Category: Security

Security incidents refer to any event that compromises the integrity, confidentiality, or availability of an organization's information systems. These incidents can include successful ransomware attacks, data security breaches, and phishing attempts, among others.

1. **Threat Detection and Response Time**

   Question: How effectively are we detecting, containing, and resolving security threats, and what can we do to reduce response times and mitigate their impact?

   Metrics:

   a. Mean Time to Detect
   b. Mean Time to Acknowledge
   c. Mean Time to Contain
   d. Mean Time to Resolve
   e. Mean Time to Recovery
   f. Virus Infection Monitoring
      i. Frequency of scans
      ii. Detection rate of virus, malware, malicious code
   g. Cost per incident
      i. Response and recovery costs
      ii. Productivity loss
      iii. Resource expenditure

Correlation: Shorter detection and response times correlate with faster containment and recovery, essential for reducing damage and recovery costs. Virus Infection Monitoring can complement detection and response benchmarks by showing effectiveness in prevention. Higher incident rates typically drive up costs per incident. Reducing MTTR, MTTC, and MTTA should correlate with lower total costs and minimized productivity loss.

2. **Vulnerability and Patch Management**

   Question: How efficiently are we identifying, prioritizing, and deploying patches to address vulnerabilities, and what steps can we take to improve patch management processes?

Metrics:

a. Patching Rate: Total number of patches deployed within a certain timeframe (hours, days, weeks, months, years - depending on level of granularity chosen)

b. Average Open vs Closed Vulnerabilities based on severity rate
    i. Vulnerability ratings: Critical, High, Medium, Low, and None

c. Scan Rate: At least once per year
d. Mean Time to Detect
e. Mean Time to Resolve
f. Business Unit Risk Score
g. Vulnerability Maturity
h. Average Number of Granted Exceptions
i. Average Audit Score
j. Patch Prioritization Based on Vulnerability Rating

3. Data Loss Prevention and Access Control

Question: How well are our data loss prevention and access control measures preventing unauthorized data access, and where can we enhance these systems to reduce the risk of data breaches?

Metrics:

a. Data Loss Prevention Effectiveness
    i. Incident Prevention Ratio
    ii. DLP response time
    iii. False positives and negatives

b. Access Management

Correlation: Effective DLP and access control systems reduce the number of data incidents and response times, supporting incident containment. A low false-positive rate aids response times, making threat detection more reliable.

4. Network and Endpoint Security

Question: How robust are our network and endpoint security protocols in detecting and preventing threats, and how can we improve these measures to better safeguard against attacks?

Metrics:

a. Non-human traffic
b. Network Security Rating (a score between A and F)
c. Intrusion attempt vs. actual incidents

Correlation: A higher rate of non-human traffic can indicate potential bot activity, which should correlate with network security metrics. Intrusion attempt data paired with incident response rates can highlight the effectiveness of threat prevention measures.

5. Security Awareness and Policy Compliance

Question: How effective are our security awareness programs in ensuring compliance with security policies, and what improvements can be made to increase employee adherence?

Metrics:

a. Number of cybersecurity incidents reported
b. Security awareness training completion
c. Incorrect SSL configurations
d. Data Transferred via corporate network

References:

1. Developing Realistic Benchmarks to Track and Improve Cybersecurity Incident Response | Bitdefender
2. MTTD: An In-Depth Overview About What It Is and How to Improve It | StackState
3. 22 Cybersecurity Metrics & KPIs to Track in 2024 | SecurityScorecard
4. Top 5 Recommendation for Cybersecurity Benchmarking | Fire Compass
5. 5 Easy Steps for Benchmarking Cyber Security | Autobahn Security
6. 14 Cybersecurity Metrics + KPIs You Must Track in 2024 | UpGuard
7. What are Metrics & KPIs in Cyber security – Detailed Guide | Sprinto
8. Top 15 Cybersecurity Metrics and KPIs for Better Security | Cyber Talents
9. Top 10 Cybersecurity Metrics and KPIs | Mimecast

10. Decoding Cybersecurity Metrics: Top 10 KPIs Every CISO Must Know | RSAConference

11. A guide to cybersecurity metrics and KPIs | RiskXchange

12. The 10 Most Important Cybersecurity Metrics & KPIs for CISOs to Track | Secureframe

13. KPI Examples for Patch and Vulnerability Management | Heimdal