infrastructure Security
- Cloud Security
- Application Security
- Incident Response and Handling

Cybersecurity Threat

Cybersecurity Terminology

- **Intrusion Detection**
  - The process and methods for analyzing information from networks and information systems to determine if a security breach or security violation has occurred.
- **Exploit**
  - To use something to one's own advantage is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized)
- **Malware**
  - An umbrella term that describes all forms of malicious software designed to wreak havoc on a computer. Common forms include: viruses, trojans, worms and ransomware.
- **Breach**
  - Any incident that results in unauthorized access of **data**, applications, services, networks and/or devices by bypassing their underlying **security Controls**

Cybersecurity Terminology

- **Ransomware**
  - A form of malware that deliberately prevents you from accessing files on your computer – holding your data hostage. It will typically encrypt files and request that a ransom be paid in order to have them decrypted or recovered.
- **Bot / Botnet**
  - A type of soft ware application or script that performs tasks on command, allowing an attacker to take complete control remotely of an affected computer.
- **Distributed Denial of Service (DDoS)**
  - A form of cyber attack This attack aims to make a service such as a website unusable by “flooding” it with malicious traffic or data from multiple sources (often botnets).
- **Phishing / Spear Phishing**
  - A technique used by hackers to obtain sensitive information.For example, using hand-crafted email messages designed to trick people into divulging personal or confidential data such as passwords and bank account information.

What Are The Threat Actors Seeking?

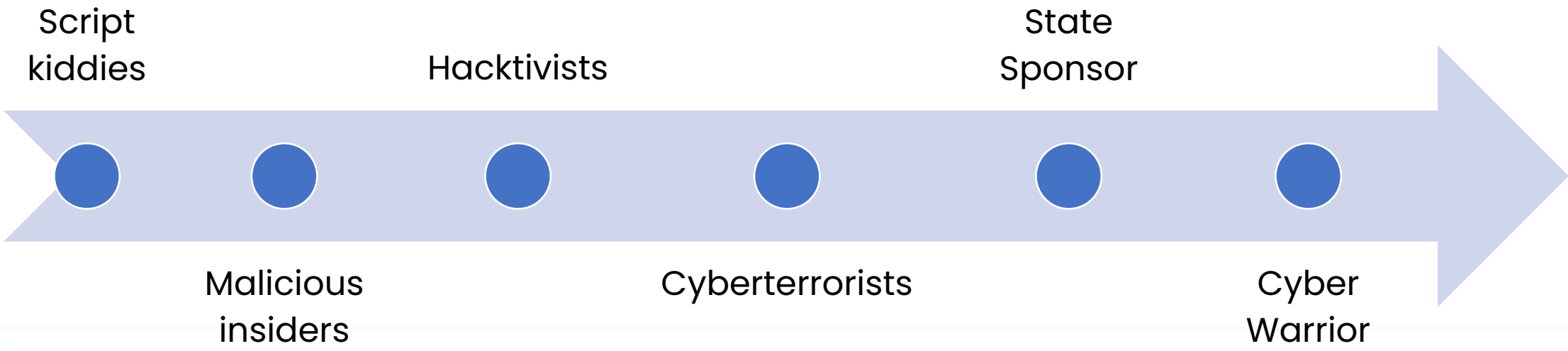
Threat actors want data and secrets, and/or to blackmail/extort money from your organization

- Usernames and passwords
- Sensitive company documents
- Protected Health Information (PHI)
- Credit card and banking information
- Export controlled technologies
- Intellectual property and sensitive technological documents
- Personal Identifying Information (PII)
- Contact lists (emails, phone directories, etc.)
- Confidential Emails

Internet Cybersecurity Risk

- System Compromised
- Identity Theft
- Social Engineering Attack
- Data Leakage
- Web Defacement
- Malware Infection (APT)
- Denial of Service

Type of Threat Actor



Cybersecurity Threat

- Scanning & Vulnerability Assessment
- Malware
  - Key Logger
  - Trojan
  - Botnet
  - Rootkit
  - Ransomware
  - Adware
  - Spyware

Cybersecurity Threat

- Password Cracking
- Sniffing
- Exploitation (Buffer Overflow)
  - Remote Exploitation
  - Local Exploitation
  - Client side Exploitation
  - Server side Exploitation
- Denial of Service & Distributed Denial of Service
- Social Engineering

What is Denial of Service Attack?

- **Denial-of-service attack** (**DoS attack**) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to a network. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled

- **Distributed denial-of-service attack** (**DDoS attack**), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source

Introduction to Denial of Service Attack

ATTACK IS LAUNCHED...

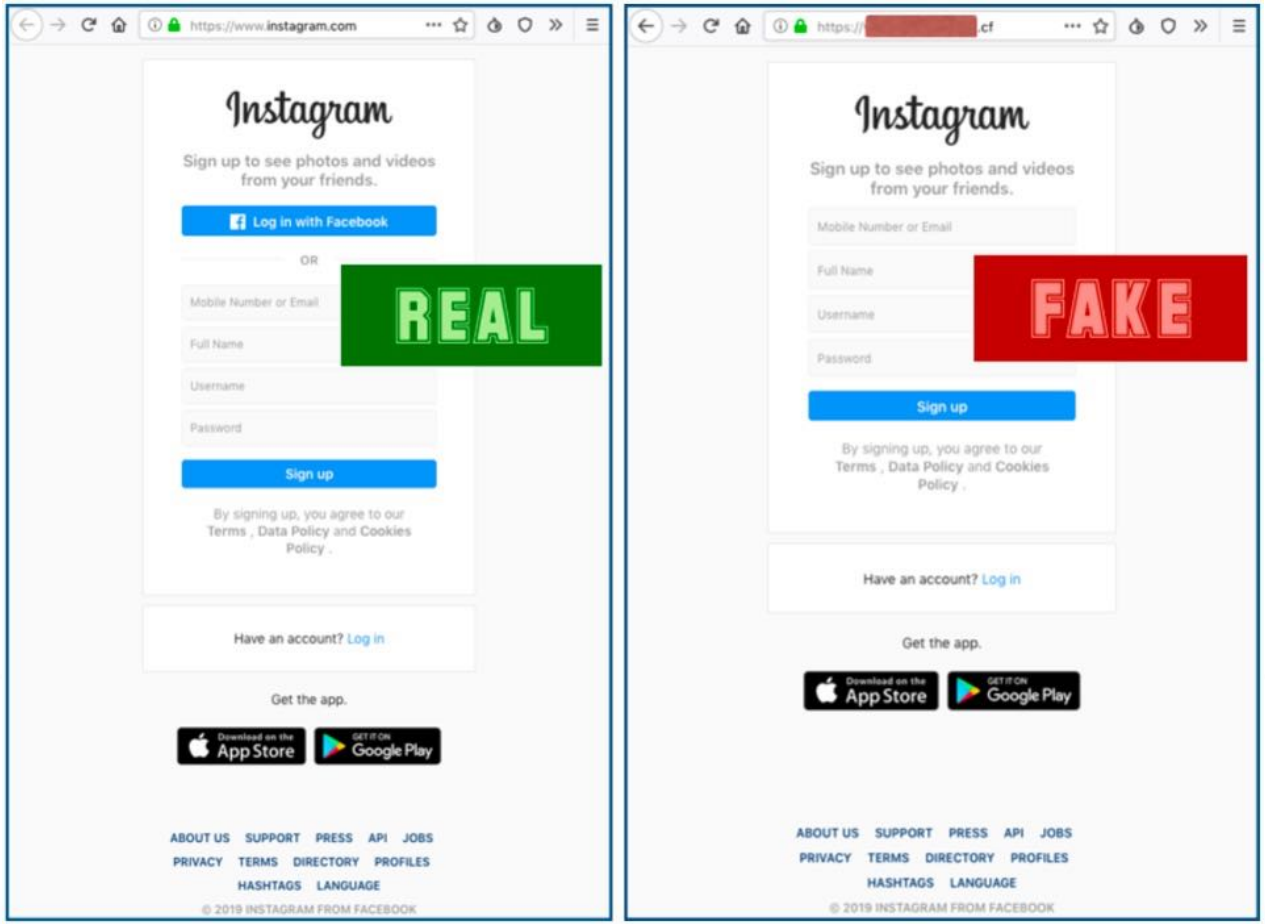
	STOPPING SERVICES	EXHAUSTING RESOURCES
LOCALLY	• Process killing • System reconfiguring • Process crashing	• Forking processes to fill the process table • Filling up the whole file system
REMOTELY	• Malformed packet attacks (e.g., Land, Teardrop, etc.)	• Packet floods, (e.g., SYN Flood, Smurf, Distributed Denial of Service

Types of Social Engineering

- Spoofing
- Impersonation
- Hoax
- Phishing
- Vishing
- Whaling
- URL hijacking/typo squatting
- Spam and spim
- Shoulder surfing
- Dumpster diving
- Tailgating

Phishing Attack

Example of Phishing Page



Spear Phishing Attack

How Does Spear Phishing Work

Hacker Identifies a target and researches victim

Hacker sends a targeted email to the user

User provides sensitive info or credentials

System is infected and the hacker uses access to steal data or traverse network.

Email SCAM

Subject: Re: Change of EFT Details
Date: 2016-07-15 02:27
From:
To:
Reply-To:

SCAM REMITTANCE ADVICE EMAIL WITH SCAM LETTER

Dear Sir/Madam,

Further to our discussion, please find attached a letter confirming a change in our account details and a paying in slip as confirmation. Please note a change in our remittance email also.

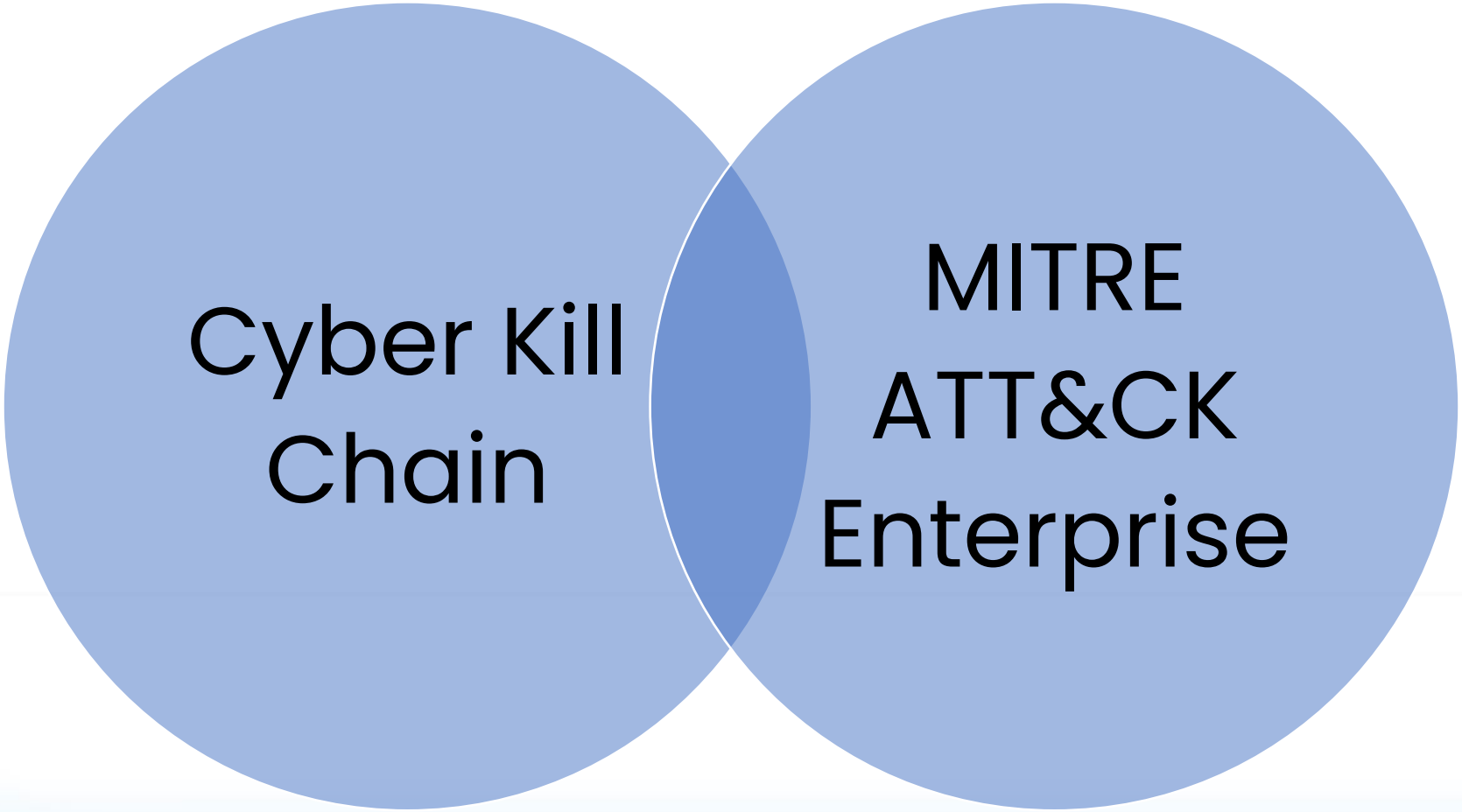
Will you be kind enough to send an email to confirm once the changes have been applied to our account.

Kind Regards,

ACCOUNTS MANAGER

T: +61
E:
W

Cyber Attack Methodology



Phases of the Intrusion Kill Chain

Research, identification, and selection of targets

Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files)

Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)

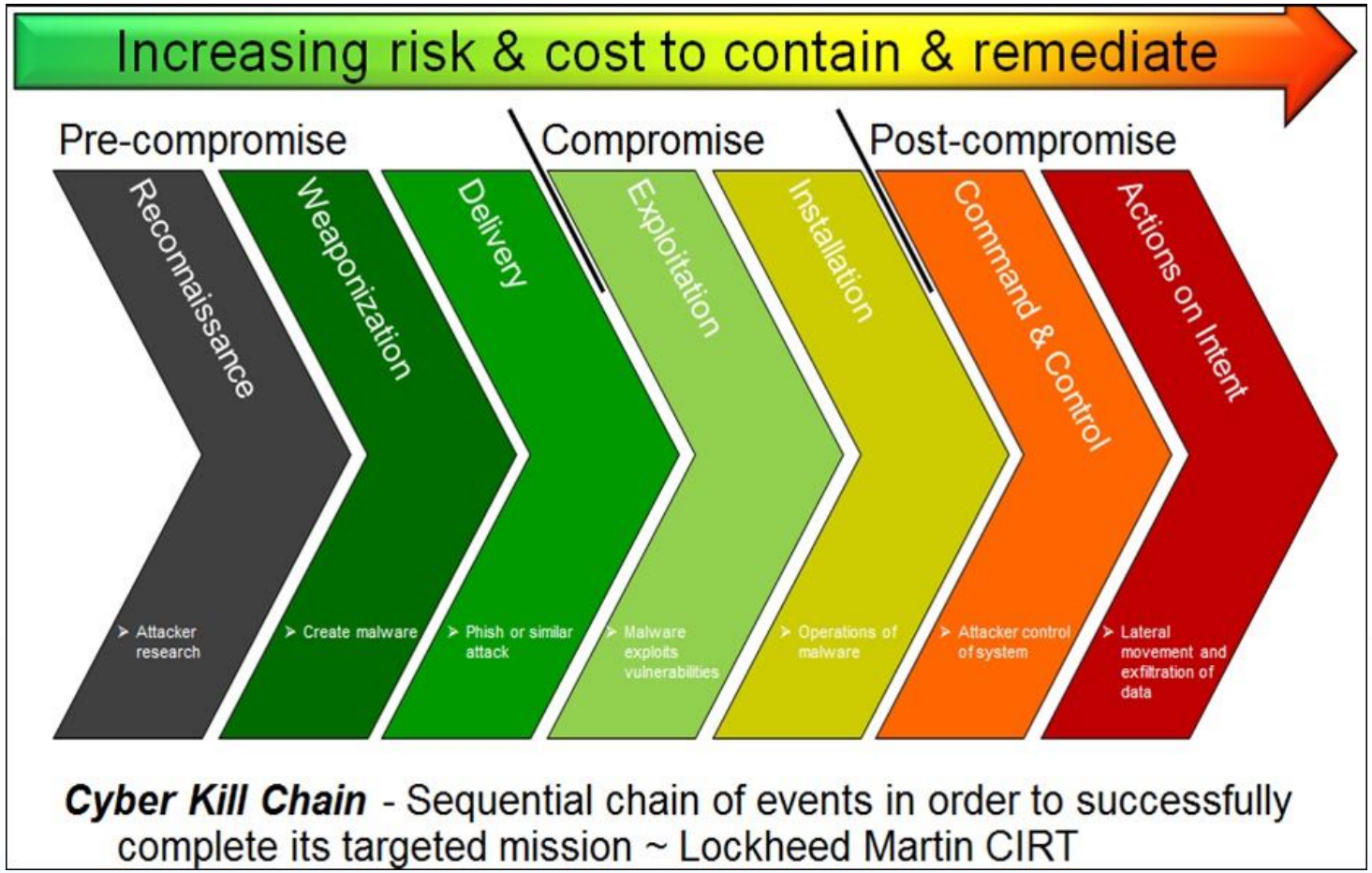
Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems

The weapon installs a backdoor on a target's system allowing persistent access

Outside server communicates with the weapons providing "hands on keyboard access" inside the target's network.

The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target

Cyber Kill chain



Cyber Kill Chain - Sequential chain of events in order to successfully complete its targeted mission ~ Lockheed Martin CIRT

ATT&CK for Enterprise

PRE-ATT&CK

Priority Definition
- Planning, Direction

Target Selection
Information Gathering
- Technical, People, Organizational

Weakness Identification
- Technical, People, Organizational

Adversary OpSec
Establish & Maintain Infrastructure
Persona Development
Build Capabilities
Test Capabilities
Stage Capabilities

Enterprise ATT&CK

Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command and Control

MITRE ATT&CK Techniques

https://attack.mitre.org/

ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking

MITRE ATT&CK Enterprise Tactics

SOSECURE

ID	Name	Description
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

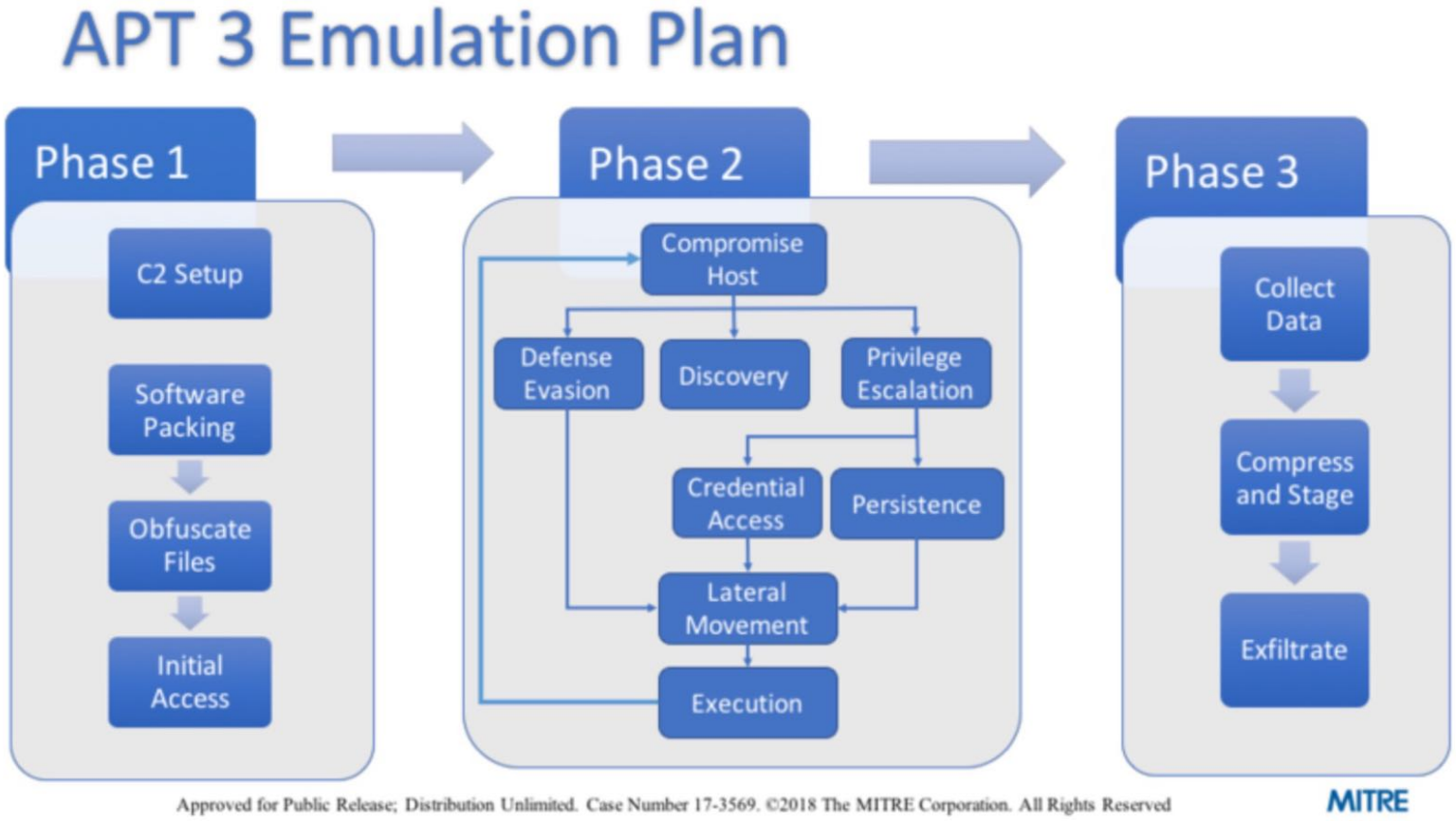
MITRE ATT&CK Techniques

SOSECURE

Techniques: 59

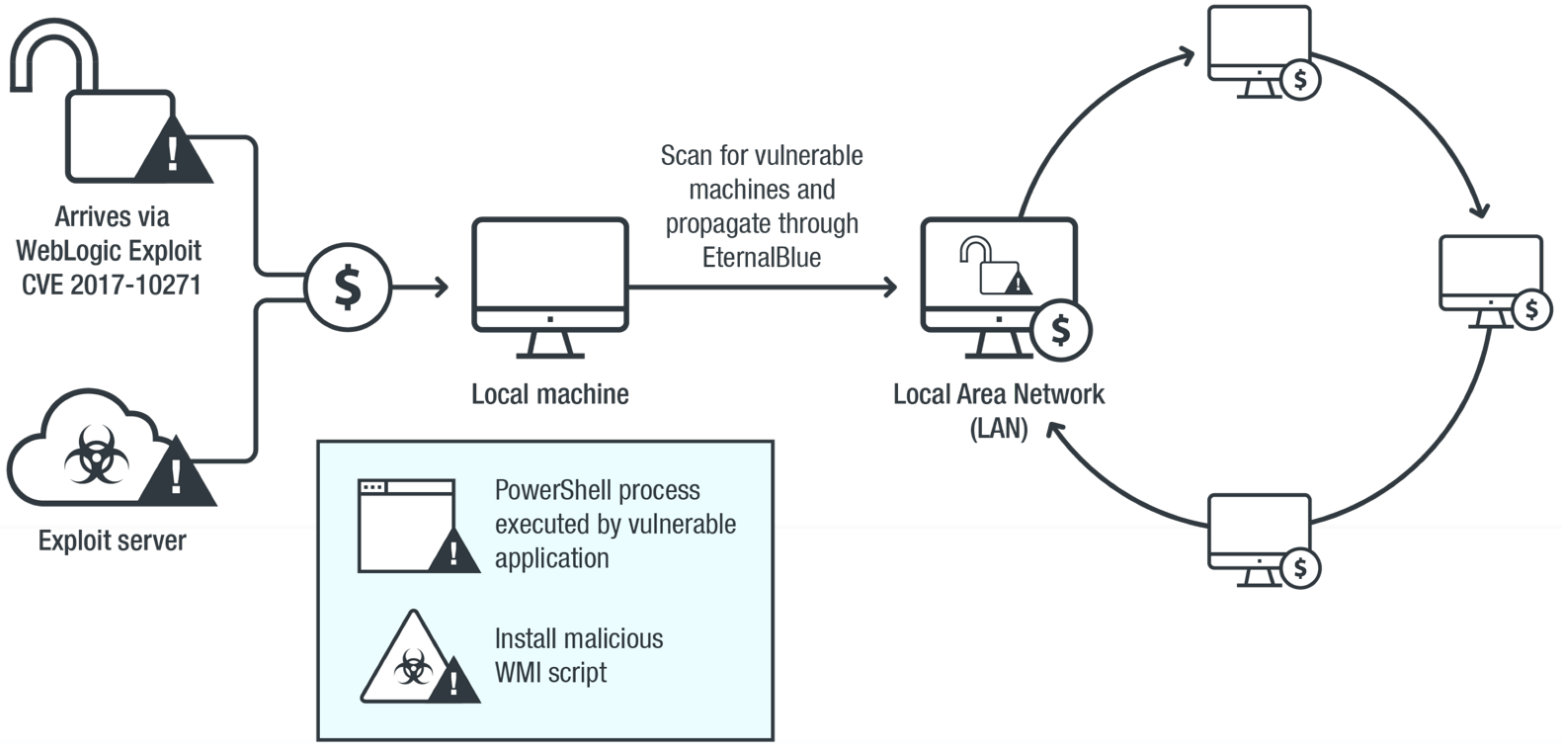
ID	Name	Description
T1156	.bash_profile and .bashrc	`~/.bash_profile` and `~/.bashrc` are executed in a user's context when a new shell opens or when a user logs in so that their environment is set correctly. `~/.bash_profile` is executed for login shells and `~/.bashrc` is executed for interactive non-login shells. This means that when a user logs in (via username and password) to the console (either locally or remotely via something like SSH), `~/.bash_profile` is executed before the initial command prompt is returned to the user. After that, every time a new shell is opened, `~/.bashrc` is executed. This allows users more fine grained control over when they want certain commands executed.
T1015	Accessibility Features	Windows contains accessibility features that may be launched with a key combination before a user has logged in (for example, when the user is on the Windows logon screen). An adversary can modify the way these programs are launched to get a command prompt or backdoor without logging in to the system.
T1098	Account Manipulation	Account manipulation may aid adversaries in maintaining access to credentials and certain permission levels within an environment. Manipulation could consist of modifying permissions, modifying credentials, adding or changing permission groups, modifying account settings, or modifying how authentication is performed. These actions could also include account activity designed to subvert security policies, such as performing iterative password updates to subvert password duration policies and preserve the life of compromised credentials. In order to create or manipulate accounts, the adversary must already have sufficient permissions on systems or the domain.
T1182	AppCert DLLs	Dynamic-link libraries (DLLs) that are specified in the AppCertDLLs value in the Registry key `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager` are loaded into every process that calls the ubiquitously used application programming interface (API) functions CreateProcess, CreateProcessAsUser, CreateProcessWithLoginW, CreateProcessWithTokenW, or WinExec.

Adversary Emulation Plans

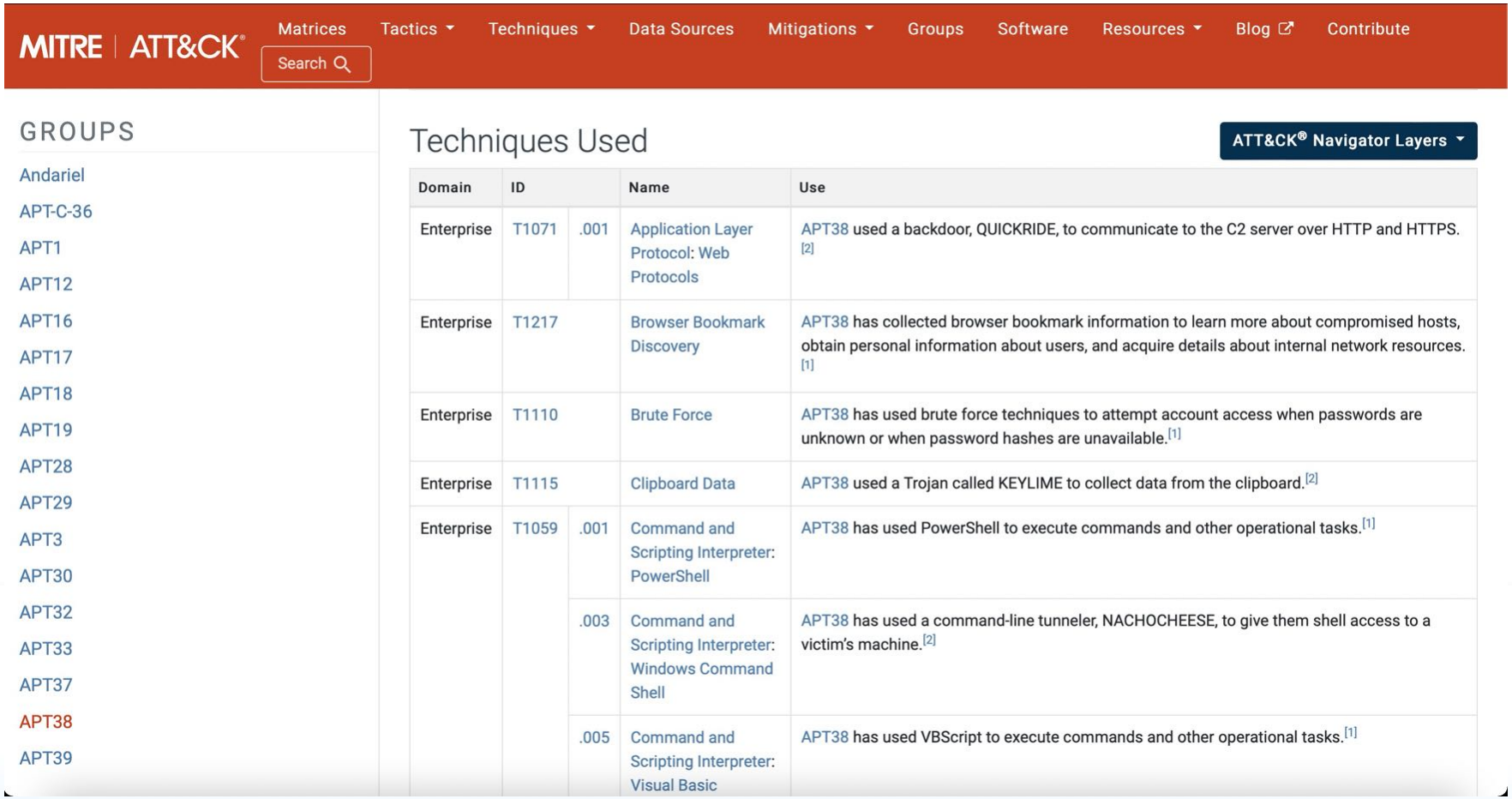


https://attack.mitre.org/resources/adversary-emulation-plans/

Example of APT (Advanced ,Persistent ,Threat)



Example of APT



Overview Cybersecurity

Security Objectives

- **Confidentiality**
  - "Preserving authorized restriction on information access and disclosure, including means for protecting personal privacy and proprietary information." (44 USC Sec. 3542)

- **Integrity**
  - "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity." (44 USC Sec. 3542)

- **Availability**
  - "Ensuring timely and reliable access and use of information." (44 USC Sec. 3542)

Security Implementation Principles

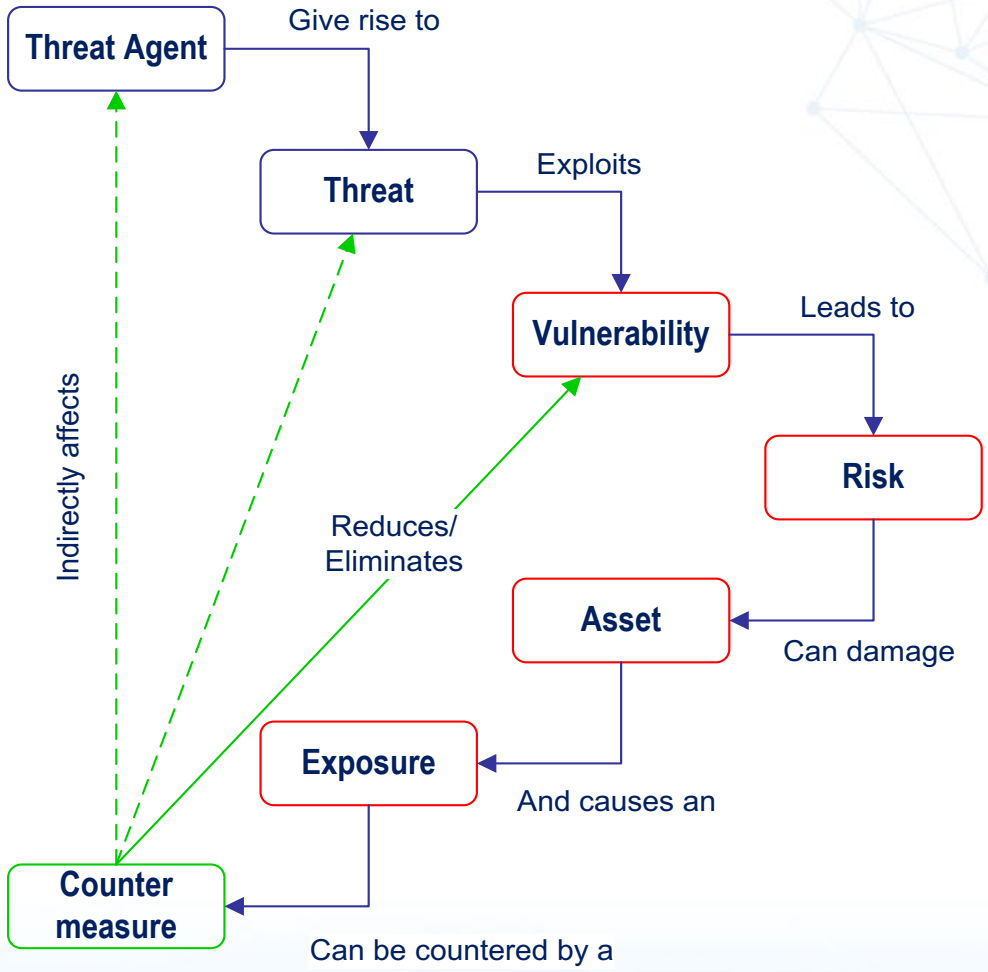
- **Confidentiality**, **Integrity**, **Availability**
- **Need-to-know**
  - Users should only have access to information (or systems) that enable them to perform their assigned job functions.
- **Least privilege**
  - Users should only have sufficient access privilege that allow them to perform their assigned work.
- **Separation of duties**
  - No person should be responsible for completing a task involving sensitive, valuable or critical information from the beginning to end.
  - No single person should be responsible for approving his/her own work.

Security Best Practices

- Security Domain
- Compartmentalization
- Need-to-know
- Least privilege
- Separation of duties
- Job rotation
  - To reduce risk of collusion
  - To ensure no single point of failure
- Mandatory vacation
  - To allow auditors to review records

Relationships between Threat, Risk, and Countermeasure

- **Threat Agent.**
  An entity that may act on a vulnerability.
- **Threat.**
  Any potential danger to information life cycle.
- **Vulnerability.**
  A weakness or flaw that may provide an opportunity for a threat agent.
- **Risk.**
  The likelihood of a threat agent exploits the discovered vulnerability.
- **Exposure.**
  An instance of being compromised by a threat agent.
- **Countermeasure / safeguard.**
  An administrative, operational, or logical mitigation against potential risk(s).



Reference: *Information Assurance Technical Framework (IATF)*, Release 2.3

Security Controls

- "Security controls are the management, operational, and technical safeguards or countermeasures employed within an organizational information system to protect the confidentiality, integrity, and availability of the system and its information."

  - What security controls are needed to adequately mitigate the risk incurred by the use of information and information systems in the execution of organizational missions and business functions?
  - Have the selected controls or is there a realistic plan for their implementation?
  - What is the desired or required level of assurance (i.e., grounds for confidence) that the selected security controls, as implemented are effective in their application?

Reference: NIST SP 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems.*

Categories of Security Controls

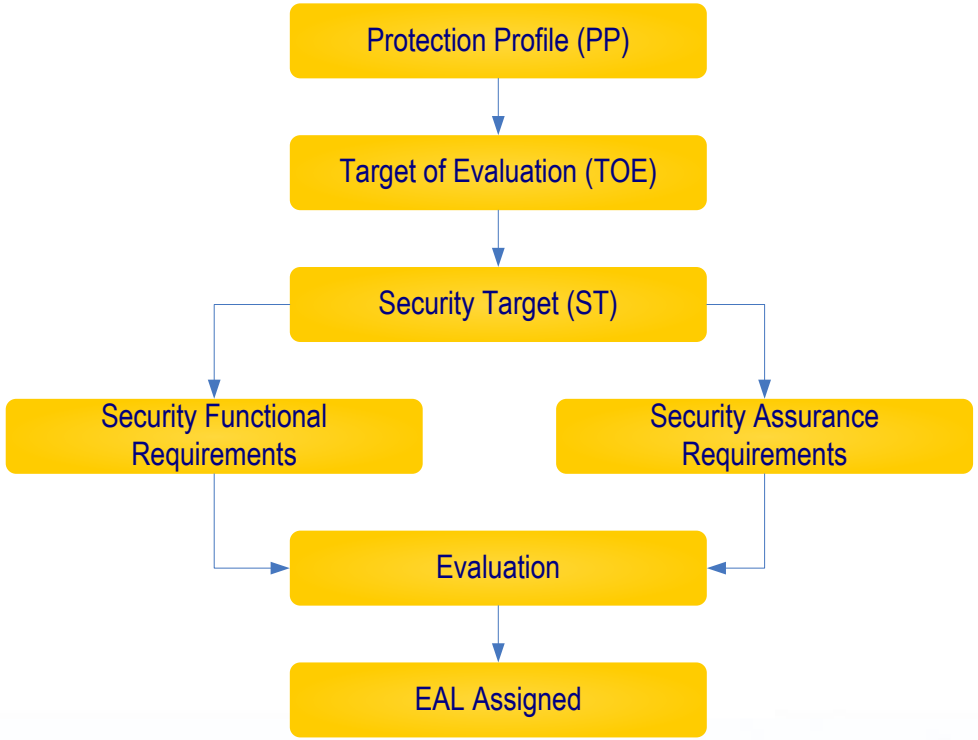
- **Management (Administrative) Controls.**
  - Policies, Standards, Processes, Procedures, & Guidelines
    - Administrative Entities: Executive-Level, Mid.-Level Management
- **Operational (and Physical) Controls.**
  - Operational Security (Execution of Policies, Standards & Process, Education & Awareness)
    - Service Providers: IA, Program Security, Personnel Security, Document Controls (or CM), HR, Finance, etc
  - Physical Security (Facility or Infrastructure Protection)
    - Locks, Doors, Walls, Fence, Curtain, etc.
    - Service Providers: FSO, Guards, Dogs
- **Technical (Logical) Controls.**
  - Access Controls, Identification & Authorization, Confidentiality, Integrity, Availability, Non-Repudiation.
    - Service Providers: Enterprise Architect, Security Engineer, CERT, NOSC, Helpdesk.

Categories of Security Controls

CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
	Planning	PL
	System and Services Acquisition	SA
	Security Assessment and Authorization	CA
	Program Management	**PM**
Operational	Personnel Security	PS
	Physical and Environmental Protection	PE
	Contingency Planning	CP
	Configuration Management	CM
	Maintenance	MA
	System and Information Integrity	SI
	Media Protection	MP
	Incident Response	IR
	Awareness and Training	AT
Technical	Identification and Authentication	IA
	Access Control	AC
	Audit and Accountability	AU
	System and Communications Protection	SC

Concept of Security Requirements & Common Criteria (ISO/IEC 15408)

- The new draft NIST SP 800-53, Rev. 4 now maps its security controls to Common Criteria



Reference:

- Draft NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, February 2013.
- ISO/IEC 15408, *Common Criteria Evaluation & Validation Scheme (CCEVS)*, Version 2.3, August 2005.

Types of Security Controls

- **Directive Controls.** Often called administrative controls, these are intended to advise employees of the behavior expected of them during their interfaces with or use the organization's information systems.
- **Preventive Controls.** Included in preventive controls are physical, administrative, and technical measures intended to preclude actions violating policy or increasing risk to system resources.
- **Detective Controls.** Detective controls involve the use of practices, processes, and tools that identify and possibly react to security violations.
- **Corrective Controls.** Corrective controls also involve physical, administrative, and technical measures designed to react to detection of an incident in order to reduce or eliminate the opportunity for the unwanted event to recur.
- **Recovery Controls.** Once an incident occurs that results in the compromise of integrity or availability, the implementation of recovery controls is necessary to restore the system or operation to a normal operating state.

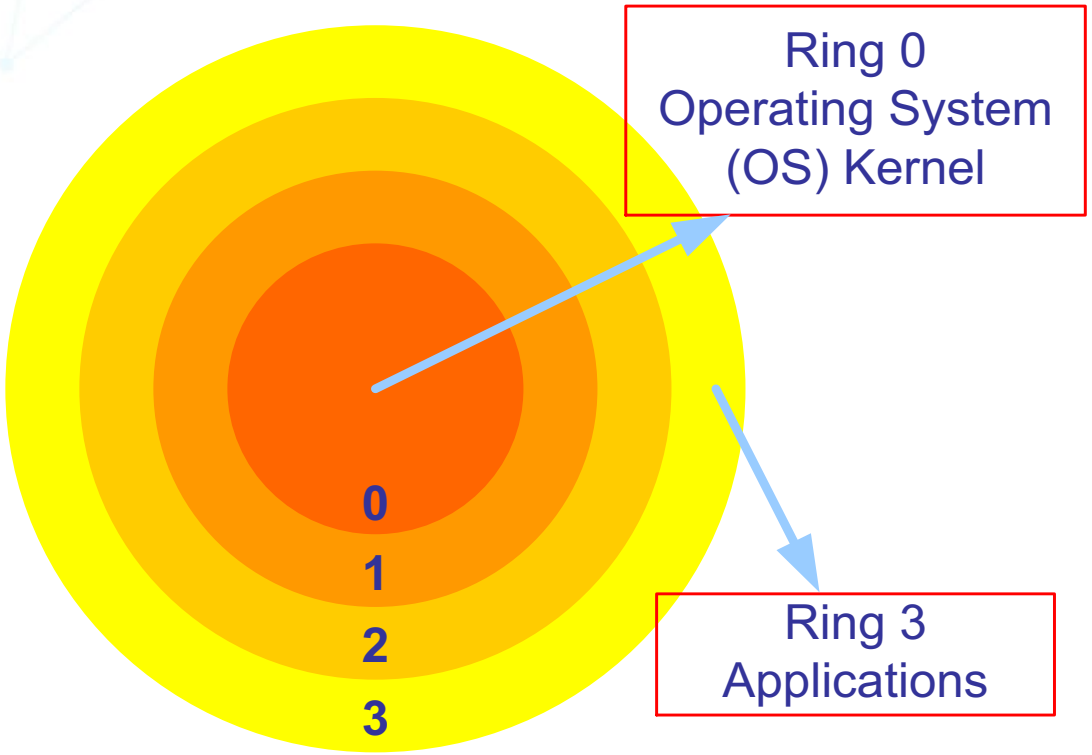
Reference: *CISM Review Manual – 2007*, ISACA.

Due Care vs. Due Diligence

- **Due Care**
  - Policies and implemented actions that an organization has taken to minimize risk to its tangible and intangible assets (i.e. information assets, customers, employees, resources and reputation.)

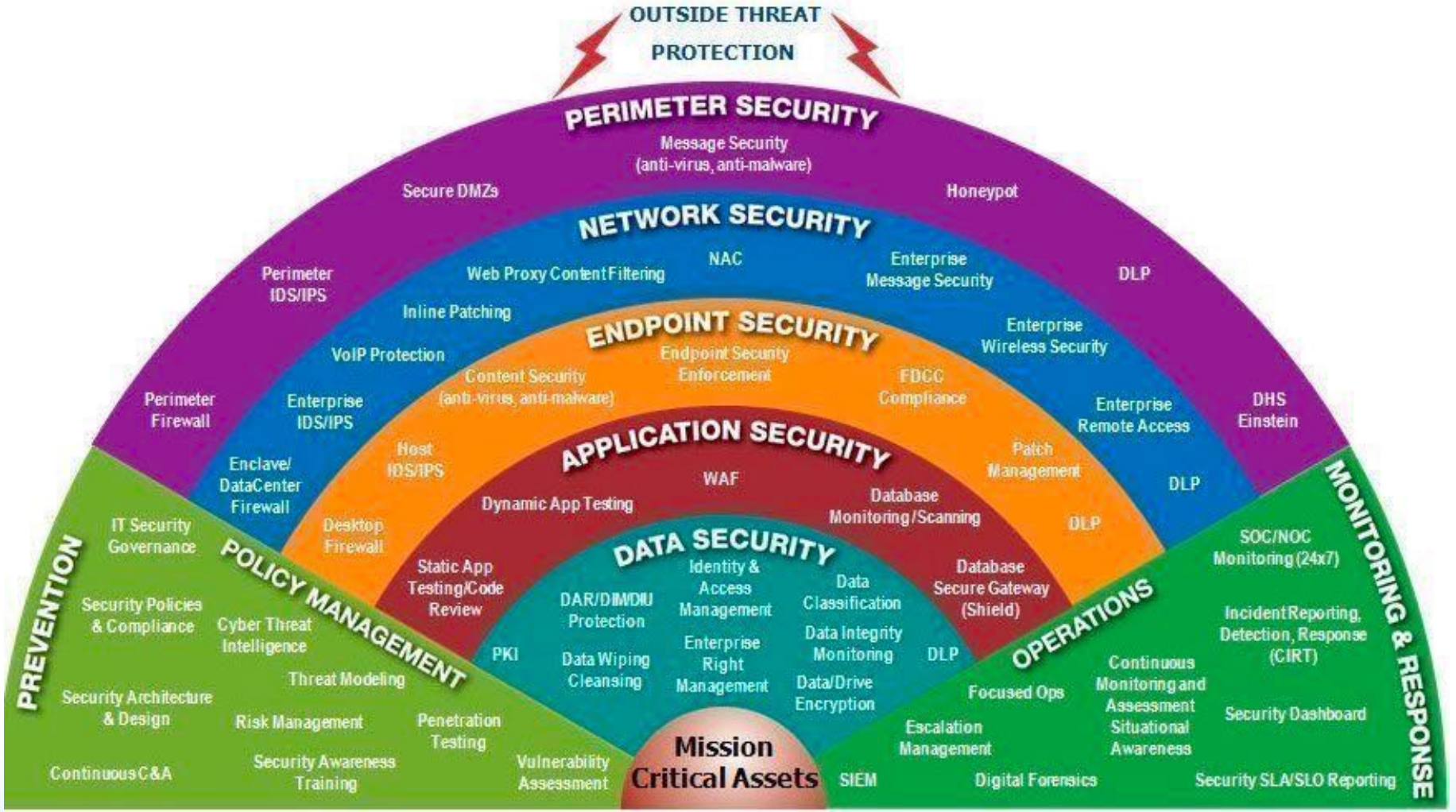
- **Due Diligence**
  - Continual actions that an organization are doing to protect and minimize risk to its tangible and intangible assets.

Defense-in-Depth Model – Rings of Protection



- Ring number determines the access level.
- A program may access only data that resides on the same ring, or a less privileged ring.
- A program may call services residing on the same, or a more privileged ring.
- Ring 0 contains kernel functions of the OS.
- Ring 1 contains the OS.
- Ring 2 contains the OS utilities.
- Ring 3 contains the applications.

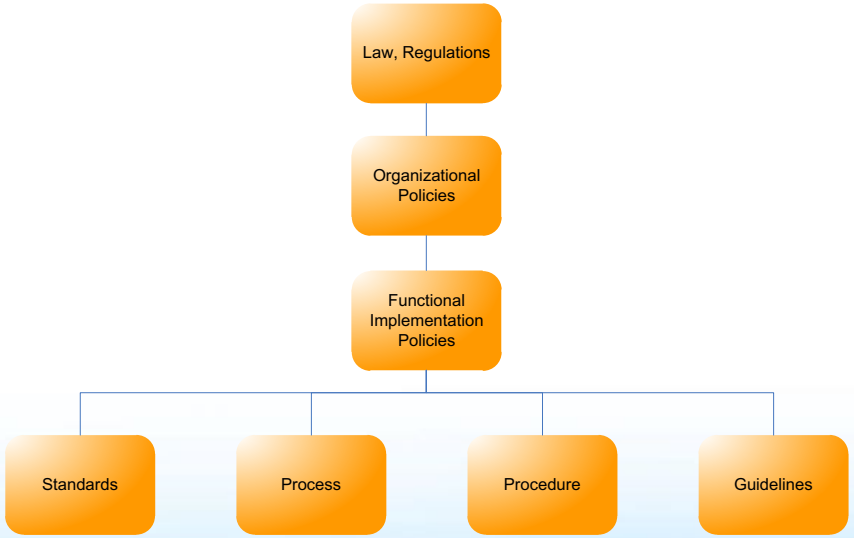
Defense in Depth Landscape

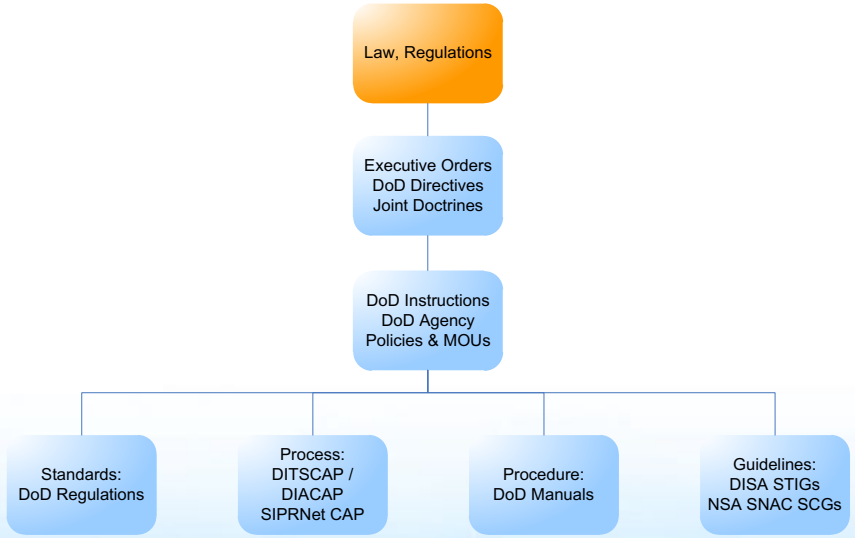


https://blog.knowbe4.com/great-defense-in-depth-infographic

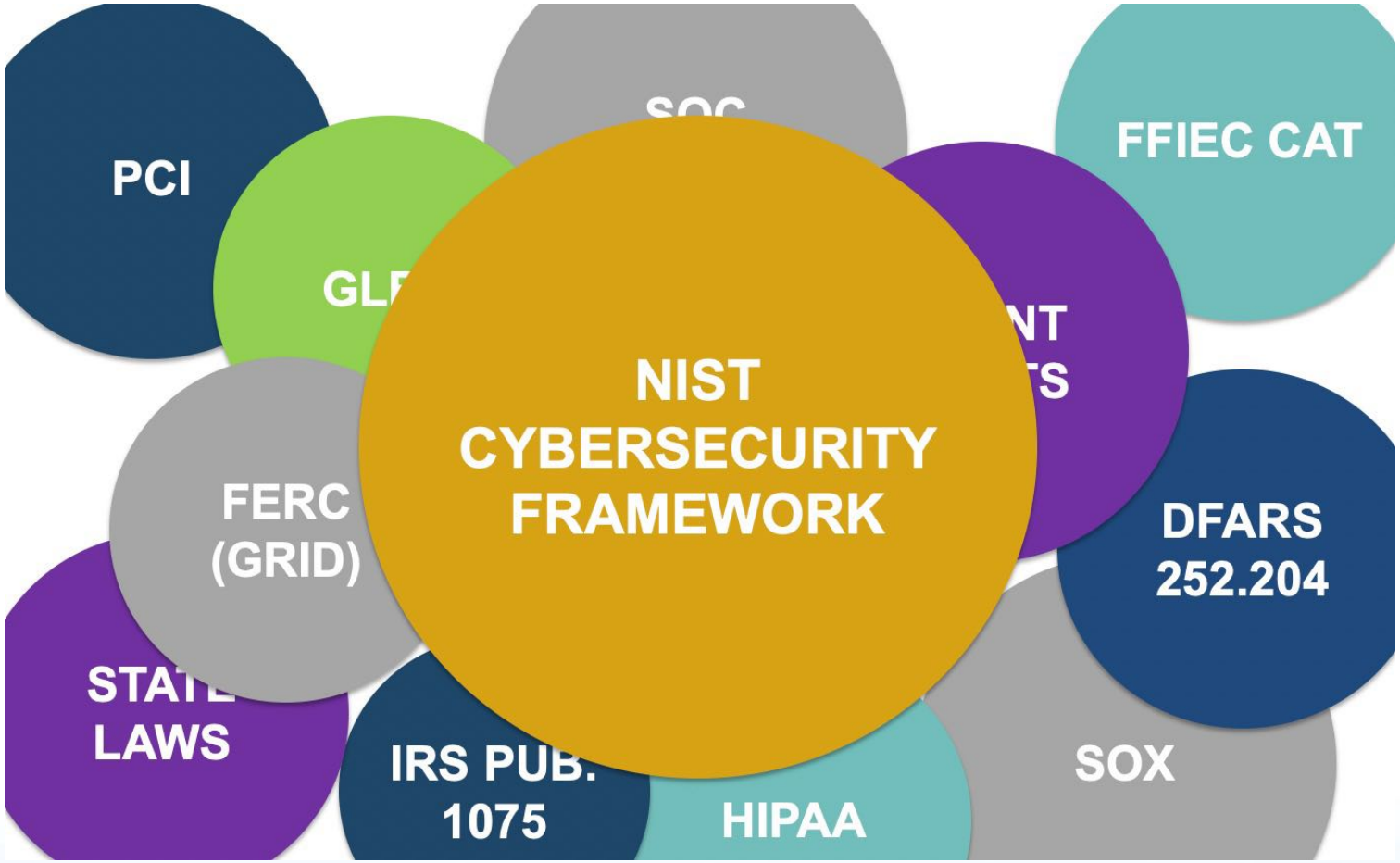
Information Security Governance

- Policy. Management directives that establish expectations (goals & objectives), and assign roles & responsibilities
- Standards. Functional specific mandatory activities, actions, and rules
- Process & Procedure. Step-by-step implementation instructions
- Guideline. General statement, framework, or recommendations to augment process or procedure

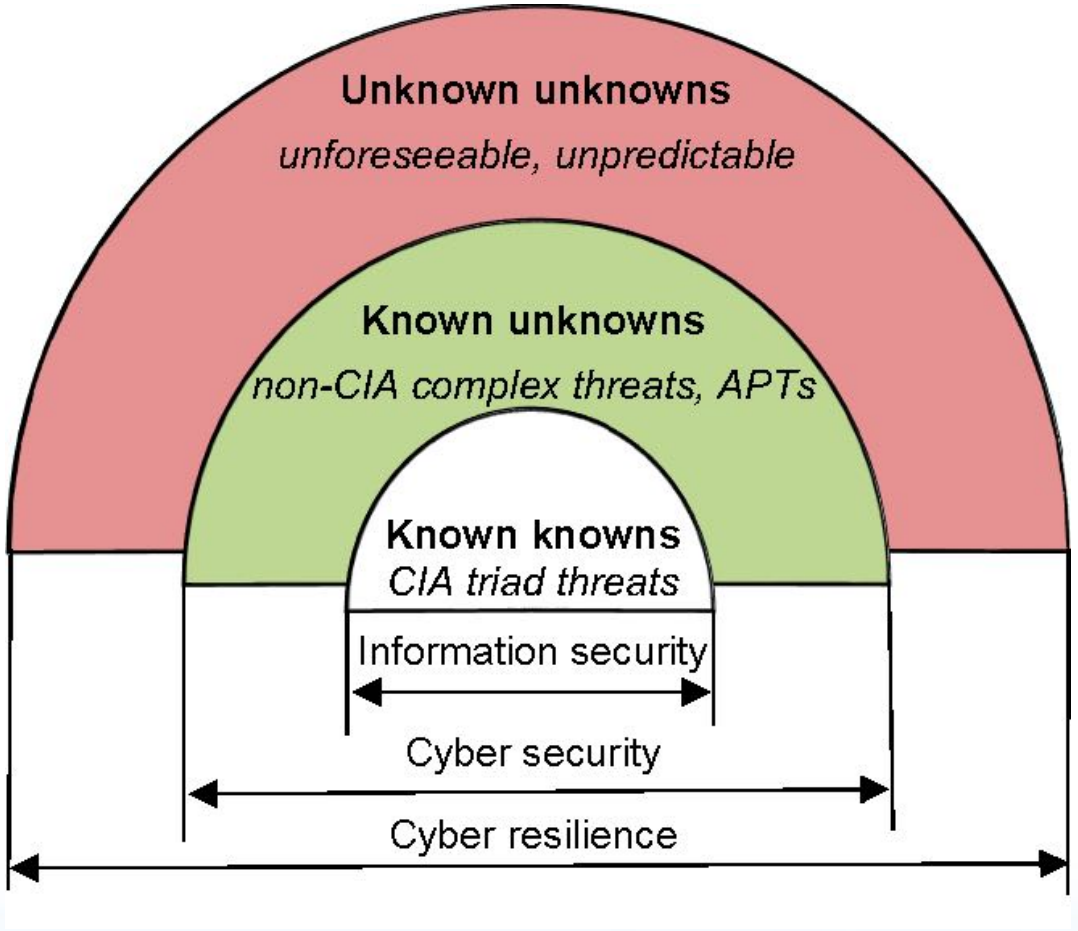




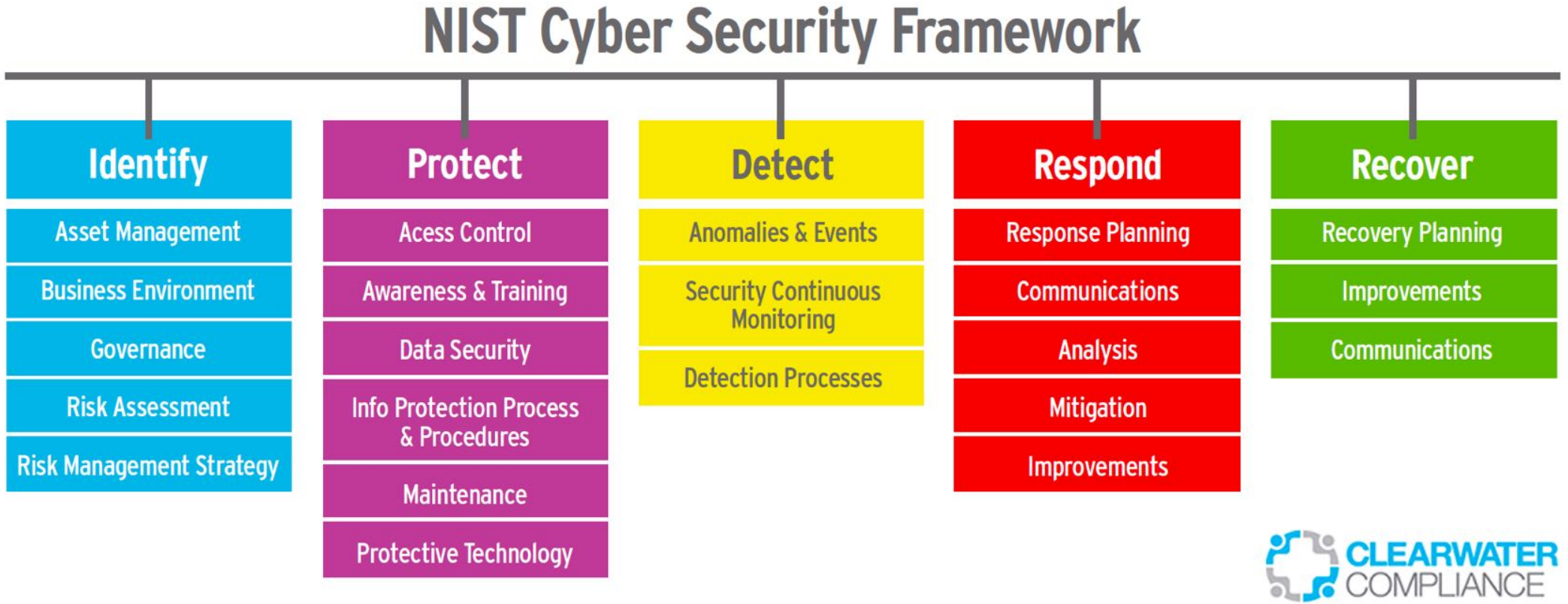
Trends in Cybersecurity



Cyber resilience Concept



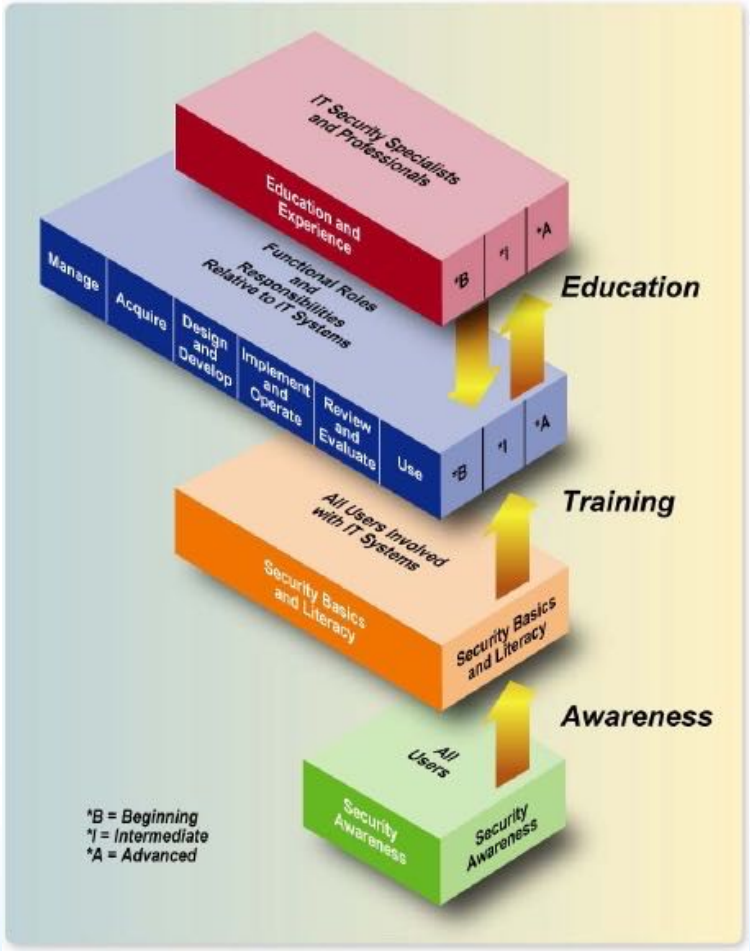
Cybersecurity Framework



Cybersecurity Training & Education

Security Education, Training and Awareness (SETA)

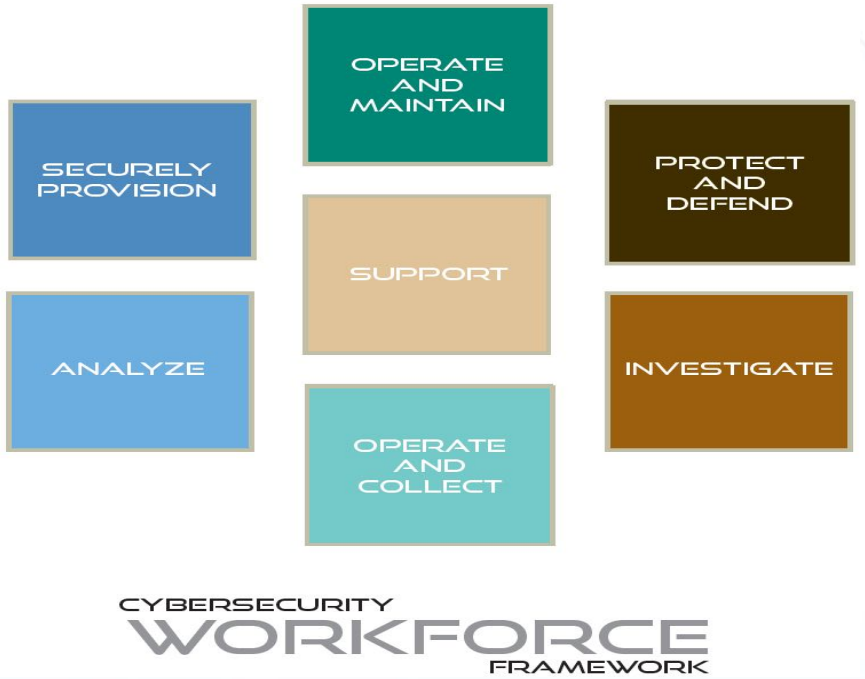
- **Awareness**
  - Orientation briefs and materials to inform and remind employees of their security responsibilities and management's expectation.
- **Training**
  - Course and materials to provide employees the necessary skills to perform their job functions.
- **Education**
  - Course and materials to provide employees the necessary decision-making and management skills to improve their promotional ability and mobility.



Reference: NIST SP800-50, *Building an IT Security Awareness and Training Program.*

National Initiative for Cybersecurity Education (NICE)

- NICE is a part of Comprehensive National Cybersecurity Initiative (CNCI) where government and industry collaborated to create a training & educational framework for cybersecurity workforce.



Reference: http://csrc.nist.gov/nice/

National Initiative for Cybersecurity Education (NICE)

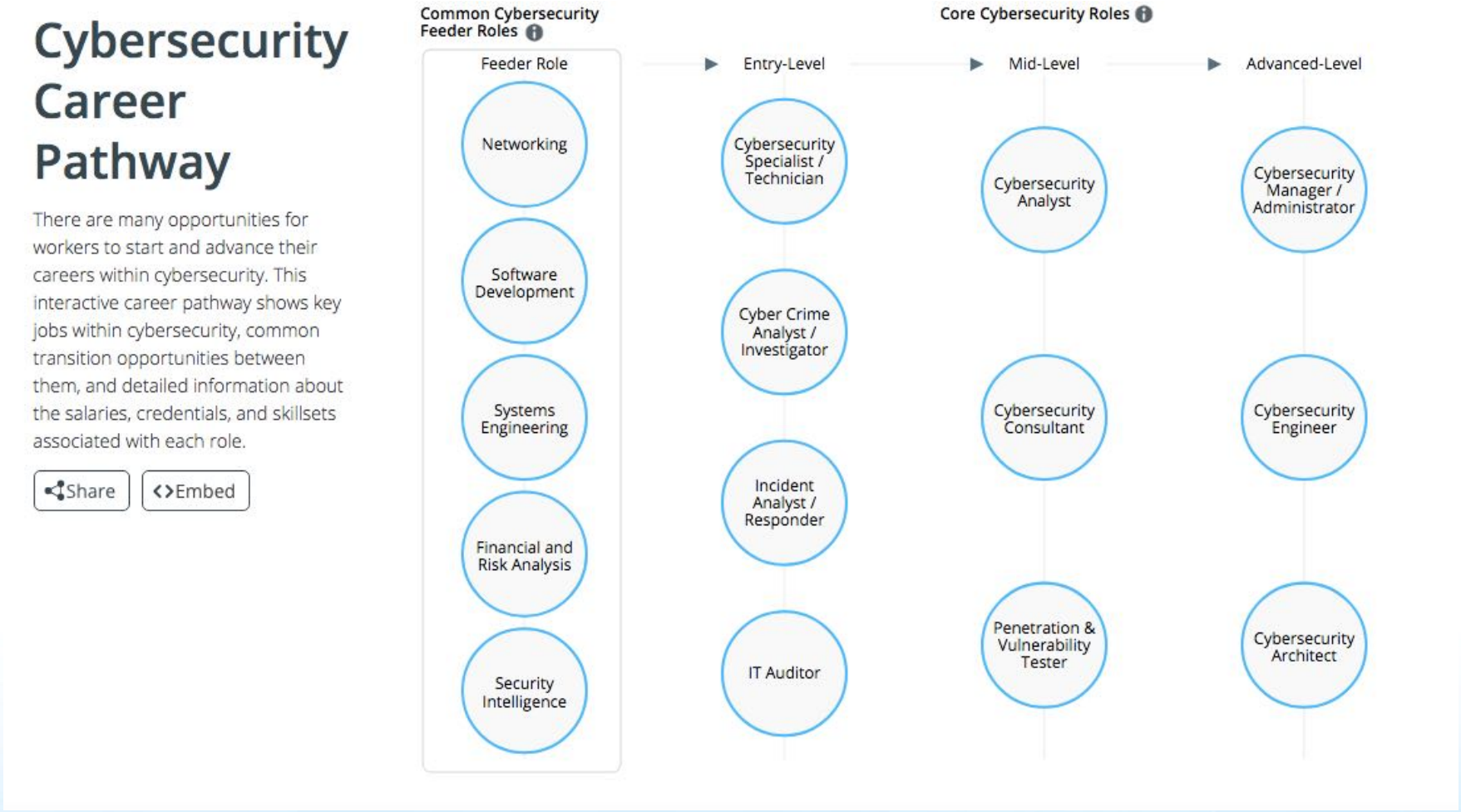
Securely Provision	Specialty areas concerned with conceptualizing, designing, and building secure IT systems.
Operate and Maintain	Specialty areas responsible for providing the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security.
Protect and Defend	Specialty area responsible for the identification, analysis and mitigation of threats to IT systems and networks.
Investigate	Specialty areas responsible for the investigation of cyber events or crimes which occur within IT Systems and networks.
Operate and Collect	Specialty areas responsible for the highly specialized and largely classified collection of cybersecurity information that may be used to develop intelligence.
Analyze	Specialty area responsible for highly specialized and largely classified review and evaluation of incoming cybersecurity information.
Support	Specialty areas that provide critical support so that others may effectively conduct their cybersecurity work.

Roles of Cybersecurity NICE Framework

https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework

Cybersecurity Career Pathway

https://www.cyberseek.org/heatmap.html



https://resources.infosecinstitute.com/overview-of-the-cyberseek-cybersecurity-career-pathway

Cybersecurity Career Pathway

Penetration & Vulnerability Tester

AVERAGE SALARY

$103,000

Penetration & Vulnerability Tester

COMMON JOB TITLES

- Penetration Tester
- Senior Penetration Tester
- Network Relations Consultant
- Application Security Analyst

REQUESTED EDUCATION (%)

TOP SKILLS REQUESTED

1. Information Security
2. Penetration Testing
3. Linux
4. Python
5. Java
6. Vulnerability Assessment
7. Information Systems
8. Software Development
9. Project Management

TOTAL JOB OPENINGS

15,078

Penetration & Vulnerability Tester

COMMON NICE CYBERSECURITY WORKFORCE FRAMEWORK CATEGORIES

- Securely Provision
- Protect and Defend
- Analyze

TOP CERTIFICATIONS REQUESTED

- SANS/GIAC Certification (Various)
- Certified Information Systems Auditor (CISA)
- CompTIA Security+
- Certified Ethical Hacker (CEH)

https://resources.infosecinstitute.com/overview-of-the-cyberseek-cybersecurity-career-pathway

Cybersecurity Career Pathway

Cybersecurity Specialist / Technician

AVERAGE SALARY

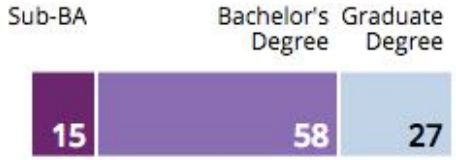
$75,000

Cybersecurity Specialist / Technician

COMMON JOB TITLES

- Information Security Specialist
- IT Specialist Information Security
- Cyber Security Specialist
- Information Technology Specialist - Information Security
- IT Security Specialist

REQUESTED EDUCATION (%)



TOP SKILLS REQUESTED

1. Information Security
2. Information Systems
3. Information Assurance
4. Network Security
5. Vulnerability assessment
6. Intrusion detection
7. Linux
8. Customer Service
9. Project Management

TOTAL JOB OPENINGS

7,792

Cybersecurity Specialist / Technician

COMMON NICE CYBERSECURITY WORKFORCE FRAMEWORK CATEGORIES

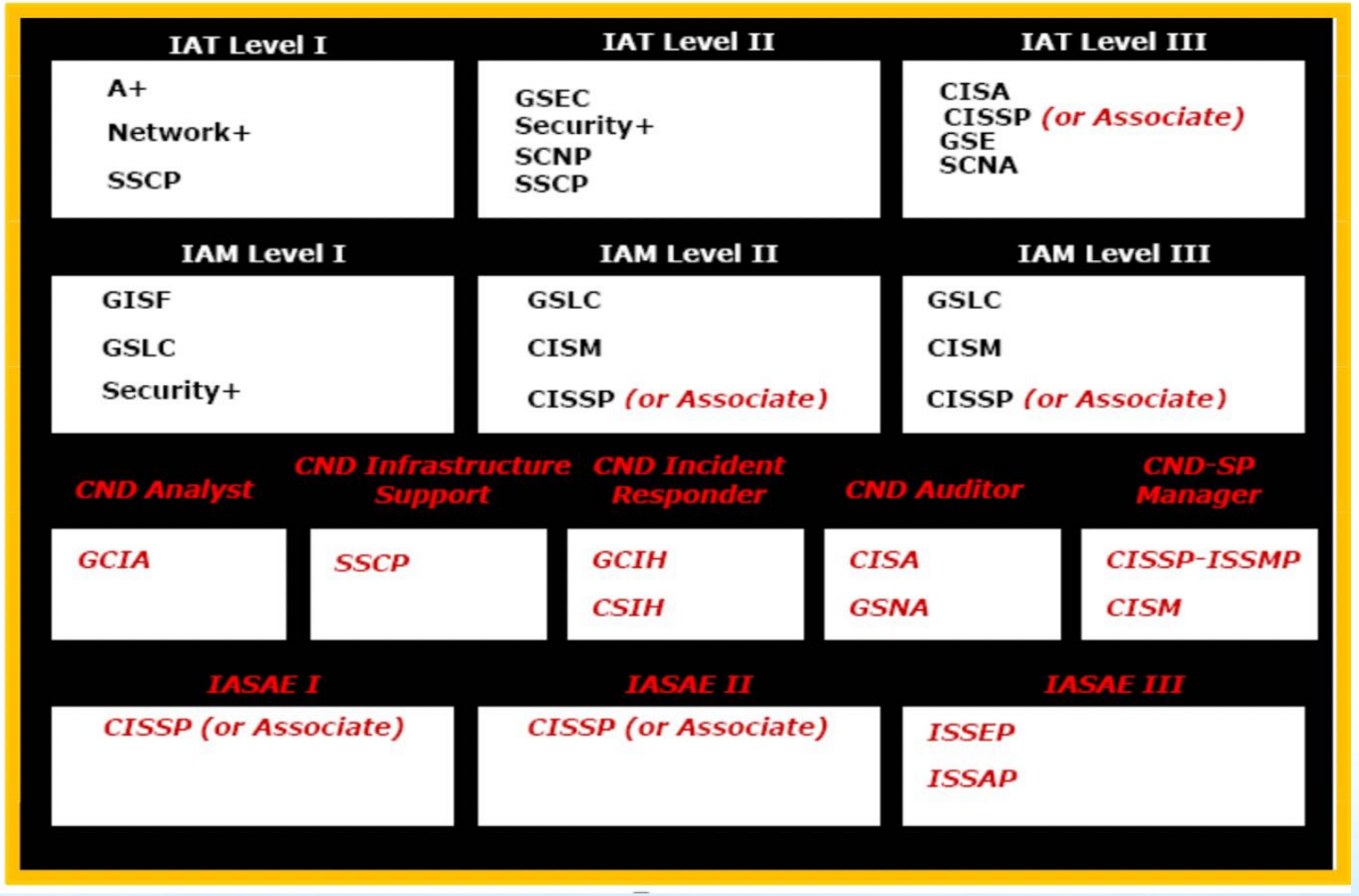
- Operate and Maintain
- Protect and Defend

TOP CERTIFICATIONS REQUESTED

- CISSP
- GIAC
- Security+
- CISM
- CISA

https://resources.infosecinstitute.com/overview-of-the-cyberseek-cybersecurity-career-pathway

DOD 8570.01-M



Risk Management

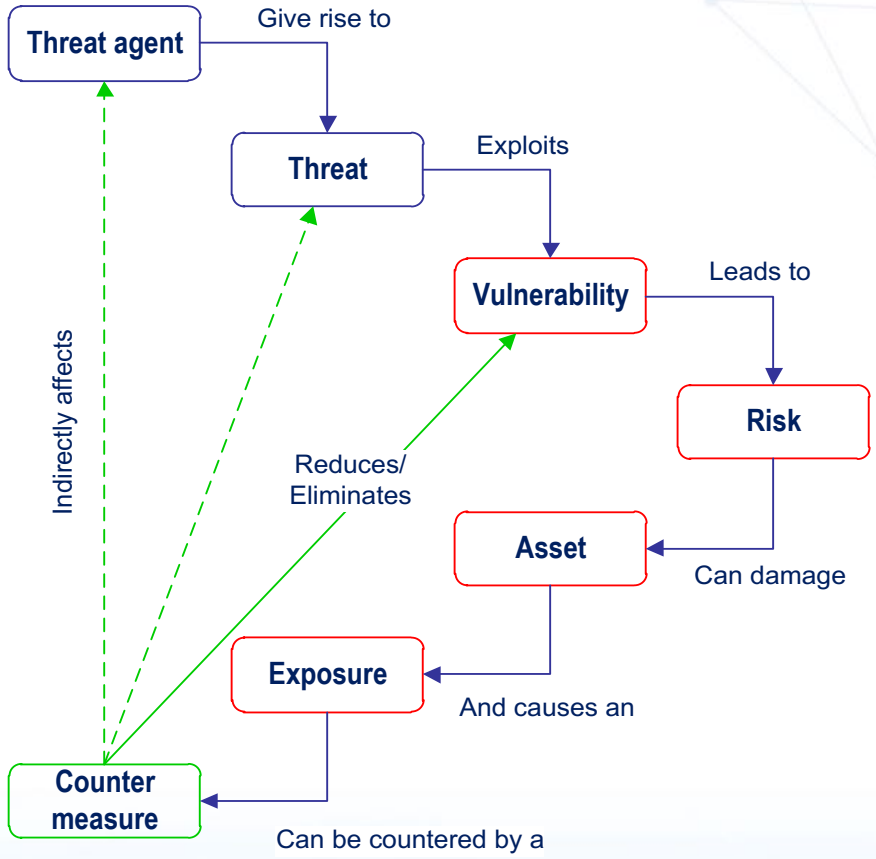
Risk definition

- The principal goal of an organization's risk management process should be to protect the *organization and its ability to perform their mission*, not just its IT assets.

- *Risk* is a function of the *likelihood* of a given *threat-source's* exercising a particular potential *vulnerability*, and the resulting *impact* of that adverse event on the organization.

Relationship between Threat, Risk, and Countermeasure

- Threat Agent. An entity that may act on a vulnerability.
- Threat. Any potential danger to information life cycle.
- Vulnerability. A weakness or flaw that may provide an opportunity for a threat agent.
- Risk. The likelihood of a threat agent exploits a discovered vulnerability.
- Exposure. An instance of being compromised by a threat agent.
- Countermeasure / safeguard. An administrative, operational, or logical mitigation against potential risk(s).



Risk Management Definitions

- Asset
- Threat-source
- Threat Agent
- Threat
- Exposure
- Vulnerability
- Likelihood
- Attack
- Controls
- Countermeasures
- Safeguards
- Total Risk
- Residual Risk

Example of Cybersecurity Thrat , Actor and Motivation

Threat-Source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

Risk Management Concept Flow

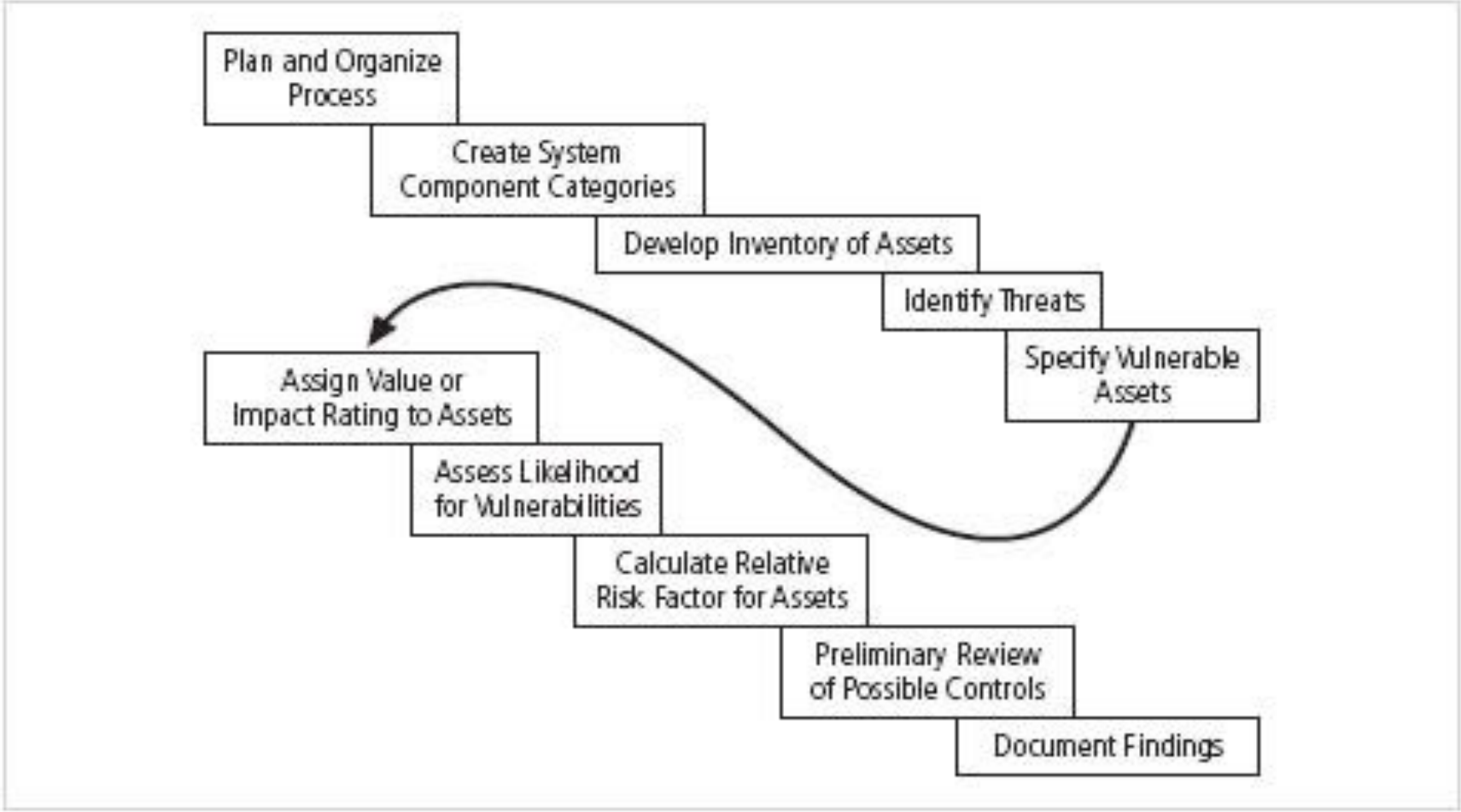


FIGURE 7-1 Risk Identification Process

NIST SP 800-30: Risk Management

Risk Assessment

- Identification of risks
- Evaluation of risks
- Risk Impact
- Recommendation of risk-reducing measures

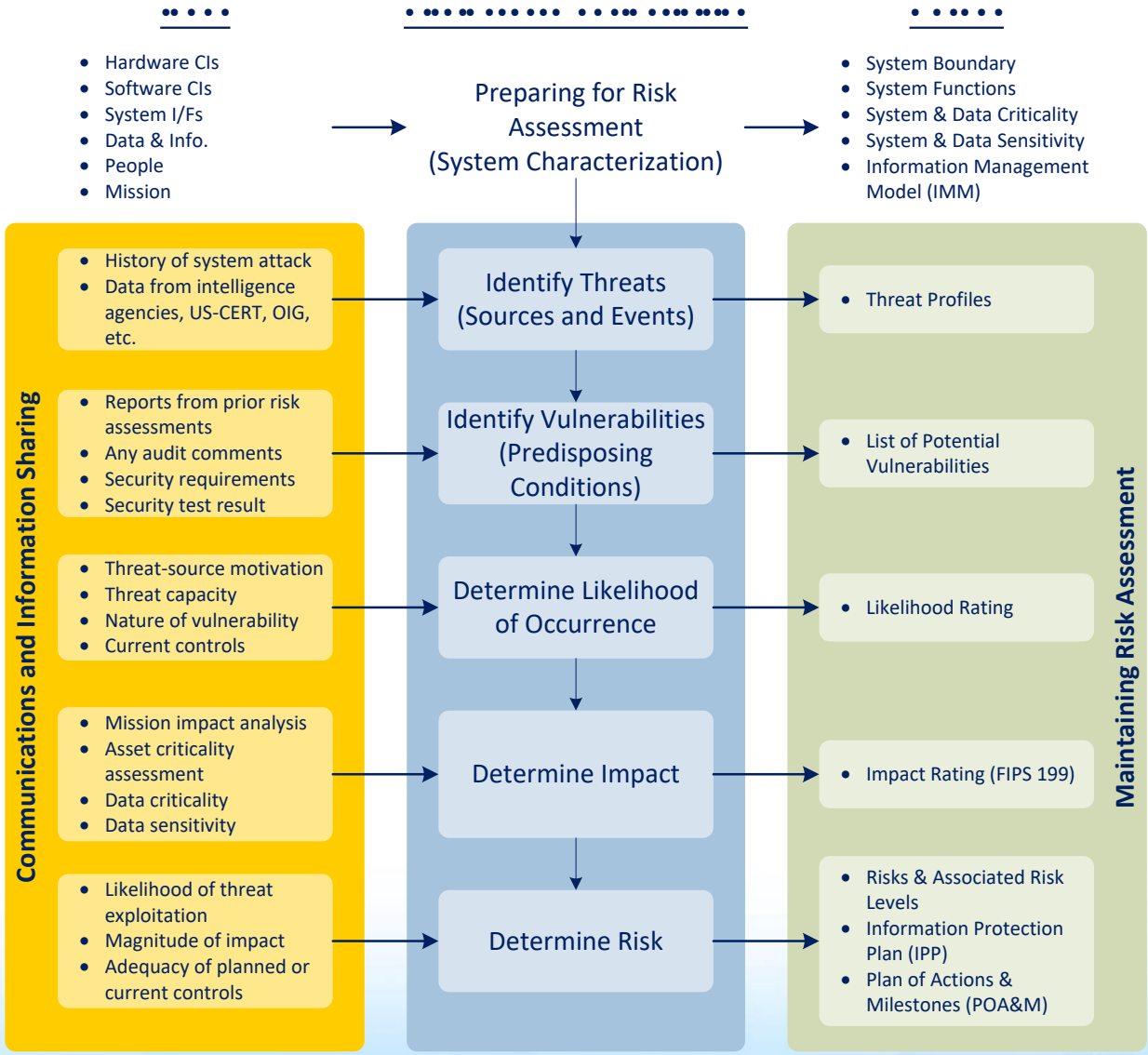
Risk Mitigation

- Risk Avoidance
- Risk Mitigation
- Risk Acceptance
- Risk Transference
- Evaluation of risks

Evaluation & Assurance

- Ongoing risk assessment
- Periodic evaluation
- Regulatory compliance

Risk Assessment Process



Reference:
- NIST SP 800-30, Rev.1, *Guide for Conducting Risk Assessments, Sept. 2011*

Benefits of Risk Analysis

- Focuses policy and resources
- Identifies areas with specific risk requirements
- Directs budget
- Supports
  - Business continuity process
  - Insurance and liability decisions
  - Legitimizes security awareness programs

Emerging Threats Vectors

- New technology
  - IOT (Internet of Things)
  - Quantum Computing
  - Blockchain Technology
- Changes in regulations and laws
- Changes in business practices
- Change in culture or environment
- Unauthorized use of technology
  - Wireless technologies, rogue modems, PDAs, unlicensed software

Sources to Identify Threats

- Users
- System Administrators
- Security Officers
- Auditors
- Operations
- Facility Records
- Community and Government Records
- Vendor/Security Provider Alerts

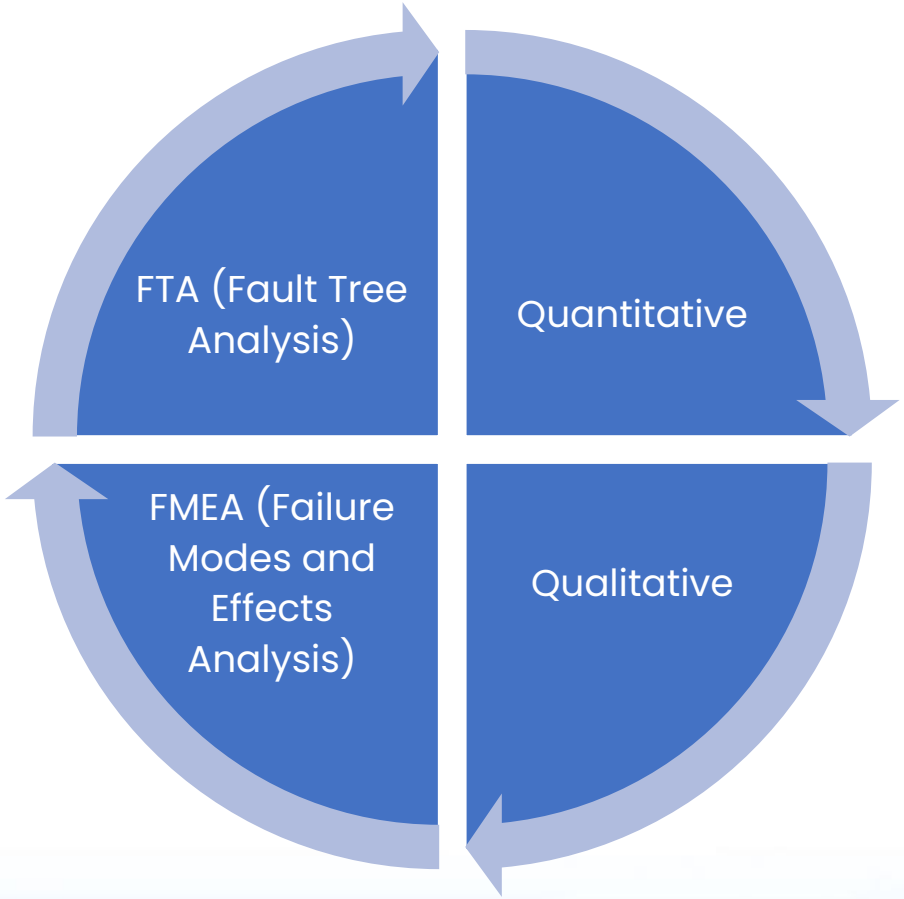
Risk Analysis Key Factors

- Management support
- Establish team
- Team members
- Automation

Preliminary Security Evaluation

- Identify vulnerabilities
- Review existing security measures
- Document findings
- Obtain management review and approval

Risk Analysis Types



Risk Assessment Methods

Quantitative

ALE = SLE x ARO

SLE = AV x EF

- Annualized Lost Expectance (ALE).
- Single Loss Expectance (SLE). Monetary loss (impact) for each occurrence of a threatened event
- Annualized Rate of Occurrence (ARO). The frequency which a threat is expected to occur on an annualized basis
- Asset Value (AV). Monetary value of the information asset
- Exposure Factor (EF). Percentage of loss from a specific threat.

Qualitative

- Likelihood Determination
  - Threat agent motivation & capability
  - Nature of the vulnerability
  - Existence and effectiveness of current controls.
- Impact Analysis (Confidentiality, Integrity & Availability)
  - System mission (e.g., the processes performed by the IT system)
  - System and data criticality (e.g., the system's value or importance to an organization)
  - System and data sensitivity.

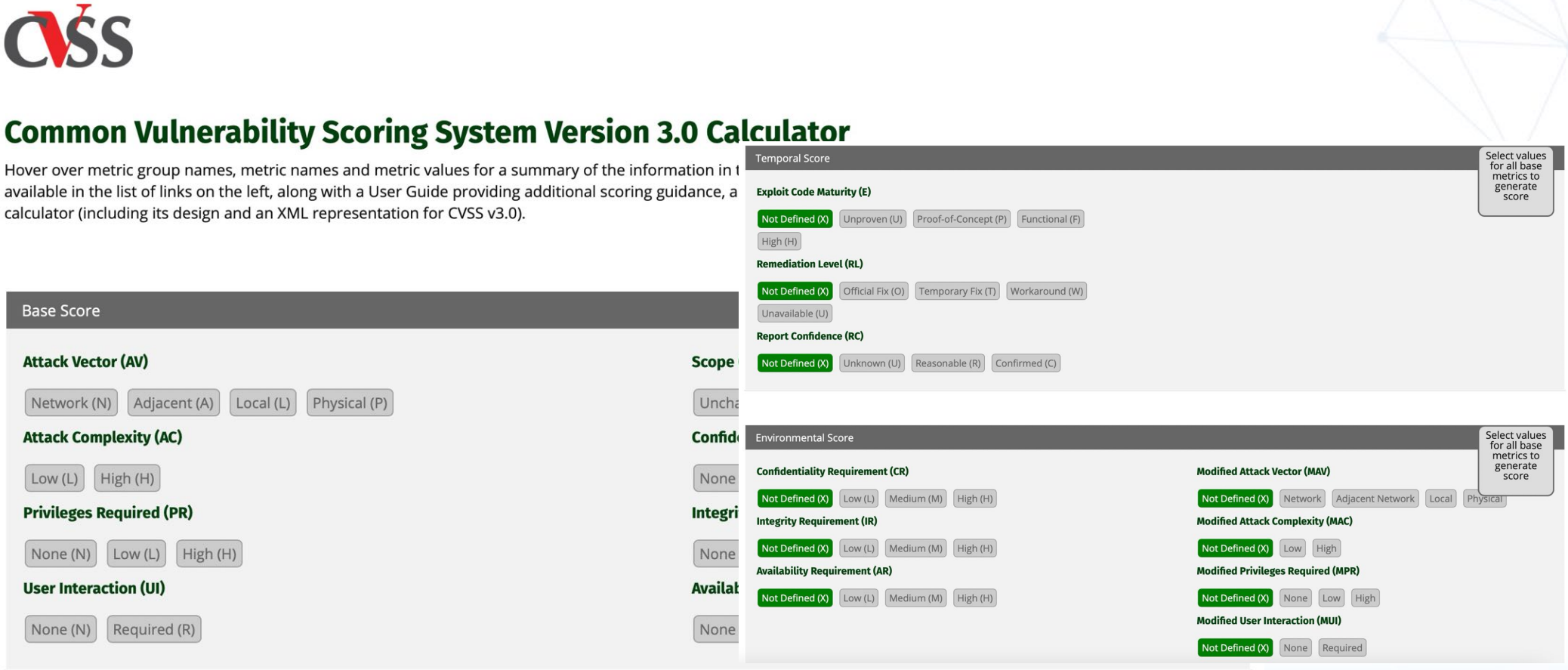
		Likelihood Level		
		Low	Medium	High
	Significant (High)	2	3	3
	Serious (Moderate)	1	2	3
	Mild (Low)	1	1	2

Risk Levels (AS/NZ 4360 Standard)

	Consequence:				
	Insignificant	*Minor*	*Moderate*	*Major*	*Catastrophic*
Likelihood:	*1*	*2*	*3*	*4*	*5*
A (almost certain)	H	H	E	E	E
B (likely)	M	H	H	E	E
C (possible)	L	M	H	E	E
D (unlikely)	L	L	M	H	E
E (rare)	L	L	M	H	H

E	Extreme Risk: Immediate action required to mitigate the risk or decide to not proceed
H	High Risk: Action should be taken to compensate for the risk
M	Moderate Risk: Action should be taken to monitor the risk
L	Low Risk: Routine acceptance of the risk

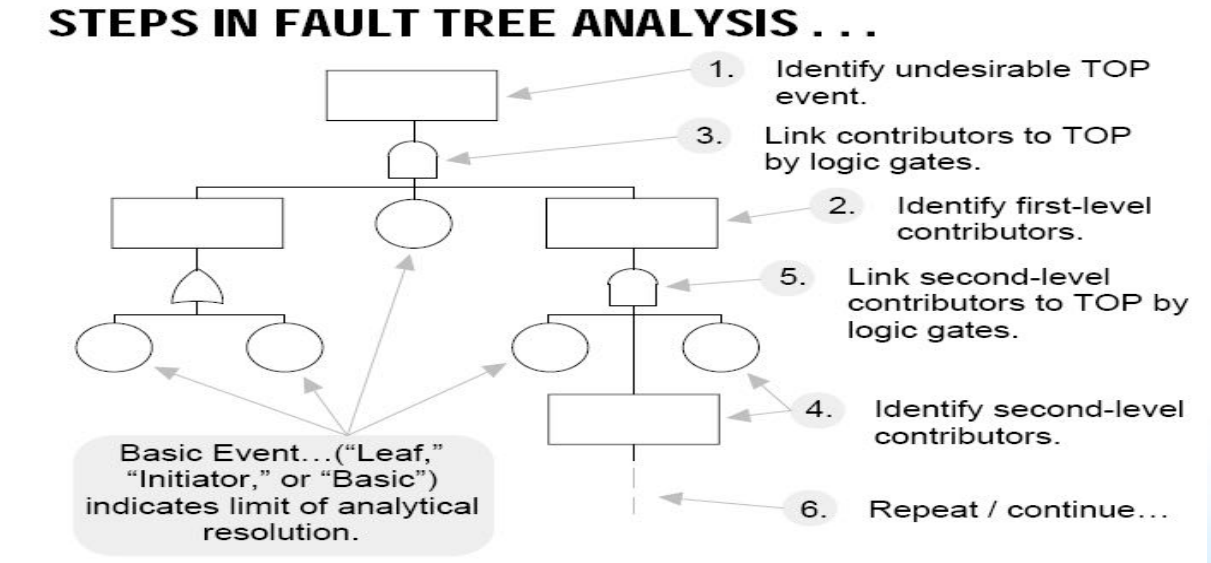
CVSS Version 3



OWASP Risk Rating

Other Risk Analysis Methods

- Failure Mode and Effects Analysis
  - Manufacturing
- Fault Tree Analysis
  - Safety systems & Design



Risk Mitigation Options

- Acceptance = Absorb the effect of an incident
- Reduction = Implement Controls
- Transference = Insurance
- Avoidance = Stop it

Data Protection and Privacy

Topic

- What is Data Privacy & Data Protection
- Data Privacy Threat
- Data Protection Controls
  - Confidentiality
  - Integrity
  - Availability
  - Access Controls
  - Data Protection Technology

Data Privacy Threat

Data Privacy Threat

- Malware
  - Ransomware
  - Trojan Horse
  - Spyware & Keylogger
- Data Exfiltration attack
- Unauthorized Access
- Human Risk
- Human Mistaken
- Social Engineering

Data Exfiltration attack

- Exfiltration of job application data from a website
- Exfiltration of hashed password from a website
- Credential stuffing attack on a banking website

Human Risk

Exfiltration of business data by a former employee

Accidental transmission of data to a trusted third party

Stolen Data

- Stolen material storing encrypted personal data
- Stolen material storing non-encrypted personal data
- Stolen paper files with sensitive data

Human Mistaken

Sensitive personal data sent by mail by mistake

Personal data sent by mail by mistake

Social Engineering attack

- Identity theft
- Email exfiltration
- Impersonation

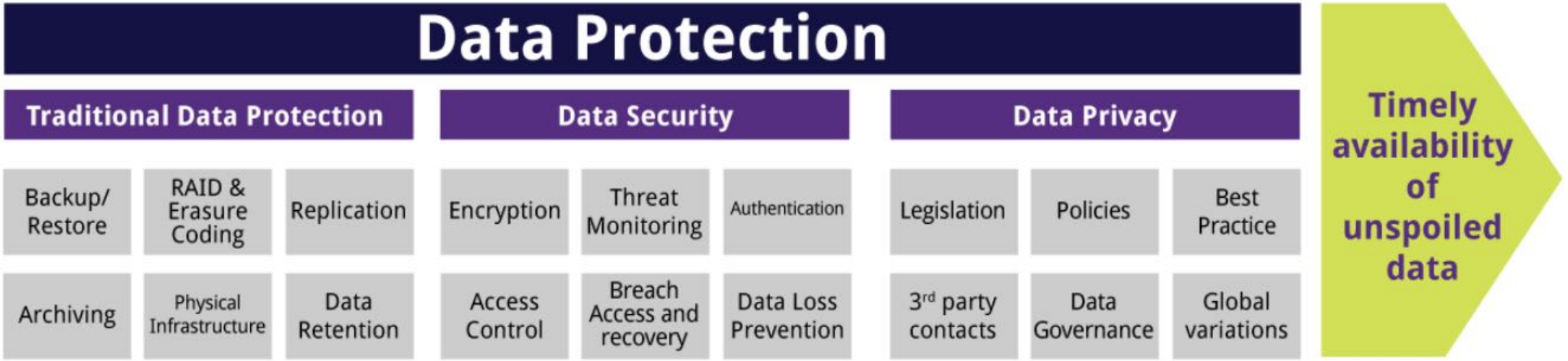
Overview Data Protection

What Is Data Privacy and Why Is it Important?

- **Data privacy** is a guideline for how data should be collected or handled, based on its sensitivity and importance. Data privacy is typically applied to personal health information (PHI) and personally identifiable information (PII). This includes financial information, medical records, social security or ID numbers, names, birthdates, and contact information.

- **Data protection** regulations govern how certain data types are collected, transmitted, and used. Personal data includes various types of information, including names, photos, email addresses, bank account details, IP addresses of personal computers, and biometric data.

The Three Categories of Data Protection



Data Protection Technologies

- Data discovery
- Data loss prevention (DLP)
- Storage with built-in data protection
- Backup
- Snapshots
- Replication
- Firewalls
- Access Controls
- Encryption
- Endpoint protection
- Data erasure
- Disaster recovery

Data protection and data security concept

- **Confidentiality :** Protection of data, information and programme against unauthorized access and disclosure.
- **Integrity :** Factual and technical accuracy and completeness of all information and data during processing.
- **Availability :** Information, data, applications, IT systems and IT networks are available for processing.
- **Resilience :** Denoted as an aspect of availability and thus the capacity of information, data, applications, IT systems and IT networks in the event of malfunction, failure or heavy use.

Confidentiality

Access control

- Identification
- Authentication
- Authorization
- Accountability

Physical security

- Business premises and buildings are monitored 24 hours a day, seven days a week by security staff.
- The data center – and thus the hardware, server or components – is located in a separate secure area that is segregated from normal office premises.
- Opening of doors is also technically monitored.
- There are service contracts for technical surveillance systems.
- Access is logged.
- An identity check is carried out by security staff.
- Access is only granted to authorized persons after checking and establishing identity.

Access Control

- Access authorization is granted to users on the basis of authorization procedures.
- Measures for password security (length, complexity and safekeeping) and rules for the use of passwords are in place.
- A rule that makes a need-to-know and a need-to-do principle compulsory for authorization procedures is in place.
- Administrator accounts are exclusively used for strictly limited activities.
- Rules are in place for authorised persons leaving the company or changing jobs.
- Unauthorized attempted access is detected (for example logging of system use) and investigated accordingly.

Logging of access

- Access to data processing systems and workstations is logged (for example in a log file).
- Use of data processing systems is verifiable (logging of access).
- Remote access via the (SSL) VPN gateway is logged.
- The granting/changing of access authorization is logged.
- Logs are regularly evaluated.

Secure Data Storage

- Encrypted data storage devices are available.
- The safekeeping of data storage devices is controlled.
- Data storage devices are not repaired, but rather are subject to more secure deletion/destruction
- Persons authorized for data storage device removal are specified.
- Hard drives are hardware encrypted.

Integrity

- Regulation concerning electronic transfer
  - External networks are used exclusively (VPN, dedicated line).
  - Filter mechanisms prevent connections to/from unauthorised IT systems (firewall).
  - There is the option of encrypting data (for example S-MIME, PGP) and transferring encrypted data (for example SSL, TLS).
  - Emails are authenticated (digital signature).
- Regulation concerning storage on removable media
- Regulations concerning the transportation of data storage devices
- Regulations concerning the disposal of data storage devices

Availability and resilience/recoverability

- Creation and safekeeping of backups
- Safeguarding of day-to-day operations
- Resilience (Operational availability)
- Uninterruptible power supply
- Fire protection
- Air-Conditioning
- Internet connection
- Data Backup Operation in place
- Business Continuity Management

Infrastructure Security

Network Device Security

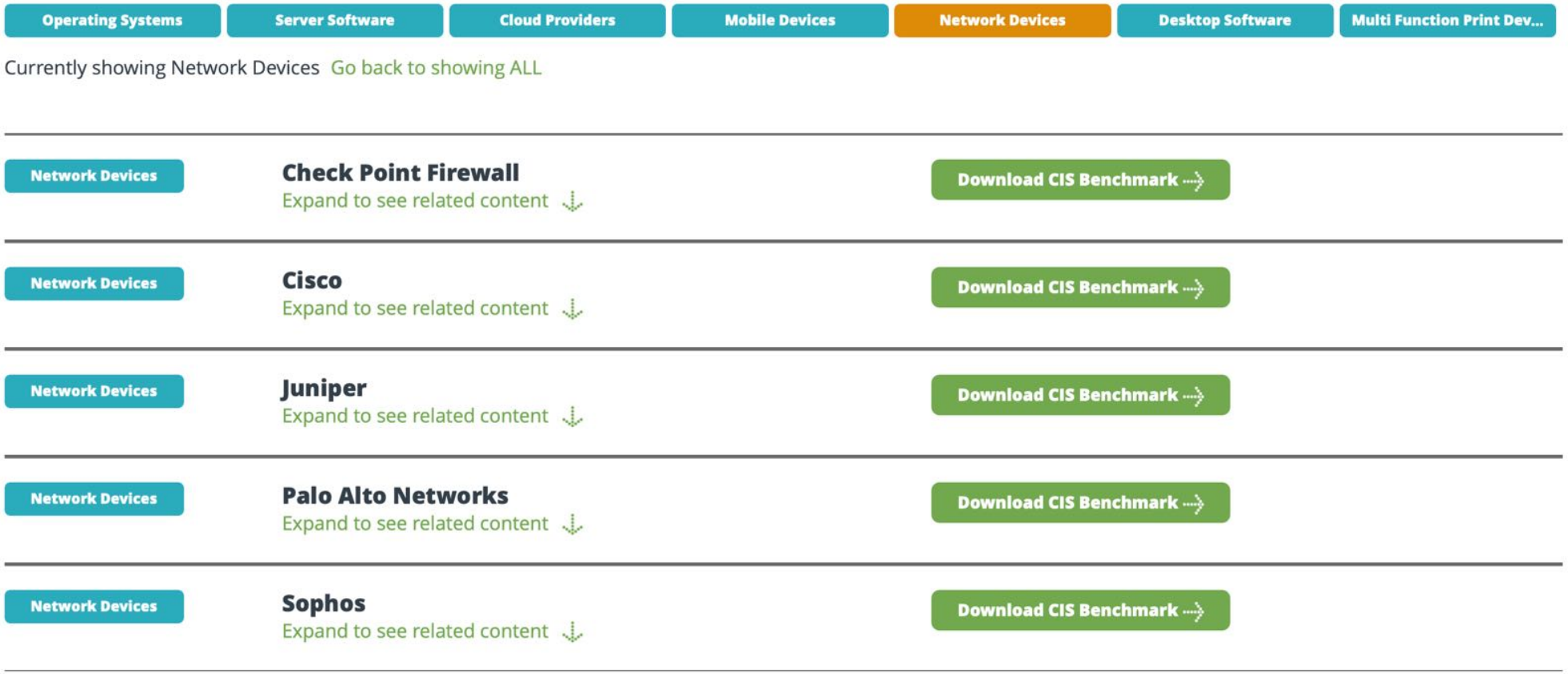
Security of Network Equipment

- Time synchronization
  - Use multiple time sources.
  - Use NTP for all Layer 3 equipment to synchronize their time.
  - Use NTP authentication between clients, servers, and peers to ensure that time is synchronized to approved servers only.
- Event Logging
  - Configure key ACLs to record access violations.
  - Example: Anti-spoofing violations, VTY access attempts, Router filter violations, ICMP, HTTP, SNMP…etc.

Security of Network Equipment

- Physical Access Control
  - Dedicated access ports for management
    - Console Port, Auxiliary Port, VTY (Virtual TTY) Port.
  - Dedicated monitoring I/Fs for SNMP
    - Use SNMPv3, or SNMPv2c, no default community strings
    - For SNMPv2c, treat community strings as “password”.
- Logical Access Control
  - Set password & privilege levels.
  - Implement AAA (Authentication, Authorization & Accountability).
  - Implement centralized authentication & authorization mechanism: TACACS+ or RADIUS.

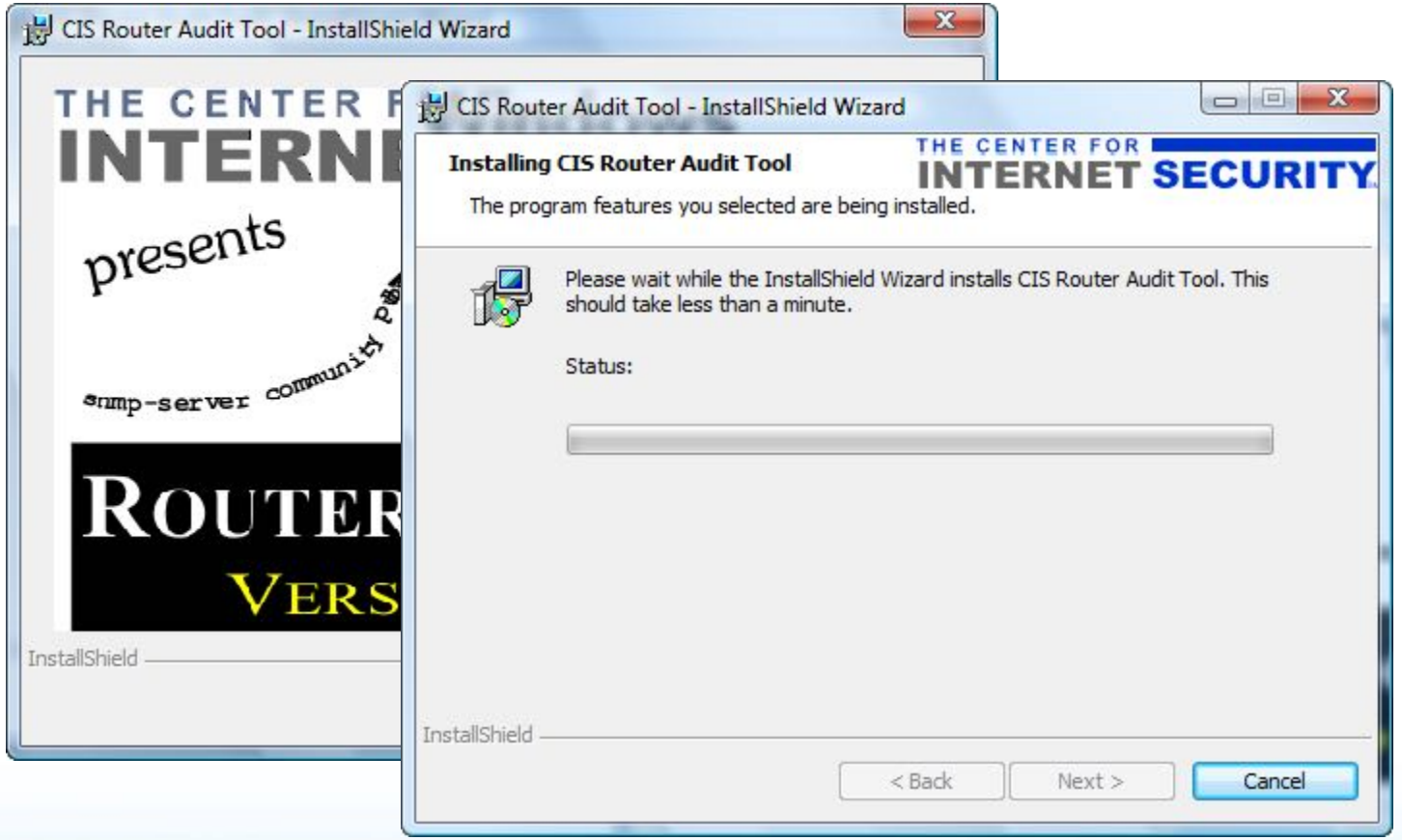
CIS Benchmark Network Devices

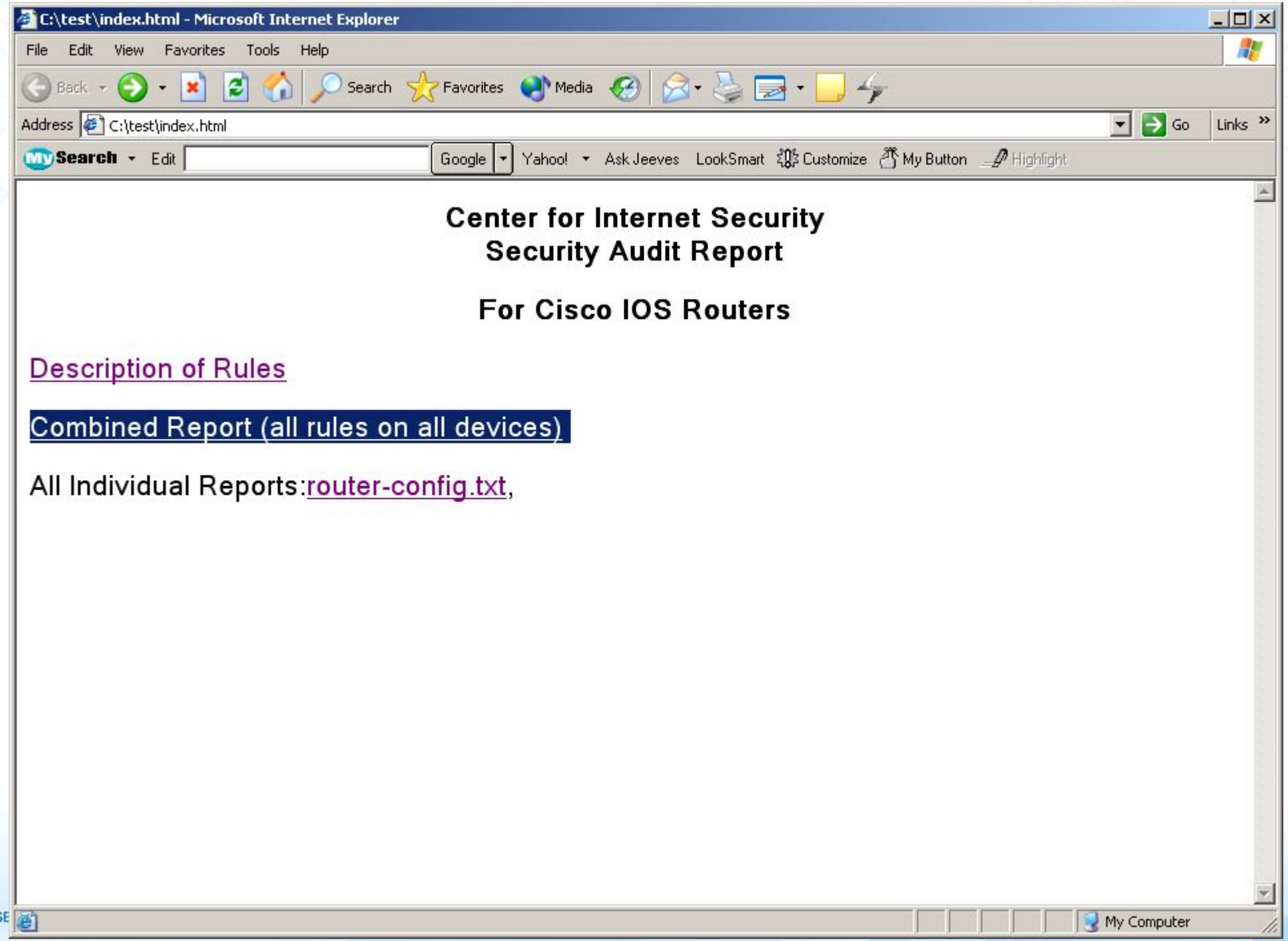


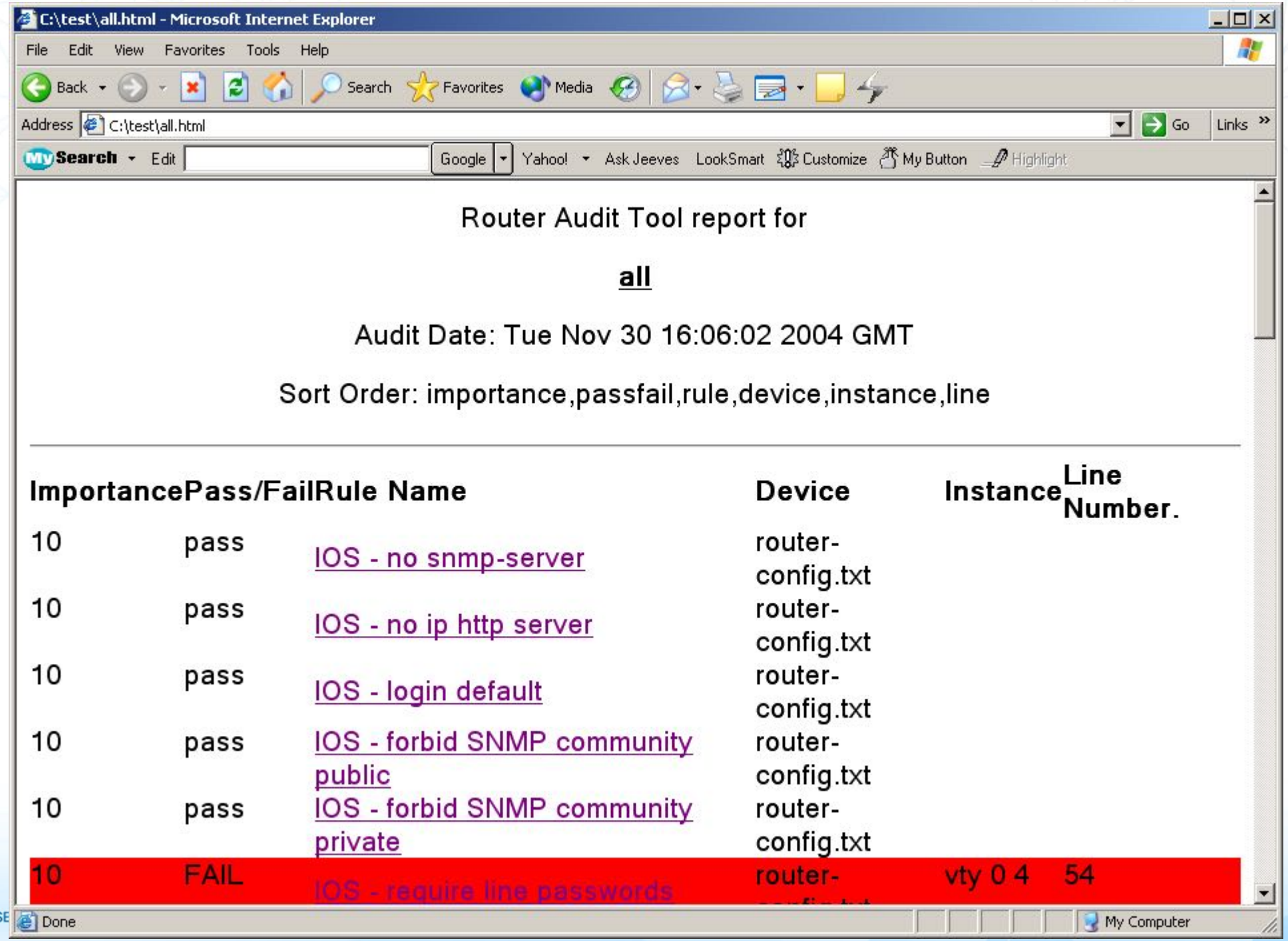
CIS Benchmark

CIS Benchmark

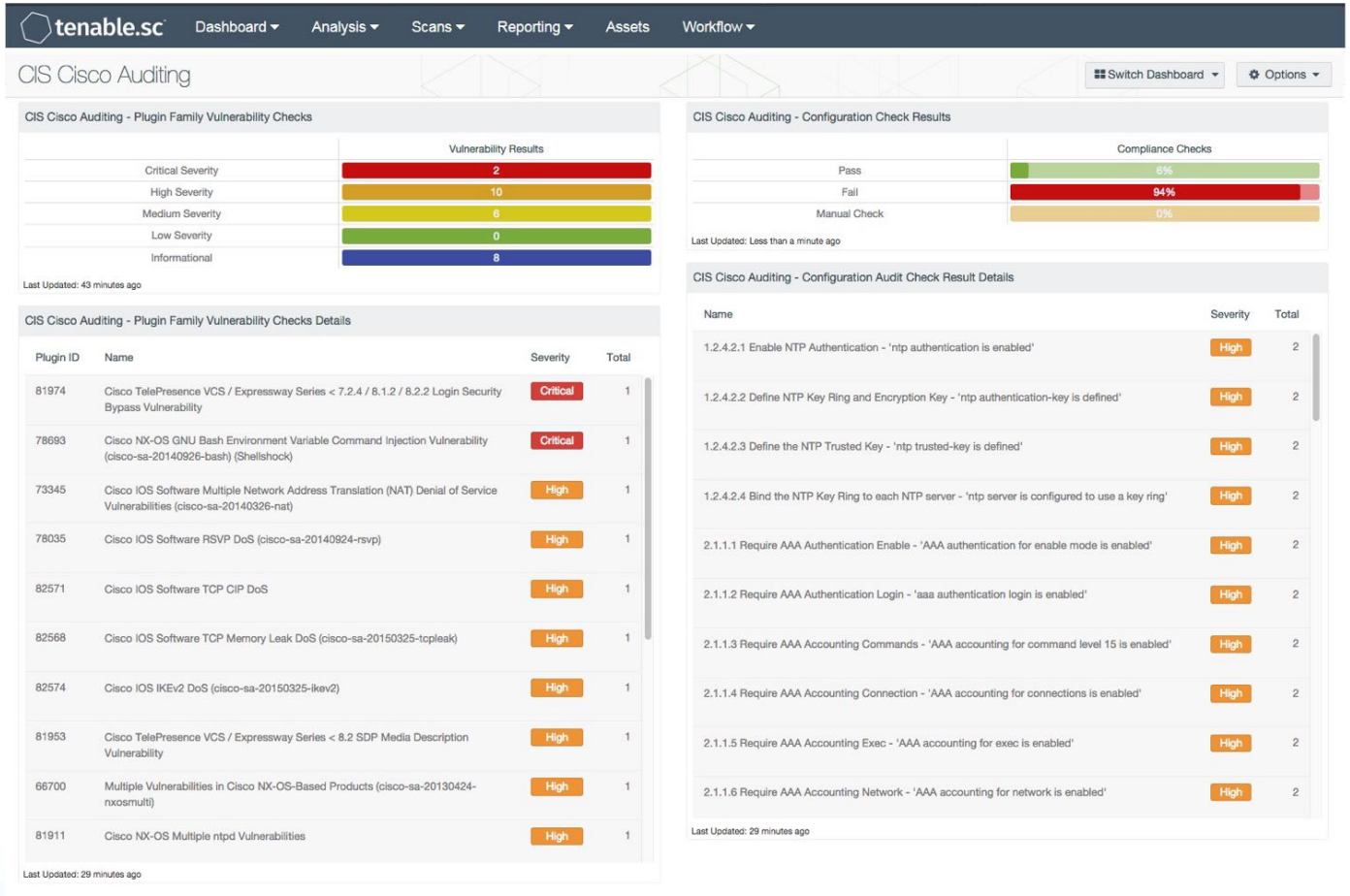
RAT for Windows







Network Device Audit Tools



Firewall

Firewalls

- Packet-filtering firewall (i.e. Router ACLs)
  - Do not examine Layer 4-7 data. Therefore it cannot prevent application-specific attacks
- Proxy firewall
  - It supports selected IP protocols (I.e. DNS, Finger, FTP, HTTP, LDAP, NNTP, SMTP, Telnet). For multicast protocols (PIM, IGMP…etc) must be **TUNNEL** through the firewall
- Stateful inspection firewall
  - It's faster than proxy firewall and more flexible because it examines TCP/IP protocols not the data
  - Unlike proxy firewall, it does not rewrite every packets and does not "talk" on application server's behalf

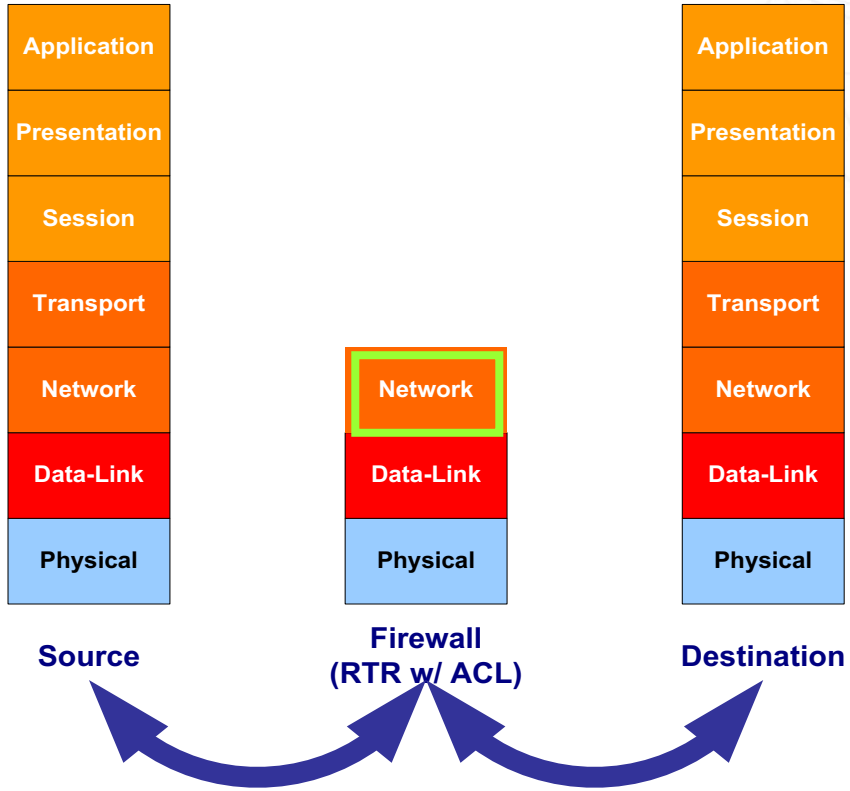
Firewalls

Hybrid Firewalls…

- Circuit-level proxy firewall
  - IETF created SOCKS proxy protocol (RFC 1928) for secure communications
  - SOCKS creates a circuit between client and server without requiring knowledge about the internetworking service. (No application specific controls)
  - It supports user authentication
- Application proxy firewall
  - Application proxy + Stateful inspection
  - A different proxy is needed for each service
  - It supports user authentication for each supported services.
  - e.g. Checkpoint Firewall-1 NG

Packet-filtering firewalls

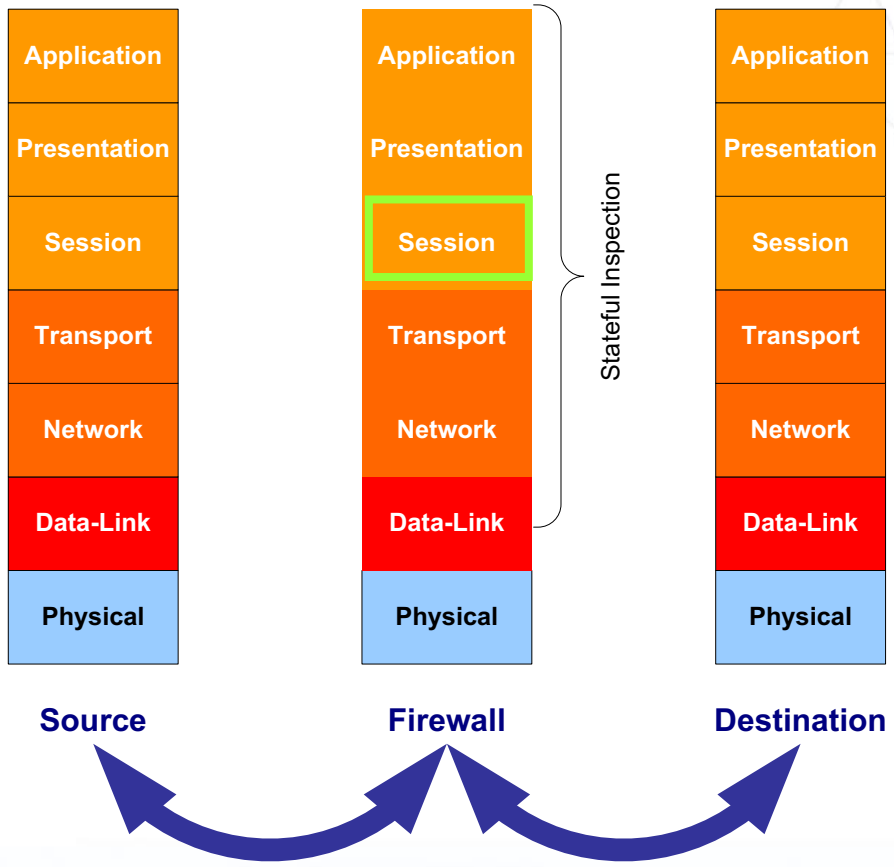
- Router ACL's ~ Packet-filter firewall
- Firewall Policy: Deny by default, Permit by exception
  - Understand the data-flow (i.e. source, destination, protocols, and routing methods), so the security engineer knows how to apply IP filtering
  - Knows the specific inbound and outbound
  - Disable all un-necessary protocols & services



Source: DISA FSO *Network STIG*

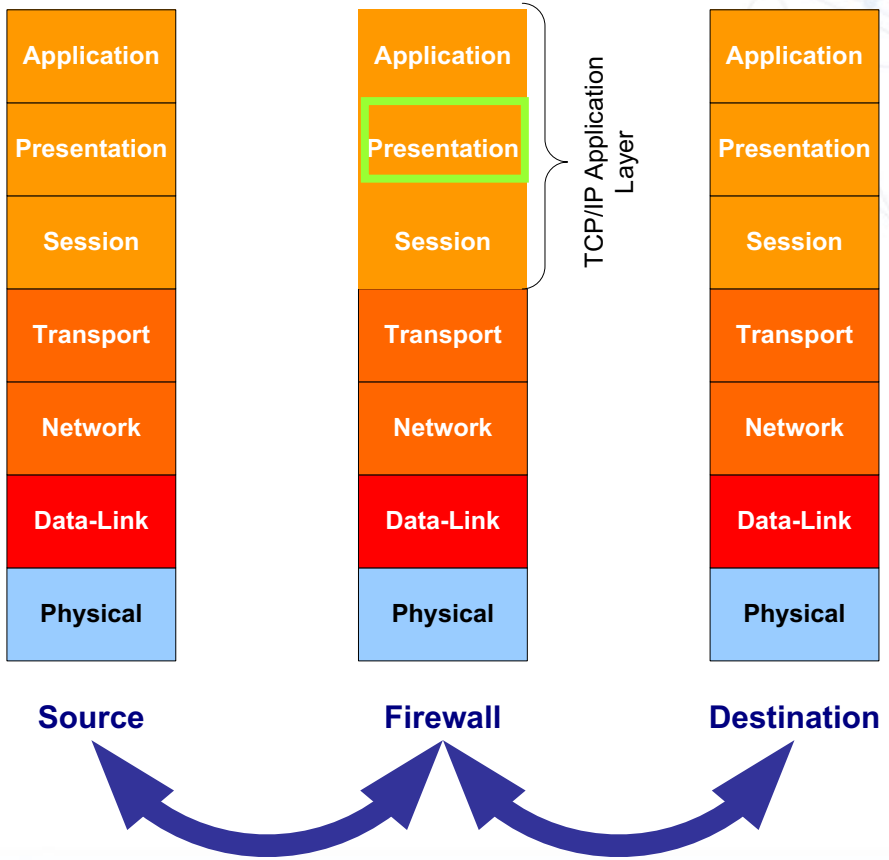
Stateful inspection firewalls

- Supports all TCP/IP-based services, including UDP (by some)
- Inspects TCP/IP packets and keep track of states of each packets. Low overhead and high throughput
- Allows direct TCP/IP sessions between internal computing hosts and external clients
- Offers no user authentication



Proxy firewalls

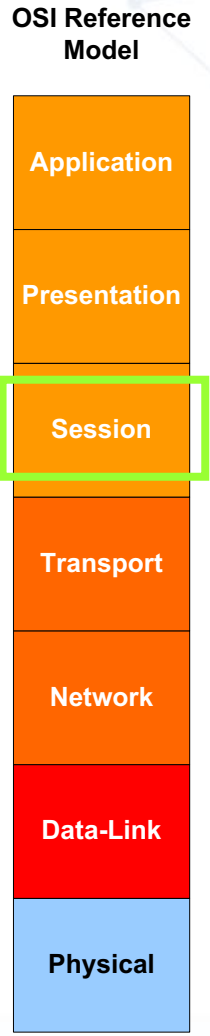
- Do not allow any direct connections between internal and external computing hosts
- Able to analyze application commands inside the payload (datagram)
- Supports user-level authentications. Able to keep a comprehensive logs of traffic and specific user activities



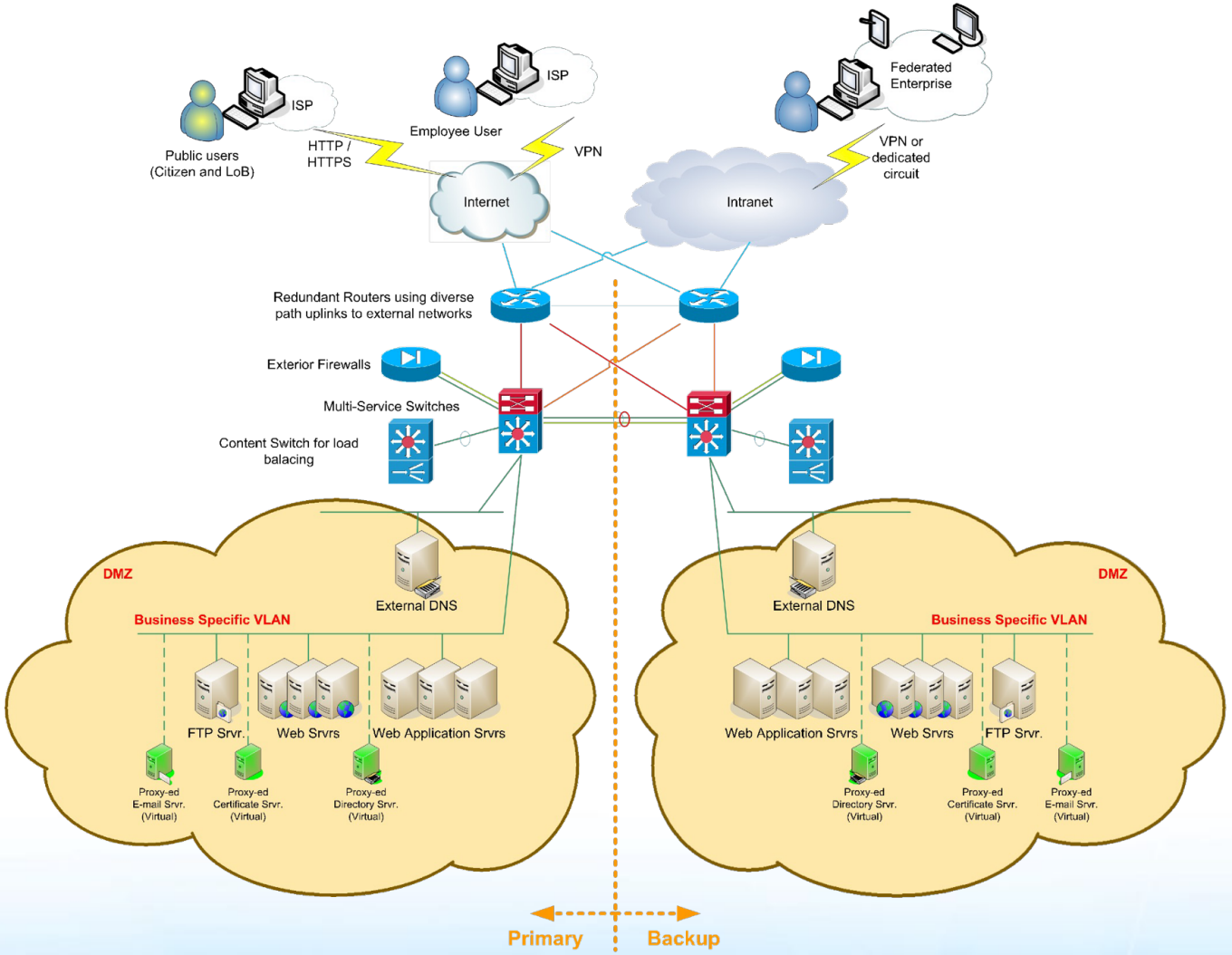
Firewall Policy

In principal, firewall performs three actions:

- *Accept*: where the firewall passes the IP packets through the firewall as matched by the specific rule
- *Drop*: where the firewall drops the IP packets, and not return an error message to the source system. (i.e., Like a “black hole”)
- *Reject*: where the firewall drops the IP packets when not matched by the specific rule and return an error message to the source system. (log entries are generated)



Network Design with Firewalls



Network Security Zones

- Internet Zone - No Trust
- External DMZ - Low Trust
- Enterprise Zone - Medium Trust
- Extranet Zone - Medium Trust
- Internal DMZ - High Trust
- Management Zone - Highest Trust
- Restricted Zone - Highest Trust

Internet Zone

- The Internet Zone includes the Internet, the Public Switched Telephone Network (PSTN), and any Internet Service Provider (ISP) public backbone networks

External DMZ

The External DMZ houses systems that require exposure to the Internet. This zone proxies access between systems in the Enterprise Zone and the Internet

- External web servers
- E-mail gateways
- FTP servers
- Web proxy servers
- Remote access services

Enterprise Zone

- The Enterprise Zone is where end-user systems reside, including end-user workstations, printers, and VoIP Phones. Endpoint protection is a critical control in this zone to limit the exposure of end-user systems to malware.

Extranet Zone

- The Extranet Zone houses connections with highly trusted 3rd party business partners and can be an extension of the Enterprise Zone.
- Nonetheless, it is recommended that traffic between the Enterprise and Extranet Zones is monitored and filtered at the zone's perimeter to allow only business approved traffic to enter and leave the zone

Internal DMZ

- The Internal DMZ mediates access between systems in the Enterprise/Extranet Zones and Restricted Zone. Internal application servers typically live in this zone. End-users must authenticate before gaining access to the data hosted in the Restricted Zone.

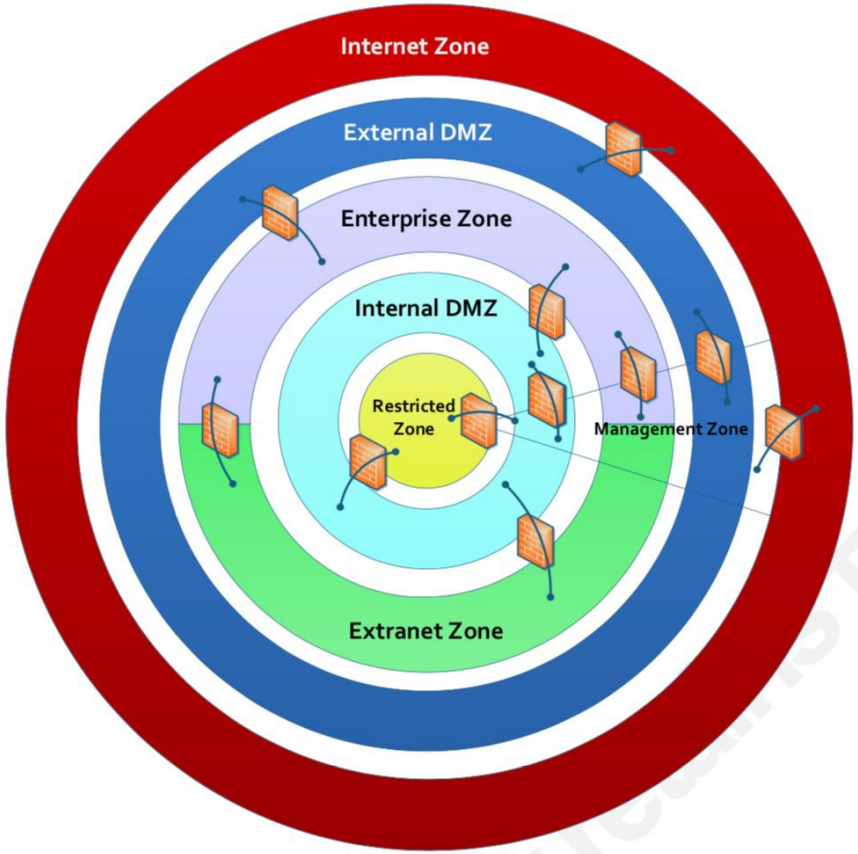
Restricted Zone

- User database servers
- Human Resources database servers
- Financial Database servers
- Intellectual property database servers

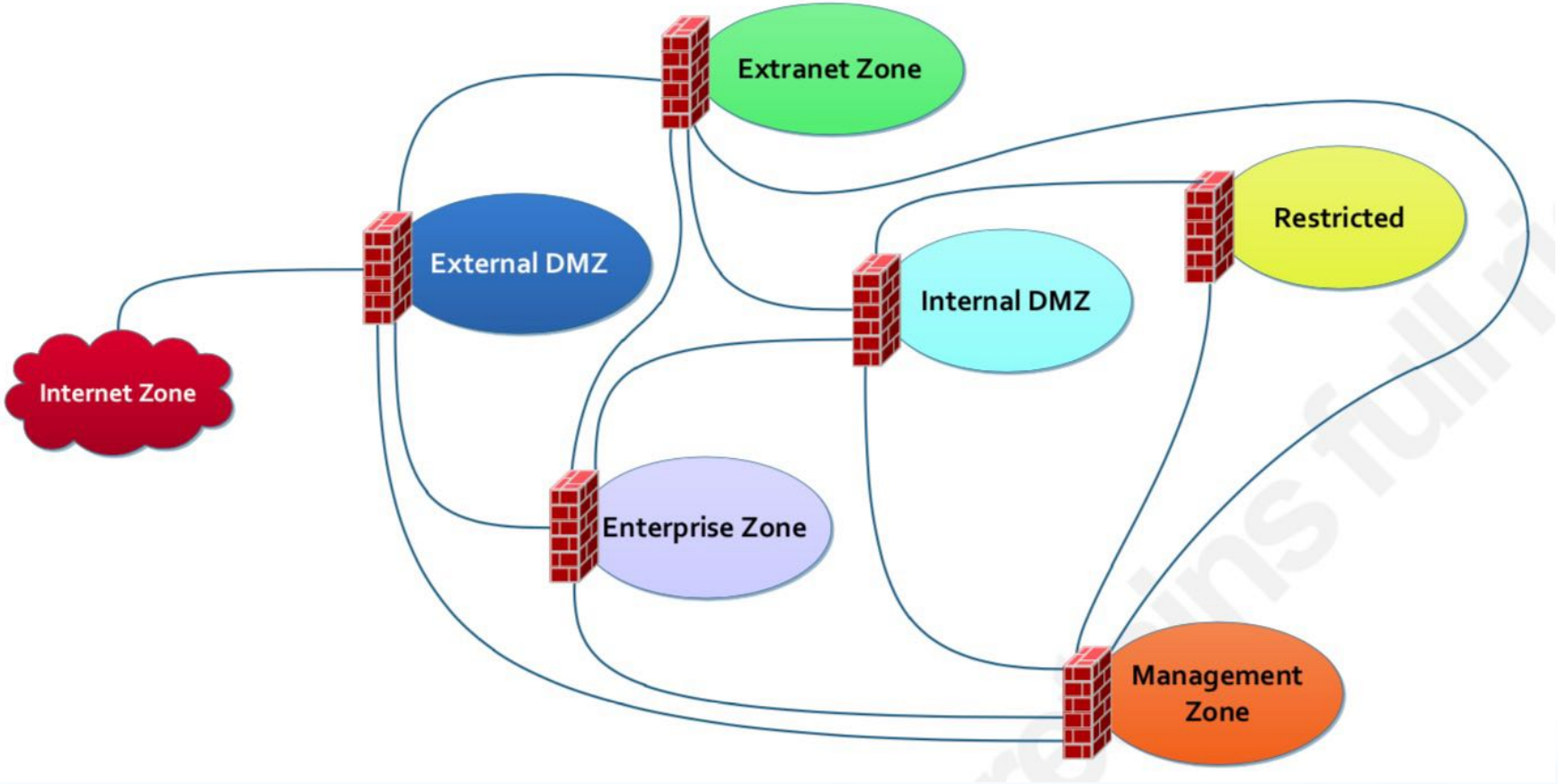
Management Zone

- The Management Zone houses administration and monitoring systems such as performance servers, configuration management servers, log management servers

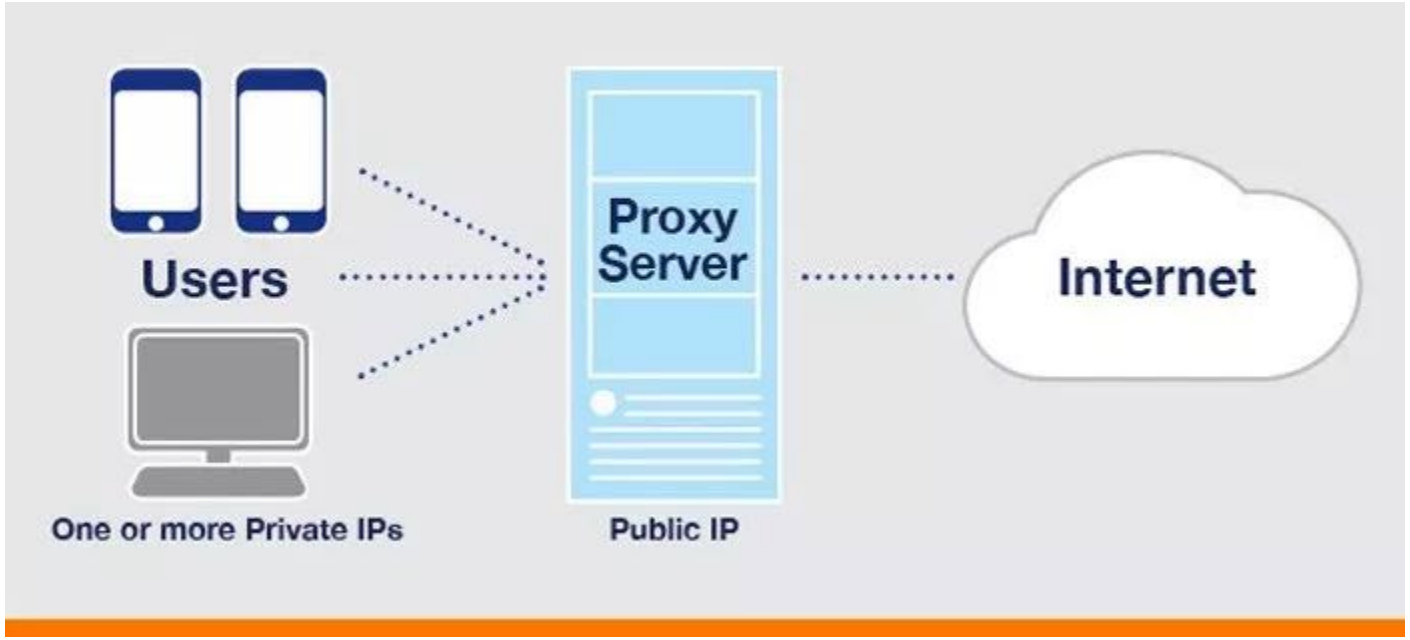
Zoning Network Infrastructure



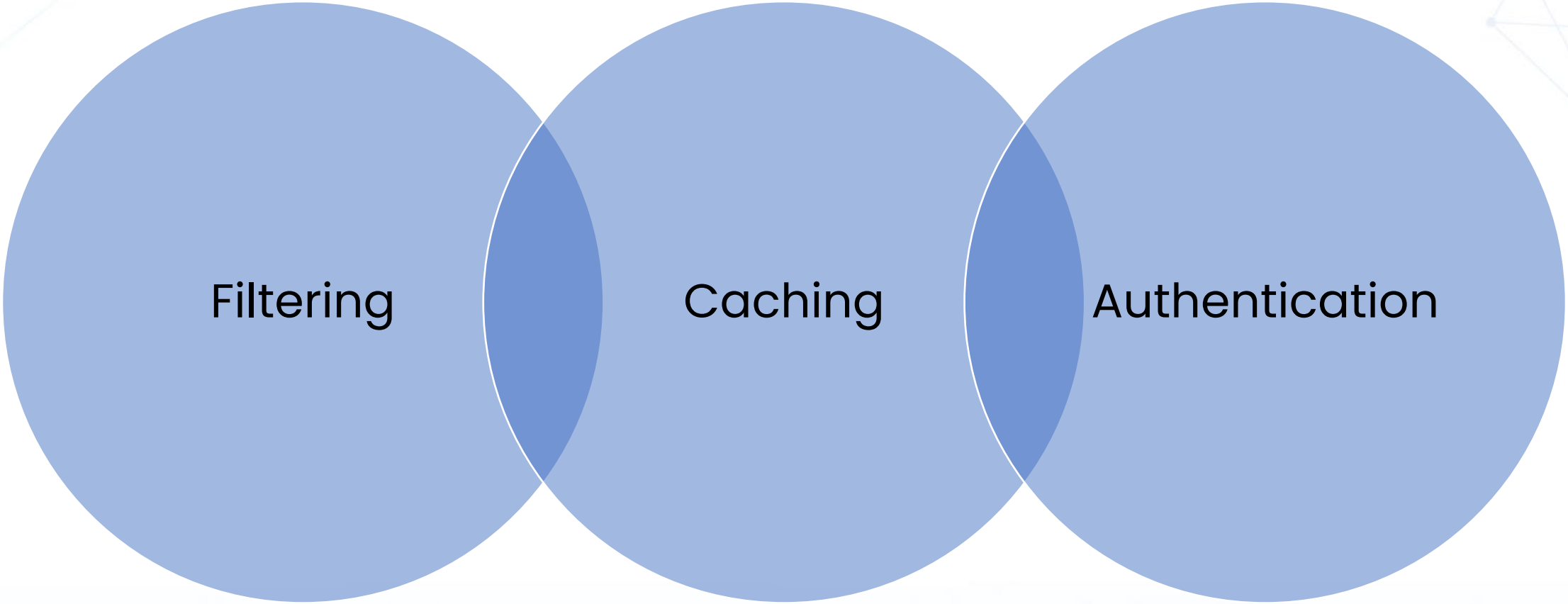
Rules Communication



Proxy



Proxy Functions



What is Web Application Firewall ?

- A software or hardware solution that protects your web enabled applications from threats/attacks.
- The solution must understand web protection at the application layer (HTTP and HTTPS conversations to your web applications, XML/SOAP, and Web Services).
- Detect/prevent OWASP Top Ten Threats.
- Many solutions learn about the web applications they protect.

What is the difference between WAFs and other Security Protection

- First generation firewalls (stateful inspection & proxy)
- Next Generation firewalls
  - Concentrate on application stream signatures which work well for outbound/ Internet traffic – very little inbound web server protection
- Network IDS/IPS
  - Broad network inspection support around TCP/IP, focus is wide, typically extension based for deeper understanding of HTTP. Typically, signature based. No user, session awareness

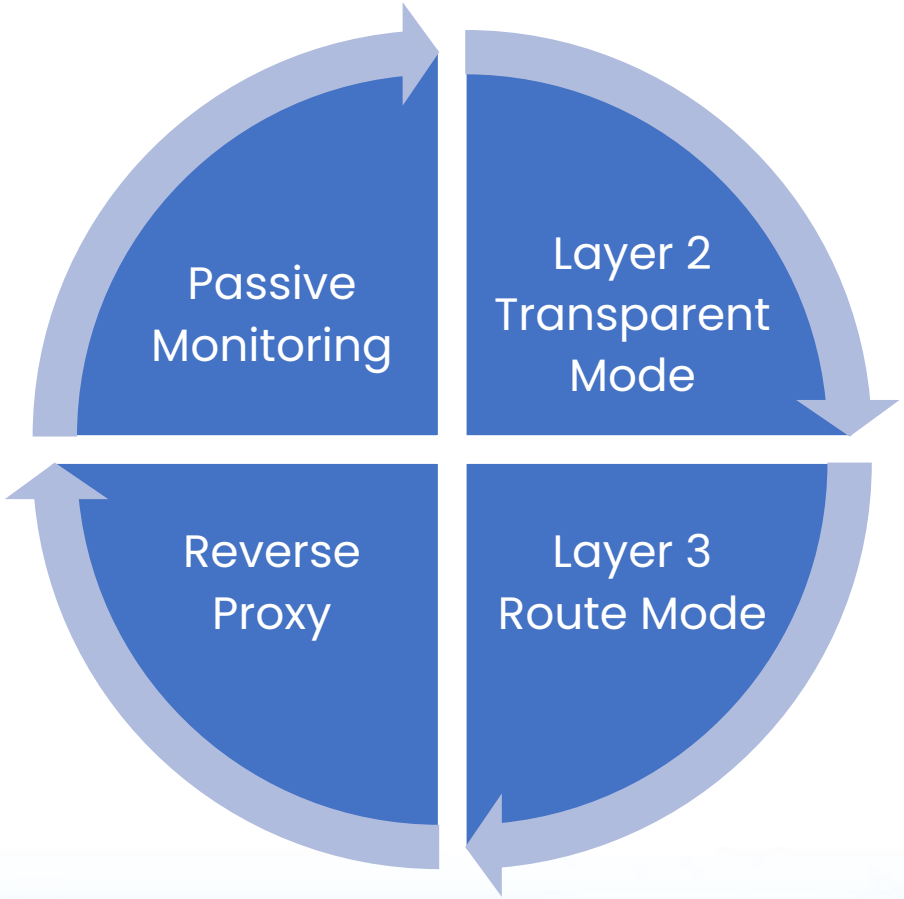
Main Feature of Web Application Firewall

- HTTP protocol support
- XML/SOAP support
- Anti-evasion
- SSL Decryption / Inspection
  - Decoding & path standardization
- Signatures
  - Generic attack (directory traversal, web-cgi, web-php, ...)
  - Known web application vulnerabilities (CVE defined web app vulnerabilities, wikis, phpmyexplorer, ...)
- Policy engine
- Alert / Auditing

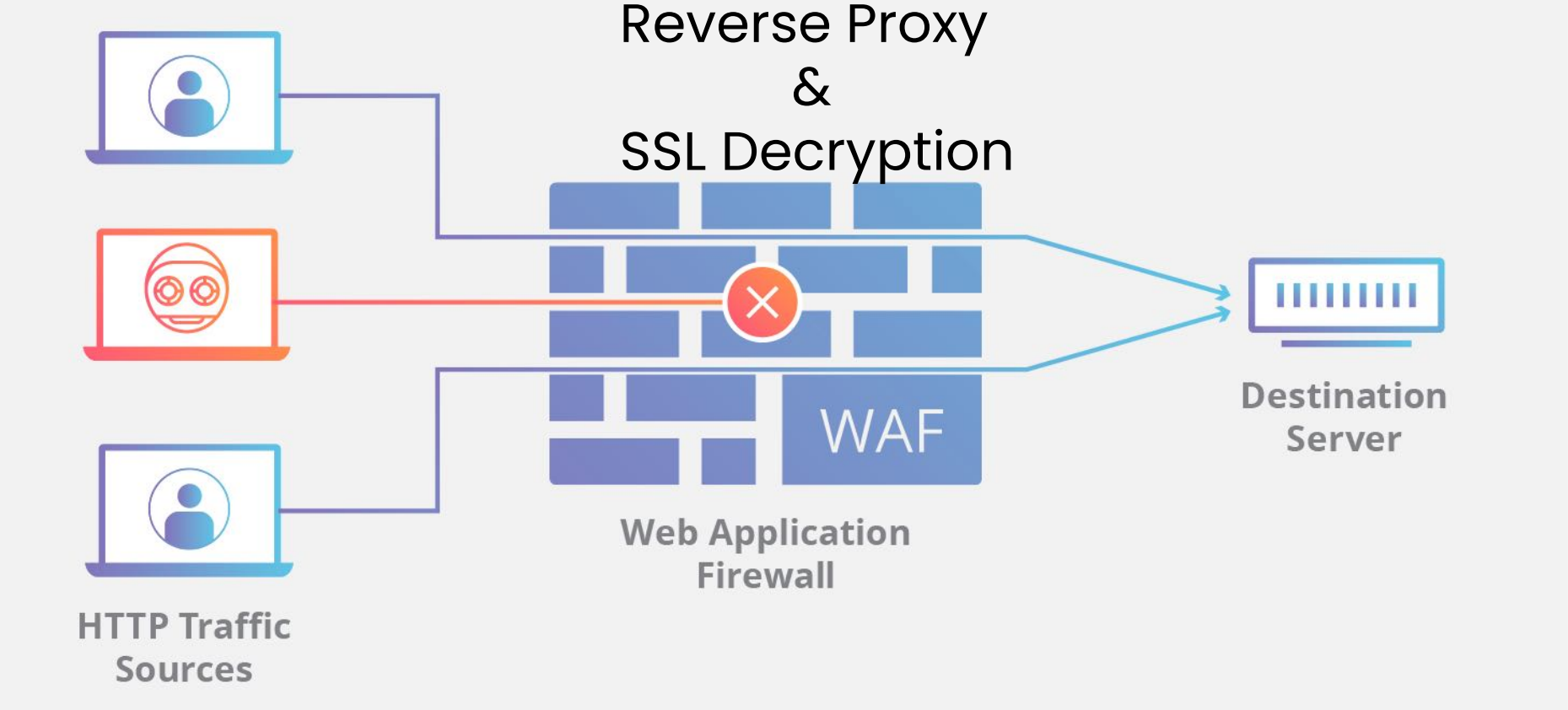
Web Application Firewall Securing Issues

- Yet-another-proxy argument (increased complexity of the IT infrastructure)
- Web Application Performance
- False positives (which may have a significant business impact)
- More complex troubleshooting
- Any potential effect on the web application if the WAF terminates the application session, for example
- Cost-effectiveness

Web Application Firewall Deployment

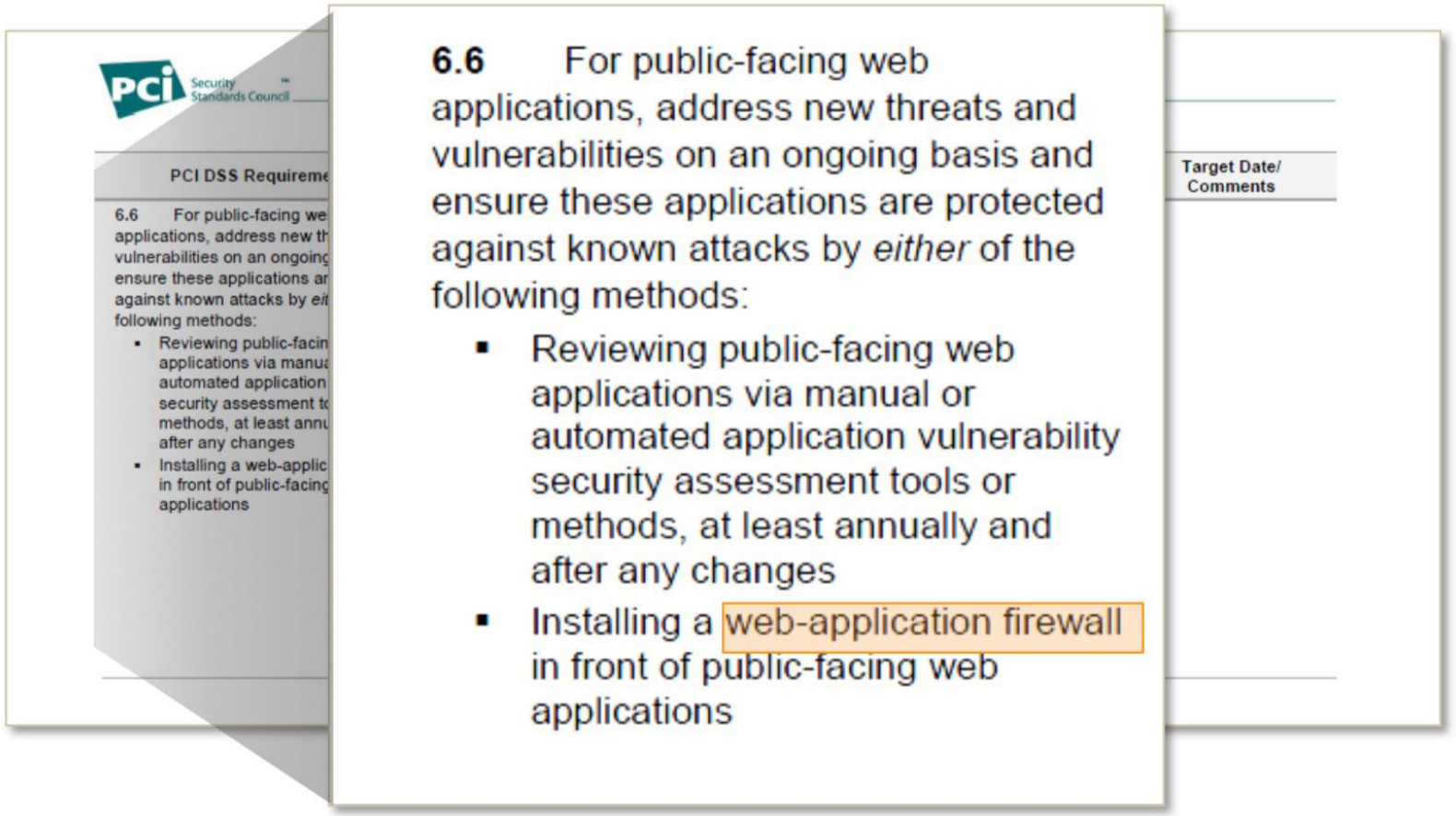


Web Application Firewall Typically Placement



https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/

Web Application Firewall for Compliance



Web Application Firewall Vendor

Figure 1. Magic Quadrant for Web Application Firewalls

Source: Gartner (August 2018)

Intrusion Detection and Prevention System

Intrusion Detection System (IDS) & Intrusion Prevention System (IPS)

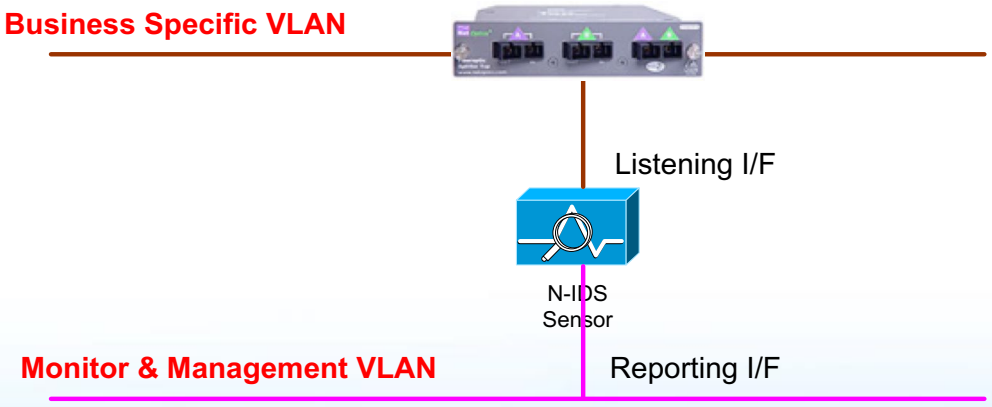
- Network-IDS (Intrusion Detection System) is a "passive" device
  - To detect attacks and other security violations
  - To detect and deal with pre-ambles to attacks (i.e., "doorknob rattling"/ probing / scanning)
  - To document the threat to a network, and improve diagnosis, recovery and correction of an unauthorized intrusion
- Network-IPS (Intrusion Prevention System) is a "in-line" device
  - Has all the same service features of a N-IDS, plus
  - Inference the internetworking "behavior" to PREVENT further damage to internetworking services

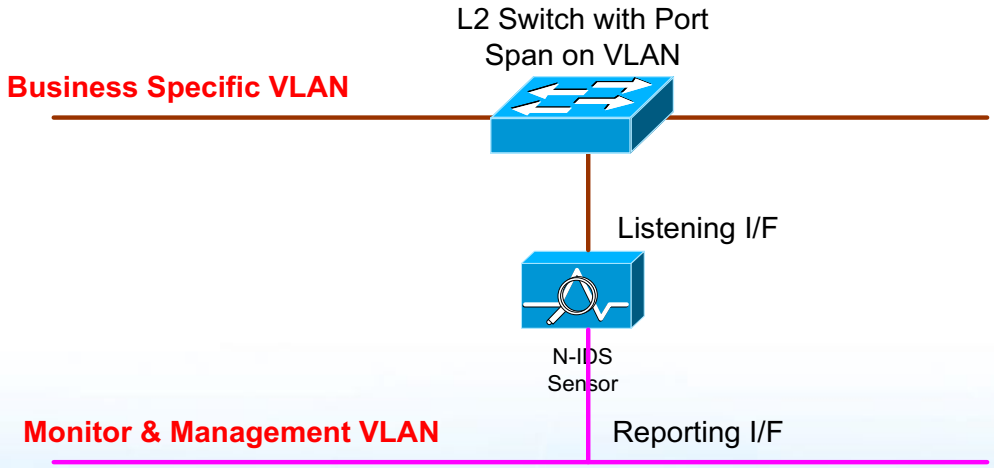
Intrusion Detection System (IDS) & Intrusion Prevention System (IPS)

- N-IDS (and Host-IDS) use "knowledge-based" (a.k.a. "signature-based") methodology to detect intrusions
  - Uses a database of known attacks and vulnerabilities called signatures
  - Only as good as the last signature update
  - Can be difficult to tune – false positives, acceptable behavior.
- N-IPS uses "behavior-based" methodology to detect and prevent intrusions.
  - Learns normal network or host behavior
  - Alerts when behavior deviates from the norm such as malformed packets, abnormal network utilization, or memory usage

Network-based Intrusion Detection System (N-IDS)

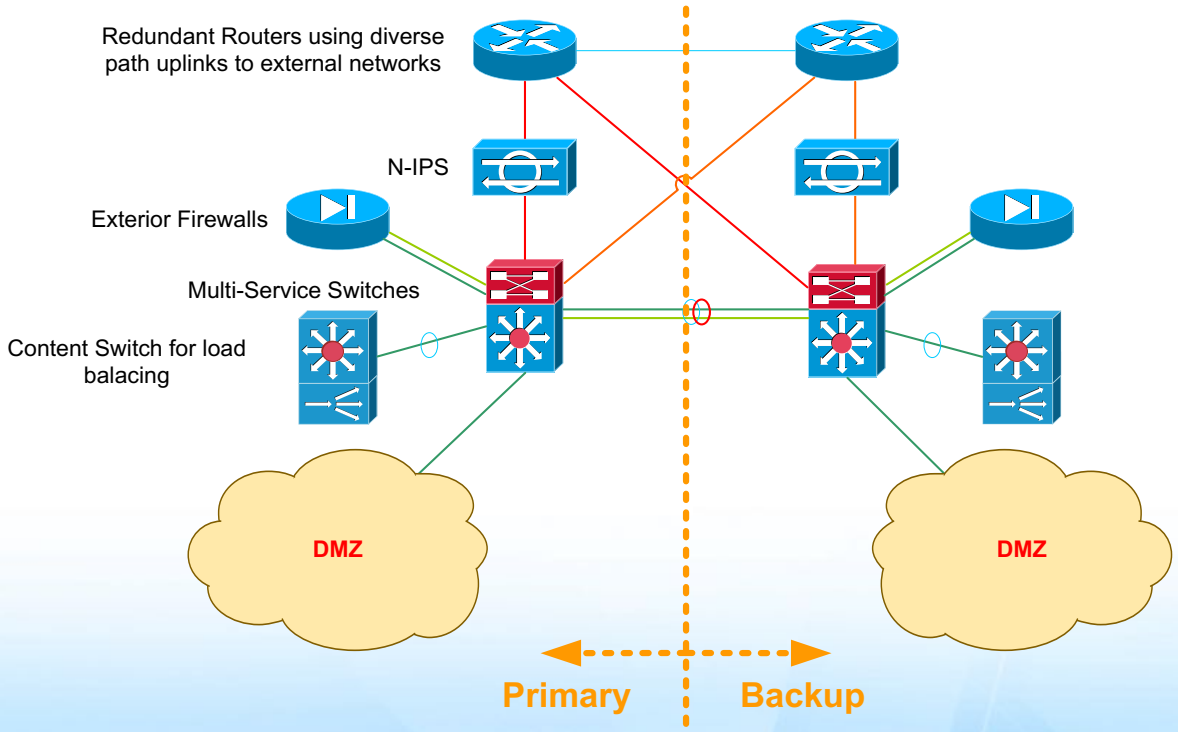
- Network-IDS (intrusion detection system) is a "passive" device
  - There are two way to setup the listening interfaces: Network TAP and VLAN Port Spanning on L2 switch
  - N-IDS is composted of two components: Pre-processor (Sensor) and Event Collector/Analyzer
    - Pre-processor assembles the packets and match them against a pre-defined signature database
    - Event Collector/Analyzer collects the events from all the sensors, correlate and present intrusion pattern



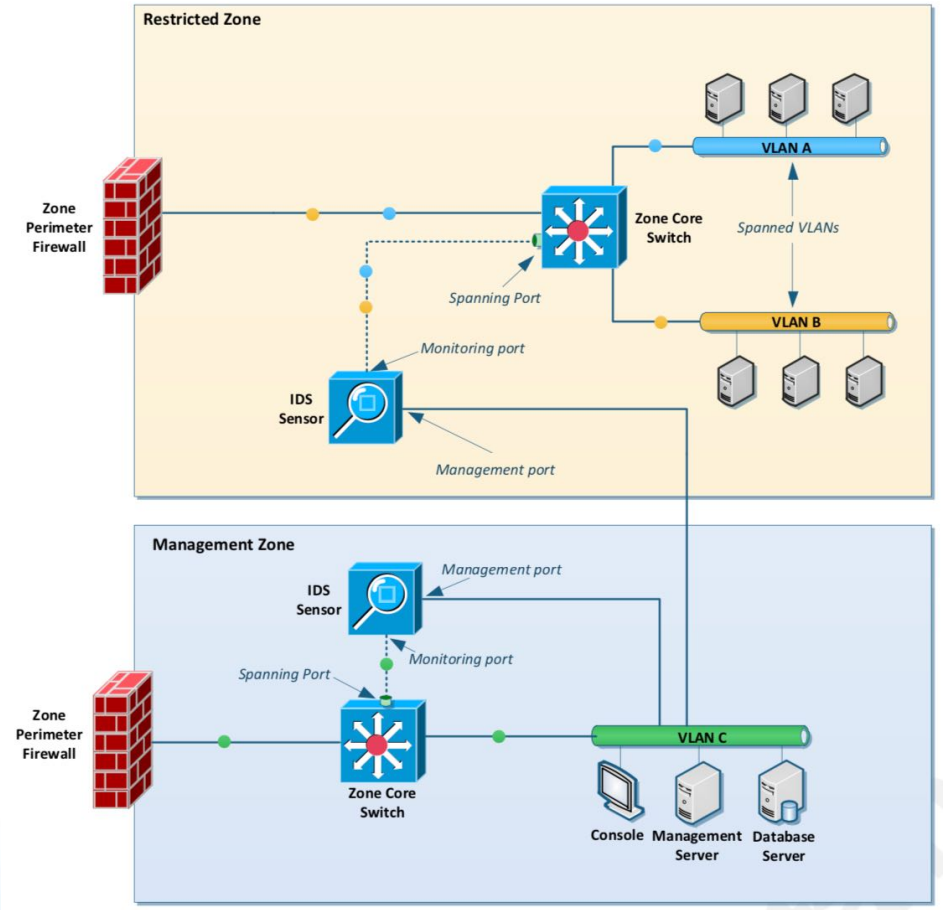


Network-based Intrusion Prevention System (N-IPS)

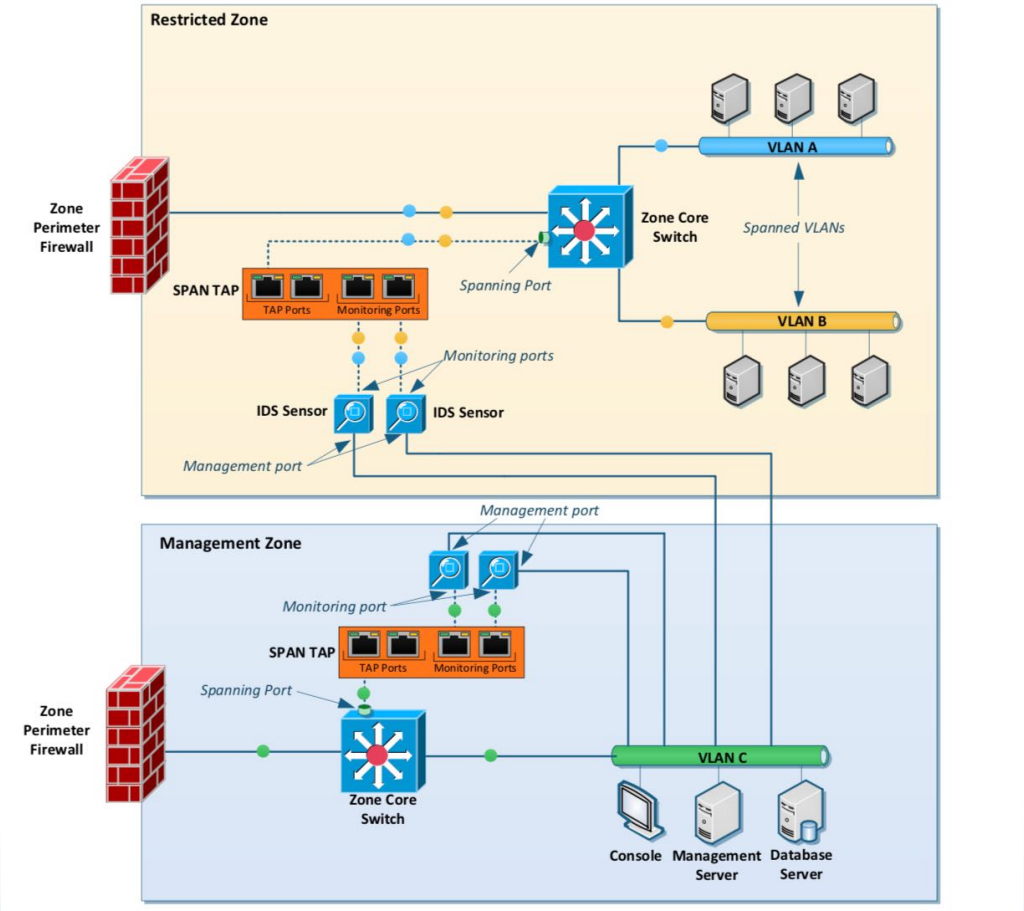
- Network-IPS (intrusion prevention system) is an "in-line" device
  - Examines network traffic and automatically blocks inappropriate or malicious traffic
  - However, it may block some "normal" enterprise internetworking LAN traffic. So, it's best to use it between the edge router and exterior perimeter firewall



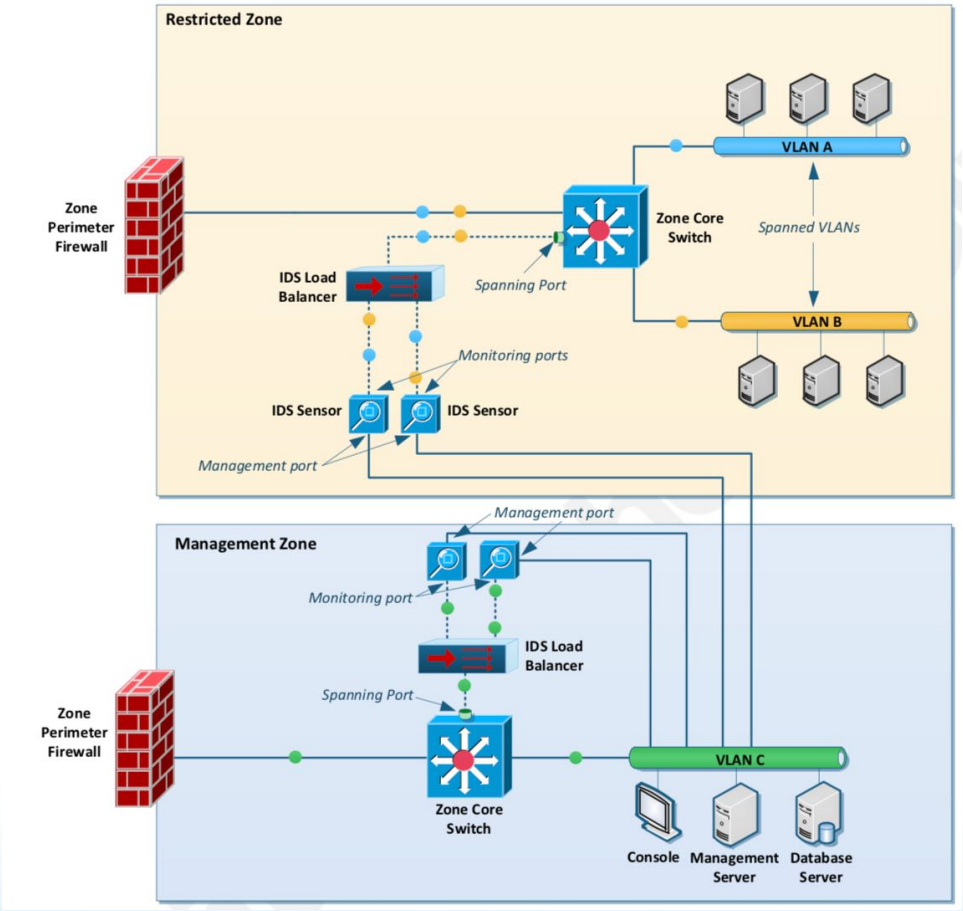
Network Intrusion Detection and Prevention Systems in Network Infrastructure



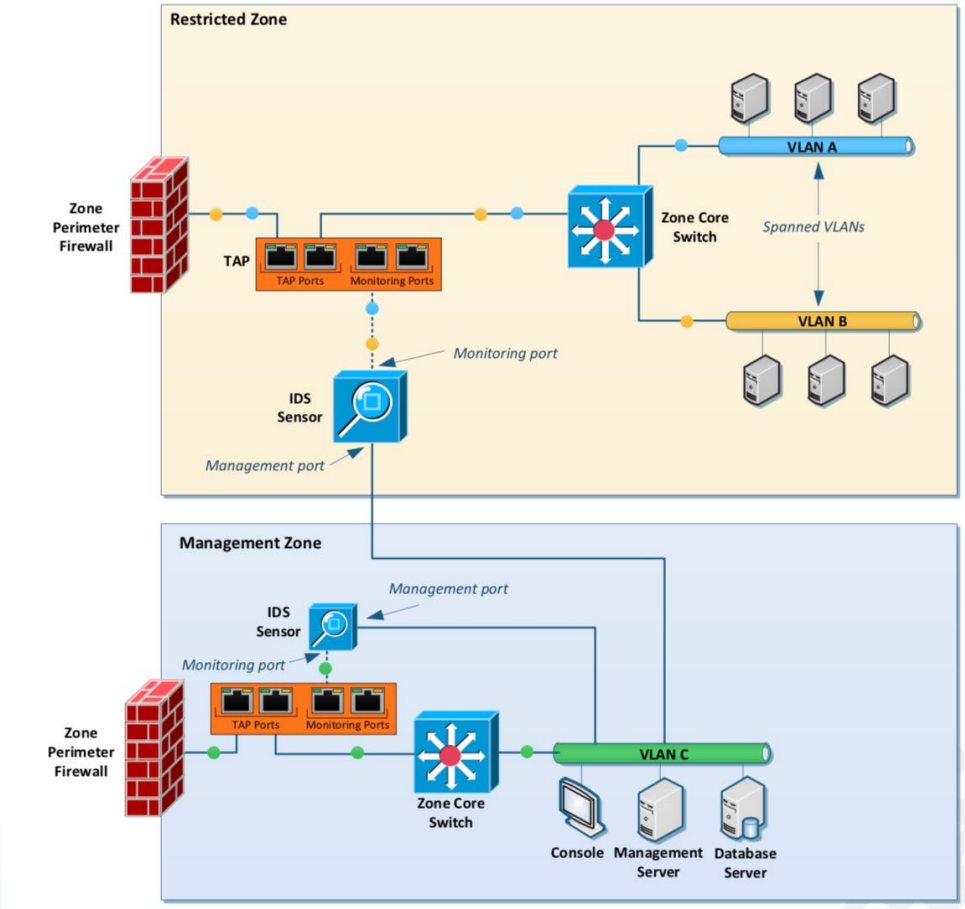
Network Intrusion Detection and Prevention Systems in Network Infrastructure



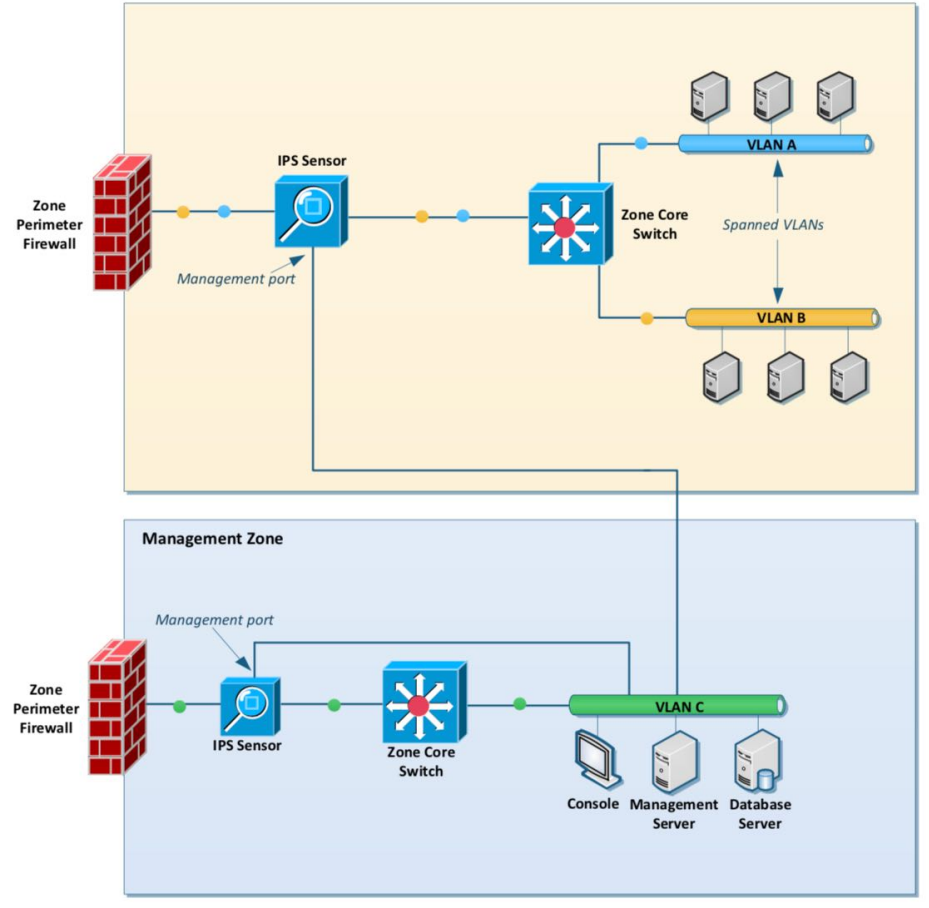
Network Intrusion Detection and Prevention Systems in Network Infrastructure



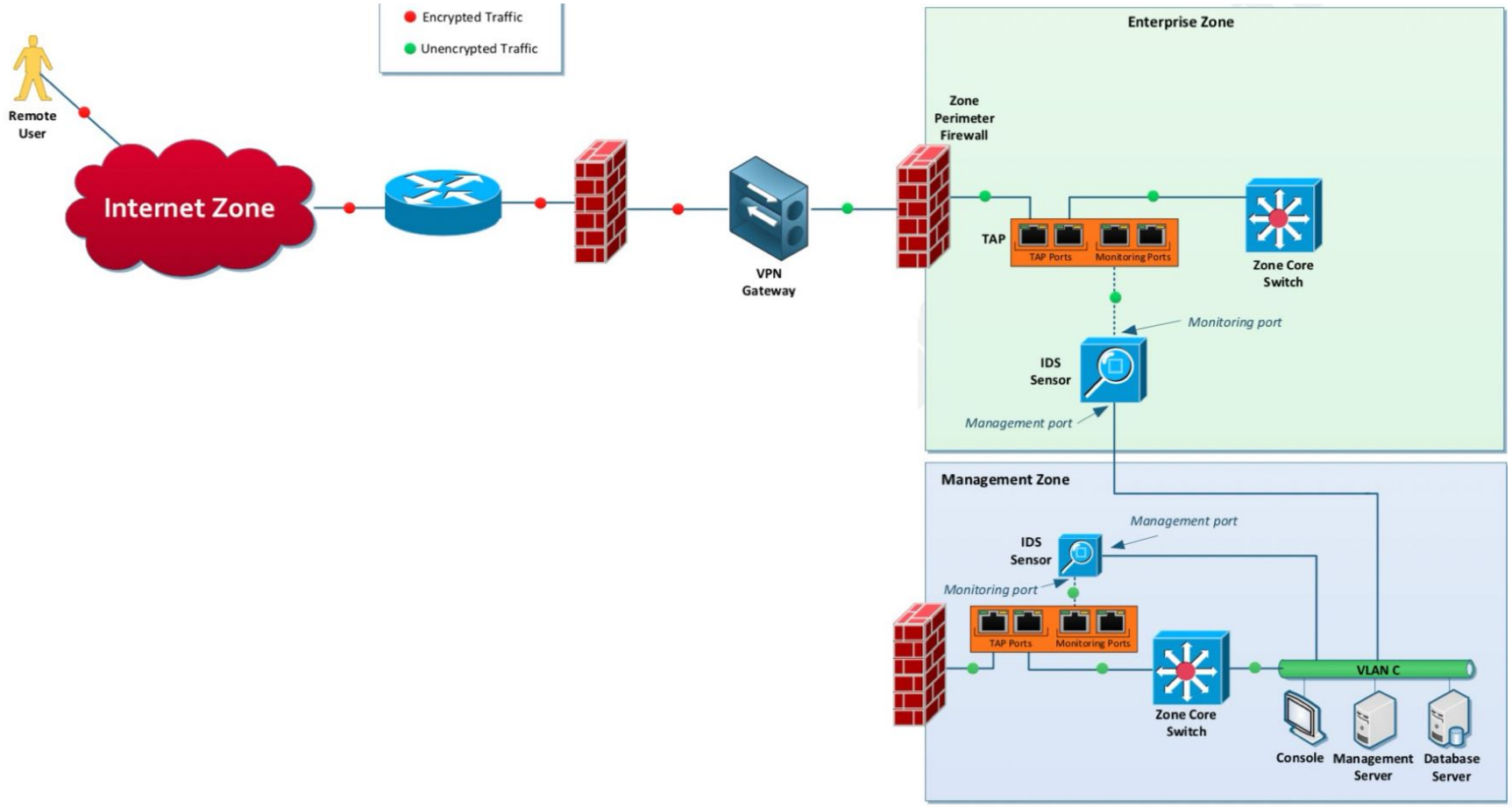
Network Intrusion Detection and Prevention Systems in Network Infrastructure



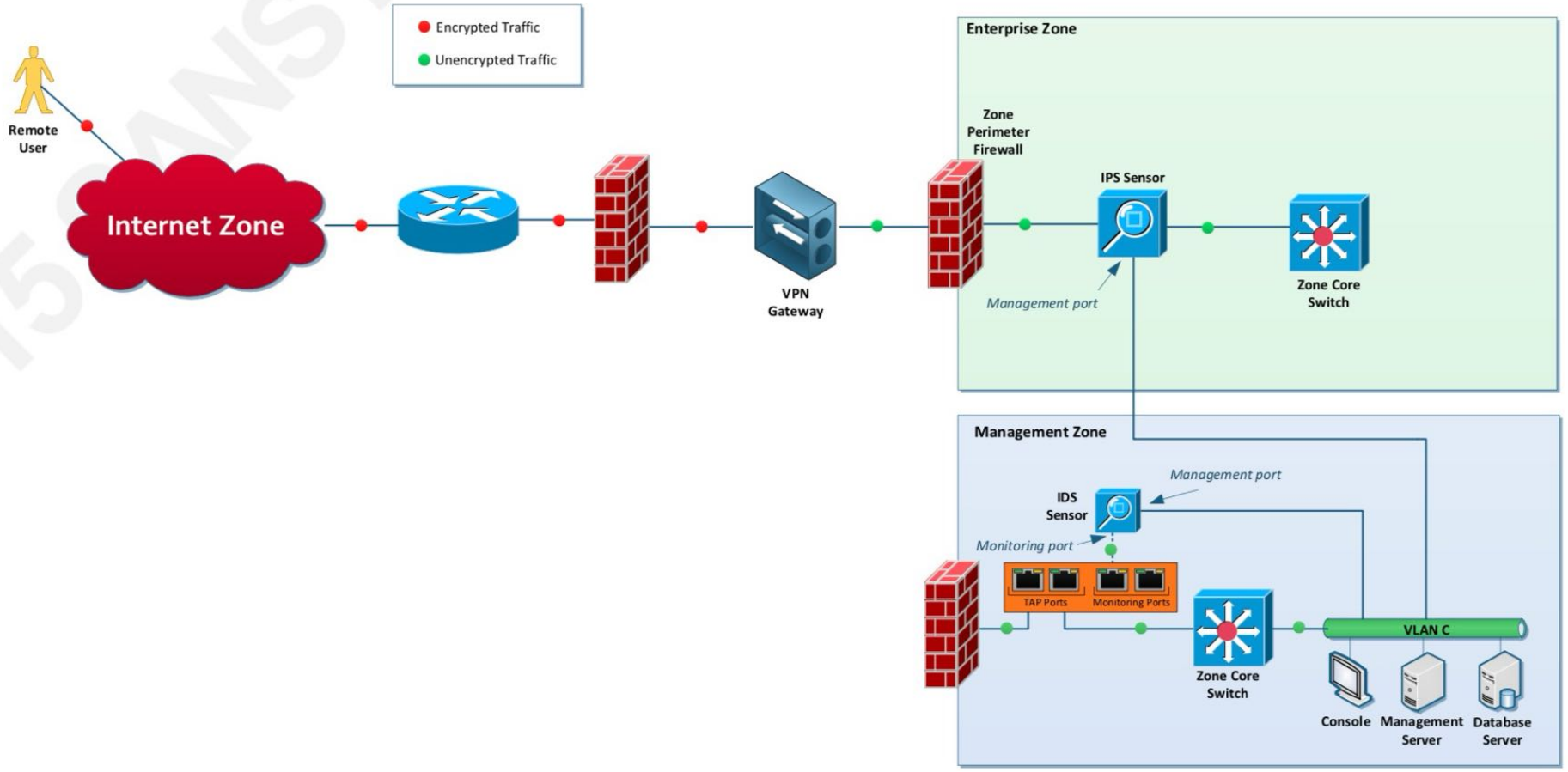
Network Intrusion Detection and Prevention Systems in Network Infrastructure



Monitoring via Unencrypted Network Traffic



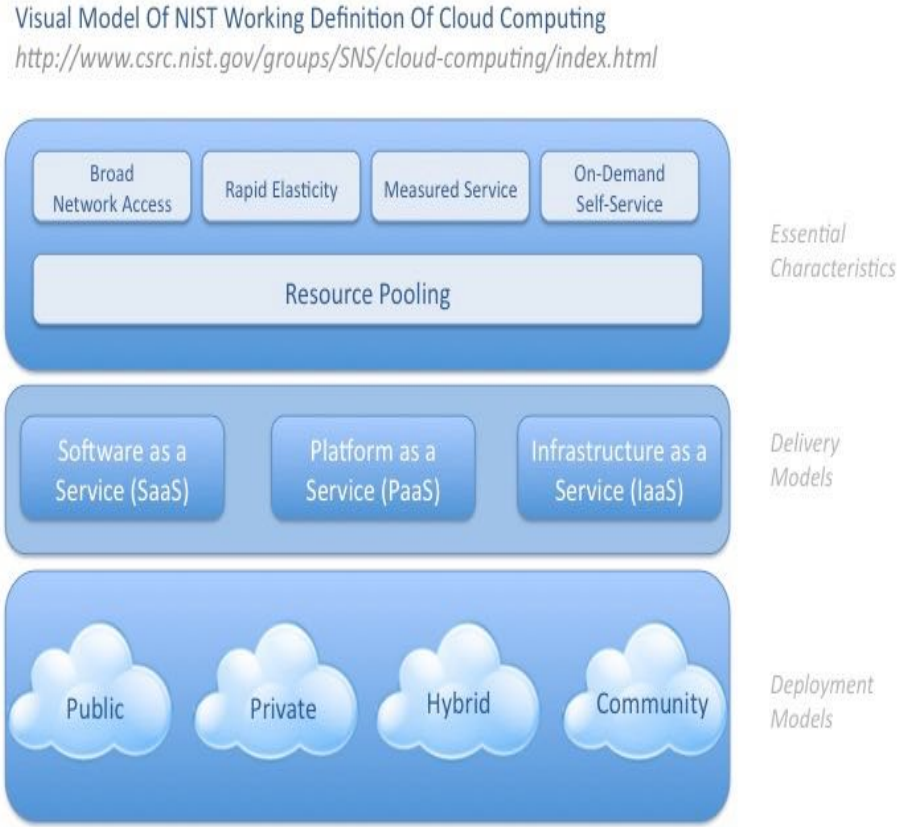
Monitoring unencrypted VPN traffic using IPS



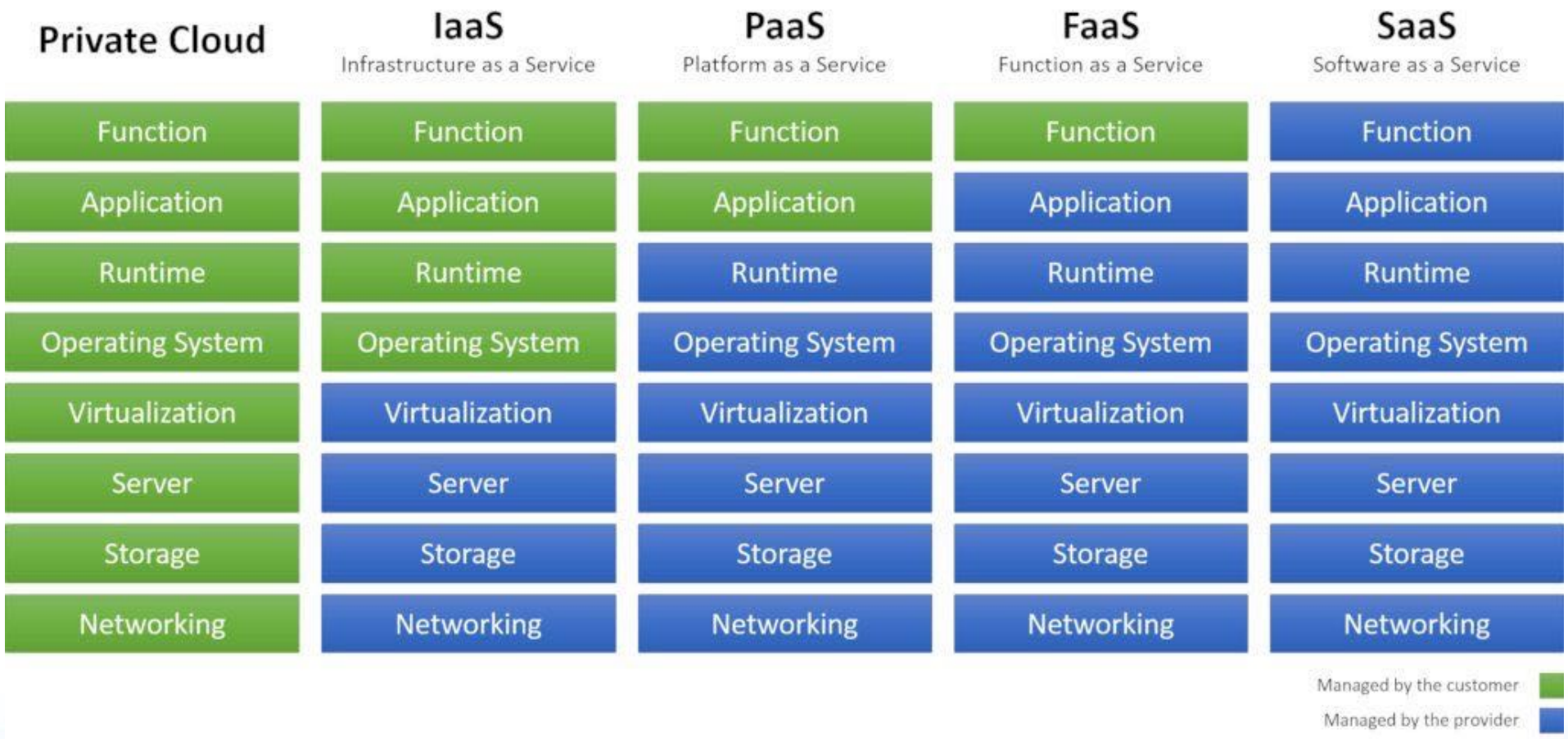
Cloud Security

What is Cloud Computing?

- Compute as a utility: third major era of computing
- Cloud enabled by
  - Moore's Law
  - Hyperconnectivity
  - SOA
  - Provider scale
- Key characteristics
  - Elastic & on-demand
  - Multi-tenancy
  - Metered service
- IaaS may track energy costs



CSA Reference Model



Cloud Service Model

PUBLIC CLOUD

- Offered by third-party providers
- Available to anyone over the public internet
- Scales quickly and convenient

HYBRID CLOUD

- Combination of both public and private cloud
- Shared security responsibility
- Helps maintain tighter controls over sensitive data and processes

PRIVATE CLOUD

- Offered to select users over the internet or a private internal network
- Provides greater security controls
- Requires traditional datacenter staffing and maintenance

About the Cloud Security Alliance

- Global, not-for-profit organization
- Over 23,000 individual members, 100 corporate members, 50 chapters
- Building best practices and a trusted cloud ecosystem
- Agile philosophy, rapid development of applied research
  - GRC: Balance compliance with risk management
  - Reference models: build using existing standards
  - Identity: a key foundation of a functioning cloud economy
  - Champion interoperability
  - Enable innovation
  - Advocacy of prudent public policy

"To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing."

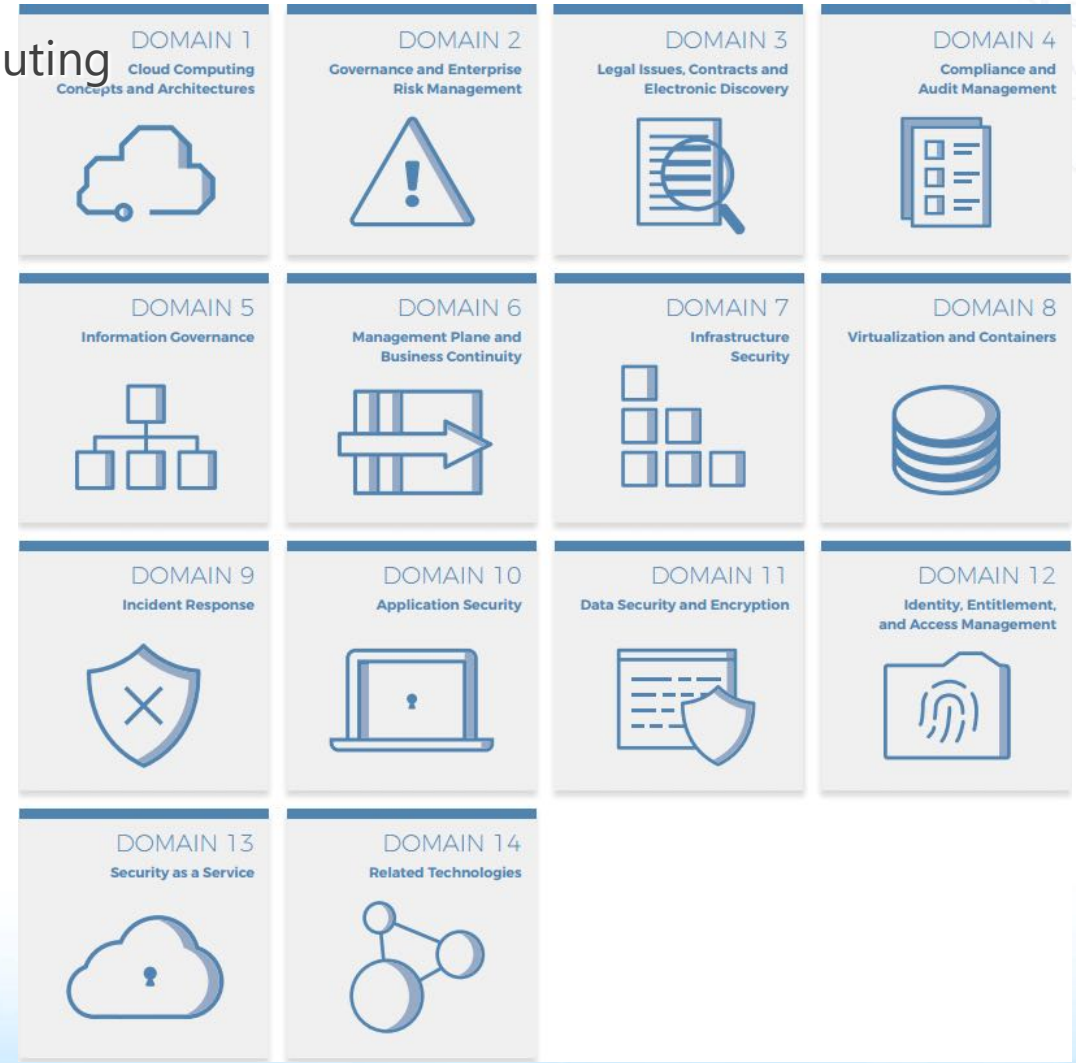
Key Cloud Security Problems of Today

From CSA Top Threats Research:

- Trust: Lack of Provider transparency, impacts Governance, Risk Management, Compliance
- Data: Leakage, Loss or Storage in unfriendly geography
- Insecure Cloud software
- Malicious use of Cloud services
- Account/Service Hijacking
- Malicious Insiders
- Cloud-specific attacks

CSA Guidance Research

- Popular best practices for securing cloud computing
- Flagship research project
- V2.1 released 12/2009
- V4 released 07/2017
- wiki.cloudsecurityalliance.org/guidance



Guidance > 100k downloads:
cloudsecurityalliance.org/guidance

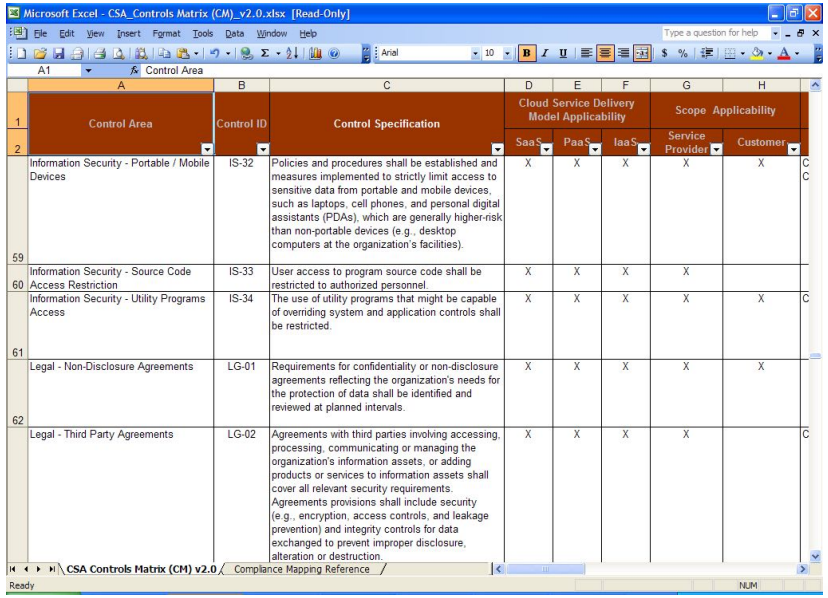
A Complete Cloud Security Governance, Risk, and Compliance (GRC) Stack

Delivering	← Stack Pack →	Description
Continuous monitoring … with a purpose	CTP™	• Common technique and nomenclature to request and receive evidence and affirmation of current cloud service operating circumstances from cloud providers
Claims, offers, and the basis for auditing service delivery	Cloud Audit™	• Common interface and namespace to automate the Audit, Assertion, Assessment, and Assurance (A6) of cloud environments
Pre-audit checklists and questionnaires to inventory controls	CAI™	• Industry-accepted ways to document what security controls exist
The recommended foundations for controls	CCM™	• Fundamental security principles in specifying the overall security needs of a cloud consumers and assessing the overall security risk of a cloud provider

Cloud Controls Matrix Tool

- Controls derived from guidance
- Customer vs. Provider role
- Mapped to ISO 27001, COBIT, PCI, HIPAA
- Help bridge the gap for IT & IT auditors

CCM™
Cloud Controls Matrix


Microsoft Excel - CSA_Controls Matrix (CM)_v2.0.xlsx [Read-Only]

Control Area	Control ID	Control Specification	Cloud Service Delivery Model Applicability			Scope Applicability		
			SaaS	PaaS	IaaS	Service Provider	Customer	
Information Security - Portable / Mobile Devices	IS-32	Policies and procedures shall be established and measures implemented to strictly limit access to sensitive data from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities).	X	X	X	X	X	C C
Information Security - Source Code Access Restriction	IS-33	User access to program source code shall be restricted to authorized personnel.	X	X	X	X		
Information Security - Utility Programs Access	IS-34	The use of utility programs that might be capable of overriding system and application controls shall be restricted.	X	X	X	X	X	C
Legal - Non-Disclosure Agreements	LG-01	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of data shall be identified and reviewed at planned intervals.	X	X	X	X	X	
Legal - Third Party Agreements	LG-02	Agreements with third parties involving accessing, processing, communicating or managing the organization's information assets, or adding products or services to information assets shall cover all relevant security requirements. Agreements provisions shall include security (e.g., encryption, access controls, and leakage prevention) and integrity controls for data exchanged to prevent improper disclosure, alteration or destruction.	X	X	X	X		C

CSA Controls Matrix (CM) v2.0 | Compliance Mapping Reference

Ready

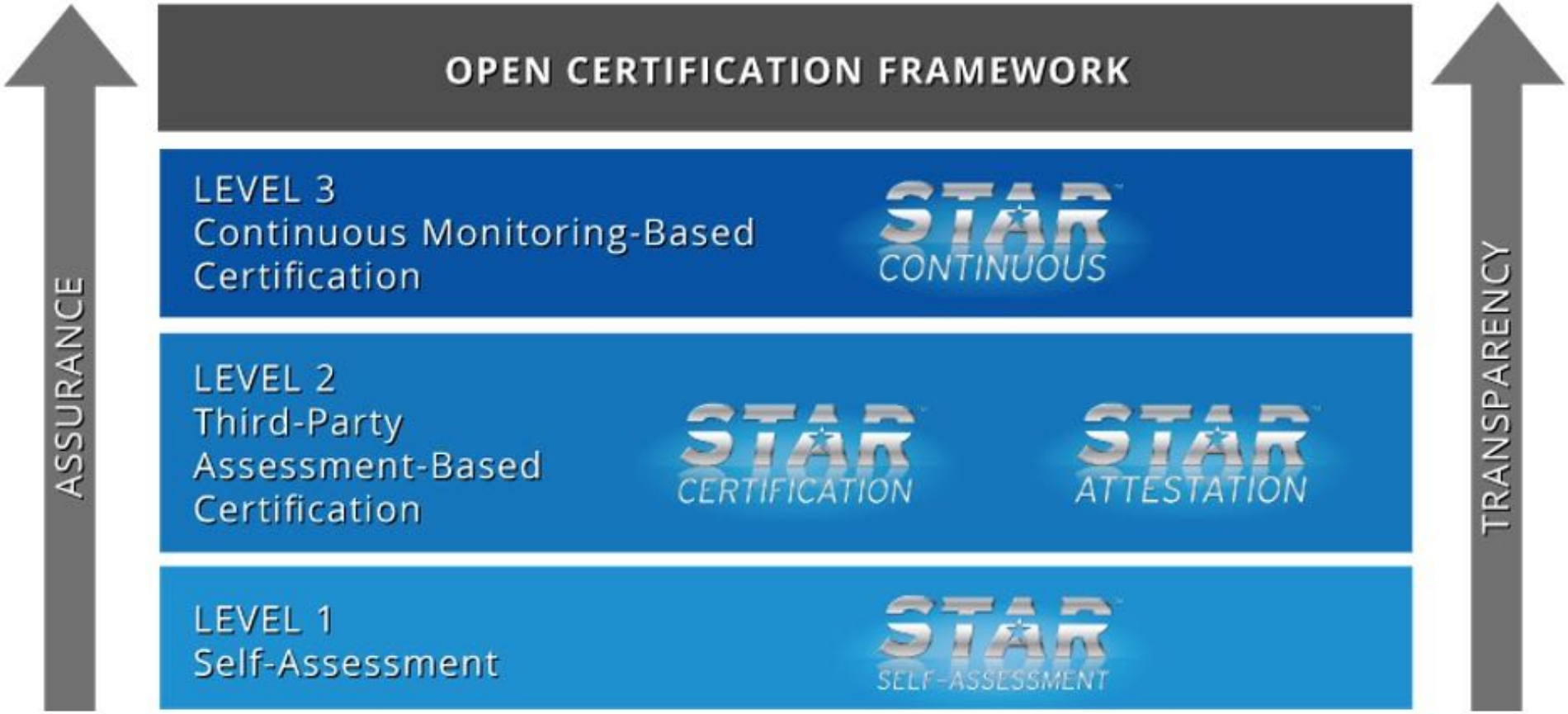
Consensus Assessment Initiative

- Research tools and processes to perform shared assessments of cloud providers
- Integrated with Controls Matrix
- Version 1 CAI Questionnaire released Oct 2010, approximately 140 provider questions to identify presence of security controls or practices
- Use to assess cloud providers today, procurement negotiation, contract inclusion, quantify SLAs
- www.cloudsecurityalliance.org/cai.html

CSA STAR Registry

- CSA STAR (Security, Trust and Assurance Registry)
- Public Registry of Cloud Provider self assessments
- Based on Consensus Assessments Initiative Questionnaire
  - Provider may substitute documented Cloud Controls Matrix compliance
- Voluntary industry action promoting transparency
- Free market competition to provide quality assessments
  - Provider may elect to provide assessments from third parties
- Available October 2011

Open Certification Framework



The CSA Open Certification Framework is an industry initiative to allow global, accredited, trusted certification of cloud providers.

CCSK – Certificate of Cloud Security Knowledge

- Only user certification for cloud security
- Web-based test for competency in CSA guidance
- $295 USD price
- www.cloudsecurityalliance.org/certifyme
- Training courses are available now!

Cloud Security Guideline Publication

Browse Publications

guidance

Filter Results

- By Cloud Experience -
- By Industry -
- By Working Group -
- By Topics -
- By language -

SecaaS Category 3 // Web Security Implementation Guidance

Release Date: 10/08/2012

The vendor and academic community have come together to form a set of solutions called Security as a Service. This document specifically addresses one elemen...

Request to download →

SecaaS Category 10 // Network Security Implementation Guidance

Release Date: 10/08/2012

In a cloud environment, a major part of network security is likely to be provided by virtual security devices and services, alongside traditional physical ne...

Request to download →

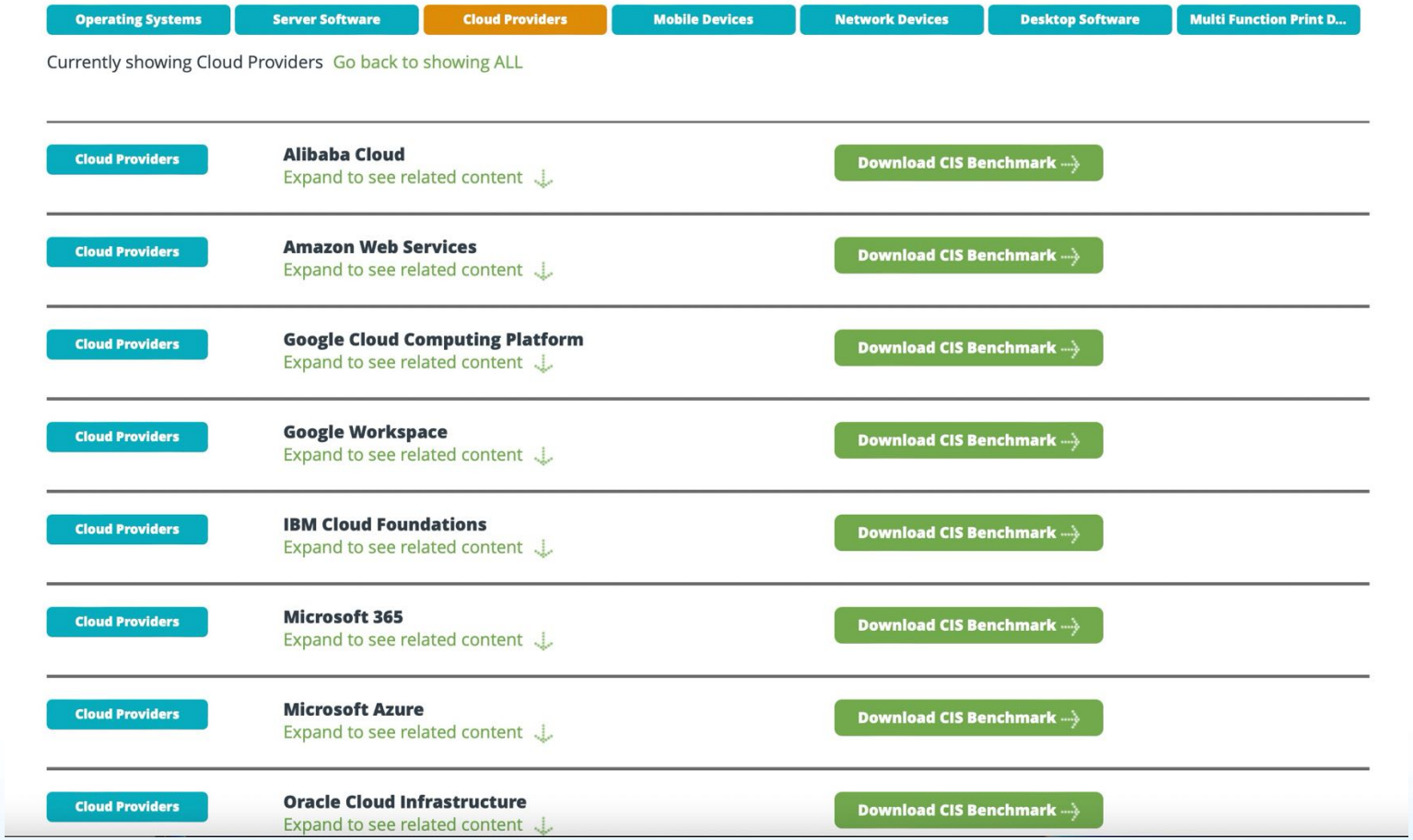
SecaaS Category 1 // Identity and Access Management Implementation Guidance

Release Date: 09/26/2012

This document addresses personnel involved in the identification and implementation of

https://cloudsecurityalliance.org/research/artifacts/?

CIS Benchmark for Cloud Computing



Cloud Security Assessment Tools

- https://github.com/0xVariable/AWS-Security-Tools
- https://github.com/kmcquade/awesome-azure-security#security-assessment-tools
- https://github.com/kuzeyardabulut/azure-assessment

Defensive (Hardening, Security Assessment, Inventory)

- **ScoutSuite**: https://github.com/nccgroup/ScoutSuite - Multi-Cloud Security auditing tool for AWS, Google Cloud and Azure environments (Python)
- **Prowler**: https://github.com/toniblyx/prowler - CIS benchmarks and additional checks for security best practices in AWS (Shell Script)
- **CloudSploit**: https://github.com/cloudsploit/scans - AWS security scanning checks (NodeJS)
- **CloudMapper**: https://github.com/duo-labs/cloudmapper - helps you analyze your AWS environments (Python)
- **CloudTracker**: https://github.com/duo-labs/cloudtracker - helps you find over-privileged IAM users and roles by comparing CloudTrail logs with current IAM policies (Python)
- **AWS Security Benchmarks**: https://github.com/awslabs/aws-security-benchmark - scrips and templates guidance related to the AWS CIS Foundation framework (Python)
- **AWS Public IPs**: https://github.com/arkadiyt/aws_public_ips - Fetch all public IP addresses tied to your AWS account. Works with IPv4/IPv6, Classic/VPC networking, and across all AWS services (Ruby)
- **PMapper**: https://github.com/nccgroup/PMapper - Advanced and Automated AWS IAM Evaluation (Python)
- **AWS-Inventory**: https://github.com/nccgroup/aws-inventory - Make a inventory of all your resources across regions (Python)
- **Resource Counter**: https://github.com/disruptops/resource-counter - Counts number of resources in categories across regions
- **ICE**: https://github.com/Teevity/ice - Ice provides insights from a usage and cost perspective, with high detail dashboards.
- **SkyArk**: https://github.com/cyberark/SkyArk - SkyArk provides advanced discovery and security assessment for the most privileged entities in the tested AWS.
- **Trailblazer AWS**: https://github.com/willbengtson/trailblazer-aws - Trailblazer AWS, determine what AWS API calls are logged by CloudTrail and what they are logged as. You can also use TrailBlazer as an attack simulation framework.
- **Lunar**: https://github.com/lateralblast/lunar - Security auditing tool based on several security frameworks (it does some AWS checks)

CS Suite

Scout2
First thing you should look at !

Prowler
Second best thing !

Web & Network
Info on: CDN, CERTS, DNS, ELB

Data Stores
Info on: EC, ES, RDS, REDSHIFT

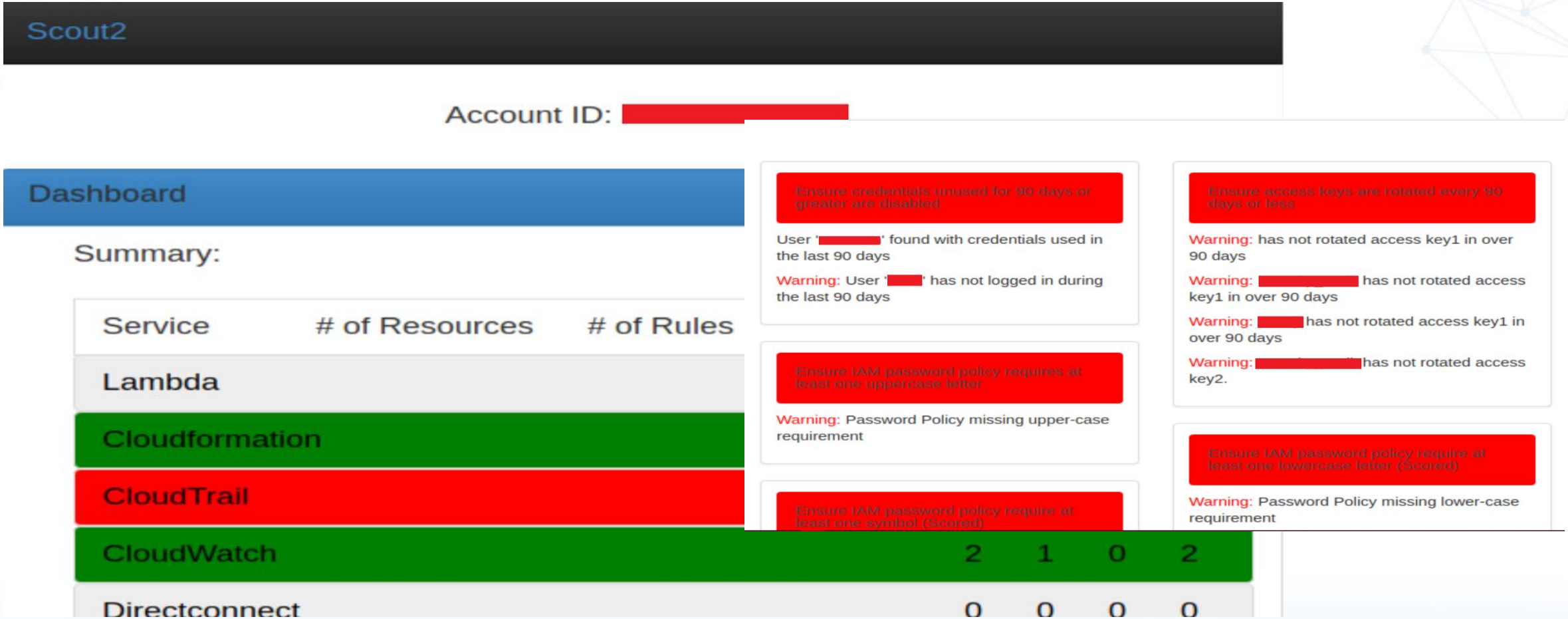
Notification
More info on: CloudFormation, SES, SNS

Configs
More info on: EC2, KEYS, AWS Config, VPC

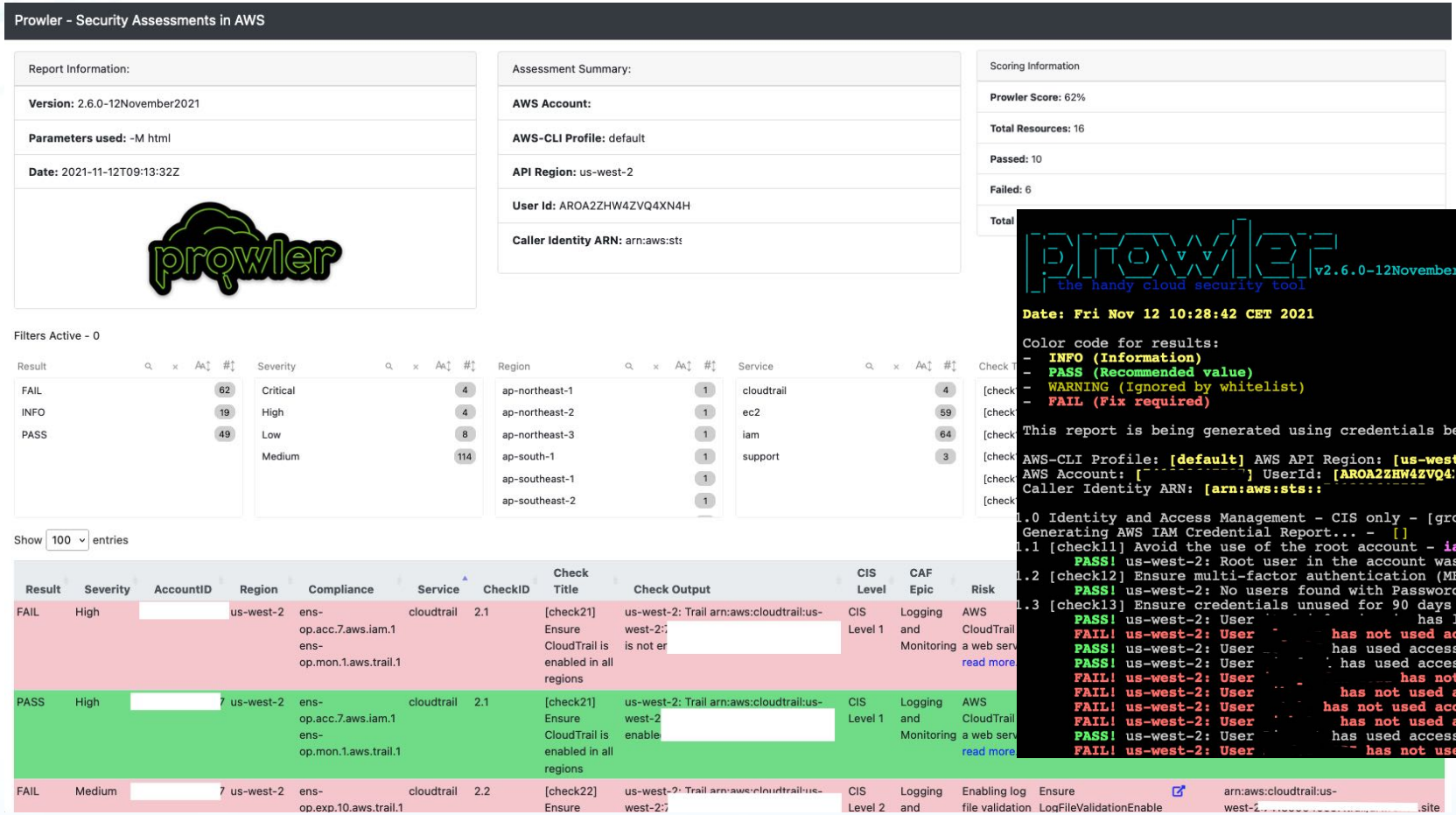
AWS Trusted Advisor
More info on: Checks from AWS Trusted Advisor

IP Audit
Check IP Audit results

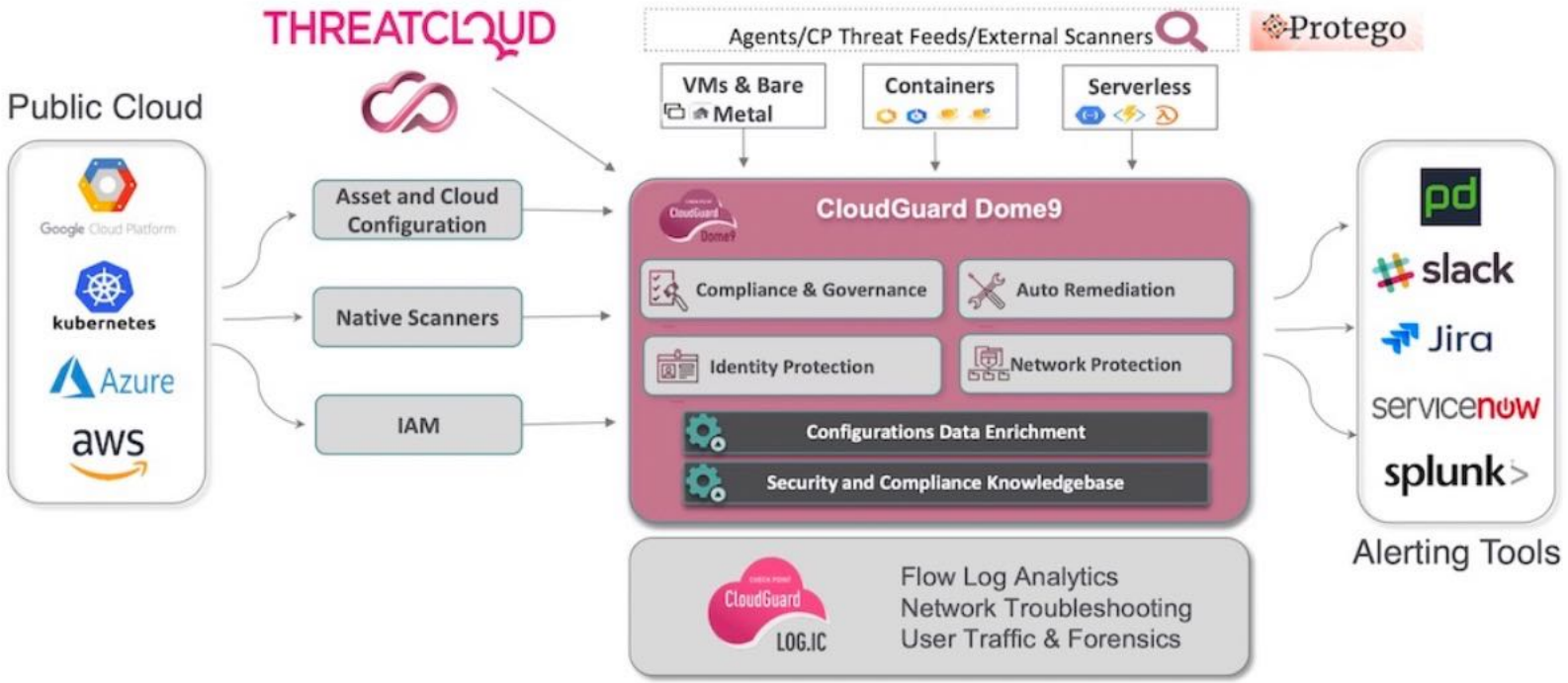
CS Suite Result



Prowler



Checkpoint Dome9



Endpoint Security

Endpoint Security Controls

Protection of servers (network focused)…

- Securing Core OS
- Security Update
- Be specific on service functions
  - Limit services, minimize potential exposures
  - Focus on a single function…

Web Server	Web Pages
DNS Server	DNS
E-mail Server	E-mail
DB Server	DB Services
- Install Host-IDS / Secure 3rd Party Application
  - Enforce CM and Change Control
- Install Anti-Virus
- Disable all processes/services not in use
- Enforce strict access control

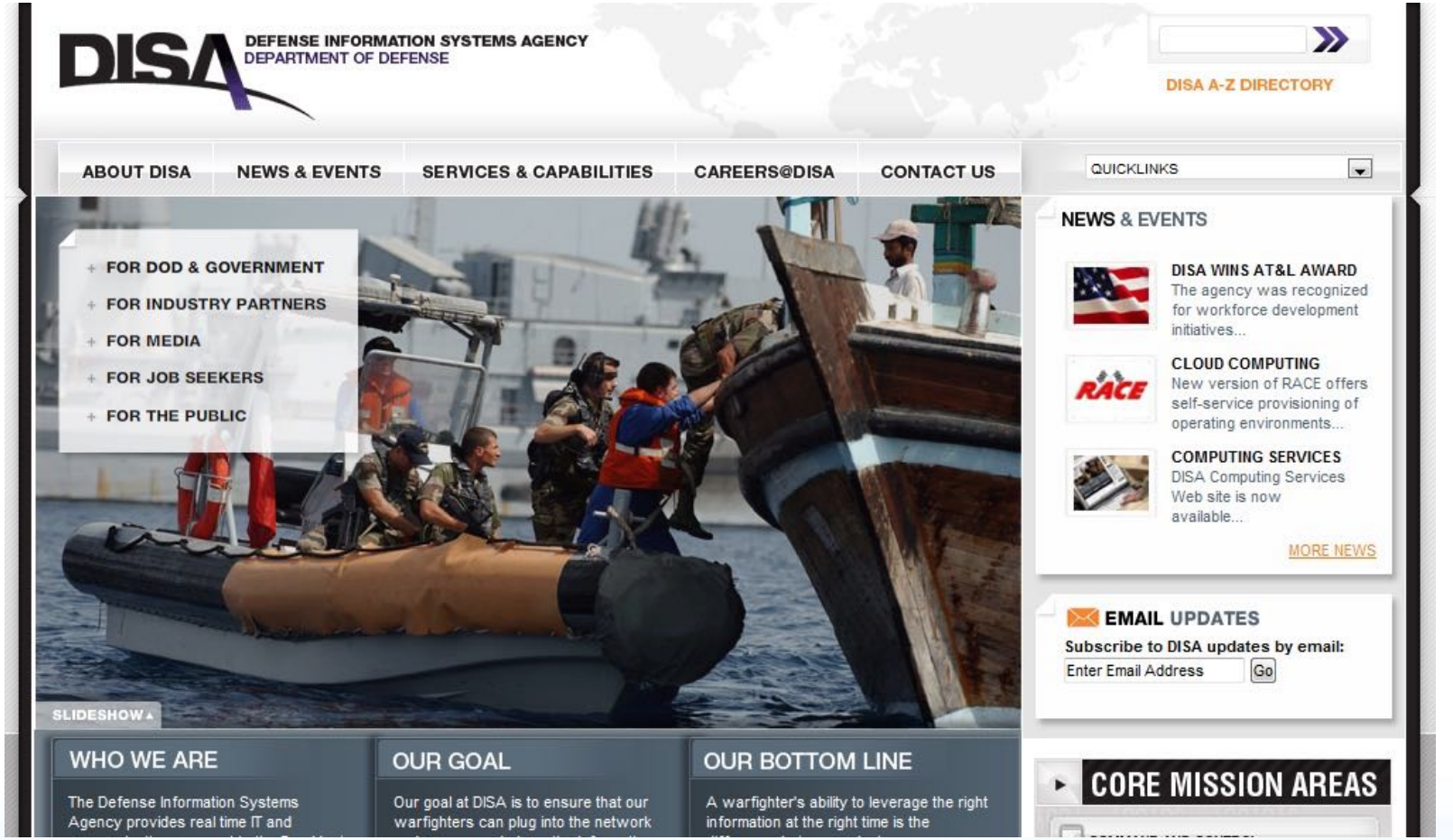
Technical Countermeasures in IATF v3.1

Defense-In-Depth	Security Mechanism	Security Services
Defending the Network & Infrastructure	Redundant & Diverse Comm. Links	Availability
	Encryptors	Confidentiality, Integrity
	Routers	Access Control
Defending the Enclave Boundary	Firewalls	Access Control, Integrity
	Multi-Service & Layer 2 Switches	Access Control
Defending the Computing Environment	Network-based & Host-based IDS's	Integrity
	Hardened OS	Access Control, Integrity
	Anti-Virus Software	Access Control, Integrity
Supporting the Infrastructure	PKI (X.509-based Messaging: DMS)	Confidentiality: Access Control, Identification, Authentication, Integrity, Non-Repudiation

Security Services Spectrum:

- Access Control
- Confidentiality
- Integrity
- Availability
- Non-Repudiation

DISA (http://www.disa.mil)



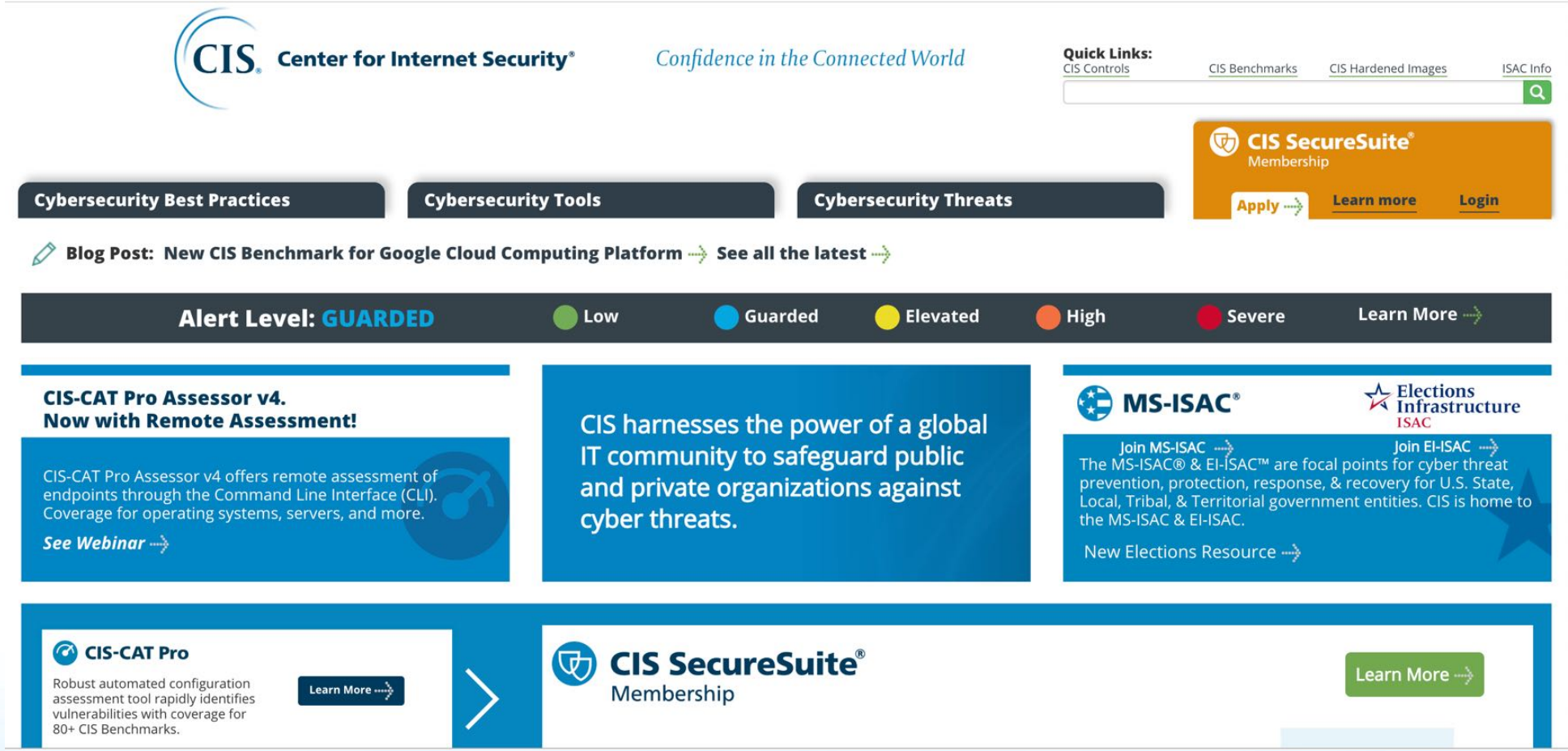
DISA STIGS

- Security Checklists
- Security Readiness Review Evaluation Scripts
- Security Technical Implementation Guides

http://iase.disa.mil/stigs/

NSA (http://www.nsa.gov)

Center for Internet Security (http://www.cisecurity.org)



Microsoft Windows Security

Microsoft Windows Security

Attack	Windows 10 protection
Extraction of domain accounts NTLM hashes	Credential Guard
Extraction of local accounts NTLM hashes	**Still possible**
Extraction of clear-text domain passwords for running sessions	Windows 8.1 removed clear-text
Extraction of clear-text local passwords	Windows 8.1 removed clear-text
Extraction of secrets through DMA	Credential Guard (VT-d / IOMMU)
Pass-the-Hash on domain accounts	Credential Guard
Overpass-the-hash	Credential Guard
Pass-the-ticket (TGS)	**Still possible**
Bootkit	Secure Boot (UEFI)
Rootkit loaded before anti-malware solution	ELAM[1] and Device Guard
Malware and unauthorized applications	Device Guard (or AppLocker)
Tampering with whitelisting solution	Device Guard
Tampering with whitelisting ruleset	Device Guard signed ruleset

https://www.kudelskisecurity.com/sites/default/files/files/Kudelski_Security_Publication_Win10_security_EN.pdf

Other Security Guidelines

- DISA STIGs
- NSA IA Guidance
- The CIS Benchmarks

Member Server Baseline

- Modify and apply the Member Server Baseline security template to all member servers

- Settings in Member Server Baseline security template
  - Audit Policy
  - User Rights Assignment
  - Security Options
  - Event Log
  - System Services

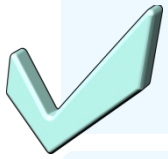
Template Deployment

- Test before deployment

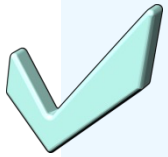
- Periodic analysis
  - Security Configuration and Analysis snap-in
  - Scripting (Secedit.exe)

- Deployment Methods
  - Group Policy (Active Directory)
  - Security Configuration and Analysis snap-in
  - Scripting (Secedit.exe)

Best Practices for Using Security Templates



Review and modify security templates before using them



Use security configuration and analysis tools to review and modify template settings before applying them

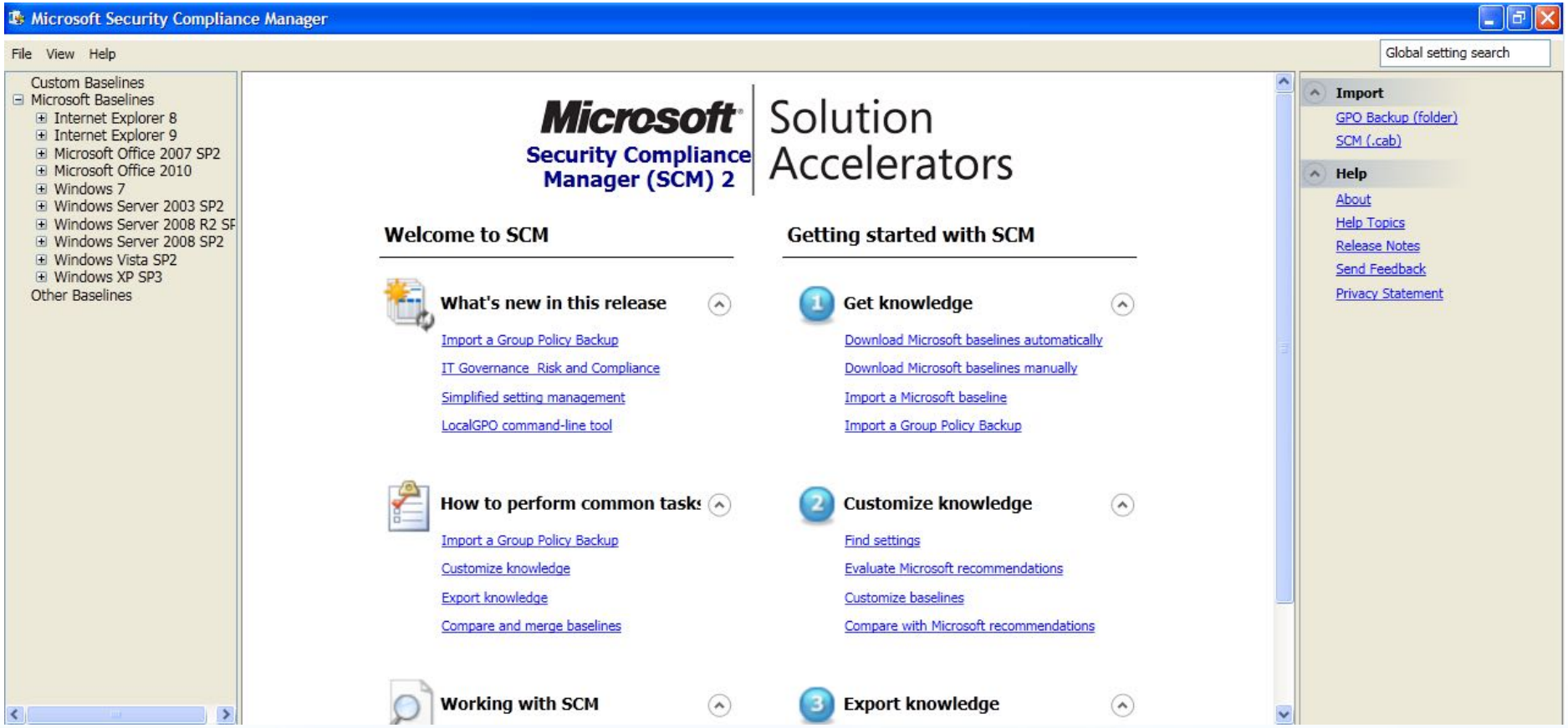
Test templates thoroughly before deploying them

Store security templates in a secure location

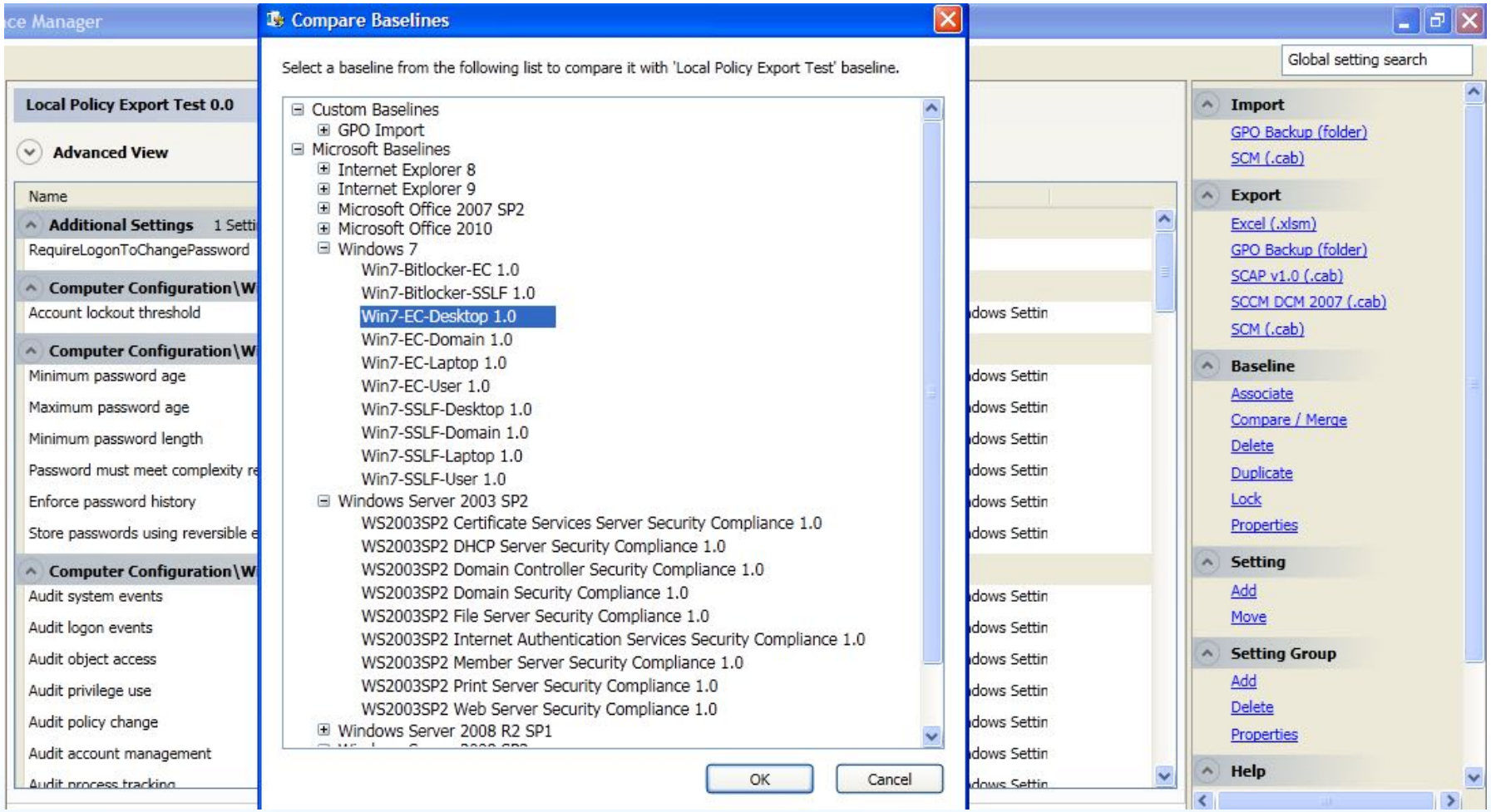
Security Compliance Manager

- Centralized Management and Baseline Portfolio
- Baseline Customization
- Baseline Comparison and Export
- Baseline Compliance Monitoring and Verification

Security Compliance Manager



Baseline in SCM



Security Configuration Guidance

- *Microsoft, the Center for Internet Security (CIS), the National Security Agency (NSA), the Defense Information Systems Agency (DISA), and the National Institute of Standards and Technology (NIST) have published "security configuration guidance" for Microsoft Windows.*
- *The high security levels that are specified in some of these guides may significantly restrict functionality of a system. Therefore, you should perform significant testing before you deploy these recommendations.*
- Please see http://support.microsoft.com/default.aspx?scid=kb;en-us;885409 for details.

Hardening Guides (Security Guide)

- Operating System Hardening
  - Windows Server Security Guide
    - Includes info for web server hardening
- Mail Server Hardening
  - Microsoft Exchange Server Security Hardening Guide
- Database Hardening
  - SQL Server Security Features and Best Practices

Hardening Server Roles

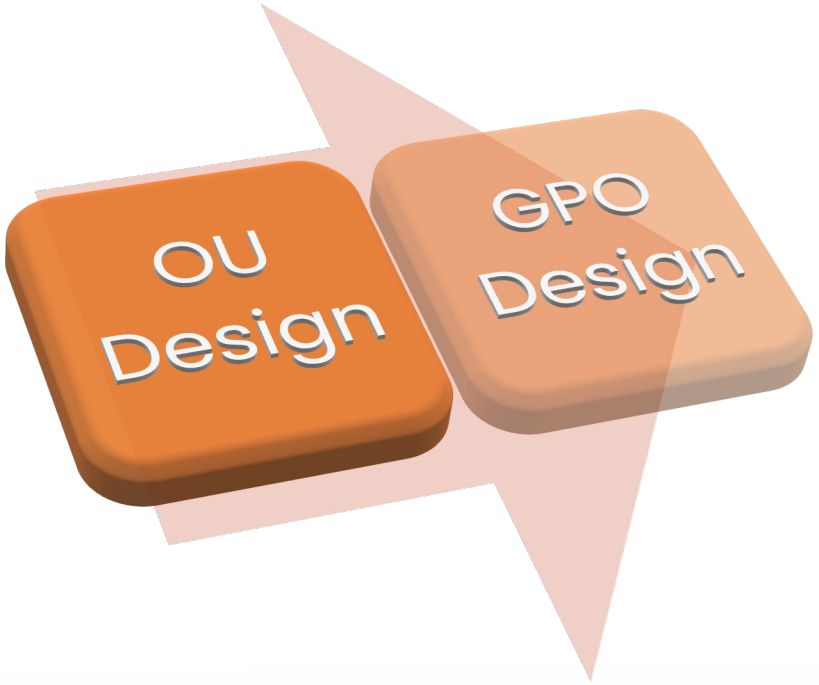
- Hardening guidance is provided for a group of distinct server roles.
- The countermeasures described and the tools provided assume that each server will have a single role; if you need to combine roles for some of the servers in your environment then you can customize the security templates so that an appropriate combination of services and security options are configured for servers with multiple roles.

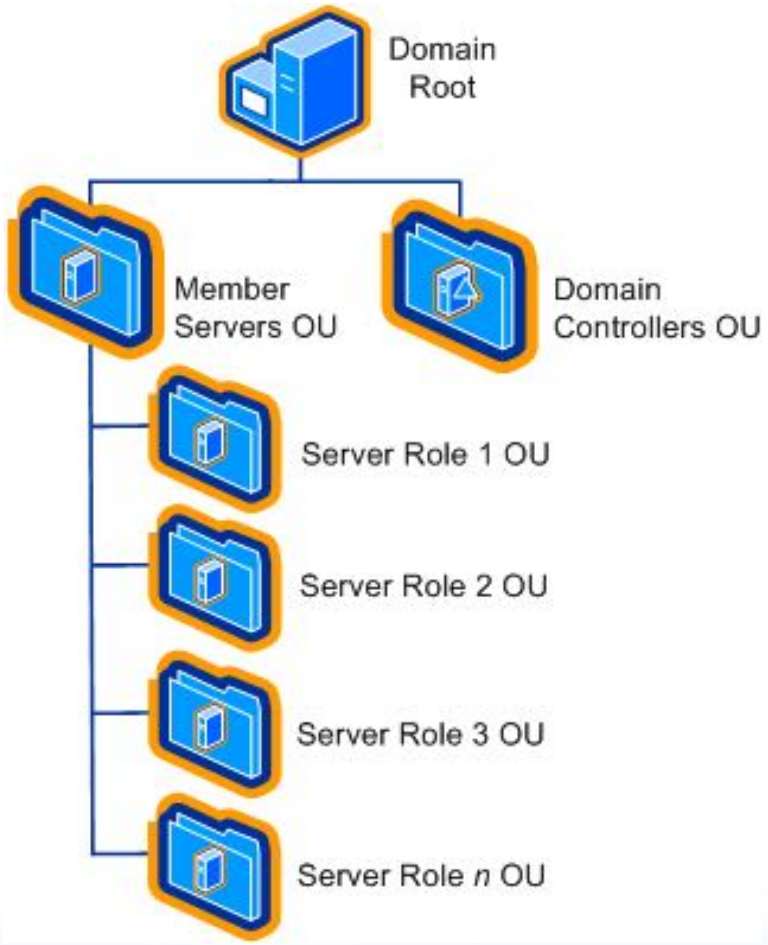
- Roles covered by the Windows Server Security Guide include:
    - Domain controllers
    - Infrastructure servers
    - File servers
    - Print servers
    - Internet Information Services (IIS) servers
    - Internet Authentication Services (IAS) servers
    - Certificate Services servers
    - Bastion hosts

Using Active Directory to Implement Security

- Design OU structure with client security in mind
- Design OU hierarchy to separate user and computer objects based on role
- Apply Group Policy with appropriate security settings for each computer role

Security Design





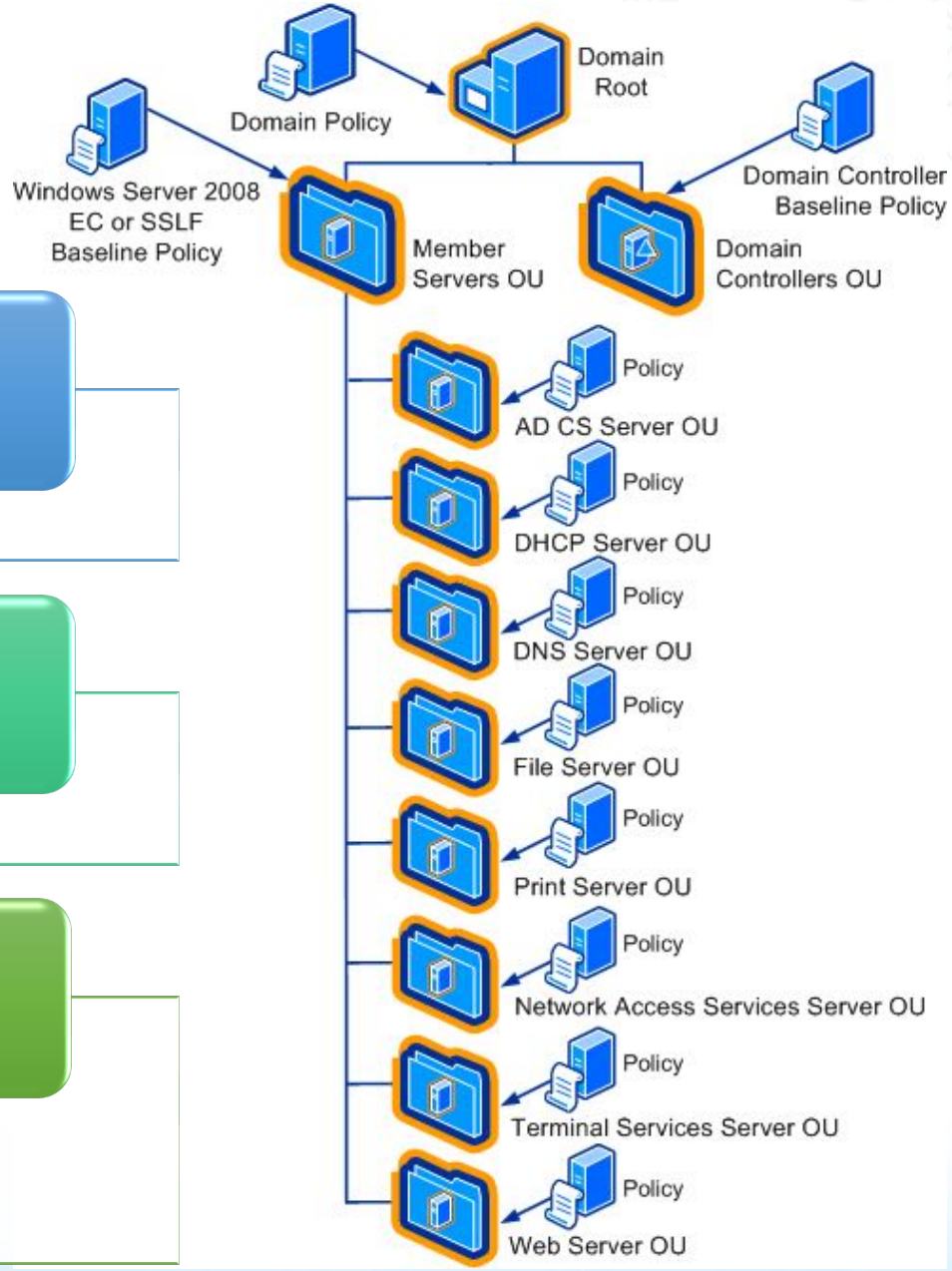
Example: OU Structure

Domain Root

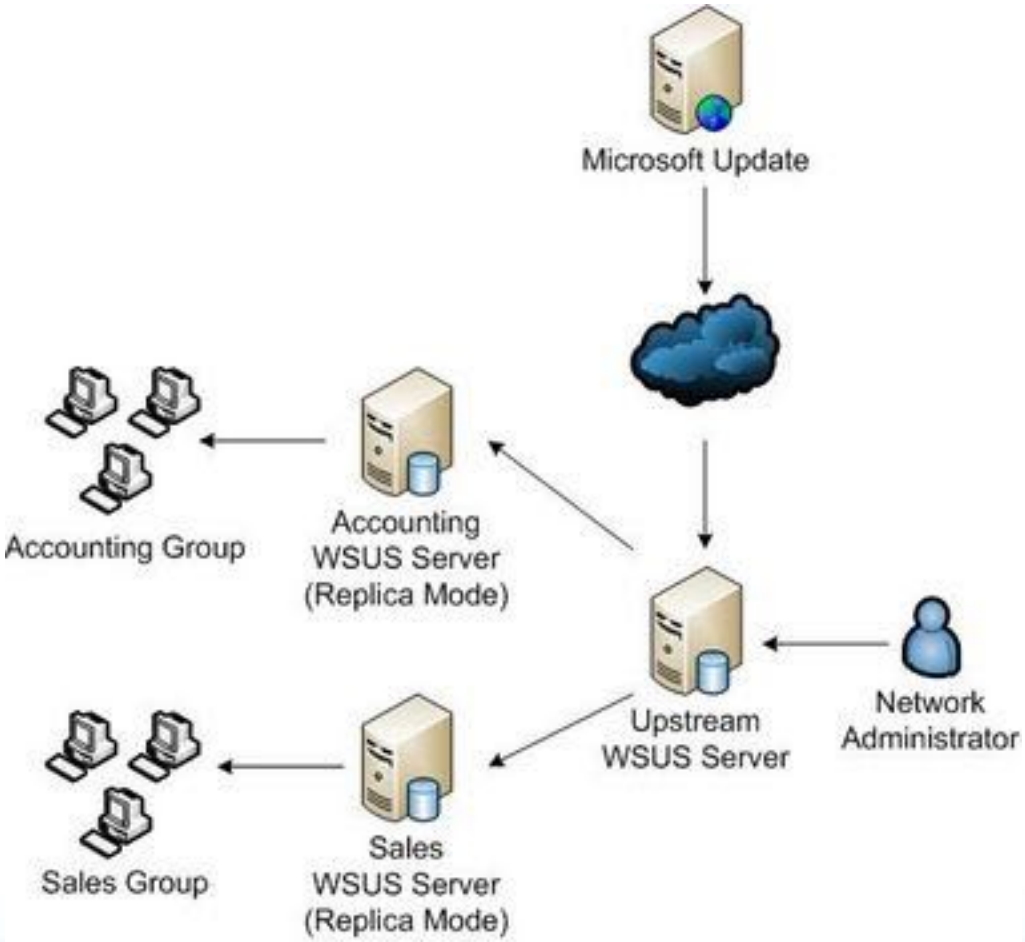
Domain Controllers OU

Member Servers OU

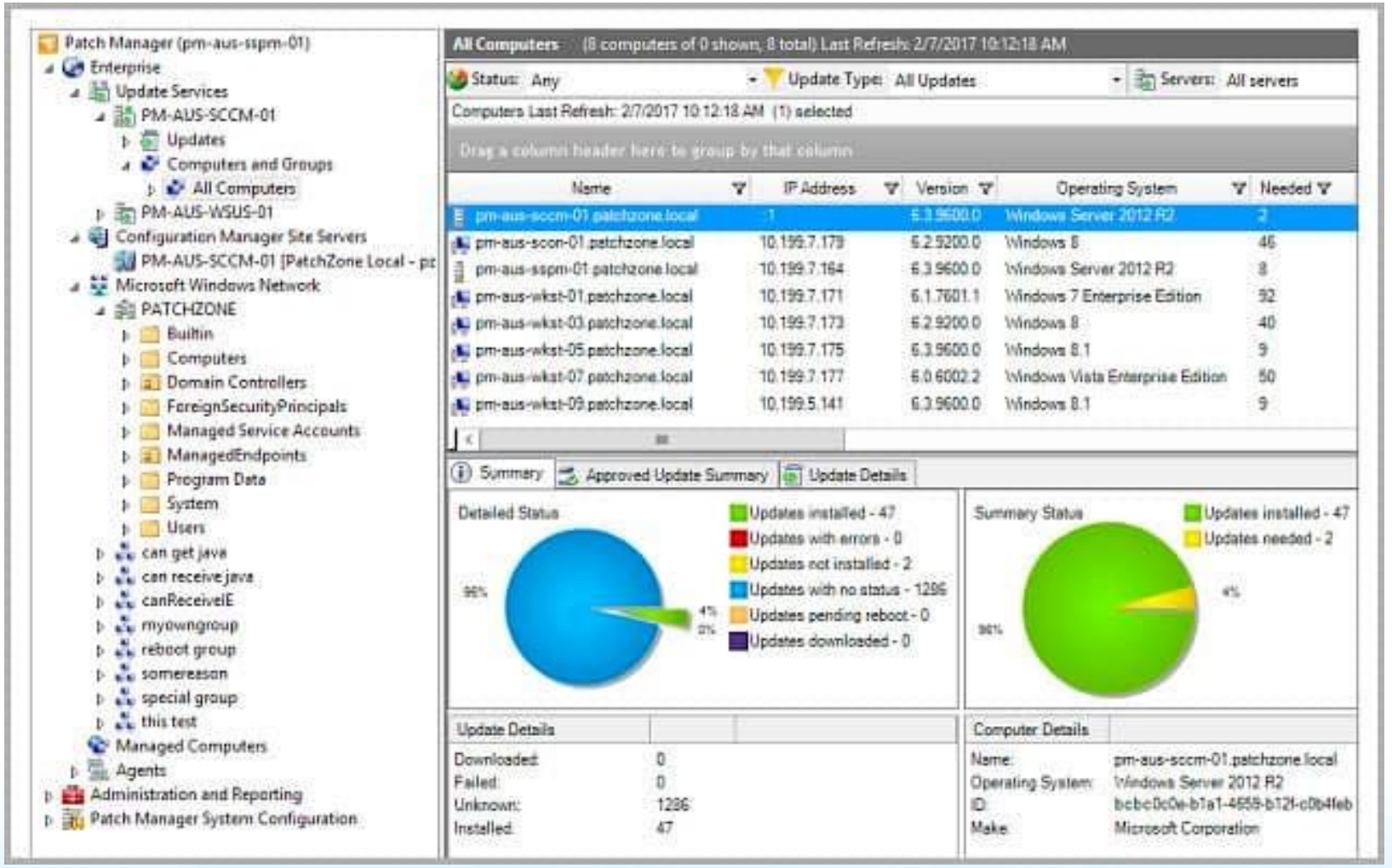
- **Server Role OUs**



Microsoft Windows Update Service (WSUS)



Microsoft Windows Update Service (WSUS)



Microsoft Windows Security Best Practice

Microsoft Windows Security Best Practice

Remediation:

To establish the recommended configuration via GP, set the following UI path to `1 or more day(s)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password age
```

Impact:

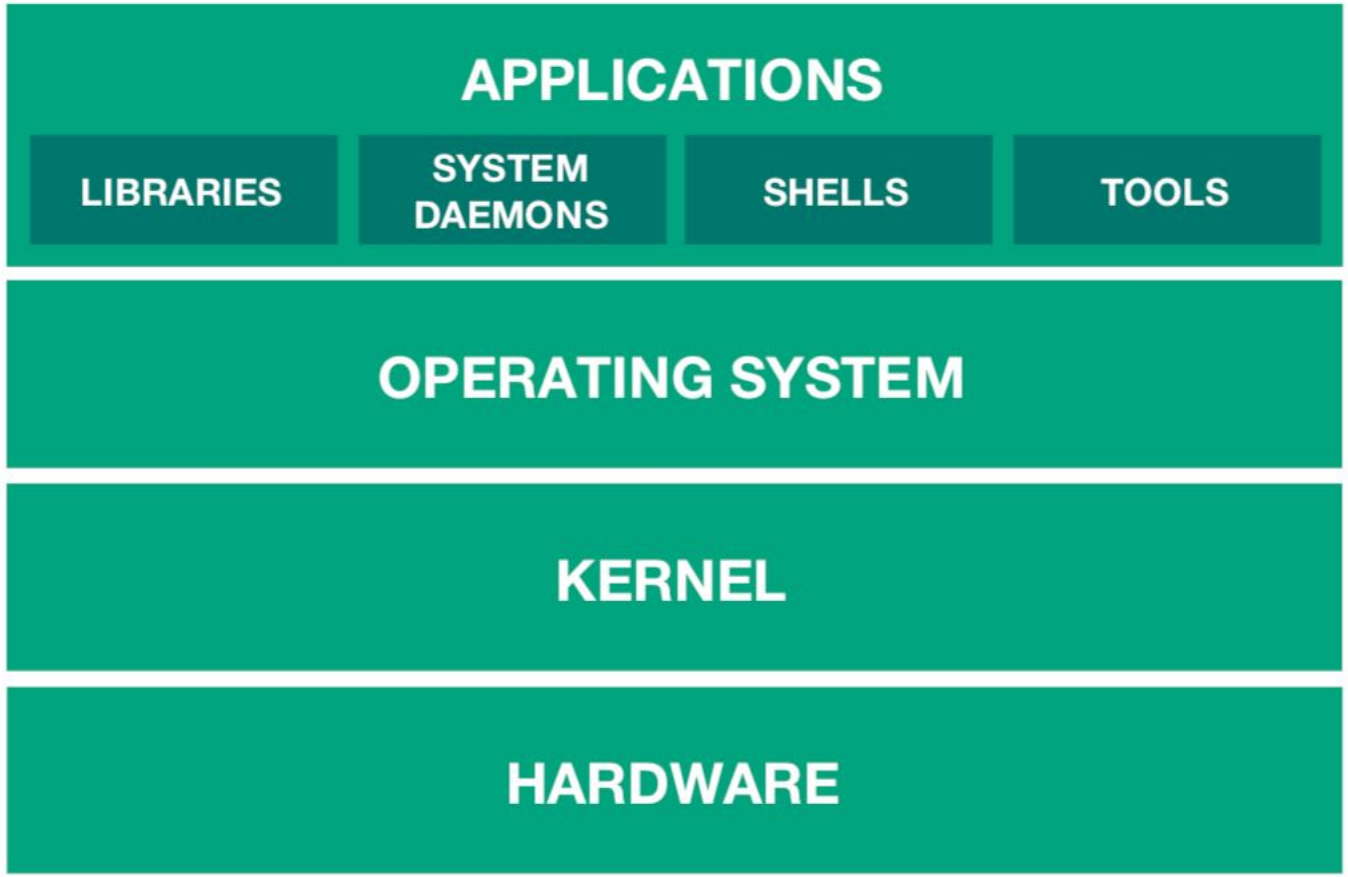
If an administrator sets a password for a user but wants that user to change the password when the user first logs on, the administrator must select the User must change password at next logon check box, or the user will not be able to change the password until the next day.

Default Value:

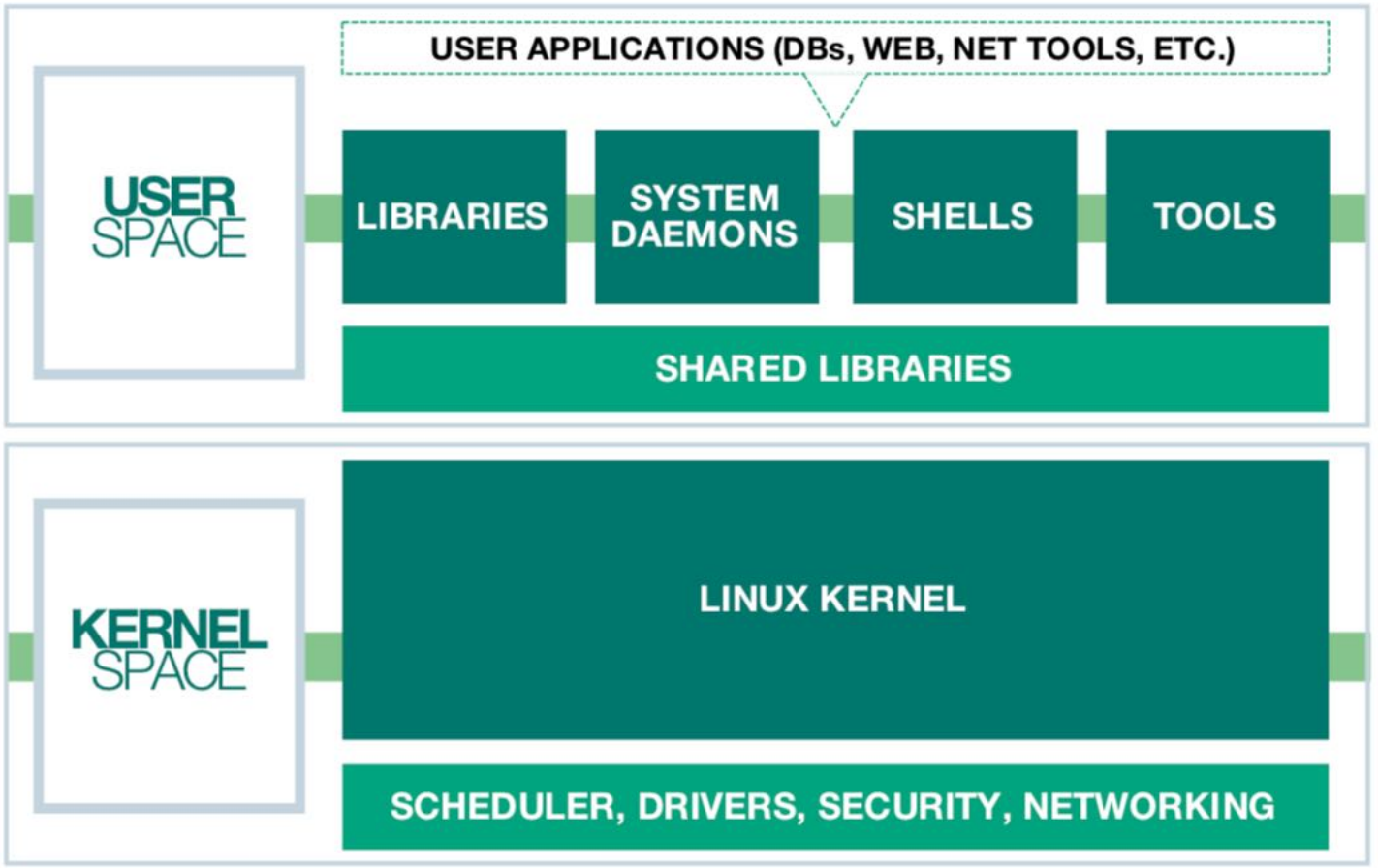
0 days

Linux security

Operating system structure



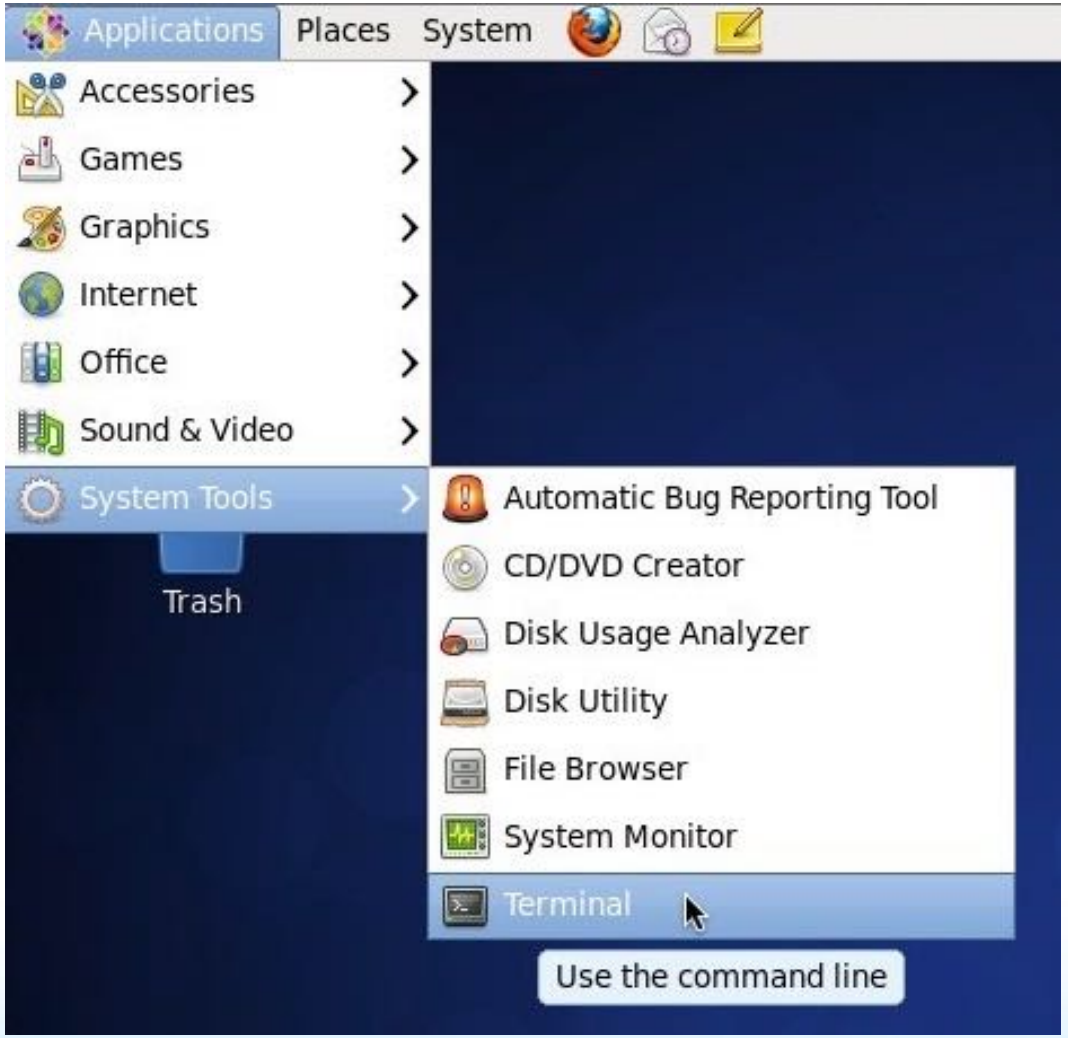
Kernel Space and User Space



Shell

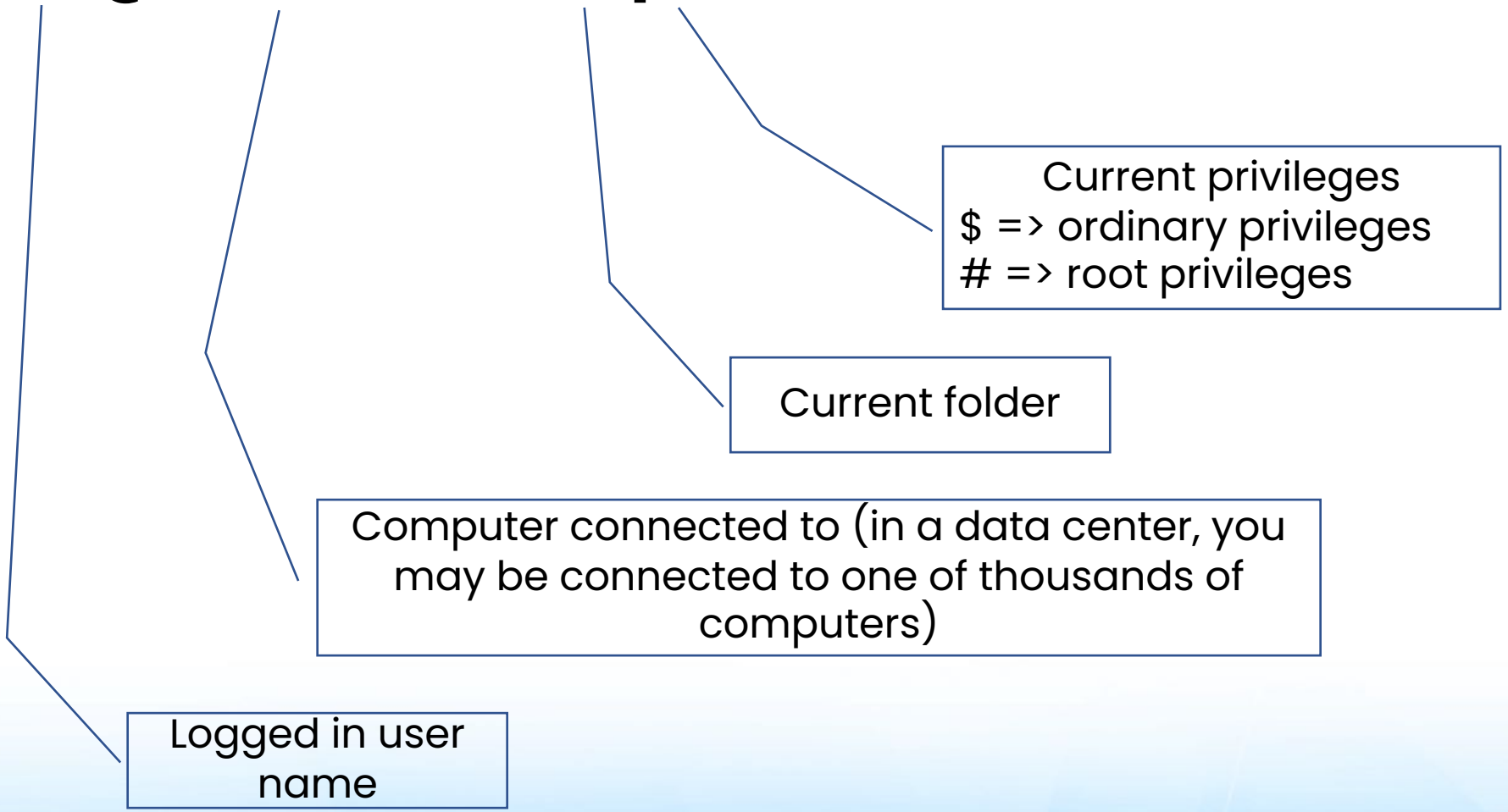
- Primary interface for system administrators
  - Direct access to OS structures
    - In plain English
  - Low network bandwidth needs
  - Scripting (automation) capabilities
- Windows
  - PowerShell runs as a separate program
    - Relatively new introduction to the OS (Windows 7, Server 2008)
- Unix
  - Ready on OS start-up
  - Easily accessible from Windows
  - Focus of course

Bash prompt



Bash prompt information

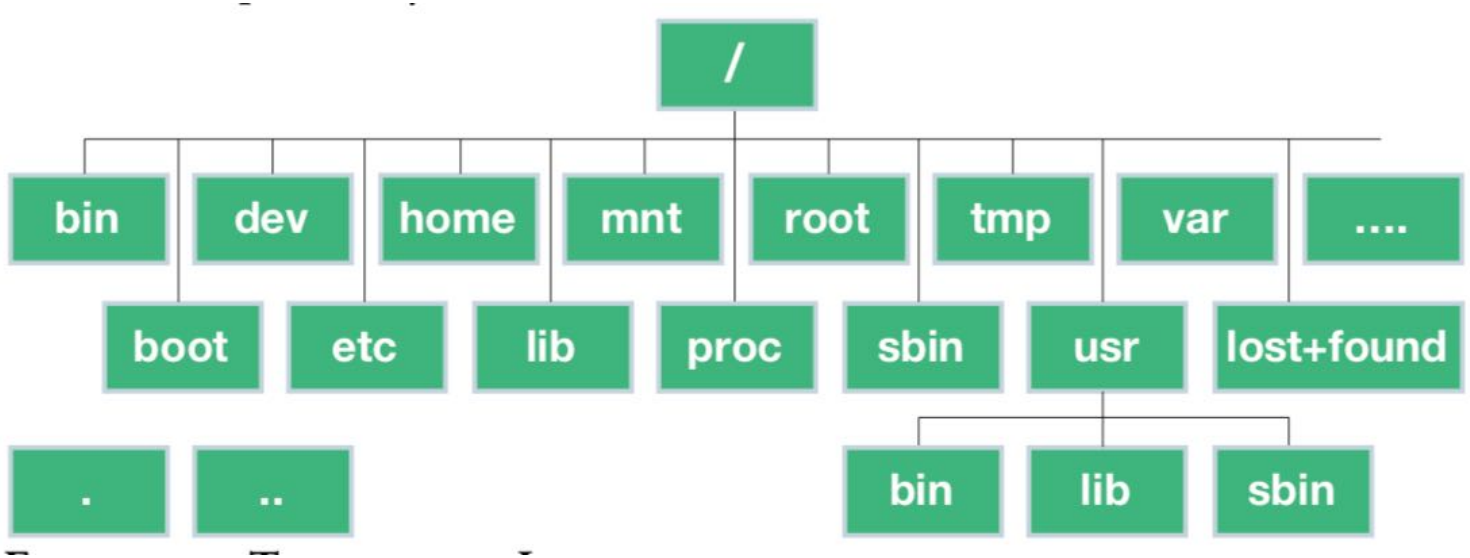
- [alice@sunshine usr]$



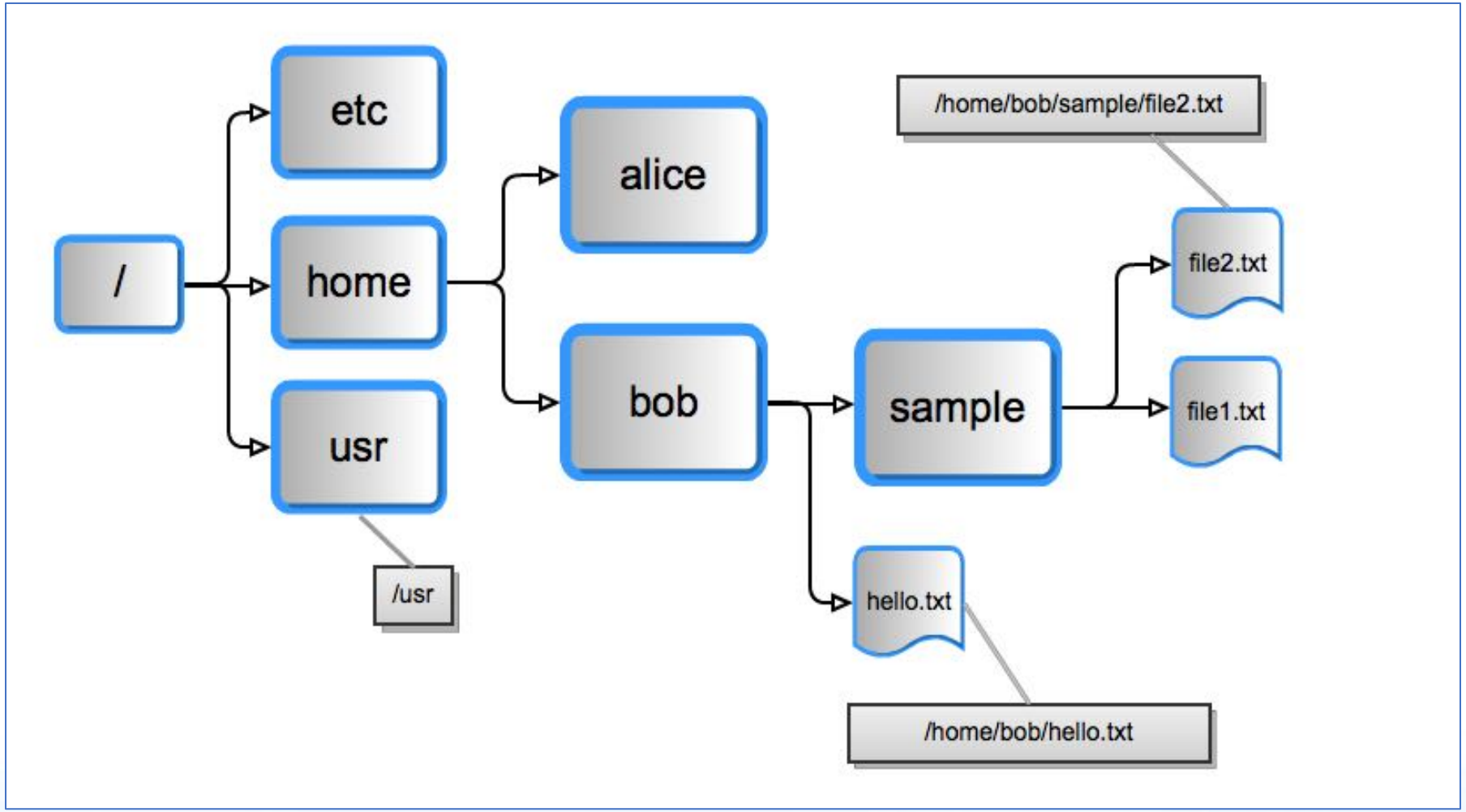
Common operations

- File navigation
- File management
- File content viewing and editing
- Search
- Access control
- User management
- Access control lists
- File permissions
- Software installation and updates

Linux File Directory



File system navigation



File system navigation

- Filesystem root
  - Top of the file hierarchy
  - Represented as a single slash
    - /

- Path
  - Location of a file or directory in the hierarchy
  - Representation
    - Two ways
      - Absolute
      - Relative

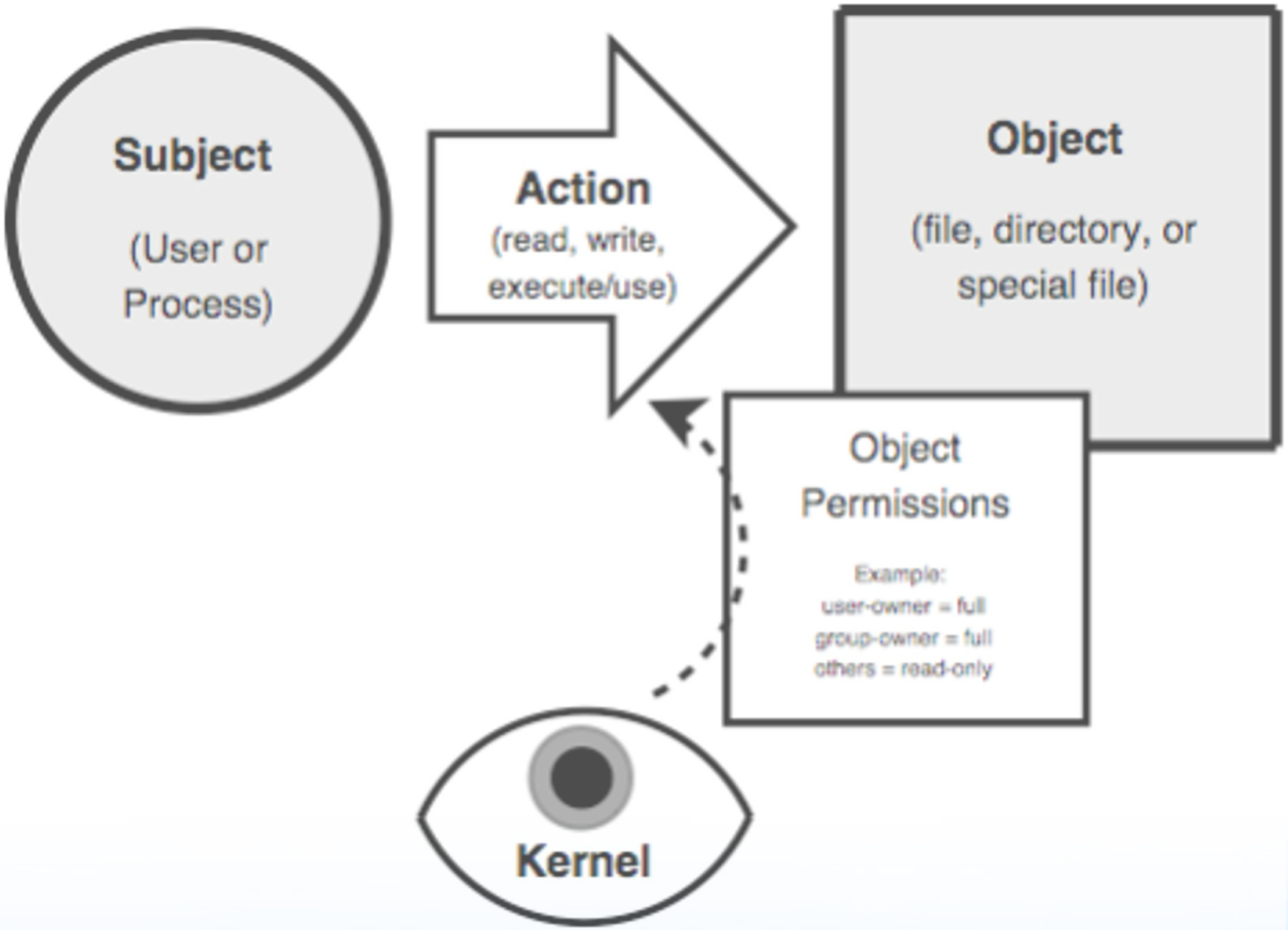
Linux Security

- Linux has evolved into one of the most popular and versatile operating systems
- many features mean broad attack surface
- can create highly secure Linux systems
- will review:
  - Discretionary Access Controls
  - typical vulnerabilities and exploits in Linux
  - best practices for mitigating those threats
  - new improvements to Linux security model

Linux Security Model

- Linux's traditional security model is:
  - people or proceses with "root" privileges can do anything
  - other accounts can do much less
- hence attacker's want to get root privileges
- can run robust, secure Linux systems
- crux of problem is use of **Discretionary Access Controls** (DAC)

Linux Security Transactions



File System Security

- in Linux *everything* as a file
  - e.g. memory, device-drivers, named pipes, and other system resources
  - hence why filesystem security is so important

- I/O to devices is via a “special” file
  - e.g. `/dev/cdrom`

- have other special files like named pipes
  - a conduit between processes / programs

Users and Groups

- Only two things aren't files on UNIX systems:
- a user-account (user)
  - represents someone capable of using files
  - associated both with humans and processes
- a group-account (group)
  - is a list of user-accounts
  - users have a main group
  - may also belong to other groups

Users and Groups

- user's details are kept in `/etc/passwd`

```
maestro:x:200:100:Maestro Edward
  Hizzersands:/home/maestro:/bin/bash
```

- additional group details in `/etc/group`

```
conductors:x:100:

pianists:x:102:maestro,volodya
```

- To manage and modify group memberships, use **useradd**, **usermod**, **userdel**

File Permissions

- files have two owners: a user & a group
- each with its own set of permissions
- with a third set of permissions for other
- permissions are to read/write/execute in order user/group/other, cf.

```
-rw-rw-r--  1  maestro user 35414 Mar 25 01:38
 baton.txt
```

- set using chmod command

Directory Permissions

- read = list contents
- write = create or delete files in directory
- execute = use anything in or change working directory to this directory
- e.g.

```
$ chmod g+rx extreme_casseroles
$ ls -l extreme_casseroles
 drwxr-x--- 8 biff  drummers 288  Mar 25 01:38
 extreme_casseroles
```

Sticky Bit

- originally used to lock file in memory
- now used on directories to limit the ability to delete
  - if set must own file or dir to delete
  - other users cannot delete even if have write
- set using chmod command with +t flag, e.g.

```
chmod +t extreme_casseroles
```

- directory listing includes t or T flag

```
drwxrwx--T  8  biff  drummers  288  Mar 25 01:38
  extreme_casseroles
```

- only apply to specific directory not child dirs

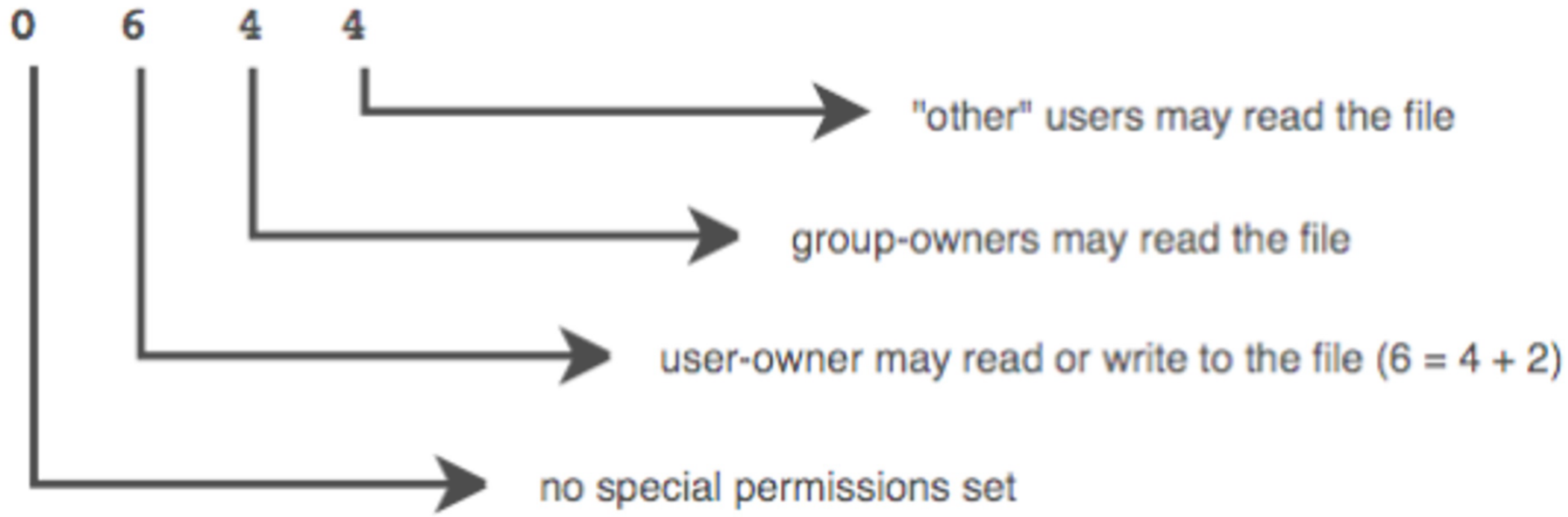
SetUID and SetGID

- setuid bit means program "runs as" owner
  - no matter who executes it
- setgid bit means run as a member of the group which owns it
  - again regardless of who executes it
- "run as" = "run with same privileges as”
- *These are are very dangerous* if set on file owned by root or other privileged account or group
  - only used on executable files, not shell scripts

SetGID and Directories

- setuid has no effect on directories
- setgid does: causes any file created in a directory to inherit the directory's group
- useful if users belong to other groups and routinely create files to be shared with other members of those groups
  - instead of manually changing its group

Numeric File Permissions



Kernel vs User Space

- Kernel space
  - refers to memory used by the Linux kernel and its loadable modules (e.g., device drivers)
- User space
  - refers to memory used by all other processes
- since kernel enforces Linux DAC and security, it is critical to isolate kernel from user
  - so kernel space never swapped to disk
  - only root may load and unload kernel modules

setuid root Vulnerabilities

- a **setuid root** program runs as root
  - *no matter who executes it*
- used to provide unprivileged users with access to privileged resources
- must be very carefully programmed
- if can be exploited due to a software bug
  - may allow otherwise-unprivileged users to use it to wield unauthorized root privileges
- distributions now minimise setuid-root programs
- system attackers still scan for them!

Web Vulnerabilities

- a very broad category of vulnerabilities
  - because of ubiquity of world wide web have big and visible attack surfaces
- when written in scripting languages
  - not as prone to classic buffer overflows
  - can suffer from poor input-handling
- few “enabled-by-default” web applications
- but users install vulnerable web applications
- or write custom web applications having easily-identified and easily-exploited flaws

Rootkits

- allow attacker to cover their tracks
- if successfully installed before detection, all is very nearly lost
- originally collections of hacked commands, like ls, etc., but would hide attacker's files, directories, processes
- now use loadable kernel modules
  - intercepting system calls in kernel-space
  - hiding attacker from standard commands
- may be able to detect with chkrootkit
- generally have to wipe and rebuild system

Linux System Hardening

- It is worth considering how to mitigate Linux security risks at system and application levels

- Note that a general theme will be “only use what you need to”. Linux has a LONG history of insecure applications, so (as always) half the battle is keeping things updated.

OS Installation

- security begins with O/S installation
- especially what software is run
  - since unused applications liable to be left in default, un-hardened and un-patched state
- generally should not run:
  - X Window system, RPC services, R-services, inetd, SMTP daemons, telnet etc
- also have some initial system s/w configuration:
  - setting root password
  - creating a non-root user account
  - setting an overall system security level
  - enabling a simple host-based firewall policy
  - enabling SELinux

Patch Management

- installed server applications must be:
  - configured securely
  - kept up to date with security patches
- patching can never win “patch rat-race”
- have tools to automatically download and install security updates
  - e.g. up2date, YaST, apt-get
  - note should not run automatic updates on change-controlled systems without testing

Network Access Controls

- As we've seen, the network is a key attack vector to secure
- TCP wrappers is a key tool to check access
  - originally tcpd inetd wrapper daemon
  - before allowing connection to service checks
    - if requesting host explicitly in hosts.allow is ok
    - if requesting host explicitly in hosts.deny is blocked
    - if not in either is ok
  - checks on service, source IP, username
  - now often part of app using libwrappers

Network Access Controls

- also have the very powerful **netfilter** Linux kernel native firewall mechanism
  - and **iptables** user-space front end
- as useful on firewalls, servers, desktops
- direct config tricky, steep learning curve
- do have automated rule generators
- typically for “personnal” firewall use will:
  - allow incoming requests to specified services
  - block all other inbound service requests
  - allow all outbound (locally-originating) requests
- if need greater security, manually config

Antivirus Software

- Historically, Linux not as vulnerable to viruses
  - more to lesser popularity than security, honestly
- Prompt patching is fairly effective for worms
- However, viruses abuse users privileges
  - non-root users have less scope to exploit, but can still consume resources
- Growing Linux popularity mean exploits
  - hence antivirus software will more important
  - various commercial and free Linux antivirus packages are available already: McAfee, Symantec, Sophos, ClamAV

User Management

- guiding principles in user-account security:
  - need care setting file / directory permissions
  - use groups to differentiate between roles
  - use extreme care in granting / using root privs
- commands: chmod, useradd/mod/del, groupadd/mod/del, passwd, chage
- info in files /etc/passwd & /etc/group
- manage user's group memberships
- set appropriate password ages: /etc/login.defs

Root Delegation

- have "root can to anything, users do little" issue
- "su" command allows users to run as root
  - either root shell or single command
  - must supply root password
  - means likely too many people know this
- SELinux RBAC can limit root authority, but is very complex
- "sudo" allows users to run as root
  - but only need their password, not root password
  - /etc/sudoers file specifies what commands allowed
- or configure user/group perms to allow, which can be tricky

Logging

- Effective logging is a key resource
- Linux logs using syslogd or Syslog-NG
  - receive log data from a variety of sources
  - sorts by **facility** (category) and **severity**
  - writes log messages to local/remote log files
- Syslog-NG preferable because it has:
  - variety of log-data sources / destinations
  - much more flexible “rules engine” to configure
  - can log via TCP which can be encrypted
- should check and customized defaults

Log Management

- balance number of log files used
  - size of few to finding info in many
- manage size of log files
  - must rotate log files and delete old copies
  - typically use logrotate utility run by cron
  - to manage both system and application logs
- must also configure application logging

Application Security

- This is a large topic: really depends on which particular application you wish to secure
- However, many security features are implemented in similar ways across different applications
- Some issues to consider:
  - running as unprivileged user/group
  - running in chroot jail
  - modularity
  - encryption
  - logging

Running As Unprivileged User/Group

- every process “runs as” some user
- extremely important this user is not root
  - since any bug can compromise entire system
- may need root privileges, e.g. bind a low port
  - have root parent perform privileged function
  - but main service from unprivileged child
- user/group used should be dedicated
  - easier to identify source of log messages

Running in chroot Jail

- chroot confines a process to a subset of /
  - maps a virtual “/” to some other directory
  - useful if have a daemon that should only access a portion of the file system, e.g. FTP
  - directories outside the chroot jail aren’t visible or reachable at all
- contains effects of compromised daemon
- complex to configure and troubleshoot
  - must mirror portions of system in chroot jail

Modularity

- applications running as a single, large, multipurpose process can be:
  - more difficult to run as an unprivileged user
  - harder to locate / fix security bugs in source
  - harder to disable unnecessary functionality

- hence modularity a highly prized feature
  - providing a much smaller attack surface

- cf. postfix vs sendmail, Apache modules

Encryption

- sending logins & passwords or application data over networks in clear text exposes them to network eavesdropping attacks (obvious)

- hence many network applications now support encryption to protect such data
  - often using OpenSSL library

- may need own X.509 certificates to use
  - can generate/sign using openssl command
  - may use commercial/own/free CA

Logging

- applications can usually be configured to log to any level of detail (debug to none)
- need appropriate setting
- must decide if use dedicated file or system logging facility (e.g. syslog)
  - central facility useful for consistent use
- must ensure any log files are rotated

Mandatory Access Controls

- Linux uses a DAC security model, but Mandatory Access Controls (MAC) impose a global security policy on all users
  - users may not set controls weaker than policy
  - normal admin done with accounts without authority to change the global security policy
  - but MAC systems have been hard to manage
- Novell's SuSE Linux has AppArmor
  - Restricts specific processes but leaves all else to DAC
- Fedora and RedHat Enterprise Linux has SELinux
  - Restricts network daemons, but all else to DAC
- Pure SELinux usually only used on high security machines

SELinux

- iNSA's powerful implementation of mandatory access controls for Linux
- Linux DACs still applies, but if it allows the action SELinux then evaluates it against its own security policies
- "subjects" are processes (since these run user cmds)
- Actions are "permissions”
- Objects are not just files & dirs, but also processes and systems resources
- To manage complexity SELinux has:
  - "that which is not expressly permitted, is denied”
  - groups of subjects, permissions, and objects

Security Contexts

- each individual subject & object in SELinux is governed by a **security context** being a:
  - user - individual user (human or daemon)
    - SELinux maintains its own list of users
    - user labels on subjects specify account's privileges
    - user labels on objects specify its owner
  - role - like a group, assumed by users
    - a user may only assume one role at a time,
    - may only switch roles if and when authorized to do so
  - domain (type) - a sandbox being a combination of subjects and objects that may interact with each other
- this model is called **Type Enforcement** (TE)

Decision Making in SELinux

- Two types of decisions:
- **access** decisions
  - when subjects do things to objects that already exist, or create new things in expected domain
- **transition** decisions
  - invocation of processes in different domains than the one in which the subject-process is running
  - creation of objects in different types (domains) than their parent directories
  - transitions must be authorized by SELinux policy

RBAC and MLS Controls

- SELinux also incorporates **Role Based Access Control** (RBAC)
  - rules specify **roles** a user may assume
  - other rules specify circumstances when a user may **transition** from one role to another

- and **Multi Level Security** (MLS), based on Bell-LaPadula model
  - concerns handling of classified data
    - “no read up, no write down”
  - MLS is enforced via file system labeling

40 Linux Server Hardening Security Tips

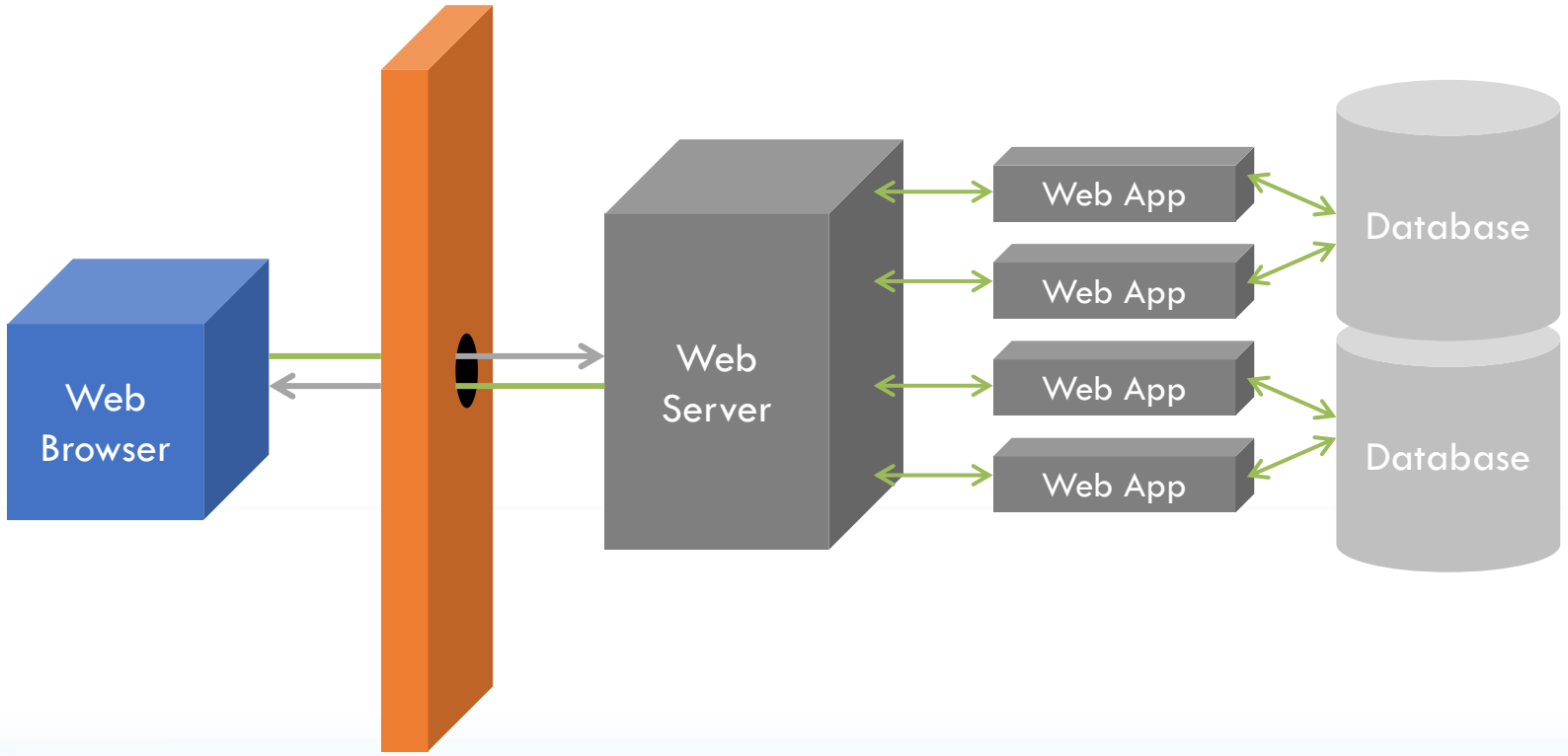
- https://www.cyberciti.biz/tips/linux-security.html

Linux Security Best Practice

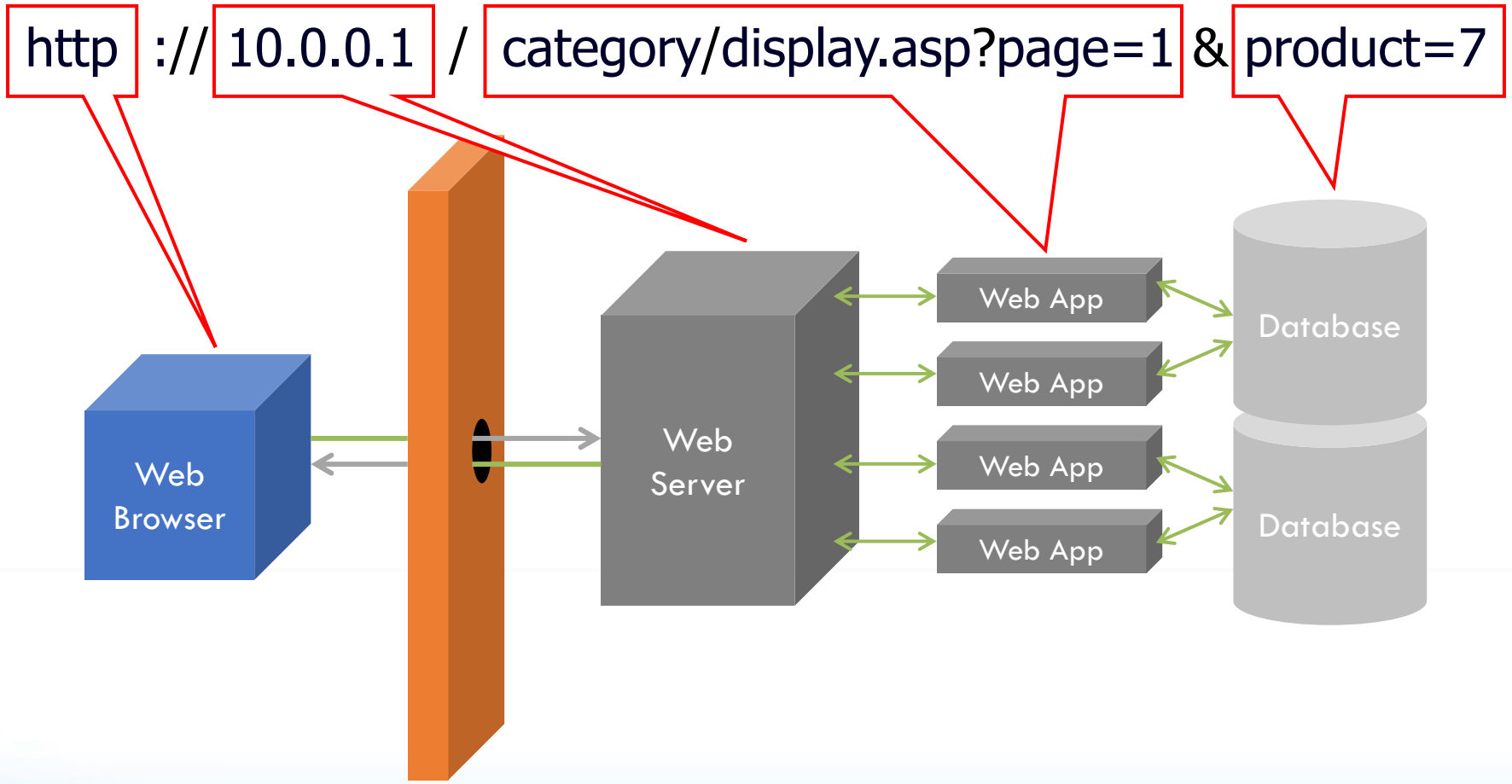
Linux Security Best Practice

Introduction to Web Application Security

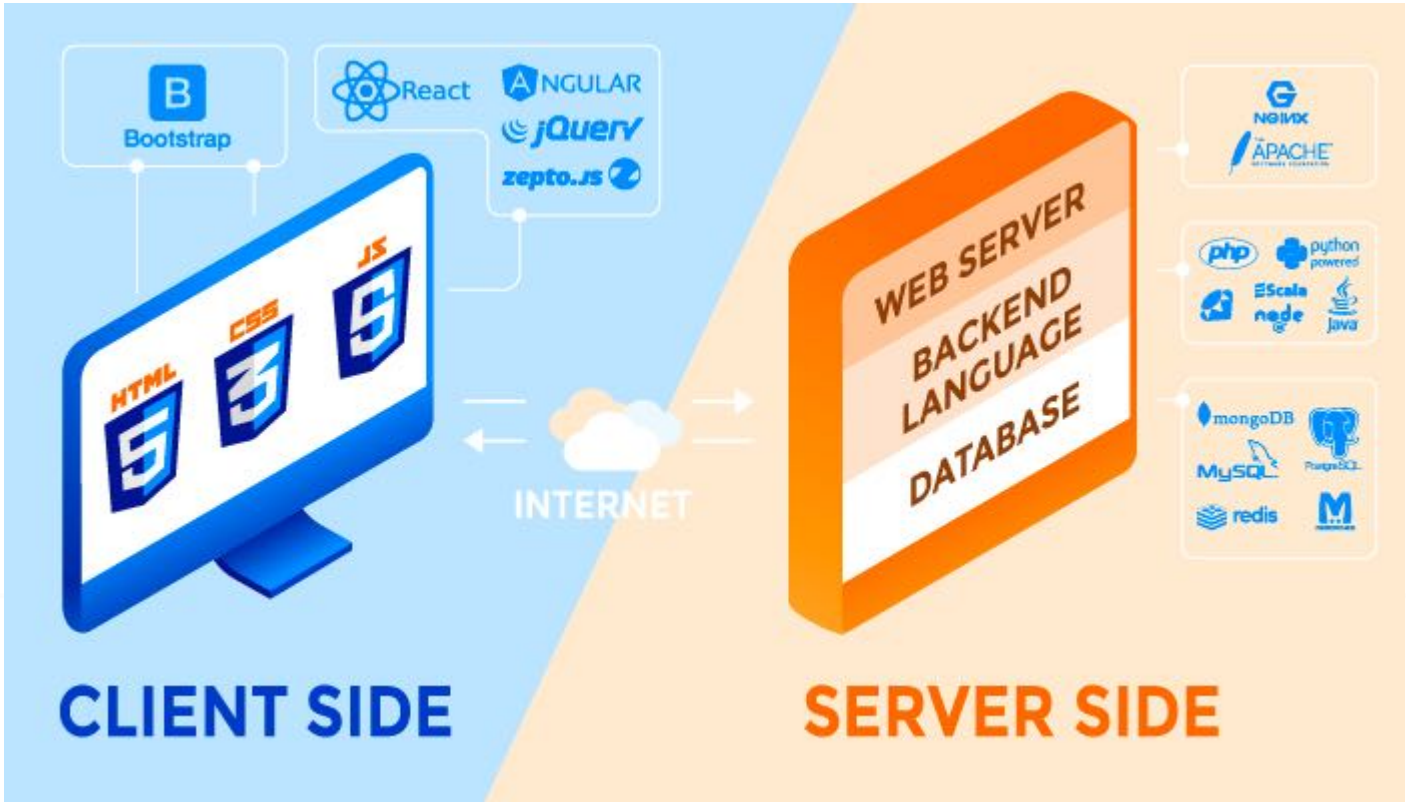
Enterprise Web Environments



Enterprise Web Environments

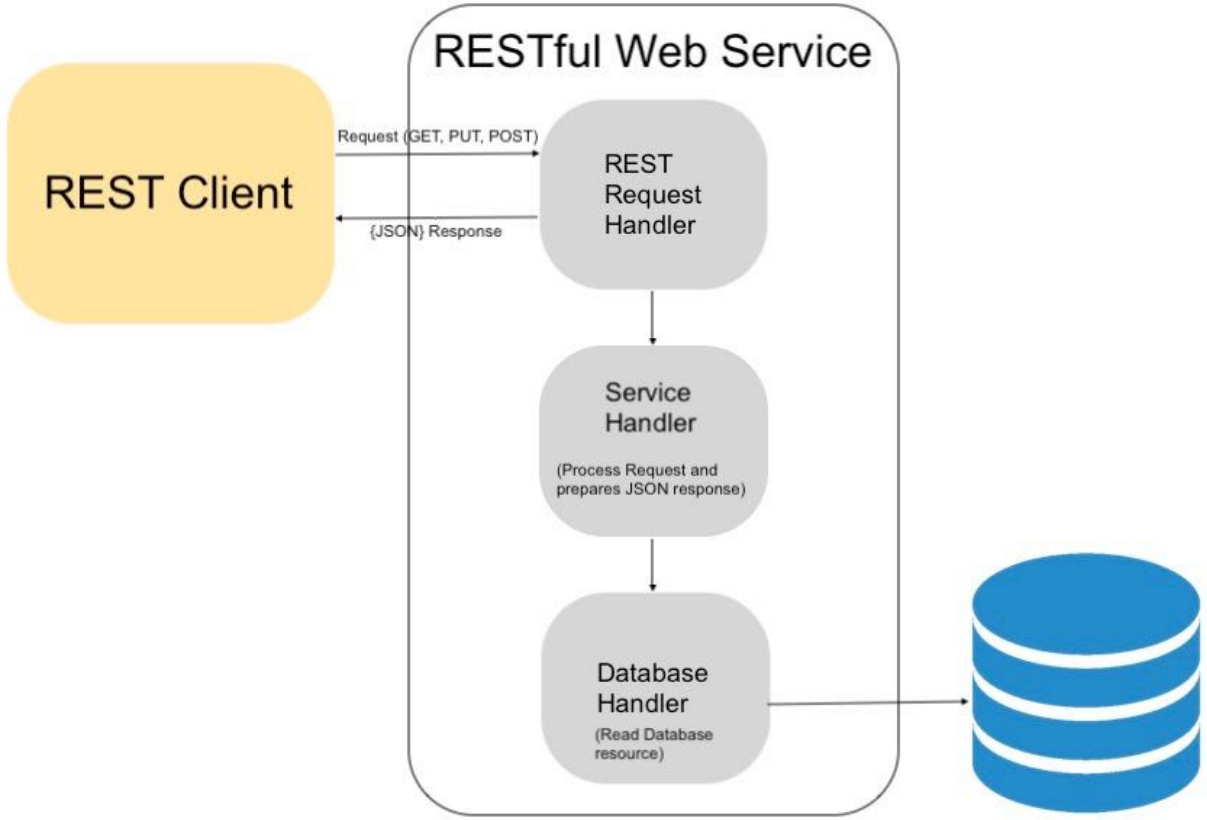


Overview Web Application Technology

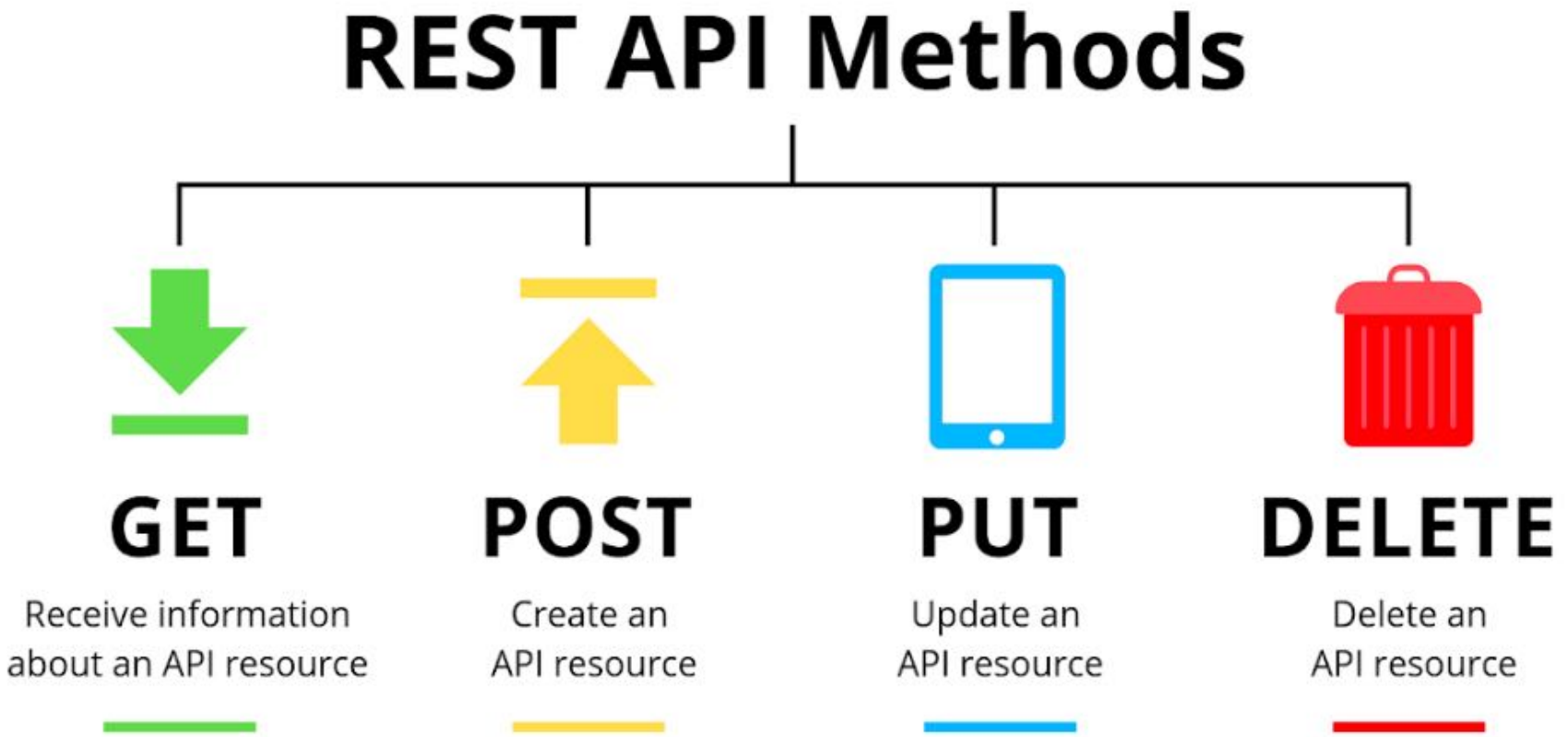


https://rubygarage.org/blog/technology-stack-for-web-development

Overview Web Application Technology

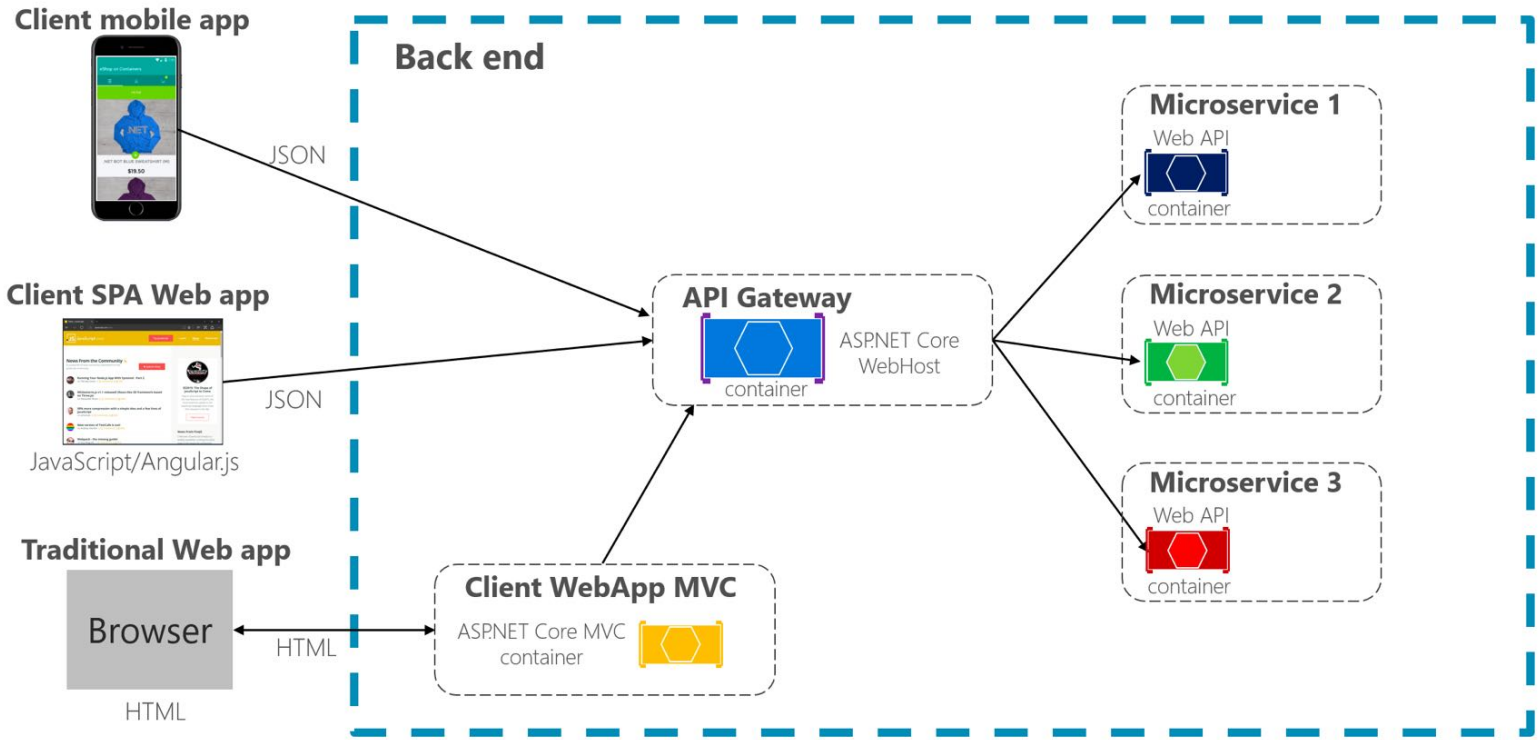


REST API Methods



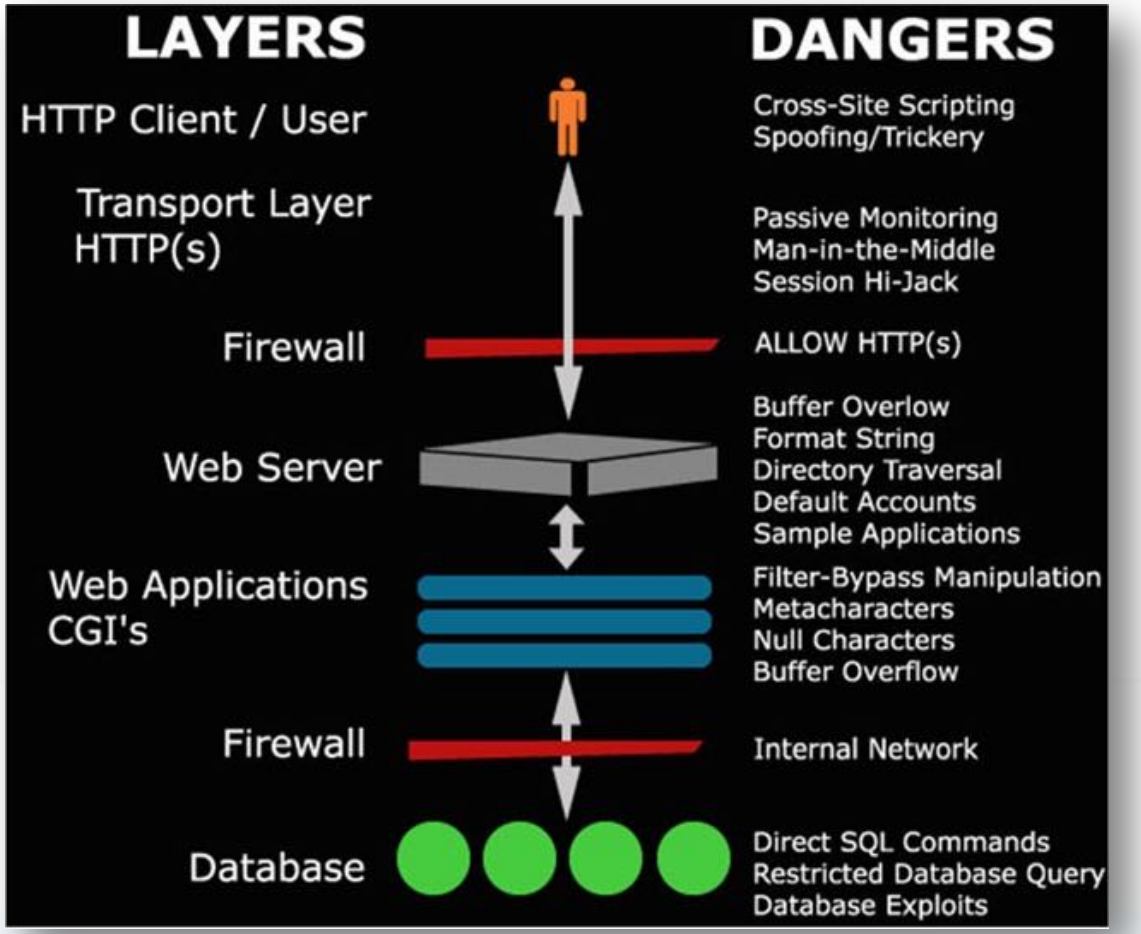
API Gateway

Using a single custom **API Gateway service**

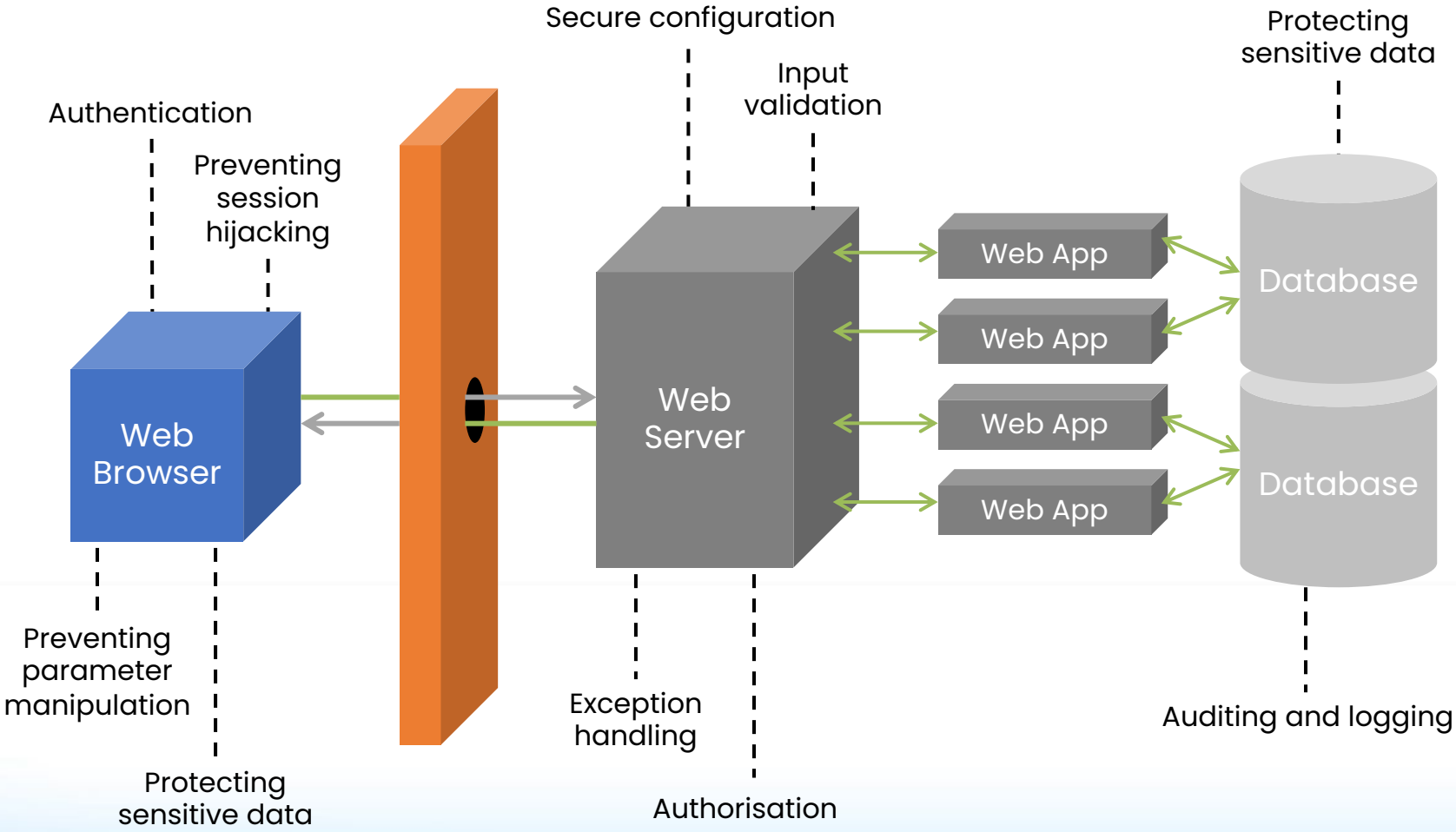


https://docs.microsoft.com/en-us/azure/architecture/microservices/design/gateway

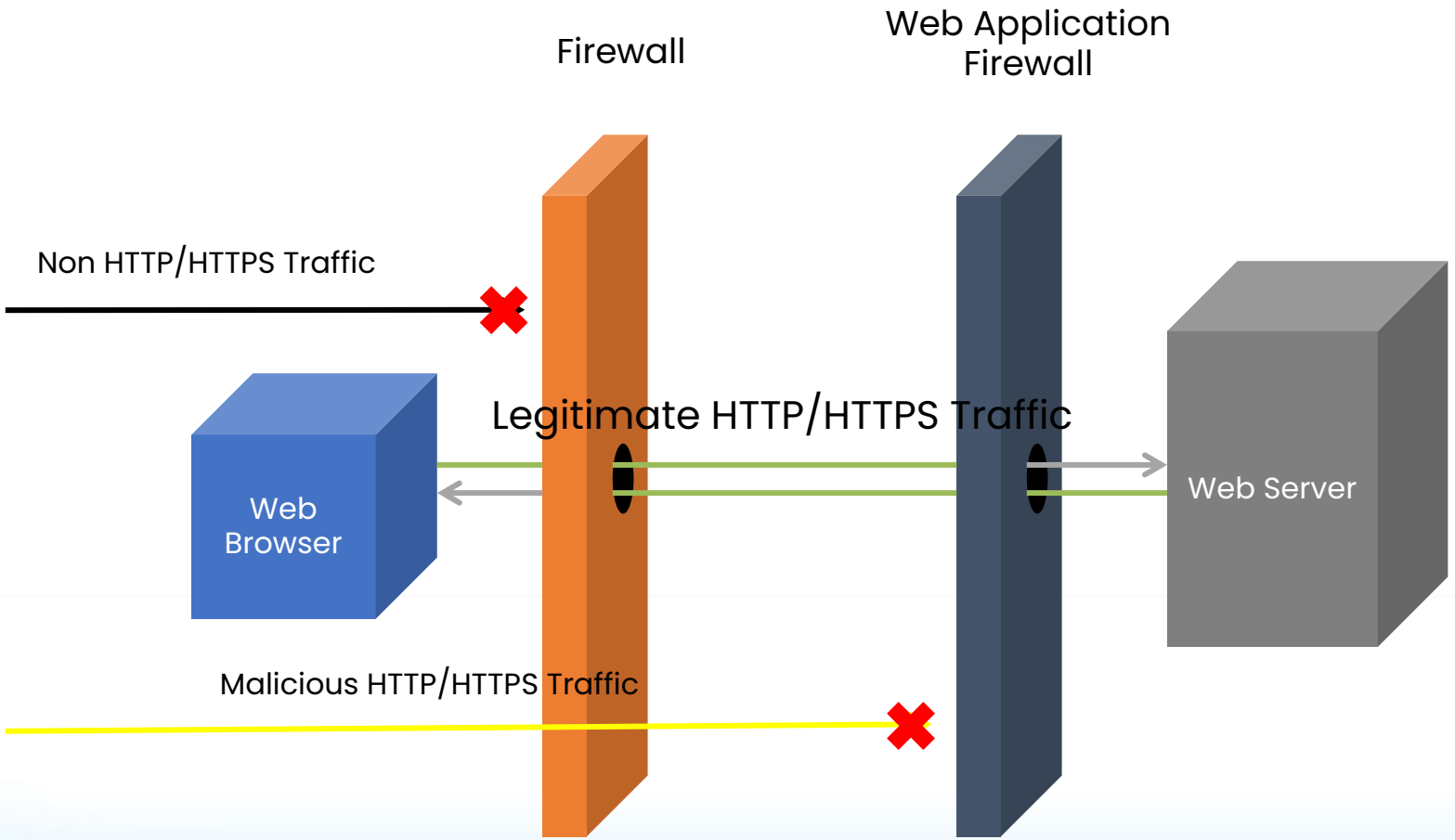
Web Application Security



Web Application Security



Web Application Security



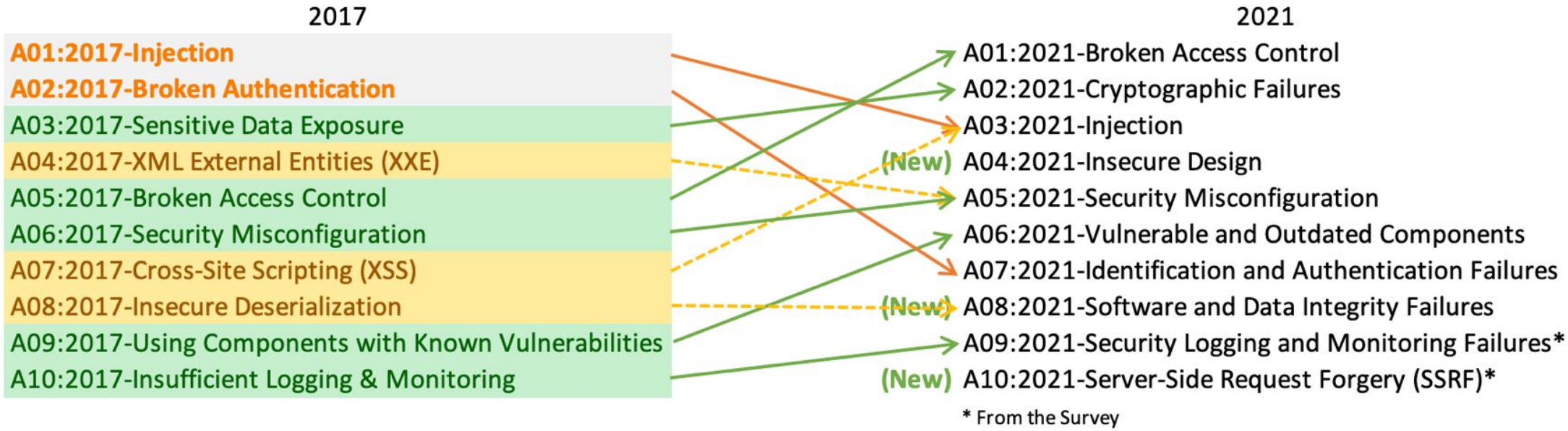
Open Web Application Security Project

Who is the OWASP Foundation?

SOSECURE

- The Open Web Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.
- Tools and Resources
- Community and Networking
- Education & Training
- For nearly two decades corporations, foundations, developers, and volunteers have supported the OWASP Foundation and its work. Donate, Join, or become a Corporate Member today.

OWASP Top 10 Project



OWASP API Security Top 10 2019

- API1:2019 Broken Object Level Authorization
- API2:2019 Broken User Authentication
- API3:2019 Excessive Data Exposure
- API4:2019 Lack of Resources & Rate Limiting
- API5:2019 Broken Function Level Authorization
- API6:2019 Mass Assignment
- API7:2019 Security Misconfiguration
- API8:2019 Injection
- API9:2019 Improper Assets Management
- API10:2019 Insufficient Logging & Monitoring

OWASP API Top 10

1	Broken object level authorization	1	Broken access control
2	Broken user authentication	7	Identification and authentication failures
3	Excessive data exposure		
4	Lack of resources & rate limiting		
5	Broken function level authorization	1	Broken access control
6	Mass assignment		
7	Security misconfiguration	5	Security misconfiguration
8	Injection	3	Injection
9	Improper assets management		
10	Insufficient logging & monitoring	9	Security logging and monitoring failures

CWE Top 25

SOSECURE

1. Out-of-bounds Write
   CWE-787 | CVEs in KEV: 70 | Rank Last Year: 1
2. Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
   CWE-79 | CVEs in KEV: 4 | Rank Last Year: 2
3. Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
   CWE-89 | CVEs in KEV: 6 | Rank Last Year: 3
4. Use After Free
   CWE-416 | CVEs in KEV: 44 | Rank Last Year: 7 (up 3) ▲
5. Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
   CWE-78 | CVEs in KEV: 23 | Rank Last Year: 6 (up 1) ▲
6. Improper Input Validation
   CWE-20 | CVEs in KEV: 35 | Rank Last Year: 4 (down 2) ▼
7. Out-of-bounds Read
   CWE-125 | CVEs in KEV: 2 | Rank Last Year: 5 (down 2) ▼
8. Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
   CWE-22 | CVEs in KEV: 16 | Rank Last Year: 8
9. Cross-Site Request Forgery (CSRF)
   CWE-352 | CVEs in KEV: 0 | Rank Last Year: 9
10. Unrestricted Upload of File with Dangerous Type
    CWE-434 | CVEs in KEV: 5 | Rank Last Year: 10
11. Missing Authorization
    CWE-862 | CVEs in KEV: 0 | Rank Last Year: 16 (up 5) ▲
12. NULL Pointer Dereference
    CWE-476 | CVEs in KEV: 0 | Rank Last Year: 11 (down 1) ▼
13. Improper Authentication
    CWE-287 | CVEs in KEV: 10 | Rank Last Year: 14 (up 1) ▲
14. Integer Overflow or Wraparound
    CWE-190 | CVEs in KEV: 4 | Rank Last Year: 13 (down 1) ▼
15. Deserialization of Untrusted Data
    CWE-502 | CVEs in KEV: 14 | Rank Last Year: 12 (down 3) ▼
16. Improper Neutralization of Special Elements used in a Command ('Command Injection')
    CWE-77 | CVEs in KEV: 4 | Rank Last Year: 17 (up 1) ▲
17. Improper Restriction of Operations within the Bounds of a Memory Buffer
    CWE-119 | CVEs in KEV: 7 | Rank Last Year: 19 (up 2) ▲
18. Use of Hard-coded Credentials
    CWE-798 | CVEs in KEV: 2 | Rank Last Year: 15 (down 3) ▼
19. Server-Side Request Forgery (SSRF)
    CWE-918 | CVEs in KEV: 16 | Rank Last Year: 21 (up 2) ▲
20. Missing Authentication for Critical Function
    CWE-306 | CVEs in KEV: 8 | Rank Last Year: 18 (down 2) ▼
21. Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
    CWE-362 | CVEs in KEV: 8 | Rank Last Year: 22 (up 1) ▲
22. Improper Privilege Management
    CWE-269 | CVEs in KEV: 5 | Rank Last Year: 29 (up 7) ▲
23. Improper Control of Generation of Code ('Code Injection')
    CWE-94 | CVEs in KEV: 6 | Rank Last Year: 25 (up 2) ▲
24. Incorrect Authorization
    CWE-863 | CVEs in KEV: 0 | Rank Last Year: 28 (up 4) ▲
25. Incorrect Default Permissions
    CWE-276 | CVEs in KEV: 0 | Rank Last Year: 20 (down 5) ▼

Other OWASP Projects

- **OWASP Software Assurance Maturity Model**: Building a usable framework to help organisations formulate and implement a strategy for application security that is tailored to the specific business risks facing the organisation.
- **OWASP Development Guide**: Practical guidance for application-level security including J2EE, ASP.NET, and PHP code samples.
- **OWASP Application Security Verification Standard**: A standard for performing application-level security verifications.
- And more.

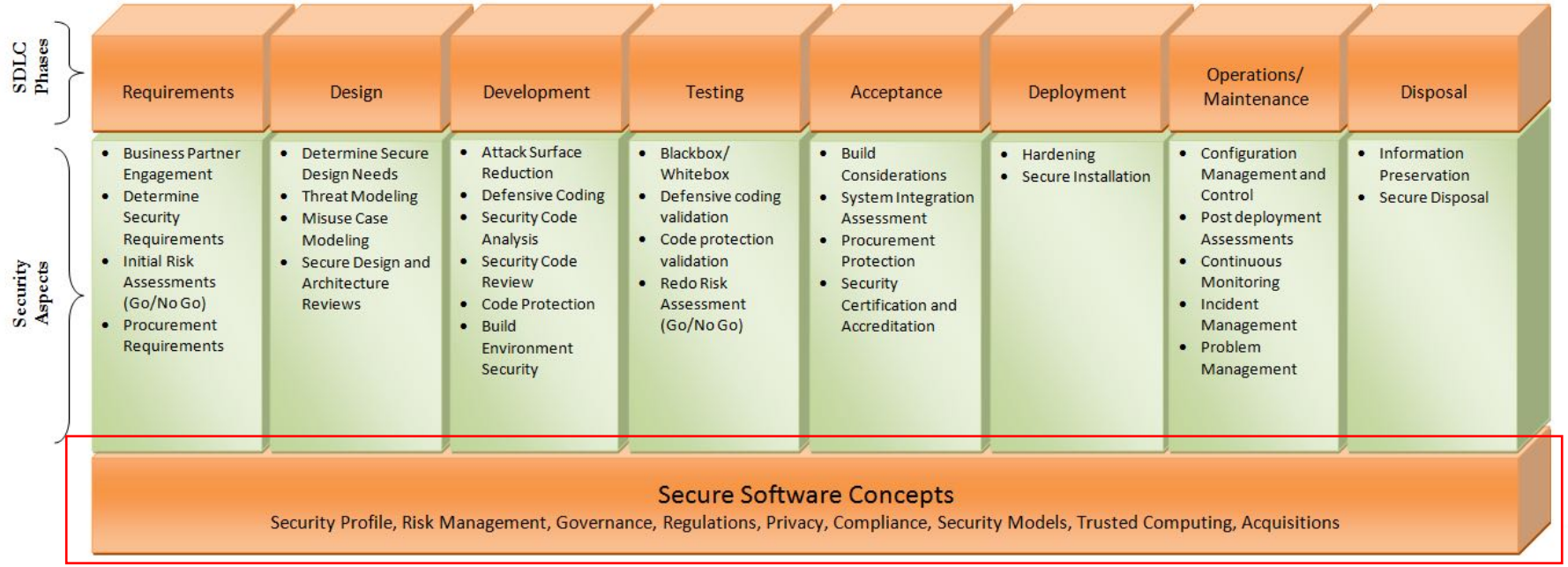
Other OWASP Projects

https://owasp.org/projects/

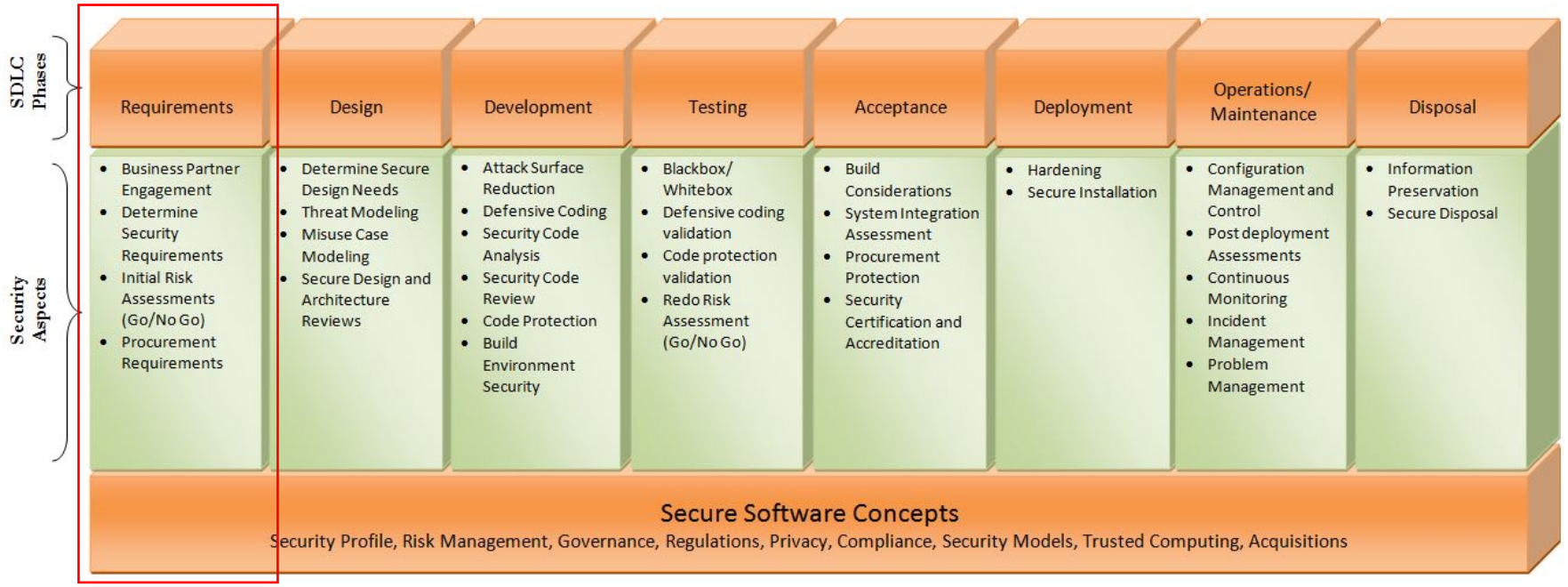
- OWASP ModSecurity Core Rule Set
- OWASP OWTF
- OWASP Risk Assessment Framework
- OWASP SAMM
- OWASP security Knowledge Framework
- OWASP Security Shepherd
- OWASP Top Ten
- OWASP Web Security Testing Guide
- OWASP ZAP
- OWASP Amass
- OWASP Application Security Verification Standard
- OWASP Cheat Sheet Series
- OWASP CSFRGuard
- OWASP Defectdojo
- OWASP Dependency-Check
- OWASP Dependency-Track
- OWASP Juice Shop
- OWASP Mobile Security Testing Guide
- OWASP Mobile Top 10

Secure Software Development Life Cycle

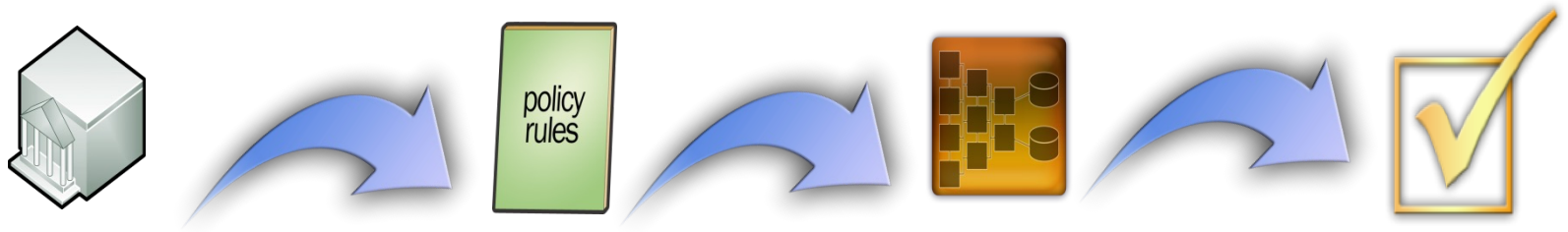
โมเดลการพัฒนาซอฟต์แวร์อย่างปลอดภัย



Requirements



Requirements Elicitation



Policies/ Standards/ or PnPs and External requirements

- SOX
- PCI DSS
- Authentication Policy
- HIPAA

High level Objectives

- Confidentiality
- Secure Transmission
- Privacy

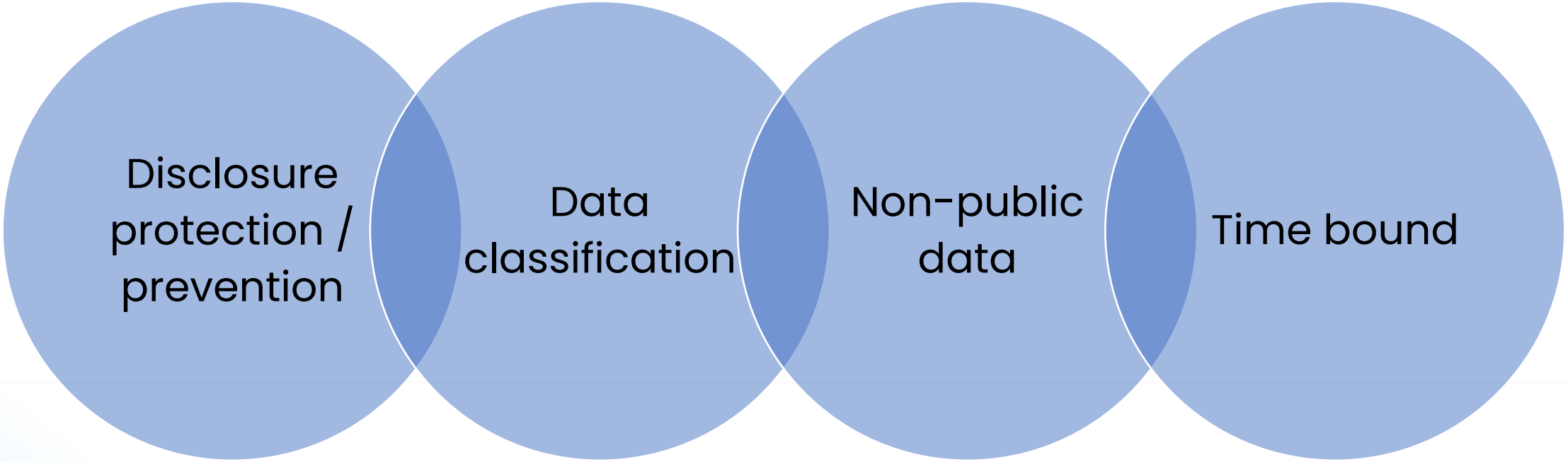
Security Requirements

- Information Classification & Handling
- Identity Management

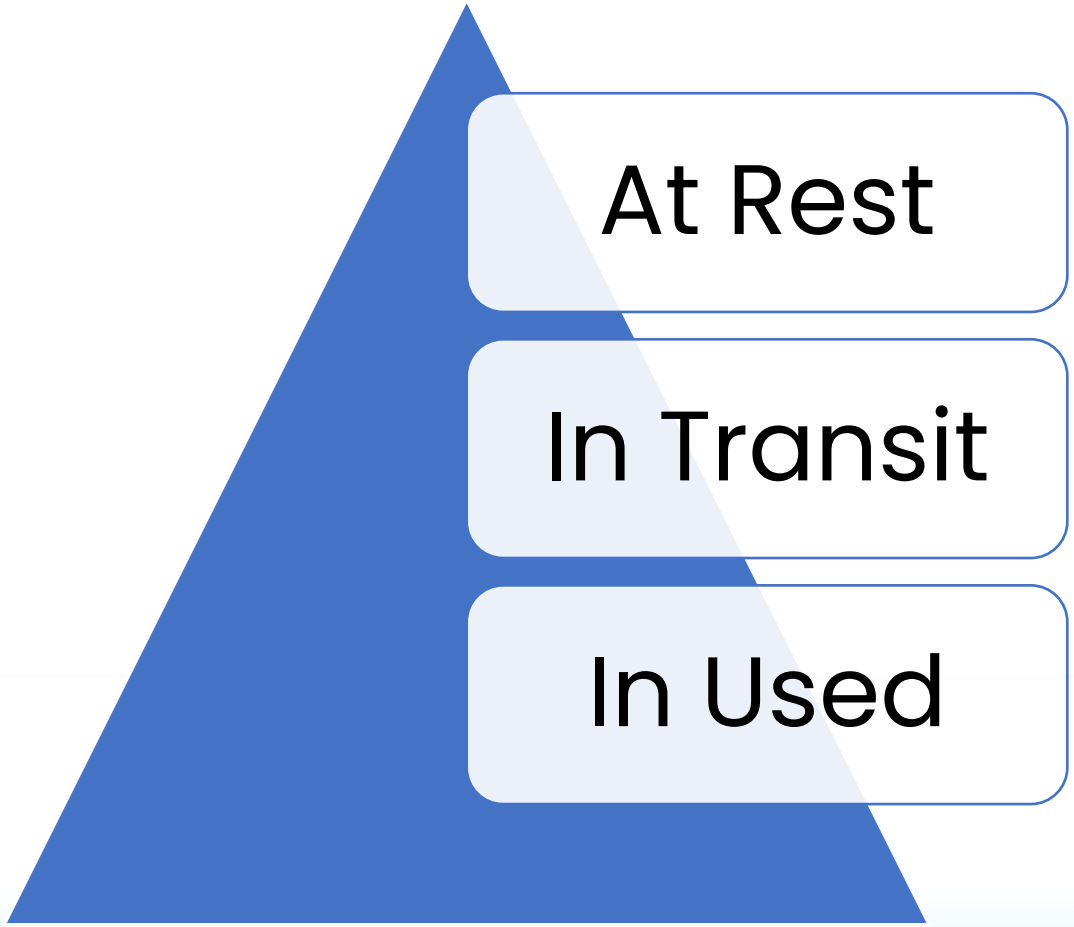
Software Security Requirements

- Input Validation
- Exception Handling
- Output Encoding

Confidentiality Requirements



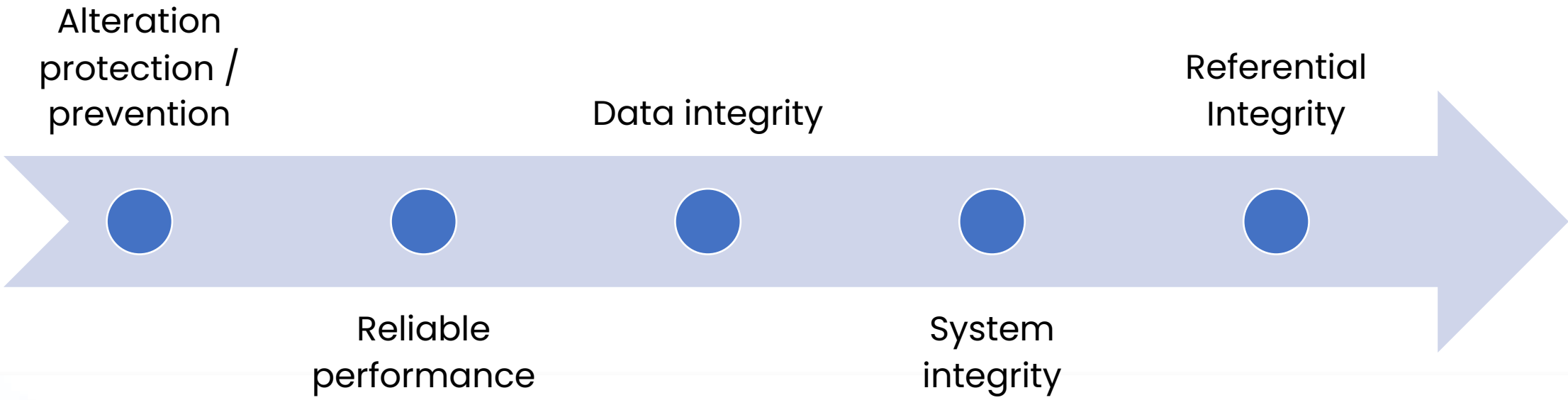
Confidential Requirements



Confidentiality Mechanisms

- Encryption
- Hashing
- Masking

Integrity Requirements



Integrity Mechanisms

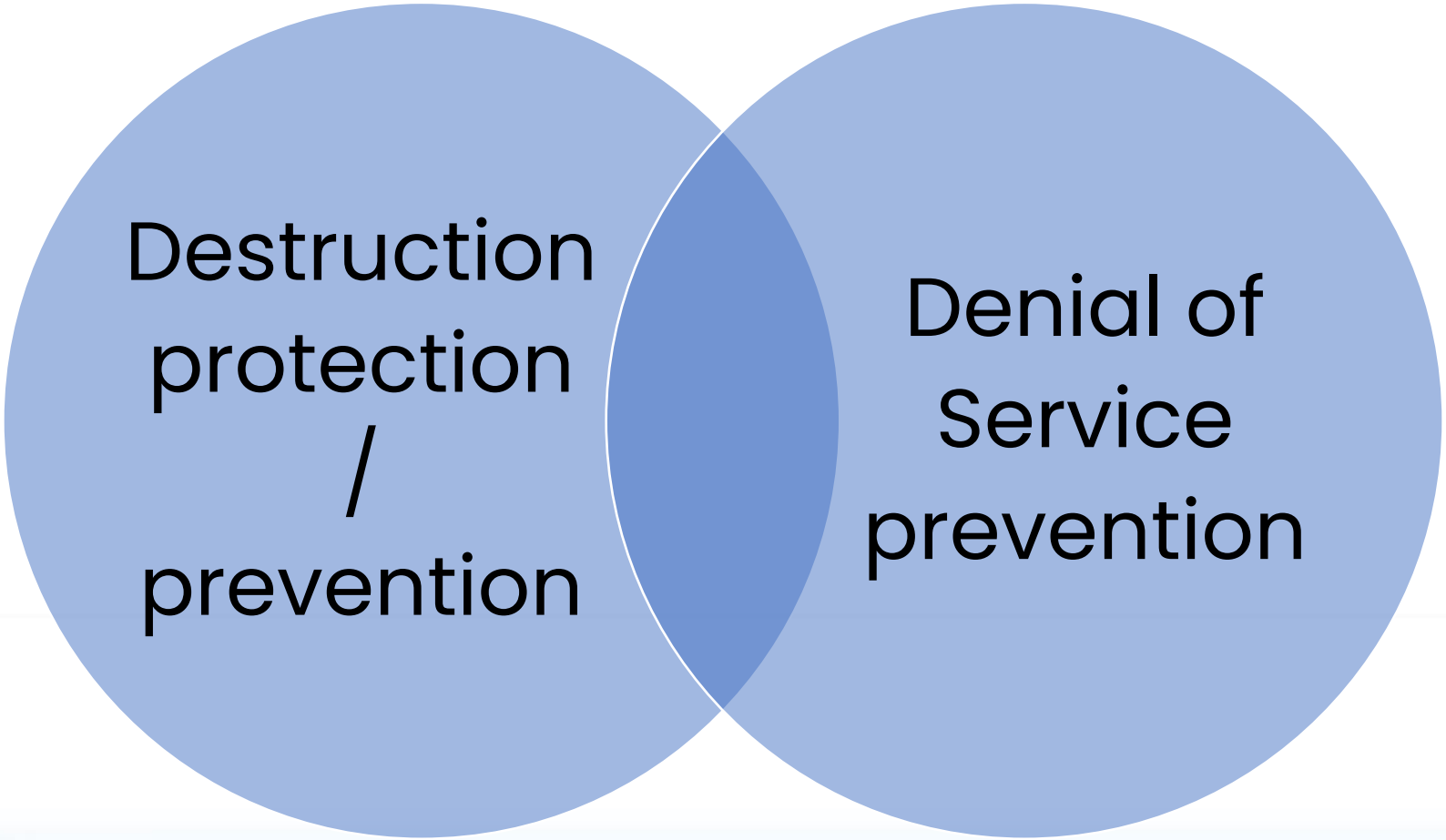
Input Validation

Hashing

Database Integrity (ACID)

- Atomicity
- Consistency
- Isolation
- Durability

Availability Requirements



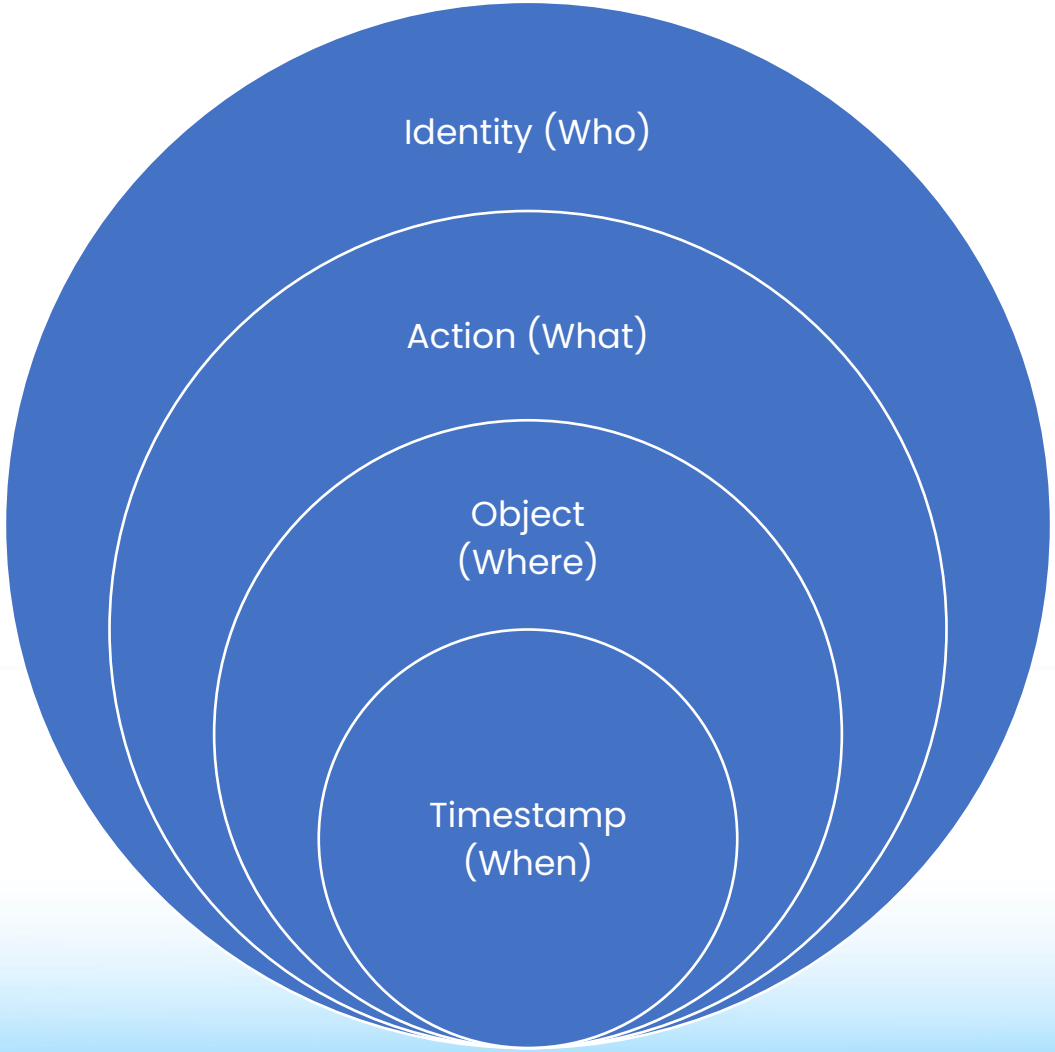
Authentication – Basic Rules

- Don’t reinvent the wheel
- Use Integrated Authentication (Kerberos, NTLM) if possible
- Use client certificates if feasible
- Custom authentication, only if necessary

Authorization Requirements

- Resource request access
- Allowed specific actions
- Layered on top of authentication

Auditing (Logging) Requirements



What to log?

- Critical business transactions
- Administrative functionality
- Authentication attempts

Other Requirements

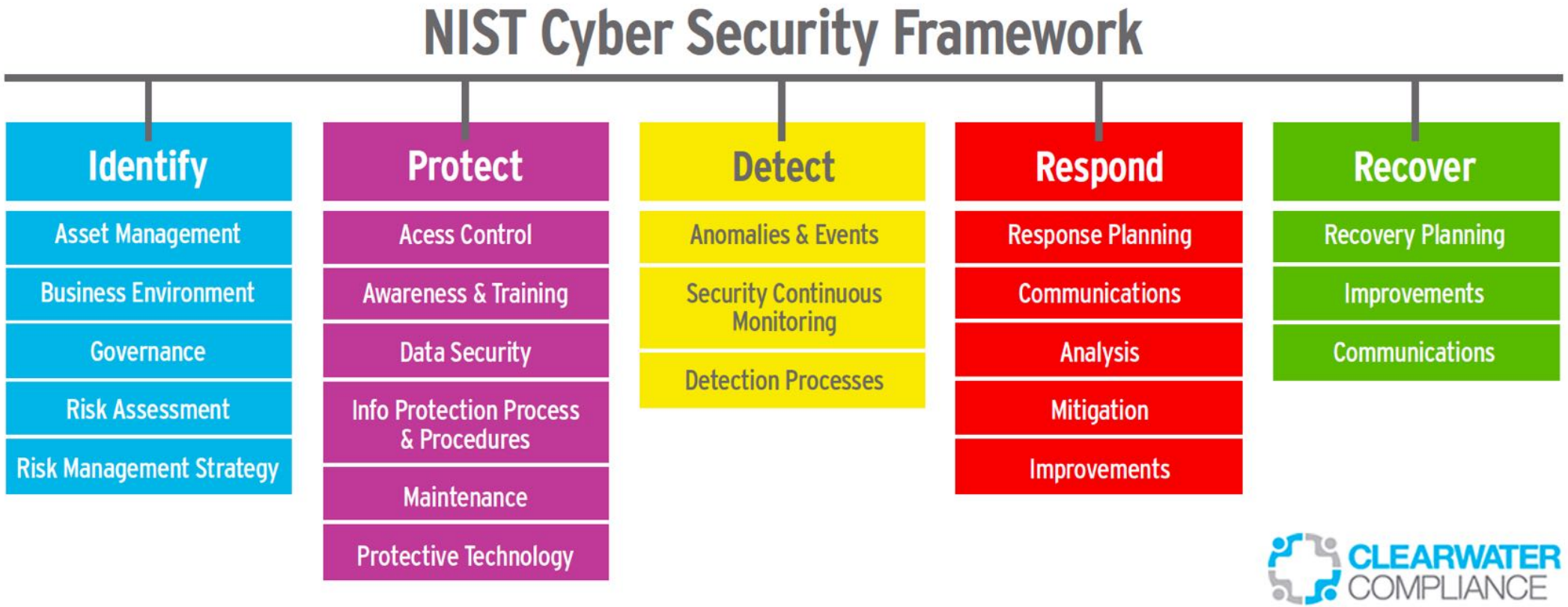
- Deployment Environment
- Archiving
- International
- Procurement

Deployment Environment

- Intranet, Extranet, and Internet
- Demilitarized Zones (DMZs)
- Infrastructure Hardening and Security Baseline

Introduction of Incident Management

Cybersecurity Framework



What's the Goal of an Incident Response Team

Goal	Key Questions	Key Tactics
Investigation/Analysis	Is this an incident that requires attention now? Which assets are impacted?	Determine and document the scope, priority, and impact.
Reporting/Communications	Which types of security incidents do we include in our daily, weekly, and monthly reports? Who is on the distribution list? What information can we provide to the executive team to maintain visibility and awareness (e.g. industry reports, user behavioral patterns, etc.)?	Define and categorize security incidents based on asset value/impact. Document and educate team members on appropriate reporting procedures. Collect relevant trending data and other information to showcase the value the incident response team can bring to the overall business.
Response/Improvement	What's the most effective way to investigate and recover data and functionality? How do we improve our response capabilities?	Investigate root cause, document findings, implement recovery strategies, and communicate status to team members.

What is Incident Management?

- What is a computer security **incident**?
  - **Adverse event** in information system infrastructure
  - Threat of the occurrence of adverse event
- What is an **event**?
  - **Any observable occurrence** in a system or network
  - Sometimes indicates an incident is occurring

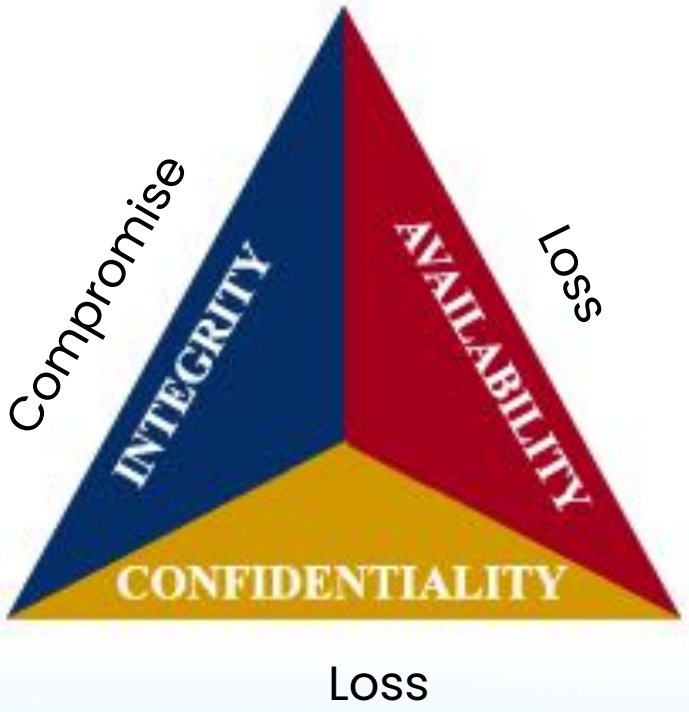
What is Incident Management?

- **Incident Types**
  - Malicious code attacks
  - Unauthorized access
    - Attempted intrusion
    - Reconnaissance activity
  - System compromise/ intrusion
  - Loss of, theft of or missing assets, data, etc.

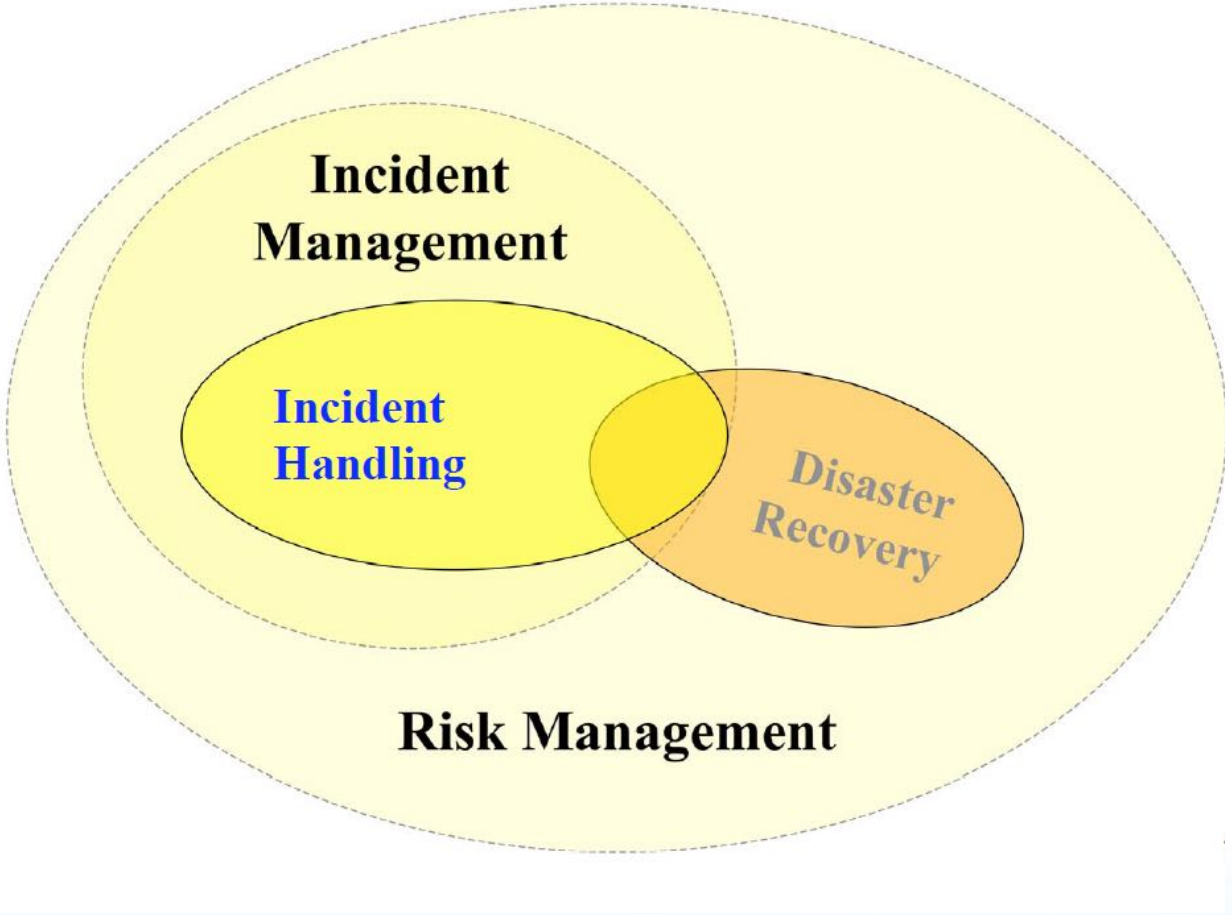
- **Incident Types**
  - Disruption of service
  - Unauthorized use / Misuse
    - Infraction of policy
    - Illegal activity
  - Espionage
  - Hoaxes (False information)

What is Incident Management?

Incidents are resulting in ... of data / service / identity



What is Incident Management?



What is Incident Management?

- **Aims of Incident Management:**
  - Restore normal service as quickly as possible
  - Minimize adverse impact on business
  - Ensure no incident goes undetected
  - Ensure incidents are handled with consistent processes
  - Reduce number of incidents in time
  - Build working relationships across organization with open communication

NIST Incident Response Function

- Response Planning
  - Response plan is executed during or after an event
- Communications
  - Personnel know their roles and order of operations when a response is needed
  - Events are reported consistent with established criteria
  - Information is shared consistent with response plans
  - Coordination with stakeholders occurs consistent with response plans
  - Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness

NIST Incident Response Function

- Analysis
  - Notifications from detection systems are investigated
  - The impact of the incident is understood
  - Forensics are performed
  - Incidents are categorized consistent with response plans
- Mitigation
  - Incidents are contained
  - Incidents are mitigated
  - Newly identified vulnerabilities are mitigated or documented as accepted risks
- Improvements
  - Response plans incorporate lessons learned
  - Response strategies are updated

Why do we need Incident Management?

- Not all incidents can be prevented and anticipated.
  - …despite risk mitigations
- New kinds of security incidents emerge with new technologies.
  - Zero Days Attacks
- Incident handling is a complex undertaking.
- Upon occurrence of incident:
  - Time to execute plans, not start thinking about them!

Six Phase Approach

- **Incident Management Strategy**
  - Preparation
    - Have a game plan. Be ready
  - Identification
    - Who does what and how? Where is XYZ?
    - Assessment of situation.
  - Containment:
    - Close the fire gate
  - Eradication:
    - Remove the threat and **vulnerability**
  - Recovery:
    - Restore health. Rebuild if necessary
  - Lessons learned:
    - Review what has (and has not) been done.
    - How can we improve?

Threat Categories

- Unauthorized Access
- Malicious Code
- Inappropriate Usage
- Multiple Component
- Denial of Service
- Attempt Access

Example of Unauthorized Access Incident

- Performing a remote root compromise of a server
- Defacing a Web server
- Guessing or cracking passwords
- Viewing or copying sensitive data, such as payroll records, medical information, and credit card numbers, without authorization
- Using an unattended, logged-in workstation without permission.

Example of Malicious Code Incident

- Malware Infected
  - Virus
  - Worm
  - Trojan
  - Spyware & Keylogger
  - Ransomware

Example of Inappropriate Usage Incident

- Download password cracking tools or pornography
- Send spam promoting a personal business
- Email harassing messages to coworkers
- Set up an unauthorized Web site on one of the organization's computers
- Use file or music sharing services to acquire or distribute pirated materials
- Transfer sensitive materials from the organization to external locations

Example of Multiple Component Incident

- Malicious code spread through email compromises an internal workstation
- An attacker (who may or may not be the one who sent the malicious code) uses the infected workstation to compromise additional workstations and servers
- An attacker (who may or may not have been involved in Steps 1 or 2) uses one of the compromised hosts to launch a DDoS attack against another organization

Example of Denial of Service Incident

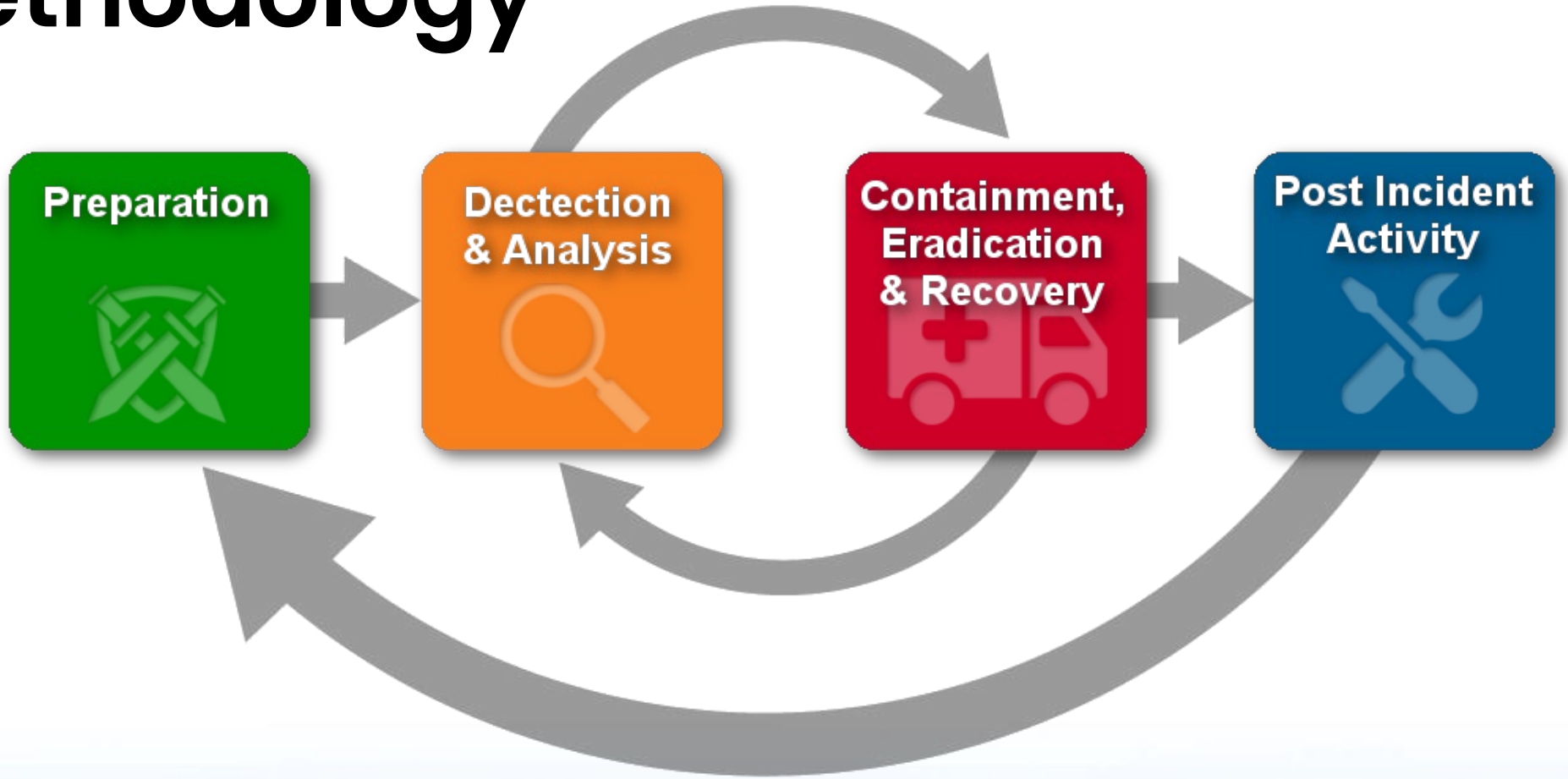
- Using all available network bandwidth by generating unusually large volumes of traffic
- Sending malformed TCP/IP packets to a server so that its operating system will crash
- Sending illegal requests to an application to crash it
- Making many processor-intensive requests so that the server's processing resources are fully consumed (e.g., requests that require the server to encrypt each reply)
- Establishing many simultaneous login sessions to a server so that other users cannot start login sessions

Example of Attempt Access Incident

- Scan Port
- Service Fingerprint
- Vulnerability Assessment
- Active Password Cracking

Incident Handling Methodology

Incident Response & Handling Methodology



5. Six Phase Approach

- Incident Management Strategy
  1. Preparation
  2. Identification
  3. Containment
  4. Eradication
  5. Recovery
  6. Lessons learned

Incident Response Preparation

Preparation

- Form a Computer Incident Response Team (CIRT)
  - Need a designated leader with authority to tap resources
  - Provide training – management and front-line team
- Prepare a plan of action
  - Mission
  - Strategies and goals
  - Management Approval
  - Approach to incidents
  - Communications
  - Metrics for response
  - Training and Testing

Preparation (cont.)

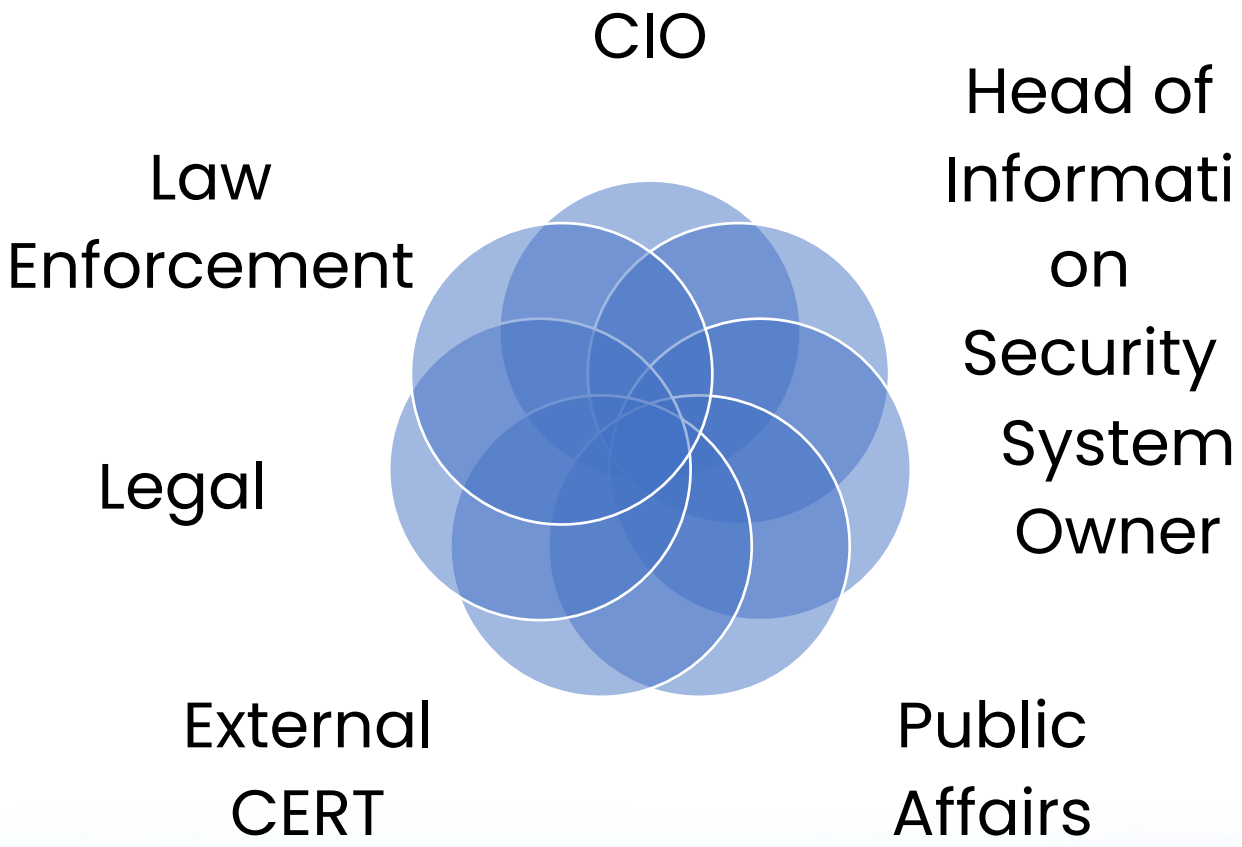
- Team Toolkit
  - Contact information – Key management, team members, vendor contacts, escalation policy
  - Issue tracking system
  - Smartphones – communications and onsite web access
  - War room
  - Forensic tools – clean laptops, blank media, analysis tools (sniffer)
  - Evidence gathering accessories and knowledge
  - Detailed network configuration data and diagrams access

Prevention beats Incident Handling

Incident Response Team Services

- Develop Incident Response Process
- Exercise an Incident Response Plan and Playbooks
- Training and Self Improvement
- Vulnerability Assessment
- Intrusion Detection
- Education and Awareness
- Technology Watch

Who you Communicate with?



Communication Channel

Email

Ticket Management Software (Intranet-based)

Telephone calls

Voice mailbox

Instant Messaging

Incident Response Team

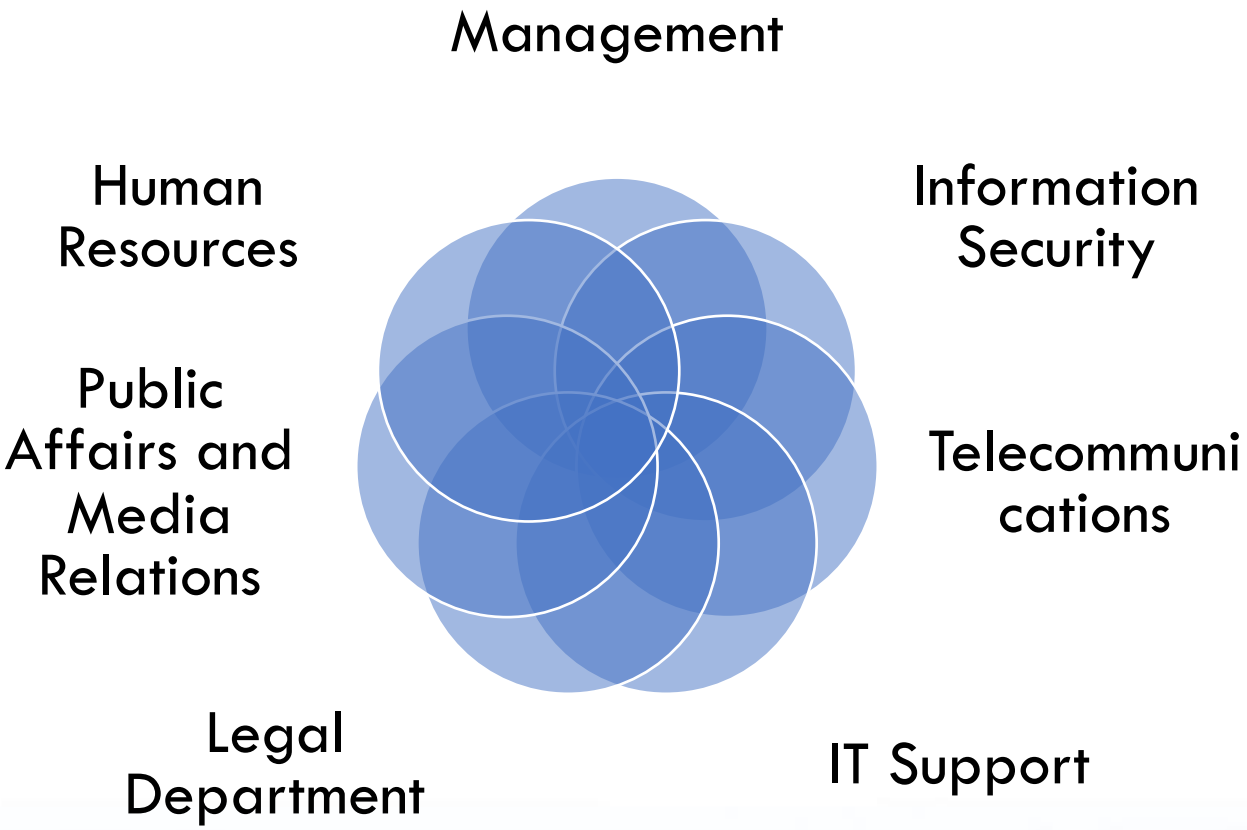
The Computer Security Incident Response Team (CSIRT)

- To set up a CSIRT, organizations can opt for three different staffing models:
  - Employees
  - Partially Outsourced
  - Fully Outsourced

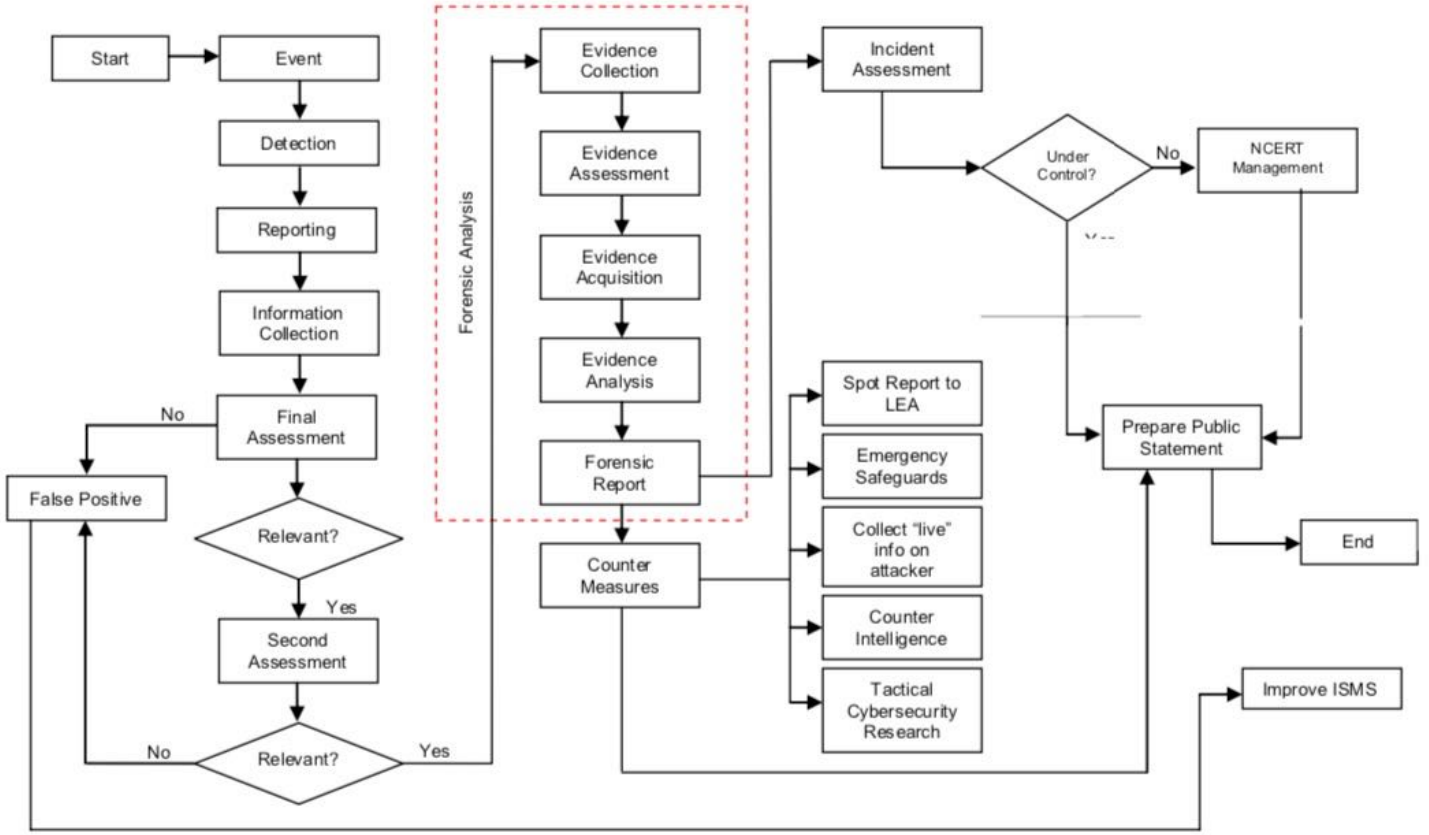
Team Model Selection

- The Need for 24/7 Availability
- Full-Time Versus Part-Time Team Members
- Employee Morale
- Cost
- Staff Expertise
- Organizational Structures

Dependencies Within Organizations



Flowchart for Incident Handling Responses



Incident Response Plan

- Identify
- Develop
- Verify
- Exercise
- Lesson Learn

Thank you