

Chronicle Security Operations

Simplify threat detection, investigation and response (TDIR) using the intelligence, speed and scale of Google

The scope and scale of securely operating in today's threat landscape and complex environment can be daunting. Chronicle Security Operations is a modern, cloud-native suite that enables security teams to detect, investigate and respond to cyber threats with the speed, scale and intelligence of Google.

Chronicle SIEM

A cloud-native security information and event management (SIEM) solution designed to enable security teams to detect, investigate and hunt threats.

Chronicle SOAR

A modern security orchestration automation and response (SOAR) solution driving effective response to threats with playbook automation, case management.

Threat Intelligence

Detect advanced attacks, and drive context-driven investigations with threat intelligence via Google Cloud Threat Intelligence and Virustotal .

What makes Chronicle different



Eliminate security blindspots by ingesting all your data at a disruptive cost

- Leverage **Google's cloud-native scalable infrastructure** to store & analyze all your security telemetry
- **12 months of hot retention** to enable longer IoC correlation & uncover persistent threats
- **Fixed & predictable yearly cost** decoupled from capacity, compute and log source count



Faster time to "aha" with insights at your fingertips

- **Sub-second search across petabytes** of information
- **Threat-centric approach** groups related alerts into threat-centric cases to streamline response
- **Powerful context and visualizations** surface the most relevant information to uncover insights



Democratize security operations by leveraging Google's unparalleled threat intelligence

- **Out-of-the-box detections** leverage Google's collective insights and threat intelligence
- **Packaged response playbooks** to address common security use cases
- **Expert help when you need it** with frameworks and advisory services

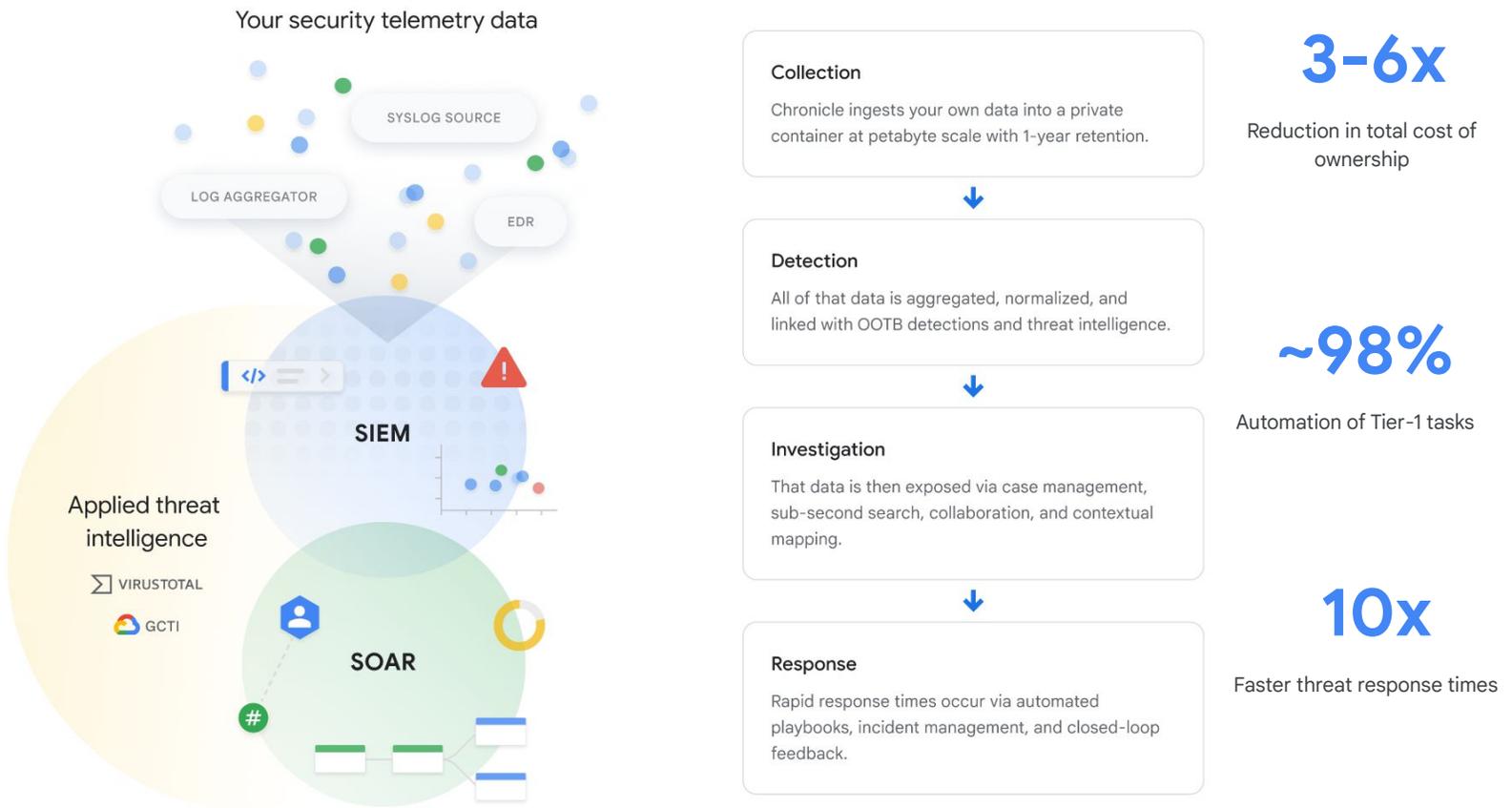


With Chronicle doing the correlation between all the threats, we can now identify the highest-priority threats. As a result, our team spends less time getting to the core information they need to address these incidents.

James Stinson, VP of Information Technology, Quanta Services

Chronicle Security Operations

Simplify threat detection, investigation and response (TDIR) using the intelligence, speed and scale of Google



Our customers trust us to look after their data, so our reputation is important to us. But the bad guys are out there and they're not going away. We feel Chronicle is the best tool available to us in countering potential attacks."

Neil Binnie, Head of Information Security and Compliance, Morgan Sindall

See how customers are driving security outcomes with Chronicle Security Operations at chronicle.security.