Project 2 – Report on Risk and Vulnerability

Cat Scan II Big Dog – Fahad Shahzad

Table of Contents

Executive Summary

After reviewing the assigned tasks, Big Dog provided us with a list of assets along with their preferred ranking of how they classify information. The assets include a Windows and Linux machines hosting webservers facing externally and internally, respectively. Big Dog also has Linux machines for their developers to create proprietary software. Furthermore, a bunch of windows machines for functions such as sales, marketing, and management. And lastly, using Kali machines to host IT and Testing systems.

Knowing this, our recommendations for sensors using PRTG focus on enhancing network monitoring using sensors like mySQL Database query sensor, File and directory sensor, HTTP load sensor and bandwidth sensors to ensure optimal performance and proactive resolutions. Furthermore, to implement SNMP sensors as to monitor network devices such as switches, routers, and firewalls. These sensors provide real-time insights into device health, bandwidth usage, and interface status, enabling administrators to detect anomalies and address potential issues promptly. By also implementing a SSH sensor, we can monitor remote access traffic on both Windows and Linx servers, allowing us to detect and respond to potential security breach to sensitive data. By using these, we can protect and monitor Big Dog's major concerns regarding information security, by covering privacy, proprietary, and admin.

By leveraging these recommended sensors, the organization can gain deeper visibility into their IT infrastructure, optimize resource allocation, and ensure seamless operations all while being able to protect and be immediately notified about changes to their sensitive and proprietary assets/information. Overall, the recommended sensor strategy empowers organizations to proactively manage their networks, improve efficiency, and deliver a superior user experience.

The Scenario

General Assets

The below are the network systems that Big Dog is using to host various operating systems, and each of those operating systems hosts their own services and applications.

First is their Windows Server which hosts the following:

- SQL database to store and process information in a relational database.
- IIS webserver to host their external webserver.
- PRTG Network Monitor to be able to manage all security sensors.

They are also using a Linux machine to:

- Used by developers to create intellectual property (IP)
- Also have an internal facing webserver.

Big Dog also makes use of Windows Workstations for different departments such as:

- Sales
- Marketing
- Management Functions

Lastly, they also make use of Kali OS to manage their IT internal operations, lab setups, and other sandboxing facilities using the below systems:

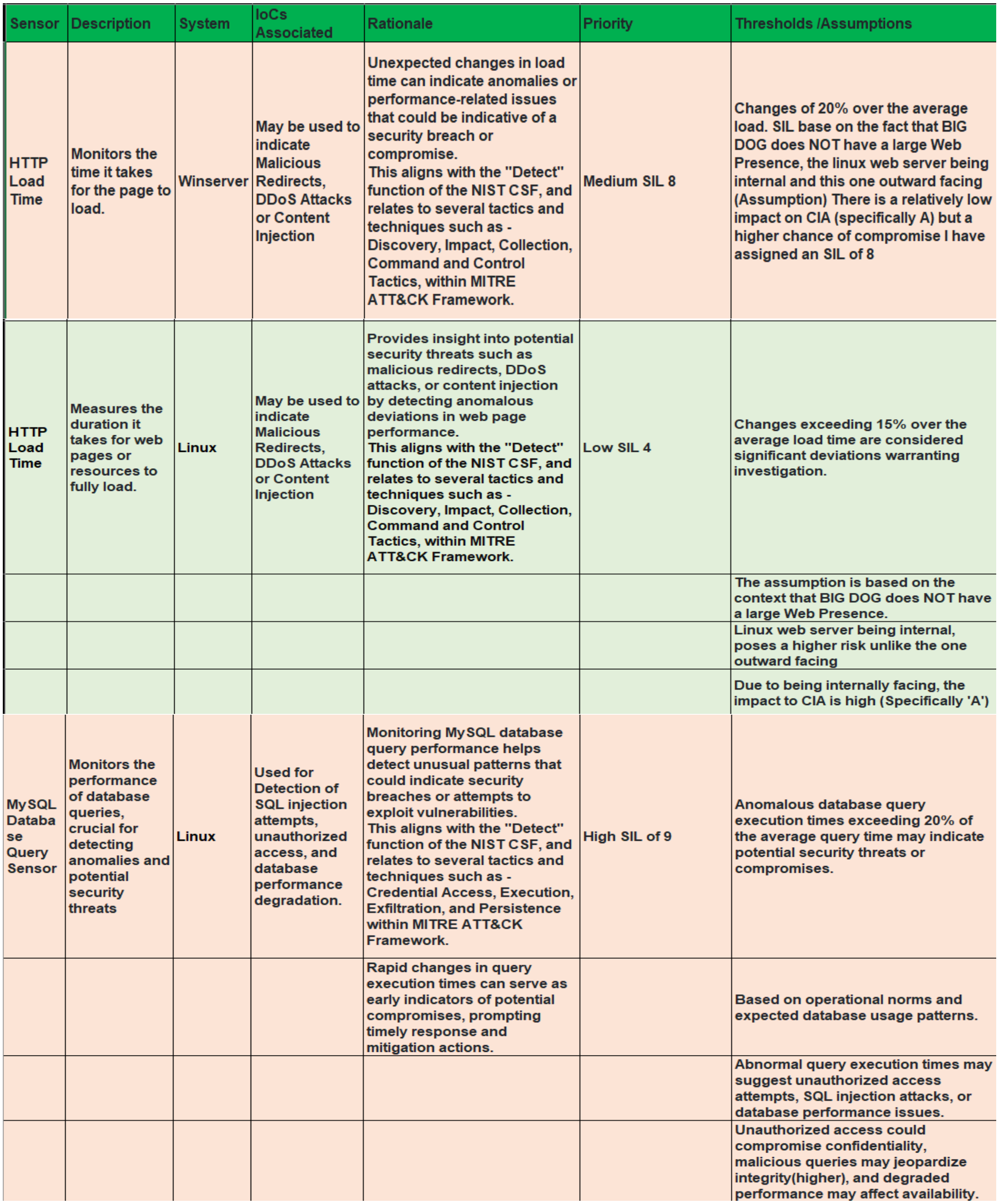
- Test Systems
- IT systems

Information Classification Ranking

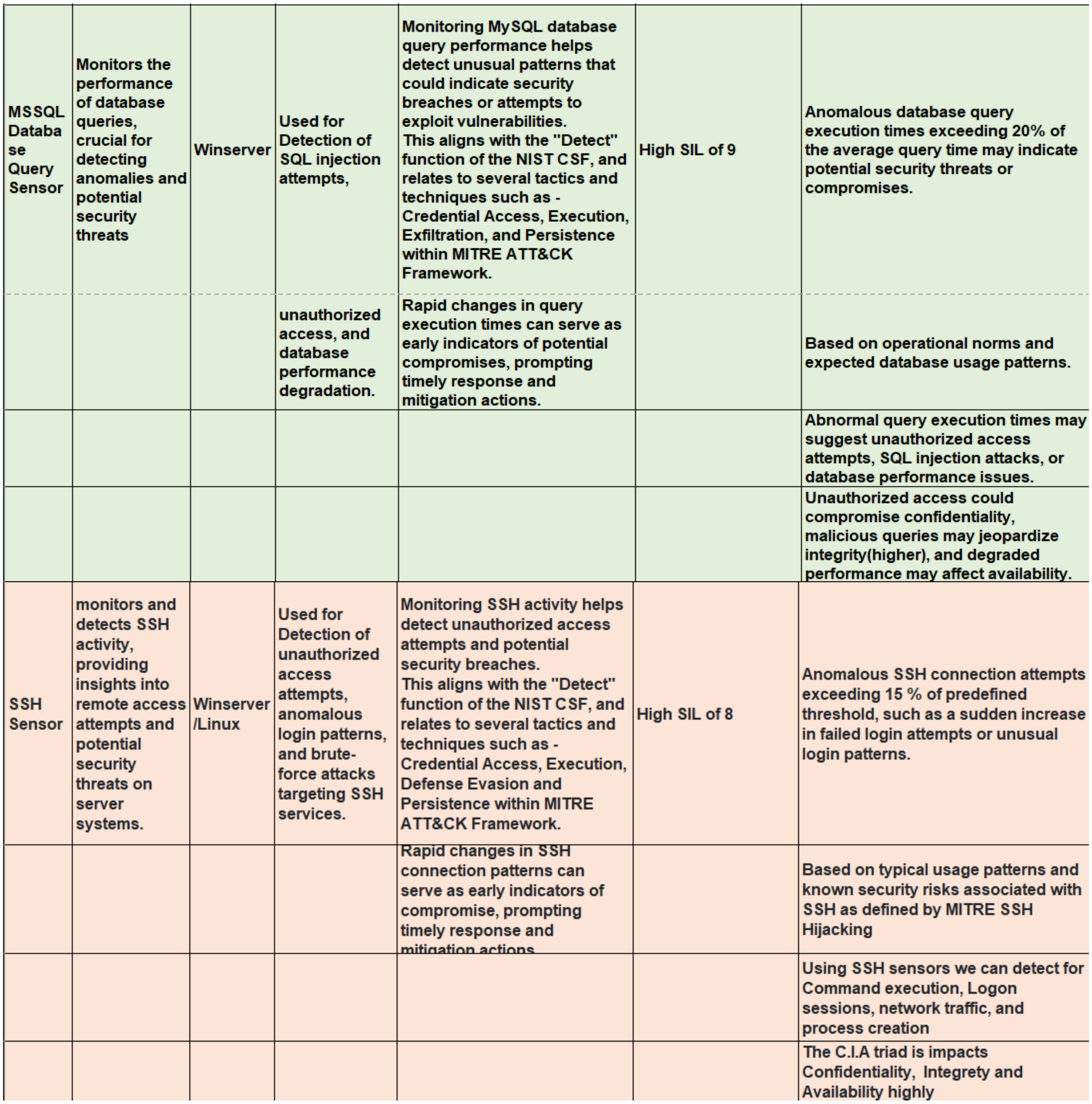
Big Dog has prioritized and listed out what and how they like to organize their information from highest importance to lowest importance, as shown below:

- Privacy (P)
- Proprietary (IP)
- Admin (A)
- Financial/accounting (F)
- Security Management (SM)
- Systems (S)

Sensor Table

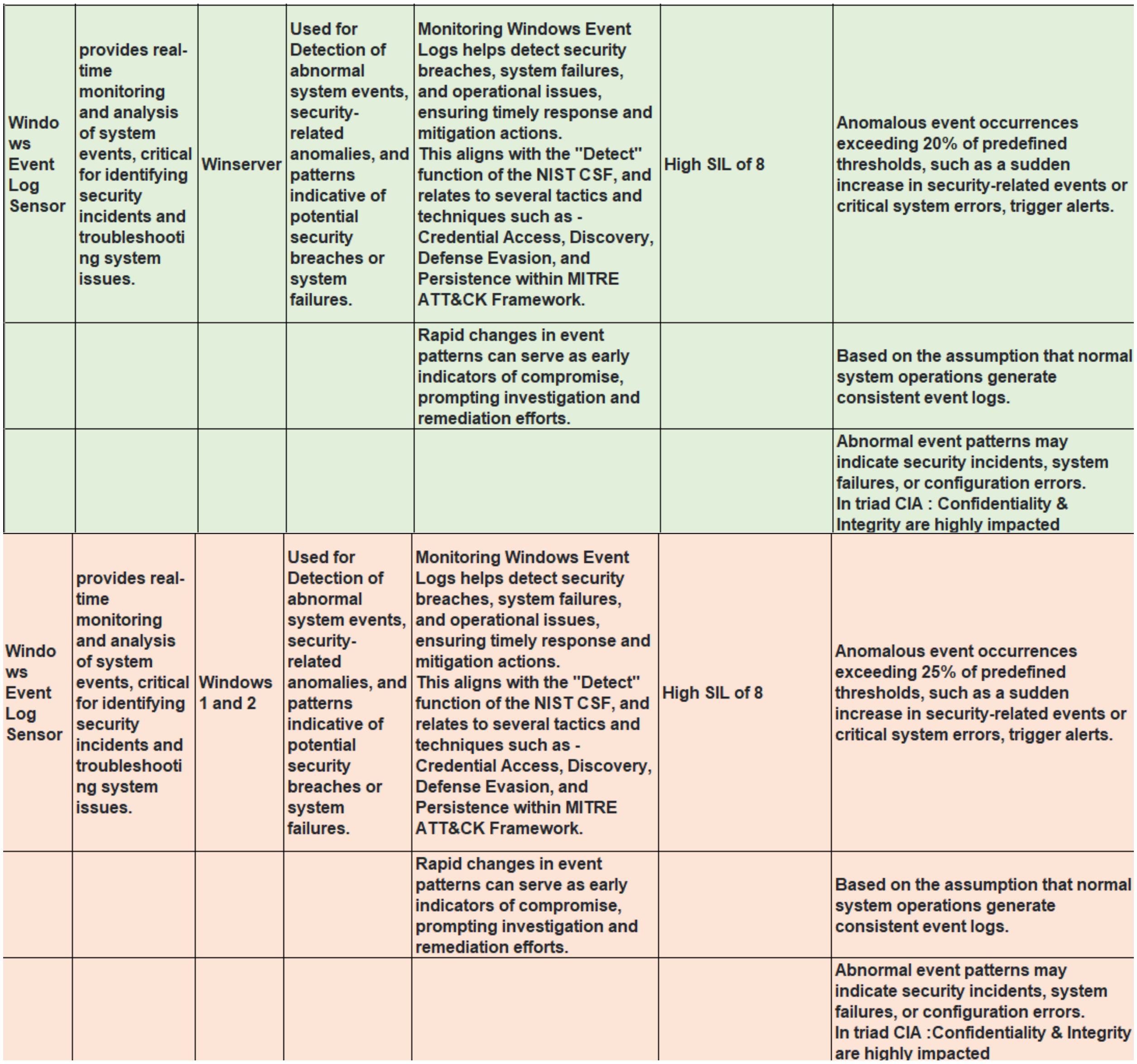


Sensor	Description	System	IoCs Associated	Rationale	Priority	Thresholds /Assumptions
HTTP Load Time	Monitors the time it takes for the page to load.	Winserver	May be used to indicate Malicious Redirects, DDoS Attacks or Content Injection	Unexpected changes in load time can indicate anomalies or performance-related issues that could be indicative of a security breach or compromise. This aligns with the "Detect" function of the NIST CSF, and relates to several tactics and techniques such as - Discovery, Impact, Collection, Command and Control Tactics, within MITRE ATT&CK Framework.	Medium SIL 8	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 8
HTTP Load Time	Measures the duration it takes for web pages or resources to fully load.	Linux	May be used to indicate Malicious Redirects, DDoS Attacks or Content Injection	Provides insight into potential security threats such as malicious redirects, DDoS attacks, or content injection by detecting anomalous deviations in web page performance. This aligns with the "Detect" function of the NIST CSF, and relates to several tactics and techniques such as - Discovery, Impact, Collection, Command and Control Tactics, within MITRE ATT&CK Framework.	Low SIL 4	Changes exceeding 15% over the average load time are considered significant deviations warranting investigation.
						The assumption is based on the context that BIG DOG does NOT have a large Web Presence.
						Linux web server being internal, poses a higher risk unlike the one outward facing
						Due to being internally facing, the impact to CIA is high (Specifically 'A')
MySQL Database Query Sensor	Monitors the performance of database queries, crucial for detecting anomalies and potential security threats	Linux	Used for Detection of SQL injection attempts, unauthorized access, and database performance degradation.	Monitoring MySQL database query performance helps detect unusual patterns that could indicate security breaches or attempts to exploit vulnerabilities. This aligns with the "Detect" function of the NIST CSF, and relates to several tactics and techniques such as - Credential Access, Execution, Exfiltration, and Persistence within MITRE ATT&CK Framework.	High SIL of 9	Anomalous database query execution times exceeding 20% of the average query time may indicate potential security threats or compromises.
				Rapid changes in query execution times can serve as early indicators of potential compromises, prompting timely response and mitigation actions.		Based on operational norms and expected database usage patterns.
						Abnormal query execution times may suggest unauthorized access attempts, SQL injection attacks, or database performance issues.
						Unauthorized access could compromise confidentiality, malicious queries may jeopardize integrity(higher), and degraded performance may affect availability.

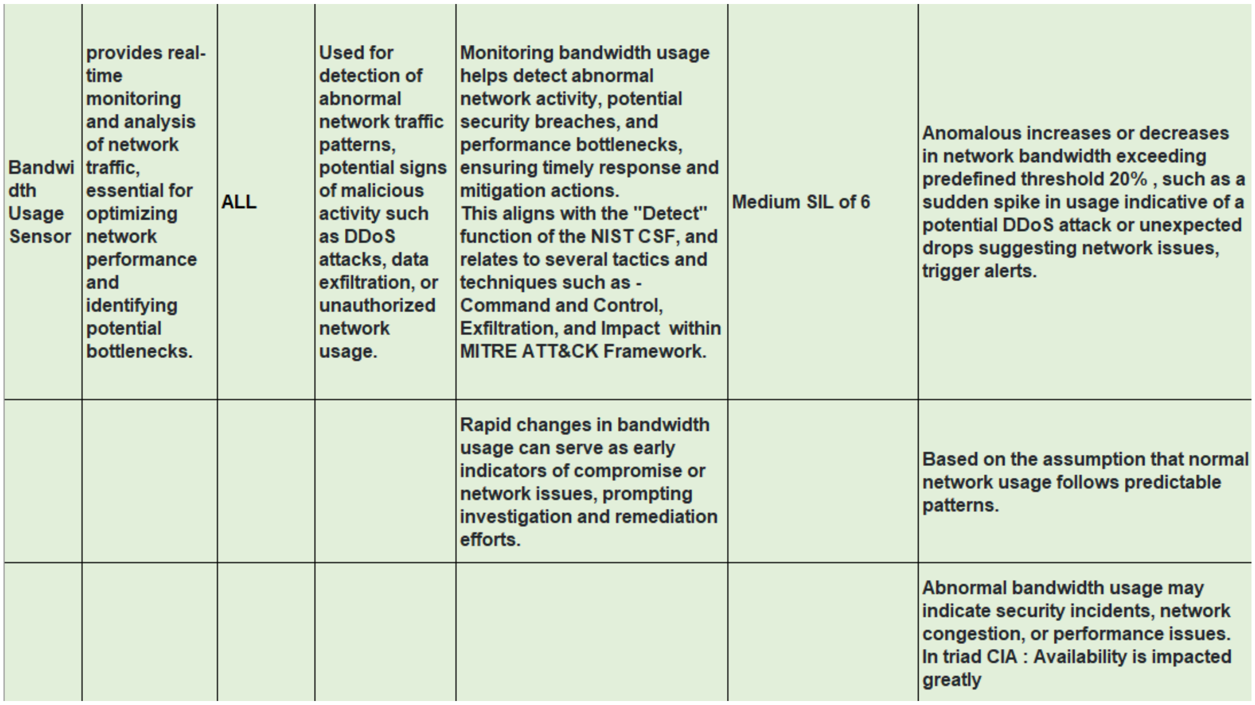


MSSQL Database Query Sensor	Monitors the performance of database queries, crucial for detecting anomalies and potential security threats	Winserver	Used for Detection of SQL injection attempts,	Monitoring MySQL database query performance helps detect unusual patterns that could indicate security breaches or attempts to exploit vulnerabilities. This aligns with the "Detect" function of the NIST CSF, and relates to several tactics and techniques such as - Credential Access, Execution, Exfiltration, and Persistence within MITRE ATT&CK Framework.	High SIL of 9	Anomalous database query execution times exceeding 20% of the average query time may indicate potential security threats or compromises.
			unauthorized access, and database performance degradation.	Rapid changes in query execution times can serve as early indicators of potential compromises, prompting timely response and mitigation actions.		Based on operational norms and expected database usage patterns.
						Abnormal query execution times may suggest unauthorized access attempts, SQL injection attacks, or database performance issues.
						Unauthorized access could compromise confidentiality, malicious queries may jeopardize integrity(higher), and degraded performance may affect availability.
SSH Sensor	monitors and detects SSH activity, providing insights into remote access attempts and potential security threats on server systems.	Winserver /Linux	Used for Detection of unauthorized access attempts, anomalous login patterns, and brute-force attacks targeting SSH services.	Monitoring SSH activity helps detect unauthorized access attempts and potential security breaches. This aligns with the "Detect" function of the NIST CSF, and relates to several tactics and techniques such as - Credential Access, Execution, Defense Evasion and Persistence within MITRE ATT&CK Framework.	High SIL of 8	Anomalous SSH connection attempts exceeding 15 % of predefined threshold, such as a sudden increase in failed login attempts or unusual login patterns.
				Rapid changes in SSH connection patterns can serve as early indicators of compromise, prompting timely response and mitigation actions		Based on typical usage patterns and known security risks associated with SSH as defined by MITRE SSH Hijacking
						Using SSH sensors we can detect for Command execution, Logon sessions, network traffic, and process creation
						The C.I.A triad is impacts Confidentiality, Integrety and Availability highly

Antivirus Status Sensor	provides real-time monitoring and updates on the antivirus protection status across systems, crucial for identifying potential security threats and ensuring endpoint security.	All	Detection of malware infections, presence of suspicious files, and indicators of compromised systems based on antivirus scan results.	Monitoring antivirus status helps detect malware infections and potential security breaches, safeguarding system integrity and data confidentiality. This contributes to the "Protect" and "Detect" functions of the NIST CSF and relates to several tactics and techniques such as - Discovery, Execution, Defense Evasion and Persistence within MITRE ATT&CK Framework.	Medium SIL 6	Anomalous antivirus scan results indicating the presence of malware or suspicious files trigger alerts when exceeding 25 % of predefined threshold.
				Rapid changes in antivirus status can serve as early indicators of compromise, prompting timely response and mitigation actions.		Based on the assumption that antivirus software is regularly updated and actively scanning for threats.
						Any deviation from expected antivirus status may suggest a compromise of system integrity or potential security threat. In triad CIA : Integrity is highly affected
File Sensor	monitors file activities, detecting unauthorized access, data breaches, and malware propagation.	Winserver /Linux	Used for Detection of unauthorized file access, data exfiltration, and malware propagation based on anomalous file activities.	Monitoring file activities helps detect unauthorized access attempts, data breaches, and malware propagation, safeguarding system integrity and confidentiality. This aligns with the "Detect" function of the NIST CSF, and relates to several tactics and techniques such as - Exfiltration, Execution, Collection, and Persistence within MITRE ATT&CK Framework.	High SIL of 8	Anomalous file changes or creations exceeding 20% of predefined threshold, such as sudden increases in new or modified files, trigger alerts.
				Rapid changes in file activities can serve as early indicators of compromise, prompting timely response and mitigation actions.		Based on the assumption that file changes occur within expected usage patterns.
						Abnormal file activities may indicate unauthorized access, data exfiltration, or malware propagation. In triad CIA : Confidentiality & Integrity are highly impacted



Windows Event Log Sensor	provides real-time monitoring and analysis of system events, critical for identifying security incidents and troubleshooting system issues.	Winserver	Used for Detection of abnormal system events, security-related anomalies, and patterns indicative of potential security breaches or system failures.	Monitoring Windows Event Logs helps detect security breaches, system failures, and operational issues, ensuring timely response and mitigation actions. This aligns with the "Detect" function of the NIST CSF, and relates to several tactics and techniques such as - Credential Access, Discovery, Defense Evasion, and Persistence within MITRE ATT&CK Framework.	High SIL of 8	Anomalous event occurrences exceeding 20% of predefined thresholds, such as a sudden increase in security-related events or critical system errors, trigger alerts.
				Rapid changes in event patterns can serve as early indicators of compromise, prompting investigation and remediation efforts.		Based on the assumption that normal system operations generate consistent event logs.
						Abnormal event patterns may indicate security incidents, system failures, or configuration errors. In triad CIA : Confidentiality & Integrity are highly impacted
Windows Event Log Sensor	provides real-time monitoring and analysis of system events, critical for identifying security incidents and troubleshooting system issues.	Windows 1 and 2	Used for Detection of abnormal system events, security-related anomalies, and patterns indicative of potential security breaches or system failures.	Monitoring Windows Event Logs helps detect security breaches, system failures, and operational issues, ensuring timely response and mitigation actions. This aligns with the "Detect" function of the NIST CSF, and relates to several tactics and techniques such as - Credential Access, Discovery, Defense Evasion, and Persistence within MITRE ATT&CK Framework.	High SIL of 8	Anomalous event occurrences exceeding 25% of predefined thresholds, such as a sudden increase in security-related events or critical system errors, trigger alerts.
				Rapid changes in event patterns can serve as early indicators of compromise, prompting investigation and remediation efforts.		Based on the assumption that normal system operations generate consistent event logs.
						Abnormal event patterns may indicate security incidents, system failures, or configuration errors. In triad CIA :Confidentiality & Integrity are highly impacted



Bandwidth Usage Sensor	provides real-time monitoring and analysis of network traffic, essential for optimizing network performance and identifying potential bottlenecks.	ALL	Used for detection of abnormal network traffic patterns, potential signs of malicious activity such as DDoS attacks, data exfiltration, or unauthorized network usage.	Monitoring bandwidth usage helps detect abnormal network activity, potential security breaches, and performance bottlenecks, ensuring timely response and mitigation actions. This aligns with the "Detect" function of the NIST CSF, and relates to several tactics and techniques such as - Command and Control, Exfiltration, and Impact within MITRE ATT&CK Framework.	Medium SIL of 6	Anomalous increases or decreases in network bandwidth exceeding predefined threshold 20% , such as a sudden spike in usage indicative of a potential DDoS attack or unexpected drops suggesting network issues, trigger alerts.
				Rapid changes in bandwidth usage can serve as early indicators of compromise or network issues, prompting investigation and remediation efforts.		Based on the assumption that normal network usage follows predictable patterns.
						Abnormal bandwidth usage may indicate security incidents, network congestion, or performance issues. In triad CIA : Availability is impacted greatly

Discussion of Assets and Vulnerabilities

The first sensor implemented will be the HTTP Load time sensor which is monitoring the external webserver hosted on the Winserver. The IoC as mentioned indicates that it is possible to detect a DDoS or content injection attacks. Which is why the threshold set is at 20% while also set as a high priority risk since there is access to the outside network.

The next sensor to be implemented will be the HTTP Load Time sensor which is monitoring the internal webserver hosted on the Linux machine. Now, due to the webserver being closed off from the external web/network, the risk of this being compromised isn't as high, hence prioritized it as low. Furthermore, since the access to resource is already low due to it facing inwards, along with volume of users who will use this being few, setting the threshold at 15% is the most appropriate option.

The sensor implemented thereafter will be the MySQL Database sensor monitoring both Linux and Winserver machines. The before mentioned IoC impacting the database is unauthorized access, content injection, and even SQL injections. If this was to occur, Big Dog organization would be in great trouble, as their proprietary and customer data is most likely to be stored here, which is why the priority is set to High. Regarding the threshold set at 20%, is due to the case where if the database was to increase in size and there is more data added, the sensor would not be triggered falsely.

The SSH sensor is the next to be implemented. This is an important sensor since it will be monitoring SSH activity (remote connection activity). If in the event of a compromise, the organization will be at risk of losing proprietary information and their systems will lose integrity. IoC that come with SSH related risk are unauthorized access and even brute force attacks. And since the number of authorized users will have access and will be signing in on a regular basis is but a few, the set threshold is set at 15%.

Implementing the Antivirus status sensor will be the next course of action, but not of high priority. Since Big Dog as set the information classification requirements for security management to be quite low, yet regarding keeping an active watch on potential threats puts this sensor to a mid priority. The associated IoC with this sensor would lead to an inability to detect malware or even compromised systems. Hence setting the threshold to 25% of detected inconsistencies.

The next sensor to be implemented is the File sensor, which is responsible for monitoring activity on both the Linux and the Winserver. In the case of a compromise, the IoC associated will be to detect all unauthorized access, modifications to documents, creation of files, and any unauthorized activities. Since this is relating to data that is proprietary to the organization along with potential customer information as well, the priority if compromised is High. Which is why, the set threshold is set to 20% to monitor any changes in usage patterns.

Also implemented will be Windows Event log sensors monitoring both Winserver and Linux machines. The IoC as mentioned will relate to any abnormal sign on attempts, systems breach, account creation, and unauthorized access to accounts. And since this is relating to systems access, but also relates to the privacy and security management of the organization at Big Dog, the priority is set to High, which is why the threshold is set to 20% to be able to quickly detect and manage the inconsistencies.

Finally, the Bandwidth sensor will be implemented. This sensor used for monitoring the network traffic flow, doesn't pose a great risk to the organization. The most impact notice will be to availability; hence the priority isn't high. The IoC that is associated with this sensor are being able to detect any abnormal traffic flow, and mainly DDoS attacks. Due to which the threshold is set to 20%.

Recommendations

After looking at the sensors already implemented, understanding where the gaps are is imperative. Below are recommendations that fill potential security gaps and should be implemented to prevent compromise.

1) SSH Hijacking – Since we are already using an SSH sensor to monitor all interactions/commands over an unsecured network. There is still a risk of SSH Hijacking which is unauthorised individuals hijacking existing/active connections of legitimate users already on a SSH session. This is typically done by hijackers taking advantage of public keys. For this reason, the following are recommended counter measures that extend beyond the implemented sensor:

    - M1042 – Disabling and/or removing features/programs.
    - M1027 – Password Policies
    - M1026 – Privileged Account Management
    - M1022 – Restrict File and Directory Permissions

2) Scheduled task/job – Since there are assets that restart, either due to testing or on a regular basis due to being part of the production environment, or because there are updates that need to be implemented. There are going to be functionalities that will initiate planned maintenance. Hijackers can exploit this to execute programs or scripts at startup on a scheduled basis, to gain privilege access. For this reason, the following are recommended counter measures that extend beyond File sensors and Windows event log sensors:

    - M1047 – Audit, which performs scans of systems to identify weaknesses.
    - M1028 – Operating System Configuration to harden against OS changes.
    - M1026 – Privileged Account Management
    - M1022 – Restrict File and Directory Permissions
    - M1018 – User account management
    - Also implement sensor:
        i. While PRTG does not provide an all-around sensor for managing and detecting creation of tasks we can use SCHEDULEDTASK2XML to create a custom sensor to manage existing tasks
        ii. DS0003 – Scheduled job creation to monitor newly constructed tasks/jobs.

3) Data Destruction – After reviewing what assets Big Dog is using, I noticed they are at a great risk of losing all data in the event of a major cyber attack. Data that is related to systems, services and network resources are all at risk of being deleted, encrypted, and/or overwritten. For this reason, the following are recommended counter measures that extend beyond File sensors and Windows event log sensors:

   - M1053 – Data Backup (Disaster Recovery)
   - DS0017 – Monitoring Command Execution occurring on the systems

4) Network Sniffing – This is where criminals can get access to basic information by scanning network traffic, and in some cases if communication is unencrypted then user account data, running service, open/active ports, and more network details. For this reason, the following are recommended counter measures that extend beyond File sensors and Windows event log sensors:

   - M1030- Network segmentation
   - M1032 – Multi-Factor authentication
   - M1041 – Encrypt Sensitive Information

Reference

Available Sensor Types | PRTG Manual. (n.d.).
PAESSLER. https://www.paessler.com/manuals/prtg/list_of_available_sensor_types#linux

MITRE ATT&CK®. (n.d.-b). https://attack.mitre.org/

Remote Service Session Hijacking: SSH Hijacking, Sub-technique T1563.001 - Enterprise | MITRE ATT&CK®. (n.d.). https://attack.mitre.org/techniques/T1563/001/

PRTG Tools Family. (n.d.-b). SCHEDULEDTASK2XML. In *PRTG Tools Family*. https://prtgtoolsfamily.com/manuals/ScheduledTask2XML.pdf

Scheduled Task/Job, Technique T1053 - Enterprise | MITRE ATT&CK®. (n.d.). https://attack.mitre.org/techniques/T1053/

Data Destruction, Technique T1485 - Enterprise | MITRE ATT&CK®. (n.d.). https://attack.mitre.org/techniques/T1485/

Network Sniffing, Technique T1040 - Enterprise | MITRE ATT&CK®. (n.d.). https://attack.mitre.org/techniques/T1040/