DATA SHEET

LOGSENTINEL SIEM FEATURES

Simplify Security and Compliance

Easy and high-quality security monitoring for the mid-market

LOG COLLECTION

Centralized log collection, aggregation and normalization

THREAT DETECTION

Discover anomalous behavior and insider threats

INCIDENT RESPONSE

Kill malicious processes in the bud

DASHBOARDS AND REPORTING

SECURITY MONITORING

IMPLEMENTATION, SUPPORT AND MANAGED SERVICES

ADVANCED SECURITY AND COMPLIANCE

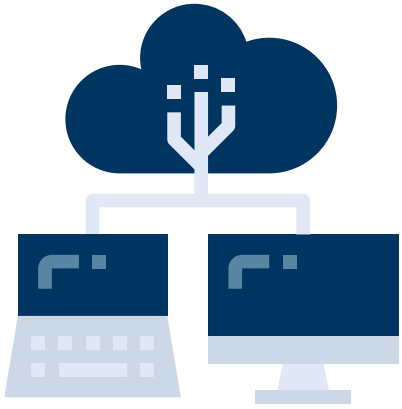
CENTRALIZED LOG COLLECTION, AGGREGATION AND NORMALIZATION

UNLIMITED ON-PREMISE INTEGRATIONS

Our flexible collector allows for unlimited data sources for on-premise systems – servers, network appliances, endpoints, legacy applications, databases.

UNLIMITED CLOUD INTEGRATIONS

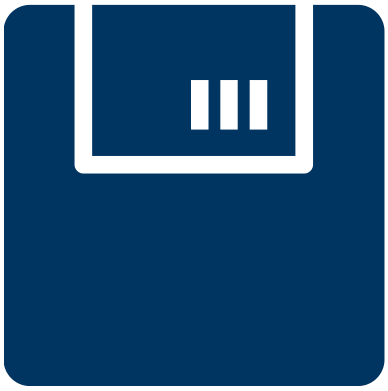
LogSentinel SIEM supports out-of-the-box integrations with major IaaS and SaaS – AWS, Azure, GCP, videoconferencing services, cloud CRMs, etc.



CUSTOM CONNECTORS

Customers can flexibly define multiple sources by configuring text file and database table sources as well as adding simple custom scripts for extracting logs.

CENTRALIZED LOG COLLECTION, AGGREGATION AND NORMALIZATION



LONG-TERM RETENTION

Our hot/warm/cold search engine setup allows for long-term retention with performance hits. Keep relevant data for years, if needed for compliance purposes.

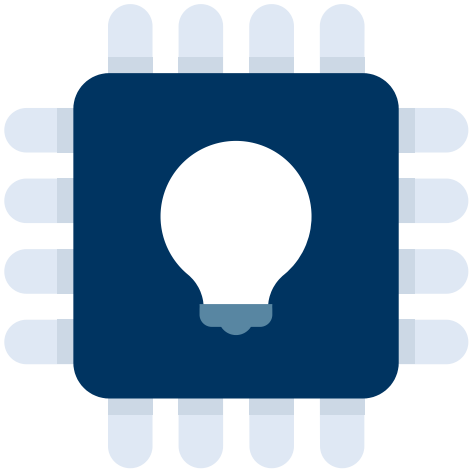
PER-SOURCE RETENTION

Define retention periods per data source, allowing for flexibility in terms of compliance and storage optimization

ASSET DISCOVERY

Automatically discover new on-premise assets to assist connecting them to LogSentinel SIEM

THREAT DETECTION

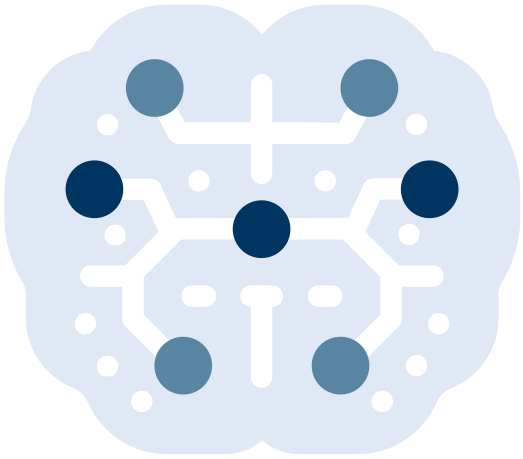


RULE-BASED EVENT CORRELATION & THREAT DETECTION

Use a flexible UI to define rules and make use of many built-in ones for discovering potentially malicious activity across data sources.

MACHINE-LEARNING THREAT DETECTION

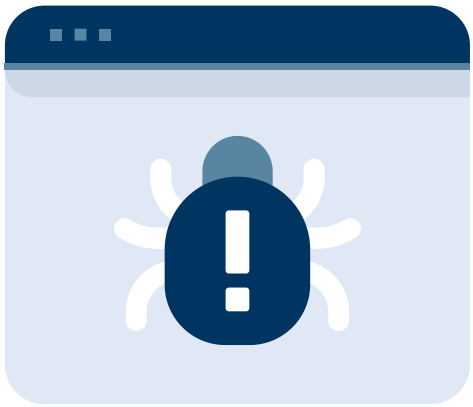
Our fine-tuned machine learning monitors the normal activity of each of your systems and alerts you in case of anomalies.



FILE INTEGRITY MONITORING AND REGISTRY INTEGRITY MONITORING

Collect data about any changes to crucial files and directories on each endpoint, thus getting early warnings about ransomware and other malware attacks.

THREAT DETECTION

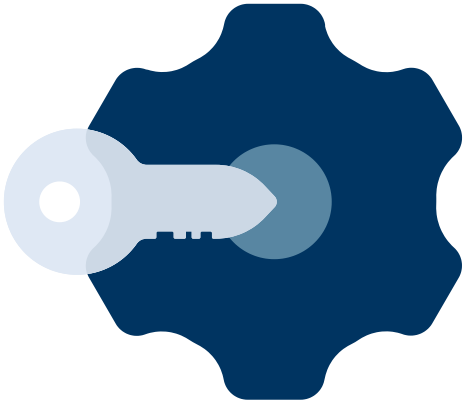


THREAT HUNTING

Proactively detect potential threats based on the already collected data via our flexible threat hunting dashboard and tools

PHISHING DETECTION

Connect our collector to your email server to get all emails inspected for phishing and get alerted in real-time in case of a phishing attack against employees



LEAKED CREDENTIALS DETECTION

Get alerted whenever the credentials of any employee get leaked online, regardless of which service was used, as long as there's an email match.

THREAT DETECTION

WEBSITE FORMJACKING DETECTION

Monitor your websites for malicious modifications to static resources that usually harvest credit card data and other sensitive information.

THREAT INTELLIGENCE

You are automatically subscribed to dozens of threat intelligence feeds that help you discover known malicious actor that try to abuse your IT infrastructure.

HONEYPOT DATA COLLECTION

Run our collector in “deceptive” mode to collect IP addresses of potentially malicious actors doing reconnaissance on your network

INCIDENT RESPONSE

INCIDENT RESPONSE CAPABILITIES

Execute automated commands on each endpoint in case malicious activity is detected – block IPs, kill processes, disable accounts, etc.
Automate the incident response workflow through integrations with SOAR and other automation tools.

INVESTIGATION AND TRIAGE

Easily investigate the details of each suspected incident, through forensic information and collected indicators of compromise and threat intel.

FLEXIBLE THREAT NOTIFICATIONS

Get notified for alerts on multiple channels, including email, SMS and existing monitoring and alerting solutions.

DASHBOARDS AND REPORTING

CUSTOM SECURITY DASHBOARDS

Build custom dashboards by combining multiple charts and saved searches to reflect your team's preference for presenting the data

MANAGEMENT REPORTING

Get scheduled or tailor-made management reports about system and user activity, alerts and threats

COMPLIANCE REPORTING

Get compliance reports, useful for various standards and regulations, including user activity reports, out-of-hours activity reports, data processing activity reports and more.

SECURITY MONITORING

APPLICATION MONITORING

Monitor the security logs and audit logs of any application – on-premise, cloud or even internally built legacy applications with our flexible collector.

DATABASE ACTIVITY MONITORING

Monitor changes to the structure and contents of database schemas and tables and get notified in case of potential malicious modifications.

NETWORK MONITORING

Connect your syslog and NetFlow/IPFIX network appliances to get real-time monitoring for threats

SECURITY MONITORING

SAP SECURITY MONITORING

Collect and monitor SAP security logs, read audit logs and other data without the need to install and maintain any 3rd party plugins

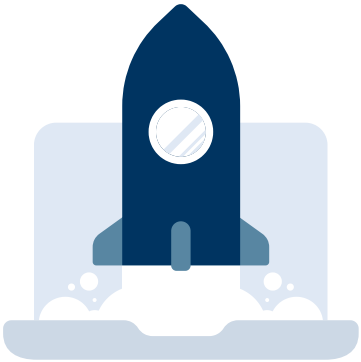
MANAGEMENT REPORTING

Get scheduled or tailor-made management reports about system and user activity, alerts and threats

IAM SECURITY MONITORING

Collect the audit logs from your IAM solution and get alerted on anomalous authentication and authorization activities.

IMPLEMENTATION, SUPPORT AND MANAGED SERVICES

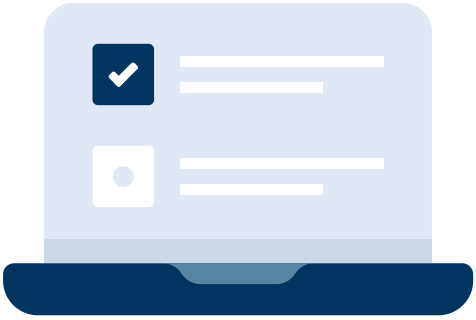


FLEXIBLE DEPLOYMENT OPTIONS

Use LogSentinel SIEM SaaS, deploy it on-premise or in your cloud environment. We support on-premise multitenancy and multi-site deployments.

MANAGED DETECTION AND RESPONSE

We can help your team by monitoring and handling alerts as much as possible. We'll present you with regular reports and a managed detection dashboard for what we've done.



AUTOMATED IMPLEMENTATION PLAN

Automatically generate implementation templates and email communication for required permissions and credentials to streamline the implementation process.

EMAIL AND PHONE SUPPORT

Support on multiple channels is included in the license.

ADVANCED SECURITY AND COMPLIANCE

DIGITAL EVIDENCE

Our cryptographically guaranteed integrity and non-repudiation of logs makes them usable as strong legitimate legal evidence.

END-TO-END LOG ENCRYPTION

In addition to encrypting data in transit and at rest, we allow you to send use encrypted logs and still be able to search in them through our searchable encryption implementation.

About LogSentinel

Easy and high-quality security monitoring for the mid-market

We, at **LogSentinel**, are passionate about information security and believe in privacy as a human right. LogSentinel's mission is to help your organization boost IT security processes by leveraging the latest technologies including blockchain and AI. We deliver robust and reliable solutions designed to protect against data breaches and insider attacks, we ensure a higher level of compliance with legal regulations.

LET'S CONNECT

https://logsentinel.com

contact@logsentinel.com

REQUEST DEMO