Corelight Investigator Privacy Datasheet

This Privacy Datasheet document describes the personal data processed by Corelight's Investigator product. Corelight Investigator a cloud-native platform that is built on Amazon Web Services ("**AWS**").

Corelight Investigator Overview

Corelight Investigator is a cloud-based software as a service (SaaS) platform that streamlines network security investigations by providing threat detection, incident response, log search and storage capabilities. A customer's deployed Corelight Sensors transmit network data and alerts ("**Network Data**") to Corelight Investigator. Corelight Investigator processes this Network Data to generate detections which are then displayed back to the customer via Corelight Investigator's multifaceted user interface. Corelight Investigator also provides incident response workflows, enabling customers to view, triage and investigate the detections and alerts using the context of additional Network Data generated by the Corelight Sensors.

Categories of personal data processed and stored by Corelight Investigator

Data Source	Data Elements	Categories of Personal Data	Purpose of Processing
Network Data	Logs Session data Telemetry Threat intelligence data Threat detection information Raw packet capture data Network traffic metadata	Full name Username Email Phone number Title Location IP address Device name / hostname Network activity WiFi Serial number	Provision of the cloud product offering

Access to the personal data processed by Corelight Investigator

The table below outlines who can access personal data and the purpose of the access.

Personal Data Source	Who Has Access	Purpose of the Access
Network Data	Customer	Use of the cloud product offering (as determined by each customer in connection with deployment of the product).
	Corelight*	For platform management, maintenance, and support purposes.

**Only limited Corelight personnel have access to Corelight Investigator's production environment through authenticated, audited, and controlled access.*

How Corelight protects personal data processed by Corelight Investigator

Corelight Investigator's technical and organizational security measures ("**Security Measures**") are published here.

Corelight Investigator personal data retention and deletion practices

The personal data retention practices and the purpose of such retention are outlined below.

Personal Data Source	Retention Period	Purpose of Retention
Network Data	Customer: By default, Investigator retains: (a) alerts and detections for a ninety-day period; and (b) Zeek and Suricata logs for a thirty-day period unless additional log retention days are purchased.	Use of the cloud product offering (as determined by each customer in connection with deployment of the product).
	Corelight: For duration of the subscription term purchased by customer, subject to the retention periods for specific data elements above.	For platform management, maintenance, and support purposes

Portability of personal data processed by Corelight Investigator

Data may be exported from Corelight Investigator by the customer through the Corelight Investigator user interface or via API.

Data center locations where Corelight Investigator processes personal data

Personal data may be stored in the following data center locations.

Personal Data Source	Data Center Provider	Data Center Location
Network Data	AWS	Customers have the ability to select one of the following regional data center locations: • Germany • UAE • United States

Corelight Investigator Subprocessors

A list of the subprocessors Corelight utilizes to provide Corelight Investigator is available at www.corelight.com/legal/subprocessors.

Compliance

Data Processing Addendum

Corelight processes all personal data in accordance with Corelight's Data Processing Addendum ("**DPA**").

Cross-Border Data Transfers

Corelight's DPA incorporates the EU Standard Contractual Clauses related to the lawful use of personal data across jurisdictions.

Security Certification

Corelight Investigator is a SOC2-audited service built on top of AWS. To obtain a copy of Corelight Investigator's SOC 2 Type 2 audit report, please visit Corelight's Trust & Compliance self-service portal.