LIGHTHOUSE LAB

CYBERSECURITY

REPORT ON RISK & VULNERABILITIES

CAT SCAN II BIG DOG

DANIEL D. OLUWAYALE

Table of Contents

Executive Summary

Keeping data from getting out into the wild or being damaged by cyber attackers is what keeps CISOs, the executive team and boards of directors up at night. To protect organizations, cybersecurity needs to be automated and real-time, it needs to learn contextually like we do, and it needs to monitor for threats at every corner of the network in a way that organizations can afford without sacrificing coverage. (Vectra AI, 2023)

This project is simply about recommending appropriate system defense monitoring sensors to Big Dog Network systems based on the type of potential attack or threat, it severity and impact on the reputation and operation of the organization. The level of threshold that is necessary to trigger alert for critical response is also discussed.

Sensor	**Description**	**System**	**IoCs Associated**	**Rationale**	**Priority**	**Thresholds**
HTTP Load Time	Monitor time taken for server to load web pages	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)	High condition is monitored for as it's a good thing if it's takes lesser time to load
HTTP Load Time	Monitor time taken for server to load web pages	Linux	Used to detect unusually high response time due to large quantity of ARP	Higher than normal load time would nine out of ten times be because of an attacker	High (SIL of high)	High condition is monitored for as it's a good thing if it's takes lesser time to load

			request in a short time.			
MySQL Database Query Sensor	Monitors query response time of the database	Linux	Used to detect database overload due to malicious SQL injection and DoS attack	A security breach or compromise like the IoCs mentioned can lead to high execution time or unavailability of the database	High (SIL of High)	High condition as it is not of concern if the database responds in lesser time than normal
SSH Sensor	Monitor number of failed login attempts for remote access	Linux	Used to monitor multiple failed logins attempt from same user	This is sensor is critical in the sense that it notifies of any attempt for initial access into the system	High (SIL of high)	Monitor for high condition within limited time
Antivirus Status Sensor	Monitors the health of systems defender and fast antivirus scan systems	All	This is used to measure how strong an antivirus defends the system against any obfuscating virus and malwares	This sensor is used to ensure the antivirus is healthy and strong enough to defend against any virus that easily spreads through the network	High (SIL of high)	Monitor for high condition as a lesser scanning time indicates a healthy antivirus
File Sensor	Monitors numbers of file modified,	Linux	Used to detect modifications to files and	Presence of unusual or strange file can indicate	High (SIL of high)	Monitor for high condition

	created, accessed or created within a given time.		exfiltration which could be because of ransomware attack	the presence of ransomware		
Windows Event Log Sensor	Monitors logs of specific events as multiple failed login attempt and system errors.	Windows11	Used to detect predefined patterns and suspicious activities logged for windows work stations	Logs of activities reveal specific patterns	Medium (SIL of medium)	Monitor for high condition as lower-than-normal condition means all is good.
Windows Event Log Sensor	Monitors log of creation of new accounts	Windows11	Used to detect logged suspicious activity like new account creation	Sensor would help to detect account creation activity to access Big Dog's PRTG	Low (SIL of High	Monitor of High condition
Bandwidth Usage Sensor	Monitors amount of data transmitted over a network	All	Used to detect abnormal or excessive bandwidth usage which could be as a result of attack like DDoS	A congested network or a lower-than-normal bandwidth usage is as a result of attack	High (SIL of medium	Monitor for high and low condition

Discussion Section

1. SQL Database Query Sensor

AdRem Software (n.d.) explains that SQL sensors allow for measuring connectivity, query execution time, and result data processing as metrics or statuses in their NetCrunch documentation.

- IoC for this sensor determining if database is suffering from higher-than-normal load which could be due to SQL injection. HackerOne (n.d.) says SQL Injection is a type of cyber-attack where malicious code is inserted into an SQL statement, thereby manipulating the execution of the statement to gain unauthorized access to sensitive data or perform malicious actions.
- The priority is high as a successful SQL injection attack will be devastating to Big Dog as their data in the SQL Database can be compromised, controlled and exfiltrated
  SC = (Confidentiality, High), (Integrity, High), (Availability, High)
  SIL is of High
- Threshold is of high condition as a low condition of query response time is an indication of no compromise

2. HTTP Load Time
   - IoC monitored by this sensor is malicious content injection or DDoS. (MITRE, n.d.) Adversaries may perform Network Denial of Service (DoS) attacks to degrade or block the availability of targeted resources to users. Network DoS can be performed by exhausting the network bandwidth services rely on.
   - The priority is High as this greatly impacts the server the organization uses to create their intellectual property if an attack is successful.
     SC = (Confidentiality, High), (Integrity, High), (Availability, High)
     SIL is High
   - The threshold is high condition as low load time is good and an indication of no compromise. (Lighthouse Labs, n.d.) We are not concerned if our webserver responds faster than usual. As a matter of fact, that would likely be seen as a good thing. So, we will set upper limits (for warnings and errors) to let us know if the response takes too long, but we won't bother to set lower limits in this case because we aren't interested in knowing if the server is responding too fast.

3. Bandwidth Usage Sensor
    - IoC monitored by this sensor is DDoS attack which can slow down Big Dog's network or stop it from functioning which would negatively impact the reputation of the organization.
    - The priority is High as Big Dog can not afford to have their systems malfunctioning or having a downtime which can be expensive due to loss of paying customers.
      SC = (Confidentiality, Medium), (Integrity, Medium,), (Availability, High)
      SIL is Medium
    - Threshold is High condition as the sensor monitors for excessive usage of the bandwidth and an SNMP can used to detect the breakdown of any system in the network
4. File Sensor
    - IoC: the IoCs monitored here are file integrity and exfiltration. (MITRE, n.d.) Modifications may include changing specific access rights, which may require taking ownership of a file or directory and/or elevated permissions depending on the file or directory's existing permissions. This may enable malicious activity such as modifying, replacing, or deleting specific files or directories.
    - The priority is High as this is concerning Linux which the organization uses to develop their intellectual properties which is categorized as very important
      SC = (Confidentiality, High), (Integrity, High), (Availability, High)
      SIL is High
    - The threshold is high condition as a low condition is an indication of no compromise

5. Antivirus Status Sensor
    - IoC: The IoC of this sensor is longer-than-usual scan time which could mean that the antivirus is not strong or healthy enough to do its job. Anti-virus can be used to automatically detect and quarantine suspicious files, including those with high entropy measurements or with otherwise potentially malicious signs of obfuscation. (MITRE, n.d.)
    - The priority is High as this includes all the assets of the organization regardless of their importance
      SC = (Confidentiality, High), (Integrity, High), (Availability, High)
      SIL is High

- The threshold is High Condition as a low scan time indicates a healthy antivirus

Recommendations

1. Set account lockout policies after a certain number of failed logins attempts to prevent passwords from being guessed. Too strict a policy may create denial-of-service conditions and render environments unusable, with all accounts used in the brute force being locked out. Use conditional access policies to block logins from non-compliant devices or from outside defined organization IP ranges. (MITRE, n.d.)
2. The use of VLANs in the workstation creates an extra layer of network security by segmenting and separating network traffic. VLANs keep unauthorized users out of restricted regions and provide a strong security foundation for safeguarding valuable data, like zero trust concepts.
3. Software updates should be done regularly to prevent threats, and Backup should be done for the databases in case the organization's data is compromised or stolen.
4. The network monitoring tool (PRTG) should be high on the priority list of the organization as this is the tool that is being used to manage the security of all the organization's network.
5. SNMP should also be adopted to track and monitor the functionality of the systems within the organization's network. Its usefulness in network administration comes from the fact that it allows information about network-connected devices to be collected in a standardized way across a large variety of hardware and software types. (Paessler, n.d.)

Reference

AdRem Software. (n.d.). *SQL query sensors*. NetCrunch. https://www.adremsoft.com/adoc/view/netcrunch/12168614717731/sql-query-sensors

HackerOne. (n.d.). *SQL injection attack: How it works and 4 preventive measures*. HackerOne. https://www.hackerone.com/knowledge-center/sql-injection-attack-how-it-works-and-4-preventive-measures

MITRE. (n.d.). *T1498: Data Staged*. MITRE ATT&CK. https://attack.mitre.org/techniques/T1498/

Lighthouse Labs. (n.d.). *W02D4 - Activity 2857: Cybersecurity*. Lighthouse Labs. https://web.compass.lighthouselabs.ca/p/cyber/days/w02d4/activities/2857

Vectra AI. (2023, November 16). *Cybersecurity sensors: Threat detection throughout a distributed network*. Vectra AI. https://www.vectra.ai/blog/cybersecurity-sensors-threat-detection-throughout-a-distributed-network

Paessler. (n.d.). *What is SNMP? Simple Network Management Protocol explained*. Paessler AG. https://www.paessler.com/it-explained/snmp