Service description document: Cortex XSIAM – Autonomous Security Operations Platform

Cortex XSIAM – Autonomous Security Operations Platform

Service overview

Cortex XSIAM is a cloud-delivered security operations platform designed to unify, automate, and transform enterprise security operations. It consolidates core SOC capabilities, including SIEM, XDR, SOAR, UEBA, attack surface management, threat intelligence, and analytics into a single SaaS platform that centralises security data and applies machine learning to detect, investigate, and respond to known and unknown threats.

The service is delivered as an Infrastructure Software as a Service (iSaaS) subscription, providing scalable security operations without the need for on-premises infrastructure.

What the service provides

Cortex XSIAM delivers an integrated, autonomous SOC capability by bringing together telemetry from endpoints, networks, cloud environments, identities, and third-party sources into a unified security data foundation. The platform applies AI-driven correlation, behavioural analytics, and automation to dramatically reduce alert volumes and accelerate incident response.

The service provides:

- Centralised security data ingestion and storage via a unified data lake
- AI-driven detection and correlation across multiple security domains
- Automated investigation and response workflows natively embedded in the platform
- Proactive exposure and attack surface management
- Identity threat detection and response capabilities
- Cloud detection and response for hybrid and multi-cloud environments
- Integrated case management and analyst workflows
- Quantifiable security metrics and reporting for governance and assurance

Cortex XSIAM is designed to replace multiple point products while also ingesting and enriching data from existing security tools.

Service features

Cortex XSIAM includes the following core features:

- AI-driven incident correlation
- Converged SOC platform
- Unified security data lake
- Automation-first response with embedded SOAR
- Proactive exposure management
- Cloud detection and response
- Identity threat detection and response

- High-fidelity threat detection
- Agentic AI to augment analysts
- Simplified licensing and total cost of ownership

Service benefits

Cortex XSIAM enables organisations to:

- Significantly reduce alert volumes and analyst fatigue
- Lower total cost of ownership by consolidating security tools
- Accelerate incident detection and response
- Transform SOC analyst productivity and effectiveness
- Improve detection efficacy for advanced threats
- Reduce organisational cyber risk proactively
- Establish a resilient and scalable security data foundation
- Support business growth without linear SOC expansion
- Improve analyst retention and job satisfaction
- Produce measurable, auditable security outcomes

Service scope and dependencies

Cortex XSIAM is delivered as a public cloud SaaS service. It operates as a platform rather than a traditional add-on, although it can extend deployments that begin with individual Cortex components such as XDR.

The service requires deployment of the Cortex endpoint agent on supported and compatible endpoints. Internet connectivity is required to access the service and ingest telemetry. Cortex XSIAM can ingest data from a wide range of third-party security and IT systems to enrich detection and response workflows.

Customisation and configuration

Customers can customise Cortex XSIAM extensively to align with their security operations model. Customisation includes:

- Creation of custom dashboards and analytics using Cortex Query Language (XQL)
- Design and modification of automated response playbooks
- Configuration of detection rules, thresholds, and incident logic
- Customisation of incident layouts and metadata fields
- Integration with third-party tools and data sources

Customisation is performed through the browser-based management console and APIs, with role-based access controls ensuring only authorised users can make changes.

Access and user experience

Cortex XSIAM is accessed through a unified, browser-based management interface designed to support an autonomous SOC operating model. The interface consolidates monitoring, investigation, response, and reporting into a single workspace.

The service supports accessibility features aligned with WCAG 2.1 Level AA, including keyboard-only navigation, screen-reader compatibility using ARIA labels, and appropriate visual contrast for

alerts and dashboards. A natural-language interface allows users to query security data and perform tasks without navigating complex graphical menus.

Support and service management

Vendor-backed support is available via online ticketing, phone, and web chat, depending on the selected support tier.

Support response targets include:

- **Platinum:**
  - Critical: under 15 minutes
  - High: under 30 minutes
  - Medium: under 2 hours
  - Low: under 4 hours
- **Premium:**
  - Critical: under 1 hour
  - High: under 2 hours
  - Medium: under 4 hours
  - Low: under 8 hours
- **Standard:**
  - Available Monday to Friday, 7am–6pm UK time, with response targets aligned to Premium during service hours

Technical account management and additional support services may be provided as optional professional services.

Availability and service levels

Cortex XSIAM is covered by a vendor Service Level Agreement providing a 99.9% Monthly Uptime Availability commitment.

Availability is calculated based on total minutes in a calendar month, excluding defined events such as scheduled maintenance, customer environment issues, force majeure events, licensed capacity shortfalls, beta features, and security-driven traffic blocking. Delays in data ingestion are not considered downtime.

If the service level is not met, eligible customers may claim service credits, subject to the SLA terms. Credits are calculated as a percentage of the monthly subscription fee for the affected Cortex product, with caps applied per day and per calendar month.

Service status and regional availability information are published via a public status portal, where customers can subscribe to automated notifications.

Security and data protection

Cortex XSIAM is built with security embedded throughout the service lifecycle. Protections include:

- Encryption and secure transport for data in transit
- Segmentation, firewalls, and advanced threat detection within the platform
- Continuous monitoring and behavioural analysis using AI
- Regular vulnerability scanning and penetration testing

- Rapid patching of critical security issues
- Secure data storage within a centralised security data lake

Customer data is sanitised and permanently erased in line with defined data destruction and cryptographic erasure processes at contract end.

Onboarding and offboarding

Onboarding is supported through comprehensive documentation, online help, training resources, playbooks, and optional professional services. Documentation is available via web-based formats, knowledge bases, and video tutorials.

At contract end, access to the service ceases in line with contractual terms. Customers can export logs, reports, and data in standard formats and complete migration or transition activities, with vendor assistance available where required.

Commercial model

Cortex XSIAM is provided under a subscription-based licensing model, with pricing determined by licensed capacity and selected service components. The subscription includes access to the Cortex XSIAM platform and vendor support aligned to the chosen support tier.

Additional services, including enhanced support levels, technical account management, and professional services, are available at additional cost.

Out of scope

The following are not included unless explicitly contracted:

- Managed SOC or analyst services
- Customer network connectivity
- End-user device support
- Custom software development beyond documented capabilities
- On-premises infrastructure provisioning

business
secure, managed solutions for all.