**Report**

# Risks & Vulnerabilities

Student: Ismail Yasin

**Date 22.01.2024**

**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.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **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 | Monitors the time it takes for the page load | 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 compromise | Medium (SIL of 7) | Changes of 25% over the average load. SIL based 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. |
| MySQL Database Query Sensor | Keep track of MySQL database requests. abnormal queries that result in unsafe database or unauthorized changes | Linux | It could be Unusual or unauthorized database queries | Abnormal database queries may indicate unauthorized access or attempts to exploit vulnerabilities in the MySQL database. | High (SIL of 9) | Anomalous or unauthorized database queries. There is a relatively high impact on CIA (specifically CIA) but a higher chance of compromise. I have assigned an SIL of 9. |
| MSSQL Database Query Sensor | Keep track of MySQL database requests. abnormal queries that result in unsafe databases or unauthorized changes | Winserver | Unusual or unauthorized database queries | Abnormal database queries may indicate unauthorized access or attempts to exploit vulnerabilities in the MSSQL database. | High (SIL of 9) | Anomalous or unauthorized database queries. There is a relatively high impact on CIA (specifically CIA) but a higher chance of compromise. I have assigned an SIL of 9. |
| SSH Sensor | Uses remote system access to keep an eye on any login attempts or activity. | Winserver/Linux | It could be Unusual SSH login attempts, unauthorized access to systems. | Detection of unauthorized access attempts via SSH, which could indicate a security compromise or an attempted breach. | High (SIL of 8) | Multiple failed login attempts, anomalous SSH activity. There is a relatively medium impact on CIA (specifically CI) but a higher chance of compromise. I have assigned an SIL of 8. |
| Antivirus Status Sensor | 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 7) | Disabled antivirus protection, detection of known malware. There is a relatively high impact on CIA (specifically CIA) but a low chance of compromise. I have assigned an SIL of 9. |
| File Sensor | Mechanism used to track changes, access, or other activities related to files within a computer system. | Win server/Linux | Unauthorized file changes, deletion, or access | Detection of suspicious file activities that may indicate unauthorized access or malware presence. Unauthorized file transfer or modification of losing integrity. | High (SIL of 8) | Unexpected file changes, deletions, or access. There is a relatively Medium impact on CIA (specifically CIA) but a higher chance of compromise. I have assigned an SIL of 9. |
| Windows Event Log Sensor | Monitoring Windows event logs insights activities health of Windows operating system. System Health, Security Monitoring, Troubleshooting and Diagnostics | Win server | Security-relevant events, authentication failures, policy changes. Security Monitoring | Detection of security-related events and unauthorized access in Windows systems and System changes. | High (SIL of 8) | Anomalous events, authentication failures, policy changes. There is a relatively Medium impact on CIA (specifically CIA) but a higher chance of compromise. I have assigned an SIL of 8. |
| Bandwidth Usage Sensor | Monitoring bandwidth usage to measure the amount of network bandwidth, devices consumption, applications, or services in a computer network. | Windows, Linux | It could be Unusual or excessive bandwidth consumption | Detection of potential network-based attacks, data exfiltration, or abnormal activity that may impact bandwidth usage. | High (SIL of 8) | Unusual or excessive bandwidth consumption. There is a relatively high impact on CIA (specifically CIA) but a medium chance of compromise. I have assigned an SIL of 8. |

**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.

**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 Cybersecurity 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.

**References:**

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