**KEHINDE TALABI**

**REPORT**

**(Risks and Vulnerabilities)**

**CAT SCAN II**

**BIG DOG ENVIRONMENT**

Date of submission: 05/11/2024

**TABLE OF CONTENT**

1. Executive Summary……………………………………………………I
2. Table of Sensors……………………………………………………....II
3. Discussion Section………………………………………………....…III
   1. The connections between the Sensors, IoCs, and threshold…...IV
4. Recommendation Section………………………………………….…V
   1. Security Impact Level(SIL)……………………………………VI
   2. Application of SIL in Big Dog Environment Monitoring Dashboard……………………………………………………...VII

5.0 Solution……………………………………………………………………...VIII

6.0 Reference and Citations………………………………………………….IX

**1.0 Executive Summary**

This report is a succinct synopsis that highlights the report’s main conclusions, recommendations and goal. I highlighted the top five SILs (Such as the Windows Event logs, MySQL Database, SSH, Bandwidth Usage, and Anti-virus status sensor) They describe the situations they monitor using PRTG, along with important thresholds. When monitoring using frameworks such as Nist Risk Management, MITRE ATTACK, and MITRE CVE7.When using a sensor to measure tool in the IT environment to detect changes in anomalies in systems, applications, and networks, designed to collect specific data points and look for indicators of compromise(IOCs) such as abnormal traffic, several unauthorized attempts, or modifying files that may cause a security threat

**2.0 Table of Sensor**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Sensor** | **Description** | | | **System** | | **IOCs Associated** | | **Rationale** | **Priority** | | **Thresholds/Assumptions** |
| *HTTP Load Time* | *Monitors the time it takes for the page to load.* | | | Linux | | 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 high, see assumptions***)*** | | Changes of 20% 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 high |
| MySQL  Database  Query  Sensor | Observe the structure and rate of database queries | | | Linux | | SQL Injection, Database DDoS | | Particular pertinent to the MITRE ATT&CK FRAMEWORK, high database query could be a sign of a DDOS effort or SQL Injection attack directed at data | High | | **Threshold**  The value was set to 900 and a minimum of 100, which triggers an alert in the baseline  A high SIL could affect the availability and integrity of the data.  **Assumptions**  Watch for high circumstances; a high SIL could affect the data's availability and integrity. |
| SSH Sensor | monitors SSH access and looks for anomalies. | | | Linux | | Bruteforce, Unauthorized Access | | An excessive number of login attempts could be a sign of brute force attacks, which could jeopardize system access. | High | | **Threshold**  5 login failed attempts within 7 minutes  **Assumptions**  Keep an eye out for excessive login attempts; SSH sensors are given top priority because of the possibility of access-level compromise. |
| Antivirus Status Sensor | checks for status updates and ongoing antivirus activity. | | | All | | Malware, Ransomware | | Active protection against ransomware and malware threats is ensured by real-time antivirus status. | High | | **Threshold**  More than 2 viruses within 5 minutes  **Assumptions**  High and low conditions; if antivirus software is not running or is out of date, it will not be given priority. |
| File Sensor | Monitor file changes and any unauthorized modifications | | | Linux | | Malware, File Tampering | | According to MITRE's data integrity strategies, modifications to sensitive files could be a sign of malware or tampering. | Medium | | **Threshold**  Greater than 30 shows a high condition number of modification  **Assumptions**  Medium SIL because of lower criticality; high change rates indicate compromise risk. |
| Windows Event Log Sensor | Records and evaluations Check the Windows event logs for anomalous occurrences | | | Windows11 | | Unauthorized Access, Privilege Escalation | | Logs show instances of privilege escalation and illegal access that could jeopardize system integrity. | High | | **Threshold**  More than 5 failed logins within 10 minutes  **Assumptions**  Keep an eye out for any unusual activity patterns while in high condition. |
| Bandwidth Usage Sensor | | Monitors network traffic for unexpected spikes. | All | | Data Exfiltration, DDos | | Unexpected network traffic spikes could indicate data exfiltration attempts or a DDoS attack, highlighting the confidentiality risks in MITRE's impact tactics. | | High | **Threshold**  High conditions, sudden spike in outbound traffic, which in the baseline could reach 30%  **Assumptions**  Both conditions (spike in traffic) are critical due to the confidentiality implications. | |

**3.0 Discussion Section**

**3.1 The connections between the Sensors, IoCs, and threshold**

* **Http Load Time Sensor:**

**Connection:** The firewall was obstructing the server and the connection, so I opened port 80 and 443 to establish a connection, the DDoS attack attempt to overwhelm a web server, and the indicator shows that the server was struggling under high potentially malicious traffic.

**Threshold:** The SIL is 20% or greater increase over a normal load time can set as a threshold to trigger alerts to further investigation, if the Http load time spikes it would suggest the actual user experiencing slow access

**IOCs :** Malicious redirect happens when a treat actor alters a legitimate web content to redirect user to phishing sites , malware-laden pages or unauthorized destination. Credential information could be easily accessed.

* **My SQL Database Query Sensor**

**Connection**: This focuses on the nature of the SQL queries being executed, however when adding a sensor, it shows the baseline is low and can lead too several SQL injection attempt, when monitoring the query frequency, it helps detect the surge in database access which could point to malicious activities

**Threshold:** The value was set to 900 and a minimum 100, which triggers an alert, which set for administrators to investigate. This is especially useful for detecting anomalies, as abnormally high query rates may indicate an automated attack or database misconfiguration, whereas unusually low activity may indicate a system malfunction or disruption.

**IOCs:** Attackers may search publicly available technical databases for victim information that can be used during targeting. Online databases and repositories may contain information about victims, such as domain/certificate registrations and public collections of network data/artifacts gathered from traffic and/or scans. This can affect the confidentiality and integrity of the organization.

* **SSH Sensor**

Connection: The SSH track was successfully created by going through the setting and adjusting the metrics, so far, the SIL gives high priority this shows that the generate alerts. The SSH connection failed due to (-1) time out connecting. The SSH target device was not compatible, installed secure SSH, awaiting connection. Several login attempts can indicate brute force attack where an attacker is trying to guess the password.

**Threshold:** High Condition Threshold: Set to alert after 5 failed login attempts within 1 minute. Detected unexpected inactivity or no login attempts on critical servers, which could indicate a security control failure. **Priority and SIL**: Because of SSH's role in system access, this sensor is generally given a high priority and SIL, especially on sensitive systems, where it directly affects system confidentiality and integrity.

**IOCs:** Disconnection can indicate system tampering, where an attacker disconnects to avoid detection, which is an unexpected logout pattern**.**

* **Antivirus Status Pattern**

**Connection**: Monitors endpoint antivirus activity and provides information about Indicators of Compromise (IoCs) associated with malware and other threats. This sensor aids in the detection of malicious behavior, system infections, and potential configuration issues by allowing you to set thresholds.

**Threshold**: Alerts, multiple threats are detected within a short period i.e. more than 2 viruses it could result to 5 minutes, this indicates a wider infection or potential outbreak

**IOCs**: Malware identifies the risk in potential breach in confidentiality, integrity, or availability of a system, was a month-long ransomware intrusion that successfully deployed Avoslocker onto a compromised network. The unidentified actors gained initial access to the victim network through an exposed server and used a variety of open-source tools prior to execution

* **File Sensor:**

**Connection:** The sensor is particularly valuable for identifying unauthorized modifications, deletions, or access attempts that may indicate malicious activity such as ransomware, insider threats, or data tampering. For example, system files may indicate a backdoor installation.

**Threshold:** This is a high condition number of modification, whereby access to sensitive files or directories outside of regular business hours or from unapproved locations can trigger alerts

**IOCs:** Unplanned changes to file content, permissions, or ownership in critical system or application files.

* **Windows Event log**

**Connection:** This sensor helps identify suspicious activities, audit user behavior, and detect potential security incidents in Windows environments**,** logs that can affect the confidentiality and integrity of the organization, which gives unauthorized changes

**Threshold:** Privilege change event, especially for sensitive groups e.g. Administration or Domain Admin, this is a high condition that gives an immediate alert

**IOCs**: Unusual login Times and location- logins from unexpected geographical locations, devices or times outside of business hours can affect the integrity of the business

* **Bandwidth Usage Sensor**

**Connection:** During traffic monitoring, tracks incoming and outgoing data network , providing insight into network loads and application usage

**Threshold**: High condition, a sudden spike in outbound traffic, which in the baseline could reach 30% in risk, designed to detect data exfiltration and large file transfers. This threshold may trigger an alert to investigate potential data breaches or unauthorized uploads.

**IOCs:** A large volume of data is sent to unfamiliar external IP addresses or domains, sustaining high data transfers over time; often indicates data exfiltration, in which sensitive data is transferred outside the organization, or malware communications with external servers.

**4.0 Recommendation Section**

**4.1 Security Impact Level(SIL)**

In the Big Dog environment, assigning Security Impact Levels (SIL) to monitoring activities enables alerts to be prioritized based on their potential impact on critical assets, services, and business functions. Big Dog's operational structure, data sensitivity, and specific threats can all be used to assign an appropriate SIL to each sensor and its associated IoCs. Here's how SIL could be used based on Big Dog's requirements and risk tolerance.

**4.2 Application of SIL in Big Dog’s Monitoring Dashboard**

This project approach is consistent with best practices from frameworks such as NIST RMF and MITRE ATT&CK, focusing resources on high-impact incidents while remaining vigilant for moderate and low-risk activities in the Big Dog environment.

**5.0 Solution**

Security best practices are the foundation for developing a strong cybersecurity posture within an organization. These practices are intended to protect data, systems, and networks from a variety of threats, and when implemented correctly, they help to reduce risk and improve resilience. Here's an overview of key security best practices, with a focus on principles relevant to the Big Dog environment:

1. Implement the principle of least privilege (PoLP). Limit user and system access rights to what is required to do their jobs. Application for the Big Dog: Ensure that administrative access is restricted to essential personnel, and audit permissions on a regular basis to ensure that users and applications have only the minimum amount of access required.

Benefit: Lowers the attack surface and limits the potential damage from compromised accounts

2. Multi-factor authentication (MFA) involves adding an extra layer of verification to user authentication processes, such as using a token or mobile app. Application for the Big Dog: Implement multi-factor authentication for remote access, sensitive applications, and privileged accounts, such as SSH and remote management tools. Benefit: Prevents unauthorized access, particularly in the case of compromised passwords.

**6.0 Reference and Citation:**

* *Search Open Technical Databases: Scan Databases, Sub-Technique T1596.005 - Enterprise | MITRE ATT&CK®,(n.d.)*

<https://attack.mitre.org/techniques/T1596/005/>

* *Brute Force I/O, technique T0806 - ICS | MITRE ATT&CK®. (n.d.)*

[*https://attack.mitre.org/techniques/T0806/*](https://attack.mitre.org/techniques/T0806/)

* *C0018,CampaignC0018|MITREATT&CK®(n.d.)* <https://attack.mitre.org/campaigns/C0018/>
* Obtain capabilities: Malware, Sub-technique T1588.001 - Enterprise | MITRE ATT&CK®. (n.d.)<https://attack.mitre.org/techniques/T1588/001/>
* *Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce. (n.d.). Authorize Step - NIST Risk Management Framework | CSRC | CSRC*

<https://csrc.nist.gov/Projects/risk-management/about-rmf/authorize-step>

* *Valid Accounts, technique T1078 - Enterprise | MITRE ATT&CK®. (n.d.)* https://attack.mitre.org/techniques/T1078/