Cat Scan II Big Dog

Table of Contents

Executive Summary

This report presents the findings and recommendations for Big Dog organization regarding implementing specific sensors to monitor critical systems. The analysis prioritizes sensors according to their Security Impact Level (SIL), highlighting the potential risks, vulnerabilities, and threats the organization may encounter. The five highest-priority sensors identified are HTTP Load Time, MySQL Database Query Sensor, SSH Sensor, Antivirus Status Sensor, and Windows Event Log Sensor. Each sensor is monitored with defined thresholds to detect potential security incidents promptly. The recommendations focus on strengthening Big Dog's security posture in alignment with industry best practices.

Sensors

Sensor	Description	System	IoC Associated	Rationale	Priority	Threshold
HTTP Load Time	Monitors the time a webpage loads	Linux	Malicious redirects, DDoS Attacks, Content Injection	Changes in load time can indicate performance issues tied to security breaches (NIST, 2021)	Medium	Changes of 20% over the average load. It is assumed to have a low impact on Confidentiality but a higher impact on Availability.
MySQL Database Query Sensor	Monitors database queries for anomalies	Linux	SQL Injection, Data Exfiltration	Links to MITRA ATT&CK techniques for database attacks (MITRE 2023)	High	Monitor for high and low conditions to detect anomalies.
Antivirus Status Sensor	Monitors antivirus health and status	All	Malware Infection, Outdated definitions	Aligns with industry best practices for endpoint security (CIS, 2023)	High	Monitor for high and low conditions to ensure antivirus software is up to date.
Windows Event Log Sensor	Monitor Windows Event Logs for	Windows	Unauthorized Access, System	Important for detecting	High	Monitor high and low conditions to

	suspicious activity.		Integrity Violations.	insider threats (NIST, 2021)		ensure system integrity.
Bandwidth Usage Sensor	Monitors network bandwidth for unusual spikes.	All	Data Exfiltration, DDoS Attacks	Tied to NIST guidelines on network security (NIST, 2021)	Medium	Alerts for bandwidth usage exceeding 80% capacity.

Discussion

These sensors play a critical role in detecting specific Indicators of Compromise (IoCs) that are closely tied to vulnerabilities and risks.

- HTTP Load Time: Anomalies in load time could indicate a Distributed Denial of Service (DDoS) attack which is a malicious attempt to disrupt the functionality of a targeted server by overwhelming it with internet traffic. Given that the web presence of Big Dog is limited, a medium priority is assigned, reflecting the lower impact on confidentiality but recognizing the potential risk to availability (Akram et al. 2018)
  This sensor is assigned a medium priority as it is assumed to have a relatively low impact on Confidentiality.
- MySQL Database Query Sensor: By monitoring database queries, this sensor helps identify attempts at SQL injection, which can lead to significant data breaches (MITRE, 2023). Due to the severe implications of database compromise, this sensor is prioritized as high, emphasizing the need for stringent monitoring of database activity.
- SSH Sensor: This sensor tracks SSH login attempts and active sessions, providing insights into potential unauthorized access. Monitoring SSH access is crucial because improper use can lead to significant security breaches (NIST, 2021). Given its importance in maintaining system integrity, a high priority is warranted.
- Antivirus Status Sensor: Monitoring the health and status of antivirus software is essential in ensuring that endpoints are protected against malware. As noted by the Center for Internet Security (CIS, 2023), outdated antivirus solutions significantly increase the risk of infection. Thus, a medium priority is assigned to this sensor to ensure antivirus measures are effective.
- Windows Event Log Sensor: This sensor plays a critical role in identifying unauthorized access and potential insider threats through the analysis of Windows event logs. As indicated by NIST guidelines, monitoring system logs is vital for detecting anomalies (NIST, 2021). Given the potential consequences of insider threats, this sensor is prioritized as high.
- Bandwidth Usage Sensor: Unusual spikes in bandwidth usage can indicate data exfiltration attempts or ongoing DDoS attacks (NIST, 2021). While this sensor has a

medium priority, its ability to signal potential security incidents is important for overall network security.

Prioritizing these sensors reflects their critical roles in safeguarding Big Dog's assets and responding to potential threats effectively. Each sensor's specific focus on Indicators of Compromise (IoCs) ties directly into the broader cybersecurity framework, emphasizing the importance of comprehensive monitoring in today's threat landscape.

Recommendations

To enhance the security posture of the Big Dog organization, several strategic recommendations are proposed. These recommendations focus on improving monitoring capabilities, employee training, and overall security measures, aligning with industry best practices.

1. Implement Intrusion Detection Systems (IDS**)**: Deploying an IDS can significantly bolster the organization's ability to detect and respond to threats in real-time. IDS solutions such as Snort or Suricata provide network traffic analysis and can alert administrators to suspicious activities (SANS, 2023). This is particularly important as cyber threats become increasingly sophisticated and prevalent. An IDS would complement existing sensors, providing an additional layer of defence against potential intrusions.
2. Conduct Regular Security Audits: Routine security audits are essential for assessing the effectiveness of current security measures and ensuring compliance with industry standards (NIST, 2021). These audits can identify vulnerabilities that may have emerged since the last assessment, allowing for timely remediation. Organizations that engage in regular audits are better equipped to address gaps in their security posture and adapt to evolving threats (CIS, 2023).
3. Enhance User Training and Awareness Programs: Human error remains a significant factor in security breaches. Establishing comprehensive training programs that educate employees about cybersecurity risks and safe practices is crucial. Programs should include phishing awareness, password management, and safe browsing habits. According to the Cybersecurity and Infrastructure Security Agency (CISA), regular training can reduce the likelihood of successful attacks (CISA, 2023). Creating a culture of security awareness empowers employees to act as the first line of defence against cyber threats.
4. Implement Multi-Factor Authentication (MFA): MFA adds an essential layer of security by requiring multiple forms of verification before granting access to critical systems. This practice can dramatically reduce the risk of unauthorized access, particularly in environments where remote access is common (NIST, 2021). Implementing MFA for sensitive systems and accounts is a widely recognized best practice and aligns with the latest NIST guidelines on identity management.
5. Adopt Endpoint Detection and Response (EDR) Solutions: Integrating EDR solutions can enhance the organization's capability to monitor, detect, and respond to threats on endpoints. EDR tools continuously monitor endpoint activity and provide advanced

analytics to identify potential threats (MITRE, 2023). These solutions are effective in responding to sophisticated attacks that may bypass traditional antivirus solutions, enabling organizations to react swiftly to security incidents.

6. Establish an Incident Response Plan (IRP): Developing a comprehensive Incident Response Plan (IRP) is crucial for ensuring a swift and coordinated response to security incidents. The plan should outline roles, responsibilities, and procedures for identifying, containing, and eradicating threats (CIS, 2023). Regularly updating and practicing the IRP will ensure that all stakeholders are prepared to act effectively in the event of a security breach.

These recommendations aim to create a robust security framework for Big Dog, ensuring that the organization can effectively monitor and respond to evolving threats while fostering a culture of cybersecurity awareness.

References

Akram, U., Asim, M., & Shah, A. (2018). A survey of DDoS attack and defence mechanisms. *Journal of Network and Computer Applications, 126*, 101-124. https://doi.org/10.1016/j.jnca.2018.10.006

Cybersecurity & Infrastructure Security Agency (CISA). (2023). *Cybersecurity awareness training*. https://www.cisa.gov/cybersecurity-awareness-training

Center for Internet Security (CIS). (2023). *CIS controls version 8*. https://www.cisecurity.org/controls/

MITRE. (2023). *MITRE ATT&CK®*. https://attack.mitre.org/

National Institute of Standards and Technology (NIST). (2021). *Framework for improving critical infrastructure cybersecurity*. https://www.nist.gov/cyberframework

SANS Institute. (2023). *Intrusion detection systems: A comprehensive guide*. https://www.sans.org/white-papers/intrusion-detection-systems-guide/