**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

****

1. **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 medium 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 8.5 see  assumptions) | Changes of 12% over the average load. SIL of 8.5 and SC of high indicates the importance of monitoring this sensor for any change in activity. The use of a Linux system proves its high importance to Big Dog. Confidentiality, according to the CIA triad, is of very high importance in this case as confidential private information is to be secured and given high priority. |
| 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 8.5 see  assumptions) | Changes of 15% over the average threshold load. SIL of 8.5 and SC of high should indicate to Cat that this sensor on the Win Server is of high priority. Accessing private & confidential information is at key here and Big Dog holds privacy to be the most important. |
| 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 14% over the average threshold load. SIL of 8 and a SC of high should indicate to Cat that SSH sensor is of high importance and priority. This sensor allows for secure communication between client and server therefore confidentiality, integrity and availability is of high importance. |
| 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 8.5 see  assumptions) | Changes of 17% over the average threshold load. SIL of 8.5 and SC of high should tell Cat that this sensor is of high importance. Antivirus applications that are either disabled, or outdated affecting the detection of malicious activities happening that the system would otherwise be alerted of. This is also on all servers including Linux therefore Availability is high. |
| 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. | Medium (SIL of 6) | Changes of 22% over the average threshold load. SIL of 6 and SC of medium indicates to Cat that this sensor is of medium importance. Availability & Integrity high. |
| 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. | Medium (SIL of 7) | Changes of 21% over the average threshold load. SIL of 7 and SC of medium indicates to Cat that this sensor is of medium importance. Availability & Integrity high. |
| 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 of 21% over the average threshold load. SIL of 6 and SC of medium indicates to Cat that this sensor is of medium importance. Availability & Integrity high. |
| 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. | medium (SIL of 7) | Changes of 21% over the average threshold load. SIL of 7 and SC of medium indicates to Cat that this sensor is of medium importance. Availability & Integrity high. |

1. **Discussion:**

After conducting the aforementioned analysis, it is essential to delve into a more detailed discussion with Cat regarding the critical sensors that necessitate meticulous monitoring, along with the rationale behind such prioritization. The MySQL database query sensor on the Linux server emerges as the paramount sensor, demanding top priority. With a security impact level of 8.5 and a high security categorization, this sensor holds significant importance. Indicators of compromise, such as unauthorized access attempts and include SQL injection attempts, unauthorized data retrieval, potentially signaling an attacker's attempt to breach the system, underscore the need for vigilant monitoring.

Additionally, the client Big Dog places a substantial emphasis on privacy and proprietary rights, especially concerning the use of a Linux server by developers for generating crucial proprietary intellectual property. Adhering to the principles of the CIA Triad, the company accords high importance to confidentiality, recognizing the imperative of securing private information. Setting the threshold at no more than 12% ensures that Cat is promptly alerted to even the slightest changes. This aligns with the principles outlined in the NIST Risk Management Framework, emphasizing the importance of swift notification to enable Cat in selecting, implementing, assessing, authorizing, and monitoring potential anomalies.

Another critical sensor deserving of Cat's focused attention is the SSH sensor, operational on both Windows Server and Linux platforms. Facilitating secure communication between client’s and. Assigned a security impact level of 8 and a high security classification, this sensor is instrumental in detecting unusual login attempts and failed authentications, indicative of potential brute-force attacks. Any change exceeding 14% in the threshold load triggers alerts to Cat, ensuring proactive intervention against malicious activities such as brute-force attacks.

Given Big Dog's commitment to prioritizing client privacy, the company places utmost importance on confidentiality, integrity, and availability. Timely monitoring and alerting of activities, particularly those suggestive of potential threats such as brute-force attacks, are imperative to prevent the compromise of personal and confidential information. The alignment with Big Dog's emphasis on privacy underscores the significance of confidentiality, integrity, and availability in safeguarding their interests.

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