Cat Scan II Big Dog

TABLE OF CONTENTS

Introduction:

This report aims to find ways to secure Big Dog Organization. I looked at a lot of things to figure out what could be potential problems. Then, came up with the ideas to strengthen Big Dog's defenses against cyber attacks.

Methodology:

This report involves a systematic approach to gather, verify and secure the devices of the Big Dog Organization. The following steps outline the methodology used for this project.

- I started by carefully examining Big Dog's computers, networks, and other important parts of their setup and prioritized the assets.
- I looked for places where hackers might try to get in and cause problems for the Organization.
- Focused on the most important parts of Big Dog's setup that could be easily attacked or cause the most damage if compromised.
- Created a list of sensors, each designed to spot specific signs that something is wrong in Big Dog's systems.
- Based on the analysis, I provided practical advice and suggestions for steps Big Dog can take to improve their security

Executive Summary:

The security assessment conducted for Big Dog Organization aimed to identify the vulnerabilities and recommend measures to enhance the organization's cybersecurity posture. Key findings from the assessment revealed several critical vulnerabilities across Big Dog's infrastructure, including unauthorized access to databases, SQL injection vulnerabilities, and insecure configurations on key systems. These vulnerabilities pose significant risks to the confidentiality, integrity, and availability of the organization's data and systems. To mitigate these risks, I recommend implementing measures such as regular security patching, multi-factor authentication for sensitive systems, and employee training on cybersecurity best practices.

The top five Security Impact Levels (SILs) prioritize sensors monitoring critical systems, including databases, SSH activity, antivirus status, file changes, and Windows event logs. Thresholds for monitoring include detecting unauthorized access, unusual file modifications, and suspicious activity in event logs, enabling proactive threat detection and response.

Table of sensors:

Sensor	Description	System	Iocs	Rationale	Priority	Thresholds
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 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 7

HTTP Load Time Sensor	Monitors the time it takes for the page to load	Linux	May be used to indicate Malicious Redirects, DDoS Attacks, Content Injection.	Unexpected changes in load time can indicate anomalies or performance-related issues that could be an indicative of a security breach or compromise.	Medium to high, with a Security Impact Level (SIL) of 7.	Changes of 20% over the average load are considered significant and should trigger alerts. Assumptions include stable network conditions, consistent server load, and relatively low web presence, impacting the SIL assignment.
MySQL Database Query Sensor	Monitors queries made to the MySQL database	Linux	May be used to indicate SQL Injection, Unauthorized Access,	Any unusual or unauthorized queries could be an indicative of SQL injection attacks or unauthorized access attempts.	High,SIL 8	Databases contain sensitive information and are prime targets for attackers.
MSSQL Database Query Sensor	Monitors queries made to the MSSQL database	Winserver	May be used to indicate SQL Injection, Unauthorized Access	Any unusual or unauthorized queries could be a indicative of SQL injection attacks or unauthorized access attempts.	High,SIL 8	Databases contain sensitive information and are prime targets for attackers.
SSH Sensor	Monitors SSH activity such as login attempts and commands executed	Winserver/Linux	May be used to indicate Brute Force Attacks, Unauthorized Access,SSH is a common entry point for attackers	Any suspicious login attempts, unusual command executions could be an indicative of unauthorized access or brute force attacks.	High,SIL 8	Unauthorized access via SSH can lead to significant data breaches or system compromise.
Antivirus Status Sensor	Monitors the status of antivirus software.	all	May be used to indicate Malware infections	Any deviations from the expected antivirus status could be an indicative of malware infections	High,SIL 8	Malware infections can lead to data loss, system compromise, and significant disruption.
File Sensor	Monitors changes to files and directories	Winserver/Linux	May be used to indicate Unauthorized File Access, Ransomware	Any unauthorized file access or modifications could be an indicative of ransomware attacks.	High,SIL 8	Unauthorized file access can lead to data breaches, data loss, or system compromise.

Windows Event Log Sensor	Monitors Windows event logs for security-related events	Winserver	May be used to indicate Account Logon Failures, Security Policy Changes	Any suspicious activity or security policy violations on Windows systems could be an indicative of Potential security threats or breaches.	High, SIL 8	Security event logs provide valuable information for detecting and investigating security incidents.
Windows Event Log Sensor	Monitors Windows event logs for security-related events.	Windows1	May be used to indicate Account Logon Failures, Security Policy Changes	Any suspicious activity or security policy violations on Windows systems could be an indicative of Potential security threats or breaches.	High,SIL 8	Security event logs provide valuable information for detecting and investigating security incidents.
Bandwidth Usage Sensor	Monitors network bandwidth usage	All	May be used to indicate DDoS Attacks	Unusual spikes or drops in bandwidth usage can indicate potential DDoS attacks or data exfiltration attempts.	High,SIL 8	Network bandwidth is critical for communication and unusual activity may indicate malicious intent.

Discussion:

Vulnerabilities associated with the assets:

Unauthorized Access to SQL Database (P)- Unauthorized access to the SQL database can lead to the theft or manipulation of critical business data, including customer information. This poses a significant risk to the confidentiality, integrity, and availability of sensitive data, potentially resulting in financial losses, legal repercussions, and damage to the organization's reputation.

SQL Injection Vulnerabilities (P)- SQL injection vulnerabilities in the SQL database can be exploited by attackers to execute malicious SQL queries, potentially leading to data breaches, data manipulation, or unauthorized access to sensitive information. SQL injection attacks are a prevalent and severe threat to database security, requiring immediate attention to mitigate the risk.

Microsoft SQL Server Denial of Service Vulnerability CVE-2023-36728

Vulnerabilities in IIS Webserver (P): vulnerabilities in the IIS webserver can be exploited by attackers to gain unauthorized access to web applications, compromise user data, or disrupt business operations. Given the critical role of web applications in modern business operations, addressing vulnerabilities in the web server is essential to prevent potential security breaches and maintain the integrity of online services.

IIS Webserver buffer overflow CVE-2010-3972
Buffer overflow in Microsoft Internet Information Services (IIS) CVE-2010-2730

Unauthorized Access to Management Workstations (P): Management workstations often contain sensitive business information, including financial data, strategic plans, and employee records. Unauthorized access to these workstations can result in data breaches, compromise of confidential information, and unauthorized changes to critical systems. Protecting management workstations from unauthorized access is crucial to safeguarding sensitive business assets and maintaining operational integrity.

Insecure inherited permissions CVE-2023-38541
Improper access control in some Intel HotKey Services CVE-2023-32544

Unauthorized Access to Sales and Marketing Workstations (P): Sales and marketing workstations may contain sensitive client information, marketing strategies, and market research data. Unauthorized access to these workstations can lead to data breaches, theft of confidential information, and compromise of customer trust. While the impact of unauthorized access to sales and marketing workstations may be lower than management workstations, it still poses significant risks to the organization's reputation and compliance with data protection regulations.

A flaw in Thales SafeNet Authentication CVE-2023-7016

Exploitation of Vulnerabilities in PRTG Network Monitor (SM): Exploitation of vulnerabilities in the PRTG Network Monitor can result in unauthorized access to network infrastructure, interception of sensitive network traffic, or disruption of network monitoring operations. While the impact may vary depending on the specific vulnerabilities exploited, addressing these vulnerabilities is essential to maintaining the security and integrity of the organization's network infrastructure.

PRTG Network Monitor Cross-Site Scripting Authentication Bypass Vulnerability CVE-2023-51630

Exposure of Test Systems to Unauthorized Access (S): Test systems are typically used for testing software applications, network configurations, and security measures. While unauthorized access to test systems may result in the exposure of sensitive testing data or configurations, the impact is generally lower compared to production systems or critical infrastructure. However, it is still important to protect test systems from unauthorized access to prevent potential security breaches or misuse of testing resources.

The Contact Form builder with drag & drop for WordPress CVE-2024-1218

Exposure of IT Systems to Vulnerabilities (S): IT systems, including infrastructure components and support systems, may be exposed to vulnerabilities due to misconfigurations, outdated software, or lack of security controls. While vulnerabilities in IT systems can pose risks to the organization's overall security posture, the impact is typically lower compared to assets directly involved in data processing or customer interactions. Nevertheless, addressing vulnerabilities in IT systems is important to maintain the overall integrity and availability of organizational resources.

The Contact Form builder with drag & drop for WordPress CVE-2024-1218

IoCs and Vulnerabilities/Risks/Threats:

Malicious Redirects: Indicates potential compromise of web servers leading to unauthorized redirection of users to malicious websites.

SQL Injection: Indicates attempts to exploit vulnerabilities in databases by injecting malicious SQL queries.

Brute Force Attacks: Indicates unauthorized attempts to gain access to systems by trying multiple combinations of usernames and passwords.

Malware Infections: Indicates the presence of malicious software on systems, which can lead to data breaches or system compromise.

Unauthorized File Access: Indicates unauthorized access or modifications to critical files, which may lead to data breaches or system compromise.

Sensors and SILs:

HTTP Load Time Sensor: The SIL is determined based on the potential impact of anomalies in load time on the availability of web services. Since unexpected changes in load time could disrupt normal operations and lead to service unavailability, a moderate SIL (e.g., SIL 7) is assigned.

MySQL Database Query Sensor: The SIL is determined based on the potential impact of unauthorized access or SQL injection attacks on the confidentiality and integrity of the database. Since databases contain sensitive information and unauthorized access can lead to data breaches or unauthorized modifications, a higher SIL (e.g., SIL 8) is assigned.

SSH Sensor: The SIL is determined based on the potential impact of unauthorized SSH access on the confidentiality, integrity, and availability of the system. Since unauthorized SSH access can lead to significant data breaches or system compromise, a higher SIL (e.g., SIL 8) is assigned.

Antivirus Status Sensor: The SIL is determined based on the potential impact of malware infections on the confidentiality, integrity, and availability of the system. Since malware infections can lead to data loss, system compromise, and disruption, a higher SIL (e.g., SIL 8) is assigned.

File Sensor: The SIL is determined based on the potential impact of unauthorized file access or ransomware attacks on the confidentiality, integrity, and availability of critical files and data. Since unauthorized file access can lead to data breaches or system compromise, a higher SIL (e.g., SIL 8) is assigned.

Windows Event Log Sensor: The SIL is determined based on the potential impact of security-related events detected in Windows event logs. Since security event logs provide valuable information for detecting and investigating security incidents, a higher SIL (e.g., SIL 8) is assigned.

Bandwidth Usage Sensor: The SIL is determined based on the potential impact of unusual bandwidth usage patterns on the availability of network resources and communication. Since unusual bandwidth usage may indicate potential DDoS attacks or data exfiltration attempts, a higher SIL (e.g., SIL 8) is assigned.

Recommendation:

To enhance Big Dog's security posture, we recommend implementing additional measures such as:

- Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) to detect and prevent network-based attacks.
- Security Information and Event Management (SIEM) system for centralized logging, analysis, and correlation of security events.
- Endpoint Detection and Response (EDR) solutions to monitor and respond to threats at the endpoint level.
- Regular security assessments and penetration testing to identify and address vulnerabilities proactively.
- Implementing multi-factor authentication for sensitive systems.
- Employee training on cybersecurity best practices.

Conclusion:

By implementing these recommendations, Big Dog can strengthen their security posture and better protect their systems and data from cyber threats.

References:

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

CVE-2023-36728 : NVD - CVE-2023-36728 (nist.gov)

CVE-2010-3972: NVD - CVE-2010-3972 (nist.gov)

CVE-2010-2730: https://nvd.nist.gov/vuln/detail/CVE-2010-2730

CVE-2023-38541: https://nvd.nist.gov/vuln/detail/CVE-2023-38541

CVE-2023-32544: https://nvd.nist.gov/vuln/detail/CVE-2023-32544

CVE-2023-7016: https://nvd.nist.gov/vuln/detail/CVE-2023-7016

CVE-2023-51630: https://nvd.nist.gov/vuln/detail/CVE-2023-51630

IOCs information: https://sec.cloudapps.cisco.com/security/center/resources/iocs.html

Information on IOCs: https://www.fortinet.com/resources/cyberglossary/indicators-of-compromise#:~:text=1.,or%20another%20breach%20in%20security.

MITRE and ATT&CK: https://attack.mitre.org/

How to determine SIL: https://www.linkedin.com/pulse/how-determine-cybersecurity-impact-level-using-fips-199

SQL Vulnerabilities: https://www.linkedin.com/advice/3/what-most-important-sql-security-vulnerabilities-gxsyf-

SQL security best practices: https://codedamn.com/news/sql/sql-security-best-practices-protecting-database-

Best practices for Network Monitoring: https://www.spiceworks.com/tech/networking/articles/network-monitoring-best-practices/

List of Sensors: https://www.paessler.com/manuals/prtg/wmi_security_center_sensor-

IIS windows server: https://thehackernews.com/2023/09/protecting-your-microsoft-iis-servers.html-

Sensor recommendations in PRTG: https://www.paessler.com/manuals/prtg/recommended_sensors

Video Presentation:

Here is the link for the video Presentation. https://drive.google.com/file/d/1ncJQLAlSX-xMyagGZxM4_71XXCfe-6Fq/view?usp=drive_link