

guardsix SIEM



OTD BİLİŞİM

GLOBAL VAD

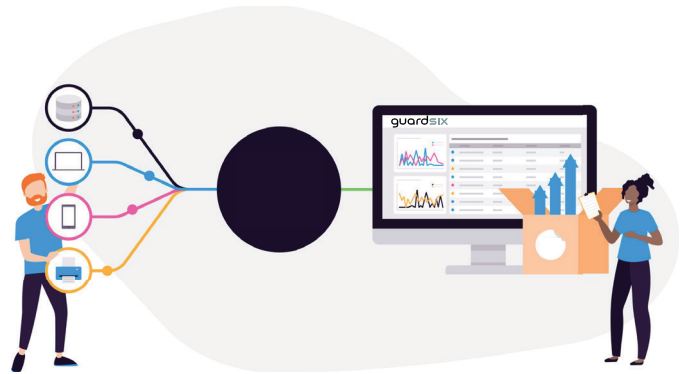
USE CASE GUIDE: GUARDSIX SIEM

Guardsix's latest release for Guardsix SIEM comes with new features designed to optimize security operations, Mean Time to Respond (MTTR), threat hunting, and log collection. Overall, Guardsix aims to ensure frictionless improvement of your security posture. This use case guide will provide you with insights on two main features: Default Syslog accept and status indicators for log source monitoring.

Default Syslog: Simplified SIEM deployment with out-of-the-box Syslog ingestion support

Quick and efficient log ingestion is not just a technical detail; it's a fundamental requirement for effective and smooth security operations, which in turns help maintain a strong security posture. How you set up your log sources for log ingestion determines the speed of the SIEM deployment process.

Guardsix's latest release eliminate the complexity of manual configuration and enables immediate log collection after installation. By allowing you to accept Syslog messages by default, Guardsix decreases setup time, streamlines security workflows, and enhances incident response. With this out-of-the-box support for Syslog ingestion, Guardsix ensures frictionless onboarding experience and scalability. Default Syslog ingestion can be disabled when needed from the system settings.



Instant log capture for new deployments

Default Syslog enables security teams to ingest logs from day one, preventing critical log loss during the initial setup phase. By eliminating manual configurations, organizations ensure that no security-relevant data is missed.

Optimized log collection for MSSPs

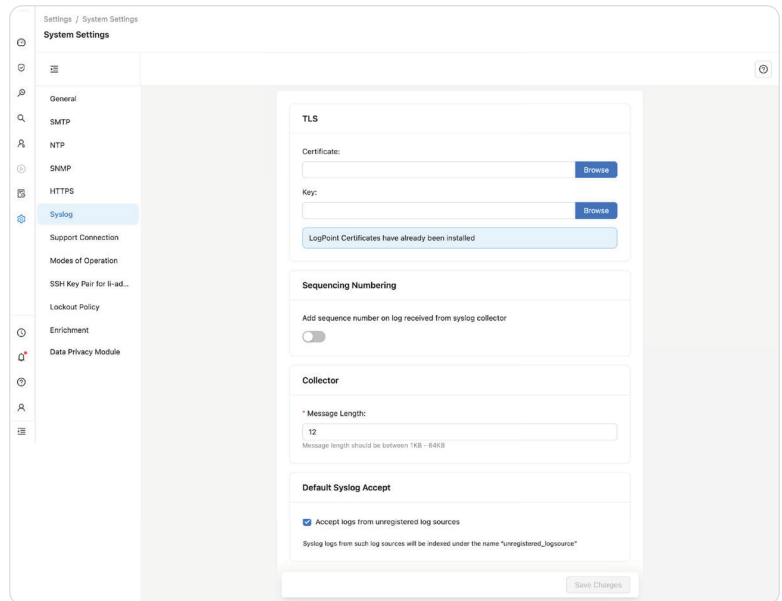
Managed Security Service Providers (MSSPs) must ensure that all client logs are captured without data loss. With immediate log ingestion, Default Syslog eases onboarding and ensures continuous security data availability.

Customizable for long-term data integrity

While Default Syslog provides an easy start, teams can later configure sources and normalizers to ensure structured log ingestion. Without these configurations, some logs may not be fully parsed, limiting analytical insights.

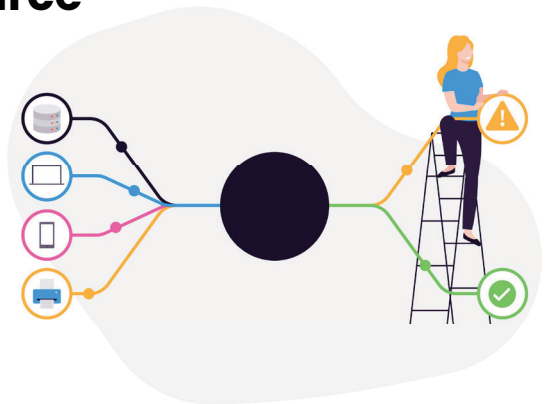
Scale without data gaps

As businesses scale, adding new Guardsix instances can lead to temporary log loss if configurations are not set up correctly. Default Syslog prevents this by automatically accepting logs, ensuring continuity in data collection.



Log Source activity: Proactive Log Source monitoring with status indicators

Continuous log collection is what makes SIEM effective, allowing security teams to maintain visibility and respond to threats effectively. However, detecting inactive log sources in time has traditionally required manual effort. Guardsix's latest release simplifies this by introducing automated tracking and color-coded indicators next to the last log received status to ensure proactive issue resolution.



Continuous log collection is what makes SIEM effective, allowing security teams to maintain visibility and respond to threats effectively. However, detecting inactive log sources in time has traditionally required manual effort. Guardsix's latest release simplifies this by introducing automated tracking and color-coded indicators next to the last log received status to ensure proactive issue resolution.

Guardsix SIEM provides real-time visibility over log source activity without having to run manual queries. With a visual status system based on pre-defined time thresholds, security teams can identify and resolve log source inactivity that otherwise would have gone unnoticed. This feature enhances security operations, improves response times, and prevents critical log loss through a more intuitive, automated approach to log source tracking. In addition to configurable color-coded indicators, it's possible to receive alerts and notifications to ensure uninterrupted log collection, improving security posture and operational efficiency.

Detect inactive log sources on the spot

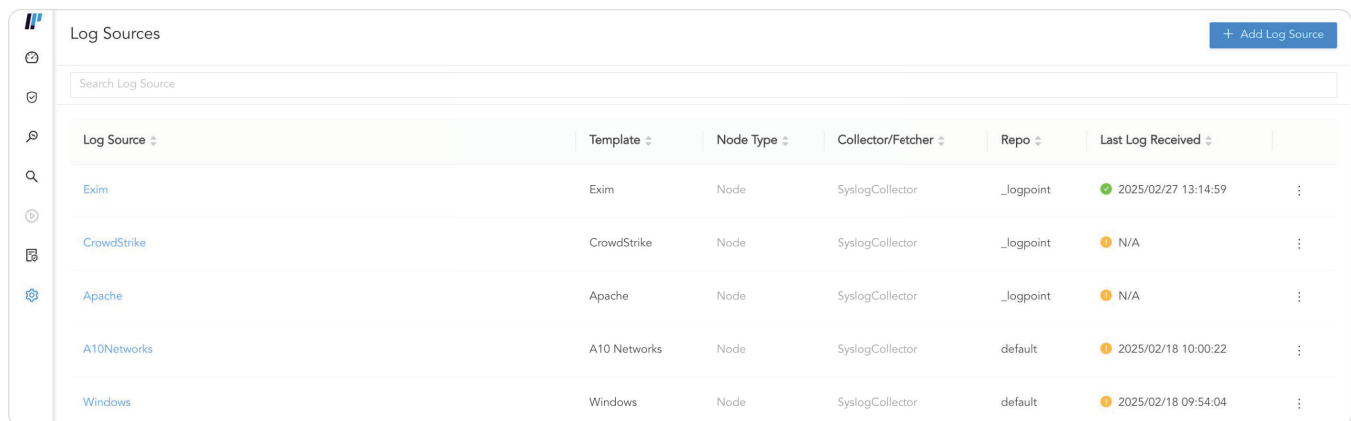
Guardsix's enhancement of the log source monitoring feature enables security teams to immediately detect and address log source failures. Real-time monitoring and automated notifications help prevent blind spots in security analysis, ensuring that no logs are missed due to undetected inactivity.

Uninterrupted alerting across multiple channels

Guardsix wants to make sure that your team never misses critical log source failures by allowing you to set up alerts through email or Guardsix notifications within the platform or SNMP monitoring integration, allowing seamless alerts within existing monitoring setups.

Perfect for enterprises with large deployments:

Organizations managing large-scale log sources can leverage the log source monitoring feature's SNMP integration to streamline their log management operations. By automating inactivity detection and sending SNMP alerts, they can track log sources alongside their broader IT infrastructure, ensuring proactive issue detection, reducing operational overhead, and maintains continuous log collection at scale.



Log Source	Template	Node Type	Collector/Fetcher	Repo	Last Log Received	
Exim	Exim	Node	SyslogCollector	_logpoint	2025/02/27 13:14:59	⋮
CrowdStrike	CrowdStrike	Node	SyslogCollector	_logpoint	N/A	⋮
Apache	Apache	Node	SyslogCollector	_logpoint	N/A	⋮
A10Networks	A10 Networks	Node	SyslogCollector	default	2025/02/18 10:00:22	⋮
Windows	Windows	Node	SyslogCollector	default	2025/02/18 09:54:04	⋮

Color-coded indicators for easier monitoring

With a color-coded status system, users can visually identify log source activity:

- Green: Active log source
- Yellow: Inactive log source

This quick visual reference reduces troubleshooting time and enables faster remediation.

Customizable for operational efficiency:

The log source monitoring feature allows users to configure thresholds for source inactivity based on the type of source being dealt with. Security teams can define inactivity periods before flagging source as irregular, reducing noise and ensuring actionable insights.

guardSIX

OTD BİLİŞİM

GLOBAL VAD