Google Cloud

Resources

Introduction to SecOps on GDC

Explore these resources to enhance your knowledge and gain a deeper understanding of the course material.

Module 1 resources

- Google Cloud's digital sovereignty vision
- Kubernetes' Operator Pattern
- GDC publicly-available documentation:
  - GDC Overview
  - GDC Security
  - GDC Operator Guidelines: OC IT Setup
- GDC Practitioner Fundamentals course

Module 2 resources

- What is a Security Operations Center (SOC)? ↗
- Mandiant website ↗
- Locard's exchange principle ↗
- How cyber attacks work ↗
- What is zero-trust security? ↗

Module 3 resources

- Why the “Autonomous Security Operations Center” Is a Pipe Dream ↗
- SIEM: Security Information & Event Management Explained ↗
- What Is Endpoint Detection and Response? ↗
- What is SOAR? ↗
- NetFlow Basics: An Introduction to Monitoring Network Traffic ↗
- What is the SOC (Security Operations Center) Visibility Triad? ↗
- Incident Response Management: Key Elements and Best Practices ↗
- Incident Response: A Brief Introduction ↗
- Root Cause Analysis: A Beginner’s Guide ↗
- Incident management for high-velocity teams: Understanding incident severity levels ↗
- The Top 3 Cybersecurity Incidents Caused by Unintentional Insider Risk ↗
- Gamifying tabletop exercises: 5 steps for effective TTXs ↗
- Shifting from Reactive to Proactive Security Operations ↗
- Asset inventory is foundational to security programs ↗
- A curated list of awesome Threat Intelligence resources ↗
- What Is Vulnerability Scanning? Types, Tools and Best Practices ↗
- The 3 Types of Security Controls (Expert Explains) ↗

Module 4 resources

- How to implement and use the MITRE ATT&CK framework ↗
- Implementing the OODA Loop in Cyber Warfare ↗
- What is a DMZ network and why would you use it? ↗
- Anthos clusters on VMWare ↗
- Kubernetes Operator pattern ↗
- Grafana Documentation ↗
- Prometheus Documentation ↗
- Cortex Scalable AlertManager ↗
- FluentBit: Official Manual | Hands On! 101 ↗

- Loki: label best practices ↗
- ServiceNow Learning: Security Operations (SecOps) Security Incident Response (SIR) Implementer ↗
- The ultimate guide to GitOps with GitLab ↗
- Kubernetes GitOps best practices with Config Sync ↗
- Harbor Documentation: Working with Images, Tags, and Helm Charts ↗
- RHEL: Command-Line Interface Reference ↗
- Splunk: Training ↗
- How To: Run Your First Vulnerability Scan with Nessus ↗
- Getting started with Burp Suite ↗
- Trellix HX: Endpoint Security Server User Guide ↗
- Palo Alto Next-Generation Firewall Docs: Threat Prevention ↗
- STIG: Palo Alto Networks IDPS Security Technical Implementation Guide ↗
- Basic Searching in Splunk Enterprise ↗
- Creating Dashboards in Splunk Enterprise ↗
- Setup Detectors and Alerts for Actionable Insights ↗
- How to build a Prometheus query in Grafana ↗
- Effective troubleshooting with Grafana Loki - query basics ↗
- Grafana 10.1: How to build dashboards with visualizations and widgets ↗
- How to create an alert in Grafana ↗
- Viewing a ticket using ServiceNow ↗

Module 5 resources

- Splunk Documentation: Query logs in Log Observer ↗
- Splunk Documentation: Overview of metrics ↗
- Dashboards in Splunk Observability Cloud ↗