SCOTT MACLEAN

OCTOBER 2024

CAT SCAN II BIG DOG

TABLE OF CONTENTS

EXECUTIVE SUMMARY

We have conducted a thorough assessment of your companies network infrastructure and needs. This report gives a comprehensive monitoring solution designed to enhance the security posture of your organization.

By implementing the recommended PRTG sensors and alert thresholds, you can effectively detect and respond to potential threats.

This report will detail the specific sensors tailored to each system, the rationale behind their selection, their priority level, related Indicators of Compromise (IoCs), and recommended alert thresholds. The goal is to provide a secure monitoring solution that prioritizes the most important assets and minimizes the risk of security breaches.

Sensor	Description	System	IoCs Associated	Rationale	Priority	Thresholds/Assumptions
HTTP Load Time Sensor	Monitors the time it takes for the page to load.	Windows	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.	High	Changes of 20% over the average load. SIL base on the fact that BIG DOG does NOT have a large Web Presence, the windows 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	Monitors database query performance and errors.	Windows Server (SQL)	Slow query performance, excessive resource usage, unauthorized access attempts	Detects anomalies that may indicate malicious activity or performance issues affecting the database.	High	Increased query execution time by 50% over baseline, excessive resource consumption, 10% more failed login attempts within an amount of time. We have assigned this high priority as SQL database could hold private information of clients
SSH Sensor	Monitors SSH login attempts and authentication failures.	All	Brute-force attacks, unauthorized access attempts	Detects suspicious login activity that may indicate a security breach.	High	10% more failed login attempts within a short time frame, unusual login times or locations. We have assigned this a high priority as any breach could threaten propriety data.
Antivirus Status Sensor	Monitors the status of antivirus software and detected threats.	All	Malware infections, virus outbreaks	Ensures that antivirus software is up-to-date and actively scanning systems.	Medium	Antivirus definitions outdated, malware detected, any virus detection. We have assigned this a medium priority being that the antivirus should be on auto update but detecting threats for machines is important.
File Sensor	Monitors file integrity and unauthorized modifications.	All	File tampering, data exfiltration, ransomware	Detects changes to critical files that may indicate malicious activity.	High	Unauthorized file modifications, file deletion, file creation by unauthorized users. We have assigned this a high priority as the integrity of files is important for your company
Windows Event Log Sensor	Monitors Windows event logs for security-related events.	Windows Server	Security policy changes, failed login attempts, privilege escalation attempts	Detects security incidents and system anomalies.	Medium	Security policy changes, 10% more failed login attempts, privilege escalation attempts. We have assigned this a medium priority as we do want to be notified if any authorization changes have been made in real time which could threaten the accessibility of your data.
Bandwidth Usage Sensor	Monitors network bandwidth usage.	All	DDoS attacks, data exfiltration, unauthorized network traffic	Detects unusual network activity that may indicate a security breach.	High	25% increase in bandwidth usage, unusual traffic patterns, excessive data transfer. We have assessed this as high priority as high bandwidth usage could indicate a breach of confidential and proprietary information being transferred out.

DISCUSSION

for the connections between sensors

Using the sensors provided by PRTG, we can create a strong network of security for your infrastructure. By combining the sensors together and setting the right thresholds, we can detect and respond to a wide range of attacks.

The file sensor and antirivus status sensor used together can detect file changes or any data tampering and possibly where those changes were done from when looking at the antivirus logs.

The HTTP Load time sensor and bandwidth usage sensor could indicate a potential DDoS attack if you're seeing a spike in both metrics. This is because attackers flood the server with traffic to slow things down. If there's a lot of bandwidth usage occuring, this could indicate a large file transfer. [1]

The SSH Sensor and windows event log sensor could work together to detect unathorized logins usually associated with brute force attacks.

The file sensor and antirivus status sensor used together can detect file changes from malicious sources or any sort of tampering done. This could indicate a malware infection or some sort of breach.

Using all of the sensors in conjuction can give you a comprehensive picture at the health of your network while preventing and mitigating an impact from an attack. But we can also provide additional security measures for your company.

RECOMMENDATIONS

for added sensors and rationale

Network Segmentation

By using VLANs to isolate critical systems, such as the Windows Server, Linux server, Windows Workstations and Kali Server, we can reduce possible attack damage. [2]

Web Firewall

A web application firewall can help protect web applications from attacks such as SQL injection. [3]

Syslog Sensor

The Event Log Sensor, that's already in place, can monitor your windows server. Having a Syslog Sensor would monitor your Linux and Kali systems for failed login attempts, unathorized access and security policy changes.

Employee Training

By training employees on best practices when using email or personal devices with company information, this will reduce the amount of human error. This could include things like clicking a suspicious email or downloading malware. [3]

Incident Response Plan

Having a proper response plan in place can help your company more properly deal with any attacks that occur and also mitigate the amount of data stolen or tampered with. [3]

By implementing these recommendations and continuously monitoring the network, your company can significantly enhance its security posture and protect its valuable assets.

CITATIONS AND REFERENCES

1. Network denial of service. Network Denial of Service, Technique T1498 - Enterprise | MITRE ATT&CK®. (n.d.). https://attack.mitre.org/techniques/T1498/
2. Compass. Network Segmentation (Cyber Security Immersive). (n.d.). https://web.compass.lighthouselabs.ca/p/14/aca9ea4f-0bb0-4e4c-9722-b0a000f8bf31
3. Government of Canada / Gouvernement du Canada. (2020, February 18). Baseline Cyber Security Controls for small and medium organizations. Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations