Chronicle Security Operations

The modern, AI-powered security operations platform for the modern SOC

Chronicle's modern, cloud-native SecOps platform combines Google's hyper-scale infrastructure along with unparalleled visibility and understanding of cyber adversaries to provide security teams with curated outcomes that proactively uncover the latest threats in near real-time, and enable them to detect, investigate and respond with speed and precision.

Product Highlights

- Ingest and analyze your data at Google speed and scale

- Proactively find and defend against attacks in near real-time

- Elevate your team's talent and productivity with generative AI

Why Chronicle Security Operations?

Say goodbye to legacy SIEMs and hello to a modern security operations platform.

Google scale and speed

Eliminate security blind spots by ingesting, normalizing, analyzing and searching all security telemetry at Google scale and speed.

Applied threat intelligence

Proactively uncover and defend against novel attacks in near real-time without extensive custom engineering. Curated outcomes apply Google's vast threat and exposure visibility to your unique environment.

AI-infused productivity

Elevate your team's talent and productivity with a unified platform infused with generative AI and expert help when you need it before, during and after an incident.

Google Cloud

Transform SecOps to proactive cyber defense

Eliminate blind spots. Ingest and analyze your security telemetry at scale with 12 months of hot data retention.

Detect more. Engineer less. Leverage curated detections from Google and easily build your own context and risk-aware detections using Yara-L.

Get to ah-ha quicker. "Google search" your data at lightning speed and get the root cause quickly with a context-rich investigation workbench.

Work threats, not alerts. Leverage unique threat-centric case management that combines reactive and proactive actions for analysts

Get ahead of threat actors. Automatically correlate active breach threat intelligence by Mandiant with your data to receive early warning signals.

Respond with speed and precision. Build rich playbooks to automate repetitive tasks and reduce toil.

"
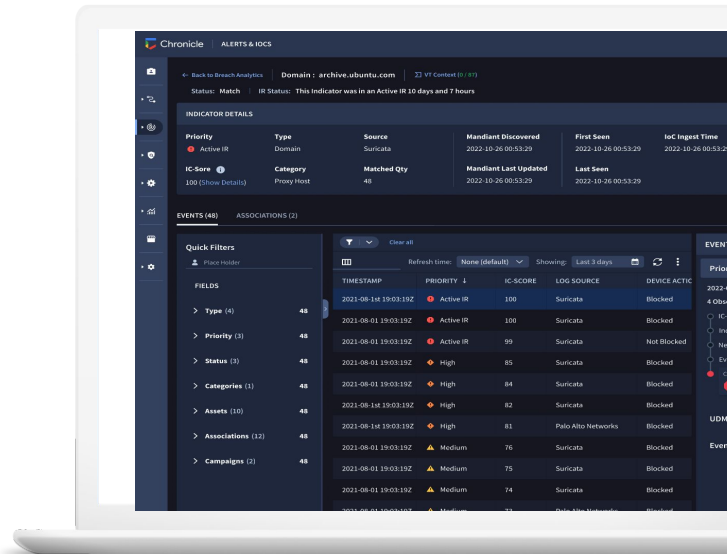
Chronicle is one of the few security platforms that continues to innovate for security professionals and to make their lives easier.

Principal Engineer, 30B+ Bank

Gartner
Peer Insights™

Let's modernize your SOC.
Experience Chronicle Security Operations today. Visit us at https://chronicle.security for more information.