Service description document: Cortex XSOAR – Security Orchestration, Automation and Response Platform

Cortex XSOAR – Security Orchestration, Automation and Response Platform

Service overview

Cortex XSOAR is a cloud-delivered Security Orchestration, Automation and Response platform designed to standardise, automate, and accelerate security operations. It unifies incident case management, automation, collaboration, and threat intelligence management into a single service.

The platform enables organisations to respond to security incidents faster and more consistently by replacing manual processes with playbook-driven workflows across cloud environments.

What the service provides

Cortex XSOAR provides a centralised security operations platform that coordinates people, processes, and technology during security incidents. It allows organisations to manage alerts, investigations, and responses from a single interface while automating repetitive tasks and enforcing consistent response procedures.

The service provides:

- Centralised incident and case management
- Playbook-driven automation for security workflows
- Integrated threat intelligence management
- Real-time collaboration through a virtual war room
- Extensive integrations with security tools, ticketing systems, and collaboration platforms
- Automated documentation and audit trails
- Dashboards and reporting for operational visibility
- Mobile access for monitoring and response actions

Cortex XSOAR is designed to operate as both a standalone orchestration platform and as an extension to existing security tools.

Service features

Key technical features include:

- Playbook-driven automation
- Extensive integration marketplace
- Unified case management
- Virtual war room collaboration
- Native threat intelligence management
- Machine-learning-driven virtual assistant
- Automated documentation and audit trails
- Indicator repository and correlation
- Interactive dashboards and reporting
- Mobile application support

Service benefits

Cortex XSOAR enables organisations to:

- Reduce mean time to respond to incidents
- Increase security analyst productivity
- Eliminate alert fatigue through automation
- Standardise incident response processes
- Accelerate onboarding and training of analysts
- Improve return on investment from existing tools
- Improve threat intelligence quality and usage
- Enhance collaboration during incidents
- Maintain audit-ready compliance
- Scale security operations across cloud and operational technology environments

Service scope and dependencies

Cortex XSOAR is delivered as a public cloud Infrastructure Software as a Service (iSaaS) offering.

The service can operate independently or extend other platforms by orchestrating their responses. It integrates with security tools such as endpoint detection platforms, cloud security services, SIEMs, ticketing systems, and collaboration tools to coordinate response actions.

The service requires internet connectivity and compatible endpoints or integrations where automation actions are executed.

Customisation and configuration

Cortex XSOAR is highly configurable to align with an organisation's security operations model. Customers can:

- Build and customise response playbooks
- Configure dashboards, reports, and widgets
- Tailor incident layouts and metadata
- Define automation logic and enrichment steps
- Control permissions using role-based access control

Customisation is performed through a browser-based management interface and APIs. Administrative permissions determine the scope of changes users are permitted to make.

Access and user experience

Cortex XSOAR is accessed through a web-based interface designed for security operations teams. The interface consolidates incident management, automation, and collaboration into a single operational view.

The service supports accessibility aligned with WCAG 2.1 Level AA. Features include keyboard-only navigation, screen-reader compatibility through ARIA labels, and appropriate colour contrast for dashboards and alerts.

Mobile access supports monitoring and response actions, while complex playbook development is optimised for desktop use.

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:**
  - Monday to Friday, 7am–6pm UK time, with response targets aligned to Premium during service hours

Technical account management and professional services are available at additional cost.

Availability and service levels

Cortex XSOAR 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 scheduled or emergency maintenance, high availability or scaling events, customer environment issues, force majeure events, insufficient licensed capacity, beta or preview features, and security-driven service blocking. Delays in data ingestion are not considered downtime.

If availability falls below the committed service level, eligible customers may claim service credits equivalent to 2% of the monthly fee for qualifying incidents, subject to daily and monthly caps as defined in the SLA.

Service status and regional availability are published via a public status portal with optional alert subscriptions.

Security and data protection

Cortex XSOAR incorporates security controls across the service lifecycle, including:

- Encryption of data in transit and at rest
- Segmentation, firewalls, and threat detection
- Continuous vulnerability scanning and penetration testing
- Automated and manual incident response processes
- Centralised logging and audit data retention

Data is stored and processed in approved regions, including the UK and EEA, and the service aligns with recognised security standards such as ISO/IEC 27001, ISO 27017, ISO 27018, ISO 27701, SOC 2, and PCI where applicable.

Onboarding and offboarding

Onboarding is supported through documentation, online help, knowledge bases, video tutorials, training resources, and optional professional services.

At contract end, customers can export logs, reports, and incident data in standard formats including CSV, JSON, and PDF. Services cease in accordance with contractual terms, and customers may retrieve data or transition to alternative solutions with vendor assistance if required.

Commercial model

Cortex XSOAR is provided under a subscription-based licensing model.

The subscription includes access to the Cortex XSOAR platform and standard vendor support. Enhanced support tiers, technical account management, and professional services are available at additional cost. Fees for professional or managed services are excluded from SLA credit calculations.

Out of scope

The following are not included unless explicitly contracted:

- Managed security operations services
- Customer network connectivity
- End-user device management
- Custom software development beyond supported configurations
- On-premises infrastructure provisioning

business
secure, managed solutions for all.