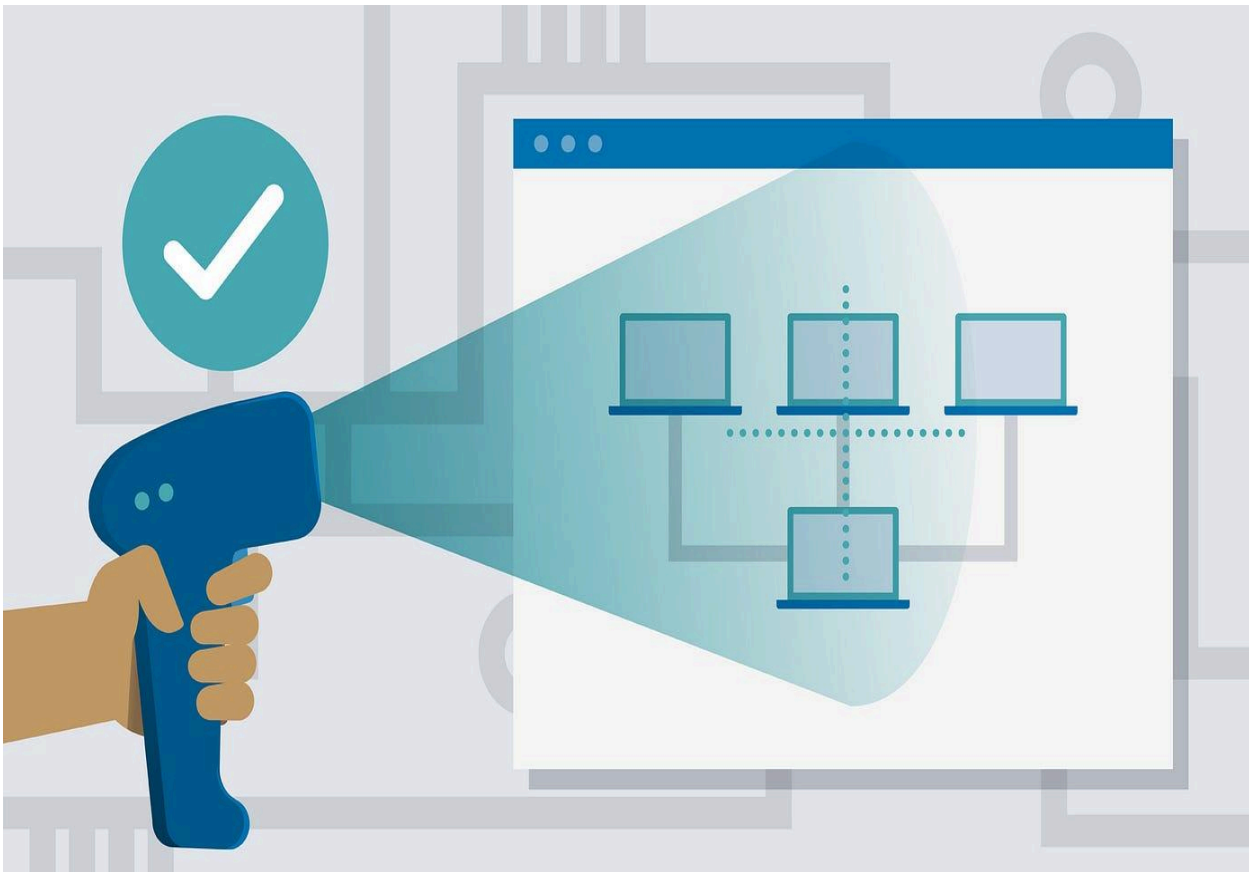
Cat Scan II Big Dog



By: Mahad Mohamood

Executive summary

In this report, we present a security monitoring solution for Big Dog's mixed Windows and Linux environment using PRTG. We identified various sensors to monitor critical assets, including Windows Server, Linux systems, Windows workstations, and Kali systems. Based on security Impact Levels (SILs) for Privacy (P), Proprietary (IP), and Security Management (SM) data, we highlight the SILs and recommend specific sensors and thresholds for effective security monitoring and incident detection. You can view an video-overview of the report here

Table of sensors

Sensor	Description	System	IoCs Associated	Rationale	Priority	Thresholds /Assumptions
HTTP Load Time	Monitors how fast websites load on Linux servers	Linux	Slow load times Unusual HTTP error codes (like 404) Unexpected redirects	Ensures websites load quickly for developers	Medium to High Slow load times can affect development	Alerts for slow loads above normal baseline (high threshold) Alerts for sudden increases in errors (low threshold) to catch potential issues promptly
MySQL Database Query Sensor	Monitors the speed and efficiency of MySQL database queries on Linux	Linux	Slow query times Errors in SQL syntax or permissions	Critical for ensuring efficient access to SQL databases hosting important business data	High Delays in database queries can impact operations and decision-making	Alerts for queries taking longer than usual (high threshold) Alerts for SQL errors (low threshold) to maintain database performance

						and data integrity
SSH Sensor	Monitors SSH (Secure Shell) connections on Linux servers	Linux	Unauthorized access attempts Unusual login times or locations	Essential for detecting and preventing unauthorized access to Linux systems	High Protects sensitive company data and system integrity	Alerts for multiple failed login attempts (high threshold) Alerts for SSH sessions outside normal hours (low threshold) to mitigate security risks effectively
Antivirus Status Sensor	Monitors the status of antivirus software on Linux servers, Windows workstations, and servers	All	Outdated antivirus definitions Disabled antivirus protection	Essential for detecting and mitigating malware threats across both Linux and Windows systems	High Protects against potential malware infections and data breaches on critical operating systems	Alerts for outdated antivirus definitions (high threshold) Alerts for disabled antivirus protection (low threshold) to ensure comprehensive security monitoring and response
File Sensor	Monitors changes and access to files on Linux systems	Linux	Unauthorized file access Unexpected file modifications or deletions	Critical for detecting potential data breaches or unauthorized access to sensitive files on Linux systems	High Protects confidential data and ensures compliance with security policies	Alerts for unauthorized access attempts (high threshold) Alerts for significant changes to critical files (low threshold) to maintain

						data integrity and security
Windows Event Log Sensor	Monitors events logged by Windows on a Windows 11 system	Windows 11	Security breaches System errors Application crashes	Essential for detecting and responding to security incidents, system failures, and application issues on Windows 11	High Helps maintain system stability, security, and operational continuity	Alerts for unauthorized access attempts or system compromises (high threshold) Alerts for system errors or application crashes (low threshold) to ensure prompt response and mitigation of potential risks
Bandwidth Usage Sensor	Monitors network bandwidth usage on both Linux and Windows systems.	All	Unusually high bandwidth consumption Potential network abuse or malicious activity.	Critical for managing network performance , detecting anomalies, and ensuring optimal resource allocation on both Linux and Windows platforms.	High Excessive bandwidth usage can impact network performance and indicate security threats	Alerts for bandwidth usage exceeding normal thresholds (high threshold) to prevent network congestion and potential security breaches. Consistently monitoring helps in adjusting network resources efficiently (low threshold) based on usage patterns and demands.

Discussion Section:

According to Paessler, “PRTG is a unified monitoring tool that can monitor almost any object that has an IP address. It consists of the PRTG core server and one or more probes. The PRTG core server is responsible for configuration, data management, PRTG web server, and more. Probes collect data and monitor processes on devices via sensors.” This section explains the connections between the PRTG sensors, IoCs and thresholds.

HTTP Load Time Sensor:

- Sensor significance: This sensor checks how quickly web applications on Linux systems load, focusing on the development environment for proprietary IP.

- IoCs: Slow load times and unusual HTTP errors can signal server issues or malicious activity.

- Thresholds: Alerts trigger if load times exceed the normal baseline or if HTTP errors increase, allowing for quick identification of performance issues.

MySQL Database Query Sensor:

- Sensor significance: This sensor ensures fast access to SQL databases, vital for the company’s operations and decision-making.

- IoCs: Slow query times and SQL syntax errors can harm database performance and data accuracy.

- Thresholds: Alerts are set for slow queries and SQL errors, keeping database performance optimal.

SSH Sensor:

- Sensor significance: Monitors SSH connections on Linux servers to spot unauthorized access attempts.

- IoCs: Multiple failed login attempts and unusual login times or locations suggest

potential unauthorized access.

- Thresholds: High threshold for failed login attempts and low threshold for logins at odd hours enhance security.

Antivirus Status Sensor:

- Sensor significance: Tracks antivirus status on all systems to ensure they are protected against malware.

- IoCs: Outdated antivirus definitions and disabled protection raise the risk of malware infections.

- Thresholds: Alerts for outdated definitions and disabled protection ensure robust malware defense.

File Sensor:

- Sensor significance: Watches file access and changes on Linux systems, crucial for safeguarding sensitive data.

- IoCs: Unauthorized access and unexpected file modifications can indicate data breaches.

- Thresholds: High threshold for unauthorized access attempts and low threshold for changes to critical files maintain data integrity.

Windows Event Log Sensor:

- Sensor significance: Keeps an eye on Windows events to catch security breaches and system/application errors.

- IoCs: Critical security events and system errors can affect system stability and security.

- Thresholds: High threshold for security events and low threshold for system

errors ensure a quick response.

Bandwidth Usage Sensor:

- Sensor significance: Monitors network bandwidth usage across all systems to manage performance and detect anomalies.

- IoCs: High bandwidth usage and network abuse can signal potential security threats.

- Thresholds: Alerts for bandwidth usage above normal levels prevent network congestion and security breaches.

Prioritization of Security Impact Levels (SILs):

According to NIST, SIL [security impact level] is “the assessed potential impact resulting from a compromise of the confidentiality, integrity, or availability of an information type, expressed as a value of low, moderate, or high.” Below I will outline the process that we followed for identifying the SIL’s and some of the interesting discoveries.

STEP 1: List and categorize all assets within the network or system.

Windows Server, runs:

- SQL database
- IIS web server
- PRTG Network Monitor

Linux:

- Used by developers to create important proprietary intellectual property (IP) for the company

Windows workstations:

- Sales
- Marketing
- Management functions

Kali

- Test systems

- IT systems

STEP 2: Determine the types of data each asset handles and rank them based on their importance to the organization.

The heads of the company have stated that all company information falls within the following classifications:

- Privacy (P)
- Proprietary (IP),
- Financial (F)
- Admin (A)
- Security mManagement (SM)
- Systems (S)

Also, they have further ranked the importance of each class of information from most important to least important as follows:

- Privacy (P)
- Proprietary (IP)
- Admin (A)
- Financial/accounting (F)
- Security Management (SM)
- Systems (S)

When we map the assets onto the ranking of data-types we get the following table:

Rank	Asset	Data type
1	Windows Server (SQL)	Privacy (P)
2	Linux Systems	Proprietary (IP)
3	Windows Workstations	Admin (A)

4	Windows Server (IIS)	Financial (F)
5	PRTG Network Monitor	Security Management (SM)
6	Kali Systems	Systems (S)

STEP 3: Construct the CIA matrix for each asset and based on the CIA matrix, assign Security Impact Levels (SILs) to each asset or data type.

Rank	Asset	Data type	Confidentiality	Integrity	Availability	Explanation	SIL value
1	Windows Server (SQL)	Privacy (P)	High	High	High	Contains sensitive financial and proprietary data (SQL database). Access must be restricted to authorized personnel.	SIL 1
2	Linux Systems	Proprietary (IP)	High	Medium	Medium	Stores proprietary intellectual property (IP) crucial for a company's competitive advantage. Access must be controlled to prevent leaks.	SIL 2
3	Windows Workstations	Admin (A)	Medium	Low	Medium	Handles administrative functions with	SIL 3

						medium impact on confidentiality and availability.	
4	Windows Server (IIS)	Financial (F)	Low	Low	High	Hosts financial applications with low confidentiality impact but high availability requirements.	SIL 4
5	PRTG Network Monitor	Security Managem ent (SM)	Low	Low	Hight	Manages security monitoring and management (SM), critical for network security but low impact on confidentiality and integrity	SIL 5
6	Kali Systems	Systems (S)	Low	Low	Low	Used for testing and IT systems, minimal impact on CIA principles due to non-critical data.	SIL 6

Since we received a list of PRTG sensor, when we map the list of provided PRTG sensors onto the assets and data types we get the following table :

Rank	Asset	Date type	PRTG Sensors
1	Windows Server (SQL)	Privacy (P)	MySQL Database Query Sensor
2	Linux Systems	Proprietary (IP)	HTTP Load Time, MySQL Database Query Sensor, SSH Sensor, File Sensor, Bandwidth Usage Sensor
3	Windows Workstations	Admin (A)	Antivirus Status Sensor, Bandwidth Usage Sensor
4	Windows Server (IIS)	Financial (F)	Antivirus Status Sensor, Bandwidth Usage Sensor

5	Windows Server (PRTG monitor)	Security Management (SM)	Windows Event Log Sensor, Bandwidth Usage Sensor
6	Kali Systems	Systems (S)	Antivirus Status Sensor, Bandwidth Usage Sensor

At this point we run into some interesting inconsistencies :

1. The provided list of assets includes a Windows Server with SQL database. However, it is unusual that the sensor table associates the 'MySQL Database Query Sensor' with a Linux system, despite the Linux system not being identified as having a SQL database in the assets list.

2. When a Windows Server has a SQL database, that is typically identified as MS SQL Server, but this was not identified in the assets.

3. Since the windows server was identified as having a SQL database, then shouldn't there be an MS SQL sensor ?

Recommendations

To further enhance Big Dog's security, we recommend the following additional measures:

Enhanced Network Segmentation:

- Industry Best Practice: According to Frankel (2022), "Network segmentation divides a network into smaller subnetworks to enhance security, control access, improve performance, simplify management, and aid regulatory compliance by isolating critical systems and data flows." Segmenting the network to isolate sensitive systems and data reduces the attack surface and limits attackers' movement within the network.

- Implementation: Create separate network segments for critical servers, development environments, and general workstations.

Regular Security Audits:

- Industry Best Practice: According to intuit mailchimp, “an IT security audit is a comprehensive evaluation of an organization's security posture that encompasses a wide range of aspects, including policies, controls, processes, and overall infrastructure.” Conducting regular security audits and vulnerability assessments helps identify and address potential risks.

- Implementation: Schedule periodic audits using both automated tools and manual reviews to ensure thorough security checks.

Employee Training and Awareness Programs:

- Industry Best Practice: According to cybsafe, “security awareness training is the process of educating people to understand, identify, and avoid cyber threats. The ultimate goal is to prevent or mitigate harm—to both the organization and its stakeholders—and reduce human cyber risk.” Educating employees on security best practices and phishing awareness reduces the risk of social engineering attacks.

- Implementation: Implement regular training sessions and simulated phishing exercises to improve employee vigilance.

Multi-Factor Authentication (MFA):

- Industry Best Practice: According to Yasar “Multi Factor authentication (MFA) is an account login process that requires multiple methods of authentication from independent categories of credentials to verify a user's identity for a login or other transaction. Multi Factor authentication combines two or more independent credentials -- what the user knows, such as a password; what the user has, such as a security token”. Enforcing MFA for all critical systems adds an extra layer of security, making unauthorized access more difficult.

- Implementation: Deploy MFA solutions for accessing critical servers, databases, and administrative interfaces.

Advanced Threat Detection Solutions:

- Industry Best Practice: Enhances the ability to detect and respond to sophisticated threats by using advanced threat detection and response solutions such as :
    - Endpoint Detection and Response (EDR)
        - According to Palo Alto networks, “endpoint detection and response (EDR) is a technology platform that detects and investigates threats on endpoints. It helps security teams find suspicious endpoint activity to eliminate threats quickly and minimize the impact of an attack. EDR tools typically provide detection, investigation, threat hunting, and response capabilities.”
    - Security Information and Event Management (SIEM)
        - According to IMB, “Security information and event management, or SIEM, is a security solution that helps organizations recognize and address potential security threats and vulnerabilities before they have a chance to disrupt business operations.”
- Implementation: Integrate EDR and SIEM solutions with the existing PRTG monitoring system for comprehensive threat visibility and response capabilities.

References

1. CybSafe. (2023, October 24). *7 reasons why security awareness training is important in 2023*. https://www.cybsafe.com/blog/7-reasons-why-security-awareness-training-is-important/

2. Editor, C. C. (n.d.). *Impact value - glossary: CSRC*. CSRC Content Editor. https://csrc.nist.gov/glossary/term/impact_value

3. Frankel, A. (2022, September 25). *Network segmentation: All you need to know about its benefits*. Zero Networks Blog. https://zeronetworks.com/blog/network-segmentation-all-you-need-to-know

4. *PRTG Manual: Introduction: Monitoring with PRTG*. Paessler. (n.d.). https://www.paessler.com/manuals/prtg/introduction_monitoring_with_prtg

5. *Security audits: Best practices to ensure data protection*. Mailchimp. (n.d.). https://mailchimp.com/resources/security-audit/

6. *What is endpoint detection and response (EDR)?*. Palo Alto Networks. (n.d.). https://www.paloaltonetworks.com/cyberpedia/what-is-endpoint-detection-and-response-edr

7. *What is Siem?*. IBM. (2023, June 23). https://www.ibm.com/topics/siem

8. Yasar, K., & Shacklett, M. E. (2023, October 2). *What is multifactor authentication?: Definition from TechTarget*. Security. https://www.techtarget.com/searchsecurity/definition/multifactor-authentication-MFA