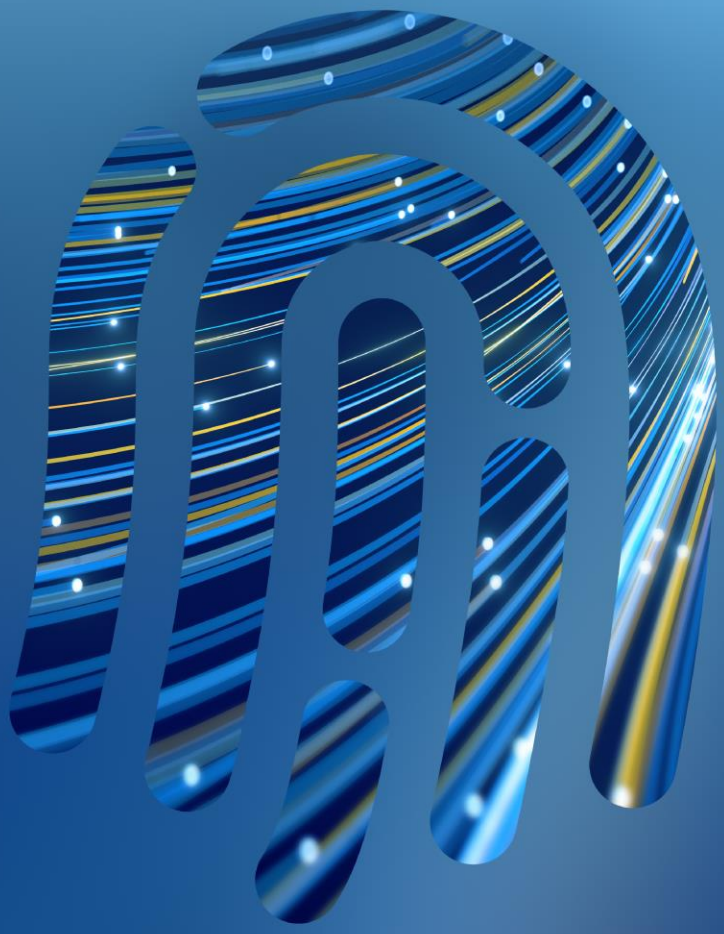


PRODUCT SHEET

SIEM as a Service

OT Cybersecurity alerts detection and visualization for energy automation systems

SIEMENS

Contents

Overview

SIEM-as-a-Service (SIEMaaS) is a cloud-hosted Security Information and Event Management service designed to give power grid operators and industrial organizations continuous security visibility across their critical energy automation, substation, and SCADA environments. It helps security and operations teams collect, normalize, and correlate security-relevant logs and events from key systems and network components, enabling a more modern approach to monitoring than traditional, infrastructure-heavy SIEM deployments.

By detecting and prioritizing cybersecurity-relevant activity such as repeated or anomalous login attempts, privilege misuse, configuration changes, unexpected communication paths, and network access attempts by unidentified parties, SIEMaaS supports faster investigation and response while maintaining the scalability needed for distributed sites and increasing event volumes. The service is built to support the operational realities of OT environments, where availability, reliability, and control management are essential.

SIEMaaS also provides a practical foundation for establishing and maturing cyber incident response practices. Through consistent event handling and improved situational awareness, organizations can move from reactive troubleshooting to a structured process for identifying threats, assessing impact, coordinating response actions, and documenting outcomes helping strengthen resilience and security posture over time.

Benefits of SIEM-as-a-Service

- Short Implementation Time
- Detection content provides more than 300 optimized threat detection rules for power systems.
- Built for OT supporting security monitoring of the power infrastructure
- Customers are prepared for future changes by scalable cloud delivery without complex on-prem scaling efforts.
- Enable compliance with regulations

Features

AWS public cloud environment

Includes all the necessary resources (e.g., data storage capacity, CPU, RAM) on the AWS public cloud data center in Frankfurt, Germany, to host a dedicated cloud environment for the Customer's SIEM-as-a-Service instance.

Dashboards

Customizable dashboards provide a quick overview of the most important incident alarms filtered by various log sources – from operational IT systems such as Windows OS, firewalls, networking devices such as routers and switches, OT components such as protection relays and RTUs. The dashboards monitor the handling status of the alarms and observe their occurrence patterns across adjustable time ranges.

Analysis Views

Get a closer look into alarms originating from specific log source types, further subclassified along different root causes, for example: unsuccessful logon attempts reported by RTUs, circuit breaker operations reported by protection relays, reboot events reported by OT components, and more, in a flexible manner.

Incidents Views

Investigate incident alarms in detail and in their chronological order of occurrence. Each individual alarm is automatically normalized to assist the incident responder in the analysis of the alarm with information such as the originator of the event, the event description, possible cause(s), preceding and following events, and other helpful hints. Assign an alarm to the appropriate analysts and document the alarm resolution after having responded to the alarms. Generate customizable reports with a wide variety of content for audit and compliance purposes.

Reports

Generate customizable reports with a wide variety of content for audit and compliance purposes.

Notifications

Receive customizable notifications on incident alarms via E-mail, SNMP, Syslog, and other channels.

Security Information

Security measures	Details
Secured Cloud Connectivity	The cloud endpoint provided by SIEM-as-a-Service for receiving log messages from the connected Customer location(s) is strictly secured by TLS (Transport Layer Security) protected communication using state-of-the-art security mechanisms, e.g., by use of a dedicated X.509 certificate procured for the Customer and signed by a public Certification Authority (CA).
Secure Communication	Data transmission will be done via HTTPS protocol from your site(s) to your SIEM-as-a-Service instance.
Encryption Standard	TLS 1.2 is used for communication between your site(s) and SIEM-as-a-Service.
Security Concept	To protect substations, systems, machines, and networks against cyber threats, it is necessary that you implement a holistic, state-of-the-art substation security concept and continuously maintain the same. For more information, refer to www.siemens.com/gridsecurity.
Access credentials	Authentication and authorization on User level based on username and password.
Certification	Our management systems are based on principles of Siemens AG concerning quality, environmental, occupational health, and safety protection as also information security. They meet the demands of internationally approved norms and standards such as ISO 9001, ISO 14001, ISO 45001 and ISO 27001 etc. You may find the certificates for Smart Infrastructure Electrification & Automation (SI EA)

Additional Functions

Ruleset - Noise reduction before Customer handover

Covers required adjustments to the installed rule set after monitoring the running system for a period of 2 weeks to meet customer-specific operating procedures in terms of normal vs. abnormal behavior. Based on the size and complexity of the monitored installed base, a different period may be specified in the offer from our regional entity, which would take precedence over the 2 weeks period mentioned here.

This activity reduces false or unimportant alarms to the Customer.

Installation and Onboarding

Installation of a dedicated SIEM-as-a-Service instance in the AWS public cloud.

Covers Customer onboarding, Alarm Dashboard creation, report customization, cloud-side configurations for Customer log collector connectivity to the hosted SIEM-as-a-Service.

Covers the annual SIEM-as-a-Service software subscription.

Ruleset - Noise reduction after Customer handover

Covers required adjustments to the installed rule set during the operation of the service for the period of one year (annual subscription) to account for customer-specific operational workflow-related normal vs. abnormal behavior. Reduces false or unimportant alarms to the Customer. Maintenance work and adjustments to the rule sets that are included due to external factors, such as changing threats, are covered. Adjustments that fall within the customer's responsibility are not automatically included (for example, if the customer wants to use new or different hardware components or changes their internal processes, which may have implications for the rule sets) – such modifications are covered on an effort-basis as agreed between the customer and the Siemens regional entity.n

Training

Training of users with a practical complete solution based on 1-2 examples: Walkthrough of the various menu actions including alarm handling, reporting functions etc.

Environment Management

Covers quarterly security patch updates to the cloud environment for the Customer's SIEM-as-a-Service instance.

Covers annual renewal of the SSL/TLS certificate of the AWS-hosted SIEM-as-a-Service web server for secure Customer user access.

Possible Integrations

Managed Detection and response

The SIEM-as-a-Service can be enhanced with Siemens Managed Detection and Response (MDR), a 24/7 managed security service that combines advanced threat detection technology with expert-led security operations transforming hundreds of raw security events into a small number of prioritized and actionable security incidents. MDR continuously analyses and correlates security events collected across IT and OT environments to identify cyber threats, prioritize risks, and support effective incident response.

Evolving from SIEM-as-a-Service towards MDR enriches your power infrastructure with a comprehensive cyber resilience capability that extends beyond monitoring, providing continuous threat detection, expert-driven analysis, and coordinated response support for power infrastructure environments.

The service enriches SIEM monitoring capabilities with:

- 24/7 security monitoring and alert triage.
- Actionable Recommendations.
- Industry Specific detection.
- Scalable cyber resilience.
- Service governance.
- Regional proximity.

OT Companion Integration – Electrification X

The SIEM-as-a-Service provides interoperability with our IoT-enabled application OT Companion inside of our cloud-hosted platform Electrification X delivered for operators of power systems in utilities, industries, and infrastructure.

OT Companion visualizes security alerts that have been detected and correlated by Siemens' SIEM. Alerts are displayed in a dedicated overview, enabling immediate assessment of affected locations, assets, or device types. By correlating event data with the OT inventory and known vulnerability information, helps users understand which assets are impacted and how critical each incident may be within the operational context.

This integration bridges asset visibility and real-time cybersecurity monitoring, providing operators and SOC teams with a unified perspective on operational threats. The system enriches SIEM-based alerts with:

- Asset context and inventory data
- Configuration details
- Known vulnerabilities and risk profiles

Subscription

Standard subscription plan	Details
Package	Service Base (incl. 20 IPs) Addon Package: 1/30/50/100/300/500/1000/+1000 IPs
Subscription term	Annually, auto-renewal
Billing term	Annually, payment in advanced – Service Base Monthly, payment in advanced – Addon Package
Upscale	Effective immediately, pro-rated billing
Downscale/Cancellation	Effective with end of subscription term
Permitted Users	Unlimited

Standard subscription plan	Details
Package	Onboarding Base (incl. 20 IPs) Addon Package: 1/30/50/100/300/500/1000/+1000 IPs*
Subscription term	One-time
Billing term	One-time, payment in advanced

*per single onboarding request

SIEM as a Service provides a regular, scalable slab-based pricing model. Pricing consists of a Base Package including 20 IPs and Addon Package for scopes above 20IPs.

- One size parameter: Number of IPs.
- IP: Asset or node with an assigned IP address (internet protocol).
- Supports standardized scope changes during contract period.
- Price includes cloud, software, and labor (no separate vendor quotes required).

The subscription term is twelve (12) months with automatic renewal; the service is paid in advance. The subscription plan can be upscaled at any time and service fees for upscales are calculated on a pro-rated basis. The customer can also scale down the service effectively with the end of the current subscription term. The subscription fee will be adjusted for the upcoming billing term. The cloud service can be cancelled any time, effectively at the end of the current subscription term.

Prerequisites

Log Sources

The SIEM-as-a-services supports the following log servers, which must be installed in the OT sites that we want to visualize the information and events from:

- NXLog Log Collector version 5.6 and above.
- Any other similar security log collector and forwarder.

The log server collects log data from different OT/IT endpoints and send them securely to the SIEM via secured Syslog protocol.

Our onboarding field services offered by our regional entities includes (a) the on-site configuration of the monitored endpoints to activate their security-relevant event logging, and (b) the on-site configuration of the security log collector installations to receive the logs from the different endpoints, as well as establishing their connectivity to the AWS based SIEM-as-a-Service. Please engage with our regional staff to select, procure, configure, onboard, and operate the security log collector installations and the undertaking of the necessary SIEM-readiness activities.

Web browser and operating systems

SIEM-as-a-Service is a web-based application for use on Desktop PCs. The recommended screen resolution is 1920x1080px or higher. The application requires a recent version of Google Chrome, Microsoft Edge, or Apple Safari web browser.

Internet connection

A secure, firewalled Internet connection between the log collector systems (see section Log sources) and the SIEM-as-a-Service system is required. The firewall must allow outgoing TCP-connections to port 443. If your Internet router does not act as a DNS proxy or a DNS server, additionally the firewall must allow outgoing UDP connections to port 53.
The bandwidth requirement depends on the infrastructure scope and will be estimated as part of the onboarding service.

Ordering

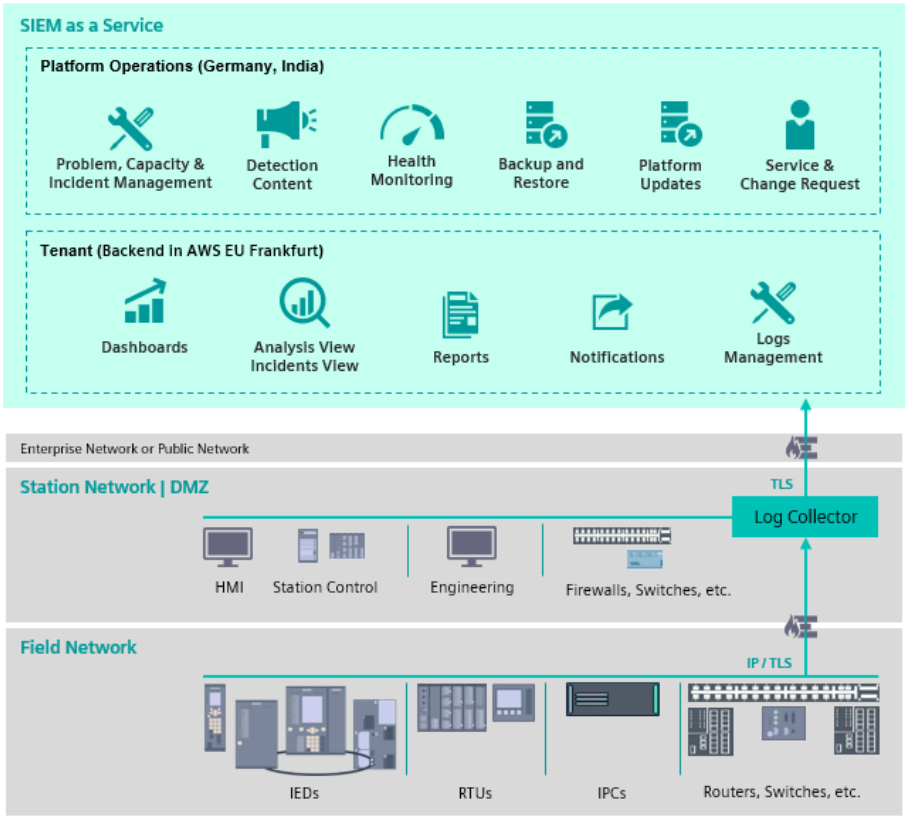
Ordering process for the subscription

To order the cloud service for the first time, customer must request a quote from its Siemens sales representative. Depending on the offering either with services, then customer will receive a link to his tenant, or without services, then the customer will receive a link to the shopping cart. In this case customer needs to (i) choose the payment options and (ii) accept the Terms and Conditions to start using the cloud service. The "Terms and Conditions" consist of the "Supplemental Terms Electrification & Automation", the Base Terms and the General Software and Cloud Supplemental Terms, the Acceptable Use Policy, the Siemens Data Processing Terms, this Product and Service Data Sheet and any other Supplemental Terms which may be referenced in either of the mentioned documents. Customer may upgrade, downgrade, and cancel the cloud services directly in the subscription manager store https://subscribe.siemens.com.

Topology

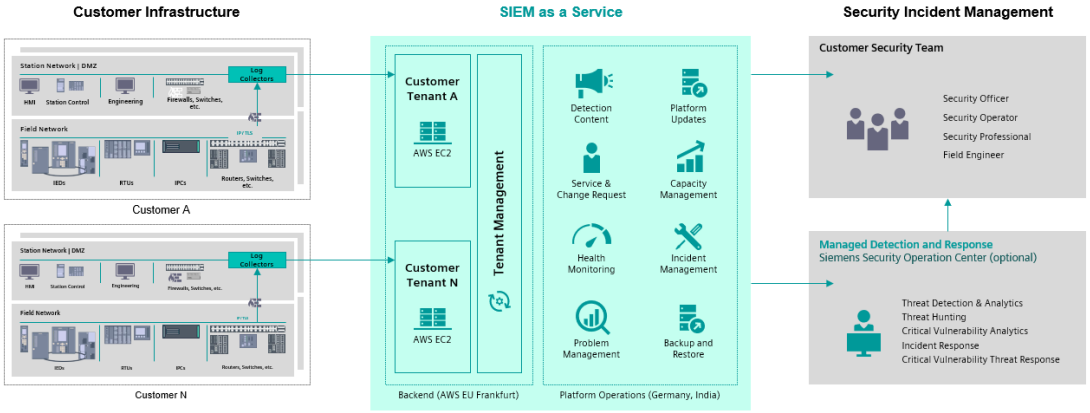
SIEM-as-a-Service

The following topology shows how the SIEM-as-a-Service offering simply collects the information from the substation level towards the customer tenant:



End-to-End Cybersecurity Architecture with SIEM-as-a-Service

The following topology illustrates how SIEM-as-a-Service integrates with customer OT environments to provide centralized monitoring, threat detection, and incident management. Combined with Managed Detection and Response (MDR), it supports an end-to-end cyber resilience approach:



General Terms

Service Level Agreement – SLA

The Monthly Availability for the AWS public cloud hosted SIEM-as-a-Service service is 99.5%.

Month means a calendar month. Total Time means all of the time during a Month (in minutes), less any time attributed directly or indirectly to SLA Exclusions. Uptime means all of the time during a Month (in minutes) when the Cloud Services are available for production use (i.e., user logon and access and use of user interfaces.)

Monthly availability means the percentage of time the Cloud Services are available on average during a Month, based on Uptime and Total Time.

SLA exclusions consist of mean unavailability or any other performance issue causing downtime of the Cloud Services as a result of:

(i) scheduled maintenance within a Regular Maintenance Window

(ii) planned downtime, agreed downtime, routine & scheduled maintenance within a regular maintenance window, and emergency maintenance for which at least 24 hours prior notice is provided to Customer

(iii) cyberattacks

(iv) the public, third party and/or customer's internet and communications networks

(v) data, software, hardware, telecommunications, infrastructure, power, or networking equipment not provided by Siemens

(vi) customers' and users' negligence or failure in using the Cloud Service and/or in not following the instructions of published documentation

(vii) system configurations and platforms not supported by Siemens

(viii) actions or inactions of Customer or any third party

(ix) unauthorized access via Customer's credentials and/or any other failure and/or factors outside of Siemens reasonable control

Third Party Terms

The Third-Party Terms are made available via the following web link:

(i) AWS Acceptable Use Policy on https://aws.amazon.com/aup/?nc1=h_ls

Data Privacy Terms

Protecting the security and privacy of personal data is important to us. Therefore, we process personal data in compliance with applicable laws on data protection and data security. The Privacy Policy is made available on www.siemens.com/dpt.

Export Control Regulations

Export Control regulation	Details
AL	N
ECCN	N

Customer support

Siemens offers helpdesk support. Customer may contact its local Siemens representative for support requests.

https://isp.portal.siemens.com/

Email: support.ea.si@siemens.com

Germany / Austria / United Kingdom Phone: +49 9131 1743072

China Phone: +86 400 150 6060

Brazil Phone: +55 0800 011 9484

India Phone: +91 1 800 266 7480

Published by
Siemens AG
Smart Infrastructure
Electrification & Automation
Mozartstrasse 31c
91052 Erlangen, Germany

For the U.S.
Published by
Siemens Industry Inc.
3617 Parkway Lane
Peachtree Corners, GA 30092
United States