**Cat Scan II Big Dog Report**

Prepared by: Harshkumar Patel

Date: December 16, 2024

[**Executive Summary** 3](#_Toc185267639)

[**Table of Sensors** 3](#_Toc185267640)

[**Discussion Section** 6](#_Toc185267641)

[**Recommendation Section** 9](#_Toc185267642)

[**References** 10](#_Toc185267643)

**Executive Summary**

This report assesses the security and monitoring of Big Dog’s IT structure, focusing on the placement and role of sensors and systems in detecting key Indicators of Compromise (IoC) to reduce vulnerabilities and risks. Sensors were prioritized based on the criticality of the systems they monitor, the sensitivity of the data, and their Security Impact Level (SIL). It aligns these with the company’s most critical information categories, such as Privacy, Proprietary, and Admin, using recognized frameworks like MITRE ATT&CK, NIST, and OWASP. Key recommendations include monitoring security patch compliance and network port activity to strengthen the company’s security. The goal is to create a secure environment by monitoring and securing the company’s IT infrastructure.

# **Table of Sensors**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sensor | Description | System | IoCs Associated (May be more than 1) | Rationale | Priority | Thresholds /Assumptions |
| HTTP Load Time | Monitors the time it takes for the page to load. | Linux | used to indicate Malicious Redirects, DDoS Attacks, or Content Injection | Unexpected changes in load time can indicate anomalies or performance-related issues that could be indicative of a security breach or compromise | Medium | The sensor will monitor high load time conditions |
| MySQL Database Query Sensor | Tracks anomalies in queries also tracks time execution | Linux | Unauthorized access, SQL Injection attack | Detects SQL database exploitation or misuse | V. High | Monitors high execution times and unauthorized patterns |
| SSH Sensor | Monitors SSH login attempts and the number of connections | Linux | Brute force attacks, Unauthorized access | Tracks for suspicious login attempts and protects sensitive data. | High | Monitor both High and Low High: for failed login attempts  Low: For unexpected access |
| Antivirus Status Sensor | Tracks viruses, malware, and ransomware | All | Malware infections, Ransomware attacks | Ensures endpoints are secure from malware threats. | High | Monitor low conditions such as outdated definitions or disabled antivirus. |
| File Sensor | Monitors changes made to sensitive files. | Linux | |  | | --- | |  |  |  | | --- | | Unauthorized file changes, Insider threats or leaks | | Protects proprietary intellectual property by detecting unexpected edits. | V.High | Monitor both high and low conditions. e.g.: changes in files or trying to get access of sensitive data. |
| Windows Event Log Sensor | Logs critical OS events and system anomalies | Windows11 | Unauthorized access, Exploits, Failed logins | Detects suspicious system activities. | V.High | Monitor both high and low conditions. High: Many failed login attempts low: deletion of records/logs |
| Bandwidth Usage Sensor | Monitors network traffic and usage patterns. | All | Data exfiltration, DDoS attacks | Detects abnormal traffic spikes indicating potential attacks. | High | Monitor high conditions like Network traffic spikes. |
| CPU Load Sensor | Monitors server CPU usage. | Windows Server | Performance cutdown | Ensures consistent server performance. | Medium | Monitors high condition loke CPU usage spike. |
| Memory Usage Sensor | Tracks server memory consumption. | Windows Server | Memory exhaustion, Performance slowdowns | Avoids disruptions due to insufficient memory. | Medium | Monitor high conditions such as excessive memory usage. |
| IIS Response Time Sensor | Monitors web server response time. | Windows Server | Slow responses, DDoS attacks | Ensures web services are responsive and secure. | High | Monitors High conditions like response latency |
| SSL Certificate Check Sensor | Validates SSL certificate validity. | Windows Server | Expired or invalid certificates | Maintains HTTPS security for web services. | High | Monitors low certificate expiration date |
| Syslog Monitoring Sensor | Aggregates and reviews system logs. | All | Anomalous activities, Misconfigurations | Centralizes insights for proactive threat detection. | High | Monitors high conditions like suspicious events. |
| DHCP/DNS Status Sensor | Monitors network service reliability. | IT Systems | Service outages, Misconfigurations | Ensures consistent availability of network services. | Medium | Monitor both  high: service failures  low: slow service response. |
| Firewall Status | Monitors firewall performance and configuration. | All | Protects network perimeters by ensuring firewalls are functional and correctly configured. | Protects network perimeters by ensuring firewalls are functional and correctly configured. | High | Monitor both  high: rule changes low: inactive firewall |
| Vulnerability Scanning | Tracks vulnerability scan results. | Kali Test Systems | Unpatched vulnerabilities, Configuration weaknesses | Ensures testing tools function to identify security gaps. | Medium | Monitor high conditions: Monitor for scanning failures or delayed results. |
| Network Traffic | Monitors for unusual network activities. | All | Exfiltration, Intrusions | Identifies unauthorized data transfers or intrusions. | High | Monitors high for an unusual traffic spike |
| Security Patch Status Sensor | Monitors the status of security updates and patches to ensure all systems are up to date. | All | Outdated software or operating system versions that may have vulnerabilities. | Ensuring timely patching is critical to reducing the attack surface. | High | Monitors high for missing critical or overdue patches. |
| Network Port Activity Sensor | Monitors open and active ports. | All | Unusual or unauthorized port activity or open ports that invite attackers to get access. | Monitoring port activity can help detect potential breaches, malware communication, or internal misuse. | High | Monitor for high conditions such as unauthorized or excessive port usage, especially on sensitive servers. |
| SQL Server Health | Monitors database performance and availability. | Windows Server | Database failure or unusual queries. | Detects performance issues or potential misuse of SQL databases, which store critical business data. | High | Monitor for high conditions like query overload or unavailability. |
| File Access Monitoring | Tracks file access/modifications | All | Rapid file deletions, unauthorized access. | Detects ransomware or unauthorized tampering. | High | Monitors High Rapid file activity or unauthorized access. |

# **Discussion Section**

In this section, we analyze the connections between each sensor, its associated Indicators of Compromise (IoCs), and the thresholds that help identify vulnerabilities, risks, and anomalies. The relationship between these elements ensures that each sensor plays a critical role in monitoring, detecting, and mitigating threats to Big Dog’s systems.

**1. HTTP Load Time Sensor**

• IoCs: Malicious redirects, DDoS attacks, content injection.

• Connection: A sudden increase in page load time can indicate a DDoS attack, web-based content injection, or unauthorized redirects. These anomalies align with the IoCs by disrupting normal page behavior.

• Threshold: Monitors high conditions—significant spikes in page load time—suggesting a need for immediate investigation.

**2. MySQL Database Query Sensor**

• IoCs: Unauthorized access, SQL Injection attacks.

• Connection: Anomalies in query execution time or patterns can signify SQL injection attempts or misuse of the database, both of which could compromise sensitive data. This sensor directly detects suspicious database activity.

• Threshold: Monitors high execution times and unusual patterns to identify unauthorized access.

**3. SSH Sensor**

• IoCs: Brute-force attacks, unauthorized access.

• Connection: Multiple failed login attempts or unexpected successful access suggest a brute-force attempt or compromised credentials.

• Threshold: Monitors high conditions (spikes in failed logins) and low conditions (unexpected or unauthorized logins).

**4. Antivirus Status Sensor**

• IoCs: Malware infections, ransomware attacks.

• Connection: Outdated or disabled antivirus software increases the risk of malware and ransomware threats. Monitoring antivirus status ensures endpoint security remains intact.

• Threshold: Monitors low conditions, such as outdated definitions, inactive scans, or disabled antivirus systems.

**5. File Sensor**

• IoCs: Unauthorized file changes, insider threats, leaks.

• Connection: This sensor detects any unauthorized file modifications, deletions, or unusual activity, which can indicate insider threats or data exfiltration attempts.

• Threshold: Monitors both high and low conditions, including frequent edits or unauthorized access to critical files.

**6. Windows Event Log Sensor**

• IoCs: Unauthorized access, system exploits, failed logins.

• Connection: Log anomalies like repeated failed login attempts or the deletion of system records align with potential exploits, unauthorized access, or insider threats.

• Threshold: Monitors high conditions (numerous failed logins) and low conditions (deletion or tampering of logs).

**7. Bandwidth Usage Sensor**

• IoCs: Data exfiltration, DDoS attacks.

• Connection: Significant spikes in network traffic can indicate a DDoS attack or unauthorized data exfiltration. Monitoring bandwidth provides early detection of malicious activity.

• Threshold: Monitors high conditions, such as abnormal increases in traffic.

**8. CPU Load Sensor**

• IoCs: Performance degradation.

• Connection: Unexpected spikes in CPU usage may suggest resource exhaustion due to DDoS attacks or underlying malicious processes consuming resources.

• Threshold: Monitors high conditions, such as CPU usage spikes.

**9. Memory Usage Sensor**

• IoCs: Memory exhaustion, performance slowdowns.

• Connection: Monitoring memory usage prevents disruptions caused by memory leaks or malicious processes exhausting system resources.

• Threshold: Monitors high conditions, such as excessive memory usage.

**10. IIS Response Time Sensor**

• IoCs: DDoS attacks, slow server responses.

• Connection: Increased response latency could indicate DDoS attacks or overloaded servers. Timely detection helps maintain web server availability.

• Threshold: Monitors high conditions, specifically increased response latency.

**11. SSL Certificate Check Sensor**

• IoCs: Expired or invalid certificates.

• Connection: Expired SSL certificates compromise HTTPS security, exposing systems to man-in-the-middle attacks or insecure connections.

• Threshold: Monitors low conditions, such as impending certificate expiration.

**12. Syslog Monitoring Sensor**

• IoCs: Anomalous activities, misconfigurations.

• Connection: Centralized log analysis detects unusual activities, like unauthorized system changes or suspicious events, aiding proactive threat detection.

• Threshold: Monitors high conditions for suspicious events or anomalies.

**13. DHCP/DNS Status Sensor**

• IoCs: Service outages, misconfigurations.

• Connection: Monitoring DNS/DHCP ensures network reliability, identifying potential outages, misconfigurations, or delays that can impact operations.

• Threshold: Monitors both high and low conditions, including failures and slow responses.

**14. Firewall Status Sensor**

• IoCs: Misconfigurations, inactive firewalls.

• Connection: Proper firewall configurations prevent unauthorized access and protect the network perimeter. Monitoring rule changes or inactivity mitigates security risks.

• Threshold: Monitors high conditions (rule changes) and low conditions (inactive firewalls).

**15. Vulnerability Scanning Sensor**

• IoCs: Unpatched vulnerabilities, configuration weaknesses.

• Connection: Ensures testing tools identify gaps in system security. Delayed results or scanning failures may compromise the detection process.

• Threshold: Monitors high conditions, such as scanning delays or tool failures.

**16. Network Traffic Sensor**

• IoCs: Data exfiltration, intrusions.

• Connection: Unusual traffic patterns can indicate unauthorized data transfers or malware-related activities. Early detection prevents data breaches.

• Threshold: Monitors high conditions, such as unexpected traffic spikes.

**17. Security Patch Status Sensor**

• IoCs: Outdated systems, unpatched vulnerabilities.

• Connection: Ensures systems are updated to reduce exposure to known vulnerabilities. Missing or overdue patches increase the attack surface.

• Threshold: Monitors high conditions for missing or overdue patches.

**18. Network Port Activity Sensor**

• IoCs: Unauthorized or excessive port usage.

• Connection: Open or unusual ports could signal potential breaches, malware communication, or misconfigurations.

• Threshold: Monitors high conditions, such as unauthorized or excessive port activity.

**19. SQL Server Health Sensor**

• IoCs: Database failures, unusual queries.

• Connection: Ensures database availability and monitors anomalies like failed connections or malicious queries.

• Threshold: Monitors high conditions, such as query overload or server downtime.

**20. File Access Monitoring Sensor**

• IoCs: Unauthorized access, rapid file deletions.

• Connection: Tracks file access/modifications to detect ransomware, unauthorized deletions, or tampering.

• Threshold: Monitors high conditions, such as excessive file activity or unauthorized access.

# **Recommendation Section**

**Enable SSL/TLS Certificate Management**

* **Recommendation**: Automate SSL certificate renewal and implement alerts for expiration warnings.
* **Rationale**: Ensuring certificates remain valid and trusted aligns with **OWASP best practices**, as expired certificates can expose the system to man-in-the-middle attacks.

**Implement Network Behavior Analysis**

* **Recommendation**: Deploy Network Behavior Analysis tools to monitor deviations in network traffic. This would complement the **Bandwidth Usage Sensor** and **Network Traffic Sensor**.
* **Rationale**: NBA tools can detect **DDoS attacks**, data exfiltration, and malware communications by identifying abnormal traffic patterns.

**Centralize Logging and Monitoring**

* **Recommendation**: Use a **SIEM** system like **Splunk**, **ELK**, or **IBM QRadar** to aggregate and analyze logs from all sensors (e.g., **Windows Event Log Sensor**, **Syslog Monitoring**).
* **Rationale**: Centralized logging improves visibility, correlates anomalies, and simplifies incident response, as outlined in **NIST SP 800-92**.

**Video Presentation Link:**

# **References**

National Institute of Standards and Technology. (n.d.). *The NIST Cybersecurity Framework (CSF) 2.0*. NIST CSWP 29. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>

*Initial Access, Tactic TA0001 - Enterprise | MITRE ATT&CK®*. (n.d.). <https://attack.mitre.org/tactics/TA0001/>

*Credential Access, Tactic TA0006 - Enterprise | MITRE ATT&CK®*. (n.d.). <https://attack.mitre.org/tactics/TA0006/>

*List of notification triggers and supported sensors | PRTG Manual*. (n.d.). PAESSLER. <https://www.paessler.com/manuals/prtg/list_of_notification_triggers_and_supported_sensors>

Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce. (n.d.). *About the RMF - NIST Risk Management Framework | CSRC | CSRC*. <https://csrc.nist.gov/Projects/risk-management/about-rmf>

*CVSS v4.0 Specification Document*. (n.d.). FIRST — Forum of Incident Response and Security Teams. <https://www.first.org/cvss/v4.0/specification-document>

*The 18 CIS Critical Security Controls*. (2021, October 28). CIS. <https://www.cisecurity.org/controls/cis-controls-list>