SIEM & SOAR on Google Cloud Course

Course Duration: 24 Hours **Course code: SSGC**

1. Course Overview

This three-day course focuses on implementing Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solutions on Google Cloud. It provides hands-on experience with tools such as Google Security Command Center and Chronicle SIEM. Learners will gain the skills to detect, analyze, and respond to security threats using automated workflows, real-time monitoring, and advanced threat intelligence in cloud environments.

2. What you'll learn?

By the end of the course, you will be able to:

- Understand SIEM and SOAR concepts and architecture
- Implement SIEM solutions using Google Chronicle
- Collect, normalize, and analyze security logs
- Detect threats using correlation rules and analytics
- Automate incident response using SOAR workflows
- Integrate multiple security tools and data sources
- Monitor, investigate, and respond to security incidents
- Improve security posture using automation and intelligence

3. Target Audience

- Security analysts and SOC engineers
- Cybersecurity professionals
- Cloud security engineers
- Incident response and threat intelligence teams

4. Pre-Requisites

Before taking this course, you should have:

- Basic understanding of cybersecurity concepts
- Familiarity with networking fundamentals
- Knowledge of cloud computing (preferably GCP)
- Basic understanding of logs and monitoring systems

5. Course content

Module 1: Course Introduction

- Introduction and course logistics
- Overview of SIEM & SOAR in cloud security
- Course objectives and lab setup

Module 2: SIEM and SOAR Fundamentals

- What is SIEM?
- What is SOAR?
- Key components and architecture
- Benefits in modern SOC environments

Module 3: Google Cloud Security Ecosystem

- Overview of GCP security services
- Introduction to Chronicle SIEM
- Security Command Center overview
- Integration with GCP services

Module 4: Log Collection and Ingestion

- Sources of security logs
- Configuring log ingestion in GCP
- Normalization and parsing of logs
- Managing large-scale log data

Module 5: Threat Detection and Correlation

- Creating detection rules
- Event correlation techniques
- Behavioral analysis
- Identifying anomalies and threats

Module 6: Chronicle SIEM Deep Dive

- Chronicle architecture and capabilities
- Searching and analyzing logs
- Threat intelligence integration
- Investigating security incidents

Module 7: Security Command Center (SCC)

- SCC features and components
- Asset inventory and risk analysis
- Security findings and alerts
- Managing vulnerabilities

Module 8: Incident Response and Case Management

- Incident response lifecycle
- Creating and managing cases
- Investigating alerts and incidents
- Documentation and reporting

Module 9: SOAR Fundamentals and Automation

- Introduction to SOAR workflows
- Automation use cases
- Playbooks and runbooks
- Orchestration strategies

Module 10: Building SOAR Playbooks

- Designing automated workflows
- Integrating APIs and tools
- Automating incident response actions
- Testing and validating playbooks

Module 11: Integration with Security Tools

- Integrating third-party tools (firewalls, IDS/IPS)
- API-based integrations
- Data exchange between systems
- Unified security operations

Module 12: Monitoring and Optimization

- Monitoring SIEM/SOAR performance
- Tuning detection rules
- Reducing false positives
- Optimizing workflows

Module 13: Compliance and Reporting

- Security compliance frameworks
- Generating audit reports
- Data retention policies
- Governance best practices

Module 14: Advanced Threat Detection and Intelligence

- Threat intelligence feeds
- Advanced analytics and ML-based detection
- Hunting threats proactively
- Emerging threats and trends

Module 15: Capstone Project and Real-World Scenarios

- Implementing a SIEM & SOAR solution
- Detecting and responding to simulated attacks
- Automating incident response workflows
- Final project and assessment

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com