Report on Risks & Vulnerabilities

Prepared by: Anastasiya Gruneva
Date: December 16th, 2024

Executive Summary/Introduction

The purpose of this technical report is to identify key vulnerabilities within Big Dog's systems, propose effective monitoring solutions, and provide actionable recommendations to enhance security.

Big Dog's infrastructure consists of critical assets such as SQL databases, IIS web servers, Linux systems, and Windows workstations, which store and manage sensitive information, including private client data, intellectual property, and financial records. Vulnerabilities, such as **SQL injection**, **misconfigurations**, and **unauthorized access**, expose these assets to significant risks.

To address these issues, a series of advanced monitoring sensors were proposed, including:

- **SQL Query Sensors** for detecting anomalies like SQL injection attacks.
- **File Integrity Monitoring (FIM)** for unauthorized modifications on critical files.
- **Bandwidth Usage Sensors** to detect data exfiltration or DDoS attacks.

These solutions align with industry frameworks like **MITRE ATT&CK** for threat detection and prioritize high-risk vulnerabilities based on CVSS scoring.

Key **recommendations** for improving security include:

1. **Enforcing Multi-Factor Authentication (MFA)** to prevent unauthorized access.
2. **Automated patch management** for systems with high CVSS vulnerabilities.
3. **Encrypting sensitive data** and maintaining offline backups.
4. **Training employees** on security best practices to mitigate phishing and insider threats.
5. **Developing Incident Response Plans (IRP)** and Disaster Recovery Plans (DRP) for operational resilience.

By implementing these measures, Big Dog can significantly reduce vulnerabilities, safeguard critical assets, and ensure a robust defense posture against evolving cyber threats.

Link to the video presentation:
https://drive.google.com/file/d/1JhszuO2hiVbesSyDCW42W_NFQU67wCdE/view?usp=drive_link

The List of Assets Owned by the Big Dog Organization and Their Vulnerabilities

The **Big Dog organization** possesses a range of critical assets and systems, each serving distinct purposes while carrying specific vulnerabilities. These assets include servers, databases, proprietary intellectual property, and tools supporting administrative, operational, and financial functions.

Network Overview and Asset Breakdown

The client's network is composed of the following key systems:

1. **Windows Servers**
   Runs:
   - SQL Database
   - IIS Web Server
   - PRTG Network Monitor (for monitoring network activity).

2. **Linux Systems**
   Used primarily by developers to create and manage proprietary intellectual property (IP).

3. **Windows Workstations**
   Support essential business functions such as:
   - Sales
   - Marketing
   - Management.

4. **Kali Systems**
   Serve as testing platforms and IT systems for security purposes.

The company categorizes all its information into six primary classes, prioritized as follows:

1. **Privacy (P):** SQL Database containing private employee and client information.
2. **Proprietary (IP):** Intellectual property, including programs and source code.
3. **Admin (A):** Administrative access credentials, configuration files, and tools.
4. **Financial/Accounting (F):** Financial data critical to company operations.
5. **Security Management (SM):** Logs, threat intelligence, and security policies.
6. **Systems (S):** Servers and networks essential for operational performance.

Security Categorization and Vulnerabilities

1. Privacy (P) – SQL Database

- **Vulnerability:** Susceptible to SQL Injection attacks, unauthorized access, and data exfiltration.
- **SC (Security Categorization):**
    - **Confidentiality:** High – A breach can lead to regulatory penalties and reputational harm.
    - **Integrity:** High – Unauthorized tampering disrupts operations.
    - **Availability:** High – Denial of access impacts continuity and trust.
- **SIL (Security Impact Level):** High, as any compromise has severe consequences.

2. Proprietary (IP) – Intellectual Property

- **Vulnerability:** Theft or alteration of source code and proprietary programs.
- **SC:**
    - **Confidentiality:** High – Competitive loss if IP is stolen.
    - **Integrity:** High – Altered code disrupts functionality and client trust.
    - **Availability:** High – Inaccessibility halts operations and revenue streams.
- **SIL:** High, given its critical value to business operations.

3. Admin (A) – Administrative Access and Tools

- **Vulnerability:** Risk of stolen credentials, misconfiguration, or privilege escalation.
- **SC:**
    - **Confidentiality:** High – Exposure of admin credentials leads to full system compromise.
    - **Integrity:** High – Altered configurations disrupt security controls.
    - **Availability:** High – Loss of access impairs incident response and operations.
- **SIL:** High, as admin access is a gateway to all critical systems and data.

4. Financial/Accounting (F) – Financial Data

- **Vulnerability:** Risk of unauthorized access, manipulation, or leaks of financial data.
- **SC:**
    - **Confidentiality:** High – Prevents unauthorized financial disclosures.
    - **Integrity:** Medium – Errors are impactful but manageable.
    - **Availability:** Medium – Access delays may inconvenience operations.
- **SIL:** Medium, as compromises are impactful but not catastrophic.

5. Security Management (SM) – Security Logs and Policies

- **Vulnerability:** Leakage or tampering with logs, policies, and configurations.
- **SC:**
    - **Confidentiality:** High – Leakage exposes defense mechanisms.
    - **Integrity:** Medium – Some measures are recoverable.
    - **Availability:** High – Downtime creates vulnerabilities.
- **SIL:** High, due to its role in overall security operations.

6. Systems (S) – Servers and Networks

- **Vulnerability:** Susceptible to exploitation, misconfigurations, and denial-of-service attacks.
- **SC:**
    - **Confidentiality:** High – Prevents unauthorized access to systems.
    - **Integrity:** Medium – Misconfigurations can disrupt performance.
    - **Availability:** High – Downtime affects overall operations.
- **SIL:** High, as system compromise impacts organizational resilience.

Table of Sensors

Sensor	Description	System	IoCs Associated	Rationale	Priority	Thresholds / Assumptions
MySQL Database Query Sensor	Monitors execution time.	SQL database	Excessive queries, failed logins, unusual access patterns.	Detects anomalies in queries affecting Privacy (P). Linked to SQL Injection (OWASP A03:2021)	High	Alerts for >10 failed logins, excessive read queries, or deviations in query behavior. Assumes moderate-normal activity during work hours.
HTTP Load Time Sensor	Monitors page load times.	IIS webserver	Malicious redirects, DDoS attacks, content injection	Detects performance degradation and potential attacks. Supports Systems (S) integrity and availability.	Medium	Triggers if response times deviate from baseline by 25%. Assumes stable baseline is predefined.
SSH Sensor	Tracks SSH access attempts, origin IPs, and command usage.	Linux Servers	Brute-force attacks, unauthorized logins	Protects Proprietary (IP) and Admin (A) data. Maps to MITRE T1110 (brute force) and T1021 (remote services).	High	Threshold for >5 failed login attempts, unusual geographic logins, or critical command execution. Assumes strong credential policies.
File Integrity Sensor	Tracks modification	Linux Servers	Malware activity, insider	Secures Proprietary (IP) and	High	Alerts on any unauthorized modifications or

	s to sensitive files on Linux servers.		threats, unauthorized deletions	Admin (A) data. Linked to MITRE T1070 (indicator removal) and T1496 (resource hijacking).		deletions of critical files. Assumes monitored file list is regularly updated.
Windows Event Log Sensor	Analyzes Windows Event Logs for abnormal patterns, privilege escalation, and login issues.	Windows workstations	Brute-force attempts, lateral movement, unauthorized user account creation	Supports Privacy (P) and Admin (A) data protection. Aligned with MITRE T1040 (credential dumping) and T1078 (valid accounts).	High	Threshold for unusual login times or privilege changes. Assumes event logs are regularly reviewed.
Bandwidth Usage Sensor	Tracks network bandwidth utilization and unusual spikes in traffic.	All	Data exfiltration, malware communication, DDoS attacks	Detects high-bandwidth anomalies affecting Privacy (P) and Systems (S). Linked to MITRE T1048 (exfiltration) and T1499 (DoS).	High	Triggers for sudden spikes exceeding baseline by 30%. Assumes normal network usage is consistent.
Antivirus Status Sensor	Monitors antivirus status and ensures real-time protection is active and updated.	All	Disabled AV, outdated signatures, unaddressed detections	Protects Privacy (P) and Security Management (SM) data. Aligned	Medium	Alerts for outdated definitions or inactive antivirus. Assumes centralized AV management for updates.

				with MITRE T1562 (disable or modify defenses).		
Web Traffic Sensor	Analyzes HTTP/HTTPS traffic patterns for anomalies like high request rates or malicious payloads.	IIS Webserver	DDoS, suspicious request rates, malicious payloads.	Protects Systems (S) and Privacy (P) by detecting web traffic anomalies. Linked to OWASP A1 (Injection) and MITRE T1499 (DoS).	High	Monitors high request rates, unusual traffic spikes. Assumes baseline web activity is well-defined.
File Integrity Sensor	Detects unauthorized changes to critical configuration files.	Windows & Linux	File modifications, deletions, or access from unknown users.	Protects Admin (A) and Proprietary (IP) data. Aligned with MITRE T1070 (indicator removal on host) and T1089 (disabling security tools).	High	Alerts for changes to sensitive files or directories. Assumes list of monitored files is updated periodically.
Vulnerability Scan Sensor	Identifies scanning tools like Nmap, unauthorized probes, or enumeration attempts.	Kali Systems	Network scans, port enumeration, vulnerability exploitation	Detects reconnaissance activities. Linked to MITRE T1046 (network service	High	Alerts on unknown scan attempts or tools from unauthorized hosts. Assumes defined whitelist of approved scanning tools.

				scanning) and T1135 (network share discovery).		

Discussion Section

Each sensor in the monitoring solution plays a vital role in securing Big Dog's network and assets. For example, the **SQL Query Sensor** monitors database interactions to detect anomalies such as excessive queries or failed login attempts. This is critical for safeguarding the Privacy (P) classification, as the SQL database contains sensitive employee and client information. Similarly, the **File Integrity Monitoring (FIM)** sensor identifies unauthorized changes to critical files, directly protecting Proprietary (IP) data.

The **Windows Event Log Monitor** examines abnormal patterns in system logs, such as privilege escalations or unauthorized access attempts, which can indicate potential threats to Admin (A) credentials. Other sensors, such as the **Bandwidth Usage Sensor**, help detect unusual network activity, such as data exfiltration or DDoS attacks, preserving Systems (S) integrity.

Connections to IoCs

Each sensor is designed to correlate specific Indicators of Compromise. For example:

- The **File Integrity Monitoring (FIM)** sensor may detect sudden, unauthorized changes to source code files, which could indicate insider threats or ransomware activity.
- The **Antivirus Health Sensor** identifies malware infections or outdated virus definitions, pointing to potential IoCs such as known malware signatures or unusual system behavior.
- The **HTTP Load Time Sensor** can detect unusual spikes in load time, possibly linked to content injection attacks or malicious redirects.

By linking sensors to IoCs, the solution ensures timely detection and mitigation of potential threats across Big Dog’s network.

Discussion of Thresholds

Thresholds are carefully chosen to minimize false positives while maximizing the detection of genuine threats:

- For the **Bandwidth Usage Sensor**, a deviation exceeding 30% of baseline usage triggers alerts, assuming normal fluctuations during peak hours.
- The **SQL Query Activity Sensor** flags more than 10 failed logins within a specified timeframe, balancing security with operational practicality.
- The **HTTP Load Time Sensor** monitors deviations significantly above average response times, accounting for occasional traffic spikes due to legitimate user activity.

These thresholds provide actionable insights without overwhelming IT staff with unnecessary alerts.

Recommendation Section

To address the identified vulnerabilities and enhance the security of Big Dog's systems, the following recommendations are made, referencing industry standards like **NIST**, **MITRE ATT&CK**, and **CVSS (Common Vulnerability Scoring System)** for context and prioritization:

1. Strengthen Access Control Mechanisms

- **Recommendation:**
  - Implement **Multi-Factor Authentication (MFA)** for administrative and user accounts across Windows servers and proprietary systems.
- **Rationale:**
  - Mitigates risks of credential theft or misuse.
- **Relevant Frameworks:**
  - **MITRE ATT&CK**: T1078 (Valid Accounts).
  - **CVSS**: Consider threats to credentials with a high impact on confidentiality and integrity.

2. Regular Patching and Vulnerability Management

- **Recommendation:**
  - Establish an automated patch management process for all software and systems, prioritizing high-severity vulnerabilities identified by CVSS scoring (e.g., CVSS 9.0+ for critical).
- **Rationale:**
  - Prevents exploitation of known vulnerabilities.
- **Relevant Frameworks:**
  - **MITRE ATT&CK**: T1068 (Exploitation of vulnerabilities for privilege escalation).
  - **CVSS**: Addresses risks with a high exploitation potential.

3. Encrypt Data and Strengthen Backup Strategies

- **Recommendation:**
  - Encrypt sensitive data.
  - Maintain offline backups of critical systems and test recovery processes regularly to ensure availability during a ransomware attack or disaster.
- **Rationale:**
  - Protects against data breaches and ensures data availability.
- **Relevant Frameworks:**
  - **CVSS**: Addresses high-impact risks on confidentiality and availability.

4. Security Awareness and Training

- **Recommendation:**

    - Conduct security awareness programs for employees, emphasizing phishing prevention, secure password practices, and recognizing suspicious activity.
    - Provide secure coding training for developers to reduce vulnerabilities in proprietary intellectual property.
- **Rationale:**
    - Reduces the risk of human error, a leading cause of security breaches.
- **Relevant Frameworks:**
    - **MITRE ATT&CK**: T1566 (Phishing).

5. Establish Incident Response and Disaster Recovery Plans

- **Recommendation:**
    - Develop a comprehensive **Incident Response Plan (IRP)** to handle breaches.
    - Design a **Disaster Recovery Plan (DRP)** for critical systems such as SQL databases.
- **Rationale:**
    - Ensures preparedness for rapid recovery and minimizes operational downtime.
- **Relevant Frameworks:**
    - **MITRE ATT&CK**: IR support for techniques like T1496 (Resource Hijacking).
    - **NIST SP 800-61**: Guidelines for effective incident handling.

By implementing these recommendations, Big Dog can significantly enhance the security of its systems, minimize risks, and protect its critical assets against potential threats.

References

Mitre ATT&CK®. MITRE ATT&CK®. (retrieved 2024-12-16). https://attack.mitre.org/

CVE. (retrieved 2024-12-16). https://cve.mitre.org/index.html

A03:2021 – injection. A03 Injection - OWASP Top 10:2021. (retrieved 2024-12-16). https://owasp.org/Top10/A03_2021-Injection/

Welcome to Paessler. Paessler. (retrieved 2024-12-16). https://www.paessler.com/

NIST NVD. (retrieved 2024-12-16). https://nvd.nist.gov/