# Cat Scan II Big Dog

# Risk & Vulnerabilities Report

**Zehra Nur Ozer**

**May 2024**

# Video Presentation

The link for the video presentation is below.

https://drive.google.com/file/d/175ueZ6yvRQYhe3iT3k9dlK0WH13RZ5MM/view?usp=drive_link

# Executive summary

This report presents the findings of evaluating various sensors within Big Dog's network environment. The sensors that have been analyzed help us prioritize assets, vulnerabilities, treatments, and risks. After describing the sensors and their impacts, our assessment included Indicators of Compromise (IoCs) to help better understand the compromises. We have identified the Security Impact Levels (SILs) based on associated risks and vulnerabilities. A rationale was provided for each IoC, with a priority (SIL) set for each sensor. All findings and recommendations have been provided in the last section.

# Table of Sensors

| Sensor | Description | System | IoCs | Rationale | Priority | Thresholds/Assumptions |
|---|---|---|---|---|---|---|
| HTTP Load Time | The time it takes to download and display an HTTP request (pingdomcom) | Win server | It could be increasing outgoing network traffic. | Unexpected changes in load time anomalies could be essential | Medium | 20% warning<br>25% high<br>30% critical |
| HTTP Load Time | A queue of requests in the storage layer that leads to increased latency (site24x7com) | Linux | High latency, slow response time or unexplained delays might be a sign of DDoS attack | Considering Linux as the production system, it is essential to optimize website performance | High | CVE-2018-17199<br>*Figure 1 |
| MySQL Database Query Sensor | Monitors execution time of MySQL database queries | Win server | Abnormal behaviour, like increased database read volume, could be brute force attacks or unauthorized access attempts. | Indicates a compromise or a significant risk to data | High | Abnormal query patterns or a high volume of queries indicate potential compromise.<br>Exp. Setting a warning if execution time exceeds 2 seconds.<br>*Figure 2 |
| MSSQL Database Query Sensor | Tracks the execution time | Win server/Linux | Abnormal behaviour, like increased database read volume, could be brute force attacks or unauthorized access attempts. | Indicates a compromise or a significant risk to data | High | Abnormal query patterns or a high volume of queries indicate potential compromise.<br>Exp. Setting a warning if execution time exceeds 2 seconds. (paessler) |
| SSH Sensor | Detects and logs secure shell access attempts and activity. | All | Unusual session durations, unauthorized access, or configuration changes might | SSH is a common target for brute force attacks and unauthorized access attempts. | Medium | Multiple attempts and fails to log in, and the configuration could be as<br>Upper Error Limit<br>Upper Warning Limit<br>Lower Warning Limit |

| Sensor | Description | System | IoCs | Rationale | Priority | Thresholds/Assumptions |
|---|---|---|---|---|---|---|
| | | | indicate a malware attack. | Monitoring SSH activity can help detect and prevent such security incidents. (appviewxcom) | | Lower Error Limit (paessler) *Figure 3 |
| File Sensor | Monitors changes and access to files within a system. | Win server/Linux. | Many requests for the same file or unauthorized access, data exfiltration | File system monitoring helps to detect suspicious file activities and malware infections. | Medium | Unauthorized file modifications or access events may signify insider threats or compromised credentials, such as file existence, size, modification time, or file count. An SSH brute force attack is a hacking technique that involves repeatedly trying different username and password combinations until the attacker gains access to the remote server. (trendmicro) |
| Windows Event Log Sensor | Captures Windows event log entries | Win server | Access control changes, such as modifications to file permissions or registry settings | It captures and analyzes event log entries, providing valuable insights into system events, errors, and potential security threats. | High | It may be configured for events indicating potential security breaches, such as failed authentication attempts. |
| Windows Event Log Sensor | Captures Windows event log entries | Windows1 | Unusual sign-in attempts (microsoftcom) | It monitors Windows event logs on specified systems for security events and anomalies. | High | For example, trigger an alert if any events with a severity level of "Error" or "Critical" are detected in the event log. |
| Bandwidth Usage Sensor | Measures network bandwidth consumption | All | Data exfiltration, sudden increase in bandwidth usage indicates DDoS attacks | The Bandwidth Usage Sensor is essential for optimizing network performance and managing bandwidth resources effectively. | Medium | Anomalies in bandwidth usage pattern |

# CVE-2018-17199 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

## Description

In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

Figure 1 – CVE-2018-17199 Description from NIST

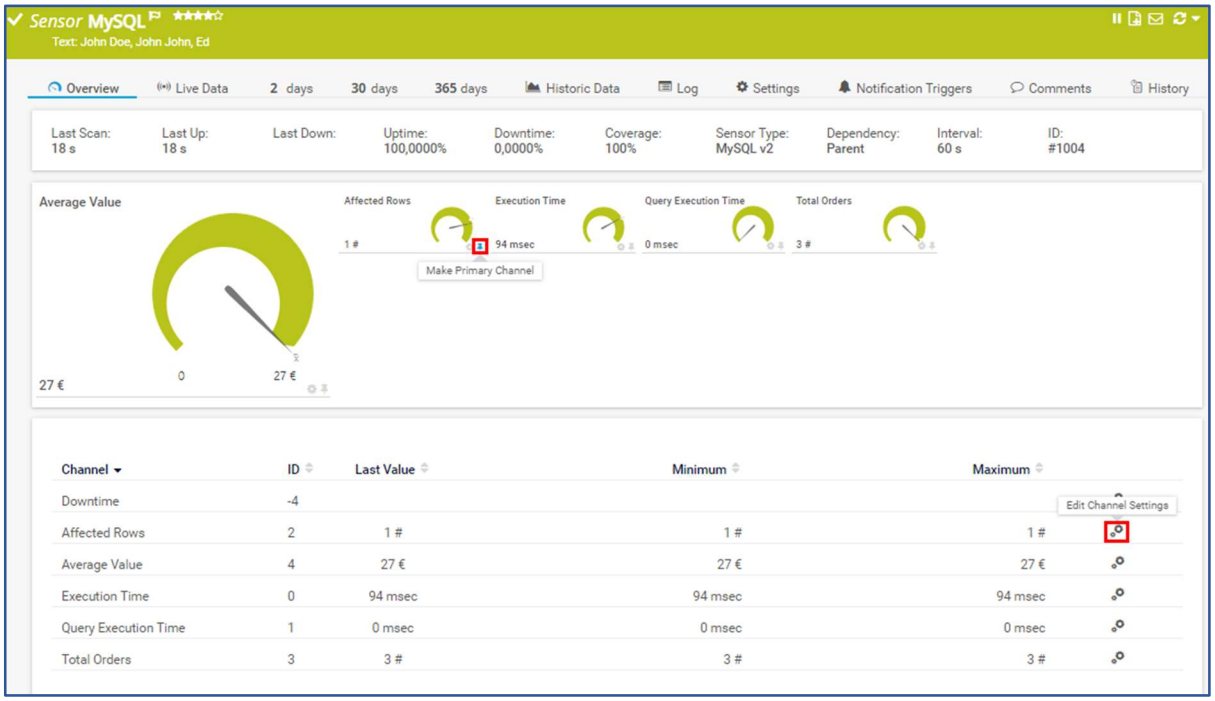



Figure 2 – PRTG MySQL Sensor

| | | | |
|---|---|---|---|
| DS0029 | Network Traffic | Network Connection Creation | Monitor for newly constructed network connections (typically port 22) that may use Valid Accounts to log into remote machines using Secure Shell (SSH). Use of SSH may be legitimate depending on the environment and how it's used. Other factors, such as access patterns and activity that occurs after a remote login, may indicate suspicious or malicious behavior with SSH.<br><br>Network Analysis Frameworks such as Zeek can be used to capture, decode, and alert on network traffic. Accordingly, they can be used to look for the creation of SSH network connections. |

Figure 3 – Example of SSH from MITRA

# Discussion

In Big Dog Organization's infrastructure, each sensor has been chosen to identify and alert specific risks that threaten the company's operations. These sensors are expected to be strategically positioned throughout the network and scan irregularities that could signify a potential breach.

The sensors given to analyze have been searched for potentials and explicitly monitored for risk and vulnerabilities. The sensors are prioritized based on their potential security impact. Additionally, the thresholds and assumptions ensure that security incidents are detected.

# Recommendations

First, continuous monitoring and scanning should be implemented to identify incidents promptly. Additionally, effective alert thresholds will establish an appropriate practice for hunting incidents. Finally, prioritizing SIL Sensors would be critical in detecting and responding to a potential security threat and will secure data integrity, confidentiality, and availability. In addition to general recommendations, individual recommendations for prevention are listed below.

**HTTP Load Sensor:**

- Use caching mechanisms to reduce the load on the server for frequently accessed resources.
- Regularly monitor server performance metrics and scale resources to handle increasing loads.

**MySQL Database Sensor:**

- Implement robust authentication mechanisms, such as two-factor authentication (2FA), to prevent unauthorized access.
- Monitor database activity for unusual or unauthorized queries and connections.

**SSH Sensor:**

- Implement key-based authentication instead of password authentication for increased security.
- Monitor SSH login attempts and implement mechanisms to detect and block brute-force attacks.
- Regularly audit SSH configurations and user accounts to ensure compliance with security policies.

**File Sensor:**

- Encrypt sensitive files to prevent unauthorized access in case of a data breach.
- Regularly scan files for malware and other malicious content using antivirus or endpoint protection solutions.

**Windows Event Log Sensor:**

- Regularly review and analyze event logs for signs of suspicious or malicious activity.
- Configure alerts and notifications for specific event IDs associated with security incidents.

**Bandwidth Sensor:**

- Monitor bandwidth usage in real-time and establish baseline metrics to identify abnormal spikes or drops.
- Regularly review and optimize network configurations to ensure efficient use of available bandwidth resources.

# References

(n.d.). Retrieved from https://www.pingdom.com/blog/page-load-time-vs-response-time-what-is-the-difference/#:~:text=Load%20time%20is%20a%20simpler,%2C%20and%20third%2Dparty%20resources.

(n.d.). Retrieved from https://www.microsoft.com/en-ca/security/business/security-101/what-are-indicators-of-compromise-ioc

(n.d.). Retrieved from https://www.site24x7.com/learn/linux/troubleshoot-high-io-wait.html

(n.d.). Retrieved from https://www.appviewx.com/blogs/identifying-and-mitigating-secure-socket-shell-ssh-key-security-vulnerabilities/

(n.d.). Retrieved from https://www.nist.gov/

(n.d.). Retrieved from https://kb.paessler.com/en/topic/70618-how-to-set-up-the-sql-v2-sensors-in-prtg-is-there-a-guide

(n.d.). Retrieved from https://www.trendmicro.com/en_ca/forHome.html