Cat Scan II Big Dog

Cat Scan II Big Dog

Executive Summary

This report assesses the security sensors deployed at Big Dog, focusing on their ability to detect potential threats and vulnerabilities. The prioritization of these sensors is determined by the criticality of the data they monitor and the systems they protect. This includes monitoring load times, database queries, SSH connections, antivirus status, file integrity, Windows event logs, and bandwidth usage across Linux and Windows systems. Additionally, this report estimates the potential cost of damage should a security breach occur.

Table of Sensors

Sensor	Description	System	IoCs Associated	Rationale	Priority	Thresholds / Assumptions	NVD Base Score (CVSS)	Estimated Cost of Breach
HTTP Load Time Sensor	Monitors the time it takes for web pages to load.	Linux	Detect malicious redirects, DDoS attacks, or content injection	Load time changes can indicate performance issues or security breaches.	Medium	Changes of 20% over the average load time. SIL is high due to a higher chance of compromise despite low impact on CIA.	7.0 (High)	$50,000 - $100,000
MySQL Database Query Sensor	Monitors database queries and their performance.	Linux	Detect SQL injection attacks, unauthorized queries	Crucial for detecting unauthorized database activities that could compromise sensitive data.	High	Monitor for unusual query patterns or high-frequency queries that may indicate an ongoing attack.	8.5 (High)	$500,000 - $1,000,000

SSH Sensor	Monitors Secure Shell (SSH) connections for remote access.	Linux	Detect unauthorized access attempts or brute-force attacks	SSH is essential for secure remote access; high severity if compromised.	High	Set to a high threshold due to the risk of unauthorized access and potential breaches.	9.8 (Critical)	$300,000 - $800,000
Antivirus Status Sensor	Checks if antivirus software is running and up-to-date.	All	Detect if antivirus is disabled or outdated	Antivirus is crucial for general malware protection, with medium priority due to its broad coverage.	Medium	Monitor for both high and low conditions, ensuring all systems are protected.	6.8 (Medium)	$50,000 - $150,000
File Sensor	Monitors file integrity and changes in critical directories.	Linux	Detect unauthorized changes, deletions, or tampering with files	Ensures the integrity of critical files, particularly those containing sensitive data.	High	Immediate fix required; monitor for medium threshold activity.	7.5 (High)	$200,000 - $600,000
Windows Event Log Sensor	Logs significant events in Windows systems.	Windows 11	Detect failed login attempts, changes in user permissions	Critical for monitoring suspicious behavior on Windows systems.	High	Monitor for high threshold activity, particularly for events that indicate potential unauthorized access.	7.8 (High)	$150,000 - $500,000

Bandwidth Usage Sensor	Monitors network traffic and usage patterns.	All	Detect unusual traffic spikes indicating possible DDoS attacks	Identifies potential denial-of-service attacks, with medium priority due to potential service disruptions.	Medium	Monitor for sudden spikes that indicate a potential attack.	5.6 (Medium)	$100,000 - $300,

---

Explanation of Thresholds

1. **FTP Sensor - High Threshold**:
   - **Why:** The FTP server stores highly sensitive information. Any unauthorized access attempt or large data transfer, specifically exceeding **10% of the average daily transfer**, should be flagged to prevent data breaches.
2. **SSH Sensor - High Threshold**:
   - **Why:** SSH is critical for secure remote access. More than **5 failed login attempts within 2 minutes** or access attempts from suspicious IP addresses should trigger alerts to prevent unauthorized access.
3. **File Sensor - Medium Threshold**:
   - **Why:** Unauthorized changes to critical files can indicate tampering. Alerts should be triggered for any unauthorized change, detected within **1 millisecond** to ensure quick response.
4. **Antivirus Status Sensor - Both High and Low Thresholds**:
   - **Why:** It's essential to ensure that antivirus software is running and up-to-date. Alerts should be triggered if the antivirus is disabled or if virus definitions are **outdated by 3 days or more**.
5. **Windows Event Log Sensor - High Threshold**:
   - **Why:** This sensor monitors important security events on Windows systems. More than **3 failed login attempts within 1 minute** or unauthorized permission changes detected within **milliseconds** should trigger immediate alerts.
6. **Bandwidth Usage Sensor - High Threshold**:
   - **Why:** Sudden spikes in network traffic can be a sign of a DDoS attack. Alerts should be triggered for traffic spikes **exceeding 20% of average daily usage** within a short time frame to ensure timely detection and response.
7. **HTTP Load Time Sensor - High Threshold**:
   - **Why:** Changes in web page load time can indicate potential security issues, such as DDoS attacks or content injection. Alerts should be triggered for load time changes exceeding **20% of the average load time** to quickly identify and address these issues.

Discussion Section

1. **HTTP Load Time Sensor - Medium Priority (CVSS 7.0)**

Connection: The HTTP Load Time Sensor is responsible for monitoring the time it takes for web pages to load on Linux servers. Significant changes in load time can indicate performance-related issues or security breaches, such as DDoS attacks or malicious content injection.

IoCs: Changes in load time exceeding 20% over the average could indicate a compromise.

MITRE ATT&CK Techniques:

- T1499: Endpoint Denial of Service - DDoS: Unusual traffic or load times might indicate DDoS attacks.
- T1071.002: Application Layer Protocol - HTTPS: Potential content injection or redirection.

Priority Justification: Medium priority, with a focus on performance and security issues related to web services.

Thresholds: Monitor for changes in load time exceeding 20% over the average.

Estimated Cost of Damage: $50,000 - $100,000. This includes potential losses from website downtime, lost customer trust, and the cost of mitigating a DDoS attack.

2. **MySQL Database Query Sensor - High Priority (CVSS 8.5)**

Connection: The MySQL Database Query Sensor monitors the performance and frequency of database queries. It is essential for detecting unauthorized queries, which may indicate SQL injection attacks or other forms of database compromise.

IoCs: Unusual query patterns, high-frequency queries, or attempts to access restricted data.

MITRE ATT&CK Techniques:

- T1190: Exploit Public-Facing Application - SQL Injection: Attempts to exploit SQL vulnerabilities.
- T1078: Valid Accounts - Unauthorized Access: Use of legitimate credentials to perform unauthorized actions.

Priority Justification: High priority due to the sensitivity of the data stored in the database and the potential impact of a breach.

Thresholds: Monitor for unusual query patterns or high-frequency queries that may indicate an ongoing attack.

Estimated Cost of Damage: $500,000 - $1,000,000. A breach could result in the exposure of sensitive data, significant regulatory fines, and loss of customer trust.

3. **SSH Sensor - High Priority (CVSS 9.8)**

Connection: The SSH Sensor remains a high priority due to its role in securing remote access to Linux systems. Unauthorized SSH access can lead to significant security breaches, including the potential for full system compromise.

IoCs: Unauthorized access attempts, brute-force attacks, or unusual login patterns.

MITRE ATT&CK Techniques:

- T1110.001: Brute Force - Password Guessing: Attempts to gain access via SSH.
- T1021.004: Remote Services - SSH: Exploiting SSH for lateral movement or remote access.

Priority Justification: High priority due to the severe impact of potential SSH compromise.

Thresholds: High threshold monitoring for activities indicating a high risk of breach.

Estimated Cost of Damage: $300,000 - $800,000. This includes potential losses from data breaches, system downtime, and the cost of recovery.

4. **Antivirus Status Sensor - Medium Priority (CVSS 6.8)**

Connection: The Antivirus Status Sensor monitors the status of antivirus software across all systems. It checks whether the software is running, updated, and functioning properly. This is crucial for general malware protection, with a medium priority due to its broad coverage.

IoCs: Disabled antivirus, outdated definitions, or failure to update.

MITRE ATT&CK Techniques:

- T1497.001: Virtualization/Sandbox Evasion - Software Discovery: Attackers disabling or bypassing antivirus.
- T1059.003: Command and Scripting Interpreter - Windows Command Shell: Potential exploitation due to lack of antivirus.

Priority Justification: Medium priority, focusing on maintaining a secure environment across all systems.

Thresholds: Monitor for high and low conditions to ensure comprehensive protection.

Estimated Cost of Damage: $50,000 - $150,000. Potential damages include system infections, ransomware attacks, and the cost of malware removal.

5. **File Sensor - High Priority (CVSS 7.5)**

Connection: The File Sensor monitors the integrity of critical files on Linux systems, ensuring that unauthorized changes, deletions, or tampering are promptly detected. This is vital for maintaining the integrity of sensitive data.

IoCs: Unauthorized changes, deletions, or attempts to modify critical files.

MITRE ATT&CK Techniques:

- T1565.001: Data Manipulation - Stored Data Manipulation: Modifying or corrupting files to disrupt operations.
- T1070.004: Indicator Removal on Host - File Deletion: Deleting logs or other files to cover tracks.

Priority Justification: High priority due to the critical nature of the data being monitored.

Thresholds: Immediate fix required; monitor for medium threshold activity to ensure file integrity.

Estimated Cost of Damage: $200,000 - $600,000. A breach could result in significant data loss, legal consequences, and the cost of restoring file integrity.

6. Windows Event Log Sensor - High Priority (CVSS 7.8)

Connection: The Windows Event Log Sensor logs significant events on Windows 11 systems, such as failed login attempts, changes in user permissions, or other activities that could indicate a security threat. This sensor is critical for detecting suspicious behavior on Windows systems.

IoCs: Failed login attempts, privilege escalation, or unauthorized changes in system configurations.

MITRE ATT&CK Techniques:

- T1078.003: Valid Accounts - Local Accounts: Attempts to use local accounts to gain unauthorized access.
- T1087.002: Account Discovery - Domain Account: Identifying and exploiting domain accounts.

Priority Justification: High priority due to the importance of monitoring for potential unauthorized access on Windows systems.

Thresholds: Monitor for high threshold activity, particularly for events that indicate potential unauthorized access.

7. Bandwidth Usage Sensor - Medium Priority (CVSS 5.6)

Connection: The Bandwidth Usage Sensor monitors network traffic and usage patterns across all systems. Unusual spikes in traffic can indicate potential DDoS attacks or other network-based threats.

IoCs: Sudden spikes in bandwidth usage or unusual traffic patterns.

MITRE ATT&CK Techniques:

- T1498: Network Denial of Service - Flooding: Overloading network resources to cause disruption.
- T1071.001: Application Layer Protocol - Web Protocols: Abnormal usage patterns indicating potential data exfiltration or attacks.

Priority Justification: Medium priority, focusing on detecting network-based threats that could disrupt services.

Thresholds: Monitor for sudden spikes in traffic that could indicate an ongoing attack.

4. Other Sensors

- **Antivirus Status Sensor (CVSS 6.8):** Medium priority with a CVSS score of 6.8, ensuring that antivirus software remains active and up-to-date to protect against a range of threats.
- **Windows Event Log Sensor (CVSS 7.8):** High priority with a CVSS score of 7.8, critical for detecting suspicious activities on Windows systems.
- **Bandwidth Usage Sensor (CVSS 5.6):** Medium priority with a CVSS score of 5.6, focused on identifying potential DDoS attacks through unusual traffic patterns.

Risk Assessment Chart

Asset	Threat	Vulnerability	Likelihood	Impact	Risk Level	Mitigation
FTP Server	Unauthorized Access, Data Exfiltration	Weak encryption, lack of multi-factor authentication	High	High	Critical	Implement strong encryption, enforce multi-factor authentication, monitor access logs.
SSH Connection	Brute-Force Attack, Credential Theft	Weak passwords, lack of account lockout policies	High	High	Critical	Enforce strong password policies, implement account lockout, monitor for unusual login attempts.
Critical File Integrity	Unauthorized File Changes, Data Tampering	Insufficient file monitoring, delayed detection of changes	Medium	High	High	Implement real-time file integrity monitoring, fix sensor errors, regular file audits.
Antivirus Software	Malware Infections	Outdated definitions, disabled antivirus	Medium	Medium	Medium	Ensure antivirus is updated regularly, monitor for antivirus status, educate users on safe practices.
Windows Systems	Unauthorized Access, Privilege Escalation	Insecure user permissions, lack of monitoring	Medium	High	High	Regularly audit user permissions, monitor event logs, implement least privilege access policies.
Network Traffic	DDoS Attack	Unmonitored bandwidth spikes	Low	Medium	Medium	Monitor bandwidth usage, set thresholds for unusual traffic spikes, implement DDoS protection tools.
MySQL Database	Unauthorized Access, SQL Injection	Lack of query monitoring, weak input validation	High	High	Critical	Implement strict input validation, regular security audits, and

---

Recommendation Section

1. Enhanced Monitoring for FTP Server: Given the elevated importance of the FTP server, it is recommended to implement additional security measures, such as encrypted data transmission, multi-factor authentication, and enhanced access controls. Regularly review and update security policies to reflect the sensitivity of the data stored.

2. Implement NIST Cybersecurity Framework (CSF) with CVSS Integration:

- **Identify:** Catalog and classify all assets, especially those containing sensitive information, integrating CVSS scores to assess the potential impact of vulnerabilities.
- **Protect:** Use CVSS scores to prioritize security controls, ensuring that high-risk systems (e.g., FTP server with a CVSS score of 9.0) are adequately protected.
- **Detect:** Enhance detection capabilities by aligning sensor thresholds with CVSS scores, ensuring that higher-risk systems are monitored more closely.

- **Respond:** Develop an incident response plan incorporating CVSS scores to prioritize response actions based on the severity of vulnerabilities.
- **Recover:** Use CVSS scores to prioritize recovery efforts, ensuring that the most critical systems are restored first.

3. Continuous Monitoring and Review: Regularly review the effectiveness of all sensors and adjust thresholds based on updated CVSS scores and the criticality of the data they protect. Implement additional sensors as needed to cover any identified gaps in monitoring.

4. Data Encryption and Access Controls: Implement strong encryption methods for data stored on the FTP server and restrict access to authorized personnel only. Regularly audit access logs to detect and respond to unauthorized access attempts.

References:

NIST Risk Management Framework RMF. (n.d.). NIST. Retrieved September 4, 2024, from https://csrc.nist.gov/Projects/risk-management/about-rmf/prepare-step

Common Vulnerability Scoring System Calculator. (n.d.). NIST .https://nvd.nist.gov/vuln-metrics/cvss/v4-calculator

Mitre Att&ACK framework. Mitre Attack Framework. (n.d.). https://attack.mitre.org/

Mitre. (n.d.). Retrieved September 4, 2024, from https://attack.mitre.org/techniques/T1210/

Exploit Public-Facing Application. (n.d.). Mitre. Retrieved September 4, 2024, from https://attack.mitre.org/techniques/T1190/

Valid Accounts: Local Accounts. (n.d.). Mitre. Retrieved September 4, 2024, from https://attack.mitre.org/techniques/T1078/003/

Indicator Removal: File Deletion. (n.d.). Mitre Techniques. Retrieved September 4, 2024, from https://attack.mitre.org/techniques/T1070/004/

Virtualization/Sandbox Evasion: System Checks. (n.d.). Mitre Techniques. Retrieved September 4, 2024, from https://attack.mitre.org/techniques/T1497/001/

Remote Services: SSH. (n.d.). Mitre Techniques. Retrieved September 4, 2024, from https://attack.mitre.org/techniques/T1021/004/

Brute Force: Password Guessing. (n.d.). Mitre Techniques. Retrieved September 4, 2024, from https://attack.mitre.org/techniques/T1110/001/

Application Layer Protocol: File Transfer Protocols. (n.d.). Mitre Techniques. https://attack.mitre.org/techniques/T1071/002/

Endpoint denial of service. (n.d.). Mitre Techniques. Retrieved September 4, 2024, from https://attack.mitre.org/techniques/T1499/

Top 10 Best Practices for Network Monitoring in 2023. (n.d.). Spiceworks. Retrieved September 4, 2024, from https://www.spiceworks.com/tech/networking/articles/network-monitoring-best-practices/

/