**Cat Scan II Big Dog**

**Executive Summary**

This report provides a comprehensive analysis and recommendations for monitoring sensors within the Big Dog organization, based on the Cat Scan II case study. The focus is on identifying key sensors, associating them with Indicators of Compromise (IoCs), and prioritizing them based on the Security Impact Levels (SIL). The top five important sensors are HTTP Load Time, MySQL Database Query, SSH, File, and Bandwidth Usage. These sensors are critical for detecting and mitigating potential threats such as DDoS attacks, SQL injection, unauthorized access, ransomware, and data exfiltration. The report also specifies alert thresholds and ties findings to industry-standard frameworks.

**Introduction**

The purpose of this report is to provide recommendations on the sensors that should be monitored for the Big Dog organization, based on the case study Cat Scan II. The report outlines the rationale for prioritizing each sensor, associating them with Indicators of Compromise (IoCs), threats, and vulnerabilities. The scope includes outlining the rationale for prioritizing each sensor, specifying alert thresholds, and aligning findings with industry-standard frameworks. It also specifies the alert thresholds and assumptions made, along with the Security Impact Levels (SIL) for each system monitored.

**Sensors and Indicators of Compromise (IoCs)**

1. **HTTP Load Time Sensor**
   * **IoCs**: Slow response times, unusual spikes in traffic.
   * **Threats**: DDoS attacks, web application attacks.
   * **Alert Thresholds**: Response time > 2 seconds, traffic spike > 100% of average.
2. **MySQL Database Query Sensor**
   * **IoCs**: Unusual query patterns, high query volume.
   * **Threats**: SQL injection, database breaches.
   * **Alert Thresholds**: high query volume > 1000 queries/min, slow query of < 20 requests/min.
3. **SSH Sensor**
   * **IoCs**: Multiple failed login attempts, unusual login times.
   * **Threats**: Unauthorized access, brute force attacks.
   * **Alert Thresholds**: > 5 failed login attempts within 10 minutes, logins outside business hours.
4. **File Sensor**
   * **IoCs**: Unusual file modifications, high file access rate.
   * **Threats**: Ransomware, data exfiltration.
   * **Alert Thresholds**: high file access rate of > 50 file modifications within 10 minutes
5. **Bandwidth Usage Sensor**
   * **IoCs**: Unusual bandwidth usage, spikes in data transfer.
   * **Threats**: Data exfiltration, DDoS attacks.
   * **Alert Thresholds**: Bandwidth usage > 80% of capacity, data transfer spike > 100% of average.
6. **Antivirus Status Sensor**
   * **IoCs:** Outdated antivirus definitions, disabled antivirus software.
   * **Threats:** Malware infections, ransomware attacks.
   * **Alert Thresholds:** Outdated antivirus definitions, disabled antivirus software.
7. **Windows Event Log Sensor**
   * **IoCs:** Repeated login failures, unusual login times, access to sensitive files.
   * **Threats:** Insider threats, persistent threats, unauthorized access.
   * **Alert Thresholds:** More than 5 login attempts, privileged access to sensitive files, unusual login times outside business hours.

A screenshot of a computer

Description automatically generated

Sensors on PRTG

A screenshot of a computer

Description automatically generated

Http Load time sensor on PRTG

A screenshot of a computer

Description automatically generated

PRTG Upper Errpr & Warning limits set for monitoring alerts

**Security Impact Levels (SIL)** The Security Impact Levels (SIL) for each sensor are determined based on the potential impact of a security breach on the organization. The following table summarizes the SILs for each sensor:

| **Sensor** | **SIL** | **Impact** |
| --- | --- | --- |
| HTTP Load Time Sensor | SIL 3 | High impact on web application performance and availability. |
| MySQL Database Query Sensor | SIL 4 | Critical impact on data integrity and confidentiality. |
| SSH Sensor | SIL 3 | High impact on system access control and security. |
| File Sensor | SIL 4 | Critical impact on data integrity and availability. |
| Bandwidth Usage Sensor | SIL 2 | Moderate impact on network performance and potential data exfiltration. |
| Antivirus Status  Sensor | SIL 2 | Moderate impact on endpoint protection and vulnerability to malware. |
| Windows Event  Log Sensor | SIL 3 | High impact on detecting insider threats and persistent threats through log analysis. |

**Table of Sensors**

| **Sensor** | **Description** | **System** | **IoCs** | **Rationale** | **Priority** | **Thresholds/Assumptions** |
| --- | --- | --- | --- | --- | --- | --- |
| HTTP Load Time | Monitors the time it takes for the page to load | Linux | Malicious Redirects, DDoS Attacks, 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 | 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 high. |
| MySQL Database Query Sensor | Tracks the performance and anomalies in MySQL database queries | Linux | Slow queries, unusual query patterns | Identifies potential SQL injection attacks and database performance issues | High | Monitor for slow query volume < 20 requests/min & high query volume > 1000 queries/min |
| SSH Sensor | Monitors SSH login attempts and activities | Linux | Unauthorized access attempts, unusual login times | Detects brute force attacks and unauthorized access attempts | High | Monitor for 5 failed login attempts within 10 min, login attempts outside business hours |
| Antivirus Status Sensor | Checks the status and updates of antivirus software | All | Outdated antivirus definitions, disabled antivirus | Ensures endpoints are protected against malware and other threats | Medium | Monitor for outdated or disabled antivirus software |
| File Sensor | Tracks changes to critical files and directories | Linux | Unauthorized file changes, unusual file access | Detects potential ransomware and unauthorized file modifications | High | Monitor for high file access rate > 50 file modifications per 10 minutes |
| Windows Event Log Sensor | Collects and analyzes Windows event logs for anomalies | Windows 11 | Repeated login failures, unusual login times, access to sensitive files | Provides insights into potential insider threats and persistent threats | Medium | Monitor for > 5 login attempts, privileged access to sensitive files, and login times outside business hours |
| Bandwidth Usage Sensor | Monitors the bandwidth usage across the network | All | Unusual bandwidth usage, data exfiltration | Detects potential data exfiltration and network performance issues | High | Monitor for Bandwidth usage > 80% capacity, data transfer spike > 100% of average |

**Prioritization Rationale**

* **Asset Prioritization**: Critical assets include network infrastructure, endpoints, databases, and sensitive data.
* **Vulnerabilities**: Key vulnerabilities include unpatched systems, weak access controls, and insufficient monitoring.
* **Threats**: Potential threats include DDoS attacks, SQL injection, brute force attacks, ransomware, and insider threats.
* **Tactics and Techniques**: Attackers may use tactics such as lateral movement, privilege escalation, and data exfiltration.
* **Risk Severity**: High-risk assets require immediate attention, while lower-risk assets can be monitored less frequently.

**Security Impact Levels (SIL) Justification**

1. **HTTP Load Time**
   * **System**: Linux
   * **SIL**: High
   * **Justification**: Monitoring HTTP load times is crucial for detecting potential DDoS attacks and server performance issues. A compromised web server can lead to significant downtime, affecting the organization’s availability and reputation.
   * **CIA Impact**:
     + **Confidentiality**: Low impact, as load times do not directly affect data confidentiality.
     + **Integrity**: Moderate impact, as compromised load times can indicate underlying issues affecting data integrity.
     + **Availability**: High impact, as slow or unresponsive servers can lead to significant downtime.
2. **MySQL Database Query Sensor**
   * **System**: Linux
   * **SIL**: High
   * **Justification**: Databases often contain sensitive and critical information. Monitoring MySQL queries helps detect SQL injection attacks and performance issues, which can lead to data breaches and operational disruptions.
   * **CIA Impact**:
     + **Confidentiality**: High impact, as databases often contain sensitive information.
     + **Integrity**: High impact, as SQL injection can compromise data integrity.
     + **Availability**: Moderate impact, as database performance issues can affect availability.
3. **SSH Sensor**
   * **System**: Linux
   * **SIL**: High
   * **Justification**: SSH is commonly used for remote management of systems. Unauthorized access via SSH can lead to full system compromise. Monitoring SSH activities helps prevent brute force attacks and unauthorized access.
   * **CIA Impact**:
     + **Confidentiality**: High impact, as unauthorized access can expose sensitive information.
     + **Integrity**: High impact, as unauthorized access can lead to data tampering.
     + **Availability**: High impact, as unauthorized access can disrupt system operations.
4. **Antivirus Status Sensor**
   * **System**: All
   * **SIL**: Moderate
   * **Justification**: Ensuring antivirus software is up-to-date and active is essential for protecting endpoints from malware. While important, the impact of outdated antivirus software is generally less immediate compared to direct attacks on critical systems.
   * **CIA Impact**:
     + **Confidentiality**: Moderate impact, as outdated antivirus software can leave endpoints vulnerable to malware.
     + **Integrity**: Moderate impact, as malware can compromise data integrity.
     + **Availability**: Moderate impact, as malware can disrupt system operations.
5. **File Sensor**
   * **System**: Linux
   * **SIL**: High
   * **Justification**: Monitoring changes to critical files can detect ransomware and unauthorized modifications. Compromised files can lead to data loss and operational disruptions, making this a high-impact area.
   * **CIA Impact**:
     + **Confidentiality**: High impact, as unauthorized file changes can expose sensitive information.
     + **Integrity**: High impact, as unauthorized file changes can compromise data integrity.
     + **Availability**: High impact, as ransomware can encrypt files, making them unavailable.
6. **Windows Event Log Sensor**
   * **System**: Windows 11
   * **SIL**: Moderate
   * **Justification**: Analyzing Windows event logs helps identify potential insider threats and persistent threats. While important for security, the impact is generally moderate as it provides insights rather than real-time prevention.
   * **CIA Impact**:
     + **Confidentiality**: Moderate impact, as logs can reveal sensitive information about system activities.
     + **Integrity**: Moderate impact, as logs can help detect unauthorized changes.
     + **Availability**: Moderate impact, as logs provide historical data rather than real-time monitoring.
7. **Bandwidth Usage Sensor**
   * **System**: All
   * **SIL**: High
   * **Justification**: Monitoring bandwidth usage is critical for detecting data exfiltration and network performance issues. Unusual bandwidth usage can indicate significant security breaches, making this a high-impact area.
   * **CIA Impact**:
     + **Confidentiality**: High impact, as data exfiltration can lead to sensitive information being leaked.
     + **Integrity**: Moderate impact, as bandwidth usage does not directly affect data integrity.
     + **Availability**: High impact, as network performance issues can disrupt operations.

**Sensor Recommendations**

1. **HTTP Load Time**
   * **System**: Linux
   * **IoCs Monitored**: Slow load times, unusual traffic patterns.
   * **Threats Addressed**: DDoS attacks, server performance issues.
   * **Alert Thresholds**: Monitor changes of 20% over the average load and consistent increase in page load time exceeding 5 seconds.
   * **Priority**: High
   * **SIL**: High
2. **MySQL Database Query Sensor**
   * **System**: Linux
   * **IoCs Monitored**: Slow queries, unusual query patterns.
   * **Threats Addressed**: SQL injection attacks, database performance issues.
   * **Alert Thresholds**: Monitor for slow query volume < 20 requests/min & high query volume > 1000 queries/min
   * **Priority**: High
   * **SIL**: High
3. **SSH Sensor**
   * **System**: Linux
   * **IoCs Monitored**: Unauthorized access attempts, unusual login times.
   * **Threats Addressed**: Brute force attacks, unauthorized access attempts.
   * **Alert Thresholds**: Monitor for 5 failed login attempts within 10 min, login attempts outside business hours
   * **Priority**: High
   * **SIL**: High
4. **Antivirus Status Sensor**
   * **System**: All
   * **IoCs Monitored**: Outdated antivirus definitions, disabled antivirus.
   * **Threats Addressed**: Malware, other threats.
   * **Alert Thresholds**: Monitor for outdated or disabled antivirus software.
   * **Priority**: Medium
   * **SIL**: Moderate
5. **File Sensor**
   * **System**: Linux
   * **IoCs Monitored**: Unauthorized file changes, unusual file access.
   * **Threats Addressed**: Ransomware, unauthorized file modifications.
   * **Alert Thresholds**: Monitor for high file access rate > 50 file modifications per 10 minutes
   * **Priority**: High
   * **SIL**: High
6. **Windows Event Log Sensor**
   * **System**: Windows 11
   * **IoCs Monitored**: Repeated login failures, unusual login times, access to sensitive files.
   * **Threats Addressed**: Insider threats, persistent threats.
   * **Alert Thresholds**: Monitor for > 5 login attempts, privileged access to sensitive files, and login times outside business hours
   * **Priority**: Medium
   * **SIL**: Moderate
7. **Bandwidth Usage Sensor**
   * **System**: All
   * **IoCs Monitored**: Unusual bandwidth usage, data exfiltration.
   * **Threats Addressed**: Data exfiltration, network performance issues.
   * **Alert Thresholds**: Monitor for Bandwidth usage > 80% capacity, data transfer spike > 100% of average
   * **Priority**: High
   * **SIL**: High

**Monitoring Recommendations**

* **High Priority**: HTTP Load Time, MySQL Database Query Sensor, SSH Sensor, File Sensor, and Bandwidth Usage Sensor for real-time detection and response.
* **Medium Priority**: Antivirus Status Sensor and Windows Event Log Sensor for detecting potential threats and providing insights into persistent threats.

**Discussion Section**

1. **HTTP Load Time**
   * **Assumption**: Big Dog does not have a large web presence, and the Linux web server being monitored is internal, with this one being outward-facing.
   * **Impact**: There is a relatively low impact on Confidentiality, Integrity, and Availability (CIA), specifically Availability, but a higher chance of compromise.
   * **IoCs**: Slow load times, unusual traffic patterns.
   * **Vulnerabilities and Risks**: DDoS attacks can overwhelm servers, causing slow load times and potential downtime.
   * **Threshold**: Changes of 20% over the average load time are monitored to detect potential anomalies.
2. **MySQL Database Query Sensor**
   * **Assumption**: The MySQL database contains critical and sensitive information.
   * **Impact**: High impact on CIA if compromised, as it could lead to data breaches and operational disruptions.
   * **IoCs**: Slow queries, unusual query patterns.
   * **Vulnerabilities and Risks**: SQL injection attacks can compromise database integrity and expose sensitive data.
   * **Thresholds**: Monitor for slow query performance and unusual query patterns to identify potential SQL injection attempts.
3. **SSH Sensor**
   * **Assumption**: SSH is used for remote management of critical systems.
   * **Impact**: High impact on CIA if unauthorized access is gained, leading to potential system compromise.
   * **IoCs**: Unauthorized access attempts, unusual login times.
   * **Vulnerabilities and Risks**: Brute force attacks and unauthorized access can lead to system compromise.
   * **Thresholds**: Monitor for repeated login failures and unusual login times to detect unauthorized access attempts.
4. **Antivirus Status Sensor**
   * **Assumption**: All endpoints must have up-to-date and active antivirus software.
   * **Impact**: Moderate impact on CIA if antivirus software is outdated or disabled, increasing vulnerability to malware.
   * **IoCs**: Outdated antivirus definitions, disabled antivirus.
   * **Vulnerabilities and Risks**: Outdated or disabled antivirus software can leave endpoints vulnerable to malware.
   * **Thresholds**: Monitor for outdated or disabled antivirus software to ensure endpoints are protected.
5. **File Sensor**
   * **Assumption**: Critical files and directories are essential for the organization’s operations.
   * **Impact**: High impact on CIA if files are modified or encrypted by ransomware, leading to data loss and operational disruptions.
   * **IoCs**: Unauthorized file changes, unusual file access.
   * **Vulnerabilities and Risks**: Ransomware and unauthorized file modifications can lead to data loss and operational disruptions.
   * **Thresholds**: Monitor for unauthorized file changes and unusual file access to detect potential ransomware activity.
6. **Windows Event Log Sensor**
   * **Assumption**: Windows event logs provide valuable insights into system activities and potential threats.
   * **Impact**: Moderate impact on CIA if insider threats or persistent threats are not detected.
   * **IoCs**: Repeated login failures, unusual login times, access to sensitive files.
   * **Vulnerabilities and Risks**: Insider threats and persistent threats can be identified through log analysis.
   * **Thresholds**: Monitor for repeated login failures, access to sensitive files, and unusual login times to detect potential insider threats.
7. **Bandwidth Usage Sensor**
   * **Assumption**: Monitoring bandwidth usage is crucial for detecting data exfiltration and network performance issues.
   * **Impact**: High impact on CIA if unusual bandwidth usage indicates data exfiltration or network performance issues.
   * **IoCs**: Unusual bandwidth usage, data exfiltration.
   * **Vulnerabilities and Risks**: Data exfiltration and network performance issues can be detected through bandwidth monitoring.
   * **Thresholds**: Monitor for unusual bandwidth usage and data exfiltration to detect potential security breaches.

**Recommendation Section**

To enhance the security of the Big Dog organization, it is recommended to:

1. **Implement Additional Sensors**: Consider adding sensors for monitoring email traffic, DNS queries, and application logs to provide a more comprehensive security posture.

**Policy**: Implement an email traffic sensor to detect phishing attempts and monitor DNS queries for unusual patterns indicating potential domain spoofing.

**Industry Standard**: NIST SP 800-53 (SI-4) for monitoring and analyzing information system activity.

1. **Regularly Update and Patch Systems**: Ensure all systems and software are regularly updated and patched to mitigate vulnerabilities.

**Policy**: Establish a patch management policy that includes regular updates of once a month and emergency patching procedures.

**Industry Standard**: CIS Control 3 for continuous vulnerability management.

1. **Conduct Regular Security Audits**: Perform regular security audits and penetration testing to identify and address potential weaknesses.

**Policy**: Schedule quarterly security audits and annual penetration tests to evaluate the effectiveness of security controls.

**Industry Standard**: NIST SP 800-115 for technical guide to information security testing and assessment.

1. **Employee Training and Awareness**: Conduct regular training sessions for employees to raise awareness about security best practices and phishing attacks.

**Policy**: Implement a phishing simulation program to educate employees on recognizing and responding to phishing attempts.

**Industry Standard**: NIST SP 800-50 for building an information technology security awareness and training program.

1. **Adopt Industry Best Practices**: Follow industry-standard frameworks such as NIST, MITRE ATT&CK, and CIS Controls to guide security practices and policies.

**Policy**: Implement these frameworks to ensure a robust and comprehensive security posture and manage risks.

**Industry Standards**: Reference NIST Cybersecurity Framework, MITRE ATT&CK, and CIS Controls for comprehensive guidelines.

By following these recommendations and continuously monitoring the specified sensors, the Big Dog organization can significantly enhance its security posture and mitigate potential risks ensuring the protection of its critical assets and data.

**Conclusion**

This report provides a detailed analysis of the sensors recommended for monitoring within the Big Dog organization. By prioritizing sensors based on the nature of the risk, Indicators of Compromise (IoCs), and the severity of potential threats, and assigning appropriate Security Impact Levels (SIL), the organization can enhance its security posture and effectively mitigate risks. Following the recommendations and continuously monitoring the specified sensors will significantly improve the organization’s ability to detect and respond to potential threats.

**References & Citation**

1. Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology*. https://doi.org/10.6028/nist.sp.800-61r2
2. *MITRE ATT&CK®*. (n.d.). https://attack.mitre.org/
3. *Security and privacy controls for information systems and organizations*. (2020). https://doi.org/10.6028/nist.sp.800-53r5
4. Ross, R., Pillitteri, V., Dempsey, K., Riddle, M., & Guissanie, G. (2020). *Protecting controlled unclassified information in nonfederal systems and organizations*. https://doi.org/10.6028/nist.sp.800-171r2
5. Souppaya, M., & Scarfone, K. (2013). *Guide to malware incident Prevention and handling for desktops and laptops*. https://doi.org/10.6028/nist.sp.800-83r1
6. Kent, K., & Souppaya, M. P. (2006). *Guide to computer security log management*. <https://doi.org/10.6028/nist.sp.800-92>
7. *About us - CIS®*. (2021, July 23). CIS. https://www.cisecurity.org/cis-benchmarks
8. Scarfone, K. A., Souppaya, M. P., Cody, A., & Orebaugh, A. D. (2008). *Technical guide to information security testing and assessment.* https://doi.org/10.6028/nist.sp.800-115