Cortex XSOAR Privacy Datasheet

The purpose of this document is to provide customers of Palo Alto Networks with information needed to assess the impact of this service on their overall privacy posture by detailing how Personal Data may be captured, processed and stored by, and within the service.

The information provided in this document refers to Cortex XSOAR 8 for SaaS deployments.

Product Summary

Cortex XSOAR™ is a cloud-based, comprehensive security orchestration and automation response (SOAR) service that unifies incident response automation, case management and threat intelligence management to serve security teams across the incident lifecycle.

Cortex XSOAR integrates with the rest of the Cortex platform and its products (XDR, XPANSE, XSIAM) to offer SOCs:

- Unified user interface and user experience
- Simplified deployment and onboarding
- Consistent user management
- Auto-provisioning of latest features and fixes
- Built-in high availability

Information Processed by Cortex XSOAR

Information is processed within Cortex XSOAR as part of the daily incident response activity of the security operations center (SOC) team, as well as general management and automation of security operations workflows via available integrations or connections to third-party tools.

Integration with third-party sources

Cortex XSOAR ingests with data from a wide variety of sources including, but not limited by:

- **SIEMs** - events, and in some cases, raw logs
  EDRs/XDRs - events, details regarding hosts, files
- **Ticketing systems** - case ticket details such as ServiceNow
- **Email** - emails sent to particular inboxes or alerts from email security products

- **Email Gateway -** quarantined emails.
- **Threat feeds** - indicator lists from threat feed subscriptions
- **Firewalls** -security events from Palo Alto Networks firewalls and third-party firewalls.
- **Authentication providers** - logs from single-sign-on (SSO) providers (Okta, Azure Active Directory, PingID)
- **Other alert-generating sources** - security alerts go directly into Cortex XSOAR
- **Sandboxes** - Files, Webpages, Remote Files.
- **Threat Intelligence platforms** - IOCs(URLs, Email Addresses, hashes, etc)

In addition, Cortex XSOAR can be customized to ingest data from any type of system via APIs (push or pull model). During investigations, customers can further query internal and other systems for more data (e.g. the customer's Active Directory or internal databases)

Cortex XSOAR also makes extensive use of threat intelligence, both within the Threat Intelligence Management (TIM) module, and in Cortex XSOAR incidents. The threat intelligence data is ingested from customer threat feed subscriptions, including Palo Alto Networks-sourced Unit42 etc.) and various third-party intel services. This threat intelligence data can be auto-enriched with context from multiple sources.

Table 1: Examples of Information Processed by Cortex XSOAR

Data Type	May Include Personal Information
Internal/external IP addresses	Yes
Usernames	Yes
Email addresses	Yes
Email content	Yes
File content	Yes
Registry path	Yes
URL	Yes
File hash (SHA1. MD5)	Yes
Domain	Yes
CIDR	Yes

Information Generated within Cortex XSOAR

Ingested information normally triggers Cortex XSOAR playbooks and sometimes also creates a human-led investigation. Both processes—the automated playbook and the manual investigation—can create additional data that resides in Cortex XSOAR. For example, an access violation event that comes from a SIEM system may be enriched and investigated in Cortex XSOAR, and as a result of correlating data from various sources. Security analysts may also attribute the violation to a particular individual or threat actor. Each step of the investigation or action taken with respect to the incident, whether automated or manual, is audited in Cortex XSOAR with a timestamp.

Subprocessors

Data processed by Cortex XSOAR is hosted in Google Cloud Platform (GCP®) data centers. Customers can designate a Cortex XSOAR region, among those available, for the storage and processing of their data. As noted previously, customers can import data from various sources into Cortex XSOAR. The product provides a number of privacy features, such as:

- Role-based access control (RBAC): Cortex XSOAR includes sophisticated RBAC that allow customers to restrict incidents viewable by specific individuals or roles, and control which user is allowed to perform which action (down to the level of which commands an analyst can run on a third-party tool).

- Third-party integrations: Cortex XSOAR integrates out-of-the-box with hundreds of third-party tools. This allows customers to enhance security and privacy controls further, depending on the third-party tools they use. For example, customers can use third-party credential storage to keep credentials separate from Cortex XSOAR.

Compliance with Privacy Regulations

Palo Alto Networks captures, processes, stores, and protects Personal Data in Cortex XSOAR in accordance with the terms in (i) Palo Alto Networks Privacy Policy, (ii) for our customers, the applicable Data Protection Addendum, and (iii) this Privacy Datasheet. Our Trust Center, Palo Alto Networks one stop-shop for everything privacy and security related, provides numerous resources, including information on how our privacy practices comply with existing and applicable privacy legislations around the globe. For more information, please visit the Privacy section in the Trust Center.

Cross-Border Data Transfer

As part of the provision of the Cortex XSOAR service and/or purchased support services, Palo Alto Networks may be required to transfer Personal Data to other countries outside of the country/region where the customer is located. To the extent that we need to transfer such data, we will do so in compliance with applicable requirements for transfer of Personal Data, which include the EU Standard Contractual Clauses, as approved by the European Commission and/or other legally binding instruments.

Data Subject Rights

Users whose Personal Data is processed by Cortex XSOAR have the right to request access, rectification, suspension of processing, or deletion of the Personal Data processed by the service. Users can open a request via Palo Alto Networks Individual Rights Form.

Palo Alto Networks will confirm identification before responding to the request. Please note that if, for whatever reason, we cannot comply with the request, we will provide an explanation. For all users whose employer is a Palo Alto Networks customer, such users may be redirected to the relevant customer/employer for a response.

How Palo Alto Networks Complies with Data Protection Rules

Palo Alto Networks is committed to protecting personal data processed by Cortex XSOAR. We will not access the content of the information in a way that would allow us to acquire meaningful information about natural persons except where it is necessary for identifying security threats or investigating suspicious activities indicative of attacks.

Any logs stored on or processed by Palo Alto Networks systems are secured with state-of-the-art technologies, and Palo Alto Networks operates rigorous technical and organizational security controls. Logs and information forwarded to a given regional data center will be kept in that region. As Palo Alto Networks is a multinational company, there may be a need, in some cases, to share logs and information with Palo Alto Networks offices in other regions. We will do so in compliance with applicable requirements for transfer of personal data, including the EU Standard Contractual Clauses as approved by the European Commission, or other legal instruments for the transfer of personal data, provided for in EU data protection law.

Access and Disclosure

Access by Customers

Through the Cortex XSOAR user interface, customer users can view data based on the permissions granted to them by the Cortex XSOAR administrator (one or more users selected by the customer to manage the customer's Cortex XSOAR environment).

As mentioned previously, each user is governed by RBAC rules that are under the customer's control. The customer may choose to grant all permissions to all users, but can also define, by user, the actions they are permitted to take and the types of data or cases/incidents they can read/write. This gives customers granular control over who gets to access data.

Access by Palo Alto Networks

Access to information in Cortex XSOAR is restricted to the 1) DevOps team, 2) Palo Alto Networks Site Reliability Engineers (SREs), 3) Threat Research Analytics Teams and 4) Customer Support Services and/or Customer Success/Focused Services teams (to the extent these services are purchased and utilized). All access is recorded and audited.

Retention and Deletion of Personal Data

Upon termination of the Cortex XSOAR service, data in active systems will be marked inactive and removed from the active systems. Permanent deletion of all data may take up to an additional 180 days following termination of the Cortex XSOAR service.

Security of Personal Data

Palo Alto Networks supports a defense-in-depth security model to help protect the customer's data at all stages of its lifecycle, in transit, in memory, and at rest, as well as through key management.

- The Trust 360 Program details the corporate-wide security, compliance, and privacy controls in place to protect our customers' most sensitive data.
- Palo Alto Networks Information Security Measures document details the technical and organizational measures that will be implemented by us to secure systems, processes and data. This document forms part of Palo Alto Networks Data Protection Addendum.

Resources

For more general information about Palo Alto Networks Privacy and Security Practices, please visit our Trust Center. Additional product-specific information can be found here:

- Cortex XSOAR Product Help Center
- Cortex XSOAR 8 FAQs
- Cortex XSOAR datasheet

About This Datasheet

Please note that the information provided with this Datasheet may be subject to change, provided that such change will not result in a material degradation of the security posture of the platform. Information concerning warranties and compliance with applicable laws may be found in Palo Alto Networks End User License Agreement.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com