Logs, IoCs, Thresholds, and Alerts case study report

Executive Summary

The objective of the audit was to conduct a thorough analysis of the network infrastructure to enhance security and stability for the "Big Dog" organization. Our focus has been on providing concise and actionable insights for executive managers, ensuring the summary is accessible to both technical and non-technical audiences.

By implementing the recommended configuration in PRTG, we can proactively monitor the network environment and detect potential threats promptly (Paessler PRTG Monitoring Solutions). The top five sensors and thresholds we recommend for monitoring are as follows:

- **Intrusion Detection System (IDS) Sensor:** This sensor monitors network traffic for suspicious activity, alerting potential intrusions or attacks.
- **Firewall Sensor:** Monitoring the status and performance of firewalls ensures proper protection against unauthorized access, with thresholds set for availability, bandwidth usage, and rule violations.
- **Server Health Sensor:** Monitoring critical server health, including CPU usage, memory utilization, disk space, and service availability, helps identify abnormal behavior or resource exhaustion.
- **Vulnerability Scanner Sensor:** Regular scans are conducted to identify known vulnerabilities in network devices and applications, prioritizing high-severity risks through threshold settings.
- **Network Bandwidth Sensor:** Monitoring network link bandwidth usage helps identify potential bottlenecks, excessive utilization, and suspicious activity, with thresholds triggering alerts for network congestion.

A. Methodology

Our security assessment followed a structured approach. We used a Kali Linux machine to scan the network and identify devices, open ports, and operating system versions. Vulnerability assessments were conducted based on industry frameworks, prioritizing risks with the help of the CVSS calculator (CVSS Calculator). To promptly detect threats, we established indicators of compromise. Additionally, we utilized PRTG for proactive network monitoring by adding sensors and setting alert thresholds (Paessler PRTG Monitoring Solutions). This methodology ensures accurate vulnerability assessment and effective threat monitoring.

B. Audit

B1. Findings 1

After running network scans to identify devices and open ports available, found 3 devices:

Winserver Machine
Windows 1 Machine
Linux Machine

Devices	Winserver	Windows 1	Linux
IP Address	172.16.14.53	172.16.14.50	172.16.14.52
Ports	135/139/445/ 3389	135/139/445/ 3389/5357	80/3389/ 9200
Open/Close	Open	Open	Open
Transmission Protocol	MSRPC/NETBIOS/ MICROSOFT-DS/ MS-WBT-SERVER	MSRPC/NETBIOS/ MICROSOFT-DS/ MS-WBT-SERVER/WSDAPI	HTTP/MS-WBT-SERVER/WAP-WSP
Operation System (Version) Details	Microsoft Windows Server 2016 build 10586-14393	Microsoft Windows 10 (1507-1607)	Linux 4.15-5.6)

B2. Findings 2

Using the Common Vulnerability Scoring System (Common vulnerability scoring system SIG) which provides a numerical rating, ranging from 0 to 10, to assess the severity of vulnerabilities; This system is widely used to evaluate the severity of publicly disclosed vulnerabilities listed in the Common Vulnerabilities and Exposures

(CVE) database. CVSS scores offer a concise and easily understandable way to gauge the severity of vulnerabilities, with higher scores indicating more critical risks.

1. **Winserver →** SQL Database,IIS, PRTG, and File Server

    a. Vulnerabilities: The identified vulnerabilities include remote code execution, insecure configurations, and unpatched vulnerabilities.
    b. Risks/Threats: These vulnerabilities pose risks such as unauthorized access, malware infections, and data breaches.
    c. Prioritization: Remote code execution vulnerabilities are of critical concern as they allow attackers to gain unauthorized access and execute malicious code. Insecure configurations and unpatched vulnerabilities also increase the risk of system compromise.

    CVE 2019-0555: An elevation of privilege vulnerability exists in the Microsoft XmlDocument class that could allow an attacker to escape from the AppContainer sandbox in the browser, aka "Microsoft XmlDocument Elevation of Privilege Vulnerability." This affects Windows Server 2012 R2, Windows RT 8.1, Windows Server 2012, Windows Server 2019, Windows Server 2016, Windows 8.1, Windows 10, Windows 10 Servers.

    CVSS: The vulnerability has a high severity rating of 7.8.

    On the CIA triad, availability is crucial for the Windows Server database to ensure data accessibility when needed.

    Fix: To address this vulnerability, a software update is required.

2. **Linux →**
    a. Vulnerabilities: Unpatched software, weak authentication, misconfigured services, software vulnerabilities, insider threats.
    b. Risks/Threats: Unauthorized access, malware infections, data breaches, denial of service attacks, privilege escalation.
    c. Prioritization: Patch management (update regularly), strong authentication (secure logins), secure configuration (proper settings), security monitoring (active surveillance), user education (awareness training).

    CVE-2020-12888: The VFIO PCI driver in the Linux kernel through 5.6.13 mishandles attempts to access disabled memory space.

CVVS: Base Score 5.3 MEDIUM

On the CIA triad, integrity is crucial for the Linux MySQL database to ensure data remains trustworthy, complete, and unaltered by unauthorized users.

Fix: A software update is required and its recommended to backup your database and update firewall.

3. **Windows 1** → Sales and Marketing:

   DNS server:

   a. Vulnerabilities: DNS cache poisoning, DDOS attacks, Unpatched software, weak authentication.
   b. Risks/Threats: DNS hijacking, Unauthorized access, malware infections, data breaches.
   c. Prioritization: DNS cache poisoning is a critical risk. DDOS attacks can affect the availability of the DNS services.

CVE-2020-1461: An elevation of privilege vulnerability exists when the MpSigStub.exe for Defender allows file deletion in arbitrary locations. To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Defender Elevation of Privilege Vulnerability'.

CVSS: Base Score: 7.1 HIGH

On the CIA triad, confidentiality is essential for protecting information on the Windows system from unauthorized access.

Fix: It is recommended to apply the latest security updates and patches provided by Microsoft for Microsoft Defender, ensuring that MpSigStub.exe does not allow unauthorized file deletion in arbitrary locations. More training for employees is also necessary.

B3. Findings 3

Big Dog Assets:

- Winserver: Hosts the SQL Database,IIS, PRTG, and File Server
- Linux: For devs
- Windows1: Sales and Marketing

Order of Priorities:

- Privacy – Database, file server
- Proprietary - Linux used by devs
- Financial - Sales and marketing
- Admin – Management
- Security Management – Websites

C. Recommendation:

We recommend that you monitor all your assets through PRTG (Paessler PRTG Monitoring Solutions). To use PRTG to add sensors, implement IoCs, and set up alerts for a database server, Windows workstation, and Linux for developers, follow these steps:

C1. Database Server Monitoring:

1. Install PRTG on a machine that has access to the database server.

2. Add a sensor for the database server. You can use the "SQL Server Sensor" if available, or configure a "Ping" or "SNMP" sensor to monitor the server's availability.

3. Enable database-specific monitoring for the sensor. For example, configure it to monitor query response time or database connection status.

4. Implement IoCs by creating a custom sensor that analyzes SQL queries or authentication logs for known attack patterns.

5. Set up alerts for unusual database access patterns, failed authentication attempts, and unauthorized schema modifications.

C2. Windows Workstation Monitoring:

1. Add a "Windows System Health" sensor to monitor the workstation's overall health, including CPU usage, memory usage, and disk activity.

2. Implement IoCs by creating custom sensors to monitor specific Windows processes or network connections associated with suspicious activities.

3. Set up alerts for suspicious Windows processes, failed login attempts, and unusual network connections.

C3. Linux Developer Workstation:

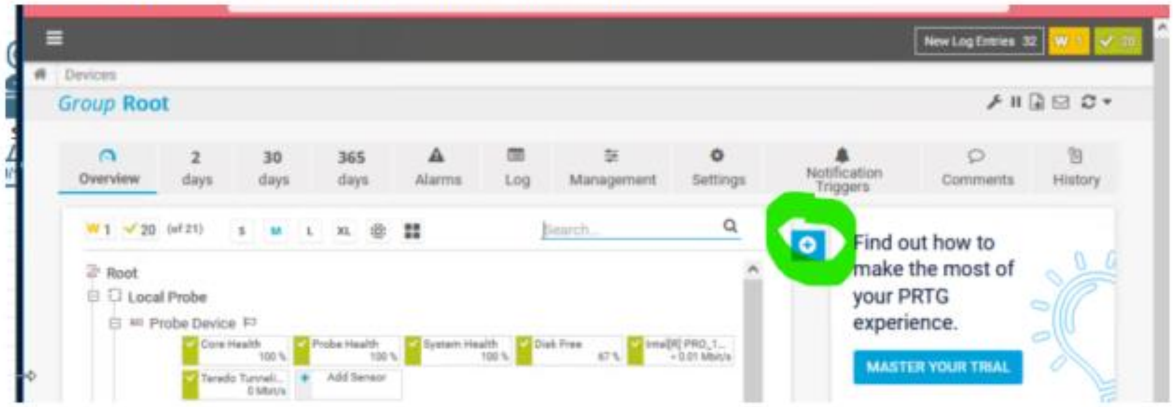
1. Add a "SSH" or "SNMP" sensor to monitor the availability and performance of the Linux workstation.

2. Implement IoCs by creating custom sensors to monitor Linux kernel exploits or unusual file access patterns.

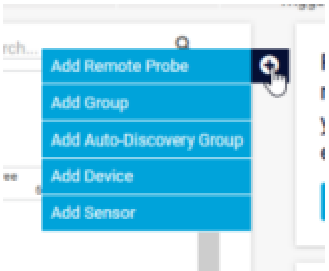
3. Set up alerts for known Linux kernel exploits, unauthorized access attempts, and abnormal file access patterns.

4. Configure alerts for failed login attempts to the Linux workstation.

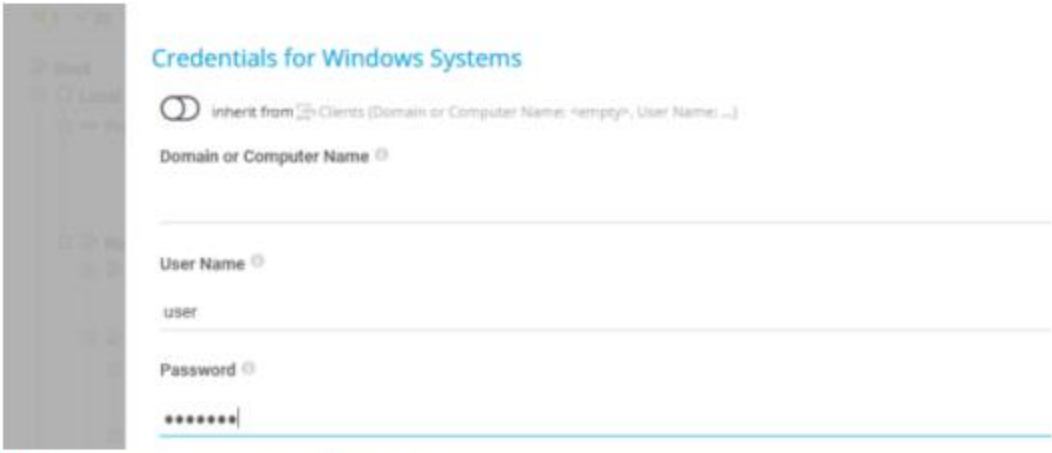
In the Devices page, click the little blue star,



and open up the blue menu.



Select “Add Device” and scroll down to select the parent group for the new device. For this example I will select Windows/Clients (we are going to add our Windows system). Give the device a name. In this case I am going to say “Windows”, I am going to give PRTG the Windows system’s IP address (10.10.10.50), select the Windows Icon, and select Standard auto-discovery. I am going to remove the check mark “Inherit from…” under the Windows Credentials, and add our username and password.



Credentials for Windows Systems

inherit from Clients (Domain or Computer Name: <empty>, User Name: ...)

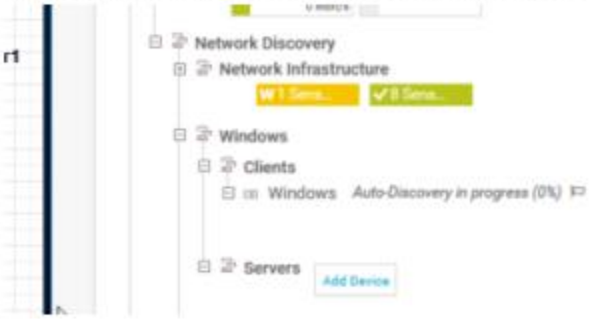
Domain or Computer Name

User Name: user

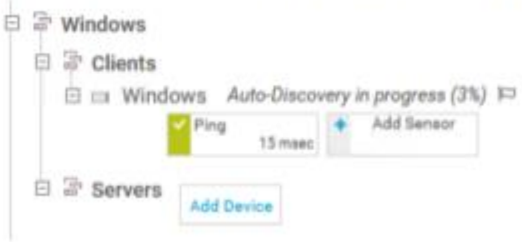
Password: •••••••

Now I am going to click OK!

I should now see the new device being added.

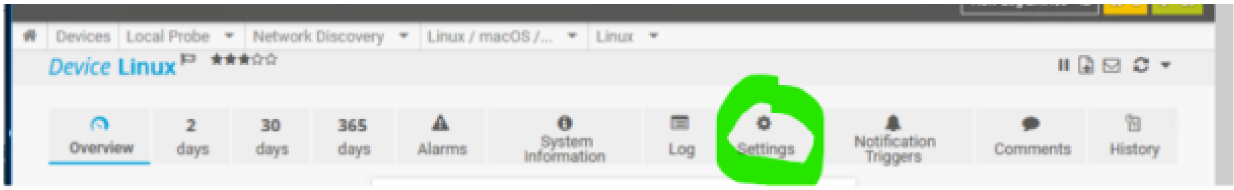


Make note that this adds a PING sensor to the device !

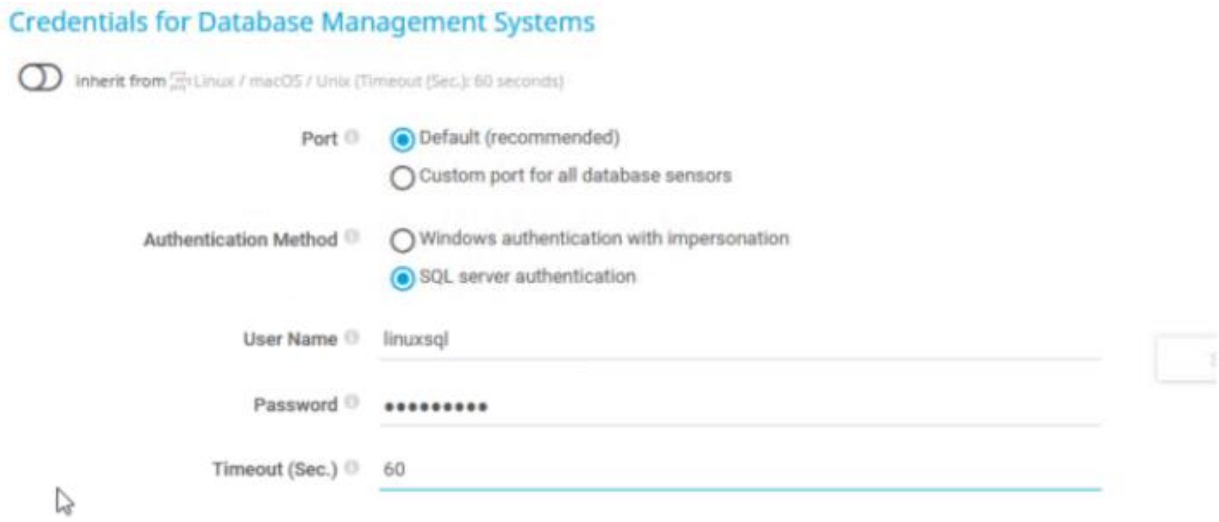


For Linux (The Linux system) we are going to add a sensor for MySQL as well! To do this, you must follow this carefully! This is a challenge! If you want to read up more first, have a look at this! Adding a MySQL sensor for the MySQL server on Linux. You can read more here, https://www.paessler.com/mysql_monitoring

Click on Settings.



Scroll down to “Credentials for Database Management Systems and remove the “Inherit from… ” option.



Credentials for Database Management Systems

inherit from Linux / macOS / Unix (Timeout (Sec.): 60 seconds)

Port: ● Default (recommended) ○ Custom port for all database sensors

Authentication Method: ○ Windows authentication with impersonation ● SQL server authentication

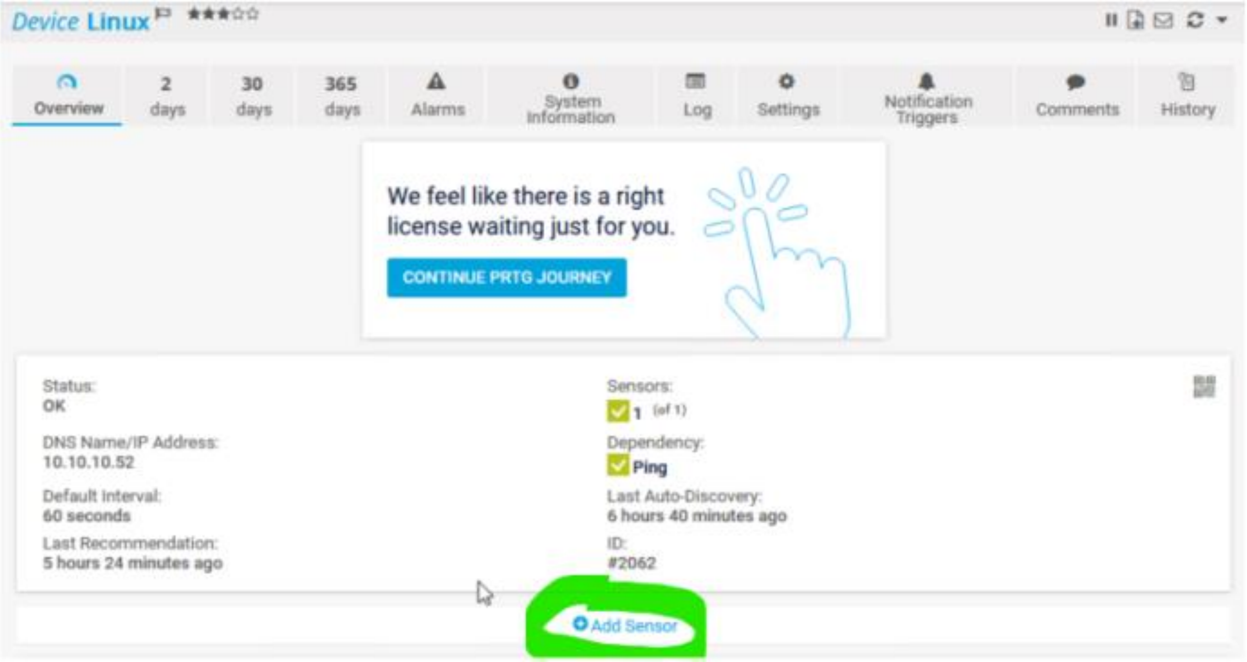
User Name: linuxsql

Password: ●●●●●●●●●●

Timeout (Sec.): 60

Now add the User Name “linuxsql” with a password of “Test123” (We created this user in your MySQL database!)

Click Save Now click the Add Sensor item.



We feel like there is a right license waiting just for you.

Status: OK

DNS Name/IP Address: 10.10.10.52

Default Interval: 60 seconds

Last Recommendation: 5 hours 24 minutes ago

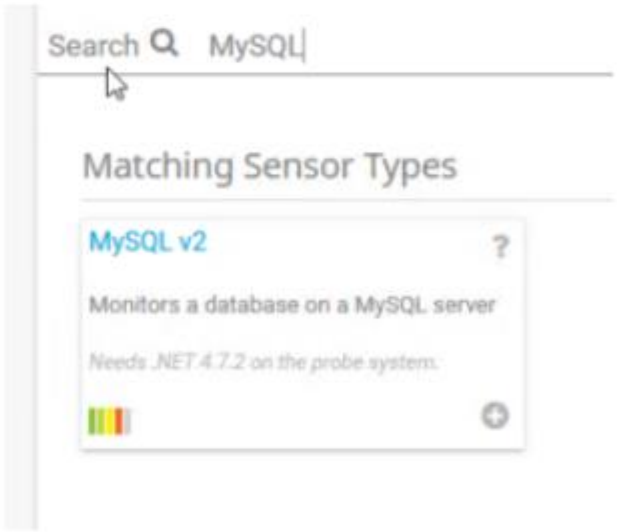
Sensors: 1 (of 1)

Dependency: Ping

Last Auto-Discovery: 6 hours 40 minutes ago

ID: #2062

Do NOT click anything in the blue square. Instead in the Search bar enter “MySQL” . You should see the following.



Search MySQL

Matching Sensor Types

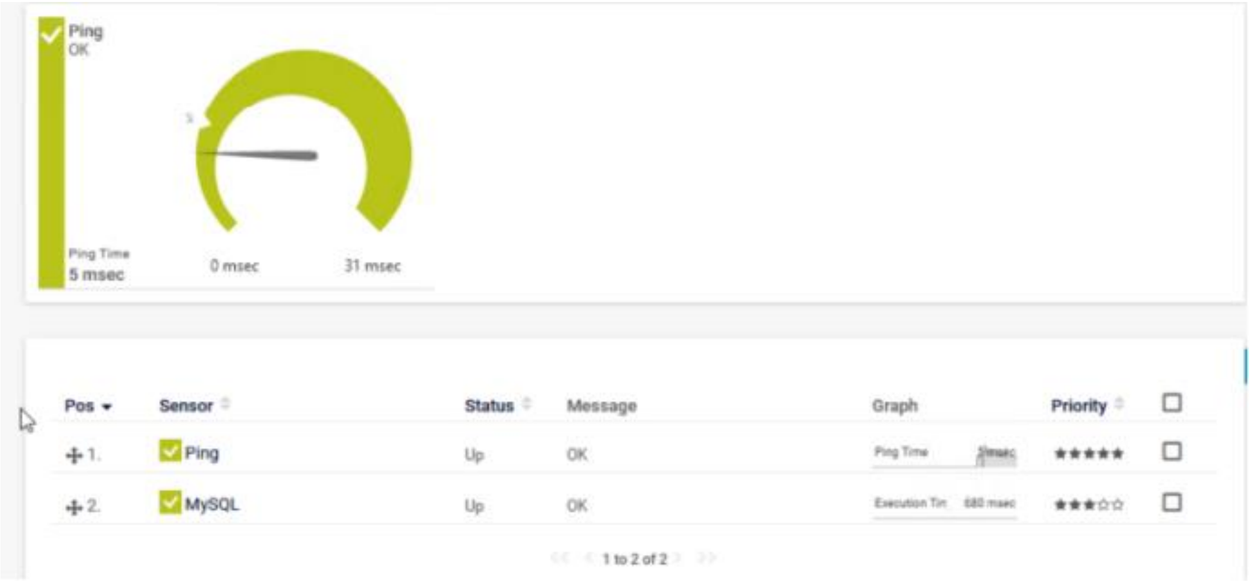
MySQL v2

Monitors a database on a MySQL server

Needs .NET 4.7.2 on the probe system.

Click on “MySQL v2”.

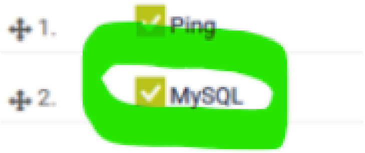
On the Database line type “TestDB” (we created this Database in your MySQL) and click on Create. That’s it! Give it a few seconds and you should see this.



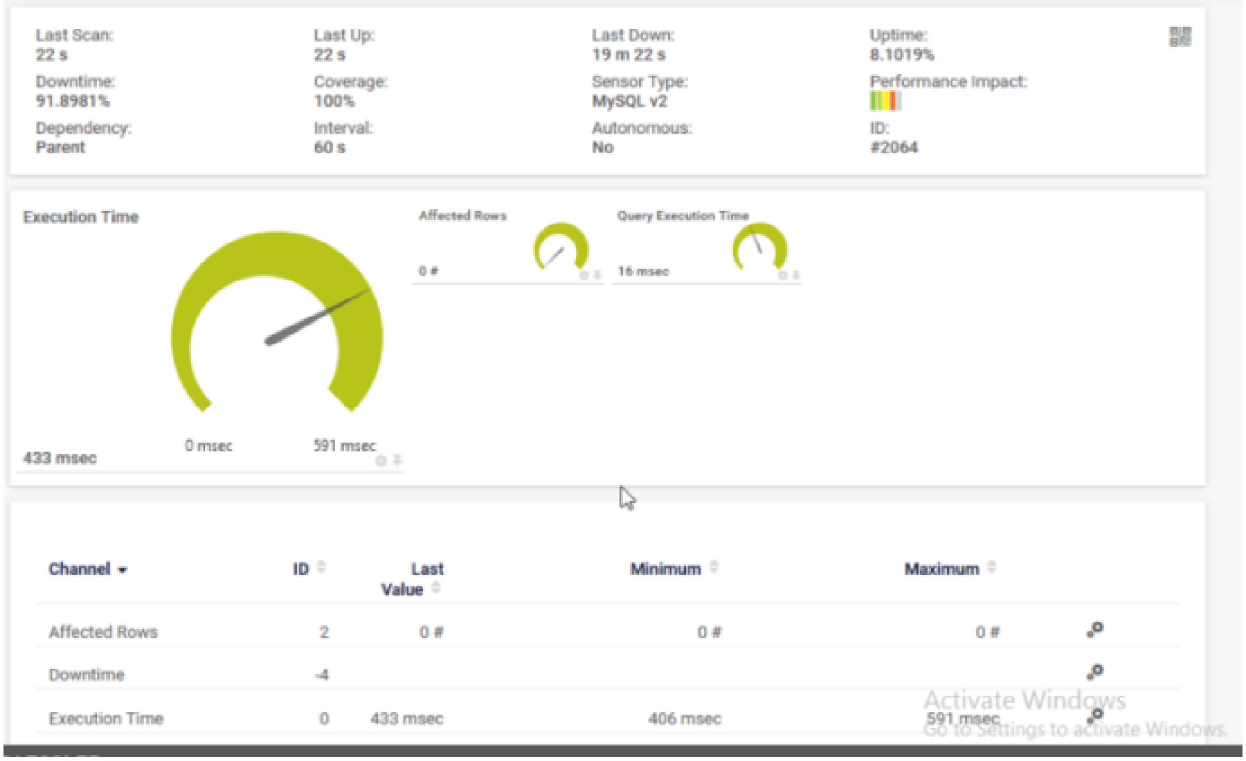
Pos	Sensor	Status	Message	Graph	Priority	□
1.	✓ Ping	Up	OK	Ping Time 5msec	★★★★★	□
2.	✓ MySQL	Up	OK	Execution Tim 680 msec	★★★☆☆	□

1 to 2 of 2

Click on the MySQL sensor.



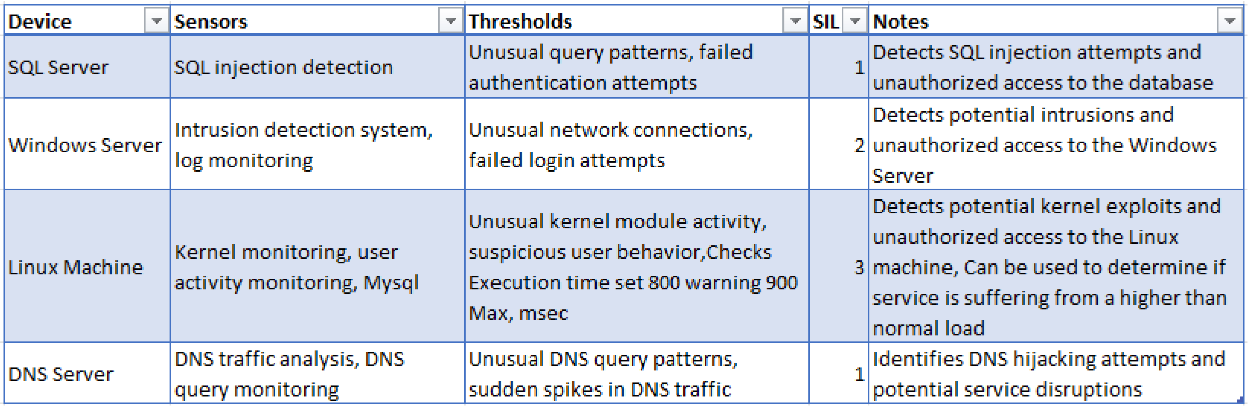
You will see some current information on the sensor,



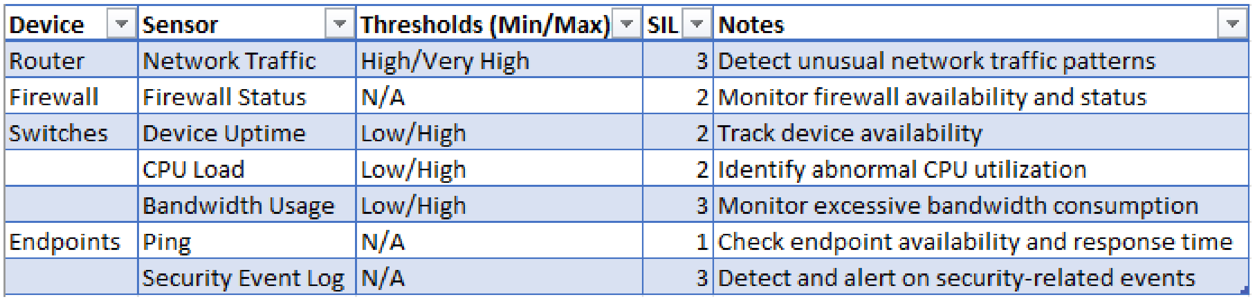
Last Scan: 22 s	Last Up: 22 s	Last Down: 19 m 22 s	Uptime: 8.1019%
Downtime: 91.8981%	Coverage: 100%	Sensor Type: MySQL v2	Performance Impact: ▮▮▮▮
Dependency: Parent	Interval: 60 s	Autonomous: No	ID: #2064

Channel	ID	Last Value	Minimum	Maximum
Affected Rows	2	0 #	0 #	0 #
Downtime	-4			
Execution Time	0	433 msec	406 msec	591 msec

Note: Remember to adjust the specific settings of each sensor according to your requirements and environment. Regularly review and update the IoCs and alerts based on emerging threats and vulnerabilities to ensure effective monitoring and threat detection.



Device	Sensors	Thresholds	SIL	Notes
SQL Server	SQL injection detection	Unusual query patterns, failed authentication attempts	1	Detects SQL injection attempts and unauthorized access to the database
Windows Server	Intrusion detection system, log monitoring	Unusual network connections, failed login attempts	2	Detects potential intrusions and unauthorized access to the Windows Server
Linux Machine	Kernel monitoring, user activity monitoring, Mysql	Unusual kernel module activity, suspicious user behavior,Checks Execution time set 800 warning 900 Max, msec	3	Detects potential kernel exploits and unauthorized access to the Linux machine, Can be used to determine if service is suffering from a higher than normal load
DNS Server	DNS traffic analysis, DNS query monitoring	Unusual DNS query patterns, sudden spikes in DNS traffic	1	Identifies DNS hijacking attempts and potential service disruptions



Device	Sensor	Thresholds (Min/Max)	SIL	Notes
Router	Network Traffic	High/Very High	3	Detect unusual network traffic patterns
Firewall	Firewall Status	N/A	2	Monitor firewall availability and status
Switches	Device Uptime	Low/High	2	Track device availability
	CPU Load	Low/High	2	Identify abnormal CPU utilization
	Bandwidth Usage	Low/High	3	Monitor excessive bandwidth consumption
Endpoints	Ping	N/A	1	Check endpoint availability and response time
	Security Event Log	N/A	3	Detect and alert on security-related events

By Jasraj Johal

Bibliography

Discover the 3 Paessler PRTG Monitoring Solutions. Home. (n.d.). https://www.paessler.com/prtg

Common vulnerability scoring system version 3.0 calculator. FIRST. (n.d.). https://www.first.org/cvss/calculator/3.0

Common vulnerability scoring system SIG. FIRST. (n.d.-a). https://www.first.org/cvss/

CVE. (n.d.). https://cve.mitre.org/

CVE-2020-12888. CVE. (n.d.-c). https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12888

CVE-2019-0555. CVE. (n.d.-b). https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0555

CVE-2020-1461. CVE. (n.d.-b). https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1461