SOFTSHIELD

Advanced Security Monitoring and Protection for Your IT Assets

SoftShield provides comprehensive cybersecurity monitoring and protection for your IT assets with its advanced **Security Information and Event Management (SIEM)** and **Extended Detection and Response (XDR)** capabilities.

Designed to safeguard your digital infrastructure, **SoftShield** enhances your organization's security posture by proactively detecting and mitigating cyber threats.

SoftShield
Security Monitoring

Overview

This dashboard provides a **comprehensive overview of your security environment**, summarizing active agents, security alerts, and various security monitoring capabilities

1. Agent Summary

Displays the number of active and disconnected security agents within your infrastructure.

2. Last 24 Hours Alert

Categorizes security alerts by severity **levels**

Critical | Hight | Medium | Low

3. Endpoint Security

- **Configuration Assessment**: Scans system configurations to ensure compliance.
- **Malware Detection**: Identifies malware-related threats.
- **File Integrity Monitoring**: Alerts on unauthorized file changes.

4. Threat Intelligence

- **Threat Hunting**: Helps investigate security incidents.
- **MITRE ATT&CK**: Maps security alerts to known adversary tactics.
- **Vulnerability Detection**: Identifies software vulnerabilities.

5. Security Operations & Compliance

Supports frameworks like PCI DSS, GDPR, HIPAA, NIST 800-53, and TSC to maintain regulatory compliance.

6. Cloud Security

Monitors security events from AWS, Google Cloud, Office 365, Docker, and GitHub.

This dashboard helps **security teams monitor, detect, and respond to threats in real time**, ensuring compliance and protection for your organization's IT assets.

SoftShield

Feature

- Threat Detection
- Threat Response
- SIEM Integration
- Endpoint Protection
- Incident Management
- Cloud Deployment
- Data Analysis & Correlation
- Compliance Management
- Automated Response (SOAR)
- Integration with External Tools
- Customizable Playbooks
- Log Analysis & Reporting
- Real-time Event Monitoring
- Subscription (Per endpoint)
- Varies by features

Hardware SoftShield Agent requirements

CPU	1 Core CPU
RAM	4 GB
Disk Space	20 GB
OS	All OS (Windows, Linux and MacOS)

SoftShield installation prequisites

Hardware SoftShield Server requirements

Small (1-25 Agents)

CPU	4 Core CPU
RAM	8 GB
Disk Space	50 GB
OS	Ubuntu

Medium (25-50 Agents)

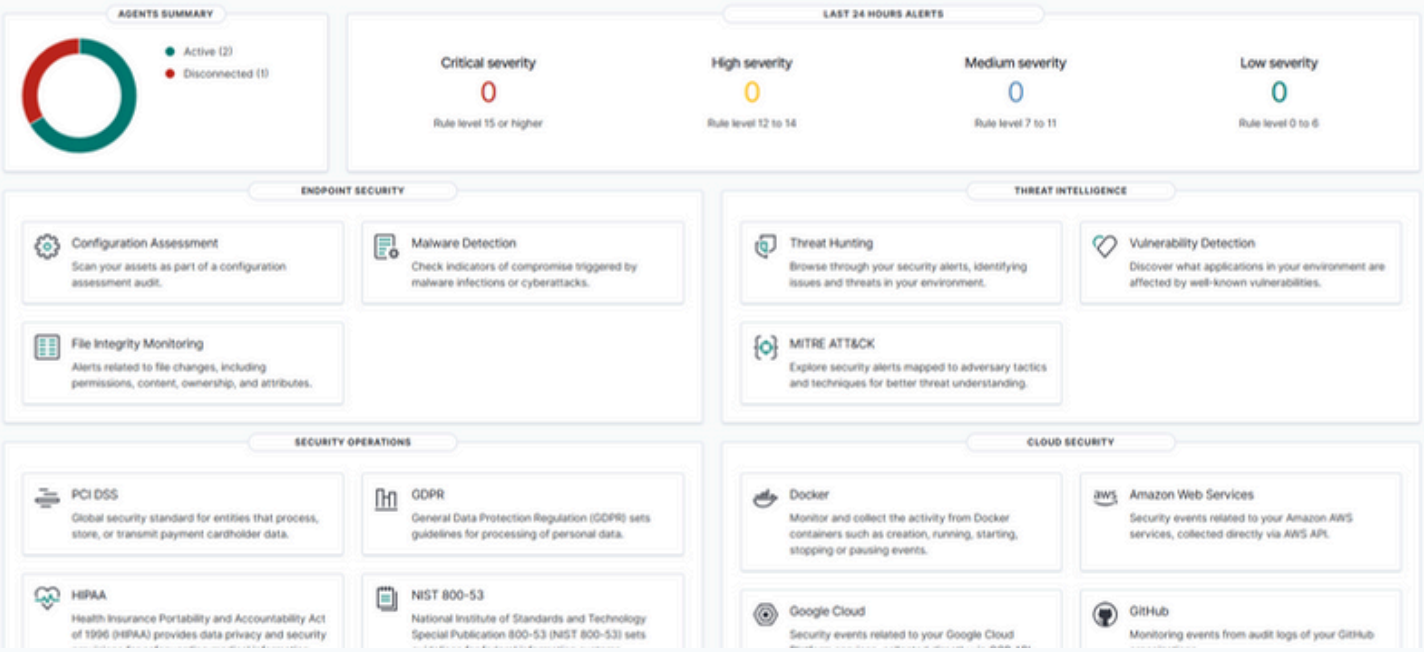
CPU	8 Core CPU
RAM	8 GB
Disk Space	100 GB
OS	Ubuntu

Large (50-100 Agents)

CPU	8 Core CPU
RAM	8 GB
Disk Space	200 GB
OS	Ubuntu

Security Configuration Assessment (SCA) with **SoftShield**

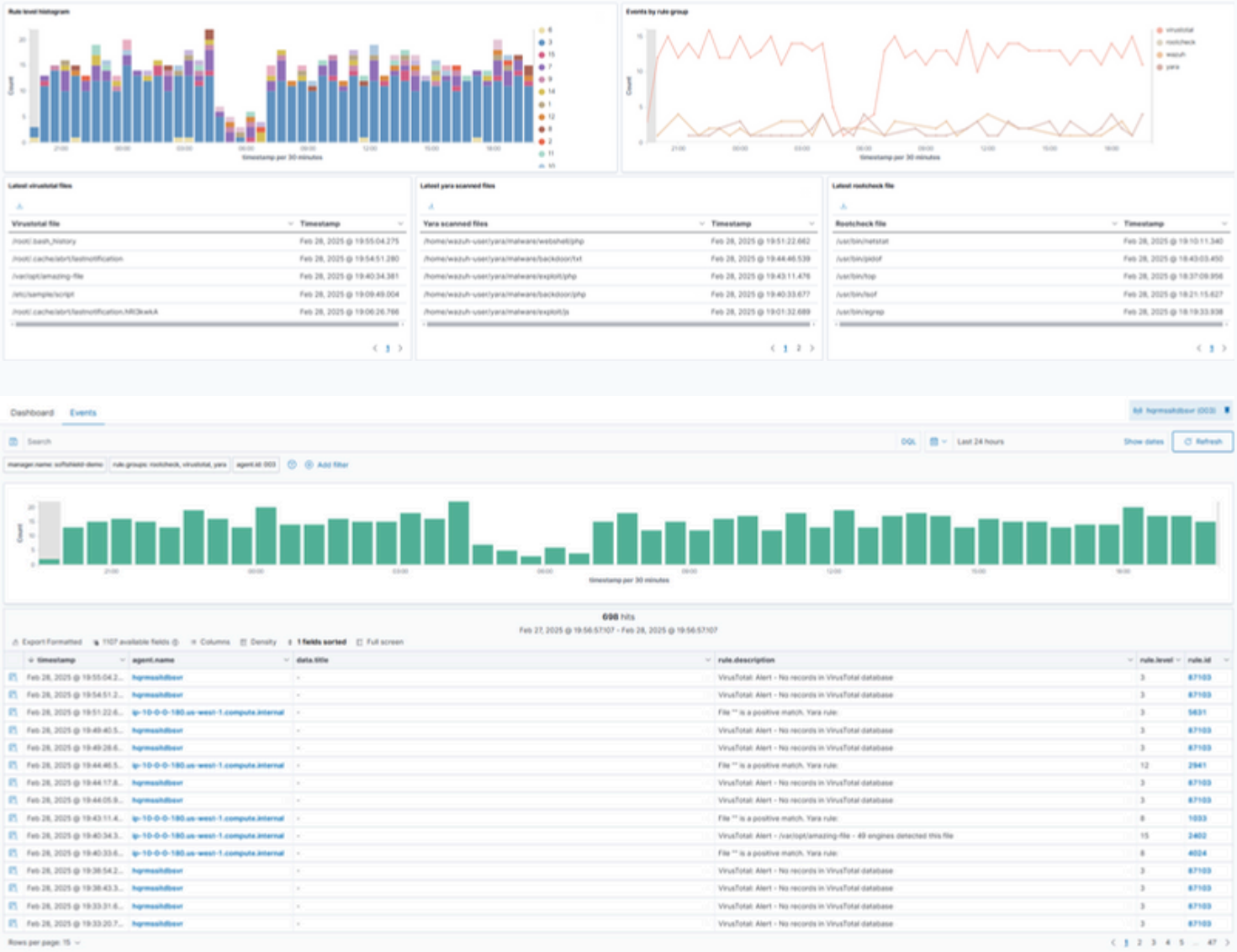
SoftShield continuously monitors **system and application configurations** to ensure compliance with **security policies, industry standards**, and hardening guidelines. Its agents perform regular scans to detect misconfigurations and security gaps that could be exploited by threats.



With **customizable configuration checks**, **SoftShield** allows organizations to tailor assessments to their specific security needs. Security alerts provide **actionable recommendations, references, and regulatory compliance mappings**, ensuring a well-protected IT environment.

Malware Detection with **SoftShield**

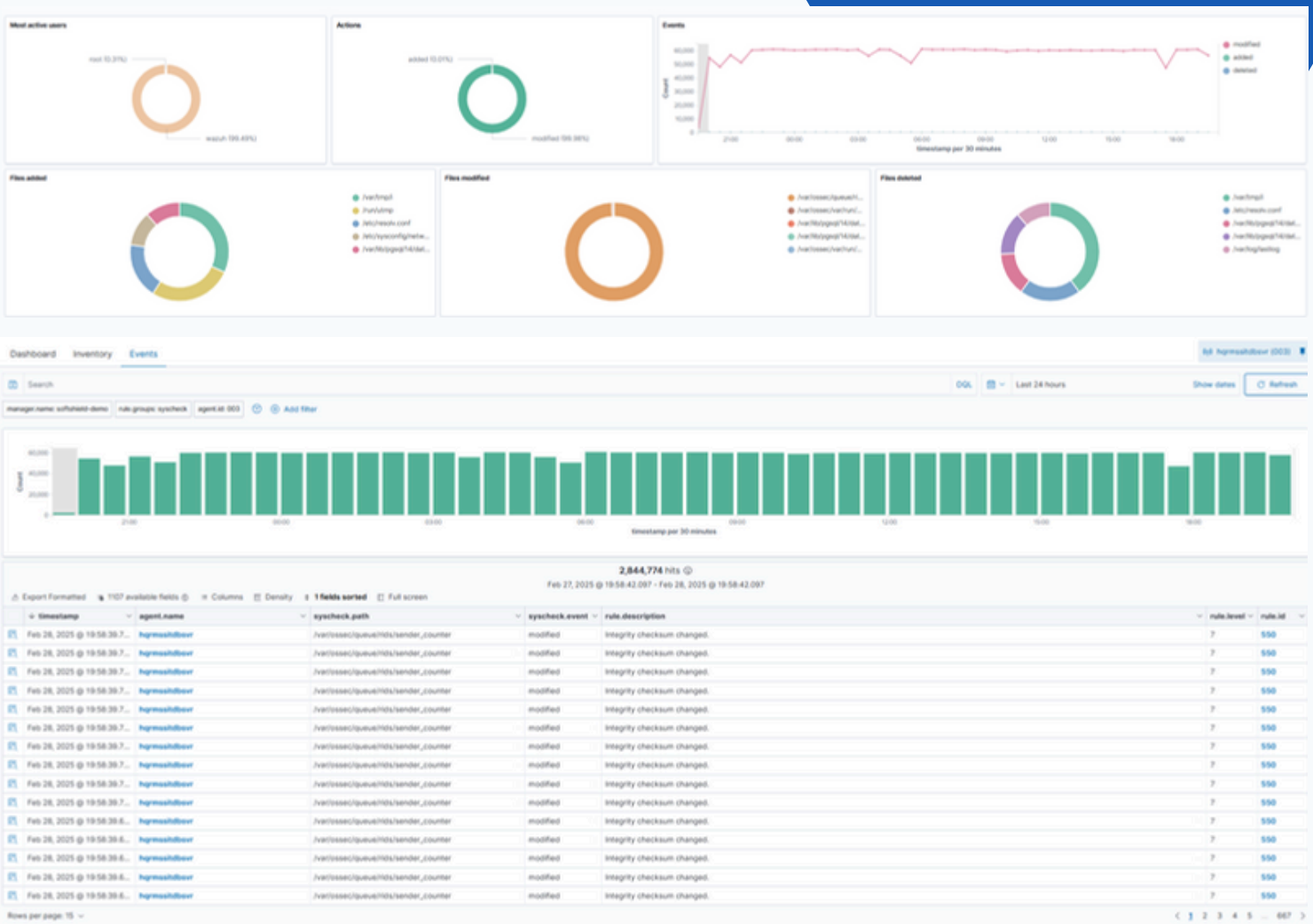
SoftShield identifies **malicious activities and indicators of compromise (IoCs)** caused by **malware infections or cyberattacks** on endpoints. With **built-in security rules** and features like **Security Configuration Assessment (SCA), Rootcheck, and File Integrity Monitoring (FIM)**, SoftShield efficiently detects threats and anomalies.



Organizations can **customize and configure** these security capabilities to align with their specific security needs, ensuring proactive **threat detection and response.**

File Integrity Monitoring with **SoftShield**

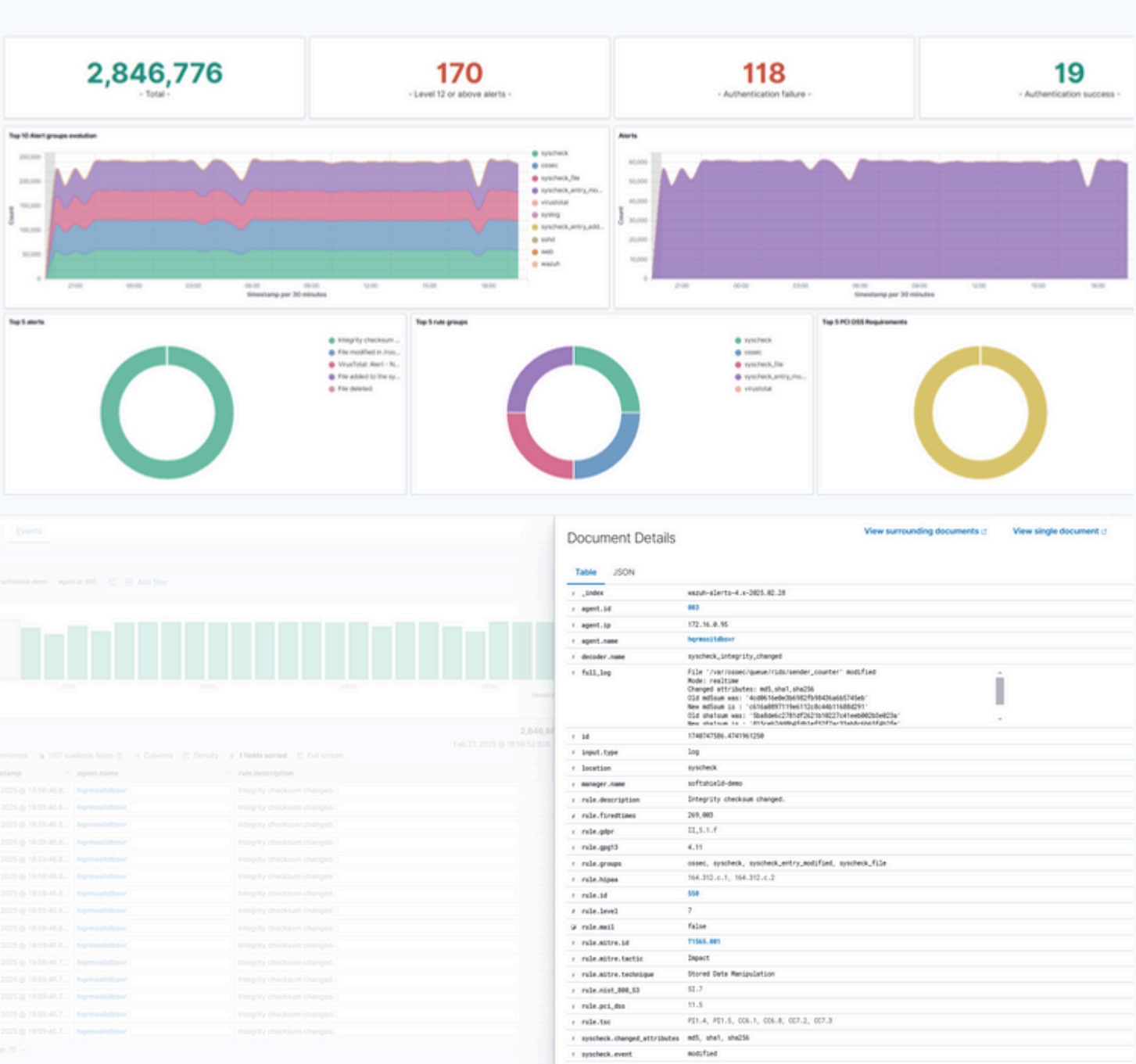
SoftShield continuously monitors file systems, detecting changes in content, permissions, ownership, and attributes of critical files. It also identifies the users and applications responsible for creating or modifying files, providing full visibility into file activities.



By integrating File Integrity Monitoring (FIM) with threat intelligence, **SoftShield** helps detect compromised endpoints and security threats. Additionally, FIM supports regulatory compliance with standards like PCI DSS, NIST, and more, ensuring a secure and well-audited IT environment.

Advanced Threat Hunting with **SoftShield**

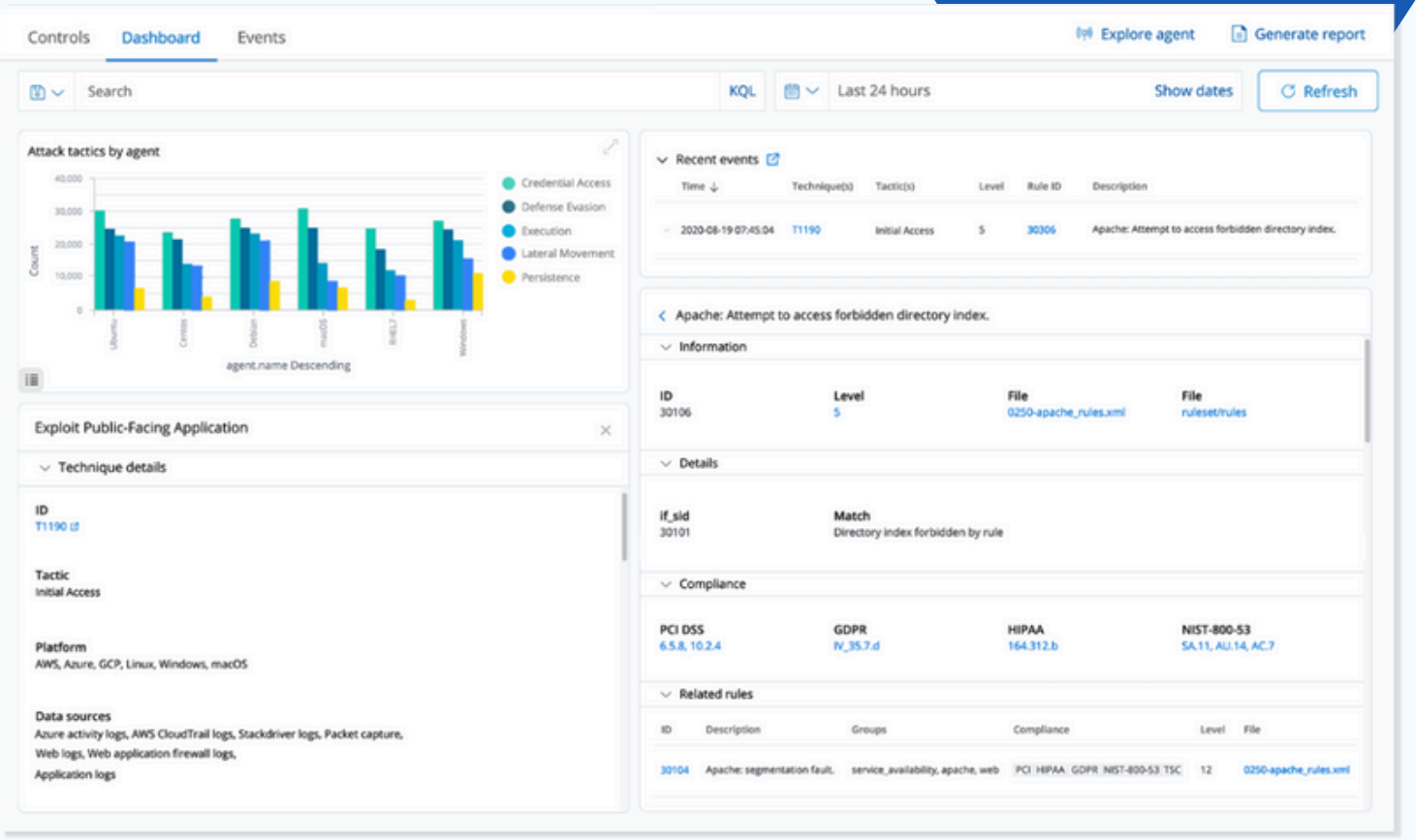
SoftShield provides deep visibility into endpoints and infrastructure, enabling proactive threat investigation. With log retention, indexing, and querying capabilities, SoftShield helps detect threats that may evade initial security controls.



Its threat detection rules align with the MITRE ATT&CK framework, aiding in the identification of attacker tactics, techniques, and procedures (TTPs). Additionally, SoftShield integrates with third-party threat intelligence feeds, enhancing threat hunting and response across your security environment.

Log Data Analysis with **SoftShield**

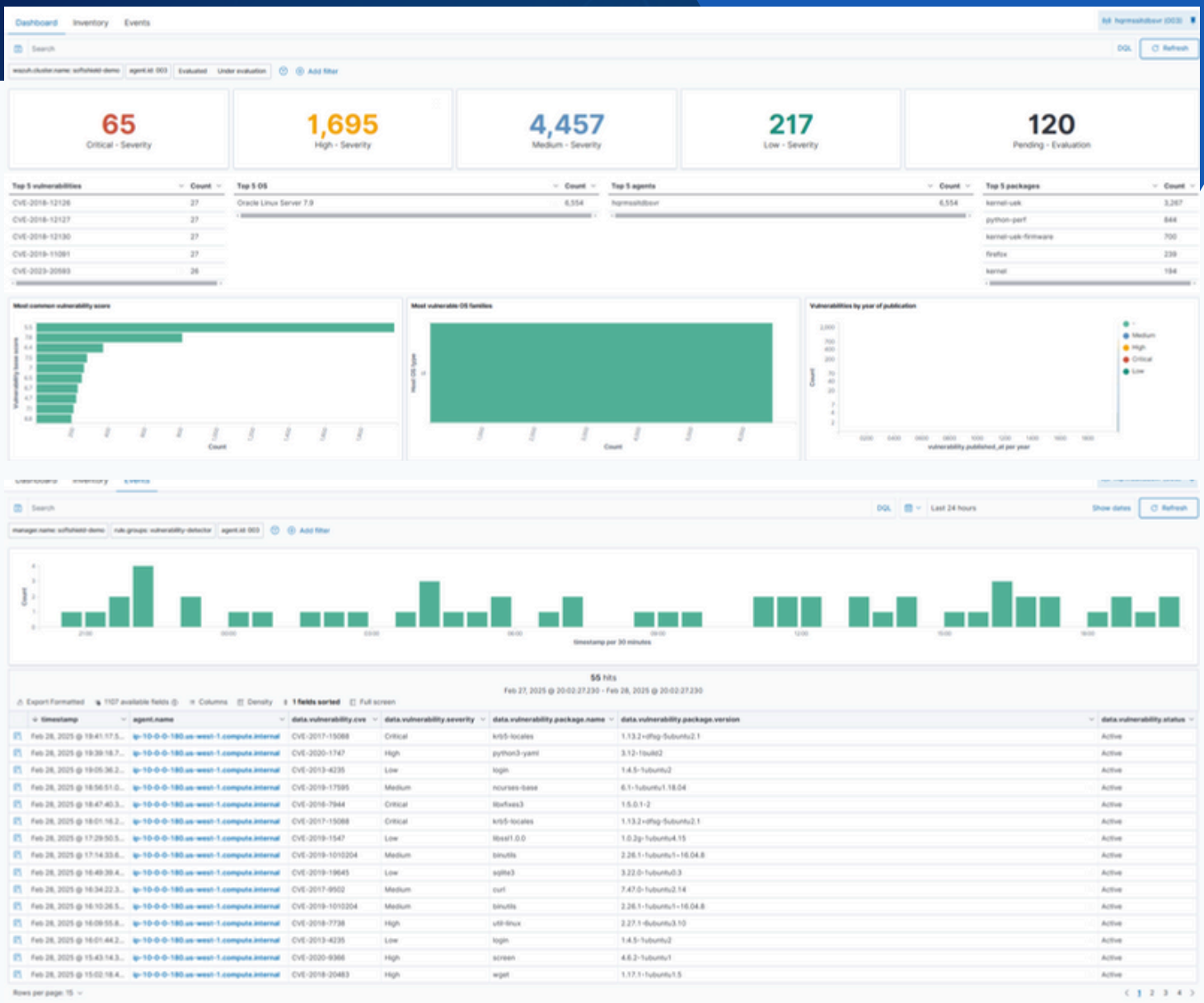
SoftShield collects and analyzes operating system and application logs, securely forwarding them to the SoftShield server for rule-based detection and storage.



Its advanced detection rules identify system errors, misconfigurations, malicious activities, policy violations, and other security or operational issues–ensuring real-time visibility and proactive threat mitigation.

Vulnerability Detection with **SoftShield**

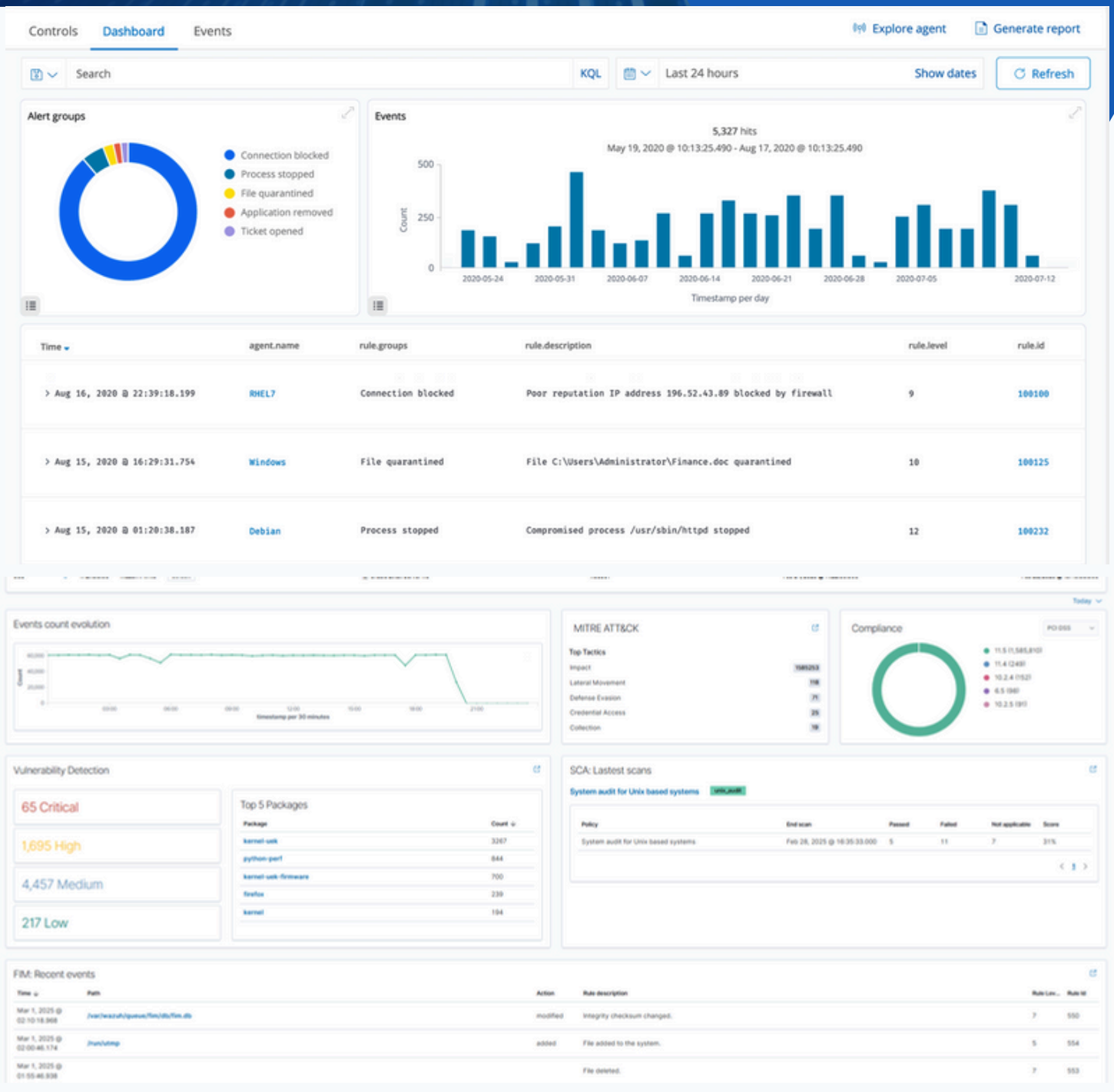
SoftShield automates vulnerability detection by collecting software inventory data and correlating it with continuously updated CVE databases to identify known vulnerabilities.



By proactively detecting flaws in critical assets, **SoftShield** enables organizations to take corrective action before attackers exploit them, strengthening overall security posture

Incident Response with **SoftShield**

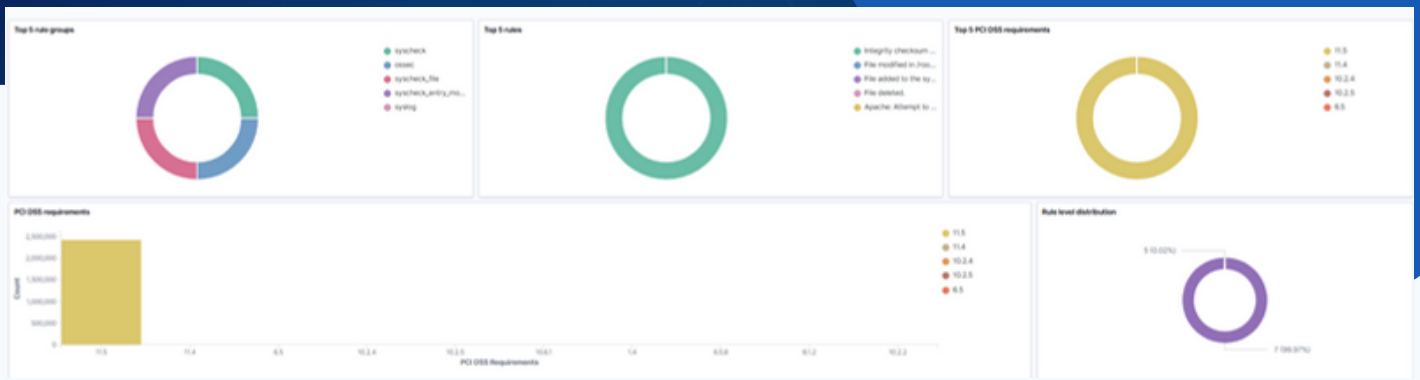
SoftShield delivers automated active responses to counter ongoing threats in real time. When predefined security criteria are met, it can block network access, isolate compromised endpoints, or take other defensive actions.



Additionally, **SoftShield** allows for remote command execution, system queries, and IOC identification, enabling rapid and effective incident response to mitigate security risks.

Reporting insights from SIEM events

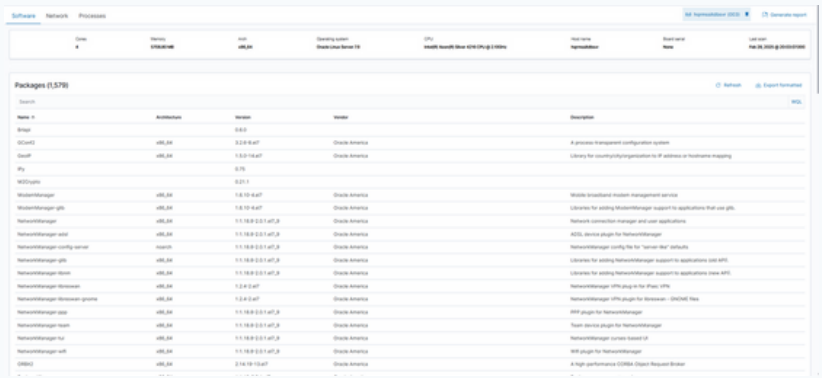
SoftShield generates **detailed security reports** with high-level analysis of SIEM events, providing **actionable insights** tailored to your needs.

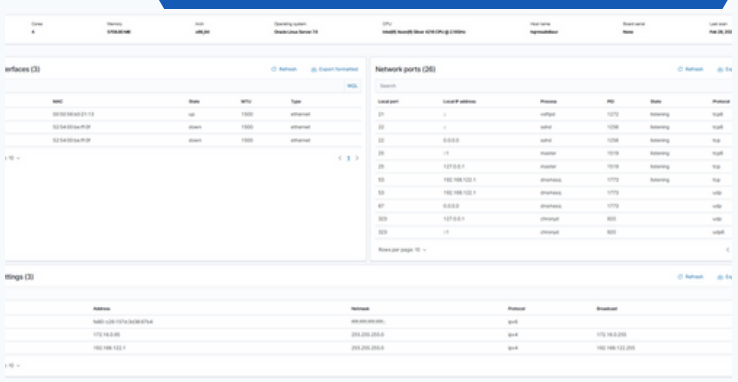


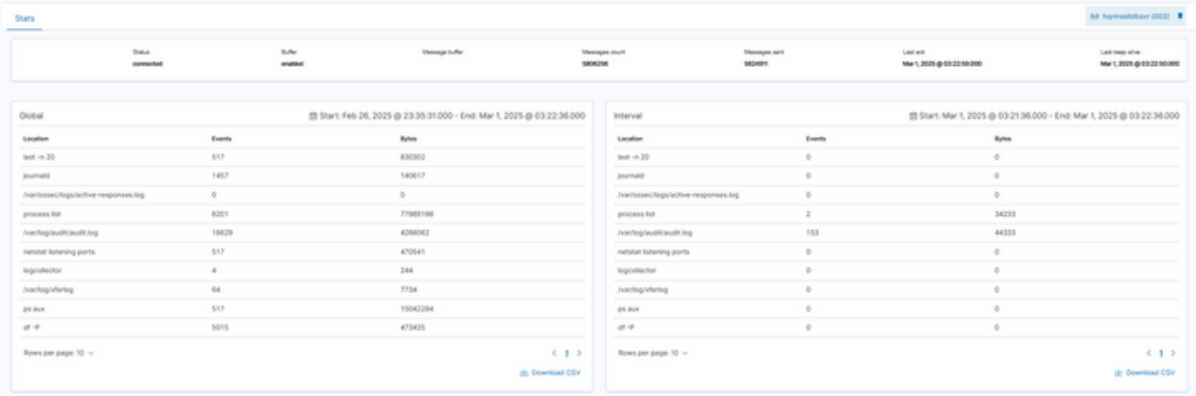
These reports help organizations **detect threats, assess security trends, and demonstrate compliance** with industry regulations and standards—ensuring a well-documented and secure IT environment.

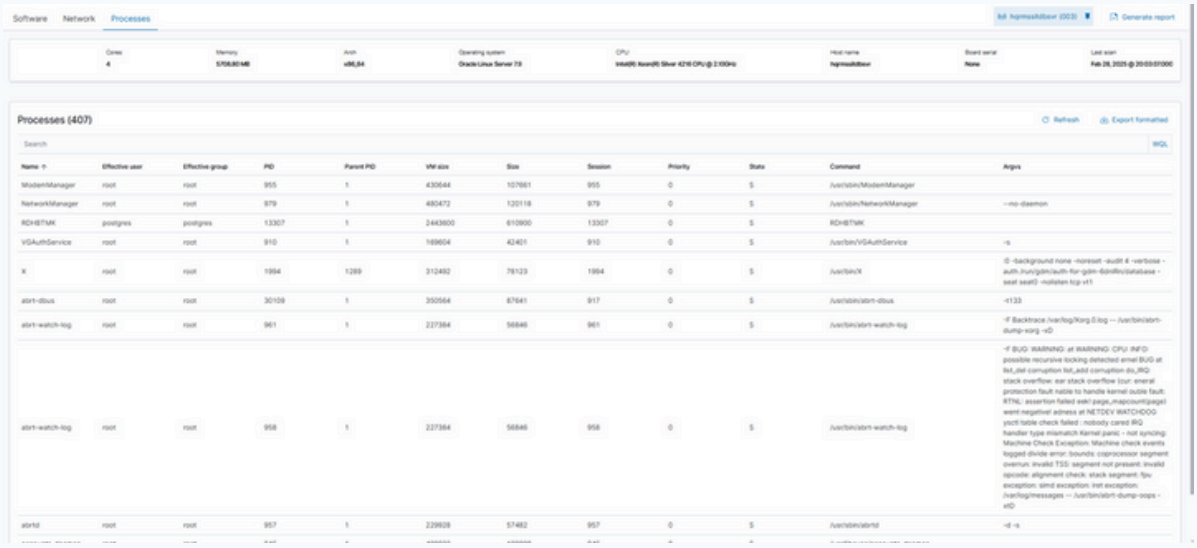
IT Hygiene with **SoftShield**

SoftShield maintains an up-to-date system inventory of all monitored endpoints, tracking installed applications, running processes, open ports, hardware, and OS details. This enhances asset visibility and ensures good IT hygiene across your infrastructure.





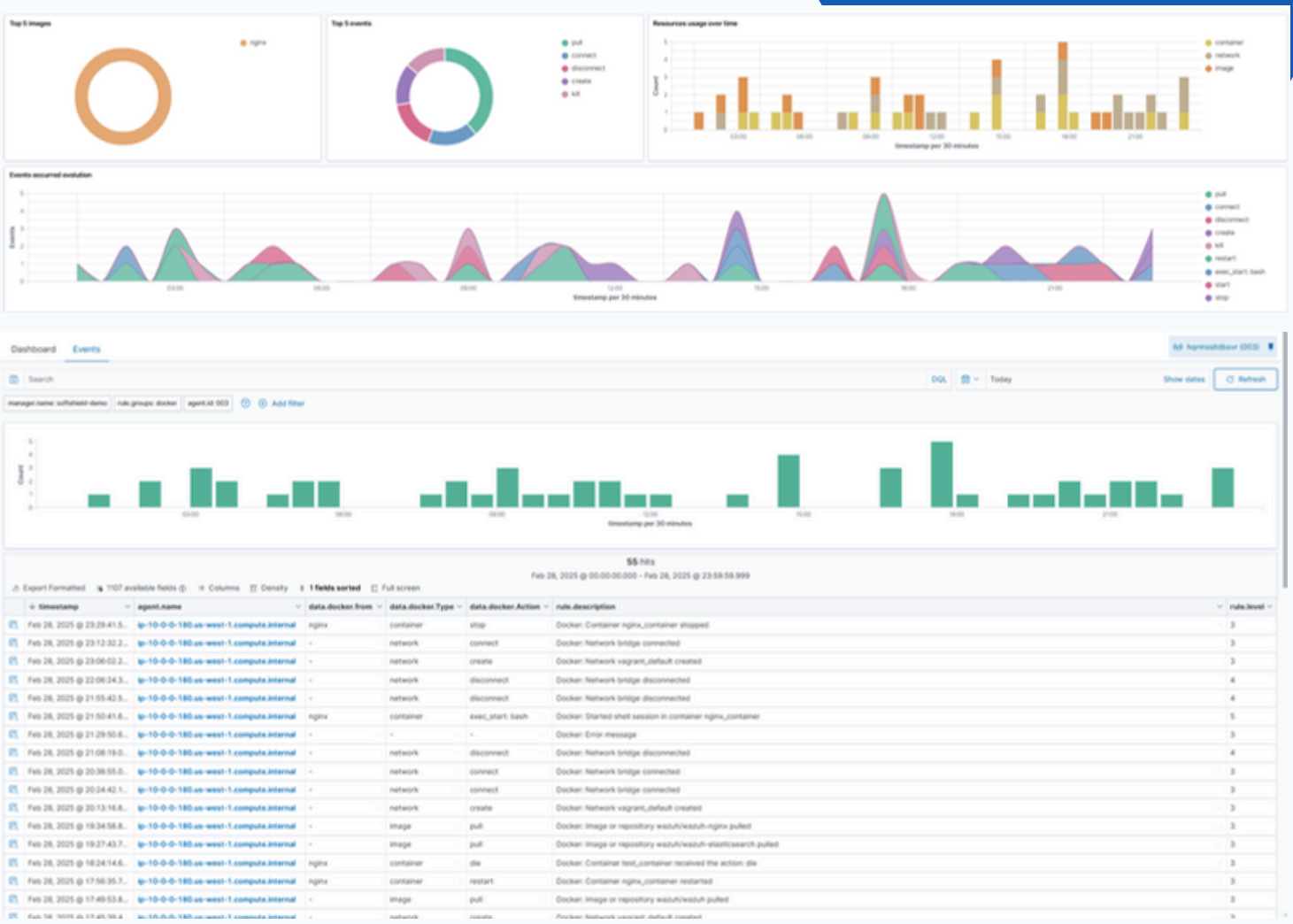




With integrated features like vulnerability detection, Security Configuration Assessment (SCA), and malware detection, SoftShield helps strengthen endpoint security and maintain a clean, well-managed IT environment.

Container Security with **SoftShield**

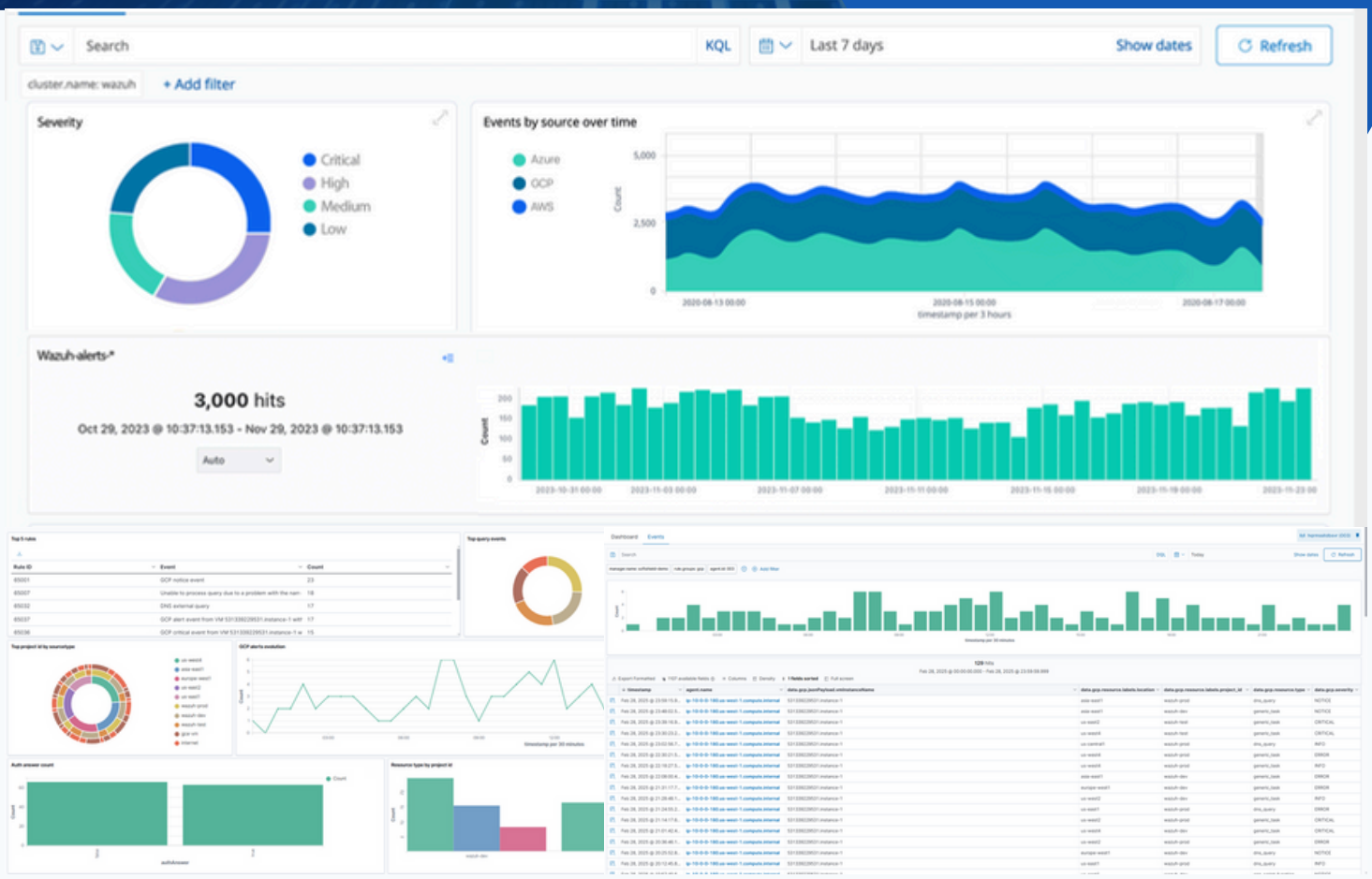
SoftShield enhances security visibility for Docker hosts and containers, monitoring their behavior to detect threats, vulnerabilities, and anomalies. With native integration into the Docker engine, **SoftShield** tracks images, volumes, network settings, and running containers in real time.



By continuously analyzing runtime activity, **SoftShield** detects risks such as privileged containers, vulnerable applications, unauthorized shell access, and changes to persistent volumes or images–ensuring a secure containerized environment.

Security Posture Management with **SoftShield**

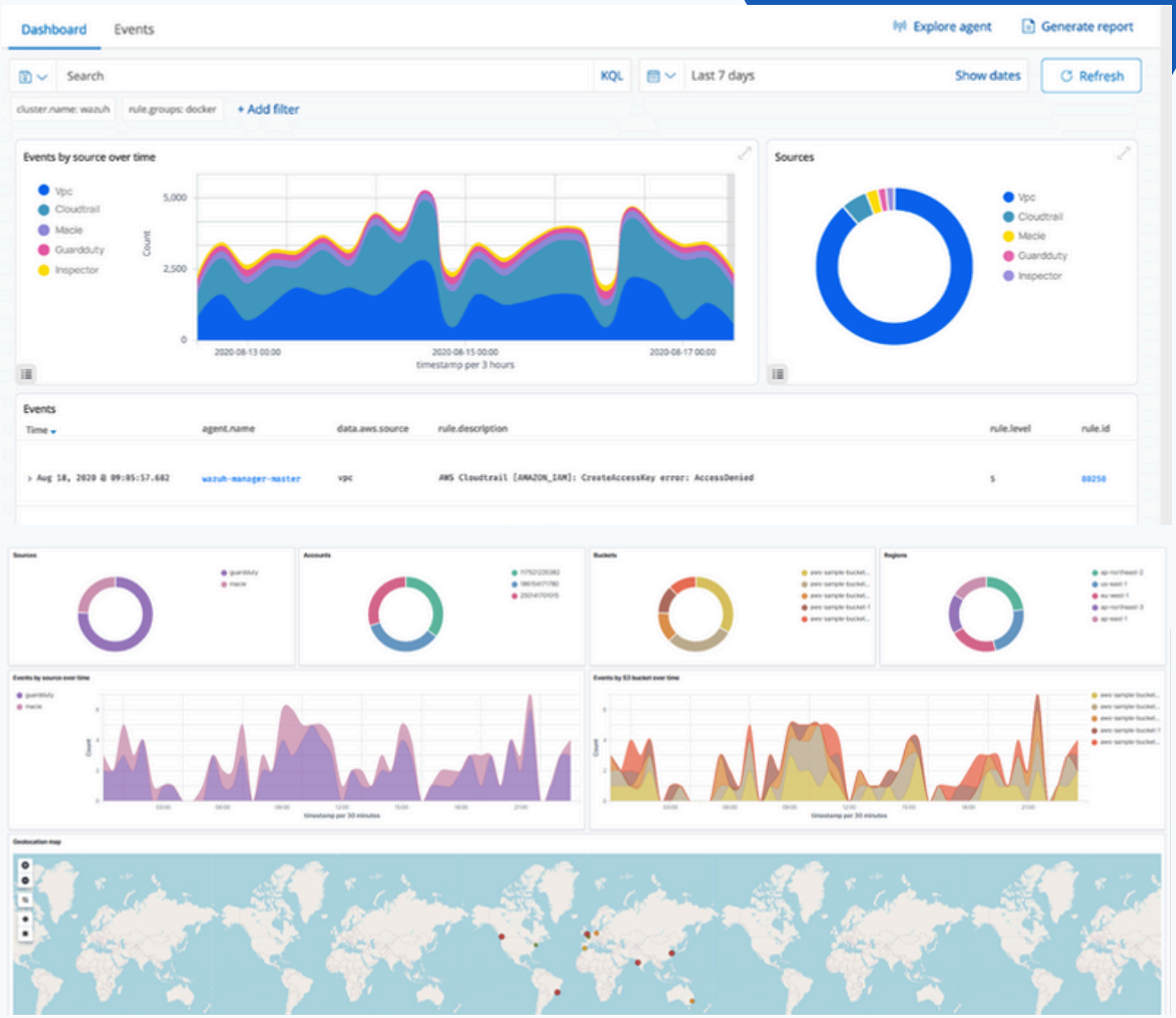
SoftShield integrates with cloud platforms, collecting and analyzing security data to provide real-time visibility into potential risks. It detects security threats and vulnerabilities, ensuring compliance with industry regulations and standards.



With automated alerts and continuous monitoring, **SoftShield** helps organizations strengthen their security posture and proactively mitigate threats.

Workload Protection with **SoftShield**

SoftShield monitors and secures workloads across cloud and on-premises environments, ensuring real-time threat detection and compliance. It integrates with AWS, Microsoft Azure, GCP, Microsoft 365, and GitHub to track services, virtual machines, and platform activities.



With centralized log management, **SoftShield** helps organizations maintain regulatory compliance while securing cloud-based and on-prem workloads against evolving threats.