Cat Scan II Big Dog

By Heather Fincati

Table of Contents

Executive Summary

After conducting a comprehensive evaluation of the information assets within the Big Dog Organization, we are delighted to introduce an improved monitoring strategy designed to enhance the security and operational efficiency of their network and devices. Our methodology revolves around the strategic placement of sensors across all devices, aiming to deliver a thorough and real-time overview of network traffic. In accordance with the established priorities defined by Big Dog, we've constructed a vulnerability matrix that intricately links system vulnerabilities to key priorities and the associated risks.

By harnessing this insightful information, we've formulated a targeted plan focused on the proactive identification and mitigation of vulnerabilities. This plan is meticulously designed to fortify Big Dog Organization against potential threats, ensuring a resilient and secure trajectory for the organization's future. Our commitment lies in not only addressing existing vulnerabilities but also establishing a robust framework that continuously monitors and adapts to emerging cybersecurity challenges. This tailored approach reflects our dedication to providing Big Dog with a comprehensive and sustainable security solution aligned with their organizational priorities and risk mitigation objectives.

Information Assets

Information asset categorization and CIA Triad score: [9]

INFORMATION ASSET	CATEGORY	CONFIDENTIALITY	INTEGRITY	AVAILABILITY	Combined Score
Kali Test Systems	S	Low	Low	High	5
Kali IT Systems	S,SM	Low	Medium	Medium	5
Sales	A	Low	Medium	High	6
Marketing	A	Low	Low	Low	3
Management Func	P,A,F	Medium	High	High	7
SQL Database	S,P	High	High	High	9
IIS web server	S	Low	Low	Low	3
PRTG Monitoring	SM	Medium	Medium	Medium	6
Linux	IP,S	High	High	Medium	8

Category Descriptions

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*	*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		Linux				
MySQL Database Query Sensor	Monitors performance and availability of the MySQL service	Linux	Unusual response times may indicate SQL Injection attacks or unauthorized access or attempted exfiltration	Increased response time could indicate a number of compromises including SQL Injection, DoS or even Data Exfiltration	9	Changes of more than 10% above baseline would be cause for concern
MSSQL Database Query Sensor	Monitors performance and availability of the MSSQL service	Winserver			8	
SSH Load Average Sensor	Checks responsiveness of SSH	Linux	Multiple Failed logins indicate brute force attack. Unusual access times may indicate unauthorized access	High Load Average spikes may indicate attempted Brute-Force. Extended high load may indicate DoS	8	The load average should remain at no more than 80% of maximum, Meaning that if there are 4 cores, the maximum should be no more than 3.2.
Antivirus Status Sensor	Monitors status and performance of the EPS	All	Changed in EPS may indicated attempt to bypass Antivirus, indicating a compromised system	Threat Actors may attempt Defence Evasion[2] by disabling Antivirus/ Endpoint Security	9	If the AV/EPS is disabled or the definitions are out of date, an alarm should be raised and the situation rectified

Sensor	Description	System	IoCs Associated	Rationale	Priority	Thresholds /Assumptions
File Sensor	Checks files exist, size, age, content, permissions, integrity and shares.[10]	Winserver /Linux	Changes in critical system files or presence of known malware hashes would indicate Compromise	The File Sensor may detect changes in files which may allow privilege escalation or remote code execution. It could also detect known malware based on file hashes.	8	If system critical files are changed If the any permissions (r/w/x) are added or changed to a file If known malware or malware hashes are detected An alert needs to be raised
Windows Event Log Sensor	Monitors critical and security-related events	Winserver	Failed logins could indicate Brute Force or changes to Event log could indicate compromise	If a Threat Actor is attempting to brute force into a system, there are going to be multiple failed login events recorded in the Event log. Additionally, if a threat actor has achieved login, they may make changes to maintain persistence[2]	9	Any new Warning/Error/Critical/Audit Failure should create an alert.
Windows Event Log Sensor	Monitors critical and security-related events	Windows1 and 2			8	
Bandwidth Usage Sensor	Monitors bandwidth usage for unusually high or low usage	All	Unusual bandwidth usage, both high and low could indicate compromise	High bandwidth could indicate Exfiltration. Low bandwidth could indicate offline systems	9	20% above the baseline or below 50% of the baseline should create an alert

Vulnerabilities

Windows SQL[7]

CVE-2024-0056	Microsoft.Data.SqlClient and System.Data.SqlClient SQL Data Provider Security Feature Bypass Vulnerability[11]	8.7 HIGH
CVE-2023-36006 CVE-2023-36402	Both Indicate: Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8 HIGH

Windows IIS Server[1,7]

CVE-2023-36434	Windows IIS Server Elevation of Privilege Vulnerability	9.8 CRITICAL
CVE-2023-3440	Incorrect Default Permissions vulnerability in Hitachi JP1/Performance Management on Windows allows File Manipulation.	8.4 HIGH[+]
CVE-2023-6352	The default configuration of Aquaforest TIFF Server allows access to arbitrary file paths, subject to any restrictions imposed by Internet Information Services (IIS) or Microsoft Windows.	5.3 MEDIUM

PRTG [3,7]

CVE-2024-25209	Barangay Population Monitoring System 1.0 was discovered to contain a SQL injection vulnerability via the resident parameter at /endpoint/delete-resident.php.	9.1 CRITICAL[8,9]
CVE-2024-25208 CVE-2024-25207	Both Indicate: Barangay Population Monitoring System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability in the Add Resident function	5.4 MEDIUM

Linux [4,7]

CVE-2024-25744	In the Linux kernel before 6.6.7, an untrusted VMM can trigger int80 syscall handling at any given point. This is related to arch/x86/coco/tdx/tdx.c and arch/x86/mm/mem_encrypt_amd.c.	5.9 MEDIUM[8,9]
CVE-2024-25741	printer_write in drivers/usb/gadget/function/f_printer.c in the Linux kernel through 6.7.4 does not properly call usb_ep_queue, which might allow attackers to cause a denial of service or have unspecified other impact.	5.1 MEDIUM[8,9]
CVE-2024-25740	A memory leak flaw was found in the UBI driver in drivers/mtd/ubi/attach.c in the Linux kernel through 6.7.4 for UBI_IOCATT, because kobj->name is not released.	4.0 MEDIUM[8,9]

Windows 11 [5,7]

CVE-2023-4759	Arbitrary File Overwrite in Eclipse JGit <= 6.6.0 In Eclipse JGit, all versions <= 6.6.0.202305301015-r, a symbolic link present in a specially crafted git repository can be used to write a file to locations outside the working tree when this repository is cloned with JGit to a case-insensitive filesystem, or when a checkout from a clone of such a repository is performed on a case-insensitive filesystem.	8.8 HIGH
CVE-2023-46756	Permission control vulnerability in the window management module. Successful exploitation of this vulnerability may cause malicious pop-up windows.	5.3 MEDIUM
CVE-2023-6352	The default configuration of Aquaforest TIFF Server allows access to arbitrary file paths, subject to any restrictions imposed by Internet Information Services (IIS) or Microsoft Windows. Depending on how a web application uses and configures TIFF Server, a remote attacker may be able to enumerate files or directories, traverse directories, bypass authentication, or access restricted files	5.3 MEDIUM

Discussion

SQL Database

SQL Injection Attacks*:* may occur when user inputs are not adequately sanitized, creating vulnerabilities that enable attackers to execute malicious SQL queries and potentially compromise the integrity of the database. For this we have utilized the HTTP Load Sensor as changes in the overall load time can be flagged.

Ioc- Delays in application responses, indicating a potential time-based blind SQL injection attack.

Weak Authentication: Insufficient authentication measures can result in unauthorized access. Attackers may exploit weak or default credentials on SQL Server instances, posing a security risk.

IoC-An increase in the number of failed login attempts, especially if they are sequential, may indicate an attacker attempting to guess weak passwords. The Windows Event Log Sensor is perfect for this as it can warn us for audit failures which failed login attempts falls under.

Misconfigured Permissions: Insufficient database user permissions pose a risk of exposing sensitive data or enabling unauthorized modifications. Conducting regular audits of user privileges is critical to identifying and mitigating this potential risk.

IoC-Creation of new database users without proper approval or justification, signaling a potential security risk. This too can be monitored by using the Windows Event Log Sensor.

IIS Webserver

Cross-Site Scripting (XSS): Vulnerabilities in web applications hosted on IIS may allow attackers to inject malicious scripts into web pages viewed by other users, leading to potential data theft or manipulation.

IoC - Keep a vigilant watch for irregularities in the web application's behavior, including unanticipated script executions, modifications to content, or uncommon patterns in data transfers. The HTTP Load Sensor is used to monitor this activity.

Denial of Service (DoS) Attacks: IIS servers are susceptible to DoS attacks, where attackers overwhelm the server with traffic, causing it to become unresponsive and potentially disrupting services.

IoC - unusual network traffic Anomalies in network traffic, such as a sudden increase in incoming requests. The Bandwidth Usage Sensor is best because by monitoring the bandwidth we can quickly see a potential DoS attack because high bandwidth could indicate Exfiltration and low bandwidth could indicate offline systems.

File Inclusion Vulnerabilities: Improper handling of user inputs may lead to file inclusion vulnerabilities, allowing attackers to execute arbitrary code on the server.

IoC - Commands being executed on the server as a result of file inclusion, indicating a potential compromise. To monitor for this we utilize the File Share Sensor.

Management Workstations

Windows Event Log Sensor is being used to monitor for all of these IoCs because it is the most efficient use of time and resources as all of these risks, vulnerabilities can be monitored in one sensor.

Unsecured Remote Access: If remote access features are enabled on management workstations without adequate security measures, it poses a risk of unauthorized access to these workstations.

IoC - Successive and rapid login trials, suggesting a potential brute-force attack targeting remote access services.

Insufficient Employee Training: Insufficient security awareness within the management team may lead to risky behaviors, including susceptibility to social engineering attacks.

IoC - A rise in unauthorized access or login attempts may occur due to compromised credentials, stemming from a lack of awareness about secure login practices.

Shadow IT: Marketing teams may utilize unauthorized applications or services without oversight from the IT department. This could result in insecure data storage or communication channels, presenting a potential security risk.

IoC - Atypical access patterns, particularly occurring outside regular business hours or from unexpected locations, may suggest unauthorized utilization of applications.

Recommendations

Implementation of a Zero Trust Model is highly recommended as it follows the NIST Risk Management Framework. Due to the increase in AI capabilities, bad actors have more ways of attacking networks. An example of this is a Deepfake[13] attack where cyber criminals use AI to look and sound like a person of authority within an organization to obtain access to sensitive data, systems and potentially gain control of a company or organization. In a Zero Trust Model trust is never assumed and supports a continuous verification and strict access stance. There are three specific aspects of the Zero Trust Model that we are recommending:

1. Multi-Factor Authentication (MFA): Multi-Factor Authentication adds an extra layer of security when accessing sensitive data and systems. It is an excellent way to prevent unauthorized access even if passwords become compromised.
2. Micro-Segmentation: Micro-Segmentation divides the network into smaller segments through the use of VLANs or Virtual Local Area Networks. We recommend segmenting Big Dog's Security Management, Sales and marketing so they are no longer on the "same" network.
3. Encryption: End to end encryption is performed in the Transport Layer Security[12] or TLS/4 as a cryptographic protocol from the OSI Model Framework that when implemented, it encrypts data during transmission between a user's web browser and a website, ensuring that the information remains confidential. By utilizing this protocol even if someone were to get a hold of the data transmission it would be illegible. A really great way to check encryption took place is in Wireshark. Wireshark[14] is an open-sourced software tool designed to scan all incoming and outgoing traffic on your network.

Citations

MITRE

1:https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=iis

Mitre CVE Search provides the vulnerabilities on this page with specific regards to IIS.
The ones listed were the most recent at the time of compiling the report.

2:https://attack.mitre.org/

The Mitre ATT&CK matrix was used to determine the correct Tactics.
The 2 identified were Defence Evasion (TA0005) and maintaining Persistence (TA0003)

3:https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=PRTG+Monitoring

Mitre CVE Search provided the vulnerabilities on this page with regards to PRTG Monitoring.
The ones listed were the most recent at the time of compiling the report.

4.https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Linux

Mitre CVE Search provided the vulnerabilities on this page with regards to PRTG Monitoring.
The ones listed were the most recent at the time of compiling the report.

5:https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Windows+11

Mitre CVE Search provided the vulnerabilities on this page with regards to Windows 11.
The ones listed were the most recent at the time of compiling the report.

Hitachi

6:https://www.hitachi.com/products/it/software/security/info/vuls/hitachi-sec-2023-145/index.html

There were 2 available CVSS scores.(/detail/CVE-2023-3440)
The one used was higher and a more reliable reference as it was published by Hitachi (which is a Certified Numbering Authority - allowing them to issue CVEs.)

NVD

7:https://nvd.nist.gov/vuln/search

The NVD is the National Institute of Science and Technology National Vulnerability Database, used as standard in the industry.
Was used for verification on all vulnerabilities to cross reference the MITRE ATT&CK

8:https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

The Vulnerability Calculator is a tool that can be used to calculate the CVSS score for vulnerabilities.
The Calculator was used to calculate the CVSS scores of the vulnerabilities mentioned in the table above that were not yet rated by NIST.

ChatGPT

9: https://chat.openai.com/

This tool was used to enumerate the vulnerabilities in terms of the CVSS scoring system. It was not used to generate any content, merely interpret the vectors of the vulnerabilities as those vulnerabilities were not yet rated by NIST.

Paessler PRTG

10:https://www.paessler.com/manuals/prtg/list_of_available_sensor_types

Paessler PRTG is the Network Monitoring software used to monitor the network infrastructure for the Big Dog Company.

Microsoft

11:https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-0056

OSI Model Transport Layer

12:https://www.plixer.com/blog/network-layers-explained/#:~:text=Transport%20and%20Network,for%20data%20delivery.

Showing how the OSI Model at the 4th or Transport layer works in my recommendations

---

Deepfake News Article

13:https://www.aicpa-cima.com/news/article/deepfakes-emerge-as-real-cybersecurity-threat#:~:text=Recent%20stories%20of%20criminals%20using,executives%20into%20disclosing%20confidential%20information

Kepczyk, R. H. (2022, September 22). *Deepfakes emerge as real cybersecurity threat CPA.CITP, PAFM Director of Firm Technology Strategy Sep 27, 2022* AICPA&CIMA.

Wireshark

14:https://www.wireshark.org/

Link to the Wireshark Website for your perusal and information. For general perusal.