Security Monitoring by Cyph3rRyx

Security Operations Center (SOC)

- A centralized team or facility responsible for safeguarding an organization's information systems and data from security threats.

Why SOC?

- **Cybersecurity Defense:** Protect against cyber threats and attacks.
- **Threat Detection:** Identify and respond to security incidents.
- **Incident Response:** Mitigate damage and recover from breaches.
- **Compliance:** Ensure adherence to regulatory and security standards.
- **Proactive Monitoring:** Stay ahead of emerging threats.

What SOC Do?

- **Monitoring:** Continuously observe network and system activities.
- **Threat Detection:** Identify anomalies and potential security threats.

- **Incident Response:** Rapidly respond to and mitigate security incidents.
- **Forensics:** Investigate and analyze security breaches and incidents.
- **Security Awareness:** Educate employees on cybersecurity best practices.
- **Security Tool Management:** Administer and maintain security tools.

Who Works in SOC?

- **Security Analysts:** Monitor, detect, and respond to threats.
- **Incident Responders:** Handle security incidents and breaches.
- **Threat Hunters:** Proactively seek out hidden threats.
- **Compliance Specialists:** Ensure adherence to standards and regulations.
- **Security Engineers:** Implement and maintain security technologies.
- **SOC Managers:** Oversee SOC operations and strategy.

Benefits of a SOC:

- Improved security posture.
- Reduced response times to threats.
- Enhanced compliance and risk management.
- Better understanding of the threat landscape.

Levels in a SOC (Security Operations Center)

1. **Level 1 - Junior Analysts:**
    - The first line of incident responders.
    - Monitor alerts and determine their urgency.
    - May manage security tools and run regular reports.
2. **Level 2 - Intermediate Analysts:**
    - Possess more expertise to investigate and assess issues.

- Quickly identify the root causes of incidents.
- Follow procedures to remediate problems and flag complex issues.

3. **Level 3 - Senior Analysts:**
    - High-level security experts actively searching for vulnerabilities.
    - Use advanced threat detection tools.
    - Diagnose weaknesses and make recommendations for security improvements.
    - May include specialists like forensic investigators and compliance auditors.
4. **Level 4 - Management and Oversight:**
    - Comprises high-level managers and chief officers.
    - Oversee all SOC team activities.
    - Responsible for hiring, training, and evaluating team members.
    - Act as liaisons between the SOC team and the organization.
    - Ensure compliance with regulations and standards.

Note:

- SOC levels represent the hierarchy within a Security Operations Center.
- Each level has specific responsibilities and expertise.
- Level 1 handles initial alert monitoring, while Level 4 oversees management and compliance.
- SOC levels work collaboratively to ensure the organization's security and response to incidents.

SOC Sweet Spot

The SOC (Security Operations Center) Sweet Spot represents an optimal state in cybersecurity operations where the balance between threat detection, efficient management, and response capabilities is achieved.

Factors Leading to the SOC Sweet Spot:

1. **Automated Tools:**
    - The sheer volume of security events in a network can be overwhelming.
    - Automation is essential to handle this "noise" and prioritize significant threats.
2. **Investments in Key Technologies:**
    - Security Information and Event Management (SIEM): Offers comprehensive network activity visibility.
    - Endpoint Protection Systems: Safeguard all devices connecting to the network.
    - Firewall: Monitors and controls incoming and outgoing traffic.
    - Automated Application Security: Streamlines vulnerability testing.
    - Asset Discovery System: Tracks tools and software usage for risk evaluation.
    - Data Monitoring Tool: Ensures data security and integrity.
    - Governance, Risk, and Compliance (GRC) System: Ensures compliance with regulations.
    - Vulnerability Scanners and Penetration Testing: Identifies network weaknesses.
    - Log Management System: Collects and stores messages from network components.

Significance of SOC Sweet Spot:

- The SOC Sweet Spot signifies the right alignment of technology, processes, and human resources to effectively manage and respond to cybersecurity threats.
- It minimizes the risk of overlooking critical security incidents while efficiently handling a high volume of alerts.
- Achieving the SOC Sweet Spot enhances an organization's ability to protect its digital assets and maintain compliance with industry regulations.

Note:

- The SOC Sweet Spot reflects the harmonious integration of automated tools and specialized technologies within the security operations center.
- These investments contribute to improved threat detection, response, and overall cybersecurity resilience.

Security and Control

- **Data Access:**
  - Control and restrict access to sensitive data.
  - Authentication mechanisms, role-based access, and least privilege principles are commonly used.
  - Ensures that only authorized users can view or modify data.
- **Encryption:**
  - Encrypt data at rest and in transit to protect it from unauthorized access.
  - Common encryption methods include SSL/TLS for communication and file encryption for stored data.
  - Mitigates the risk of data breaches and eavesdropping.
- **2-Factor Authentication:**
  - Requires users to provide two forms of identification before granting access.
  - Typically combines something the user knows (password) with something the user has (smartphone, token, etc.).
  - Enhances login security and reduces the risk of unauthorized access.
- **Disaster Recovery:**
  - Establishes strategies and processes to recover data and operations in the event of a disaster.
  - Includes data backups, redundant systems, and failover procedures.
  - Ensures business continuity and data integrity in catastrophic scenarios.
- **Third-Party Security Management:**
  - Involves managing security aspects of third-party services and vendors.
  - Evaluates and enforces security requirements for outsourced or externally provided systems.
  - Minimizes vulnerabilities introduced through third-party relationships.

Security Goals:

- **Confidentiality:**
  - Ensure that sensitive data is not disclosed to unauthorized parties.
  - Achieved through encryption, access controls, and data classification.
- **Integrity:**
  - Guarantee the accuracy and reliability of data and resources.
  - Methods include data validation, checksums, and secure update processes.
- **Availability:**
  - Ensure that systems and data are available when needed.
  - Achieved through redundancy, disaster recovery, and fault-tolerant systems.
- **Authenticity:**
  - Confirm the legitimacy of users, systems, and data.
  - Utilizes authentication mechanisms and digital signatures.
- **Accountability:**
  - Establish responsibility for actions and access.
  - Logging and audit trails are common tools for achieving accountability.
- **Non-Repudiation:**
  - Prevent users from denying their actions or transactions.
  - Digital signatures and transaction logs support non-repudiation.

Notes:

- Security and control measures are critical for safeguarding digital assets and mitigating risks.
- Security goals serve as the foundation for designing and implementing security strategies.

Top 5 Challenges Faced by Security Operations Centers (SOC)

1. **Increasing Volumes of Security Alerts:**
    - The growing number of security alerts consumes valuable analyst time.
    - Sorting through numerous alerts and triaging them are time-consuming tasks.
    - This overload results in missed alerts or more severe threats slipping through.
2. **Management of Numerous Security Tools:**
    - SOCs use a variety of security suites and technologies.
    - Monitoring and managing data generated from multiple sources become challenging.
    - Coordinating and maintaining dozens of security tools is complex.
3. **Competition for Skilled Analysts and Lack of Knowledge Transfer:**
    - A global cybersecurity talent shortage is making it difficult to find skilled analysts.
    - The competition for analysts with the required skill set is fierce.
    - Knowledge transfer between experienced and new analysts is often lacking.
4. **Budget Constraints with Increasing Incident Costs:**
    - Security operations and incident response are hard to measure and manage.
    - Justifying spending on cybersecurity is challenging without clear ROI.
    - The cost of security incidents continues to rise.
5. **Legal and Regulatory Compliance:**
    - Meeting various legal and regulatory compliance standards such as NIST, PCI, GLBA, FISMA, HITECH (HIPAA), and GDPR is necessary.
    - Different industries and geographical locations have varying compliance requirements.
    - Ensuring compliance can be complex and resource-intensive.

Notes:

- SOCs face multiple challenges in handling security operations efficiently and effectively.

- Overcoming these challenges is essential to maintain strong cybersecurity postures and protect organizations from evolving threats.

---

1. **NIST:** National Institute of Standards and Technology
    - (To enhance economic security and improve the quality of life)
2. **PCI:** Payment Card Industry Data Security Standard
    - (Related to payment via cards)
3. **GLBA:** Gramm-Leach-Bliley Act
    - (Related to financial products or services)
4. **FISMA:** Federal Information Security Management Act
    - (A framework of guidelines and security standards to protect government information and operations)
5. **HITECH (HIPAA):** Health Information Technology for Economic and Clinical Health
    - (To promote the adoption and meaningful use of health information technology)
6. **GDPR:** General Data Protection Regulation
    - (A Regulation in EU law on data protection and privacy in the EU and the European Economic Area)

Legal and Regulatory Compliance:

1. **SOX:** Sarbanes-Oxley Act
    - (Related to corporate governance and financial reporting)
2. **FERPA:** Family Educational Rights and Privacy Act
    - (Related to the privacy of student education records)
3. **COPPA:** Children's Online Privacy Protection Act
    - (Related to the online privacy of children under 13)
4. **CFAA:** Computer Fraud and Abuse Act

- (Related to computer and network security)

Security Operations Center (SOC):

1. **SIEM:** Security Information and Event Management
   - (Software used for security management and real-time event analysis)
2. **CSIRT:** Computer Security Incident Response Team
   - (A team that responds to and mitigates security incidents)
3. **IDS/IPS:** Intrusion Detection System/Intrusion Prevention System
   - (Security tools for detecting and preventing unauthorized access)
4. **DFIR:** Digital Forensics and Incident Response
   - (Investigative techniques used to respond to cybersecurity incidents)
5. **UEBA:** User and Entity Behavior Analytics
   - (Using behavior analysis to detect anomalies in user and entity actions)

What are logs?

- Records of events and activities within a computer system or network.
- Contain information about system and application activities.
- Serve as an audit trail for troubleshooting, security, and compliance purposes.

Computer Security Log Management:

- Process of collecting, storing, and analyzing log data to enhance security.
- Involves generating, transmitting, storing, analyzing, and disposing of logs.
- Essential for detecting security incidents and ensuring compliance.

Log Management Architecture

A log management infrastructure is typically structured into three tiers:

1. **Log Generation:**
   - Hosts that generate log data.

- May use logging client applications or services.
- Log data made available to log servers in the second tier.
- Various methods for log data transfer.

2. **Log Analysis and Storage:**
   - Log servers in the second tier.
   - Receive log data from the first tier.
   - Data transfer can be real-time or batch-based.
   - Some servers serve as collectors or aggregators.
   - Log data may be stored on log servers or separate database servers.
3. **Log Monitoring:**
   - Consoles for monitoring, reviewing, and analyzing log data.
   - May generate reports.
   - Provide management for log servers and clients.
   - User privileges can be limited to specific functions and data sources.

Log Management Planning:

- Define roles and responsibilities.
- Ensure system and network admins, incident response teams, security admins, and others contribute to log management.
- Consider auditors and procurement personnel.

Functions of Log Management Architecture:

1. **Generation**
2. **Analysis**
3. **Storage**
4. **Disposal**

Functions of Log Management Architecture:

1. **Generation:**
   - Log Parsing: Extract values from logs.
   - Event Filtering: Filter duplicate entries without altering original logs.
   - Event Aggregation: Combine multiple entries into a single entry.
2. **Storage:**
   - Log Rotation: Close and open log files, preserving entries and compressing them.
   - Log Archival: Retain logs for an extended period.
   - Log Compression: Reduce storage size without altering content.
   - Log Reduction: Remove unneeded entries.
   - Log Conversion: Convert log formats.
   - Log Normalization: Categorize data into standard formats.
   - Log File Integrity Checking: Use MD to ensure log integrity.
3. **Analysis:**
   - Event Correlation: Identify security incidents by linking related events.
   - Log Viewing: Make log data human-readable.
   - Log Reporting: Summarize analysis results.
4. **Disposal:**
   - Log Clearing: Remove old, unnecessary entries.

Log Management Planning:

- **Define Roles and Responsibilities:**

  A) System and Network Admins:

  - Responsible for configuring logging on systems, analyzing them, reporting them, and maintaining the system.

B) Incident Response Team:

- Those who use log data when handling some incidents.

C) Security Admins:

- Responsible for configuring firewalls, network-based intrusion detection, antivirus servers.

D) Application Developer:

- Customize apps to perform logging according to requirements.

E) Information security officers:

- Oversee the log management infrastructures.

F) Chief information officers (CIO):

- Oversee the IT resources that generate, transmit, and store the logs.

G) Auditors:

- Use log data when performing audits.

H) Individuals involved in the procurement of software:

- That should or can generate computer security log data.

- **Establish Logging Policies:**

  A) Log Generation

  B) Log Transmission

  C) Log Storage and Disposal

  D) Log Analysis

Log Management Operational Processes:

- Configure Log Sources
- Perform Analysis
- Initiate Responses
- Manage long-term storage

SIEM - Security Information and Event Management

A new type of centralized logging software compared to syslog. SIEM products have one or more log servers that perform log analysis, and one or more database servers that store the logs.

1. **Agentless:**
    - SIEM server receives data without special software on hosts.
    - Data retrieval: server pulls logs from hosts.
    - Data transfer: Hosts push logs to the server.
    - Authentication: Hosts authenticate to the server.
    - Server responsibilities: event filtering, aggregation, log normalization, analysis.
2. **Agent-Based:**
    - Agent program on log-generating host.
    - Event filtering, aggregation, log normalization by agents.
    - Real-time or near-real-time data transmission to the SIEM server.
    - Multiple agents may be needed for different log types.

SIEM Server Features:

- Event filtering and aggregation.
- Log normalization.
- Log analysis.
- Agentless: No host software required.
- Agent-Based: Requires agent programs on log-generating hosts.

SIEM Products Features:

- Graphical User Interfaces (GUIs) for analysts.
- Problem identification support.
- Data review capabilities.
- Security knowledge base.

- Information on known vulnerabilities.
- Customizable knowledge base.
- Incident tracking and reporting.
- Robust workflow features.
- Asset information storage.
- Correlation of asset data.
- Priority adjustments based on OS vulnerability or host importance.

---

12 COMPONENTS AND CAPABILITIES IN A SIEM ARCHITECTURE

1. **Data Aggregation:**
    - Collects and aggregates data from security systems and network devices.
2. **Threat Intelligence Feeds:**
    - Combines internal data with third-party data on threats and vulnerabilities for a comprehensive view.
3. **Correlation and Security Monitoring:**
    - Links events and related data to identify security incidents, threats, or forensic findings.
4. **Analytics:**
    - Uses statistical models and machine learning to uncover deeper relationships within data elements.
5. **Alerting:**
    - Analyzes events and generates alerts to notify security staff of immediate issues.
6. **Dashboards:**
    - Provides visualizations for reviewing event data, identifying patterns, and anomalies.
7. **Compliance:**
    - Gathers log data to meet regulatory standards (e.g., HIPAA, PCI/DSS, SOX) and generates compliance reports.

8. **Retention:**
    - Stores long-term historical data, essential for compliance and forensic investigations.
9. **Forensic Analysis:**
    - Facilitates exploration of log and event data to uncover details of security incidents.
10. **Threat Hunting:**
    - Allows security staff to proactively run queries on log and event data to discover hidden threats.
11. **Incident Response:**
    - Aids security teams in identifying and responding to security incidents by rapidly aggregating relevant data.
12. **SOC Automation:**
    - Advanced SIEMs can automatically respond to incidents by orchestrating security systems using Security Orchestration and Response (SOAR).

Splunk Key:

- 8089 - Management Port
- 9997 - Splunk Data
- 9887 - Index Replication Port
- 9777 - Search Head Cluster Port
- 8191 - KVStore Replication
- 8088 - HTTP Event Collector
- 443 / 80 / 8000 - Web Port
- 514 / custom - Syslog Port

Event Logs

Records system activities, including file actions, system changes, and security-related events.

Event Log Categories

1. **System Log:**
    - Records system-level events like system configuration changes and shutdowns.
2. **Security Log:**
    - Contains security events, such as successful and failed login attempts.
3. **Application Log:**
    - Logs events related to applications, including errors and warnings.
4. **Directory Service Log:**
    - Pertains to Active Directory events, e.g., user account changes.
5. **DNS Server Log:**
    - Specific to DNS (Domain Name System) events and issues.
6. **File Replication Service Log:**
    - Records events related to file replication and synchronization.

Types of Event Logs

1. **Information:**
    - Provides general system or application status information.
2. **Warning:**
    - Logs potential issues or events that might require attention.
3. **Error:**
    - Indicates critical errors or failures that need immediate attention.
4. **Success Audit (Security Log):**
    - Records successful security-related events, like successful logins.
5. **Failure Audit (Security Log):**

- Logs security events that failed, such as unsuccessful login attempts.

Log Format:

- **Definition:** Structure and organization of data in log files, specifying how information is presented and logged.
- **Purpose:** Enables standardized and consistent logging for easy parsing, analysis, and interpretation of log data.
- **Fields in Log Formats:**
  1. **Timestamp:** Date and time of the logged event for chronological order.
  2. **Source IP/Hostname:** Device or system's IP address or hostname that generated the log.
  3. **Event Severity/Level:** Importance/severity level (e.g., INFO, WARNING, ERROR).
  4. **Event Type/Category:** High-level classification (e.g., authentication, network, application).
  5. **Description/Message:** Detailed explanation or message of the event with context.
  6. **User/Actor:** User or entity involved in the event, identifying the source.
  7. **Source/Destination IP/Port:** IP addresses or port numbers for network events.
  8. **Protocol/Method:** Used protocol or method (e.g., HTTP, FTP, TCP).
  9. **Result/Status:** Outcome of the event (e.g., success, failure, denied).
  10. **Additional Custom Fields:** Specific data fields as needed for the environment.
- **Representation:** Log formats can be in plain text, JSON, XML, CSV, etc., chosen based on compatibility and analysis requirements.
- **Choice Factors:** Depend on the logging tool, ease of parsing, and compatibility with log management systems or SIEM platforms.

Log Baseline:

- **Definition:** Established and documented set of normal or expected log events and patterns within a system or network.
- **Purpose:** Serves as a reference point or benchmark for log analysis to identify anomalies, security incidents, or deviations from the expected behavior.

Key Elements of a Log Baseline:

1. **Log Frequency:**
    - Determine the expected frequency or rate of log events within the baseline.
    - Establish a baseline for log volume.
    - Identify significant increases or decreases in log activity.
2. **Log Anomalies:**
    - Document known anomalies or exceptions considered normal, such as specific error messages, maintenance activities, or authorized system changes.
3. **Log Types:**
    - Identify relevant log types, including those from operating systems, databases, applications, firewalls, intrusion detection systems, and other devices or services.
4. **Log Sources:**
    - Determine the specific sources of log data within the environment, such as individual devices, servers, and network devices.
5. **Log Patterns:**
    - Analyze log data to identify recurring patterns, events, and relationships between log entries.
    - Look for common timestamps, specific error codes, successful login attempts, network traffic patterns, or other indicators of normal operations.

Correlation Rules:

1. **Build Relationships Across Machine Data:**
    - Event correlation finds relationships between unrelated events from multiple sources.
    - Supports understanding which events are most relevant.
    - Can automate results for generating alerts and supporting business metrics.
2. **Time & Geolocation-Based Correlations:**
    - Identify relationships based on time and geographic proximity.
    - Visualize events over specific time periods and pinpoint their location.
    - Useful for security and operations investigations spanning different time periods.
3. **Transaction-Based Correlations:**
    - Track a series of events as a single transaction, producing a "duration."
    - Correlate events from various IT systems and data sources.
    - Summarize the grouped events in reports.
    - Transactions can involve different events from the same source, different sources from the same host, or similar events from different hosts and sources.
4. **Subsearches:**
    - Use the results of one search in another to create conditions (if/then logic).
    - Evaluate events in the context of the whole event set, including data across different indexes or Splunk servers in a distributed environment.
5. **Correlate Data with External Data Sources:**
    - Enhance, enrich, validate, or add context with structured data sources.
    - Utilizes lookup tables, which can be static CSV files, KV store collections, or Python script outputs.
    - Results of a search can be used to populate lookup tables.
6. **Joins:**

- Supports "SQL-like" inner and outer joins.
- Links one data set to another based on common fields.
- Enables viewing results from different datasets in a single view.

Security Incidents:

- Breaches threatening confidentiality, integrity, or availability of an organization's information systems or sensitive data.
- Range from intentional cyberattacks to unintentional security policy violations.
- Can lead to data breaches, system disruptions, unauthorized access, and data compromise.
- Data breaches, malware infections, denial of service attacks, insider threats, unauthorized access.
- Swift identification and response crucial to mitigate impact and protect assets and reputation.

Most Common Security Incidents:

1. **Malware Infections:**
   - Includes viruses, worms, Trojans, ransomware.
   - Malicious software compromises systems and data.
2. **Phishing Attacks:**
   - Deceptive emails, websites, or messages to steal sensitive information.
   - Often leads to identity theft and financial fraud.
3. **Insider Threats:**
   - Authorized personnel misuse access to data or systems.
   - Can be intentional or unintentional.
4. **Data Breaches:**
   - Unauthorized access or disclosure of sensitive data.
   - Resulting in data loss or theft.

5. **Denial of Service (DoS) Attacks:**
    - Overloading systems or networks to disrupt services.
    - Aims to render systems unavailable.
6. **Unauthorized Access:**
    - Gaining access without permission.
    - May involve exploiting vulnerabilities or weak passwords.
7. **Brute Force Attacks:**
    - Repeatedly trying password combinations.
    - Aims to gain unauthorized access.
8. **Web Application Attacks:**
    - Targeting vulnerabilities in web applications.
    - Includes SQL injection, cross-site scripting (XSS).
9. **Social Engineering:**
    - Manipulating individuals to disclose confidential information.
    - Includes pretexting, baiting, and tailgating.

Incident Response:

- **Definition:** Processes and technologies for detecting and responding to cyberthreats, security breaches, or cyberattacks.
- **Goal:** Prevent cyberattacks, minimize the cost and business disruption caused by attacks, and reduce the impact of security incidents.

Incident Response Plan (IRP):

- Formal plan defining how different types of cyberattacks should be identified, contained, and resolved.
- Specifies roles, responsibilities, security solutions, and incident response methodologies.

- Includes a business continuity plan for restoring critical systems and data in the event of an outage.
- Features a communications plan for informing stakeholders.
- Provides instructions for collecting and documenting incident information for post-mortem review and legal proceedings.

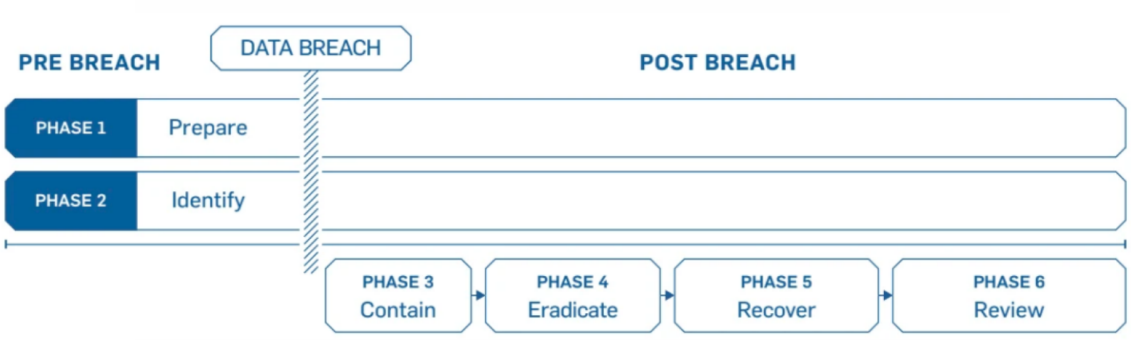
- **Purpose of Incident Response Plan:**
  - Respond to incidents systematically, following a consistent methodology.
  - Minimize loss, theft of information, and service disruptions.
  - Use gained incident information for better preparedness.
  - Address legal issues arising during incidents.

Creating an Incident Response Plan:

- **Establish a Policy:**
  - Develop an incident remediation and response policy as an evergreen document.
  - Describe general, high-level incident-handling priorities.
  - Empower incident responders and guide their decision-making during incidents.
- **Build an Incident Response Team:**
  - Establish roles and responsibilities within the incident response team.
  - Ensure team members have proper training to fulfill their roles effectively.
- **Create Playbooks:**
  - Develop playbooks outlining standardized, step-by-step actions for specific scenarios.
  - Enhance consistency, efficiency, and effectiveness in both incident response and training.
- **Create a Communication Plan:**
  - Establish a robust communication plan involving diverse stakeholders.

- Stakeholders may include the incident response team, executives, communications, legal, HR teams, customers, third-party partners, law enforcement, and the general public.

Incident Response Frameworks



1. **Preparation:**
   - Build an incident response team.
   - Create policies, processes, and playbooks.
   - Deploy tools and services to support incident response.
2. **Identification:**
   - Use IT monitoring to detect, evaluate, validate, and triage security incidents.
3. **Containment:**
   - Take steps to prevent the incident from worsening.
   - Regain control of IT resources.
4. **Eradication:**
   - Eliminate threat activity, including malware and malicious user accounts.
   - Identify vulnerabilities that attackers exploited.

5. **Recovery:**
    - Restore normal operations.
    - Mitigate relevant vulnerabilities.
6. **Lessons Learned:**
    - Review the incident to understand what happened, when, and how.
    - Identify security controls, policies, and procedures that need improvement.
    - Update the incident response plan accordingly.

Incident Response Phases:

1. **Preparation:**
    - Train employees on their incident response roles and responsibilities.
    - Develop and regularly conduct mock data breach scenarios.
    - Ensure all aspects of the incident response plan, including training and resources, are approved and funded.
    - Document roles and responsibilities.
2. **Identification:**
    - Determine if a breach or incident has occurred.
    - Assess when, how, and who discovered the incident.
    - Evaluate the impact and scope of the compromise.
    - Identify the source of the incident.
3. **Containment:**
    - Prevent the incident from spreading and causing further damage.
    - Isolate affected devices if possible.
    - Prepare short-term and long-term containment strategies.
    - Maintain redundant system backups.
4. **Eradication:**

- Find and eliminate the root cause of the breach.
- Securely remove malware.
- Harden and patch systems.
- Apply updates to ensure thorough removal.

5. **Recovery:**
    - Restore affected systems and devices.
    - Ensure the systems are patched, hardened, and tested.
    - Restore from trusted backups.
    - Monitor affected systems and implement tools for preventing future attacks.
6. **Lessons Learned:**
    - Hold an after-action meeting to analyze and document the breach.
    - Identify strengths and weaknesses in the response plan.
    - Make necessary changes to security, employee training, and system weaknesses to prevent future breaches.

Requirements of an Incident Response Plan:

1. **Mission:**
    - Define the purpose and goals of the incident response program.
2. **Strategies and Goals:**
    - Establish strategies and objectives for managing and responding to incidents.
3. **Senior Management Approval:**
    - Gain senior management support and approval for the incident response plan.
4. **Organizational Approach:**
    - Outline how the organization will approach incident response, taking into account its unique requirements, mission, size, structure, and functions.

5. **Communication:**
    - Detail how the incident response team will communicate with the rest of the organization and with external parties.
6. **Metrics:**
    - Define metrics for measuring the incident response capability and its effectiveness.
7. **Maturation Roadmap:**
    - Provide a roadmap for maturing the incident response capability over time.
8. **Integration:**
    - Explain how the incident response program fits into the overall organization and aligns with its mission and objectives.

Common Sources Of Precursors and Indicators:

1. **Network Traffic Logs:**
    - Unusual or suspicious network traffic patterns.
    - Frequent login failures.
    - Unauthorized access attempts.
2. **System Logs:**
    - Abnormal system behavior or errors.
    - Frequent system crashes or restarts.
    - Unauthorized system changes.
3. **Antivirus and Anti-Malware Alerts:**
    - Detected malware or viruses.
    - Frequent alerts indicating potential threats.
4. **Email Logs:**
    - Phishing emails or suspicious attachments.

- Unusual email patterns (e.g., mass emailing from an internal account).

5. **User Account Logs:**
    - Multiple failed login attempts.
    - User account lockouts.
    - Unauthorized access to user accounts.
6. **Web Server Logs:**
    - Unusual or malicious web traffic.
    - Web application attacks (e.g., SQL injection attempts).
7. **Firewall Logs:**
    - Blocked intrusion attempts.
    - Anomalies in traffic allowed or denied by the firewall.
8. **Intrusion Detection/Prevention System (IDS/IPS) Alerts:**
    - Detected network intrusions or suspicious activities.
    - Attacks blocked by the IDS/IPS.
9. **Security Information and Event Management (SIEM) Alerts:**
    - Aggregated alerts from various security systems.
    - Correlation of events pointing to potential incidents.
10. **Endpoint Detection and Response (EDR) Data:**
    - Suspicious activities on endpoint devices.
    - Behavior analysis and anomaly detection.

Incident Analysis:

- The incident response team should promptly analyze and validate each incident using a predefined process and document their actions.
- Perform an initial analysis to understand the incident's scope, including affected networks, systems, applications, origins, and attack methods. This

information guides subsequent actions.

1. **Profiling Networks and Systems:** Measure and understand the characteristics of expected network and system activity to detect anomalies more effectively.
2. **Understanding Normal Behaviors:** Study and document normal behavior patterns for networks, systems, and applications to recognize abnormal activities.
3. **Log Retention Policy:** Create a log retention policy specifying how long log data should be maintained to aid incident analysis and discover past incidents.
4. **Synchronize Host Clocks:** Ensure that all hosts have synchronized clocks using protocols like NTP for consistent timestamps in logs.
5. **Internet Search Engines:** Utilize internet search engines for research to find information on unusual or suspicious activities.
6. **Event Correlation:** Correlate events from multiple indicator sources to validate whether a specific incident occurred.
7. **Knowledge Base:** Maintain a knowledge base with information necessary for incident analysis, including explanations of indicators' significance and validity.
8. **Packet Sniffers:** Use packet sniffers to capture network traffic when indicators lack necessary detail for understanding ongoing incidents.
9. **Data Filtering:** Filter data to focus on the most suspicious activities, as it is not feasible to analyze all indicators.
10. **Seek Assistance:** Consult with internal or external resources, such as information security staff, US-CERT, other CSIRTs, or incident response experts, when necessary to resolve complex incidents.

Incident Damage Assessment:

- Review data to understand the incident's nature, severity, and threat origin.

- Investigate the incident thoroughly, collecting information from tools and systems, and identifying indicators of compromise (IoC).
- Quickly escalate efforts to contain and neutralize the threat using intelligence gathered during the analysis.
- Install relevant security patches, addressing malware issues and network vulnerabilities.

Cost Assessment:

- Use the Incident Cost Framework to quantify the magnitude of loss from a cyber security incident.
- Understand and measure the severity of the incident's impact on staff, departments, data, software, and hardware.
- Enhance existing processes and operations based on the assessment.
- Calculate the costs of the incident, considering hours spent, lost productivity, and reduced revenue.

Reviewing Incident Response Policy:

1. **Evaluate Existing Situation:** Assess asset vulnerability and prioritize them based on value, privacy requirements, and risk level.
2. **Establish the Incident Response Team:** Define team responsibilities, adapt to policy changes, and conduct periodic audits.
3. **Create the Incident Response Plan (IRP):** Develop a comprehensive IRP with prevention, detection, analysis, neutralization, recovery, and evaluation components.

Incident Reporting/Recording:

- **Incident reporting** involves capturing and recording incident occurrences such as injuries, property damage, or security incidents.
- It includes completing incident report forms, investigating root causes, and implementing preventive measures to avoid recurring incidents.

Initial Incident Response Steps:

Step 1: Contact Legal Counsel

- Engage legal counsel with privacy and data security expertise before an incident occurs.
- Legal counsel can advise on relevant federal and state laws, especially for data breaches.
- Provides attorney-client privilege for additional protection.

Step 2: Assemble Your Incident Response Team

- Minimum team includes IR team lead, technical leads, executive leads, legal counsel, and public relations.
- The IR team addresses the incident organization-wide.

Step 3: Determine Your Insurance Coverage

- Cyber insurance can cover costs associated with a cyber incident.
- Understand your coverage and involve legal counsel.
- Consider cyber insurance if you don't have coverage; data breaches can cost over $3 million for large companies.

Step 4: Establish a Command Center

- Set up a command center to lead and direct the incident response.
- Location for status meetings and triage; primary and backup locations should be established.
- Secure remote access is essential.

Step 5: Invoke the Emergency Communications Plan

- The plan outlines roles, responsibilities, procedures, and protocols for prompt information sharing.
- Ensures accurate and timely communication; avoid premature announcements.

Step 6: Setup a Recurring Status Meeting

- Establish daily recurring meetings to keep stakeholders informed about the incident's status.

- Communication can be in person or via remote technology.

Beyond Step 6: Follow the Typical Incident Response Procedure

- Beyond the initial steps, follow a typical incident response procedure, including containment, eradication, recovery, and lessons learned.

Conclusion:

- These steps are essential after discovering a critical cyber incident.
- Preparation ahead of time, like acquiring cyber insurance, identifying a command center, and establishing relationships with legal counsel and incident response professionals, is crucial.

Formulating an Effective Response Strategy in Incident Response

1. Preparation:

- Create an incident response team with defined roles and training.
- Prepare for various incident types, such as data breaches and malware infections.

2. Identification and Detection:

- Develop processes and tools for prompt incident identification.
- Use intrusion detection systems, network monitoring, and SIEM solutions.

3. Classification and Prioritization:

- Categorize incidents based on impact and severity.
- Prioritize to allocate resources effectively.

4. Containment:

- Outline measures to prevent the incident from spreading.
- Isolate affected systems or disconnect them from the network.

5. Eradication:

- Focus on eliminating the root cause of the incident.
- Analyze how the incident occurred and remove malicious elements.

6. Recovery:

- Plan for system and service restoration.
- Include data recovery, patching, and addressing vulnerabilities.

7. Communication:

- Establish clear channels for internal and external stakeholders.
- Maintain transparency for trust and compliance.

8. Legal and Regulatory Compliance:

- Ensure compliance with legal and regulatory requirements.
- Address data breach notification laws.

9. Documentation:

- Keep thorough records of the incident, actions taken, and lessons learned.
- Valuable for post-incident analysis and future improvement.

In summary, an effective response strategy involves proactive planning, preparation, detection, containment, recovery, and ongoing improvement. It is essential for organizations to respond effectively to security incidents and minimize their impact.

Incident Classification in IR

- **Severity:** Categorize by impact:
  - Low: Minimal or no immediate impact.
  - Medium: Moderate impact needing attention.
  - High: Significant impact requiring immediate action.
  - Critical: Severe and potentially catastrophic impact.

- **Type:** Categorize by nature:

    - e.g., malware infections, data breaches, insider threats.

- **Scope:** Define the affected extent:
    - Localized (specific systems/departments).
    - Widespread (multiple areas).
    - Enterprise-wide (whole organization).

- **Attack Vector:** Categorize based on the attack method:
    - e.g., phishing, software vulnerabilities, insider threats.

- **Compliance and Regulatory Impact:** Consider legal impact:
    - Essential for data protection and privacy compliance.

- **Repeat or Persistent Incidents:** Differentiate between:
    - Isolated incidents.
    - Persistent threats.

- **Attribution:** Identify the threat actor:
    - Often challenging.

- **False Positives:** Initially considered security incidents but later deemed benign.

- **Impact on Critical Assets:** Assess effect on sensitive data, intellectual property, and infrastructure.

- **Customer or Stakeholder Impact:** Evaluate repercussions on customers, partners, and stakeholders.

- **Response Priority:** Assign priorities based on classification:
  - Critical incidents require immediate attention.

Data Collection in IR

1. **Evidence Gathering:**
   - Collect digital evidence.
   - Includes logs, system files, network data, memory dumps.
   - Provides insights into incident timeline and threat actor tactics.
2. **Data Preservation:**
   - Preserve data in original, unaltered state.
   - Maintain evidence integrity and chain of custody.
3. **Logs and Records:**
   - Review and gather logs from various sources.
   - Firewalls, intrusion detection, authentication logs.
   - Reveal unusual or malicious activities.
4. **System Artifacts:**
   - Analyze file system metadata, registry entries, event logs.
   - Identify threat actor changes to files and settings.
5. **Memory Forensics:**
   - Examine volatile memory (RAM) for signs of malware.
   - Use tools like Volatility.
6. **Network Traffic Analysis:**
   - Capture and analyze network traffic.
   - Identify communication patterns, command traffic, data exfiltration.
7. **Malware Analysis:**

- Collect suspected malware for analysis.
- Includes executable files, scripts, or malicious documents.

8. **User and Account Activity:**
    - Review logs for unauthorized access or suspicious behavior.
    - Detect unusual login or access patterns.
9. **Endpoint Data:**
    - Gather data from affected endpoints (e.g., desktops, servers).
    - Understand incident impact and gather forensic evidence.
10. **External Threat Intelligence:**
    - Collect external threat intelligence from sources.
    - Gain insights into the threat landscape and potential IOCs.
11. **Physical Evidence (if applicable):**
    - Consider physical evidence such as security camera footage, access logs, or hardware components.

Forensic Analysis in IR

1. **Evidence Preservation:**
    - Maintain evidence integrity for legal proceedings.
    - Create forensic copies (forensic images) to prevent tampering.
2. **Timeline Reconstruction:**
    - Create a detailed event timeline.
    - Understand incident progression and attacker actions.
3. **Root Cause Analysis:**
    - Identify vulnerabilities or weaknesses.
    - Implement security controls to prevent future incidents.
4. **Malware Analysis:**
    - Analyze malware functionality, capabilities, and infection vector.

- Create malware signatures and identify IOCs.

5. **Data Recovery:**
   - Attempt data recovery, especially in data breaches or manipulation incidents.
6. **Forensic Artifacts Examination:**
   - Analyze digital artifacts, including logs, system files, registry entries, and event logs.
   - Gain insights into attacker activities.
7. **Memory Forensics:**
   - Examine volatile memory (RAM) for running processes and artifacts.
8. **Network Forensics:**
   - Analyze network traffic for communication patterns, command channels, and data exfiltration.
9. **User and Account Activity Analysis:**
   - Review logs for unauthorized access, privilege escalation, or suspicious behavior.
10. **Documentation:**
    - Document analysis activities, tools, findings, and conclusions.
11. **Chain of Custody:**
    - Maintain a chain of custody for collected evidence.

Evidence Protection in IR

1. **Chain of Custody:**
   - Maintain a clear chain of custody for all collected evidence.
   - Document handling and movement from collection to court presentation.
   - Ensure tamper-free and reliable evidence.
2. **Forensic Imaging:**

- Create forensic images (exact copies) of digital evidence using write-blocking tools.
- Preserve original data without alteration.

3. **Access Control:**
    - Limit evidence access to authorized personnel.
    - Implement access controls, permissions, and encryption as needed.
4. **Physical Security:**
    - Secure physical evidence in a controlled, locked environment.
    - Maintain access records for physical evidence.
5. **Documentation:**
    - Thoroughly document all actions related to evidence.
    - Include date, time, individuals involved, and purpose in the documentation.
6. **Hashing and Digital Signatures:**
    - Calculate cryptographic hashes (e.g., MD5, SHA-256) for file integrity.
    - Consider digital signatures to enhance authenticity.
7. **Write-Protect Media:**
    - Ensure storage media is write-protected to prevent alterations.
    - Use write-blocking devices or software.
8. **Network Traffic Capture:**
    - Store network traffic data securely with proper access controls.
    - Maintain timestamps and original format.
9. **Cloud-Based Evidence:**
    - Apply access controls and audit trails for cloud-stored evidence.
    - Follow cloud service provider guidelines for collection and preservation.
10. **Legal Considerations:**
    - Adhere to legal and regulatory requirements for evidence preservation.
    - Consult with legal counsel for compliance with evidence-related laws.
11. **Regular Backups:**

- Back up evidence regularly to prevent loss due to hardware failures or data corruption.
- Protect and maintain backups with the same care as the original evidence.

12. **Retention Policies:**
    - Establish evidence retention policies specifying how long evidence should be retained.
    - Properly dispose of evidence when no longer needed.
13. **Training and Awareness:**
    - Train incident response team members in evidence protection best practices.
    - Raise awareness about the importance of maintaining evidence integrity.

Notifying External Agencies in IR

1. **Legal and Regulatory Obligations:**
    - Comply with industry and jurisdiction-specific legal and regulatory requirements.
    - Report certain incident types based on legal mandates (e.g., data breach notification laws).
2. **Law Enforcement:**
    - Notify law enforcement agencies in cases of cybercrime.
    - Seek assistance from local police, cybercrime units, or federal agencies (e.g., FBI) for investigations and potential prosecutions.
3. **Governmental or Regulatory Bodies:**
    - Report incidents to relevant governmental or regulatory bodies based on the nature of the incident and industry.
    - Financial institutions may report to financial regulators, for example.
4. **ISACs (Information Sharing and Analysis Centers):**

- Share incident information with ISACs to support industry-specific threat information sharing and best practices.

5. **Cybersecurity Incident Response Teams (CIRTs):**
    - Seek guidance and coordination from government-established CIRTs during significant cyber incidents.
6. **Public Relations and Communication Agencies:**
    - Involve public relations or communication agencies for managing public messaging and reputation during large-scale incidents.
7. **Legal Counsel:**
    - Consult with legal counsel to ensure compliance with laws and regulations.
    - Legal advice guides decisions on whom to notify and the content of notifications.
8. **Insurance Providers:**
    - Notify cybersecurity insurance providers about the incident if coverage is applicable.
    - Timely notification may be a requirement for coverage.
9. **Affected Third Parties:**
    - Notify third-party organizations or partners if their data or systems are compromised in the incident.
    - Allow them to take security measures to protect their interests.
10. **Customers and Users:**
    - Depending on incident nature and applicable laws, notify affected customers or users about the incident.
    - Transparency is crucial for maintaining trust.

Important Considerations:

- Provide accurate, relevant information while maintaining confidentiality.
- Follow established incident response and notification procedures.
- Balance the legal, regulatory, and public safety aspects of notifications.

Systems Recovery in Incident Response

1. **Assessment of Damage:**
    - Assess the extent of damage or compromise to affected systems.
    - Determine the scope and priority of recovery efforts based on the assessment.
2. **Isolation and Containment:**
    - Isolate affected systems from the network to prevent further damage and unauthorized access.
    - Maintain containment measures from the initial response phase during recovery.
3. **Data Backup and Restoration:**
    - Restore data from available, unaffected backups.
    - Prioritize data restoration, focusing on critical systems and data.
4. **System Reimaging or Reinstallation:**
    - Reimage or reinstall systems that are impractical or risky to clean.
    - Restore systems to a known, clean state.
5. **Patch and Remediation:**
    - Apply patches, updates, and security fixes to address exploited vulnerabilities.
    - Ensure systems are up-to-date and securely configured.
6. **Verification:**
    - Test and verify the integrity of recovered systems.
    - Check for residual malicious activity to ensure systems are free from malware.
7. **Change Control:**
    - Implement change control procedures to monitor and document all changes made to systems during recovery.
    - Maintain a clear audit trail and prevent unauthorized changes.

8. **Business Continuity and Redundancy:**
    - Utilize business continuity plans and redundancy mechanisms to ensure critical systems and services' availability.
    - Shift operations to redundant systems when needed.
9. **Communication:**
    - Keep stakeholders informed about recovery progress, including employees, customers, partners, and relevant authorities.
    - Maintain transparent communication for trust preservation.
10. **Monitoring:**
    - Continuously monitor recovered systems for signs of suspicious activity or incident recurrence.
    - Promptly respond to any anomalies detected.
11. **Lessons Learned:**
    - Conduct a post-incident review to analyze the recovery process.
    - Identify areas for improvement and update the incident response plan and security measures.
12. **Documentation:**
    - Maintain detailed documentation of recovery efforts, including actions, system changes, and testing results.
    - Valuable for post-incident analysis and reporting.

- Systems recovery is crucial for minimizing downtime and mitigating incident impact.
- Effective recovery planning and procedures enhance an organization's resilience against security incidents and minimize their impact on operations and reputation.

Review and Update Response Policies in an Incident Response Plan (IRP)

1. **Regular Review Schedule:**

- Establish a routine review schedule for response policies.
- Frequency may vary based on industry, regulations, and evolving threat landscape.

2. **Incident Trends and Analysis:**
    - Analyze past incidents to identify trends, lessons, and areas for improvement.
    - Understand unique risks and vulnerabilities specific to the organization.
3. **External Threat Landscape:**
    - Stay informed about the external threat landscape through cybersecurity news, threat intelligence reports, and industry developments.
    - Understand emerging threats and attack vectors.
4. **Regulatory Changes:**
    - Stay updated on changes in relevant laws and regulations, especially those related to data protection, privacy, and incident reporting.
    - Ensure policy compliance with legal obligations.
5. **Technology Updates:**
    - Evaluate the technology stack for necessary changes or upgrades to enhance incident detection, prevention, and response.
    - Consider new security tools or updates to existing ones.
6. **Personnel and Roles:**
    - Review roles and responsibilities of the incident response team.
    - Ensure personnel have the required skills and training.
    - Adjust team compositions and contact lists as needed.
7. **Incident Classification and Prioritization:**
    - Reassess criteria for incident classification and prioritization.
    - Adapt to evolving risks and business priorities.
8. **Communication and Notification Procedures:**
    - Update communication and notification procedures to reflect changes in contact information, roles, and communication channels.

9. **Containment and Eradication Strategies:**
    - Review and enhance strategies for threat containment and eradication.
    - Consider improvements in isolation, system recovery, and vulnerability patching.
10. **Testing and Tabletop Exercises:**
    - Conduct tabletop exercises and simulations to test the effectiveness of response policies and procedures.
    - Identify weaknesses and areas requiring adjustments.
11. **Documentation and Reporting:**
    - Ensure policies for documenting and reporting incidents align with best practices and legal requirements.
    - Include provisions for evidence preservation, reporting to authorities, and post-incident analysis.
12. **Business Continuity and Redundancy:**
    - Evaluate and update business continuity and redundancy plans to minimize incident impact on critical operations.
13. **Training and Awareness:**
    - Provide ongoing training and awareness programs to educate employees and incident response team members on policy updates and best practices.
14. **Incident Escalation Procedures:**
    - Review and update procedures for escalating incidents to higher management levels or external authorities as necessary.
15. **Documentation Retention:**
    - Define the retention period for incident-related documentation, considering legal requirements and specific organizational needs.
16. **Policy Accessibility:**
    - Ensure all incident response team members have easy access to updated policies and procedures.
    - Consider using a centralized document repository or incident response platform.

What is Splunk?

- Splunk is advanced software for organizations.
- It indexes and searches log files.
- Analyzes machine-generated data in real-time.
- Utilizes a web-style interface.
- Captures, indexes, and correlates real-time data.
- Presents data through graphs, reports, alerts, dashboards, and visualizations.
- Offers solutions to business problems.

Splunk is a powerful tool for real-time data analysis, beneficial for security, IT operations, compliance, and business analytics. It aids organizations in managing and gaining insights from extensive data sources.

Splunk Architecture:

1. **Universal Forwarder (UF):**
   - Lightweight component.
   - Collects and forwards log data to the Heavy Forwarder.
   - Installed on client-side or application-side servers.
2. **Load Balancer (LB):**
   - Distributes workloads and application traffic across a cluster of servers.
   - Optimizes resource utilization and improves system performance.
3. **Heavy Forwarder (HF):**
   - Heavy component that filters collected data.
   - Responsible for collecting error logs.
   - Serves as an intermediary between the Universal Forwarder and Indexer.
4. **Indexer:**

- Stores and indexes the filtered log data.
- Enhances Splunk's performance and manages indexing automatically.

5. **Search Head (SH):**
    - Distributes searches to other indexers.
    - Provides intelligence and reporting capabilities.
    - Supports search and data analysis.
6. **Deployment Server (DS):**
    - Facilitates sharing of data between components.
    - Manages deployment configurations, including updates to UF configuration files.
7. **License Master (LM):**
    - Controls license distribution.
    - Manages licensing based on quality and usage.

Splunk Workflow:

1. **Data Collection:**
    - Universal Forwarder collects log data.
    - Data is forwarded to the Heavy Forwarder.
    - Load Balancer may distribute data flows.
2. **Data Processing:**
    - Heavy Forwarder filters and processes data.
    - Filtered data is forwarded to Indexers.
    - Indexers store and index the data for efficient retrieval.
3. **Data Search and Analysis:**
    - Search Head handles search and data analysis.
    - Searches can be distributed across multiple indexers.
    - Users access, analyze, and visualize data to gain insights.

Versions of Splunk:

- **Splunk Enterprise:**
  - Paid version with unlimited access for IT businesses.
  - Supports single and multi-site clustering for disaster recovery.
  - Gathers and analyzes data from websites, applications, and more.
- **Splunk Cloud:**
  - Hosted platform offered as a service with subscription pricing.
  - Similar features to Splunk Enterprise.
  - Clustering is managed by Splunk.
- **Splunk Light:**
  - Free version with up to 500MB indexing per day.
  - Limited features and functionalities.
  - Supports a single instance and is ideal for small-scale use.

Analyzing Live Malware Traffic Samples in SIEM:

1. **Data Collection and Integration:**
   - Configure the SIEM to collect network traffic data from various sources, such as firewalls, network appliances, IDS, and taps.
2. **Data Normalization:**
   - Normalize and enrich network traffic data to a standardized format, converting raw data into a SIEM-friendly structure.
3. **Traffic Aggregation:**
   - Create meaningful data sets by aggregating network traffic based on time intervals, source/destination IP addresses, or network segments.
4. **Alerting Rules:**
   - Establish alerting rules in the SIEM to detect known malware indicators, including IP addresses, domains, and file hashes linked to malicious

activities. Utilize threat intelligence feeds and maintain an indicator of compromise (IOC) list.

5. **Anomaly Detection:**
    - Configure the SIEM to perform anomaly detection on network traffic. Set baselines for normal behavior and trigger alerts when deviations occur, identifying potential zero-day or unknown threats.
6. **Behavioral Analytics:**
    - Implement behavioral analytics within the SIEM to detect unusual or malicious behavior patterns, such as data exfiltration, lateral movement, or privilege escalation.
7. **Packet Capture and Storage:**
    - Integrate the SIEM with packet capture solutions to capture and store packet-level data for suspicious traffic flows, enabling in-depth analysis.
8. **Deep Packet Inspection (DPI):**
    - If supported, use DPI for deeper packet content analysis, inspecting payload contents for indicators like malicious URLs, filenames, or payload encryption.
9. **Traffic Visualization:**
    - Utilize traffic visualization tools and dashboards in the SIEM to gain a visual representation of network traffic patterns, aiding quick anomaly identification.
10. **Correlation and Contextual Analysis:**
    - Correlate network traffic data with other security events and logs within the SIEM to understand the full scope of an incident.
11. **Incident Triage:**
    - Initiate an incident response process when an alert triggers. Triage the incident to assess severity and impact.
12. **Threat Hunting:**
    - Proactively hunt for threats using custom queries and searches in the SIEM based on the latest threat intelligence to identify dormant or stealthy malware.
13. **Reporting and Documentation:**

- Generate reports and documentation for each incident, outlining malware behavior, affected systems, and remediation steps.

14. **Post-Incident Analysis:**
    - After mitigating the threat, perform a post-incident analysis to identify gaps in security controls and adjust SIEM configurations and alerting rules accordingly.

Security Advisories:

- **Purpose:** Notify customers about discovered security vulnerabilities.
- **Vulnerability:** Software bugs exploitable by malicious users.
- **Common Vulnerabilities:** E.g., Cross-Site Scripting (XSS) flaws.

Components:

1. **Notification:** Inform customers of the vulnerability.
2. **Description:** Detail the flaw and its impact.
3. **Affected Versions:** Specify vulnerable product versions.
4. **Risk Assessment:** Explain potential risks.
5. **Remediation:** Guide customers to fix the issue.
6. **Preventive Measures:** Suggest risk mitigation.
7. **Acknowledgment:** Credit the reporter.
8. **Publication Date:** Include the release date.

Writing Security Advisories:

- A security advisory is a document that informs customers about a security vulnerability in a product and provides guidance on how to address the issue.

Components of a Security Advisory:

1. **Vulnerability Type:**

- Classify the vulnerability (e.g., XSS, XSRF, privilege escalation).

2. **Severity:**
    - Rate the potential impact and ease of exploitation (critical, high, moderate, low).
3. **Risk Assessment:**
    - Describe the data a hacker could access, worst-case scenario, and at-risk deployment scenarios.
4. **Vulnerability:**
    - Specify the affected area of the application, vulnerable versions, and tracking links.
5. **Risk Mitigation:**
    - Advise customers on actions to minimize exposure to attacks, especially if an immediate upgrade is not possible.
6. **Fix:**
    - Provide instructions for a permanent fix, often recommending upgrading to the latest version and applying patches if available.
7. **Acknowledgment of Reporter:**
    - Recognize the person who reported the vulnerability if they wish to be acknowledged.

Advance Warning:

- Mention the approximate release date for the advisory and fix.
- Describe the type of security flaw, its severity, and a generic risk assessment.
- Offer advice on how to prepare for the advisory and fix, including mitigation strategies.

User and Entity Behavior Analytics (UEBA):

- **Definition:** UEBA is a cybersecurity solution using algorithms and machine learning.
- **Purpose:** Detect anomalies in user and network behavior.
- **Behavior Analysis:** Monitors users, routers, servers, and endpoints.
- **Anomalies:** Identifies unusual or suspicious actions deviating from normal patterns.
- **Example:** UEBA detects significant changes like excessive file downloads.

Components:

1. Deployment on every device.
2. Learning Mode: Gathers data and defines normal behavior.
3. Testing Mode: Evaluates and identifies anomalies.

Key Components:

1. **Data Collection:** Collects user and entity behavior data.
2. **Analytics:** Builds profiles, creates statistical models, and detects unusual behavior.
3. **Integration:** Interfaces with existing security products.
4. **Presentation:** Communicates findings and may trigger automated actions.
5. **Alerts:** Notifies IT administrators or takes immediate action.

AI in SIEM Detection:

- **AI in SIEM:** Utilizes machine learning, threat feeds, and user behavior analytics.
- **Purpose:** Detects abnormal and risky activities, automating threat hunting.
- **Adaptability:** AI can be used in various SIEM functions.
- **Benefits:** Enhances data analysis, vulnerability management, and threat response.

- **AIOps:** The integration of AI and Machine Learning in SIEM with predictive analytics.

Machine Learning Algorithms in SIEM:

1. **Detecting Users' Deviation from Themselves:**
    - Abnormal increase in user activity.
    - Deviation in specific user activities.
    - Changes in user's risk posture.
    - Abnormal rate of increase in risky activity.
    - Deviation in local to remote activity.
    - Changes in user's systems or software installations.
2. **Detecting Change in User's Activity vs. Frequency:**
    - Activity and frequency distribution model.
    - Flags anomalies when user activity or frequency deviates from predictions.
    - Detects compromised credentials or behavior changes.
3. **Anomalous Deviation from Peer Groups:**
    - Creates behavioral clusters of similar users.
    - Identifies anomalies when a user deviates from peer groups.
    - Helps in prioritizing users and responding to insider threats.

Thanks for reading my notes! I hope it was helpful in your learning curve. For more such content follow me on my GitHub and Twitter :)

GitHub:

cyph3rryx - Overview

21 y/o 😁 • Cybersecurity Student💫 • CTF & Bug Bounty 👾• Security Researcher 🪲 • Screenwriter 😉• Nerd 😎 • Top 2% on TryHackMe (New Ranking System) 😌 - cyph3rryx

https://github.com/cyph3rryx

Twitter:

Ryx (@PadhiyarRushi) / X

21 y/o • Cybersecurity Student • CTF & Bug Bounty • Security Researcher • Screenwriter • Graphic Designer • In Top 2% @RealTryHackMe

https://twitter.com/PadhiyarRushi