# Cybersecurity Monitoring Strategy Using PRTG

## A Risk and Vulnerability Report

## For

## Big Dog Enterprise

By

Ifeanyi Christian Edeh

Cybersecurity Specialist

https://linkedin.com/in/ifeanyiedeh

March 5, 2025

## Table of Contents

## Executive Summary

Big Dog operates a network infrastructure consisting of Windows Servers, Linux development machines, Windows workstations and Kali test systems. The company's critical assets, including proprietary intellectual property, SQL databases, and sensitive user data, necessitate a robust cybersecurity monitoring strategy to uphold confidentiality, integrity, and availability.

This report presents a proactive cybersecurity monitoring solution using **PAESSLER's PRTG Network Monitor**, designed to detect Indicators of Compromise (IoCs), mitigate potential threats, and enhance incident response.

Through a structured analysis, five key Security Impact Levels (SILs) were identified, to prioritize Big Dog's cybersecurity efforts:

- **Privacy** – Protecting sensitive customer and employee data from unauthorized access and potential breaches.
- **Proprietary** – Securing intellectual property stored within Linux development environments to prevent data leaks or theft.
- **Administrative** – Ensuring the integrity and reliability of Windows servers that manage SQL databases and network monitoring tools.
- **Financial** – Safeguarding accounting and financial systems against fraud, unauthorized access, and data manipulation.
- **Security Management** – Securing PRTG network monitoring and security logs to ensure accurate threat detection and timely response.

These five Security Impact Levels (SILs) were identified, and corresponding sensors were recommended to proactively monitor Indicators of Compromise (IoCs) and minimize risks (Paessler, 2023). By prioritizing high-risk areas such as CPU load, network traffic, SQL database performance, SSH authentication, Antivirus integrity, system file integrity, and unauthorized access attempts, we ensure early detection of cyber threats. Thresholds have been established for each sensor based on industry best practices to prevent false positives while ensuring real-time monitoring and alerting mechanisms (NIST, 2023).

This monitoring framework is built on industry-leading best practices, integrating methodologies from **MITRE ATT&CK**, and the **NIST Cybersecurity Frameworks**.
The recommendations outlined in this report will strengthen Big Dog's cybersecurity posture, enhance real-time threat detection, minimize security risks, and ensure business continuity in an evolving threat landscape.

## Methodology

I developed a comprehensive security monitoring plan by following a strategic four-step approach.

1. **Identifying Critical Assets**: I categorized Big Dog's infrastructure under Privacy (P), Proprietary (IP), Administrative (A), Financial (F) and Network Perimeter and Customer-facing Services to determine security priorities. Mapped using **NIST RMF (Prepare)**

2. **Mapping Threats and IoCs:** Using the MITRE ATT&CK framework, we identified key attack techniques and potential vulnerabilities in Big Dog's network. Mapped using **NIST CSF (Identify)**

3. **Deploying Monitoring Sensors:** I selected PRTG sensors to monitor high-risk areas, including database performance, SSH access, file integrity, antivirus status, and bandwidth usage. Mapped using **NIST CSF (Detect)**

4. **Configuring Alert Thresholds:** I set specific monitoring thresholds based on system behavior to minimize false positives while ensuring timely detection of threats. Mapped using **NIST CSF (Respond)**

## Table of Sensors

| Sensor | Description | System | IoCs Monitored | Rationale | Priority | Thresholds |
|---|---|---|---|---|---|---|
| **CPU Load Sensor** | Monitors CPU usage to detect anomalies | Windows Server | Malware execution, resource exhaustion attacks | High CPU usage may indicate malicious processes or DoS attacks. | High | Trigger alerts for sustained CPU usage over 85%. |
| **HTTP Load Time sensor** | Monitors website response time | Linux server | DDoS attack | The server hangs or if the load time spikes | Medium | Trigger alert when more than 20% slower than baseline |
| **MySQL Database Query** | Monitors query execution time | Windows Server | SQL injection, unauthorized access | Detects abnormal database activity | High | Alert if query time greater than one second |
| **SSH Login Sensor** | Tracks SSH authentication attempts | Linux server | Brute-force attacks, unauthorized logins | Identifies suspicious login attempts | High | Alert on more than 5 failed SSH logins in 5 minutes |
| **Antivirus Status Sensor** | Checks Antivirus status and update frequency | All Systems | Antivirus disablement, malware infection | Ensures Antivirus is active and updated | High | Alert if Antivirus inactive or outdated more than 7 days |
| **File Integrity Sensor** | Detects unauthorized file modifications | Linux Server | File tampering, malware persistence | Protects system and configuration files | High | Alert on any unauthorized changes |
| **Windows Event Log Sensor** | Monitors Windows security event logs | Windows Server | Unauthorized access, privilege escalation | Identifies privilege abuse and admin activity | High | Alert on new admin account creation |
| **Bandwidth Usage Sensor** | Monitors inbound/outbound network traffic | All Systems | Data exfiltration, DDoS attacks | Identifies large data transfers or attack patterns | Medium | Alert if traffic exceeds 150% of baseline |

## Discussion

Each monitoring sensor plays a crucial role in securing Big Dog's network, ensuring early detection of suspicious activities and preventing cyber threats. This section explores the significance of each sensor, their corresponding Indicators of Compromise (IoCs), and the thresholds set to maintain Big Dog's network security and performance.

### CPU Load Sensor *(MITRE: T1055; NIST CSF: DE.CM)*

- **Importance:** High CPU usage could indicate malware execution or a distributed denial-of-service (DDoS) attack.
- **Thresholds:** Alerts trigger when CPU usage exceeds 85% for a sustained period, allowing temporary spikes from legitimate processes but flagging unusual activity.

### Bandwidth Usage Sensor *(NIST CSF: DE.AE)*

- **Importance:** Monitoring network traffic is crucial for detecting data exfiltration, brute-force attacks, or denial-of-service attempts (Cisco, 2023).
- **Thresholds:** Alerts are raised when traffic spikes exceed 150% of normal baseline levels, ensuring that security teams can react before a potential breach occurs.

### SQL Server Sensor (*MITRE: T1190; NIST CSF: DE.CM)*

- **Importance:** SQL databases are prime targets for injection attacks that compromise data integrity and allow unauthorized access (Red Gate, 2023).
- **Thresholds:** Query execution times exceeding 2 seconds may indicate database misuse or malicious attempts at database manipulation.

### HTTP Load Time Sensor (*MITRE: T1499; NIST CSF: DE.AE)*

- **Importance:** Increased web page load times can indicate DDoS attacks or server performance issues.
- **Thresholds:** Alerts activate if load times consistently exceed 5 seconds, maintaining optimal user experience and security.

### File Integrity Sensor *(MITRE: T1027; NIST CSF: DE.CM)*

- **Importance:** Unauthorized file changes can indicate malware activity, insider threats, or advanced persistent threats (APTs) (MITRE ATT&CK, 2023).
- **Thresholds:** Immediate alerts are generated for any detected modifications to monitored critical files, ensuring quick response.

### SSH Security Sensor *(MITRE: T1110; NIST CSF: DE.CM)*

- **Importance:** Brute-force login attempts on SSH servers can compromise confidentiality and system integrity (Linux Foundation, 2023).
- **Thresholds:** Alerts trigger after 5 consecutive failed SSH login attempts within 10 minutes, balancing security and usability.

### Antivirus Status Sensor *(MITRE: T1089; NIST CSF: PR.IP)*

- **Importance:** Ensuring antivirus software remains active and up-to-date is essential for preventing malware infections.
- **Thresholds:** Alerts trigger if antivirus definitions are outdated by more than 7 days or if the service becomes inactive, ensuring continued protection against evolving threats.

### Windows Event Log Sensor *(MITRE: T1078; NIST CSF: DE.CM)*

- **Importance:** Analyzing event logs helps identify unauthorized access attempts or system errors that could indicate security breaches (Microsoft, 2023).
- **Thresholds:** Alerts are raised for critical security-related errors, enabling swift investigation and response.

## Prioritizing Big Dog's Key Assets

I categorized Big Dog's assets into five Security Impact Levels (SILs) to prioritize cybersecurity efforts. By focusing on these key areas, I aligned security strategies with business-critical functions, safeguarded essential data, and reinforced operational stability.

### 1. Privacy:  Protecting Customer and Employee Data (Windows Workstations)

Big Dog's sales, marketing, and management workstations store sensitive customer data, internal communications, and employee records. Because of the potential for regulatory violations, reputational damage, and financial penalties in the event of a data breach, these workstations are classified as high SIL (CourseHero, 2023). Unauthorized access, malware infections, and data exfiltration are among the most pressing concerns. I monitored these endpoints for unusual login attempts, unauthorized data transfers, and suspicious file modifications to detect potential threats before they escalate.

### 2. Proprietary Information: Securing Intellectual Property (Linux Development Systems)

Big Dog's Linux servers house critical intellectual property (IP), including software code, product designs, and confidential research. A compromise of these systems could result in financial losses, or stolen trade secrets (CourseHero, 2023).To protect these high-SIL assets, monitoring was focused on File Integrity Sensors, and Network Traffic Analysis.

### 3. Administrative Systems: Safeguarding Core Servers and Databases

Big Dog relies on Windows Servers running SQL Databases and PRTG Network Monitoring. Since these systems are central to daily operations, an outage or security compromise could halt business entirely (CliffsNotes, 2023). I classified them as high-impact SIL because any disruption in these systems would severely affect business continuity, data integrity and service availability. To mitigate the risks, I implemented real-time monitoring of CPU, memory, and disk performance, Database integrity and unusual query pattern, Application uptime and security logs. Additionally, redundant systems and automated failover mechanisms are in place to prevent prolonged downtime.

### 4. Financial Data Systems: Protecting Transactions and Accounting Records

Financial and accounting systems must be secured to prevent fraud, unauthorized transactions, and financial data leaks. These systems are classified as medium-high SIL, given the potential for fraud, compliance violations, and monetary losses (CourseHero, 2023).
Monitoring recommendations include tracking access logs for financial records, identifying unusual transaction patterns and ensuring encryption and multi-factor authentication (MFA) for financial applications.

### 5. Network Perimeter: Securing Firewall and Web systems

Big Dog's firewall, routers, and web servers are the first line of defense against cyber threats. Since these assets control external access to internal resources, a security breach here could expose the entire network to attacks (CliffsNotes, 2023). A compromise in this area could lead to DDoS attacks affecting website availability and Network intrusion leading to lateral movement within the infrastructure. Our monitoring strategy includes firewall and Router Traffic Analysis (helps to detect external attack attempts) and Intrusion Detection (helps to identify unusual port scans or unauthorized access attempts).

## Recommendations

To effectively mitigate the identified cybersecurity risks, I have developed a comprehensive monitoring strategy that leverages PRTG Network Monitor alongside best security practices. My approach ensures real-time threat detection, proactive response, and continuous security improvements to safeguard Big Dog's critical infrastructure.

### 1. Establish Alerting and Incident Response Protocols *(NIST CSF: RS.RP; MITRE: T1070)*

- Custom alert triggers will notify the IT security team via email or SMS if abnormal activity is detected, such as a bandwidth spike, repeated failed login attempts, or unauthorized file modifications (Paessler, 2023).

- Defined escalation procedures will ensure alerts are addressed promptly, minimizing security risks. Each alert should trigger an incident response playbook that outlines who is responsible for investigating and resolving the issue.
  By having well-documented response steps, we reduce reaction time and ensure no security alert goes unnoticed.

### 2. Implement Segmented Network Architecture *(NIST CSF: PR.AC)*

- Network segmentation limits the impact of a security breach by isolating critical systems from general traffic (Cisco, 2023).
- Enforce VLANs to separate sensitive assets from less critical areas of the Big Dog's network.

### 3. Enforce Strong Access Controls and Multi-Factor Authentication *(NIST CSF: PR.AC-7)*

- Weak authentication practices are a common entry point for attackers seeking unauthorized access to sensitive systems (Microsoft, 2023).
- Action: Implement MFA for all privileged accounts and require regular password updates.

### 4. Apply Regular Patch Management *(NIST CSF: PR.IP-12)*

- Unpatched software vulnerabilities are a major attack vector, allowing attackers to exploit outdated systems
- Action: Automate patch deployment for Windows, Linux, and database servers to eliminate known vulnerabilities.

### 5. Routine Review of Security Logs and Indicators of Compromise (IoCs) *(NIST CSF: DE.AE-5; MITRE: T1005)*

While automated alerts provide critical first-line defenses, regular log analysis and manual security reviews add an extra layer of vigilance.

Periodic log reviews will be conducted to analyze system and network logs (e.g, firewall logs, Windows Event Logs, and database access logs) to detect subtle attack patterns that may not trigger automated alerts.

- IoC monitoring will help identify suspicious activities, such as unusual access patterns, network traffic spikes, or unauthorized file access.
- After-hours access audits will detect abnormal logins to sensitive data, helping prevent potential insider threats or slow-moving data exfiltration attempts.
  By combining automated threat detection with human-driven analysis, we strengthen Big Dog's ability to detect and respond to evolving threats (ManageEngine, 2023).

### 6. Enhance Security Awareness Training *(NIST CSF: PR.AT)*

Employee awareness is a key factor in reducing human-related security breaches, such as phishing attacks and credential theft (NIST, 2023).

- Conduct regular training on recognizing social engineering attacks, safe internet practices, and secure login procedures.

## Conclusion

This enterprise-aligned monitoring framework, driven by PRTG and supported by NIST and MITRE standards, positions Big Dog to proactively defend against evolving threats. Prioritized asset protection, aligned thresholds, and detection techniques offer real-time insights and timely mitigation. Continued executive support and iterative improvements will ensure resilience against advanced persistent threats, insider risks, and operational disruption.

## References

1. Cisco. (2023). *Enterprise network security best practices.* Retrieved from https://www.cisco.com/c/en/us/solutions/enterprise-networks/index.html

2. CIS. (2023). *Critical security controls v8.* Retrieved from https://www.cisecurity.org/controls/

3. CliffsNotes. (2023). *Security monitoring and network defense strategies.* Retrieved from https://www.cliffsnotes.com

4. Dark Reading. (2023). *Threat hunting and incident response best practices.* Retrieved from https://www.darkreading.com

5. Linux Foundation. (2023). *Best practices for securing Linux servers.* Retrieved from https://www.linuxfoundation.org/resources/publications/

6. ManageEngine. (2023). *Log management and security monitoring.* Retrieved from https://www.manageengine.com

7. Microsoft. (2023). *Windows security and event log analysis.* Retrieved from https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-log-security

8. Microsoft. (2023). *SQL server security best practices.* Retrieved from https://docs.microsoft.com/en-us/sql/

9. Microsoft. (2023). *IIS security best practices.* Retrieved from https://docs.microsoft.com/en-us/iis/

10. MITRE ATT&CK. (2023). *Cyber threat intelligence framework.* Retrieved from https://attack.mitre.org

11. NIST. (2023). *Framework for improving critical infrastructure cybersecurity.* National Institute of Standards and Technology. Retrieved from https://www.nist.gov/cyberframework

12. NIST SP 800-61. (2023). *Computer security incident handling guide.* Retrieved from https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

13. Paessler AG. (2023). *Microsoft server monitoring with PRTG.* Retrieved from https://www.paessler.com/microsoft_server_monitoring

14. Paessler AG. (2023). *PRTG monitoring for Linux and Windows systems.* Retrieved from https://www.paessler.com/linux_network_monitoring

15. Red Gate. (2023). *SQL server security best practices.* Retrieved from https://www.red-gate.com

16. SANS Institute. (2023). *Intrusion detection and prevention system fundamentals.* Retrieved from https://www.sans.org/white-papers/

# Appendix

Video presentation url: [Cybersecurity Monitoring Strategy Overview 🔒]

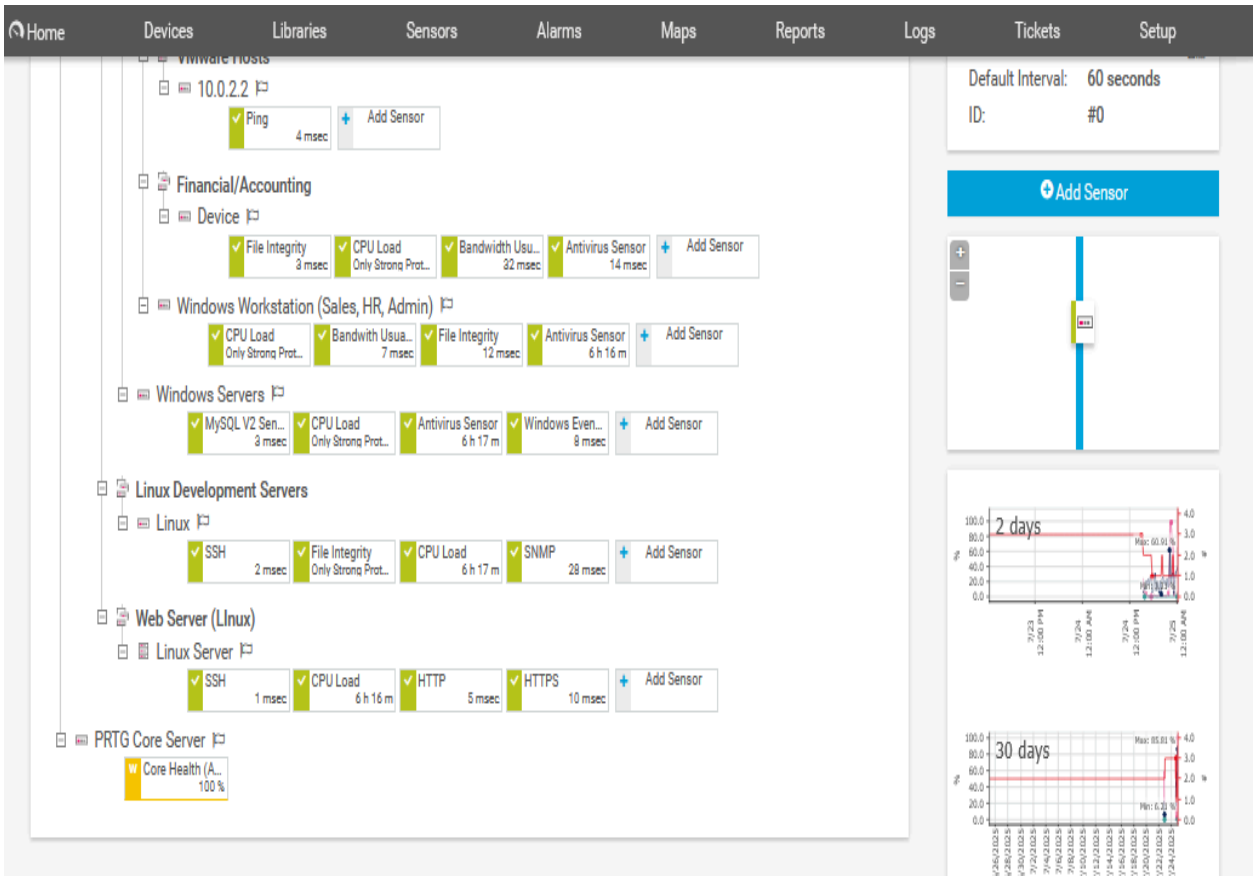


Image: This dashboard provides a visual representation of the sensor deployment strategy across Big Dog's network. Devices are categorized by function, such as Financial Systems, Workstations, Servers, and Development Environments, and assigned relevant PRTG sensors for real-time monitoring of system health, bandwidth, antivirus status, database performance, and file integrity. This structure supports targeted visibility and aligns with NIST CSF's "Detect" and "Protect" functions for critical assets