# Cat Scan II Big Dog

## Executive Summary:

This report contains the findings and recommendations of Big Dog's cybersecurity assessment. The purpose of the assessment was  to find vulnerabilities and risks/threats in the company's systems. The report explains key vulnerabilities, associated risks, indicative indicators of compromise (IoC), alerts and thresholds, and references industry standards to help businesses improve their security. The study considered the five highest levels of security impact. (SIL) and  sensors and monitoring levels offered. Examples of these are intrusion detection and prevention systems (IDS/IPS), network traffic analyzers, SIEM systems, and endpoint security solutions. Thresholds were determined based on the potential impact on data and system confidentiality, integrity and availability.

## Discussion:

1. Network Infrastructure: Assess the firewall configurations, implement the principle of least privilege, and regularly review and update firewall rules based on CIS Benchmarks.
2. Windows-based Systems: Establish a regular patch management process to ensure all software and systems are up to date, significantly reducing the likelihood of known vulnerabilities being exploited.
3. Authentication Mechanisms: Implement multi-factor authentication (MFA) for all critical systems and privileged accounts to reduce the risk of unauthorized access, following the guidelines in NIST SP 800-63B.
4. Network Traffic and Security Events: Deploy a Security Information and Event Management (SIEM) system to centralized log management, automate threat detection, and enable real-time incident response.
5. Linux System and MYSQL Database: Apply secure configurations to the Linux system, including proper access controls, regular patching, and monitoring the MYSQL database for any suspicious activities.

**Table of Devices:**

| Device | Sensor | Thresholds | SIL | Notes |
|---|---|---|---|---|
| Firewall | Firewall Logging | Log anomalies and rule changes | 1 | Detect unauthorized access attempts |
| Windows Server | Patch Management | Outdated software versions | 2 | Identify systems with known vulnerabilities |
| Windows Workstation | Authentication and MFA | Failed login attempts | 3 | Detect potential unauthorized access |
| Network Traffic | Network Traffic Analyzer | Unusual patterns and anomalies | 4 | Identify suspicious network activities |
| Linux System | Database Monitoring | Abnormal database activities | 5 | Detect unauthorized access or data exfiltration |

The top five Security Impact Levels (SILs) identified during the assessment are as follows:

SIL 1 - Poor firewall configurations and access control measures.

SIL 2 - Outdated software versions on Windows-based systems.

SIL 3 - Weak authentication components for user accounts.

SIL 4 - Lack of monitoring for network traffic and security events.

SIL 5 - restricted security measures for the Linux system hosting the MYSQL database.

**Recommendation Section:**

1. To enhance the security of your systems, we recommend the following best practices:
2. Follow the principle of least privilege and regularly update firewall rules based on CIS Benchmarks.
3. Implement a regular patch management process for all systems, ensuring up-to-date software versions.
4. Enable multi-factor authentication (MFA) for critical systems and privileged accounts.
5. Deploy a Security Information and Event Management (SIEM) system to centralize log management and automate threat detection.
6. Apply secure configurations to the Linux system, including access controls and regular patching.
7. These recommendations align with industry standards and frameworks such as NIST SP 800-40, NIST SP 800-63B, CIS Benchmarks, and the use of SIEM systems as recommended by Gartner
8. Conduct regular security awareness training for employees to educate them about common cybersecurity threats, phishing attacks, and best practices for safe computing

**Conclusion:**

In conclusion, the Cat Scan II assessment has identified vulnerabilities and risks in the systems used by Big Dog. By implementing the recommended measures and following industry best practices, you can enhance the security of your systems and mitigate potential risks effectively. Regular monitoring and maintenance, combined with proactive security measures, will help protect your business from cyber threats.

Sincerely,

Elyas Moallin

**Video of presentation**

*https://vimeo.com/872055650?share=copy#t=0*

**Citiations:**


*Compass. Welcome to Compass. (2023, October 1).* *https://cyber.compass.lighthouselabs.ca/p/2/projects/risks-report*

Splunk. (2023, April 18). *High CPU utilization alert*. Splunk Lantern. https://lantern.splunk.com/Splunk_Platform/UCE/IT_Modernization/Investigation_and_Troubleshooting/Recovering_lost_visibility_of_IT_infrastructure/High_CPU_utilization_alert#:~:text=High%20CPU%20utilization%20can%20be

Souppaya, M., & Scarfone, K. (2022, April 6). *Guide to enterprise patch management planning: Preventive maintenance for technology*. CSRC. https://csrc.nist.gov/pubs/sp/800/40/r4/final

*CIS BenchmarksTM*. CIS. (n.d.).

https://www.cisecurity.org/cis-benchmarks