Google Cloud Cyber Security Engineer

Course Overview

A Cyber Security Engineer is a digital guardian, a cyber sentinel at the frontlines of Google Cloud security, safeguarding valuable assets from the world of cybercrime. This learning path guides you through a curated collection of concepts and labs that provide you with real-world, hands-on experience using Google Cloud technologies essential to the Cyber Security Engineer role.

Duration: 10 days / 80 hours

Level: Professional

Prerequisites: There is no prerequisite for this learning path. Basic knowledge of Linux and Network administration is helpful but not mandatory.

Course Outcome: Learner will be prepared to work as a Cyber Security Engineer on Google Cloud Platform

Table of Content

Introduction to Security Principles in Cloud Computing

- Introduction to cloud computing
- Security in the cloud
- The security lifecycle
- Cloud security analyst roles and responsibilities

Strategies for Cloud Security Risk Management

- Introduction to frameworks within security domains
- Risk management and security frameworks, regulations, and standards
- The compliance lifecycle
- Cloud tools for risk management and compliance

Cloud Security Risks: Identify and Protect Against Threats

- Access control and identity management
- Threat and vulnerability management
- Cloud Native Principles of Ephemerality and Immutability
- Data Protection and Privacy

Detect, Respond, and Recover from Cloud Cybersecurity Attacks

- Detection foundations
- Detection in practice

- Incident response management and attack mitigation
- Incident recovery

Put It All Together: Prepare for a Cloud Security Analyst Job

- Cloud security-focused career resources
- The capstone project