**Report**

# Risks & Vulnerabilities

Student: Ismail Yasin

**Date 23.01.2024**

**Lighthouse Labs**

**Table of Contents**

1. Executive Summary…………………………………………………………………………………………………………………. page 3
2. Table of Sensors………………………………………………………………………………………………….Page 3
   1. HTTP Load Time Sensor Page……………………………………………………………………….Page 3
   2. MySQL Database Query Sensor…………………………………………………………….…..…Page 3
   3. MSSQL Database Query Sensor……………………………………………………………………Page 3
   4. SSH Sensor…………………………………………………………………………………………………..Page 3
   5. Antivirus Status Sensor……………………………………………………………………………….Page 4
   6. File Sensor………………………………………………………………………………………….………Page 4
   7. Windows Event Log Sensor……………………………………………………………….……….Page 4
   8. Bandwidth Usage Sensor…………………………………………………………………………..Page 4
3. Discussion……………………………………………………………………………………………………………………………Page 5
4. Recommendations……………………………………………………………………………………………………………...Page 5
5. References…………………………………………………………………………………………………………………………..Page 5
6. **Cat Scan II Big Dog**

This report I will demonstrate a comprehensive analysis and recommendations for sensor monitoring in the context of the case study Company, Cat Scan II. The selected sensors cover a range of assets, including web servers, databases, operating systems, and network infrastructure. The prioritization is based on the criticality of assets, associated vulnerabilities, and potential threats. The Security Impact Level (SIL) is assigned to each sensor to guide the implementation of monitoring solutions.

A high and medium ranking was assigned to the top SILs, which included HTTP Load Time-Winserver, HTTP Load Time-Linux, MSSQL Database Winserver, Antivirus Status Sensor, and SSH Sensor.My thresholds were established in a manner that wasconsistent with the priority levels of the sensors.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sensor** | **Description** | **System** | **LoCs Associated** | **Rationale** | **Priority** | **Thresholds/Assumptions** |
| HTTP Load Time | Monitors the time it takes for the page to load. | Window server | May be 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 (SIL of 7, see assumptions) | Changes of 20% over the average load. SIL base on the fact that BIG DOG does NOT have a large Web Presence, the linux web server being internal and this one outward facing(Assumption) There is a relatively low impact on CIA (specifically A) but a higher chance of compromise I have assigned an SIL of 7 |
| HTTP Load Time(1) | Monitors the time it takes for the page load[1] | Linux | Malicious redirects, DDoS attacks, content injection. | Unexpected changes in load time can indicate anomalies or performance-related issues that could be indicative of a security breach or may impact page load | Medium (SIL of 8 see  assumptions) | Change of over 15% Average load have very high priority reason BIG DOG Linux Server use by Developers Intellectual property (IP) for the Company. |
| MySQL Database Query Sensor(2) | Keep track of MySQL database requests. abnormal queries & runs search requests | Linux | IoCs include SQL injection attempts, Unauthorized data retrieval | Abnormal database queries or search request may indicate unauthorized access or attempts to exploit vulnerabilities in the MySQL database. | Medium (SIL of 6 see  assumptions) | Changes of 20% over average load. Has low impact on CIA(availability).There is a medium impact on the LInux Server since  It does not have the SQL Database with client information. |
| MSSQL Database Query Sensor(3) | Keep track of SQL database activities | Winserver | Unusual or unauthorized database access, may indicate brute force attacks and SQL injection attempts | Abnormal database queries may indicate unauthorized access or attempts. May indicate unusual data retrieval patterns that could be indicative of an attack. | High (SIL of 8 see  assumptions) | Changes of 19% over average load.  Anomalous or unauthorized database queries. High priority Window Server contains SQL database with client information. |
| SSH Sensor(4) | Uses remote system access to system and executes a file that is located on the target system | Winserver/Linux | Simultaneous sessions, logins, and multiple connection failures. | Chosen for anomalous behavior detection and security monitoring Or an attempted breach. | High (SIL of 8 see  assumptions) | Changes of over 13% average load. This has a high priority  Reason privacy is the most important asset to the organization but if a file that takes all of the data is executed on the system then there will be a big loss of privacy. |
| Antivirus Status Sensor(5) | Monitors the status of antivirus software, to protect any malware which cause give backdoor access to attacker access system or damage cause. | Window Server, Window desktop, Linux | It could be Malware infections, disabled antivirus protection | Changes in antivirus status may indicate malware infections or compromised systems. | High (SIL of 8 see  assumptions) | Changes of over 25% average load. High priority for all systems  Reason it’s the main sensor that’s used to detect unusual activity. |
| File Sensor(6) | Monitors files located on the Systems | Win server/Linux | Unauthorized access malicious file change | Unexpected changes to files could be a sign of bad or unauthorized behavior. | High (SIL of 5) | Changes of over 30%  Average load. Priority  medium over all  computers in the  network because  there will be a need to  continuously make  changes to files in the  Company |
| Windows Event Log Sensor(7) | Monitoring Windows event logs insights activities health of Windows operating system. System Health, Security Monitoring, Troubleshooting and Diagnostics | Win server | Security Events, System Errors | To detect security incidents and for active monitoring. | High (SIL of 7) | Changes over 25% average load.The Windows server has more sensitive data, hence priority medium is greater. |
| Windows Event Log Sensor(8) | Observes the vents and processes | Window 1, 2 | Application crashes, security events | Unusual events in windows logs may indicate | Medium(SIL of 6, see the assumptions) | Changes over 25% average load.Little impact on CIA Triad and less priority than Windows Server. |
| Bandwidth Usage Sensor(9) | Monitoring bandwidth usage to measure the amount of network bandwidth, devices consumption, applications, or services in a computer network. | All | DDos Attacks Unusual traffic patterns | Attacks may cause sudden bandwidth spikes or strange patterns. | High (SIL of 7) | Average load changes over 31%. Priority is 7 over all network computers and affects CIA. |

1. **Discussion:**

To establish a robust security framework, Big Dog, the company under monitoring, strategically deploys a diverse array of sensors across its network. These sensors are meticulously selected to detect specific Indicators of Compromise (IoCs), contributing to the company's proactive stance against potential security threats.

The chosen sensors exhibit a range of functionalities, from the MySQL Database Query sensor on the Linux server to the HTTP Load Time sensor, which is compatible with both Window Server and Linux environments. The primary objective of these sensors is to identify anomalies that could indicate security vulnerabilities or threats. For example, the HTTP Load Time sensor scrutinizes variations in a website's loading speed, aiming to identify potential issues like denial-of-service attacks or unauthorized redirections.

In alignment with the company's commitment to privacy protection, the MySQL Database Query sensor, operating on Linux, targets SQL injection attempts and unauthorized data extraction, safeguarding the confidentiality and integrity of the company's assets.

The SSH Sensor, active on both Windows Server and Linux, plays a crucial role by monitoring unsuccessful login attempts and concurrent sessions. This proactive approach aligns with the company's emphasis on safeguarding privacy and preventing unauthorized access.

Assigning a Specific Impact Level (SIL) to each sensor is a key aspect of the security architecture. The SIL reflects the significance of associated IoCs and potential risks. For instance, the high priority (SIL of 8) assigned to the MSSQL Database Query sensor on the Win Server underscores the critical importance of protecting SQL databases containing client data.

Thresholds are set to notify the organization of deviations from typical system behavior, serving as benchmarks for anomaly identification. By implementing these security measures, Big Dog aims to maintain a vigilant and resilient defense against evolving cyber threats, ensuring the security, privacy, and integrity of its network and sensitive data.

1. **Recommendations:**

To enhance Cat Scan II's system security, I recommend adopting industry best practices by incorporating additional security sensors. Consider implementing Network Intrusion Detection Systems (NIDS) to strengthen network threat detection, following CIS Control 3. For improved endpoint protection, integrate advanced Endpoint Detection and Response (EDR) solutions in line with MITRE ATT&CK's guidelines. Utilize Security Information and Event Management (SIEM) tools, aligned with the NIST Cyber security Framework, for centralized log analysis and enhanced threat detection. Expanding File Integrity Monitoring (FIM) practices, as suggested by CIS Control 1, ensures continuous monitoring of system files. These measures, coupled with routine security training, patch management, least privilege access controls, incident response planning, and vulnerability assessments (CIS Control 2 and 5), provide a solid foundation for a more resilient security posture, aligning with industry standards.

1. **References:**
2. *PRTG manual. (n.d.).* [*https://manuals.paessler.com/index.html*](https://manuals.paessler.com/index.html)
3. *PRTG Manual: MySQL V2 Sensor. Paessler. (n.d.). https://www.paessler.com/manuals/prtg/mysql\_v2\_sensor*
4. *PRTG Manual: SSH script sensor. Paessler. (n.d.-b). https://www.paessler.com/manuals/prtg/ssh\_script\_sensor*
5. *Wikimedia Foundation. (2024, January 3). Antivirus software. Wikipedia. https://en.wikipedia.org/wiki/Antivirus\_software*
6. *PRTG manual: Event log (windows API) sensor. Paessler. (n.d.-a). https://www.paessler.com/manuals/prtg/event\_log\_windows\_api\_sensor*
7. *PRTG Manual: Ping Sensor*. Paessler. (n.d.-c). https://www.paessler.com/manuals/prtg/ping\_sensor
8. *PRTG Manual: FTP Sensor*. Paessler. (n.d.-b). https://www.paessler.com/manuals/prtg/ftp\_sensor
9. Paessler AG. (2024, January 10). *Bandwidth monitoring made easy with PRTG*. Paessler. https://www.paessler.com/bandwidth\_monitoring
10. *Mitre ATT&CK®*. MITRE ATT&CK®. (n.d.). <https://attack.mitre.org/>
11. *Cybersecurity framework*. NIST. (2023, December 21). https://www.nist.gov/cyberframework