Incident response best practices with Chronicle SOAR

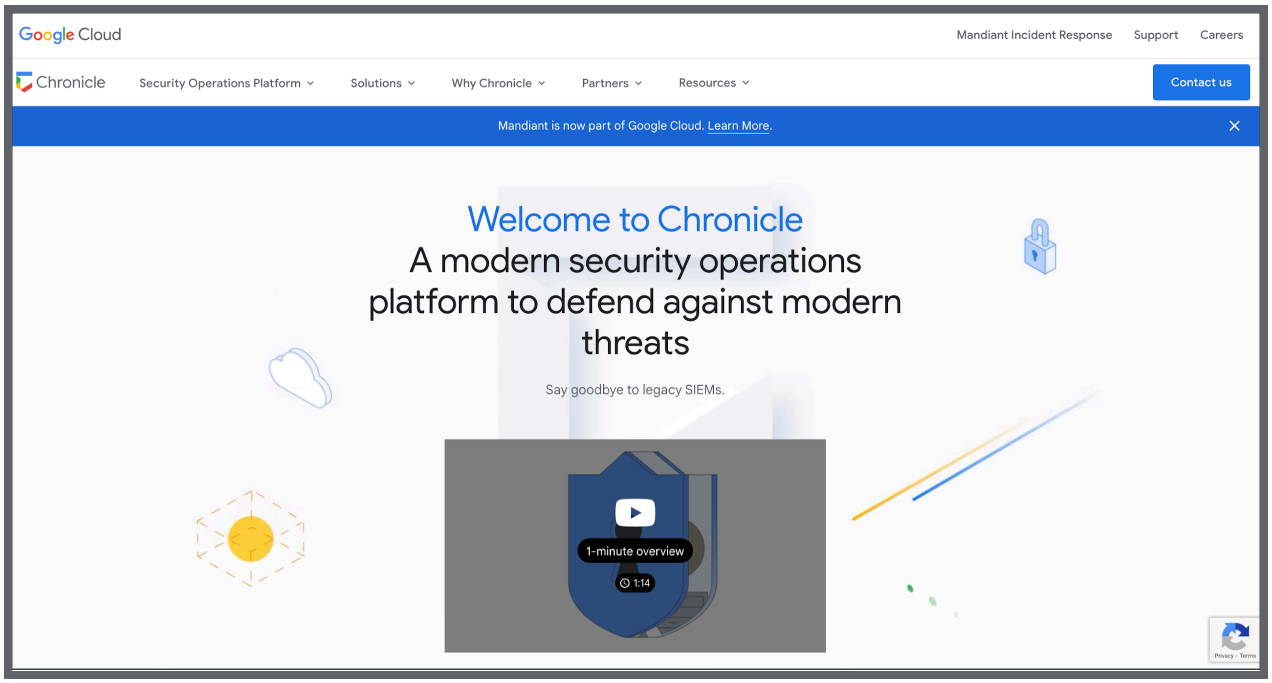
So far, you've learned that how you respond to an incident depends significantly on your preparedness. You've also learned that security orchestration, automation, and response (SOAR) is a collection of applications, tools, and workflows that use automation to respond to security events. In this reading you'll dive deeper into SOAR, and learn a few effective practices for using it.

Security orchestration, automation, and response (SOAR)

SOAR has three key software capabilities: automation; case and workflow management; and a centralized means of accessing, querying, and sharing threat intelligence.

Components of SOAR

Each cloud provider has their own security platform, so there are some differences between the platforms of different cloud providers. The examples in this reading are based on Google Cloud's Chronicle platform.



Connectors

Connectors represent the ingestion point for alerts into SOAR. Ingestion means importing data files from different sources into a single storage medium, like a database. Connectors translate raw data from various sources into SOAR data. Alerts – or equivalent data – come from 3rd party tools, then the connectors forward normalized data into the data processing layer. Security platforms like Chronicle provide out-of-the-box connectors for modern security systems, and software development kits (SDKs) in Python, or other popular coding languages. Chronicle's SDK is written in Python, and offers the flexibility to develop new connectors as needed.

Cases, alerts, and events

A case consists of alerts that were ingested from a variety of sources by connectors. Each case has one or more security events. Events are observable occurrences on a network, system, or device. The events are analyzed as soon as they're ingested into the platform. Their indicators, destinations, and artifacts – among other things – are extracted into objects called entities. An artifact is a digital object, like a file or image, that's used in the software development lifecycle.

Entities

Entities are objects that represent points of interest that were extracted from alerts. These can include indicators of compromise (IOCs) and artifacts. Entities can be automatically tracked and grouped without human intervention. Entities can also be used to hunt for malicious activity based on the relationships between them.

Entities are created through a process of mapping and modeling. This process allows you to create entities that are related to a specific model family, and to explore the connections between them in a case. Entities also provide more context to an investigation in a case.

SOAR playbooks with Chronicle

A playbook is an automation process. Playbooks can be triggered manually, or they can be triggered by a predefined trigger. For example, you trigger a playbook for each alert that contains the product name "mail." So, your playbook attaches to each alert that's ingested into Chronicle SOAR from the "mail" product.

Each playbook consists of actions configured to run manually or automatically based on the scope you've defined for the alert entries.

The actions occur in a defined order based on conditions, creating a tree of actions. The playbook reaches a resolution for the triggering alert when the final action is completed.

SOAR Effective Practices

If you're considering using automation to execute tasks, ask yourself these questions:

- Is it a routine task?
- Is this something that needs to be done on a regular basis?
- Is it a detail-oriented task?
- Is there a specific set of actions that have to be completed precisely?
- Is it a time consuming task?
- Can automating this set of actions save a significant amount of time for my team?

If you answer yes to any of these questions, automation like SOAR will be able to help you.

Here are some other tips for using SOAR:

- **SOAR is about standards:** SOAR includes scripts, procedures, playbooks, and code. Before deploying the solution, you need to have these standards in place.
- **Data hygiene:** You need to know what to discard and what to keep. Put purging procedures in place to discard what you don't need.
- **Humans are involved:** One of SOAR's main purposes is to reduce the reliance on human intervention, but it's still a good idea to have a reviewer examine the data, and occasionally adjust the workflows and playbooks.

Chronicle SOAR helps you with:

- Incident detection and investigation
- Automating incident responses

Automating incident responses with SOAR

Security automation is the execution of actions on IT systems and security tools by machines. Teams can use SOAR tools to define standardized automation steps and a decision-making workflow. SOAR provides enforcement, status tracking, and auditing capabilities.

SOAR also uses orchestration, or the ability to automate responsive actions and coordinate decisions, to automate responsive actions based on an assessment of environmental states and risks.

Here's an example: When processing a suspicious email, the SOAR tool investigates the sender. First, it investigates whether the sender has a bad reputation by using threat intelligence and DNS tools to confirm the email's origin. Then, the tool automatically extracts hyperlinks. Next, it validates these hyperlinks via URL reputation. Then it runs and monitors the code in a safe environment. If there's a confirmed incident, a playbook is run to find all messages from the

same sender in the email system. Then, the SOAR tool searches for the same links and attachments. Once it finds them, it quarantines those messages, links, and attachments.

Key takeaways

As a cloud security professional, you can leverage automation and orchestration to your advantage with SOAR. SOAR includes connectors, cases, events, and playbooks. SOAR also includes incident responses, and can be used by cloud security teams to analyze and make suggestions for a response. When using SOAR, ensure you have standards in place, and know which data to keep. And remember, it helps to have someone review the data and make any needed adjustments to the playbooks and workflows.