Google Cloud

Automate Attack Surface Reduction with Chronicle Security Operations

Proactively detect external exposures and streamline investigation and response in one platform.

Get ahead of potential threats and become more proactive with the combination of Chronicle Security Operations and Mandiant Attack Surface Management (ASM). Chronicle Security Operations offers a modern, cloud-native security operations platform that enables security teams to detect, investigate and respond to cyber threats with the speed, scale and intelligence of Google. Our customers eliminate security blind spots with the ability to ingest and analyze all relevant security telemetry, and proactively get ahead of threats by seeing their environments through an attacker's eyes.

Streamline Operations by Adding Threat Exposure Context to Investigations

Mandiant ASM collects asset and exposure information about an organization's distributed global infrastructure like an attacker would. The solution performs exhaustive discovery by scanning externally facing assets and cloud resources daily to identify software, architecture and configuration risks to your organization. It cross-checks over 250 data sources, including Mandiant Threat Intelligence, NIST National Vulnerability Database, and CISA's Known Exploited Vulnerability catalog, to assign severity levels and provide guidance for risk remediation.

Chronicle Security Operations & Mandiant ASM

Unify the analyst experience with proactive and reactive context at their fingertips. Apply Google's vast threat and exposure visibility curated to your environment to help you achieve critical security outcomes.

- ☑ Contextualize analyst investigations with exposure asset details and telemetry event data
- ☑ Automatically prioritize mitigation on the exposures being targeted
- ☑ Quickly find details on external assets and exposures using UDM Search
- ☑ Create playbooks and automate tasks based on external exposure cases
- ☑ Take action on new exposures within minutes, not days
- ☑ Centralize evidence of past and ongoing activity related to exposed assets

The combined power of Chronicle and Mandiant ASM enables customers to continuously identify and validate exploitable entry points into their organization, allowing the SecOps team to prioritize investigation and remediation efforts on the exposures that have the most potential impact.

Contact us to learn more about Chronicle Security Operations and Mandiant Attack Surface Management.