6. Security Information and Event Management

I. SIEM Architecture

- Log Management
- Real-Time Monitoring
- Alerting and Notification
- Incident Response
- Dashboards, Reports, and Visualizations
- Threat Intelligence Integration

Log Management

1. Collection
    a. Which devices will be collected from?
    b. Which events to collect?
    c. How long to retain?
    d. Where to store logs?
    e. Method of collection
        i. Agents
        ii. Agentless
2. Aggregation
    a. Collect and consolidate events
    b. Unify the timeline across the organization
    c. Enhance holistic visibility
    d. Allow for correlation analysis
3. Parsing and Normalization
    a. Ensure Consistency
    b. Extract structured information
        i. Fields, columns
        ii. Regex, parsers
    c. Convert to common schema
        i. Field Mapping

4. Retention
    a. Storing log data
    b. Ensure analysis visibility
        i. IR
        ii. Compliance
5. Indexing
    a. Turns raw log data into searchable data
    b. Efficient log retrieval
    c. Helps with scaling
6. Correlation and Analysis
    a. Linking related log events together
    b. Context
    c. Correlation Rules
    d. Analysis
7. Alerting
    a. Notify relevant people
    b. Threshold based alerts
    c. Pattern based
    d. Anomaly based
    e. Event Based

II. SIEM Components

SIEM Components

- Endpoints (Data)
- Forwarder (Agents)
- Indexer
- Search Head (GUI)
- Analyst (You)

SIEM Deployment Models

- Single Instance Deployment (small networks and home labs)
- Distributed Deployment
- Clustered Deployment

III. Log Types

- System Logs
  - Windows Event Logs
  - Sysmon Logs
  - Linux/Unix Syslogs
- Network Logs
  - Firewall logs
  - Proxy logs
  - DNS logs
- Application Logs
  - Database logs
  - Web server / HTTP logs
- Security Logs
  - Authentication Logs
  - IDS/ISP Logs
  - Endpoint Security Logs
- Cloud Logs
  - AWS CloudTrail logs
  - Azure Activity Logs
  - Log Analytics
- Audit Logs
  - Audit Trail Logs
  -

IV. Log Formats

- Unstructured Logs
  - No predefined format or syntax
  - Common Log Format (CLF)
- Semi-structured Logs
  - Some syntax structure
  - Lacks adherence of a schema
  - Syslog
  - Windows Event Log (EVT)
- Structured Logs
  - Well-defined syntax and formatting
  - Adherence to an agreed upon schema
  - CSV, TSV, JSON, XML

V. Common Attack Signatures

User Behavior Indicators

- Multiple Failed Login Attempts
  - Incorrect usernames or passwords
  - Increase in failures from a single user accounts
  - Increase in failures from multiple user accounts
- Login Times
  - Time of day that logons/access requests take place
  - Abnormalities from user baseline
- Login/Access Locations
  - Geographic locations of logons or access requests
  - Unusual countries or regions
  - Impossible Travel
- File Access Patterns
  - File paths, modifications, or other activity
- User-Agent Strings
  - Known hacker tools

SQL Injection

https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/SQL%20Injection

Keywords to look for:

- SELECT
- FROM
- WHERE
- GROUP BY
- ORDER BY
- INSERT INTO
- UPDATE
- DELETE
- UNION
- JOIN

Injection Characters:

- single quotes
- double quotes
- semicolons
- dashes
- URL encoded versions of these characters

Malformed Entries

Cross-Site Scripting

Executing malicious code by injecting Javascript

- Look for `<script>` tags
- Look for event handlers:
  - `onload , onclick , onmousover`
  - References to "javascript"
- Special Characters:
  - <, >, ", ', &, %, ;

Command Injection

Executing arbitrary OS commands

- Look for special characters:
  - ;, ||, &&
- Look for references to commands or utilities;
  - ls, echo, bash, cat, cd, cmd.exe, curl, wget
  - ping, sudo, chmod, rm, nc, nc.exe, sh
- URL encoded injection characters

Path Traversal and Local File Inclusion

`../../../../`

Accessing files outside of web root. Can lead to unauthorized access to files on the web servers OS

Local File Inclusion - LFI:

- Include a local file from the system

- Enumerate the system, read hardcoded creds

Look for path traversal symbols

- `../../../`
- URL Encoded

Look for references to sensitive files

- /etc/passwd
- /etc/shadow

VI. Command Line Log Analysis

Analysis of log file called `access.log`

```
file access.log # info about the file
ls -lh access.log # More info such as file size in human readable format
wc -l access.log # Number of lines to get an idea of number of entries
head access.log -n 1 # Get first line in the file
tail access.log -n 1 # Get last line in the file. Find total timeline
cut access.log -d " " -f <field number> | sort | uniq -c | grep -v " 1 " | sort
-nr # Find list of IOCs in the file
```

Start search based on IOCs

VII. Pattern Matching

Use grep creatively to find malicious patterns such as brackets or `../` path traversal

```
grep -E '%3C|%3E|<|>' # search for arrow brackets
```

- `-E` : Extended