DFIR
DIGITAL FORENSICS
AND INCIDENT RESPONSE

BLUE TEAM: SOC

PART - I

“SIEM” in Threat Hunting

BY,

Asif Khan

Sr. Cyber Forensics Expert

HTTPS://WWW.LINKEDIN.COM/IN/ASIF-KHAN-B5379A126/

SIEM in Threat Hunting

Security Information and Event Management (SIEM) systems are foundational tools in modern threat hunting. They aggregate logs, correlate events, and provide contextual insights into security incidents across an organization's IT infrastructure. Below is an in-depth explanation of SIEM's key functions in threat hunting with detailed examples.

Index:

1. Log Aggregation and Centralized Visibility

SIEM collects logs and events from multiple sources like firewalls, servers, endpoints, IDS/IPS, routers, and applications to provide a single pane of glass for monitoring.

Examples:

- **Firewall Logs**:
  Detect blocked outbound traffic to suspicious IPs, indicating possible malware beaconing.
  Example: Frequent outbound traffic to a known C2 (Command and Control) server could be a sign of a compromised host.
- **Server Logs**:
  Track administrative actions such as user creation, password changes, or privilege escalation.

Example: An unusual admin account created during non-working hours could suggest unauthorized activity.

- **Application Logs**:
  Monitor critical business applications like SAP, Salesforce, or custom apps.
  Example: Multiple failed login attempts on a critical application might signal a brute-force attack.

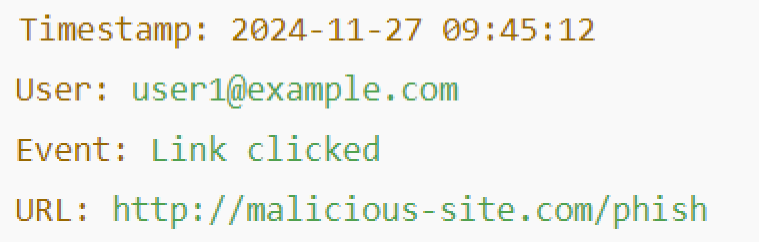
Real-Life Scenario:

A SIEM like Splunk or QRadar aggregates logs from network firewalls and detects multiple connection attempts to a disallowed port. This leads the hunter to identify an attacker scanning for open ports in the network.

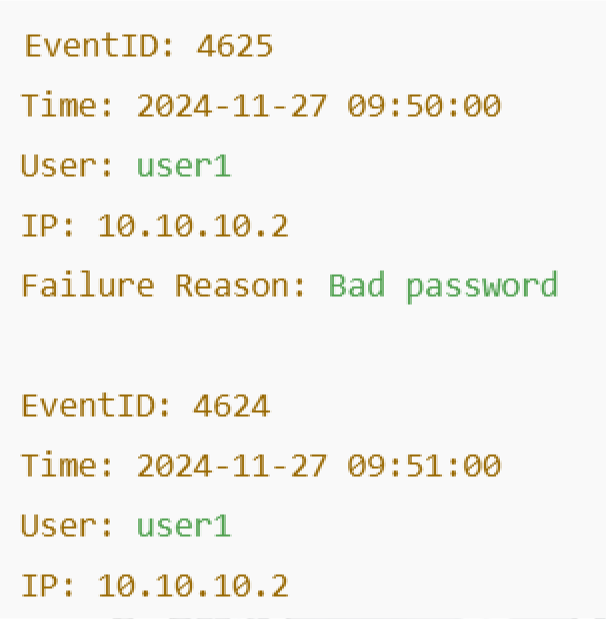
Example Use Case: Detecting Lateral Movement

Scenario:

An attacker compromises a user's credentials via phishing, escalates privileges, and moves laterally within the network to access sensitive resources.

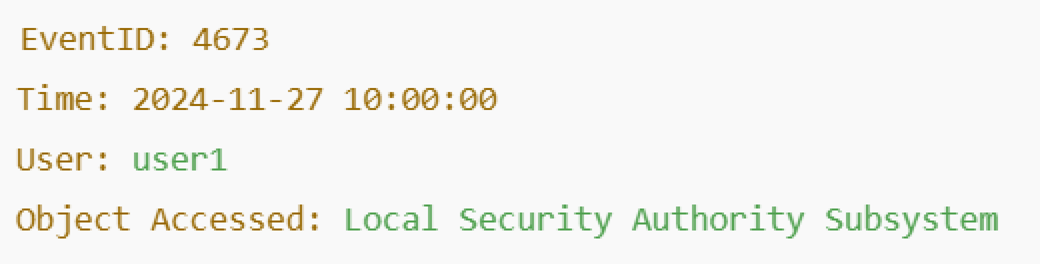
1. **Initial Event (Compromise Detection)**:
   - Log Source: Email Security Gateway
   - Event: A phishing email containing a malicious link clicked by "user1."
   - Example Log Entry:
   - 

     ```
     Timestamp: 2024-11-27 09:45:12
     User: user1@example.com
     Event: Link clicked
     URL: http://malicious-site.com/phish
     ```
2. **Credential Theft**:
   - Log Source: Windows Event Logs (Domain Controller)
   - Event: Multiple failed login attempts (Event ID 4625), followed by a successful login (Event ID 4624).
   - Example Log Entries:

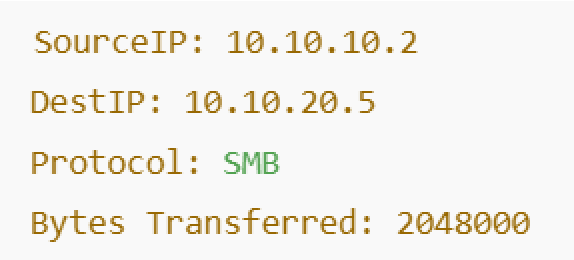
- 

```
EventID: 4625
Time: 2024-11-27 09:50:00
User: user1
IP: 10.10.10.2
Failure Reason: Bad password

EventID: 4624
Time: 2024-11-27 09:51:00
User: user1
IP: 10.10.10.2
```

3. **Privilege Escalation**:
    - Log Source: Windows Security Logs
    - Event: Sensitive privilege escalation attempt (Event ID 4673).
    - Example Log Entry:
    - 

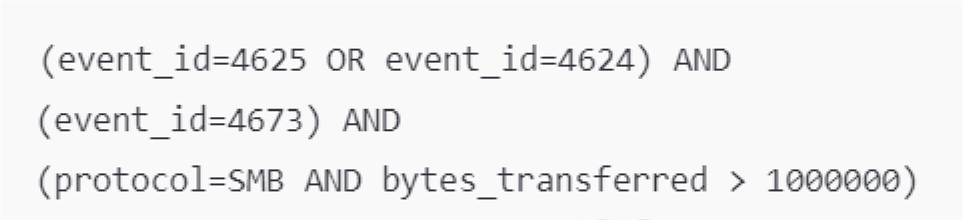
```
EventID: 4673
Time: 2024-11-27 10:00:00
User: user1
Object Accessed: Local Security Authority Subsystem
```

4. **Lateral Movement**:
    - Log Source: Network Logs (Firewalls or IDS)
    - Event: SMB (Server Message Block) traffic spikes originating from the compromised user’s workstation, targeting other hosts.
    - Example Log Entry:
    - 

```
SourceIP: 10.10.10.2
DestIP: 10.10.20.5
Protocol: SMB
Bytes Transferred: 2048000
```

SIEM Correlation Rule:

A rule in Splunk or QRadar to detect this behavior might look like:



```
(event_id=4625 OR event_id=4624) AND
(event_id=4673) AND
(protocol=SMB AND bytes_transferred > 1000000)
```

Alert Workflow:

- **Trigger**: SIEM detects multiple login failures followed by privilege escalation and unusual network activity.
- **Action**: Generate an alert with details of affected hosts and initiate automated playbook:
    1. Isolate the compromised endpoint.
    2. Notify the SOC team.
    3. Collect forensic data for deeper analysis.

Technical Benefits:

- Detects **multi-stage attacks** that individual systems might miss.
- Provides a timeline of the attack for forensic investigation.
- Automates the response to reduce mean time to detect (MTTD) and respond (MTTR).

2. Event Correlation

SIEM correlates logs and events from various systems to detect patterns of malicious behavior that individual logs might not reveal. Correlation rules can help identify multi-stage attacks.

Examples:

- **Correlation Rule**: Multiple failed login attempts followed by a successful login and unusual data transfer volumes.
  Detection: Indicates a possible brute-force attack followed by data exfiltration.
  Example: A SIEM correlates logs from an Active Directory (AD) server and a file server. If a

user logs in at midnight and uploads 10 GB of sensitive files, it could signal an insider threat or compromised credentials.

- **Phishing Campaign Detection**:
  Email gateway logs indicate several emails with suspicious attachments, while endpoint logs detect PowerShell activity post-click. Correlating these events can highlight a targeted phishing campaign.

Real-Life Scenario:

A SIEM like ArcSight identifies a pattern: an external IP sends a phishing email, a user clicks the attachment, and malicious PowerShell commands are executed on the endpoint. The correlation rule alerts the security team.

How Correlation Works

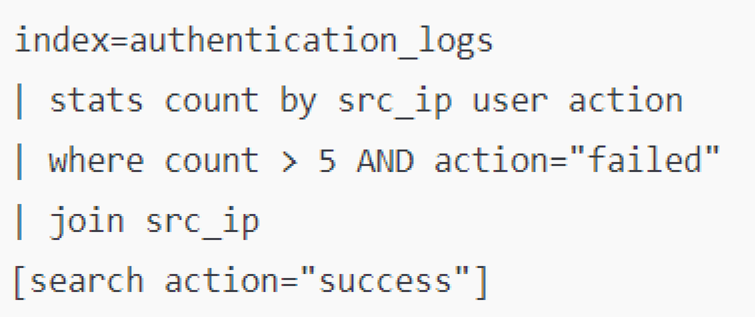
1. **Event Collection**:
   - Logs are collected from multiple sources: firewalls, endpoints, IDS/IPS, web servers, databases, and applications.
2. **Normalization**:
   - Events are parsed into a consistent schema, making fields like src_ip, dest_ip, user, and action accessible for analysis.
3. **Correlation Rules**:
   - SIEM platforms apply predefined or custom rules to detect patterns.
   - Example: A rule may track failed login attempts, followed by a successful login, to identify brute-force attacks.
4. **Alert Generation**:
   - If a rule condition is met, an alert is triggered, often enriched with contextual information for further analysis.

Key Components of Event Correlation

- **Event Aggregation**: Combine events from the same source over time (e.g., multiple login attempts from one IP).
- **Cross-source Correlation**: Link events from different systems to identify broader attack patterns (e.g., a failed login followed by privilege escalation on another system).
- **Temporal Context**: Define time windows for event correlation to limit noise (e.g., 10 failed logins within 5 minutes).

Technical Workflow Example: Detecting Brute-force Attack

1. **Log Sources**:
   - Firewall (e.g., Palo Alto logs failed SSH connections).
   - Authentication server (e.g., Microsoft AD logs failed login attempts).
2. **Rule Configuration**:
   - **Rule Name**: Brute Force Detection
   - **Condition**:
     - 5 failed login attempts from the same source IP within 10 minutes.
     - Followed by a successful login from the same IP.
   - **Implementation**:
     - In Splunk:



```
index=authentication_logs
| stats count by src_ip user action
| where count > 5 AND action="failed"
| join src_ip
[search action="success"]
```

     - In Elastic SIEM:
       - Use KQL to define the rule:

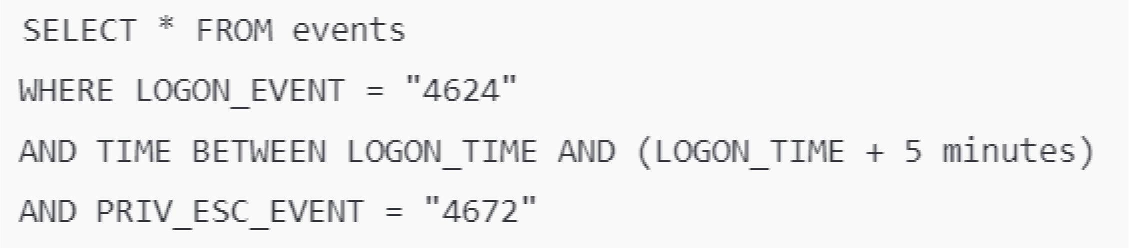
>> authentication.action: "failed" and event.count >= 5 and authentication.source_ip: * followed_by authentication.action: "success"

3. **Example Output**:
   - src_ip: 192.168.1.10
   - user: admin
   - **Pattern**: 5 failed logins followed by success.
4. **Generated Alert**:

- Description: "Potential brute-force attack detected. Successful login after multiple failures."
- Severity: High.

Advanced Use Case: Detecting Privilege Escalation

1. **Scenario**:
    - An attacker logs into a server and elevates privileges to execute unauthorized tasks.
2. **Log Sources**:
    - Windows Security Logs:
        - Event ID 4672: Special privileges assigned to new logon.
    - Linux Audit Logs:
        - sudo command execution.
3. **Correlation Rule**:
    - **Condition**:
        - A login event (e.g., Windows Event ID 4624) followed by privilege escalation within 5 minutes.
    - **Implementation**:
        - In QRadar:
            - Use AQL to define:



```
SELECT * FROM events
WHERE LOGON_EVENT = "4624"
AND TIME BETWEEN LOGON_TIME AND (LOGON_TIME + 5 minutes)
AND PRIV_ESC_EVENT = "4672"
```

- In Graylog:
    - Define pipeline rules to match login and privilege escalation events.

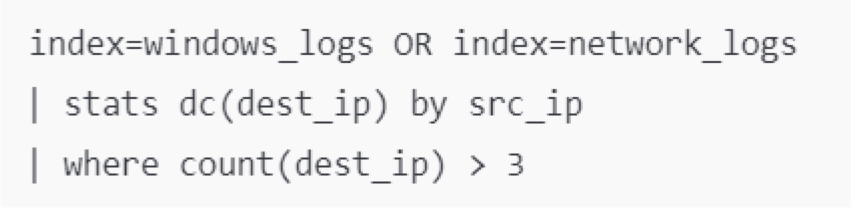
4. **Example Output**:
    - Log 1:

        - Timestamp: 2024-11-27 10:30:00
        - Event: Login Success (ID 4624)
        - User: Alice
    - Log 2:
        - Timestamp: 2024-11-27 10:33:00
        - Event: Privilege Escalation (ID 4672)
        - User: Alice
    - Correlation: Alice logged in and elevated privileges within 3 minutes.

5. **Alert**:
    - Description: "Unusual privilege escalation detected after login. User: Alice."
    - Severity: Critical.

Real-world Example: Lateral Movement Detection

1. **Scenario**:
    - An attacker gains access to one system and attempts to move laterally by authenticating against other systems using stolen credentials.
2. **Log Sources**:
    - Endpoint logs (Windows Event ID 4624: Successful Logon).
    - Network logs (SSH traffic logs).
    - File server logs (access attempts).
3. **Correlation Rule**:
    - **Condition**:
        - Successful login attempts on multiple systems from the same source IP.
    - **Implementation**:
        - In Splunk:



```
index=windows_logs OR index=network_logs
| stats dc(dest_ip) by src_ip
| where count(dest_ip) > 3
```

4. **Example Output**:
    - Source IP: 192.168.1.15
    - Target Systems: Server1, Server2, Server3.
5. **Alert**:
    - Description: "Potential lateral movement detected. Source IP accessed multiple systems."
    - Severity: High.

Integration with Machine Learning for Correlation

- **Scenario**: Detecting anomalies across correlated events.
- **Implementation**:
    - ML models are trained on normal traffic patterns.
    - Deviation in correlated events (e.g., an unusual sequence of login, file access, and data transfer events) triggers alerts.
- **Example Tool**: Elastic SIEM with ML.

3. Threat Intelligence Integration

SIEM tools integrate with external and internal threat intelligence feeds to enrich event data. This allows for the identification of known Indicators of Compromise (IOCs) such as malicious IPs, domains, or file hashes.

Examples:

- **Malicious IPs**:
  Firewall logs show outbound traffic to IPs flagged in a threat intelligence feed.
  Example: An endpoint communicating with an IP associated with a botnet like Mirai.
- **File Hashes**:
  Logs from antivirus or endpoint solutions include file hashes that match known malware samples.
  Example: A SIEM receives a hash alert from an EDR tool (e.g., CrowdStrike Falcon), correlates it with recent network activity, and detects lateral movement.

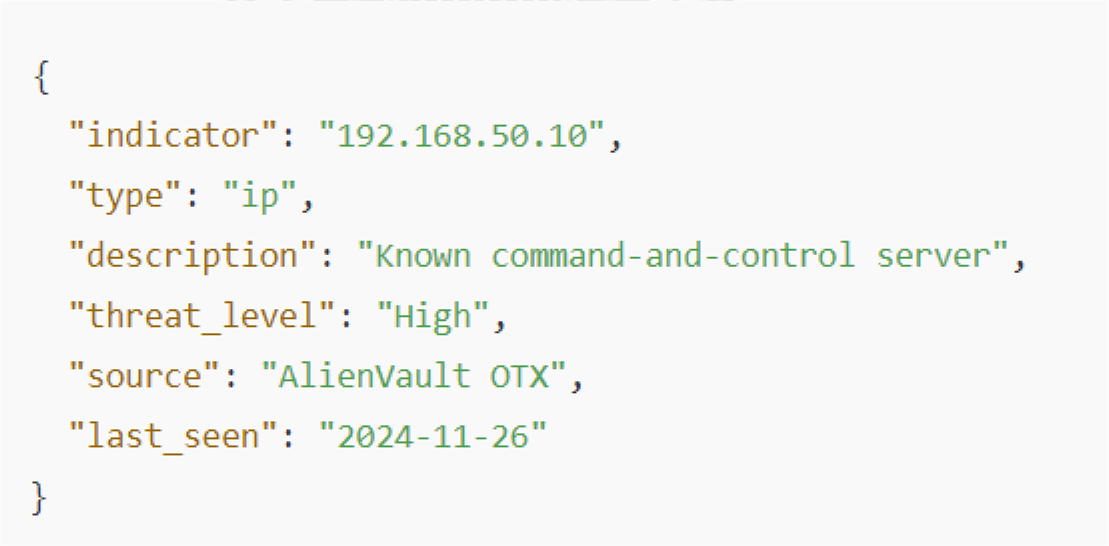
- **Domains**:
  DNS logs show connections to domains categorized as malicious in a feed like VirusTotal.
  Example: A SIEM flags a domain used in a recent ransomware campaign such as LockBit.

Real-Life Scenario:

QRadar ingests threat intelligence data, and when a log indicates connection to a flagged IP, the SOC team initiates an investigation, identifying a malware-infected endpoint.

Technical Workflow

1. **Threat Intelligence Feed Ingestion**:
   - Threat feeds are integrated into the SIEM system using APIs, data connectors, or manual imports.
   - Common Threat Intelligence Providers:
     - **Public Feeds**: AlienVault OTX, AbuseIPDB, or Spamhaus.
     - **Premium Feeds**: Recorded Future, CrowdStrike Falcon Intelligence, FireEye iSight.
     - **Industry-Specific Feeds**: FS-ISAC for financial services, InfraGard for critical infrastructure.
   - Example Feed Format:



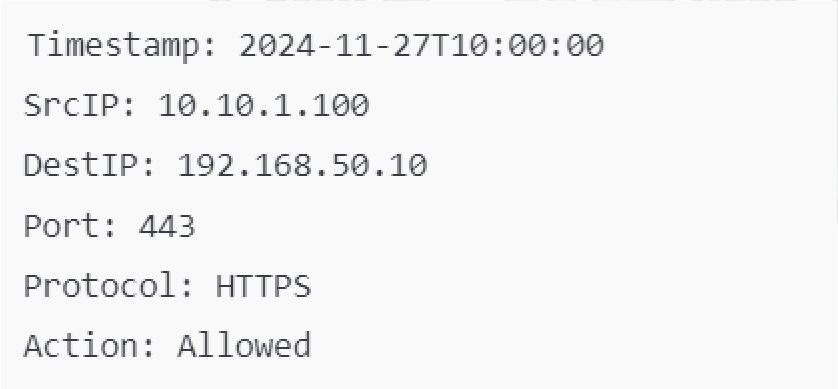
```
{
  "indicator": "192.168.50.10",
  "type": "ip",
  "description": "Known command-and-control server",
  "threat_level": "High",
  "source": "AlienVault OTX",
  "last_seen": "2024-11-26"
}
```

2. **Integration with SIEM**:
   - Threat feeds are imported into the SIEM system and correlated with logs.
   - Integration can be automated using tools like **MISP (Malware Information Sharing Platform)** or **STIX/TAXII protocols**.

3. **Real-time Correlation**:
    - SIEM continuously matches incoming log data (from sources like firewalls, proxies, and DNS servers) with threat intelligence indicators.
    - If a match is found, the SIEM triggers an alert or initiates an automated response.

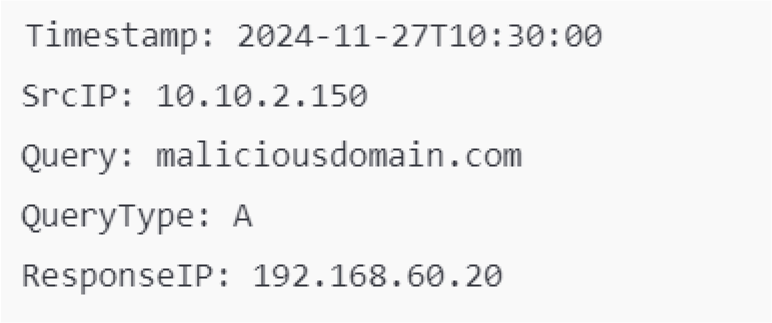
Examples of Threat Intelligence in SIEM

1. **Detecting Malicious IP Communication**:
    - **Scenario**: A SIEM ingests logs from a corporate firewall and matches outbound traffic against a threat feed of known command-and-control (C2) servers.
    - **Technical Steps**:
        - Ingest firewall logs:



```
Timestamp: 2024-11-27T10:00:00
SrcIP: 10.10.1.100
DestIP: 192.168.50.10
Port: 443
Protocol: HTTPS
Action: Allowed
```

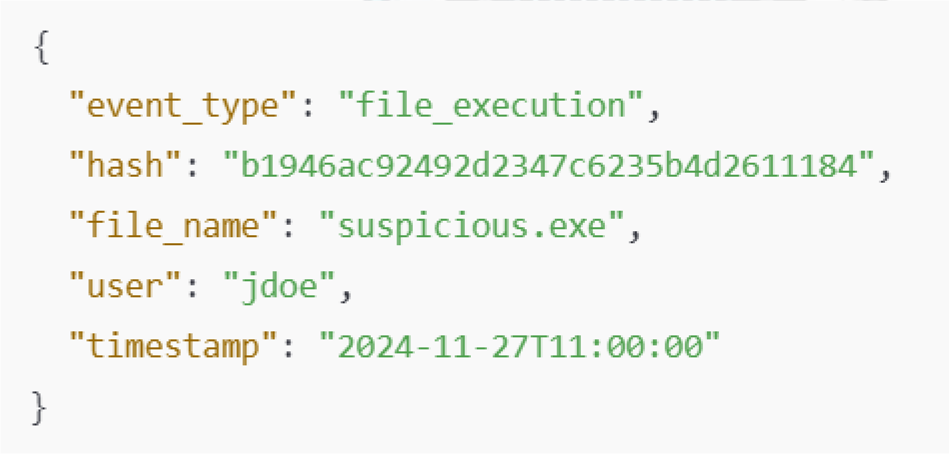
        - Correlate DestIP (192.168.50.10) with threat intelligence feed.
        - Trigger an alert: "Outbound connection to a known malicious C2 server."
    - **Use Case**: Preventing data exfiltration or lateral movement by isolating the endpoint initiating the connection.
2. **Identifying Malicious Domains**:
    - **Scenario**: DNS logs are ingested into the SIEM, and queries to domains flagged in a threat intelligence feed are detected.
    - **Technical Steps**:
        - DNS log example:



```
Timestamp: 2024-11-27T10:30:00
SrcIP: 10.10.2.150
Query: maliciousdomain.com
QueryType: A
ResponseIP: 192.168.60.20
```

        - Match Query (maliciousdomain.com) against threat intelligence feed.
        - Enrich with additional context:
            - **Domain Age**: 2 days (suspicious).
            - **Reputation**: Associated with phishing campaigns.
        - Trigger an alert: "Potential phishing domain accessed."

3. **File Hash Matching**:
    - **Scenario**: An endpoint detection tool sends file hashes to the SIEM. The SIEM matches hashes with threat intelligence databases (e.g., VirusTotal).
    - **Technical Steps**:
        - File hash from EDR log:

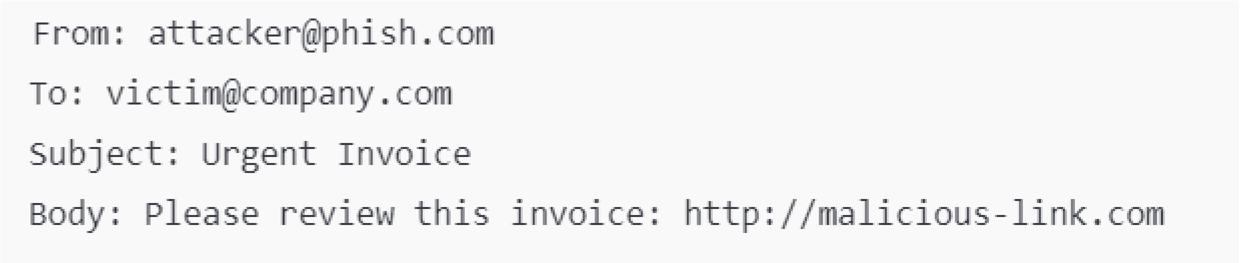


```
{
  "event_type": "file_execution",
  "hash": "b1946ac92492d2347c6235b4d2611184",
  "file_name": "suspicious.exe",
  "user": "jdoe",
  "timestamp": "2024-11-27T11:00:00"
}
```

        - Match hash with threat intelligence feed.
            - Result: b1946ac92492d2347c6235b4d2611184 identified as part of a ransomware campaign.
        - Trigger a response: Isolate the endpoint and notify the SOC team.

4. **Email Threat Detection**:

  - **Scenario**: SIEM integrates with a secure email gateway and uses threat intelligence to detect malicious URLs in emails.
  - **Technical Steps**:
    - Email log:

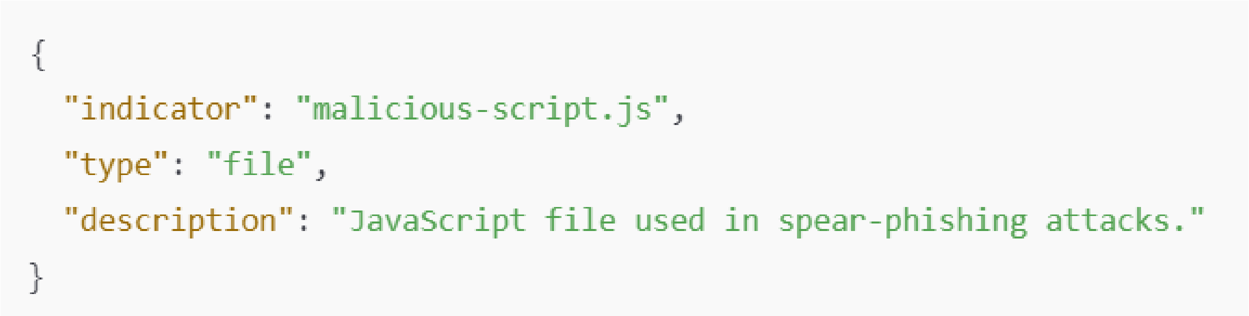


```
From: attacker@phish.com
To: victim@company.com
Subject: Urgent Invoice
Body: Please review this invoice: http://malicious-link.com
```

    - Match URL http://malicious-link.com with threat intelligence.
      - Enrichment: Linked to a phishing campaign targeting finance departments.
    - Generate an alert: "Phishing attempt detected."

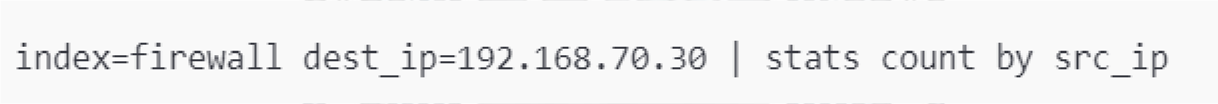
Advanced Use Cases

1. **Automated Threat Hunting with SOAR**:
   - SIEM integrates with SOAR platforms to automate responses:
     - If an IP from threat intelligence is flagged, initiate actions like:
       - Blocking the IP on the firewall.
       - Disabling a user account.
       - Running an endpoint scan via EDR.
2. **Custom Threat Feed Development**:
   - Organizations can develop internal threat feeds from proprietary data or honeypots.
   - Example:
     - Internal threat feed:



```
{
  "indicator": "malicious-script.js",
  "type": "file",
  "description": "JavaScript file used in spear-phishing attacks."
}
```

3. **Threat Hunting with Historical Data**:
   - SIEM allows querying historical logs against updated threat intelligence.
   - Example:
     - New threat feed entry: 192.168.70.30 is a malicious IP.
     - Query historical logs:



```
index=firewall dest_ip=192.168.70.30 | stats count by src_ip
```

     - Identify affected hosts and initiate a retroactive investigation.

Benefits in Threat Hunting

- **Proactive Detection**: Identifies threats based on global intelligence before they impact the organization.
- **Contextual Insights**: Enriches raw data with actionable intelligence, aiding faster investigations.
- **Reduced False Positives**: Helps validate alerts by comparing with known malicious indicators.

4. Anomaly Detection

SIEM solutions use machine learning (ML) and baselining to identify anomalies in user and system behavior. These anomalies often indicate potential threats.

Examples:

- **User Behavior Analytics (UBA)**:
  A user typically accesses files from a specific department but suddenly accesses files from multiple departments.
  Detection: Insider threat or credential misuse.

How UEBA Works

1. **Data Ingestion and Contextualization**:
   - **Sources of Data**: UEBA leverages logs from various sources, including:
     - Authentication systems (e.g., Active Directory, Okta).
     - Network devices (e.g., Cisco ASA, Palo Alto firewalls).
     - Endpoint detection tools (e.g., CrowdStrike, Carbon Black).
     - Application logs (e.g., SharePoint, Microsoft 365).
   - **Example**:
     - Logs showing user login times, geographic locations, accessed resources, and file access.
2. **Baseline Behavior Modeling**:
   - UEBA uses machine learning (ML) algorithms to analyze historical data and establish a baseline of "normal" behavior for each user and entity.
   - **Example**:
     - **User "Alice"**:
       - Normal working hours: 9 AM–6 PM.
       - Regular login location: New York.
       - Typical resource access: HR database.
       - Average file download size: <10 MB.
     - Baseline thresholds: Anomalies are flagged if deviations are significant (e.g., >3 standard deviations).
3. **Anomaly Detection**:
   - Real-time monitoring of activities identifies deviations from the baseline.
   - **Example**:
     - Anomalous behavior detected:

        - Login from Moscow at 3 AM (geographical anomaly).
        - Download of 5 GB of files from the HR database (resource access anomaly).

Technical Mechanisms of UEBA in SIEM

a) Statistical Analysis:

- Tracks metrics like login frequency, time spent accessing specific resources, and download/upload size.
- **Technical Workflow**:
    - Input: Daily login counts for a user.
    - Algorithm: Standard deviation or z-score.
    - Alert: Triggered if login count exceeds 3 standard deviations from the baseline.
- **Example**:
    - Baseline: User logs in twice daily on average.
    - Incident: 20 login attempts in one hour → Flagged as suspicious.

b) Clustering Algorithms:

- Groups users or entities based on similar behavior patterns and flags outliers.
- **Technical Workflow**:
    - Algorithm: K-means clustering.
    - Input: File access patterns across all employees.
    - Outlier: User accessing sensitive financial data who does not belong to the finance team.
- **Example**:
    - Employee from Marketing accessing "Budget_2024.xlsx" in the Finance folder.

c) Sequence Analysis:

- Detects irregular patterns in sequences of actions.
- **Technical Workflow**:
    - Sequence: Login → File Access → Email Send.
    - Anomaly: Login → Privilege Escalation → Database Dump.

- **Example**:
    - A regular user account suddenly executes privilege escalation commands (detected from Windows Event ID 4673).

d) Behavioral Peer Group Analysis:

- Compares a user's behavior with peers in the same department or role.
- **Technical Workflow**:
    - Baseline: Marketing team members download <500 MB files daily.
    - Anomaly: A marketer downloads 10 GB of data in one session.
- **Example**:
    - Peer group baseline: HR department users access payroll data weekly.
    - Incident: An HR intern accesses payroll data hourly.

Examples of Threats Detected Using UEBA

1. **Insider Threat**:
    - A disgruntled employee tries to exfiltrate sensitive data.
    - **Workflow**:
        - SIEM detects:
            - Unusual working hours: Activity at 2 AM.
            - Anomalous file downloads: Large volume of sensitive documents.
            - Suspicious email activity: Forwarding files to personal email accounts.
    - **Real-World Case**:
        - In 2019, an employee from Tesla attempted to steal trade secrets by uploading files to a personal Dropbox account. A UEBA system could have flagged this unusual activity.
2. **Compromised Account**:
    - An attacker uses stolen credentials to infiltrate a network.
    - **Workflow**:
        - SIEM detects:

        - Geographical anomaly: Logins from multiple countries within an hour.
        - Access anomaly: User accesses resources outside their typical role.
        - Privilege escalation: Attempts to elevate permissions.
   - **Example**:
     - A marketing employee's credentials are stolen and used to access engineering databases.

3. **Malware or APT Behavior**:
   - Malware spreads laterally through a network.
   - **Workflow**:
     - SIEM detects:
       - Process anomalies: Regular applications (e.g., Word) spawning PowerShell processes.
       - Network anomalies: High outbound traffic to suspicious IPs.
       - Behavioral deviations: A server typically hosting a web application begins querying internal database servers.
   - **Example**:
     - WannaCry ransomware exhibiting abnormal SMB activity and file encryption patterns.

Technical Implementations of UEBA in SIEM Tools

1. **Splunk UEBA**:
   - **Features**: Pre-built anomaly detection models, visualizations.
   - **Example Query**:

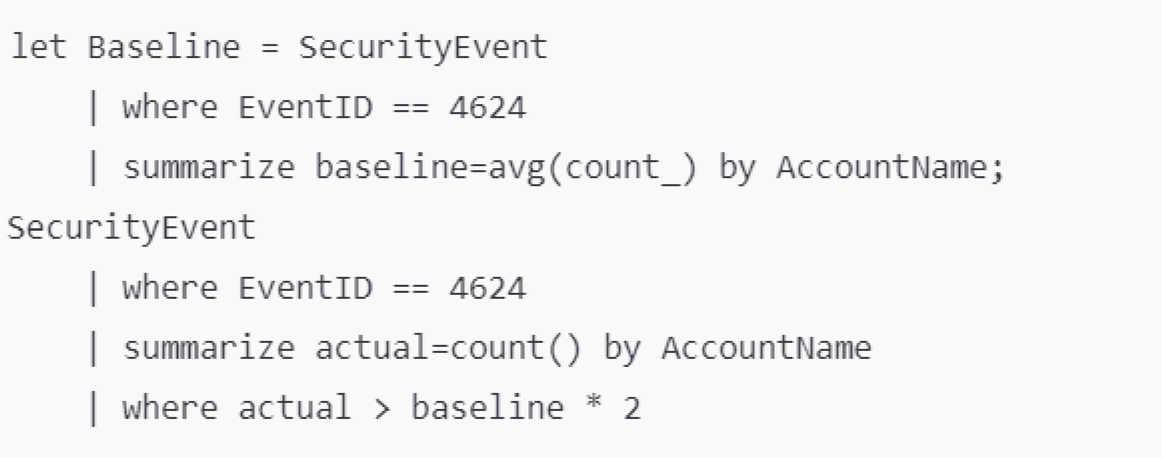
```
index=auth action=failure user!="service-account" | stats count by user, src_ip
```

     - Detect failed login attempts by users excluding known service accounts.

2. **Elastic SIEM**:
   - **Features**: Anomaly detection with Elastic ML jobs.
   - **Example Use Case**:

        - Anomaly job detecting unusual DNS requests:
            - Input: DNS logs.
            - Output: Flag if request size >95th percentile.

3. **Azure Sentinel**:
    - **Features**: Built-in UEBA capabilities with ML-based anomaly detection.
    - **Example KQL Query**:



```
let Baseline = SecurityEvent
    | where EventID == 4624
    | summarize baseline=avg(count_) by AccountName;
SecurityEvent
    | where EventID == 4624
    | summarize actual=count() by AccountName
    | where actual > baseline * 2
```

        - Detects users logging in at twice their normal frequency.

4. **IBM QRadar UEBA**:
    - **Features**: Detects deviations in user behavior, offers risk scoring.
    - **Example Workflow**:
        - Risk score incremented when:
            - Login from an unusual IP.
            - Privilege escalation detected.

Key Benefits for Threat Hunting

1. **Detection of Unknown Threats**:
    - UEBA excels at detecting novel attack patterns or threats that lack known signatures.
    - Example: Detecting zero-day malware through anomalous behavior.
2. **Reduced False Positives**:

  - Context-aware anomaly detection ensures fewer false alarms compared to rule-based systems.

3. **Prioritized Alerts**:
    - UEBA assigns risk scores to anomalies, helping analysts focus on high-priority threats.

- **Network Traffic Analysis**:
  A sudden spike in outbound traffic volume from a single endpoint.
  Detection: Possible data exfiltration.
- **Geographical Anomalies**:
  A user logs in from India at 10:00 AM and from the US at 10:05 AM.
  Detection: Impossible travel, indicative of compromised credentials.

Real-Life Scenario:

Splunk UBA detects an account behaving abnormally. Further investigation reveals a compromised account used to download confidential files.

---

5. Search and Querying

SIEM systems enable hunters to run detailed searches and queries across historical and live data. These queries can uncover hidden threats and patterns.

Examples:

1. Failed Logins

- **Query Syntax:**

>> Query: source="auth.log" AND action="failed_login"

- **Advanced Explanation:**
  - The auth.log file typically records authentication-related events (e.g., SSH logins, sudo attempts).
  - The action failed_login indicates unsuccessful login attempts, which could signify potential brute force attempts or incorrect password entries.
- **Enhancements:**
  - Add time-based filtering to refine searches:

>> Query: source="auth.log" AND action="failed_login" AND timestamp > "2024-11-26T00:00:00"

-
  - Include grouping to identify patterns:

>> Query: source="auth.log" AND action="failed_login" | stats count by user

-
  -
    - This query identifies which user accounts have the highest number of failed login attempts.

- **Use Case:**
  - **Brute Force Detection:** Focus on repeated attempts from the same IP or targeting a single user account.
  - **Geolocation Analysis:** Correlate the source IP with geographic data to identify anomalous login locations.

---

2. Specific IOC Search

- **Query Syntax:**

>> Query: source="firewall" AND dst_ip="192.168.1.100"

- **Advanced Explanation:**
  - The source="firewall" indicates that the data is extracted from firewall logs.
  - dst_ip="192.168.1.100" searches for traffic destined to a specific IP address, which might be flagged as malicious or suspicious (e.g., part of a botnet or C2 server).
- **Enhancements:**
  - Combine with port filtering for more specific results:

>> Query: source="firewall" AND dst_ip="192.168.1.100" AND dst_port="443"

-
  -
    - This query narrows the search to HTTPS traffic to the flagged IP.
  - Integrate threat intelligence feeds to validate the IOC:

>> Query: source="firewall" AND dst_ip="192.168.1.100" AND threat_intel="true"

- **Use Case:**
  - **Incident Triage:** Determine if the flagged IP corresponds to known malicious actors or unusual activity.
  - **Network Analysis:** Investigate connections between internal hosts and the flagged IP for lateral movement or exfiltration.

3. File Operations

- **Query Syntax:**

```
>> Query: action="file_deleted" AND filename="*.dll"
```

- **Advanced Explanation:**
  - The action="file_deleted" identifies deletion events from logs.
  - The filename="*.dll" filters for deleted files with the .dll (Dynamic Link Library) extension, often exploited by attackers for malicious purposes (e.g., tampering or removing evidence).
- **Enhancements:**
  - Add filtering by users or processes responsible for the action:

```
>> Query: action="file_deleted" AND filename="*.dll" AND user="SYSTEM"
```

    - This checks if system-level accounts performed the deletion.
  - Include file path analysis:

```
>> Query: action="file_deleted" AND filename="*.dll" AND filepath="/windows/system32/*"
```

    - This ensures focus on critical system files.
- **Use Case:**
  - **Malware Analysis:** Track suspicious file deletions linked to known malware behaviors.
  - **Forensic Investigation:** Identify attempts to tamper with security-related DLLs.

Key Advanced Features in Search and Querying for SIEM:

1. **Time Range Filters:**
   - Use relative or absolute time filters for precision:

```
>> timestamp >= "2024-11-26T00:00:00" AND timestamp <= "2024-11-27T23:59:59"
```

2. **Threat Enrichment:**
   - Correlate logs with external threat intelligence for deeper context:

```
>> Query: dst_ip="192.168.1.100" AND threat_category="Malware"
```

3. **Event Aggregation:**

- Use statistical functions to detect anomalies:

>> Query: action="failed_login" | stats count by user, src_ip

4. **Anomaly Detection:**
   - Identify rare or outlier events using SIEM's machine learning capabilities (if supported).

Real-Life Scenario:

A SOC analyst uses Splunk to search logs for PowerShell commands like Invoke-Mimikatz, uncovering an attacker attempting credential dumping.

6. Dashboards and Reports

SIEM platforms provide customizable dashboards and reports for real-time monitoring and historical analysis.

Key Components of Visualization in SIEM

1. **Graphical Representation of Data**:
   - Data from logs, alerts, and events is visualized as charts, graphs, heatmaps, and tables.
   - Enables pattern recognition and anomaly spotting.
2. **Customizable Dashboards**:
   - Analysts can tailor dashboards to specific threat-hunting use cases, such as user activity monitoring or network traffic analysis.
3. **Drill-Down Capabilities**:
   - Interactive dashboards allow users to click on a data point or anomaly and drill down into raw logs for deeper investigation.
4. **Real-Time Monitoring**:
   - Dashboards update dynamically, providing real-time insights into security events as they unfold.

Technical Features of SIEM Dashboards

a. Heatmaps for Geographic Analysis

- **Description**: Shows login or access patterns across geographies.
- **Technical Workflow**:
  - Collect login data with source IP addresses from logs (e.g., VPN, web applications).
  - Use a GeoIP database to map IP addresses to geographic locations.
  - Display a heatmap showing login attempts by country.
- **Example**:
  - A sudden spike in logins from regions where the organization has no presence could indicate an attack.
  - **Tool**: Splunk's "Geography Visualization" or Elastic Kibana's "Region Map."

b. Network Traffic Visualization

- **Description**: Visualizes inbound and outbound network traffic to identify unusual spikes or patterns.
- **Technical Workflow**:
  - Parse NetFlow or firewall logs to extract metrics like source/destination IP, port, protocol, and traffic volume.
  - Plot data using line or bar graphs to show traffic trends over time.
- **Example**:
  - **Scenario**: Detecting a Distributed Denial of Service (DDoS) attack.
    - Normal traffic: 10 Mbps.
    - Sudden spike: 500 Mbps from multiple IPs targeting the same server.
  - **Tool**: SolarWinds SIEM or Kibana.

c. Suspicious User Activity

- **Description**: Dashboards track user behavior anomalies, such as logins from multiple locations within a short time.
- **Technical Workflow**:
  - Aggregate authentication logs from Active Directory or other sources.
  - Identify and flag activities that breach user baseline behavior.

- **Example**:
  - User "john.doe" logs in from New York at 9:00 AM and from London at 9:10 AM.
  - Visualization highlights this anomaly with a scatter plot.
  - **Tool**: IBM QRadar's UEBA dashboard.

d. Malware Infection Patterns

- **Description**: Dashboards can track endpoints showing malware infection trends.
- **Technical Workflow**:
  - Correlate antivirus alerts, EDR logs, and file integrity monitoring data.
  - Display infection rates over time or by endpoint in a pie chart or trend graph.
- **Example**:
  - **Scenario**: Identifying an outbreak of a trojan.
    - Alerts show five endpoints were infected in the last 30 minutes, with all infections originating from the same file downloaded from a phishing email.
  - **Tool**: Elastic SIEM or Palo Alto Cortex XSOAR.

Interactive Visualization Use Case Examples

1. Port Scanning Detection

- **Scenario**:
  - A threat actor is performing port scans to identify open services.
- **Technical Workflow**:
  - Collect IDS/IPS logs (e.g., from Snort or Suricata).
  - Correlate logs showing repeated connection attempts to multiple ports from a single IP.
  - Visualization:
    - Use a bubble chart or heatmap to display "source IP vs. target port frequency."
  - **Example**:

        - IP 192.168.1.50 scans ports 21, 22, 23, 80, and 443 on 50 different hosts within 2 minutes.
    - **Outcome**: Analysts block the IP in real time.

2. Lateral Movement in Networks

- **Scenario**:
    - An attacker compromises one machine and moves laterally to others.
- **Technical Workflow**:
    - Collect Windows Event logs (e.g., Event ID 4624 for logons).
    - Map user logins across multiple hosts within short time intervals.
    - Visualization:
        - Use Sankey diagrams to show the flow of user accounts across systems.
    - **Example**:
        - User "admin" logs into machine A, then B, then C in a span of 5 minutes.
        - The visualization highlights these connections as suspicious.
    - **Outcome**: Analysts isolate affected machines to prevent further movement.

3. DNS Exfiltration Visualization

- **Scenario**:
    - Data is being exfiltrated via DNS queries.
- **Technical Workflow**:
    - Analyze DNS logs for high-frequency requests to specific domains.
    - Use a scatter plot to display the "frequency of DNS requests vs. domains."
- **Example**:
    - Domain malicious.com receives 100,000 requests in 5 minutes, compared to the normal 1,000.
    - **Tool**: Splunk’s DNS Analytics Dashboard.
    - **Outcome**: Investigate and block the domain.

Implementation Challenges

1. **Data Overload**: Dashboards need to filter relevant data to avoid overwhelming analysts.

2. **Customization Complexity**: Technical expertise is required to create meaningful and actionable visualizations.
3. **Real-Time Updates**: Ensuring low latency for real-time dashboards can strain resources.

Real-Life Scenario:

A SOC team uses QRadar's dashboard to monitor alerts on suspicious SMB activity. They identify a ransomware attack in progress and isolate the affected systems.

7. Incident Management and Alerts

SIEM tools allow hunters to define alert thresholds and automate responses, such as sending notifications, blocking traffic, or quarantining endpoints.

Examples:

1. Real-time Alerting and Threat Correlation

How it Works

- SIEM solutions use predefined correlation rules or machine learning models to detect suspicious behavior across logs and events from various sources.
- Alerts are generated based on predefined thresholds, anomaly detection, or a combination of conditions indicating potential incidents.

Technical Example

- **Scenario**: Detect brute force attacks followed by privilege escalation.
- **Correlation Rule**:

```
>> If (FAILED_LOGIN >= 5 in 10 minutes) AND (SUCCESSFUL_LOGIN from same IP) THEN Alert("Potential Brute Force Attack")
```

- **Log Sources**:
  - Authentication logs (Windows Event ID 4625 for failed logins, Event ID 4624 for successful logins).
  - Active Directory logs for privilege escalation (e.g., Event ID 4672).
- **SIEM Tool**: Splunk, Elastic SIEM.

Use Case

1. **Alert Triggered**:

    - Multiple failed logins from 192.168.1.10 within 5 minutes.
    - A successful login from the same IP.
2. **Action**: Incident automatically raised and assigned to a Security Analyst for investigation.

---

2. Workflow Integration with Incident Management Systems

How it Works

- SIEM integrates with ticketing systems like ServiceNow or Jira, automating the creation of incidents when specific alerts are triggered.
- Alerts are enriched with metadata (e.g., user, IP, geolocation, and historical data) to provide context for the incident.

Technical Example

- **Alert Trigger**: Unusual outbound traffic to known malicious domains.
- **Integration Workflow**:
    - SIEM generates an alert tagged with IOC (Indicator of Compromise) information from threat intelligence feeds.
    - The alert triggers an API call to ServiceNow, creating an incident ticket.
    - The ticket is enriched with:
        - Source IP: 10.0.0.5
        - Destination Domain: malicious-domain.com
        - Threat Feed Match: AlienVault OTX.

Use Case

1. **Incident Ticket Created**:
    - Priority: High.
    - Assigned Team: Network Operations.
2. **Action**: Network team isolates the source machine while the SOC investigates further.

---

3. Proactive Incident Detection with Threat Hunting

How it Works

- Threat hunting involves querying and analyzing logs to detect signs of advanced threats not identified by automated rules.
- SIEM’s query and analytics capabilities are essential for threat hunters to craft specific searches.

Technical Example

- **Hypothesis**: "An attacker is using PowerShell for lateral movement."
- **Search Query** (Splunk):

```
>> index=windows_logs sourcetype="WinEventLog:Security" EventCode=4688
CommandLine="*powershell.exe*"
| stats count by AccountName, ParentProcessName
```

- **Investigation**:
  - Command execution logs reveal unusual PowerShell commands executed by UserA on ServerB.
  - Lateral movement confirmed by correlating RDP connection logs (Event ID 4624) to the same machine.

Use Case

1. **Threat Identified**:
   - Persistence established through malicious PowerShell scripts.
2. **Action**:
   - Incident raised for endpoint isolation.
   - Incident notes include the timeline of lateral movement and affected hosts.

---

4. Alert Prioritization Using Risk-based Scoring

How it Works

- SIEM uses scoring models to prioritize alerts based on severity, asset value, and the likelihood of a threat.
- High-risk alerts are escalated immediately, reducing noise from benign events.

Technical Example

- **Scenario**: Outbound connection to a C2 (Command-and-Control) server.
- **Risk Scoring**:

    - Severity of IOC: High (C2 server detected in threat feeds).
    - Asset Value: High (critical database server).
    - Likelihood: High (unusual outbound traffic pattern).
- **Combined Score**: 95/100 (Critical Alert).

Use Case

1. **Alert Raised**:
    - SIEM flags the connection as critical.
    - Incident escalated directly to Tier-3 analysts.
2. **Action**: Analysts review network logs, confirm C2 communication, and terminate the connection.

---

5. Incident Enrichment and Triage

How it Works

- SIEM enriches incidents with contextual data such as:
    - Geolocation of source IP.
    - Associated IOC from threat feeds.
    - Historical activity for the affected user or system.
- Analysts use this data for triage and prioritization.

Technical Example

- **Alert**: Multiple logins from geographically distant locations within minutes (impossible travel scenario).
- **Enrichment**:
    - Login 1: New York (10:00 AM UTC).
    - Login 2: Tokyo (10:15 AM UTC).
    - User Behavior: First anomaly detected in 180 days.
- **Investigation Query**:

```
>> index=authentication_logs user="JohnDoe" | stats count by src_ip, geo_location
```

Use Case

1. **Incident Created**:

    - Priority: Medium.
    - Assigned Team: SOC Tier-2 Analysts.

2. **Action**:
    - Analysts identify the Tokyo login as suspicious.
    - User account temporarily disabled to prevent further compromise.

---

6. Automated Playbooks for Incident Response

How it Works

- SIEM integrates with SOAR (Security Orchestration, Automation, and Response) platforms to automate repetitive tasks in incident response.
- Playbooks execute predefined actions like isolating systems, resetting credentials, or blocking IPs.

Technical Example

- **Scenario**: Detection of ransomware activity (e.g., files renamed with .encrypted extension).
- **Automated Playbook**:
    1. Isolate the affected host using an EDR solution.
    2. Block associated IP addresses at the firewall.
    3. Notify the SOC team via email and Slack.
- **Tools**: Palo Alto Cortex XSOAR, Splunk Phantom.

Use Case

1. **Response Triggered**:
    - Host isolation and IP block completed within 2 minutes.
2. **Manual Review**:
    - Analysts validate ransomware indicators and begin recovery.

---

7. Forensic Incident Analysis

How it Works

- SIEM retains historical logs for deep-dive forensic investigations, enabling root cause analysis of incidents.

- Threat hunters analyze logs to trace an attacker’s actions across the environment.

Technical Example

- **Scenario**: Data exfiltration via unauthorized S3 bucket access.
- **Investigation Query** (AWS CloudTrail Logs in Splunk):

```
>> index=aws_logs eventName="GetObject" bucket="sensitive-data-bucket"
| stats count by userName, src_ip
```

- **Analysis**:
  - Identified unauthorized access by UserX from IP 203.0.113.5.
  - Correlated access to compromised credentials detected in a phishing email.

Use Case

1. **Incident Report**:
   - Timeline: Credential theft → S3 access → Data exfiltration.
2. **Action**:
   - Compromised credentials invalidated.
   - S3 bucket access policies updated.

---

8. Post-Incident Review and Reporting

How it Works

- SIEM-generated incident reports are used for post-incident analysis, helping improve future detection capabilities and response processes.
- Metrics tracked include:
  - Time to Detect (TTD).
  - Time to Respond (TTR).
  - False Positive Rate (FPR).

Technical Example

- **Report**:
  - Incident: Malware outbreak in HR systems.
  - Detection Method: Alert from correlation rule (malicious domain).
  - TTD: 15 minutes.

    - TTR: 30 minutes.

Use Case

- Post-incident review identifies gaps in EDR coverage on HR endpoints, leading to policy updates.

Summary

SIEM systems are indispensable for threat hunting, offering:

- **Centralized visibility** across diverse data sources.
- **Advanced correlation** to detect multi-stage attacks.
- **Rich threat intelligence** for proactive detection.
- **Anomaly detection** for uncovering unknown threats.
- **Powerful search** capabilities for forensic investigations.

By leveraging these features, threat hunters can uncover sophisticated attacks, contain incidents, and strengthen an organization's security posture.