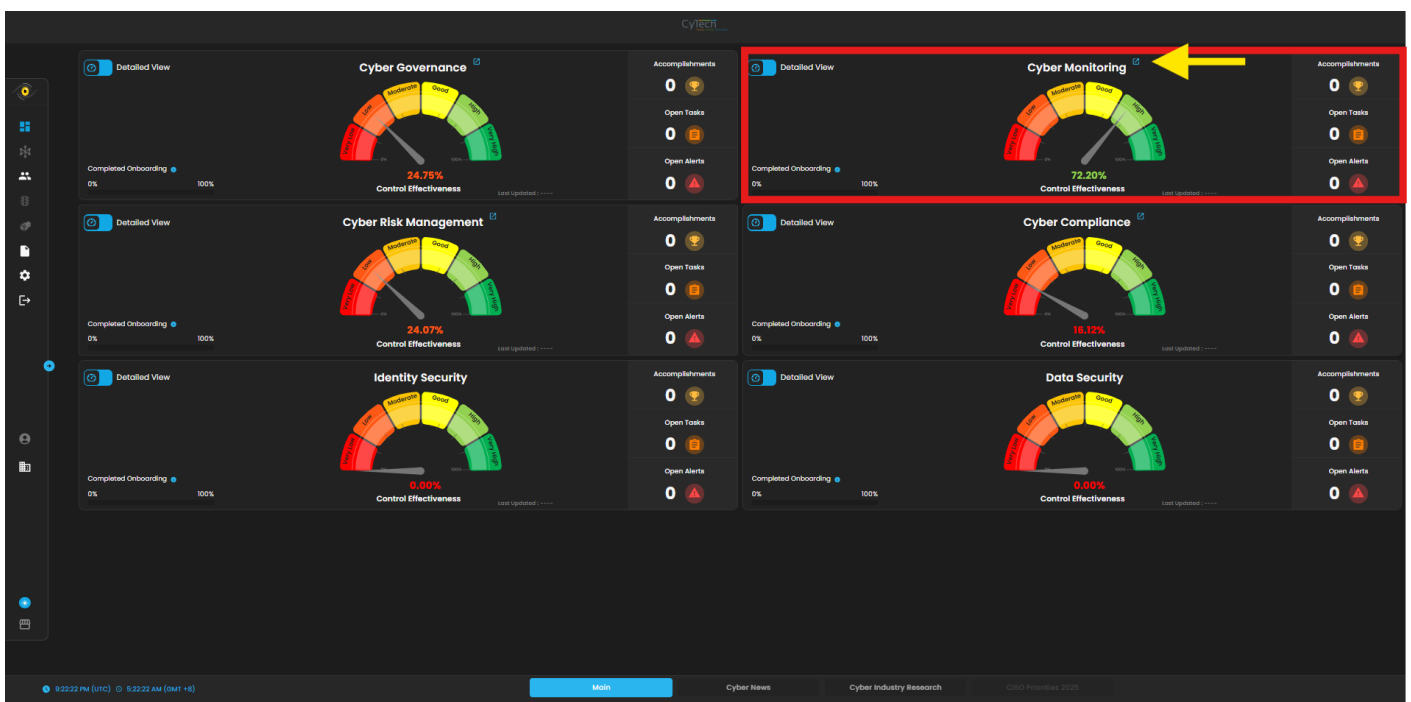


Cyber Monitoring Dashboard

Navigation to Cyber Monitoring Dashboard

To navigate your way to the Cyber Monitoring Dashboard, you must click the redirect icon  beside the "**Cyber Monitoring**" title.



This will then redirect you to the dashboard as seen below.

Welcome to Cyber Monitoring

Continuous monitoring for proactive threat detection and response.

Modules Favorites



Cyber Incident Management (SIEM and XDR)



Cloud Security Posture Management (CSPM)



Endpoint Detection and Response (EDR, MDR)



Security Orchestration, Automation and Response (SOAR)



User and Entity Behavior Analysis (UEBA)



Threat Intelligence (TI)

Overview

See what's happening in your Cyber Monitoring

Average KRI Changes

N/A

N/A

CSPM Rank

58.63 / 100

Moderate Risk



Security Measures Followed

The cloud is now secure, reducing the risk of threats like data breaches and system compromises.

Here you will see the 6 modules:

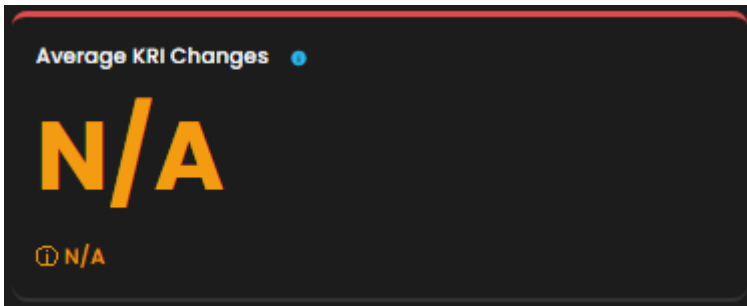
1. [Cyber Incident Management \(SIEM and XDR\)](#)
2. [Cloud Security Posture Management \(CSPM\)](#)
3. [Endpoint Detection and Response \(EDR, MDR\)](#)
4. [Security Orchestration, Automation and Response \(SOAR\)](#)
5. [User and Entity Behavior Analysis \(UEBA\)](#)
6. [Threat Intelligence \(TI\)](#)

By clicking on their icons, you will be redirected to the modules' **"Main Page"** section.

Below the modules, you will find the overview.

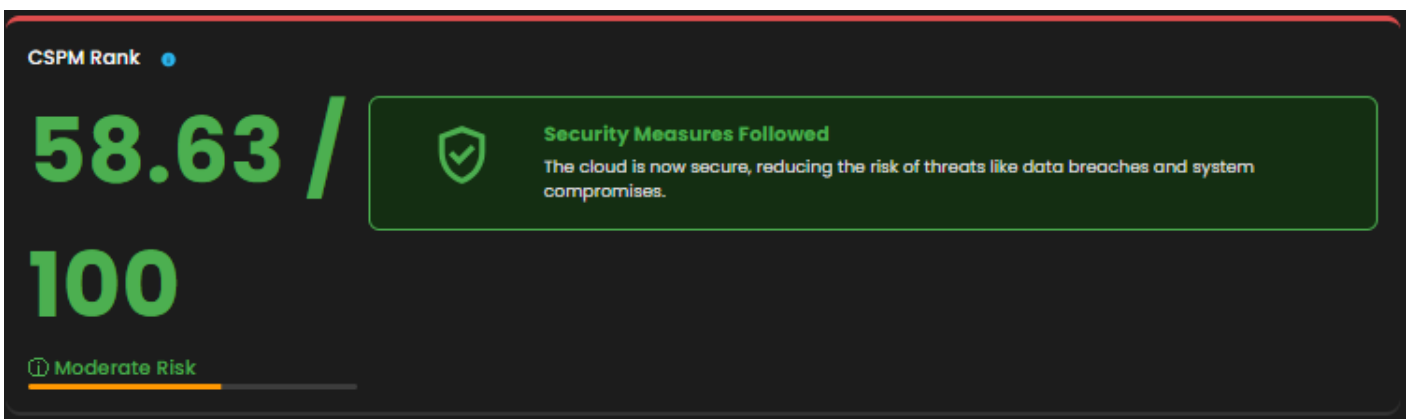
Average Key Risk Indicator (KRI) Changes

Understanding the volume of digital assets within your environment is fundamental to managing cyber risk. The total number of assets reflects the scale of your digital footprint and highlights potential vectors for exploitation. By quantifying these assets, organizations gain clarity on how broad their exposure surface truly is. This visibility allows teams to prioritize defenses, allocate resources effectively, and reduce blind spots. Recognizing the scope of what's connected is the first step toward controlling it.



CSPM Rank

Understanding the state of your cloud security is critical. The **Cloud Security Posture Management (CSPM) score** provides a quantifiable snapshot of how securely your cloud environments are configured. It reflects alignment with established best practices and recognized security standards, offering a clear benchmark for posture maturity. By highlighting deviations, gaps, or misconfigurations, the score empowers teams to prioritize remediation efforts based on risk impact. This metric doesn't just inform—it drives accountability and continuous improvement, giving organizations the visibility needed to evolve with confidence in an ever-changing threat landscape.

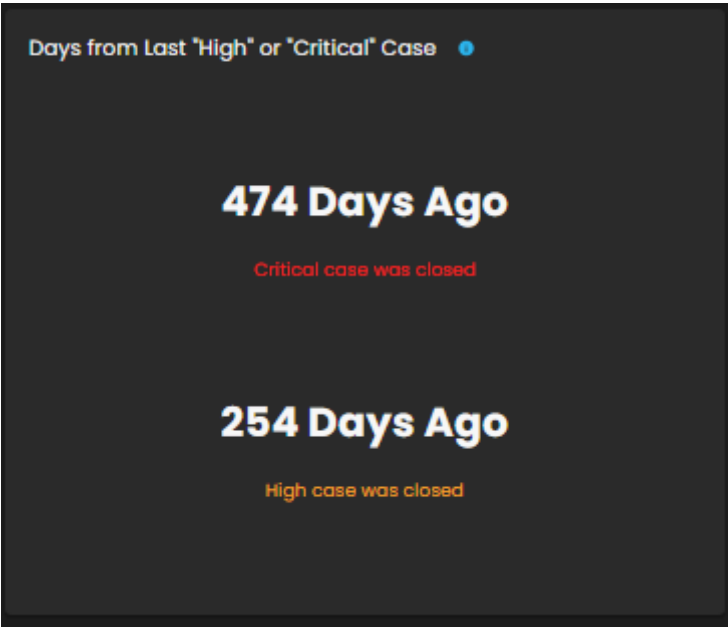


Cases

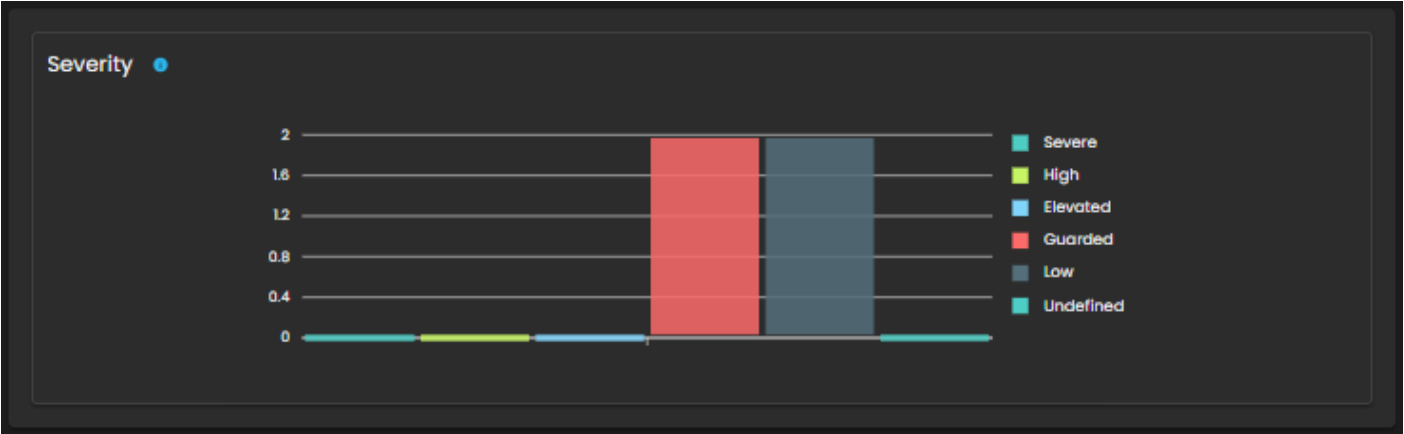
This section provides a comprehensive overview of your active and historical cases. It is designed to assist you in quickly assessing the status and urgency of each case, enabling effective prioritization and informed decision-making.



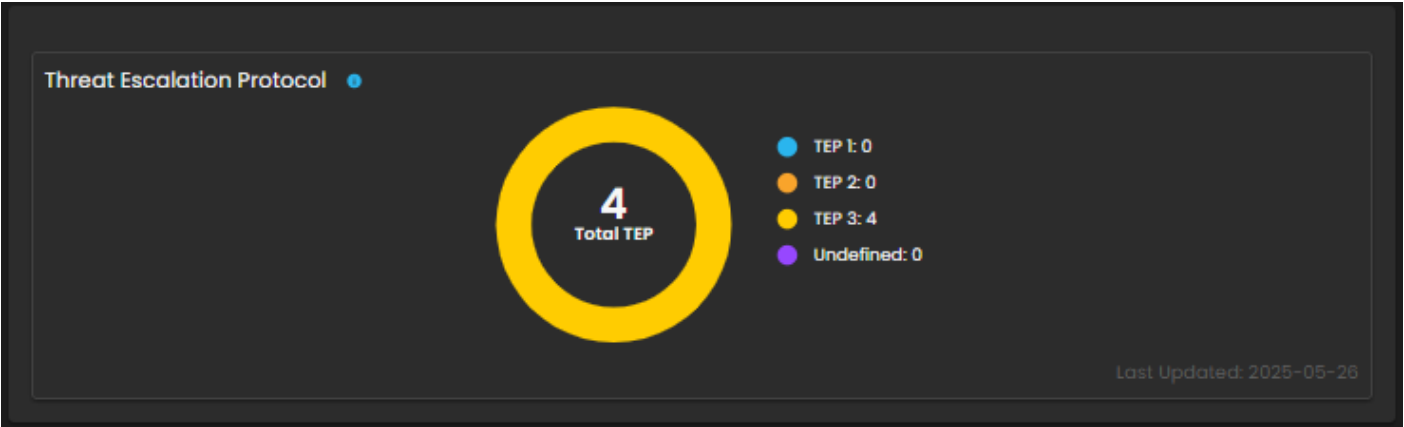
This metric displays the number of days elapsed since the most recent detection of high or critical-level monitoring alerts. A shorter interval may signal the presence of ongoing or recently emerged significant threats.



This section presents a visual breakdown of active cases categorized by severity levels: **Severe**, **High**, **Elevated**, **Guarded**, and **Low**. The distribution provides a clear snapshot of the current threat landscape and assists in the prioritization of response efforts according to the urgency of each case.

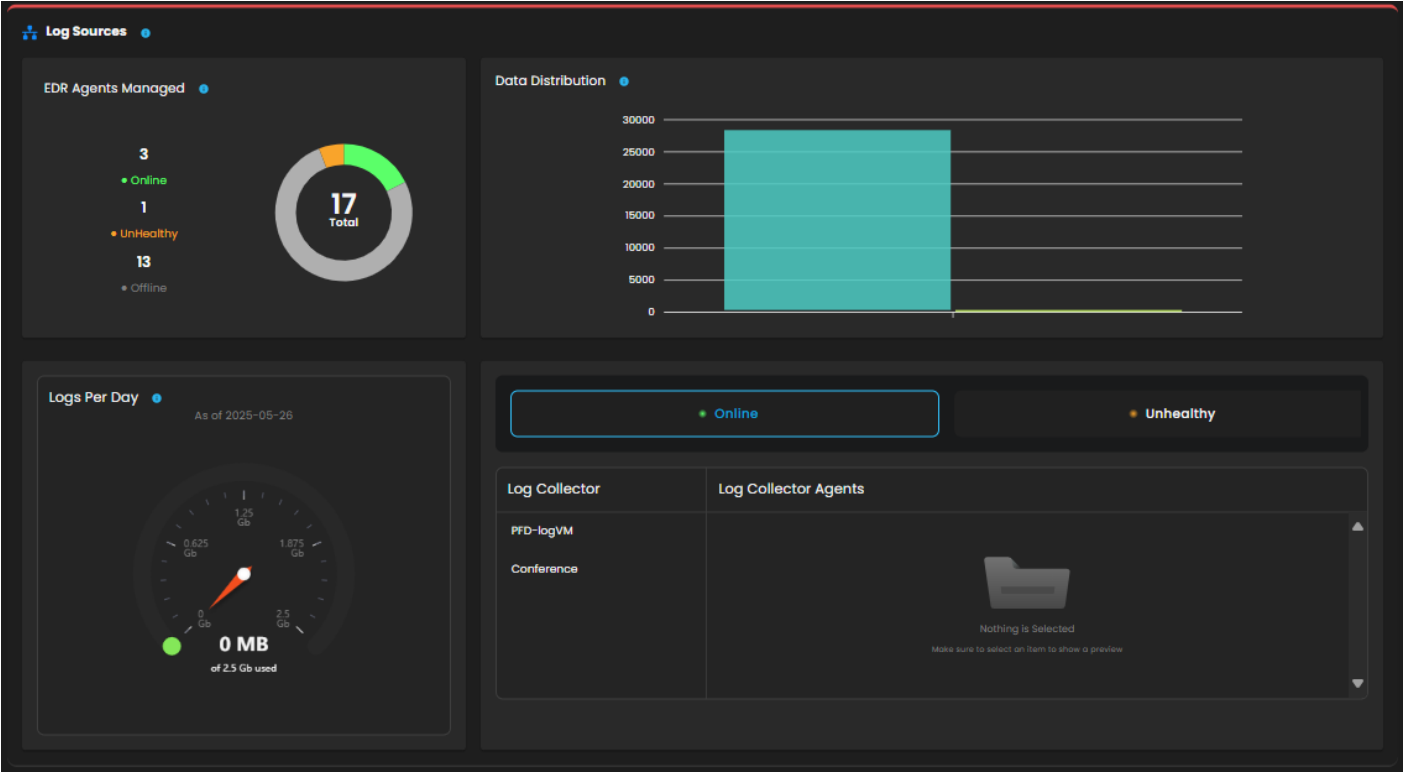


This section displays the cumulative count of open cases categorized by their current stage within the Threat Escalation Protocol (TEP). It provides a clear overview of how individual threats are advancing through the structured escalation process, enabling efficient tracking and management of threat progression.

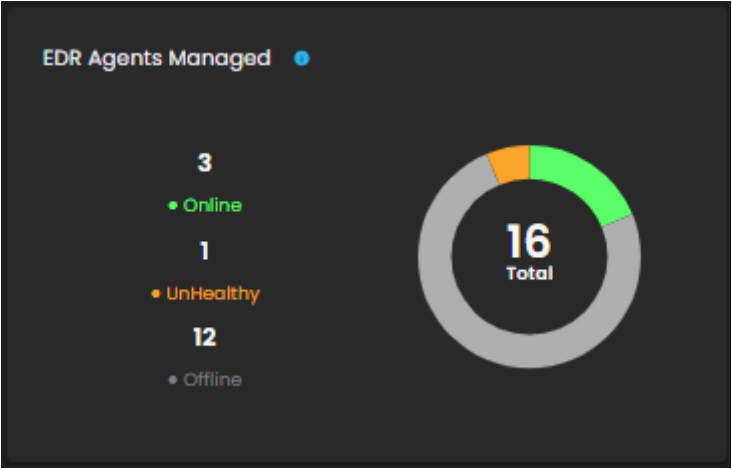


Log Sources

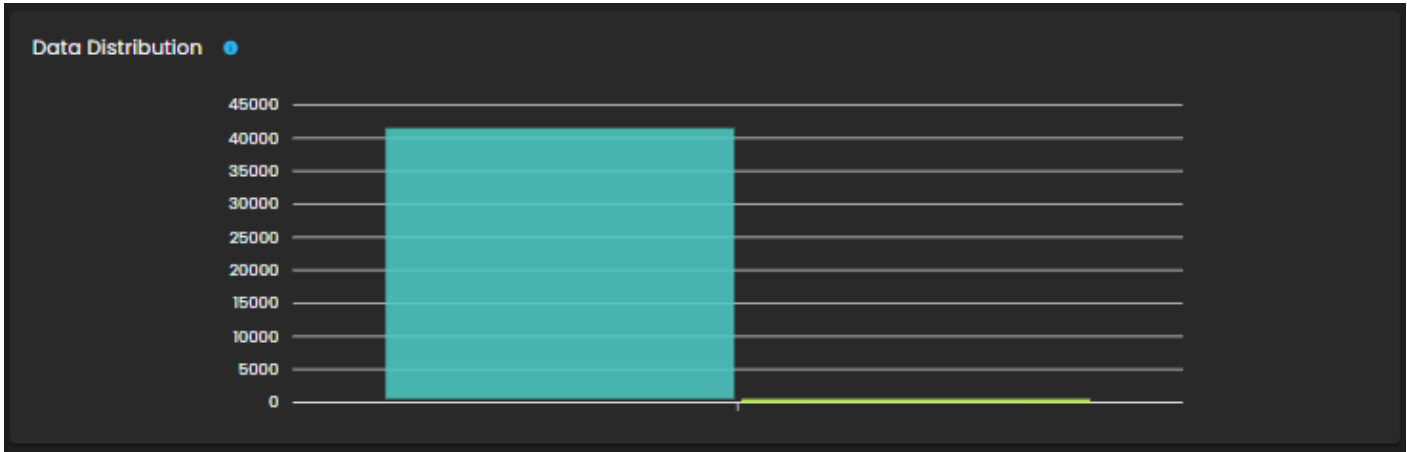
This section provides a consolidated overview of all configured log sources. Its primary purpose is to assist users in assessing the current log ingestion landscape, enabling effective prioritization of monitoring, investigation, and resource allocation efforts.



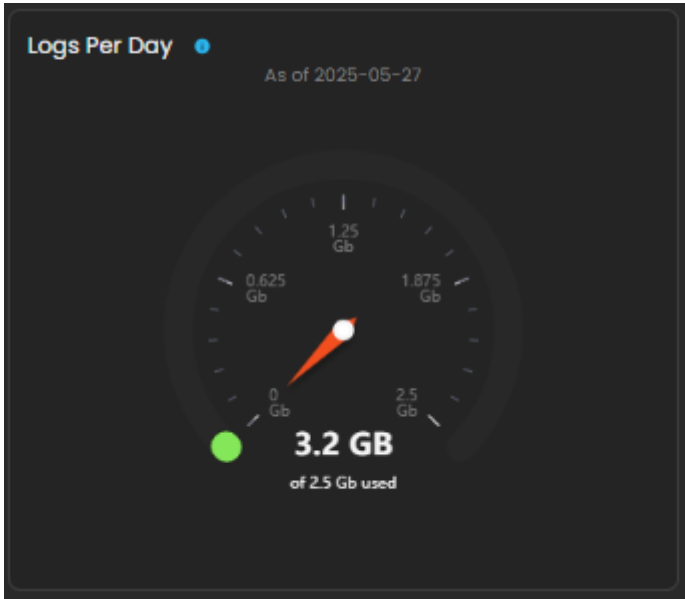
This section presents the total count of endpoints currently managed by Endpoint Detection and Response (EDR) agents. It also provides a real-time status breakdown, indicating how many endpoints are online and how many are offline.



This section presents the distribution of collected log data categorized by individual source. It serves as a valuable reference for identifying the most active log-generating systems. Understanding this distribution is essential for optimizing data flow, resource allocation, and maintaining efficient log management practices.



This shows the total volume of logs collected daily, measured against allocate capacity. Helps manage storage utilization and detect unusual log activity.



This section displays a comprehensive list of all installed log collectors, along with the agents associated with each log collector.

<div>Online</div> <div>Unhealthy</div>	
Log Collector	Log Collector Agents
PFD-logVM	<div>Nothing is Selected</div> <div>Make sure to select an item to show a preview</div>
Conference	

Revision #12

Created 26 May 2025 21:14:36 by Darryl Espancho

Updated 5 June 2025 12:54:08 by John Polestico