Google Cloud

Playbooks' role in incident response

So far, you've learned that automation and playbooks have a critical role in incident response for cloud cybersecurity professionals, like those in Security Operations (SecOps) using Chronicle SOAR. Recall that Chronicle SOAR is Google Cloud's security orchestration, automation, and response platform. Similar to other SOAR platforms, Chronicle SOAR is a collection of applications, tools, and workflows that use automation to respond to security events.

In this reading, we'll provide a more in-depth understanding of how SecOps professionals use playbooks for automation in the context of incident response.

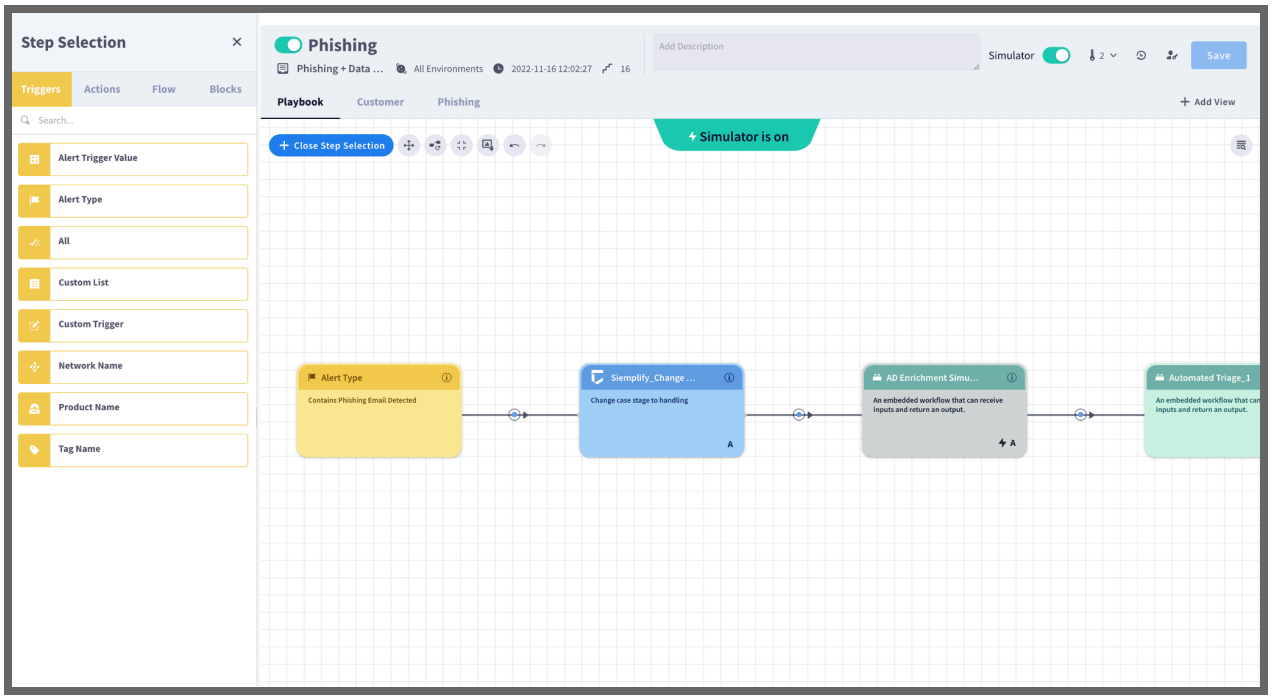
Concept of playbooks

As a security professional, you can harness the power of SOAR platforms using a playbook, which is a set of processes that provides details about any operational action. Playbooks are reusable workflows you can use to define a series of steps to take to respond to a security incident. With SOAR, you can use playbooks to respond manually or automatically to a wide range of tasks, including:

- Triaging incidents
- Gathering information
- Conducting investigations
- Remediating incidents
- Escalating incidents
- Generating reports
- Communicating with stakeholders

A playbook's role in automating incident response actions

You'll design playbooks to trigger automatically or manually, depending on your organization's needs. For example, you may need a phishing playbook to **trigger containment actions** automatically when a high-priority phishing email alert is generated. The incident response might include: identifying and blocking malicious IP addresses, alerting the affected users, and resetting compromised passwords.



Other automated playbook response examples include:

- **Gathering information** about an incident, like collecting logs, running scans, and querying security tools
- **Enriching alerts and incident data** with additional context with information from external sources, like threat intelligence platforms and vulnerability scanners
- **Rolling back an application** to a known good state
- **Sending notifications** to stakeholders about an incident, like email or text messages

Manual playbook response examples include:

- **Investigating incidents** and identifying the root cause
- **Communicating** with stakeholders or a third-party vendor, like a forensic investigator or incident response team
- **Developing and implementing remediation plans**, like removing malware or patching vulnerabilities
- **Approving the restoration of the systems** to normal operations

Examples of different types of playbooks in Chronicle SOAR

Chronicle SOAR supports a variety of different playbooks in which you can combine manual and automated tasks, including:

- **Triage playbooks:** Triage playbooks help you to quickly assess the severity and impact of an incident. They may include tasks to prioritize alerts, collect information, assess potential impact, and learn the difference between true incidents and false positives.
- **Investigation playbooks:** Investigation playbooks help you investigate the root cause of an incident and gather evidence. They may include tasks to analyze logs, query security tools, and interview witnesses.
- **Remediation playbooks:** Remediation playbooks help you contain and eradicate an incident. They may include tasks to isolate affected systems, patch vulnerabilities, and implement security controls.

Best practices for designing effective playbooks

When designing effective playbooks, it's important to consider these best practices:

- **Clarity and conciseness:** Playbooks should be clear, concise, and easy to follow.
- **Flexibility:** Playbooks should be modular in order to handle different types of incidents and scenarios.
- **Maintenance:** Maintain playbooks regularly with updates to reflect changes in your organization's security environment and threat landscape.
- **Reliability:** Ensure playbooks have reliability so that you're able to execute them successfully and effectively mitigate incidents without errors.
- **Repeatable:** You should be able to run playbooks consistently, with the same, predictable results each time. This can help reduce the impact of the incident.
- **Reusability:** You should be able to use playbooks for different types of incidents, instead of creating a new playbook for each incident. This can save time and effort.
- **Testability:** Test playbooks regularly to ensure that they're working as expected.

Note: It's important to test playbooks regularly to ensure that they're working as expected. Otherwise, there's a risk they won't work as expected when needed. This can delay or hinder the incident response process and lead to more serious consequences.

Managing and maintaining playbooks

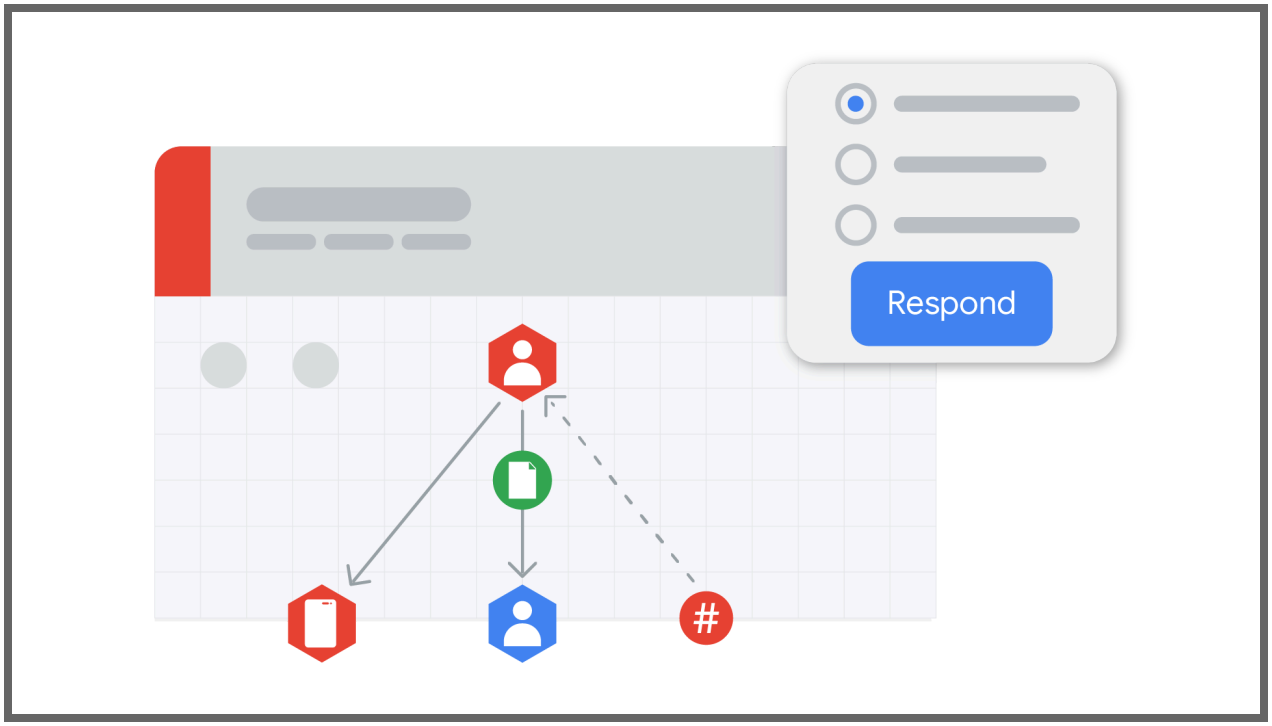
It's important to have a process in place for managing and maintaining playbooks. This process should include:

- **Version control:** Version control playbooks to track changes perform rollbacks if necessary.
- **Approval process:** Establish and follow a process for approving new playbooks and changes to existing playbooks.
- **Training:** Train all security professionals on how to use playbooks effectively.
- **Monitoring:** Monitor how security professionals use playbooks and monitor their performance to identify areas for improvement.

Use cases for playbooks in Chronicle SOAR

Here are some examples of automated use cases for playbooks in Chronicle SOAR:

- **Incident response** process, from triage to remediation
- **Security compliance** tasks, like vulnerability scanning and log management
- **Threat hunting** activities, like searching for suspicious activity in logs and security events
- **Security operations center (SOC)** tasks, like alert triage, case management, and reporting



Pro tip: Use Chronicle SOAR's playbook library to get started quickly. Chronicle SOAR provides a library of pre-built playbooks for common incident response scenarios. You can customize these playbooks to meet the specific needs of your organization.

Key takeaways

In this reading, you learned how you can use playbooks for automation in the context of incident response. Automation and playbooks are essential for you, as a security professional. With Chronicle SOAR, you can design playbooks with reusable automatic or manual workflows that define a sequence of steps to respond to a security incident. Your playbooks can help you effectively respond to a wide range of security incidents tasks, like enriching incident data, collecting evidence, isolating infected systems, notifying stakeholders, and remediating the incident. And remember, regularly test and maintain your playbooks to ensure that they're up-to-date and effective!

Resources for more information

Check out these resources to learn more about using playbooks for automation in the context of incident response:

- Chronicle SOAR documentation: https://cloud.google.com/chronicle/docs/soar
- National Institute of Standards and Technology (NIST) Cybersecurity Framework: https://www.nist.gov/itl/smallbusinesscyber/planning-guides/nist-cybersecurity-framework
- Top Security Playbooks 2022-2023: https://services.google.com/fh/files/misc/top_security_playbooks_2022.pdf