



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 prerequisites

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)

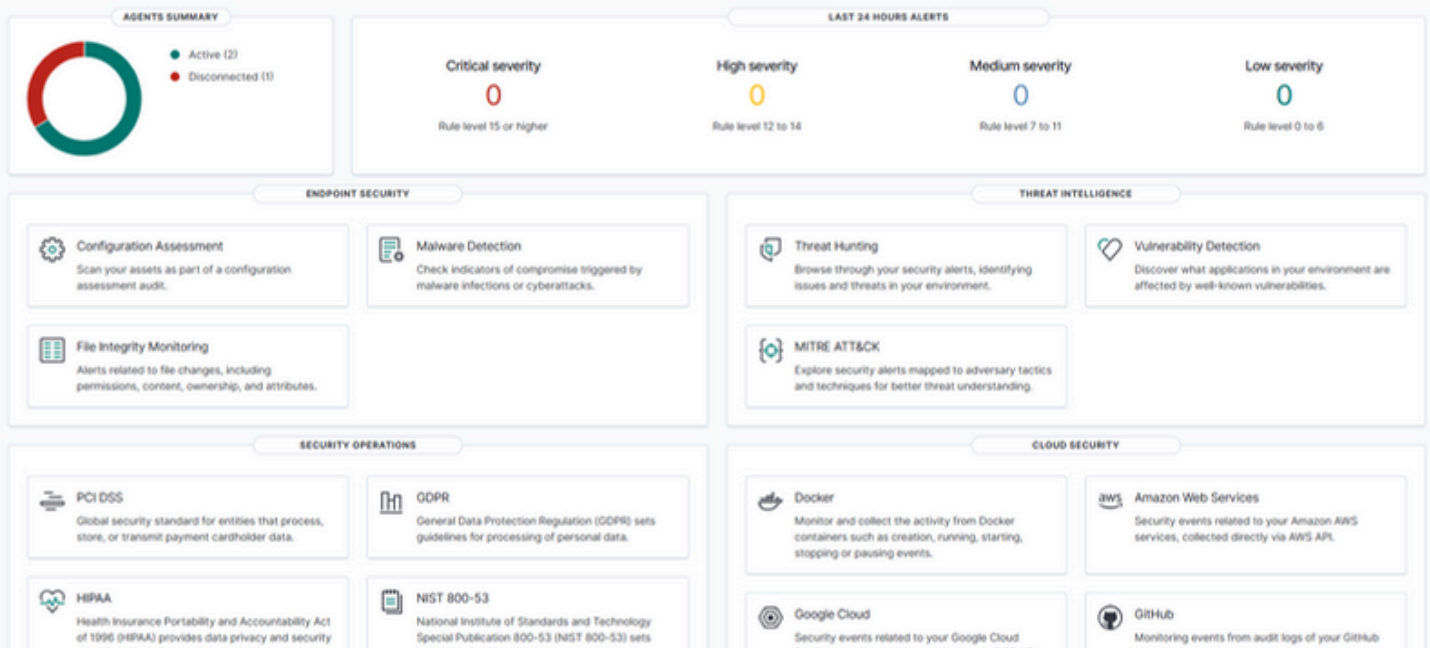
CPU	8 Core CPU
RAM	8 GB
Disk Space	100 GB
OS	Ubuntu

Large (50-100 Agents)

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

Security Configuration Assessment (SCA) with SoftShield

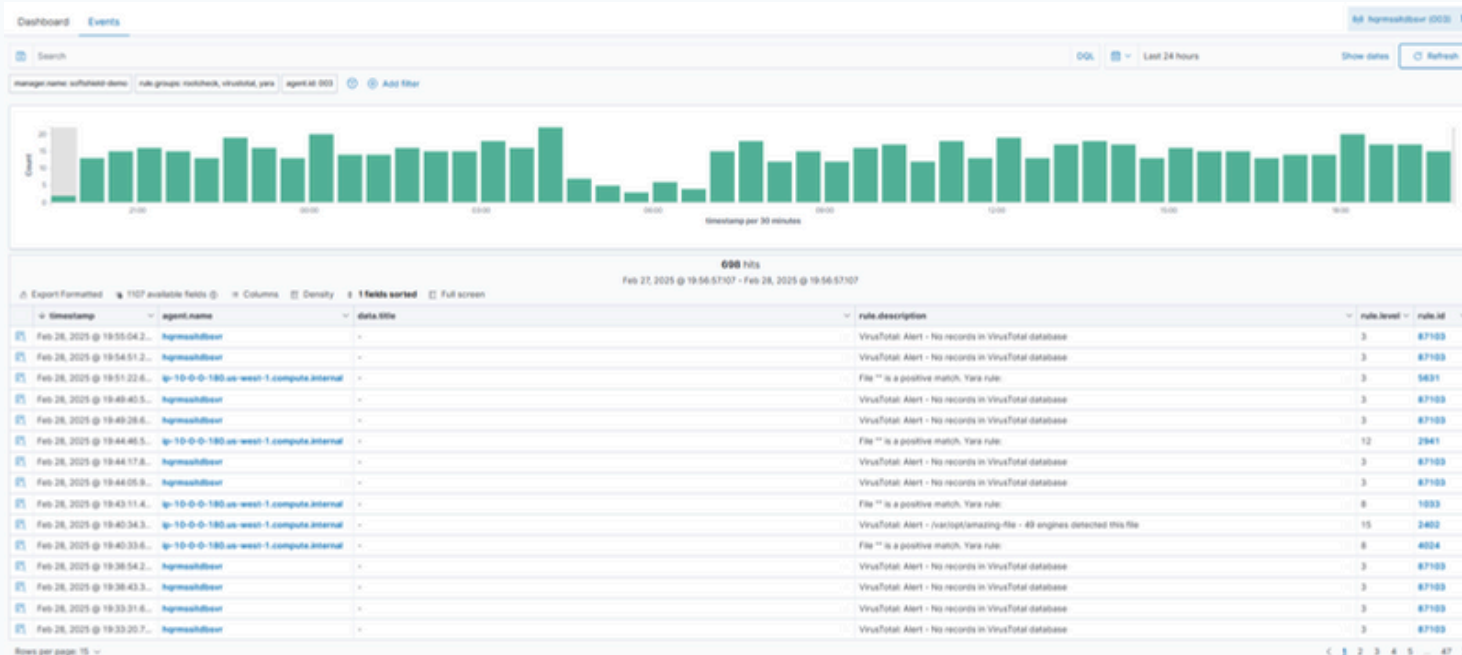
SoftShield continuously monitors **system and application configurations** to ensure compliance with **security policies, industry standards**, and hardening guidelines. Its agents perform regular scans to detect misconfigurations and security gaps that could be exploited by threats.



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

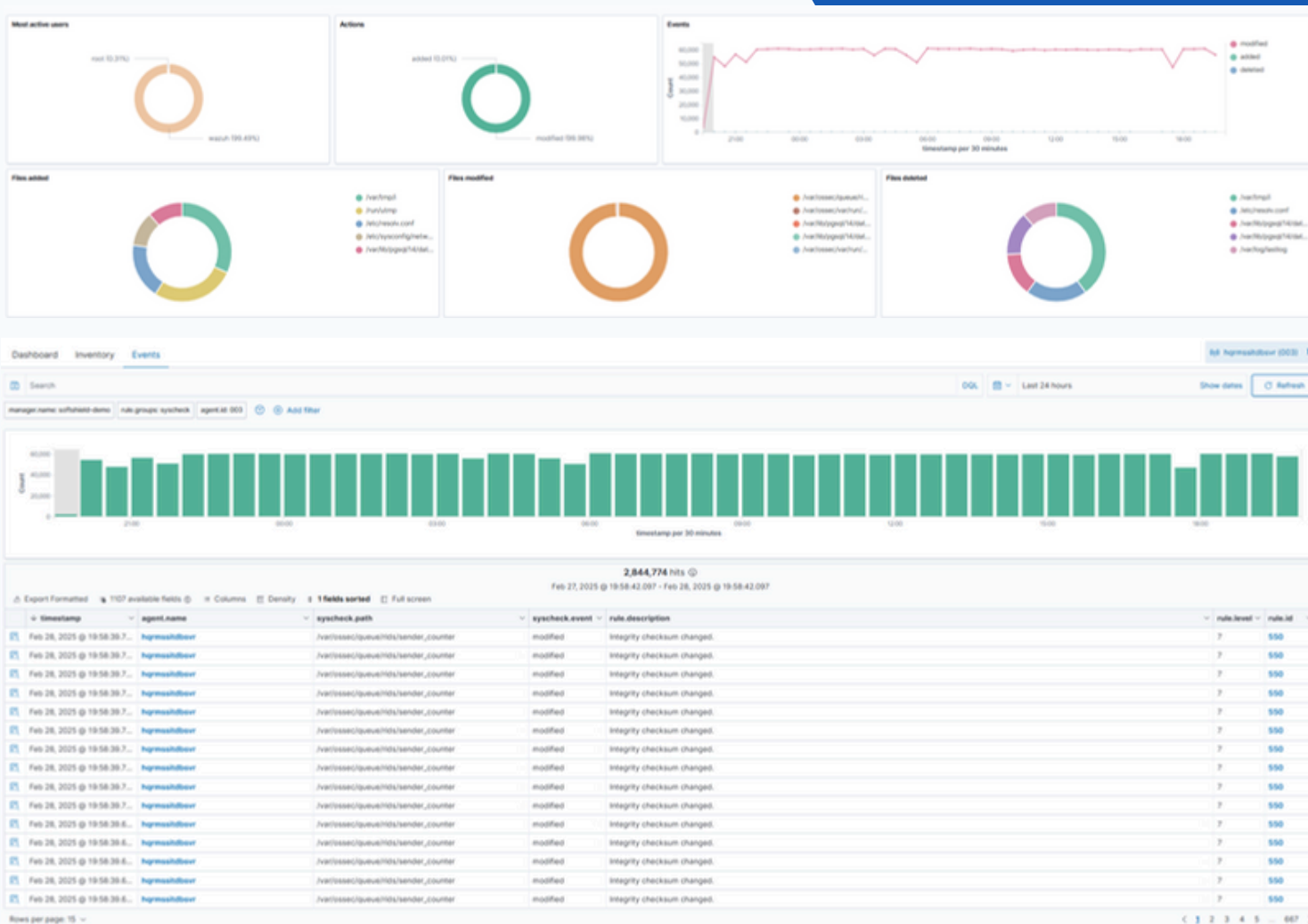
SoftShield identifies malicious activities and indicators of compromise (IoCs) caused by malware infections or cyberattacks on endpoints. With built-in security rules and features like Security Configuration Assessment (SCA), Rootcheck, and File Integrity Monitoring (FIM), SoftShield efficiently detects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



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

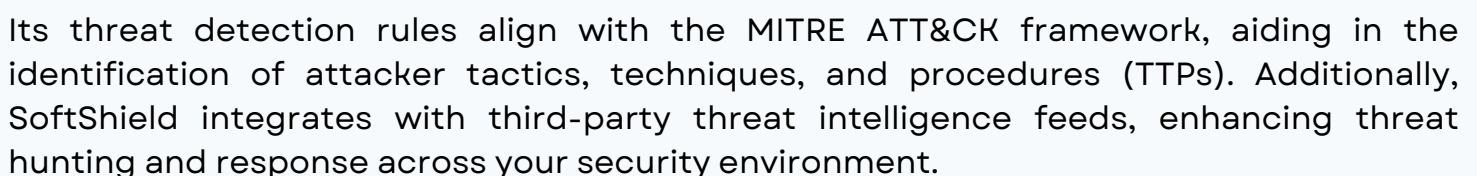
File Integrity Monitoring with **SoftShield**

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.



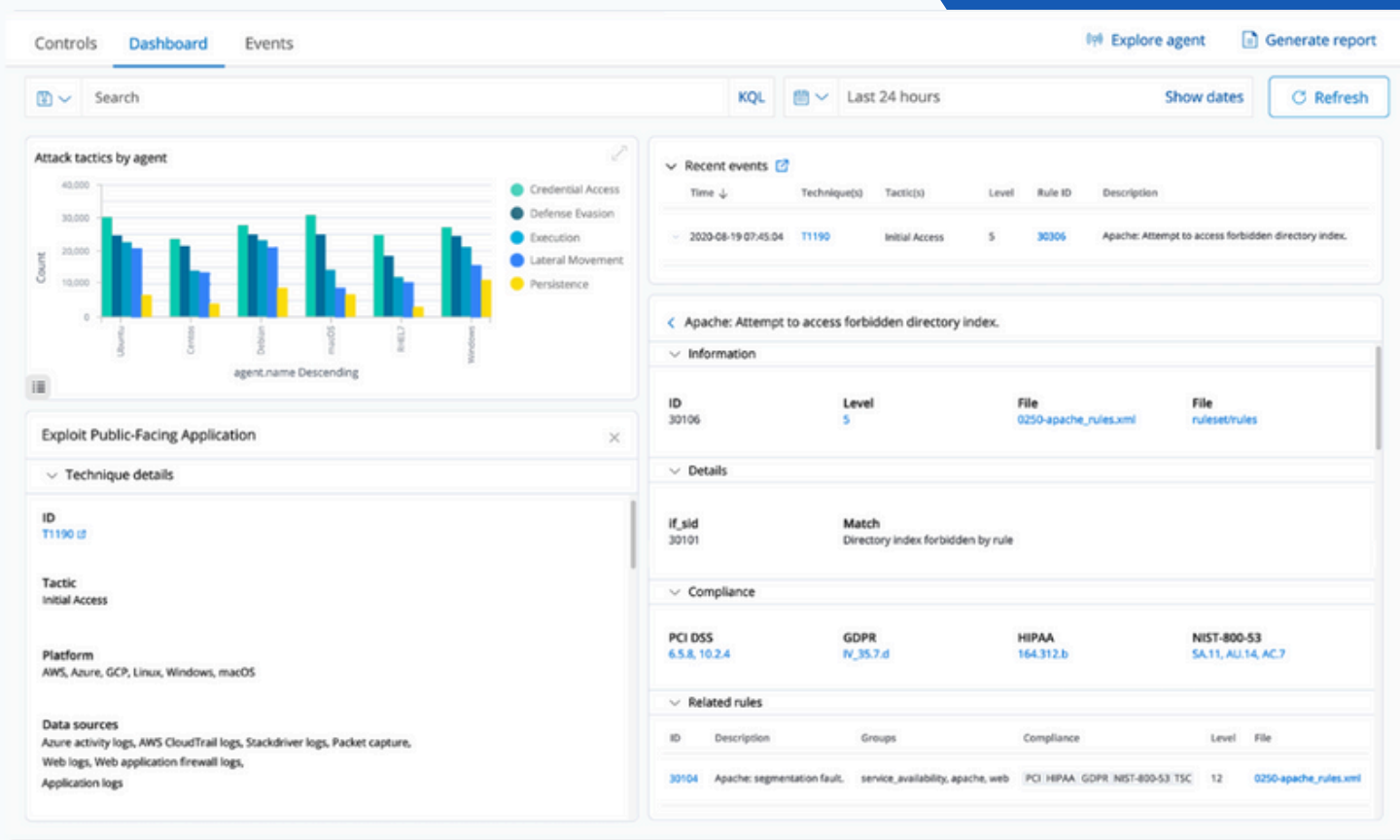
By integrating File Integrity Monitoring (FIM) with threat intelligence, **SoftShield** helps detect compromised endpoints and security threats. Additionally, FIM supports regulatory compliance with standards like PCI DSS, NIST, and more, ensuring a secure and well-audited IT environment.

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.



Log Data Analysis with SoftShield

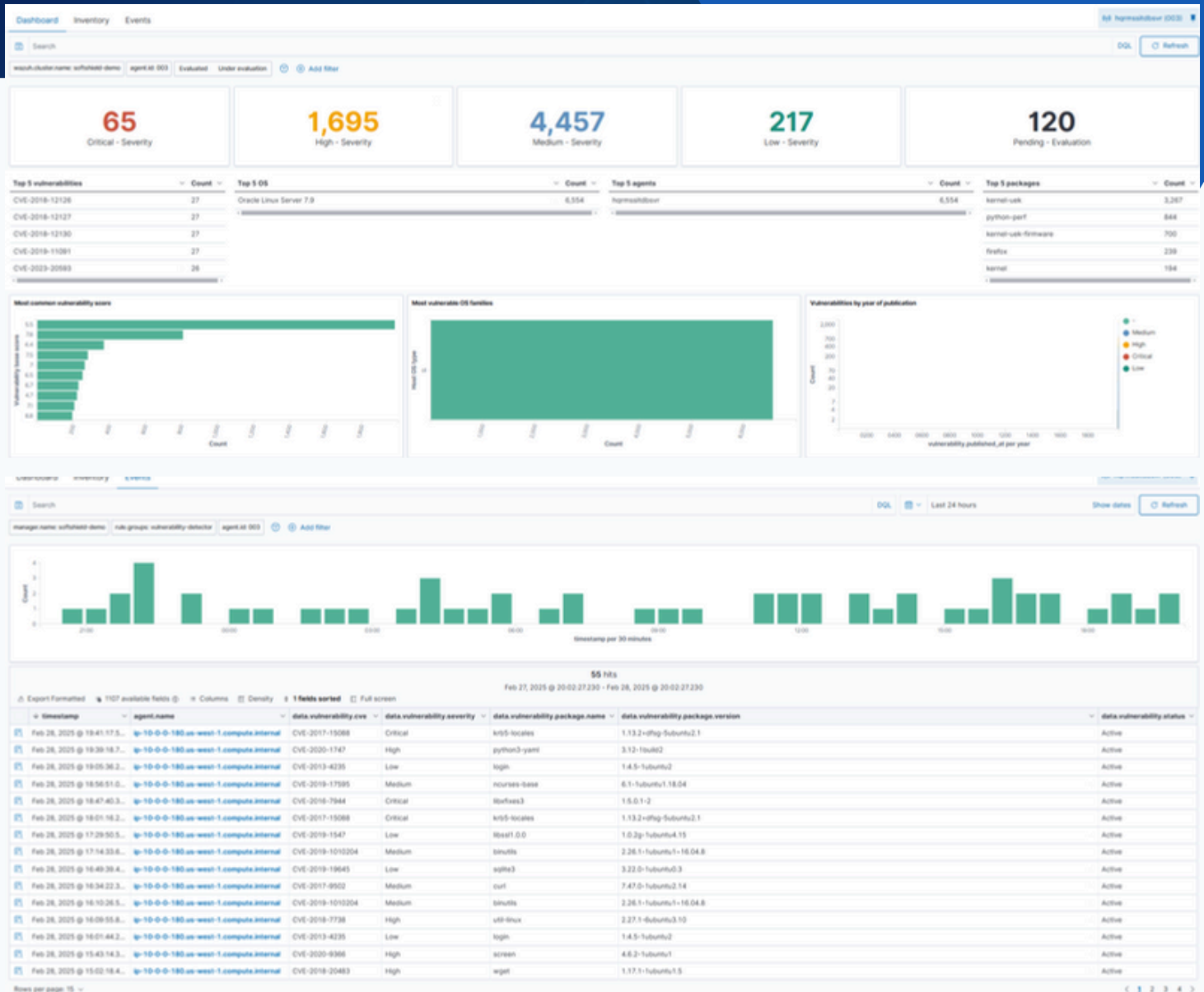
SoftShield collects and analyzes operating system and application logs, securely forwarding them to the SoftShield server for rule-based detection and storage.



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

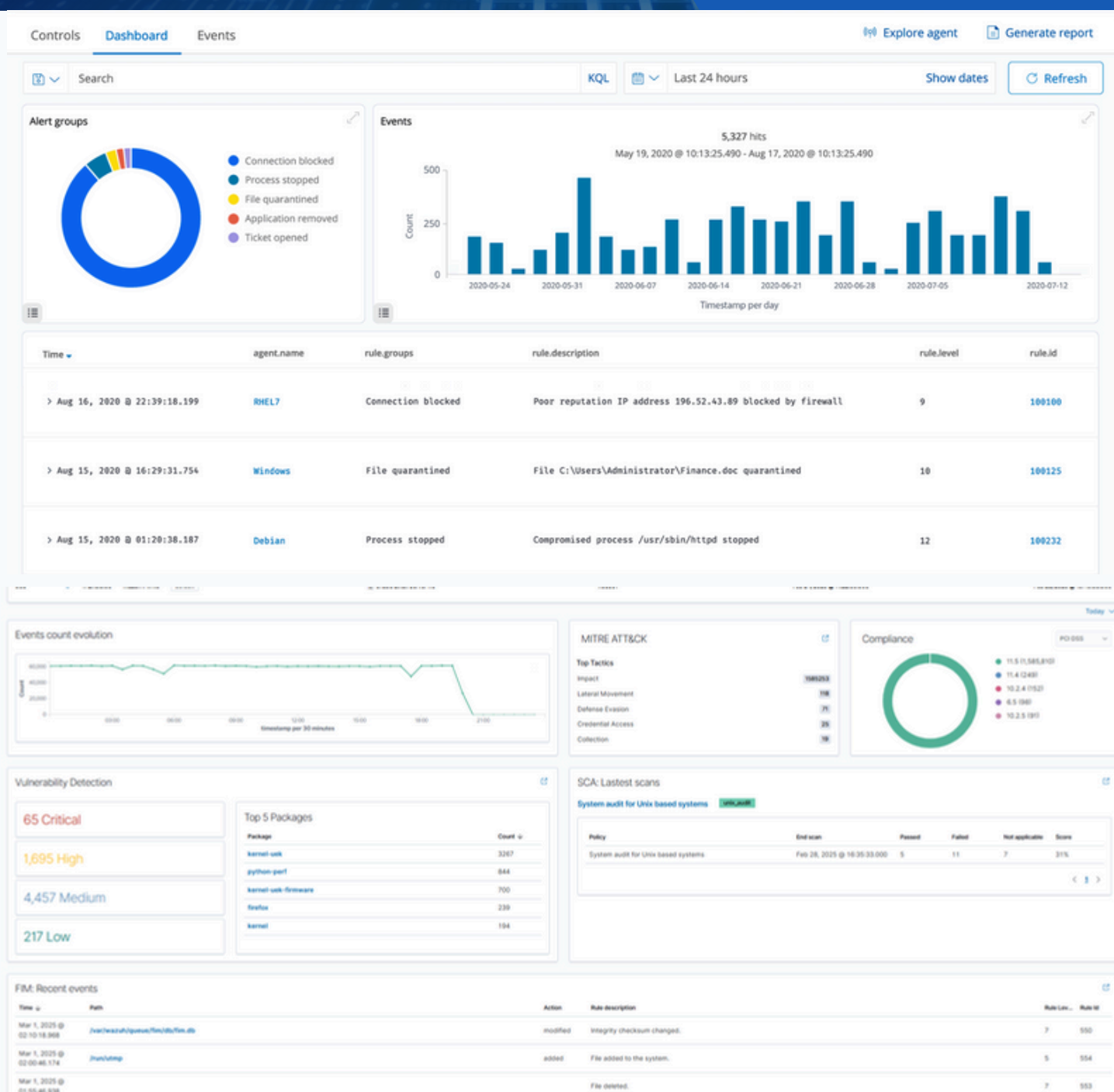
SoftShield automates vulnerability detection by collecting software inventory data and correlating it with continuously updated CVE databases to identify known vulnerabilities.



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

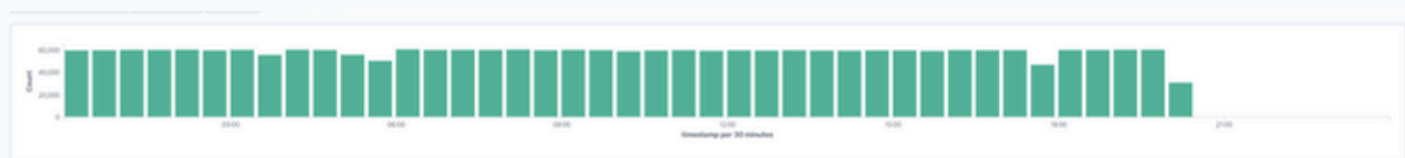
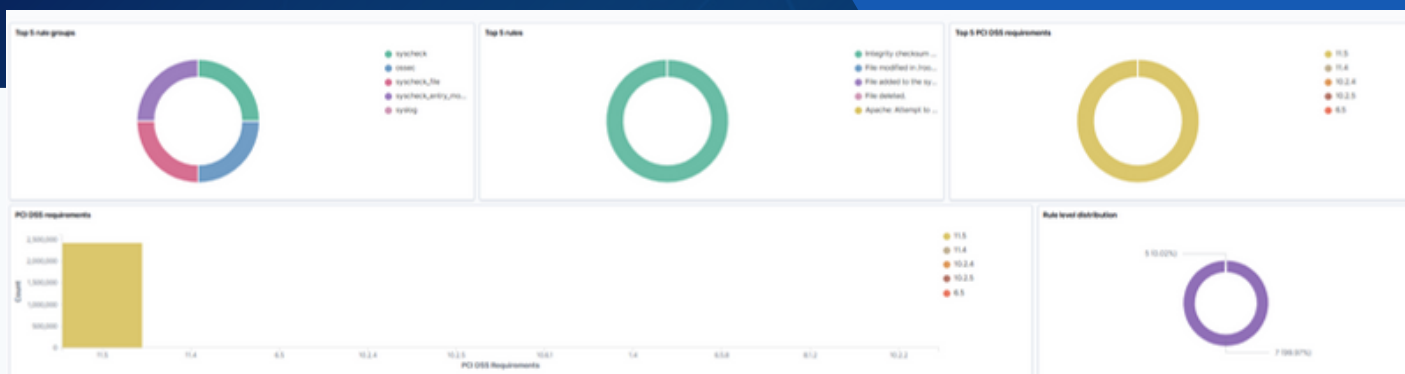
SoftShield delivers automated active responses to counter ongoing threats in real time. When predefined security criteria are met, it can block network access, isolate compromised endpoints, or take other defensive actions.



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.



2,433,054 hits

Feb 26, 2025 @ 00:00:00.000 - Feb 26, 2025 @ 23:59:59.999

timestamp	agent_name	rule_id	rule_desc	rule_level	rule_id
Feb 26, 2025 @ 23:58:05.7	ip-10-0-0-180-us-west-1.compute.internal	6.5, 11.4	Web server 400 error code.	5	31101
Feb 26, 2025 @ 23:58:03.3	ip-10-0-0-180-us-west-1.compute.internal	10.2.4, 10.2.5, 10.8.1	ssh: Attempt to login using a non-existent user.	5	5710
Feb 26, 2025 @ 23:54:37.3	ip-10-0-0-180-us-west-1.compute.internal	11.5	File added to the system.	5	554
Feb 26, 2025 @ 23:54:04.9	ip-10-0-0-180-us-west-1.compute.internal	2.2	OpenSCAP: Record Attempts to Alter Login and Logout Events (not passed)	7	81530
Feb 26, 2025 @ 23:53:44.5	ip-10-0-0-180-us-west-1.compute.internal	2.2	OpenSCAP: Set Password Minimum Length (not passed)	7	81530
Feb 26, 2025 @ 23:53:31.2	ip-10-0-0-180-us-west-1.compute.internal	2.2	OpenSCAP: Set Password Minimum Length (not passed)	7	81530
Feb 26, 2025 @ 23:47:49.7	ip-10-0-0-180-us-west-1.compute.internal	6.5, 11.4	Web server 400 error code.	5	31101
Feb 26, 2025 @ 23:43:16.5	ip-10-0-0-180-us-west-1.compute.internal	11.5	File added to the system.	5	554
Feb 26, 2025 @ 23:40:35.2	ip-10-0-0-180-us-west-1.compute.internal	6.5, 11.4	Web server 400 error code.	5	31101
Feb 26, 2025 @ 23:35:58.8	ip-10-0-0-180-us-west-1.compute.internal	1.4, 10.6.1	Netscreen Erase sequence started.	11	4505
Feb 26, 2025 @ 23:34:38.0	ip-10-0-0-180-us-west-1.compute.internal	11.4	ssh: Reverse lookup error (bad IP or attack).	5	5702
Feb 26, 2025 @ 23:33:56.5	ip-10-0-0-180-us-west-1.compute.internal	6.5, 10.2.4	Apache: Attempt to access forbidden directory index.	5	30306
Feb 26, 2025 @ 23:33:49.9	ip-10-0-0-180-us-west-1.compute.internal	11.4	ssh: Possible broken attempt (high number of reverse lookup errors).	10	5703
Feb 26, 2025 @ 23:32:18.6	ip-10-0-0-180-us-west-1.compute.internal	10.2.4	syslog: Connection blocked by Top Wrappers.	5	2503
Feb 26, 2025 @ 23:31:25.4	ip-10-0-0-180-us-west-1.compute.internal	11.5	Integrity checksum changed.	7	550
Feb 26, 2025 @ 23:28:57.8	ip-10-0-0-180-us-west-1.compute.internal	11.5	File deleted.	7	553

Feb 26, 2025 @ 23:33:08.3	ip-10-0-0-180-us-west-1.compute.internal	6.5, 10.2.4	Apache: Attempt to access forbidden directory index.	5	30306
Feb 26, 2025 @ 23:33:49.9	ip-10-0-0-180-us-west-1.compute.internal	11.4	ssh: Possible broken attempt (high number of reverse lookup errors).	10	5703
Feb 26, 2025 @ 23:32:18.6	ip-10-0-0-180-us-west-1.compute.internal	10.2.4	syslog: Connection blocked by Top Wrappers.	5	2503
Feb 26, 2025 @ 23:31:25.4	ip-10-0-0-180-us-west-1.compute.internal	11.5	Integrity checksum changed.	7	550
Feb 26, 2025 @ 23:28:57.8	ip-10-0-0-180-us-west-1.compute.internal	11.5	File deleted.	7	553
Feb 26, 2025 @ 23:27:02.7	ip-10-0-0-180-us-west-1.compute.internal	10.4	ssh: Possible attack on the ssh server (or version gathering).	5	5702
Feb 26, 2025 @ 23:26:05.5	ip-10-0-0-180-us-west-1.compute.internal	11.4	ssh: Possible broken attempt (high number of reverse lookup errors).	10	5703
Feb 26, 2025 @ 23:25:43.0	ip-10-0-0-180-us-west-1.compute.internal	11.4	ssh: Possible broken attempt (high number of reverse lookup errors).	10	5703
Feb 26, 2025 @ 23:25:17.2	ip-10-0-0-180-us-west-1.compute.internal	10.2.4, 10.2.5, 11.4	ssh: Multiple authentication failures.	5	5702
Feb 26, 2025 @ 23:23:05.1	ip-10-0-0-180-us-west-1.compute.internal	10.2	ssh: Possible broken attempt (high number of reverse lookup errors).	10	5703
Feb 26, 2025 @ 23:19:28.8	ip-10-0-0-180-us-west-1.compute.internal	6.5, 11.4	Multiple web server 400 error codes from same source ip.	5	31101
Feb 26, 2025 @ 23:18:58.3	ip-10-0-0-180-us-west-1.compute.internal	11.5	File deleted.	7	553
Feb 26, 2025 @ 23:15:47.8	ip-10-0-0-180-us-west-1.compute.internal	6.5, 11.4	Web server 400 error code.	5	31101
Feb 26, 2025 @ 23:13:01.3	ip-10-0-0-180-us-west-1.compute.internal	6.5, 11.4	Web server 400 error code.	5	31101
Feb 26, 2025 @ 23:08:36.8	ip-10-0-0-180-us-west-1.compute.internal	2.2	OpenSCAP: Audit and Connect File Permissions with RPM (not passed)	7	81530
Feb 26, 2025 @ 23:04:00.9	ip-10-0-0-180-us-west-1.compute.internal	11.4	ssh: Insecure connection attempt (bad).	5	5702
Feb 26, 2025 @ 23:03:03.2	ip-10-0-0-180-us-west-1.compute.internal	10.2.7	Snapper Network segment (default created)	5	5702
Feb 26, 2025 @ 23:03:06.1	ip-10-0-0-180-us-west-1.compute.internal	11.4	ssh: Possible broken attempt (high number of reverse lookup errors).	10	5703
Feb 26, 2025 @ 23:03:11.8	ip-10-0-0-180-us-west-1.compute.internal	6.5, 11.4	Web server 400 error code.	5	31101
Feb 26, 2025 @ 23:03:06.9	ip-10-0-0-180-us-west-1.compute.internal	11.5	Integrity checksum changed.	7	550
Feb 26, 2025 @ 23:03:04.8	ip-10-0-0-180-us-west-1.compute.internal	6.5, 10.2.4	Apache: Attempt to access forbidden directory index.	5	30306

```
{  "location.region_name": "Bomby",  "index": "secu-alerts-4-a-sample-security",  "agent_id": "803",  "agent_ip": "10.0.0.180",  "cluster_name": "ip-10-0-0-180-us-west-1.compute.internal",  "decoder_name": "ssh",  "data.timestamp": "2025-02-26T23:27:02.700Z",  "data.source": "10.0.0.180",  "data.destination": "10.0.0.180",  "decoder.parent": "ssh",  "full_log": "Feb 26 23:27:02 softshield-demo ssh[1023]: Bad protocol version identification '000' from 10.0.0.180 port 50047",  "id": "158012327.49801",  "input_type": "log",  "location": "/var/log/secure",  "manager.name": "softshield-demo",  "predecoder.hostname": "softshield-demo",  "predecoder.program_name": "ssh",  "predecoder.timestamp": "Feb 26 23:27:02",  "rule.description": "ssh: Possible attack on the ssh server (or version gathering).",  "rule.firetimes": "10",  "rule.gid": "30_35_7-0"}
```

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.

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.

Software

Network

Processes

Get Appraisal Report (2023)

Generate report

Core 4	Memory 5705.81 MB	cpu 48.84	Operating system Oracle Linux Server 7.9	CPU 9400% (total) 51w 421s CPU @ 2.50Hz	Host name kymahost01	Build serial None	Last seen Feb 28, 2025 @ 20:03:01 (UTC)
--------	-------------------	-----------	--	---	----------------------	-------------------	---

Processes (407)

Refresh

Export formatted

SQL

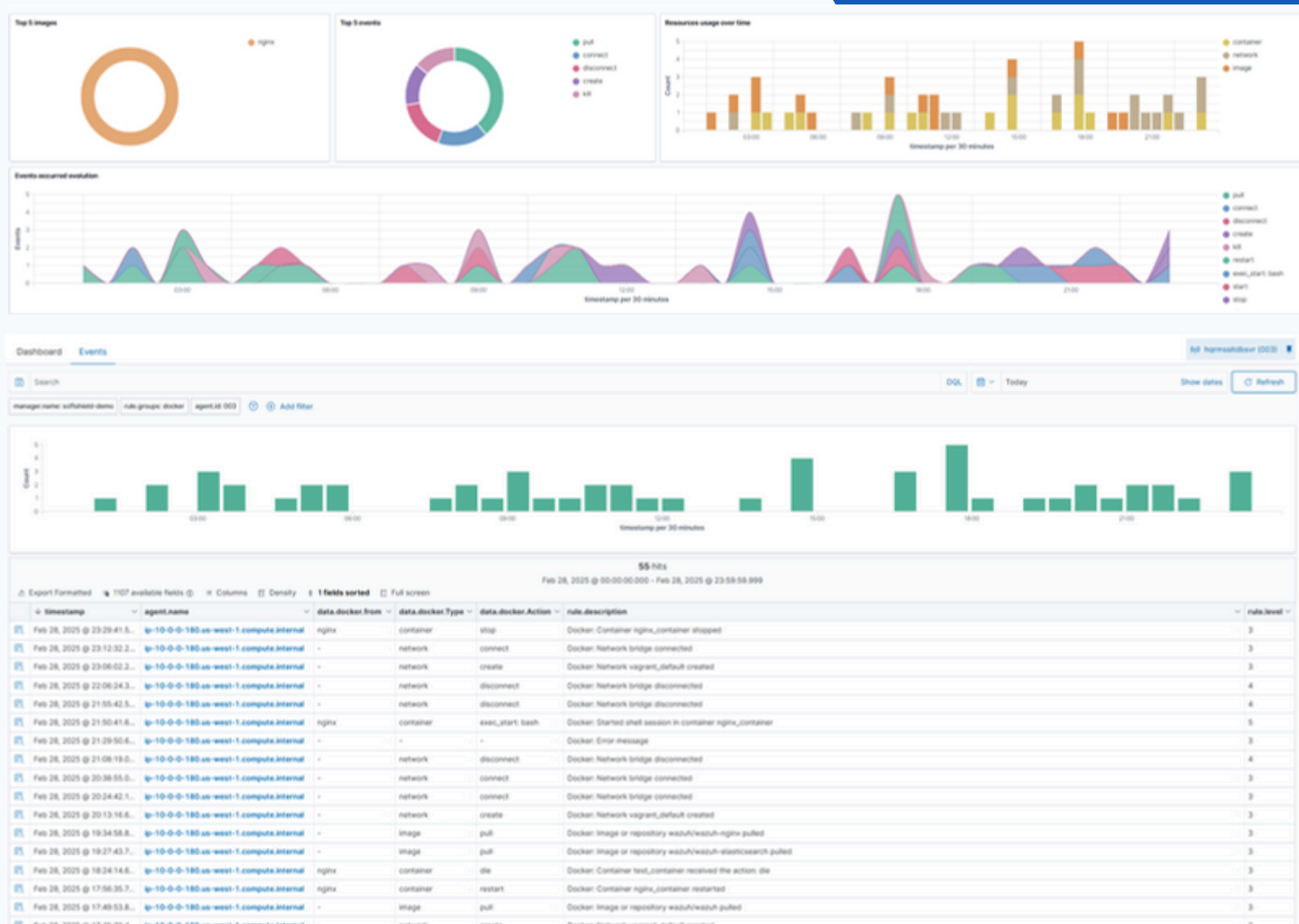
Search

Name ↑	Effective user	Effective group	PID	Parent PID	VM size	Size	Session	Priority	Status	Command	Args
ModemManager	root	root	955	1	430644	107681	955	0	S	/usr/bin/ModemManager	
NetworkManager	root	root	979	1	480472	120116	979	0	S	/usr/bin/NetworkManager	--no-daemon
ICM@TAK	postgress	postgress	13307	1	2443600	610900	13307	0	S	ICM@TAK	
VGAAuthService	root	root	910	1	169604	42401	910	0	S	/usr/bin/VGAAuthService	-s
X	root	root	1994	1289	312482	78123	1994	0	S	/usr/bin/X	-D -background none -noreset -audit 0 -verbose -auth /usr/bin/xauth for gdm-doas/database - root wait -nolisten tcp -vs
start-dbus	root	root	30109	1	390564	87561	917	0	S	/usr/bin/start-dbus	-i32
start-watch-log	root	root	961	1	227384	56846	961	0	S	/usr/bin/start-watch-log	-f Backtrace /usr/log/klog 0 log -- /usr/bin/start-dump-syslog -d
start-watch-log	root	root	958	1	227384	56846	958	0	S	/usr/bin/start-watch-log	-f BUG: nullified at matched CPU info:0 possible recursive locking detected error BUG at kMtel corruption kMtel_add corruption do_IRQ stack overflow: var stack overflow (var: error) protection fault: unable to handle kernel stack fault #TNE assertion failed exit: page_mapcount(page) went negative address at NETDEV WATCHDOG port table check failed: invalid canal IRQ handler type mismatch kernel panic - not syncing Machine Check Exception: Machine check events logged divide error: bounds comparison segment overrun: invalid TSS: segment not present: invalid opcode alignment check: stack segment /fn exception: simd exception: int exception: /usr/log/messages -- /usr/bin/start-dump-syslog -d
startd	root	root	957	1	229628	57482	957	0	S	/usr/bin/startd	-d -s

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

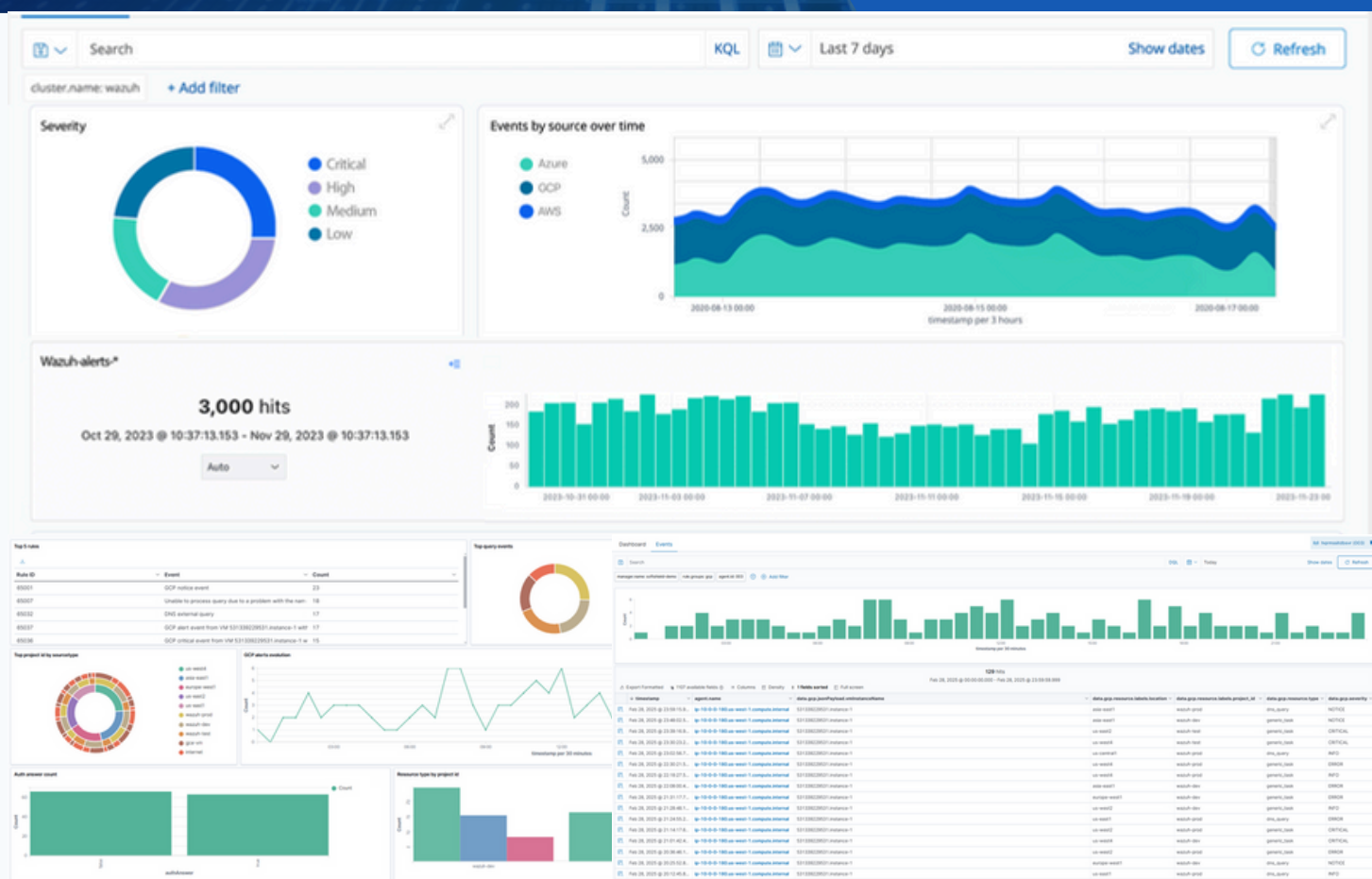
SoftShield enhances security visibility for Docker hosts and containers, monitoring their behavior to detect threats, vulnerabilities, and anomalies. With native integration into the Docker engine, **SoftShield** tracks images, volumes, network settings, and running containers in real time.



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**

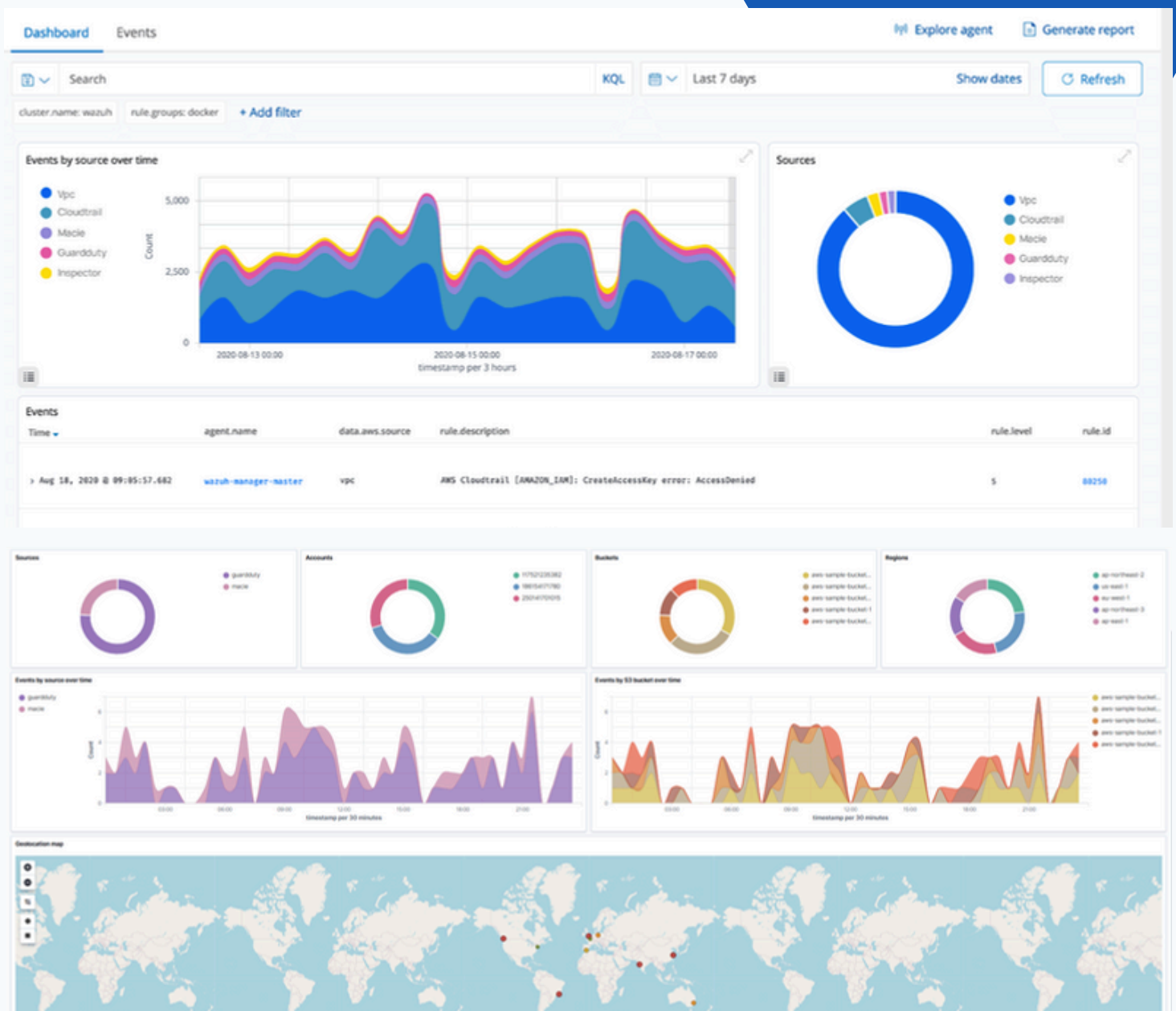
SoftShield integrates with cloud platforms, collecting and analyzing security data to provide real-time visibility into potential risks. It detects security threats and vulnerabilities, ensuring compliance with industry regulations and standards.



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.