Original page: https://cloudskillsboost.google/paths/187 (https://cloudskillsboost.google/paths/187)

(/)

Share on LinkedIn Feed Twitter Facebook

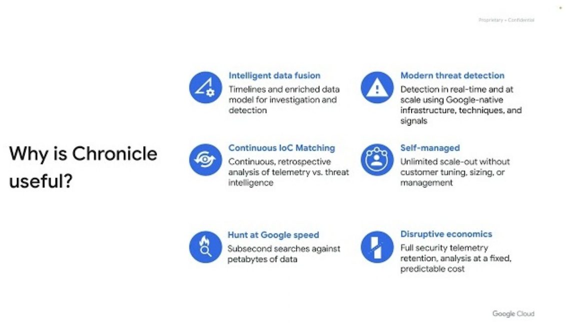
Apply your skills in Google Cloud console

Google SIEM & SOAR Learning Path

school 5 activities update Last updated over 1 year person Managed by Google Cloud

The Chronicle learning path covers the SIEM and SOAR tools available in Google Cloud. The courses in this path will showcase the skills needed within Chronicle to parse data, build rules, develop playbooks, respond to incidents and even integrate with 3rd party capabilities. This broad set of content will prepare you on your cloud security journey with Chronicle SIEM and SOAR.

Start learning path



Proprietary + Confidential

Why is Chronicle useful?

Intelligent data fusion
Timelines and enriched data model for investigation and detection

Modern threat detection
Detection in real-time and at scale using Google-native infrastructure, techniques, and signals

Continuous IoC Matching
Continuous, retrospective analysis of telemetry vs. threat intelligence

Self-managed
Unlimited scale-out without customer tuning, sizing, or management

Hunt at Google speed
Subsecond searches against petabytes of data

Disruptive economics
Full security telemetry retention, analysis at a fixed, predictable cost

Google Cloud

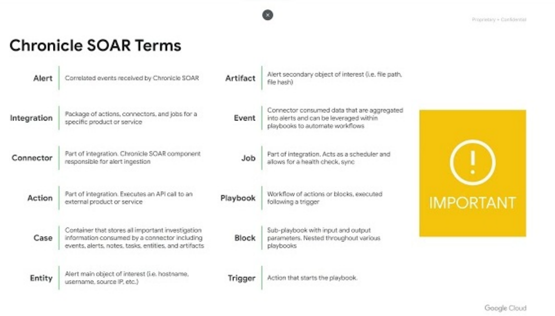
(/paths/187/course_templates/442)

01 Security Practices with Google Security Operations - SIEM

book Course
access_time 8 hours
show_chart Intermediate

Learn the technical aspects you need to know about Chronicle and how it can help you detect and action threats.

Start course



Proprietary + Confidential

Chronicle SOAR Terms

Alert	Correlated events received by Chronicle SOAR	Artifact	Alert secondary object of interest (i.e. file path, file hash)
Integration	Package of actions, connectors, and jobs for a specific product or service	Event	Connector consumed data that are aggregated into alerts and can be leveraged within playbooks to automate workflows
Connector	Part of integration. Chronicle SOAR component responsible for alert ingestion	Job	Part of integration. Acts as a scheduler and allows for a health check, sync
Action	Part of integration. Executes an API call to an external product or service	Playbook	Workflow of actions or blocks, executed following a trigger
Case	Container that stores all important investigation information consumed by a connector including events, alerts, notes, tasks, entities, and artifacts	Block	Sub-playbook with input and output parameters. Nested throughout various playbooks
Entity	Alert main object of interest (i.e. hostname, username, source IP, etc.)	Trigger	Action that starts the playbook.

Google Cloud

(/paths/187/course_templates/569)

02 SOAR Fundamentals

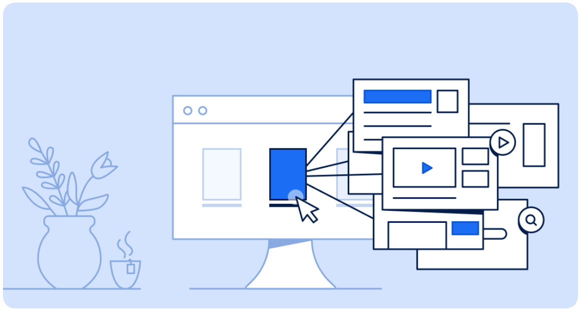
book Course

access_time 3 hours 45 minutes

show_chart Intermediate

This course will familiarize you with the core functionality of Chronicle, including the user interface, connections, and settings.

Start course



(/paths/187/course_templates/690)

03 Google Security Operations - SIEM Rules

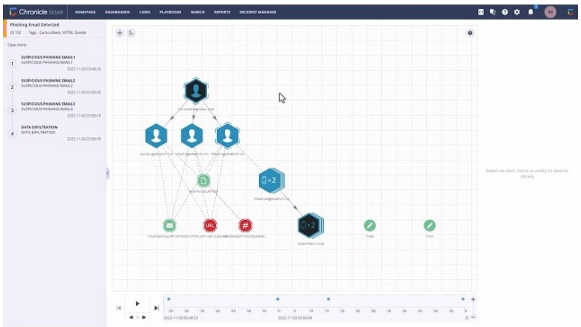
book Course

access_time 4 hours 15 minutes

show_chart Introductory

Get hands-on experience applying and building rules for Chronicle. You learn what YARA-L is and how to customize & create event rules.

Start course



Phishing Email Detected

ID 102 Tags: CarbonBlack, MITRE, Qradar

Case Alerts

1 SUSPICIOUS PHISHING EMAIL1
SUSPICIOUS PHISHING EMAIL1
2022-11-03 03:49:25

2 SUSPICIOUS PHISHING EMAIL2
SUSPICIOUS PHISHING EMAIL2
2022-11-03 03:50:09

3 SUSPICIOUS PHISHING EMAIL3
SUSPICIOUS PHISHING EMAIL3
2022-11-03 03:50:16

4 DATA EXFILTRATION
DATA EXFILTRATION
2022-11-03 03:50:59

Select an alert, event or entity to view its details

(/paths/187/course_templates/567)

04 Google Security Operations - SOAR Analyst

book Course

access_time 4 hours 15 minutes

show_chart Intermediate

This course helps you understand how to use Chronicle to properly handle security incidents.

Start course