DARKTRACE | Google Security Operations

Darktrace and Google Security Operations

Solution Overview

The Darktrace / ActiveAI Security Platform is built on industry-leading Self-Learning AI ™ that learns the normal behavior of an organization to proactively find and stop known and novel threats.

It takes a business-centric view of an organization's network, email, identities, and more to detect and neutralize novel threats in real time.

Google Security Operations offers a unified experience across SIEM, SOAR, and threat intelligence to drive better detection, investigation, and response. By combining Darktrace's unique understanding of an environment with Google's centralized platform and threat intelligence, organizations can streamline their SOC workflow and respond to threats at the earliest stage.

Use Cases

- **Automated** Alert Aggregation and Correlation
- **Targeted** Threat Hunting
- **Enhanced** Threat Detection
- **Streamlined** Incident Response

More Information

Learn more about how to integrate Darktrace with Google Security Operations here.

Key Benefits

Unified SOC Investigation

Darktrace / Cyber AI Analyst ™ reduces thousands of events to a few relevant alerts, helping security teams focus on priorities for the business. Incidents are automatically sent to Google Security Operations and correlated with Google curated detections and alerts from other security tools, presenting SOC analysts with a single threat-centric case. **Gemini** provides an AI generated summary of each case including an easy-to-understand writeup of the situation and recommended next steps. **By leveraging multiple layers of AI investigation, organizations benefit from a reduced case workload while improving incident response times.**

Streamlined Response Workflow

Darktrace Autonomous Response takes immediate action to stop anomalous activity at the first sign of a potential threat. Customizable playbooks in Google SecOps can be layered on top to enrich cases with threat telemetry, take additional response actions, and escalate to the appropriate teams. **Threats are stopped in their tracks while security teams are presented with all relevant data for a streamlined investigation.**

Power of Business & Attacker-centric Data

Darktrace provides a unique understanding of the normal behavior for an organization, while Google Threat Intelligence has unmatched visibility into the global threat landscape. Custom Search capabilities in Google SecOps enable targeted threat hunting in Darktrace, and **Darktrace alerts can be enriched with threat intelligence to provide organizations with a holistic view of their attack surface.**

How it Works

Darktrace / Cyber AI Analyst ™ Incidents and Model Alerts are shared with Google Security Operations via an API-based integration. Alerts are presented as Cases in Google SecOps and can also be configured with Playbooks to perform further enrichment or collect additional data from Darktrace or other sources.

© 2026 Darktrace Holdings Limited. All rights reserved.