**Security Operations Center (SOC) Rule Book**

**1. Introduction**

The SOC Rule Book serves as a comprehensive guide for identifying, detecting, and responding to security threats within an organization. It provides structured detection rules, incident response procedures, and escalation guidelines to ensure a standardized and effective approach to cybersecurity monitoring and response.

**2. Rule Book Structure**

Each rule in the SOC Rule Book includes the following elements:

|  |
| --- |

| **Field** | **Description** |
| --- | --- |
| **Threat Category** | Defines the type of threat (e.g., Malware, Phishing, XSS, SQL Injection, Insider Threats, etc.). |
| **Detection Rule** | The specific SIEM, IDS, or other detection rule that identifies the threat. |
| **Log Sources** | Specifies the data sources (e.g., Firewalls, IDS/IPS, Web Servers, EDR, DNS, Active Directory, etc.). |
| **Alert Severity** | Categorizes the severity level: Low, Medium, High, or Critical. |
| **False Positive Rate** | Evaluates the likelihood of generating false positives. |
| **Response Actions** | Outlines investigation and mitigation steps. |
| **Escalation Matrix** | Specifies when and how incidents should be escalated. |

**3. Threat Categories and Detection Rules**

**A. Web Security Alerts**

**Absence of Anti-CSRF Tokens**

* **Risk Level:** Medium
* **Instances:** 4
* **Description:** Missing CSRF tokens in forms exposes applications to Cross-Site Request Forgery attacks.
* **Detection Rule (Suricata):**

alert http any any -> any any (msg:"CSRF Token Missing";

content:"POST"; http\_method; content:"csrf\_token"; http\_cookie; nocase; sid:30001; rev:1;)

* **Response:** Implement CSRF protection using secure tokens in web forms.

**Content Security Policy (CSP) Header Not Set**

* **Risk Level:** Medium
* **Instances:** 47
* **Description:** Lack of CSP headers increases exposure to XSS attacks.
* **Detection Rule (ELK):**

index=web\_traffic

| where http\_headers does not contain "Content-Security-Policy"

* **Response:** Configure CSP headers to restrict resource loading and mitigate XSS risks.

**Missing Anti-clickjacking Header**

* **Risk Level:** Medium
* **Instances:** 43
* **Description:** Missing X-Frame-Options headers allows attackers to embed the site in an iframe and conduct clickjacking.
* **Detection Rule (Splunk):**

index=web\_security

| search NOT "X-Frame-Options"

* **Response:** Implement X-Frame-Options: DENY to prevent clickjacking attacks.

**B. Server Security Alerts**

**Server Leaks Information via "X-Powered-By" HTTP Header**

* **Risk Level:** Low
* **Instances:** 61
* **Description:** The X-Powered-By header reveals server details, increasing the risk of targeted attacks.
* **Detection Rule (Suricata):**

alert http any any -> any any (msg:"X-Powered-By Header Detected";

content:"X-Powered-By:"; http\_header; nocase; sid:30002; rev:1;)

* **Response:** Remove or modify the X-Powered-By header in the server configuration.

**Server Leaks Version Information via "Server" HTTP Header**

* **Risk Level:** Low
* **Instances:** 73
* **Description:** The Server header discloses the software version, making it easier for attackers to exploit known vulnerabilities.
* **Detection Rule (ELK):**

index=server\_logs

| search "Server:"

* **Response:** Configure the server to hide or obfuscate version details.

**C. Other Security Alerts**

**X-Content-Type-Options Header Missing**

* **Risk Level:** Low
* **Instances:** 67
* **Description:** Without this header, browsers may incorrectly interpret file types, leading to security vulnerabilities.
* **Response:** Add X-Content-Type-Options: nosniff to prevent MIME-type sniffing.

**Authentication Request Identified**

* **Risk Level:** Informational
* **Instances:** 1
* **Description:** An authentication attempt was detected. Requires monitoring for anomalies.

**Charset Mismatch (Header vs. Meta Content-Type Charset)**

* **Risk Level:** Informational
* **Instances:** 30
* **Description:** Mismatched charset configurations can cause encoding issues or security vulnerabilities.

**Information Disclosure - Suspicious Comments**

* **Risk Level:** Informational
* **Instances:** 1
* **Description:** Comments in source code may inadvertently reveal sensitive information.

**Modern Web Application Detected**

* **Risk Level:** Informational
* **Instances:** 9
* **Description:** A modern framework or technology was identified. Ensure security best practices are followed.

**User Controllable HTML Element Attribute (Potential XSS)**

* **Risk Level:** Medium
* **Instances:** TBD
* **Description:** User-controlled attributes could allow stored or reflected XSS attacks.
* **Detection Rule (Suricata):**

alert http any any -> any any (msg:"Possible XSS Attack";

content:"<script>"; http\_uri; nocase; sid:30003; rev:1;)

* **Response:** Sanitize user input and enforce CSP headers to prevent XSS.

**4. Incident Response & Escalation**

Each rule should be linked to a response playbook.

| **Severity** | **Action** |
| --- | --- |
| **Low** | Monitor the event and log details. |
| **Medium** | Investigate and document findings. |
| **High** | Immediate action required; notify the Security Team. |
| **Critical** | Activate Incident Response Team immediately. |

**Example: Response Playbook for Brute Force Attack**

1. **Verify failed login attempts in the logs.**
2. **Check if the source IP is from an authorized location.**
3. **If suspicious, block the IP in the firewall.**
4. **Reset affected user's credentials.**
5. **Escalate to the Threat Intelligence Team if multiple attempts occur from different IPs.**

**5. Automation & Optimization**

* **Leverage Machine Learning in SIEM** to minimize false positives.
* **Implement SOAR (Security Orchestration, Automation, and Response)** to automate repetitive tasks.
* **Continuously fine-tune IDS/IPS rules** to detect evolving threats and zero-day vulnerabilities.

**6. Conclusion**

A well-structured SOC Rule Book enables a proactive and efficient approach to cybersecurity threat detection and response. Continuous improvement and automation will ensure the SOC remains adaptive and resilient against emerging cyber threats.

**End of Document**