CIS Controls

Thursday, February 13, 2025 1:57 PM

1. Audit & Log Management (M1047)

Finding: SIEM not collecting logs from firewalls

- **CIS Control Reference:** CIS Control 6.4 (Collect audit logs for analysis)
- **MITRE ATT&CK Technique:** T1074 (Data Staged - Lack of centralized logging)
- **NSA & CISA Misconfiguration:** Insufficient internal network monitoring
- **Real-World Breach Cost Data:** Organizations without centralized logging have a **15% longer breach lifecycle**, adding up to **$370,000 in additional costs per breach** (IBM Cost of a Data Breach Report 2023).
- **ROI Analysis:** Implementing SIEM reduces incident detection time by **37%**, preventing lateral movement.
- **Performance Metric Impact:** Improves **MTTD (Mean Time to Detect)** from **14 days** to **<5 days**.
- **Financial Loss Reduction:** Potential savings of **$750K per breach** through improved early detection.
- **Cost Consideration:** Logging tools ($0–$10,866 for Tier 2) enhance threat detection while remaining cost-effective.

2. Patch Management (M1051)

Finding: 10% of servers missing critical patches

- **CIS Control Reference:** CIS Control 7.2 (Apply security updates)
- **MITRE ATT&CK Technique:** T1190 (Exploitation of Public-Facing Application)
- **NSA & CISA Misconfiguration:** Poor patch management
- **Real-World Breach Cost Data: Unpatched vulnerabilities account for 60% of breaches**, costing an average of **$4.45M per incident**.
- **ROI Analysis:** Automated patching reduces unpatched vulnerabilities by **90%**, preventing exploits.
- **Performance Metric Impact:** Increases **patch compliance rate from 65% to 95%**.
- **Financial Loss Reduction:** Reduces **breach probability by 30%**, saving up to **$1.2M per breach**.
- **Cost Consideration:** Automated patch management tools ($0–$7,200 for Tier 2) provide significant risk reduction at a reasonable cost.

3. Vulnerability Scanning (M1016)

Finding: Inconsistent or infrequent vulnerability scanning

- **CIS Control Reference:** CIS Control 7.1 (Perform automated vulnerability scanning)
- **MITRE ATT&CK Technique:** T1595 (Active Scanning)
- **NSA & CISA Misconfiguration:** Lack of routine vulnerability assessments
- **Real-World Breach Cost Data:** 60% of breaches stem from unpatched vulnerabilities, leading to an average of **$4.45M per incident**.
- **ROI Analysis:** Routine scanning identifies and mitigates vulnerabilities before exploitation.
- **Performance Metric Impact:** Improves **scan coverage compliance from 70% to 95%**.
- **Financial Loss Reduction:** Reduces breach probability, saving up to **$1.2M per breach**.

4. User Account Management (M1018)

Finding: Lack of proper user account provisioning and de-provisioning processes

- **CIS Control Reference:** CIS Control 5.1 (Establish and maintain an inventory of accounts)
- **MITRE ATT&CK Technique:** T1078.003 (Local Accounts)
- **NSA & CISA Misconfiguration:** Improper separation of user and admin privileges
- **Real-World Breach Cost Data:** Poor account management leads to **35% of insider threat incidents**, costing **$755K per event**.
- **ROI Analysis:** Strong account management reduces unauthorized access risks.
- **Performance Metric Impact:** Improves **user access audit success rate from 60% to 95%**.
- **Financial Loss Reduction:** Prevents privilege misuse, saving **$755K per breach**.
- **Cost Consideration:** Asset inventory and management tools ($0–$3,896 for Tier 2) help control unauthorized devices at a low cost.

5. Privileged Account Management (M1026)

Finding: Orphaned and excessive privileged accounts found

- **CIS Control Reference:** CIS Control 5.4 (Use dedicated administrative accounts)
- **MITRE ATT&CK Technique:** T1078.004 (Orphaned Accounts)
- **NSA & CISA Misconfiguration:** Weak privileged access controls
- **Real-World Breach Cost Data:** Privilege misuse accounts for **25% of breaches**, adding up to **$1.5M in damages per**

incident.
- **ROI Analysis:** Proper privilege access management reduces admin credential theft by **80%**.
- **Performance Metric Impact:** Improves **privileged access review success rate from 55% to 95%**.
- **Financial Loss Reduction:** Saves **$1.5M per breach** by mitigating insider threats.
- **Cost Consideration:** Multi-Factor Authentication (MFA) ($0–$8,640 for Tier 2) significantly reduces unauthorized access risks.

6. Secure Configurations

Finding: Misconfigured system settings and weak security baselines

- **CIS Control Reference:** CIS Control 4.1 (Implement and manage a secure configuration process)
- **MITRE ATT&CK Technique:** T1553 (Subvert Trust Controls)
- **NSA & CISA Misconfiguration:** Weak system configuration policies
- **Real-World Breach Cost Data:** Misconfigurations account for **26% of breaches**, adding up to **$3M in average damages per incident**.
- **ROI Analysis:** Secure configurations reduce system compromise risk by **65%**.
- **Performance Metric Impact:** Improves **configuration compliance rate from 60% to 90%**.
- **Financial Loss Reduction:** Prevents security breaches by enforcing security baselines, saving **$3M per incident**.
- **Cost Consideration:** Configuration management tools ($0–$47,494 for Tier 2) help enforce security baselines efficiently.

7. Data Recovery (Backup Solutions)

Finding: Lack of reliable backup solutions for disaster recovery

- **CIS Control Reference:** CIS Control 11.5 (Perform regular automated backups)
- **MITRE ATT&CK Technique:** T1490 (Inhibit System Recovery)
- **NSA & CISA Misconfiguration:** Poor backup policies
- **Real-World Breach Cost Data:** Ransomware attacks cause **$4.54M in average damages** if backup solutions are inadequate.
- **ROI Analysis:** Automated encrypted backups ensure resilience against data loss.
- **Performance Metric Impact:** Improves **backup success rate from 75% to 95%**.
- **Financial Loss Reduction:** Prevents data loss and downtime, saving **$4.54M per ransomware incident**.
- **Cost Consideration:** Backup solutions ($0–$11,888 for Tier 2) ensure resilience against ransomware and data loss.

8. Incident Response Planning

Finding: Lack of predefined escalation steps in incident response plans

- **CIS Control Reference:** CIS Control 19.1 (Develop an incident response plan)
- **MITRE ATT&CK Technique:** T1070 (Indicator Removal on Host)
- **NSA & CISA Misconfiguration:** Inadequate incident response planning
- **Real-World Breach Cost Data:** Unstructured incident response leads to **$1.49M in additional breach costs**.
- **ROI Analysis:** A structured response reduces containment time by **50%**.
- **Performance Metric Impact:** Improves **incident response readiness from 60% to 90%**.
- **Financial Loss Reduction:** Saves **$1.49M per breach** by reducing response time.
- **Cost Consideration:** Process-driven, with zero tooling cost but significant impact on reducing breach response time.