



AI Fluency for Enterprise Leaders

Course description

Detect, Investigate, and Respond to Security Threats with Cloud-Native Security Operations. Learn how centralized security monitoring, threat detection, investigation, and response help organizations strengthen their security posture on Google Cloud.

Through real-world security scenarios, demonstrations, guided activities, and practical exercises, learners will understand how security operations teams use centralized logging, threat detection, investigation, and response capabilities to protect cloud environments. The course also introduces the role of Security Command Center Enterprise and related Google Cloud security capabilities in building an effective security operations practice.

- Course level: Intermediate
- Duration: 1 day

Activities

This course includes instructor-led training, security operations demonstrations, scenario-based learning, log analysis exercises, threat investigation activities, incident response simulations, group discussions, knowledge checks and quizzes, and real-world security case studies to reinforce learning.

Course objectives

In this course, you will learn to:

- Understand the purpose and core components of a SIEM solution.
- Explain how security logs and telemetry are collected and analyzed.
- Identify common security threats and suspicious activities.
- Understand how SIEM supports threat detection and investigation.
- Correlate security events to identify potential incidents.
- Understand the security operations lifecycle from detection through response.
- Explain the role of Google Cloud security services in a SIEM architecture.
- Understand how Security Command Center Enterprise supports security operations.
- Apply basic incident investigation and response workflows.
- Recognize best practices for building an effective cloud security operations capability.

Key features

- Security Event Correlation
- Interactive Security Operations Learning

Intended audience

This course is intended for:

- SOC Analysts
- Security Analysts
- Security Engineers
- Cloud Security Engineers
- Cloud Architects
- Security Architects
- DevOps Engineers
- Cloud Operations Teams
- IT Administrators
- Incident Response Teams
- Cybersecurity Professionals

- Security Managers
- Technology Leaders

Prerequisites

We recommend that attendees of this course have:

- Basic understanding of cloud computing concepts recommended.
- Familiarity with basic cybersecurity concepts is helpful but not mandatory.
- No prior SIEM implementation experience is required.

Products covered

- Google Cloud Security Command Center Enterprise
- Google Cloud Logging
- Cloud Monitoring
- Identity and Access Management (IAM)
- Google Cloud security services
- Security operations and SIEM concepts Note: The course is designed as a customized SIEM/security-operations offering. The current Google Cloud ILT catalog lists Security Command Center Enterprise Essentials as a Cloud Sparks course, Logging, Monitoring, and Observability in Google Cloud as a 2-day Technical course, and Security in Google Cloud as a 3-day Technical course.

Certification details

CloudThat Course Completion Certificate will be awarded to all learners who successfully complete the training.

FAQs

Who should attend this course?

This course is designed for SOC analysts, security engineers, cloud security professionals, architects, DevOps teams, and IT professionals involved in monitoring and protecting cloud environments.

Do I need prior SIEM experience?

No. The course introduces SIEM concepts from the fundamentals and progressively moves into threat detection and investigation.

What is SIEM?

SIEM stands for Security Information and Event Management. It brings together security data and events to help organizations detect, investigate, and respond to security threats.

Is Security Command Center covered?

Yes. The course introduces Security Command Center Enterprise and its role in cloud security operations.

Will I learn how to investigate security incidents?

Yes. Learners work through security scenarios involving event analysis, threat investigation, incident prioritization, and response decisions.

Does the course cover Google Cloud logging?

Yes. The course introduces security logs and telemetry as part of centralized security monitoring and investigation.

Is this a SOC-focused course?

Yes. The course is designed around the core SOC workflow of monitor → detect → investigate → respond.

Is this a technical implementation course?

It is an intermediate, security-operations-focused course. It includes technical demonstrations and practical investigation activities but does not require learners to be expert security engineers.

Can the course be customized?

Yes. The content can be customized around the customer's security architecture, SOC processes, Google Cloud environment, compliance requirements, and preferred use cases.

Will I receive a certificate?

Yes. A CloudThat Course Completion Certificate will be awarded upon successful completion.