SIEM & SOAR on Google Cloud

Course Overview

The course on Chronicle covers the SIEM and SOAR tools available in Google Cloud. This course 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.

Duration: 03 days / 24 hours

Level: Professional

Prerequisites: Google Cloud and Cybersecurity Fundamentals are the prerequisite for this learning path.

Course Outcome: Learner will be prepared to work on Google Chronicle SIEM and SOAR

Table of Content

Security Practices with Google Security Operations - SIEM

- Foundations of Chronicle
- Collecting and Parsing Data
- Access
- Building Rules to Find Threats
- Investigating Threats
- Responding to Threats

SOAR Fundamentals

- Chronicle SOAR Fundamentals
- Platform Overview
- Case Management
- User and Environment Management
- Integrations Connectors and Ontology
- Playbooks Views
- Settings
- Dashboards Reports
- IDE
- Collaborator
- Incident Manager
- Remote Agents

Google Security Operations - SIEM Rules

- Chronicle SIEM: Introduction & Single Event Rules
- Chronicle SIEM: Multi Event Rules
- Chronicle SIEM: Outcomes & Functions

Google Security Operations - SOAR Analyst

- Introduction
- Chronicle SOAR Analyst

Google Security Operations - SOAR Developer

- Introduction
- Chronicle SOAR Developer