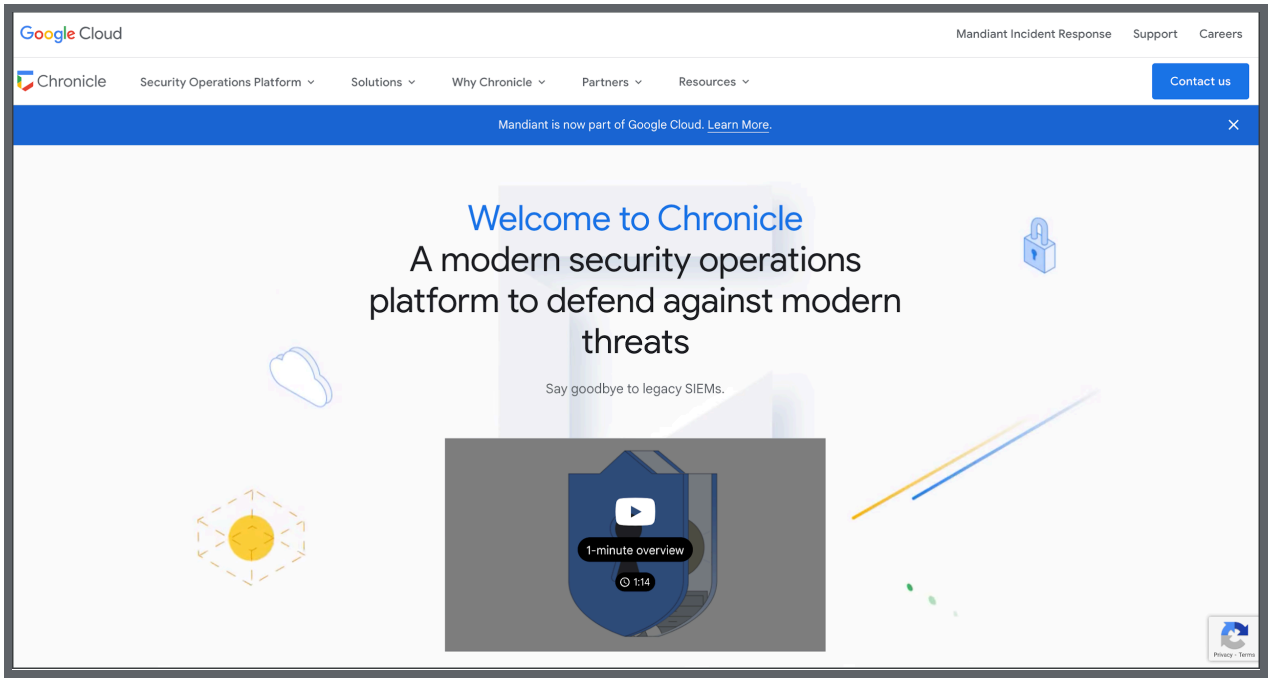
Incident response partners

Previously, you learned that part of a cloud security professional's role is identifying and responding to potential security alerts. You also learned that many alerts can turn into incidents. Luckily, there are tools, services, and frameworks that can help security teams improve their identification, analysis, and response process. In this reading, you'll explore Chronicle, Manidant, MITRE ATT&CK®, and VirusTotal. You'll also explore the benefits of these tools, services, and frameworks in the context of Google Cloud.

Google Cloud Chronicle

You've already learned about Chronicle. Now, you'll learn how Chronicle helps Security Operations (SecOp) teams.



Chronicle SIEM

Chronicle SIEM is a modern SecOps platform. It helps SecOps teams analyze and contextualize risky activity, and normalizes, indexes, correlates, and analyzes data. Chronicle also lets SecOps teams examine security information that goes back for months or longer.

Chronicle SIEM uses some of collection, detection, and investigation capabilities:

- **Collection:** Chronicle SIEM uses forwarders, which are lightweight software

components that support syslog, packet capture, and log management security information and event management (SIEM data storage areas), parsers (these store data mapping instructions), connectors, and webhooks (automated messages sent from apps). Data collection also uses ingestion APIs. These enable logs to be sent to the Chronicle Security Operations platform automatically. So, there's no need for additional software or hardware customer environments. With collection, there's also third party integrations with products from other cloud service providers.

- **Detection:** During detection, data is aggregated, or compiled into summaries, normalized with the Universal Data Model (UDM), and linked to threat intelligence and detections.
- **Investigation:** Chronicle investigates threats through search, collaboration, management, and analytics.

Chronicle SecOps (Chronicle SOAR)

Chronicle SecOps, also sometimes called Chronicle SOAR, is a cloud-native security operations platform that enables security professionals to analyze and mitigate security threats throughout their lifecycle. Chronicle SecOps offers security professionals many capabilities, including:

- **Data collection and ingestion:** Chronicle SecOps can ingest data from a variety of sources, including logs, network traffic, and endpoint data.
- **Data normalization and enrichment:** Chronicle SecOps normalizes and enriches data using the Universal Data Model (UDM), which makes it easier to analyze and search.
- **Threat detection and investigation:** Chronicle SecOps uses machine learning to detect threats, and provides a number of tools for investigating threats, including case management, search, and collaboration.
- **Incident response:** Chronicle SecOps provides a number of tools for responding to incidents, including automated playbooks and incident management.

Here are some of the other benefits of using Chronicle SecOps:

- **Improved threat detection:** Chronicle SecOps' machine learning capabilities can help detect threats that would be missed by traditional security tools.
- **Reduced time to resolution:** Chronicle SecOps' automated playbooks and incident management tools can help reduce the time it takes to resolve incidents.
- **Improved collaboration:** Chronicle SecOps' collaboration tools can help security teams work together more effectively to investigate and respond to threats.
- **Reduced costs:** Chronicle SecOps' cloud-native architecture can help reduce the costs associated with security operations.

Mandiant Platform

Mandiant assists users by improving existing security controls to help make it easier to identify malicious security incidents in a timely way. The Mandiant Advantage platform provides cloud security teams with real-time threat data and analysis expertise. It uses continuous security validation, detection, and response to help keep organizations secure from cyber threats. It can be used to create custom dashboards to view and filter relevant information and trends, as well as respond to threats faster. Mandiant also offers a variety of products and services that integrate with Chronicle.

Mandiant Breach Analytics for Chronicle

Mandiant Breach Analytics for Chronicle is a product that helps organizations identify and respond to active breaches. Breach Analytics for Chronicle uses Mandiant's threat intelligence to identify indicators of compromise (IoCs) in an organization's Chronicle data. It also provides a number of tools for investigating and responding to breaches.

Mandiant Hunt for Chronicle

Mandiant Hunt for Chronicle is a product that helps organizations hunt for and identify threats that are already present in their environment. It uses a variety of techniques, including machine learning and threat hunting to identify threats.

Enriching security data with Mandiant Threat Intelligence

Chronicle SecOps can ingest Mandiant Threat Intelligence data, which provides context and insights about threats, actors, and vulnerabilities. This enriched data can be used to improve threat detection and investigation.

Automating threat detection and response with Mandiant Security Validation

Chronicle SecOps can integrate with Mandiant Security Validation to automate the execution of Mandiant-authored security controls, and validate their effectiveness. This helps ensure that security controls are working as expected. Mandiant Security Validation can also help identify and remediate gaps in security posture.

Leveraging Mandiant Managed Defense expertise

Chronicle SecOps can integrate with Mandiant Managed Defense to provide 24/7 monitoring and response services from Mandiant experts. This can help reduce the burden on security teams, and ensure that threats are identified and responded to quickly and effectively.

VirusTotal

Users can use VirusTotal to analyze suspicious files, domains, IPs, and URLs to help detect malware and other breaches, and share them with the security community.

VirusTotal is used for event enrichment and as an IoC threat feed. Users can search VirusTotal's dataset for malware samples, URLs, domains, and IP addresses using many different criteria. They can identify files that are similar to real issues they've encountered. They can also download samples that match their search criteria so they can examine them in more detail.

The integration of VirusTotal malware intelligence with Chronicle means customers can triage and investigate within the Chronicle interface. They can also conduct enriched detection and threat hunting workflows. This provides rich context to critical workflows to orient security professionals on the importance of a detection alert or scope of a threat in the environment.

These advanced enrichments, along with VirusTotal intelligence, empower customers to:

- **Enhance the fidelity of detections:** The enrichments are natively baked in with customer telemetry, which provides richer filtering capabilities, and opportunities to hunt over an enhanced data set aligned to their critical business security requirements.
- **Scope and prioritize alerts:** Customers can immediately see relevant file context and relationships to known Internet properties at detection time, instead of through the stages of manual human triage.
- **Respond to critical alerts faster:** Customers no longer need to leave Chronicle to get the needed enrichments to understand the reputation of a binary. All of that data is enriched in the results.

MITRE ATT&CK® framework

MITRE ATT&CK® is a TTP framework that's a knowledge base of malicious tactics and techniques that have been gathered from real-world situations and scenarios. This knowledge base has been used by private entities, government agencies, and cybersecurity organizations to develop threat models.

Chronicle can be used to integrate MITRE ATT&CK® components into security strategies. Chronicle's Curated Detection page provides information about each of the rule sets active for your Chronicle account, including:

- **Last updated:** Indicates the time the GCTI last updated the rule set
- **Enabled Rules:** Indicates which of the Precise and Broad rules are enabled for each rule set
    - Precise rules find malicious threats with a high degree of confidence.

    - Broad rules search for suspicious behavior that may be more common and produce more false positives. Both Precise and Broad rules might be available for a rule set.
- **Alerting:** Indicates which of the Precise and Broad rules have alerting enabled for each rule set
- **Mitre Tactics:** Identifies the Mitre ATT&CK® tactics covered by each rule set
    - Mitre ATT&CK® tactics represent the intent behind malicious behavior.
- **Mitre Techniques:** Identifies the Mitre ATT&CK® techniques covered by each rule set
    - Mitre ATT&CK® techniques represent specific actions of malicious behavior.

Key takeaways

In this reading, you examined some of Google's incident response partners, and learned how they work together to assist users in detecting and responding to threats and incidents.

Resources for more information

Check out these links for more information about Google Cloud's response partners:

- Google Cloud Chronicle's website
- Mandiant's website
- MITRE ATT&CK®'s website
- VirusTotal's website
- Use cases for VirusTotal within Chronicle