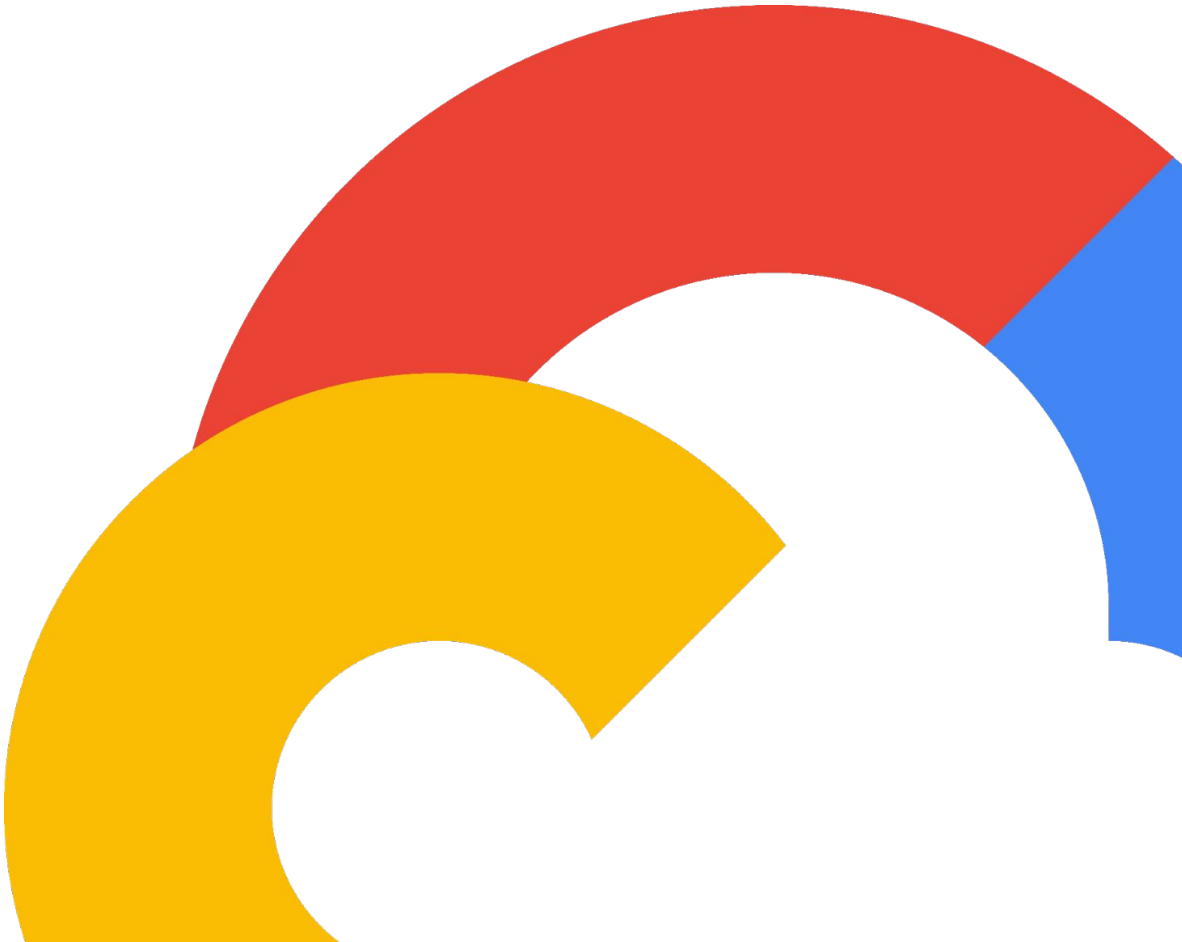
Google Cloud

Google Cloud Cybersecurity Certificate

2025



Google Cloud

Why Cloud Cybersecurity

As cloud computing has become a cornerstone of the IT industry, cybersecurity threats to the cloud continue to rise. Cloud security analysts are uniquely positioned as the first line of defense in protecting organizational cloud assets from a wide array of cyber-related crimes. To aid in the fight against these costly and invasive attacks on digital data and cloud infrastructure, cloud security analysts frequently focus their attention on identifying threats, risks, and vulnerabilities. Then, they respond to and defend against a variety of security incidents that can harm organizations.

Google Cloud Cybersecurity Certificate

This certificate program prepares learners for entry-level roles in cloud cybersecurity. A college degree is not a prerequisite, but learners should have familiarity with foundational cybersecurity concepts, skills, and tools. These can include the basics of network security, threat analysis, Security Information and Event Management (SIEM) technologies, Linux and SQL, and incident detection and documentation. Supplemental content on these concepts is included within the certificate for learners who do not have this prior knowledge.

There are five courses in the Google Cloud Cybersecurity Certificate. In each course, learners will complete hands-on labs that allow them to practice key skills and produce work examples to show potential employers. The first four courses progressively build learners' working knowledge of networks, security models, and tools used to assess and address threats, risks, and vulnerabilities. The final course includes a capstone project that focuses on applying learning principles from courses 1 -4 and prepares learners to establish a career in the cloud security field.

5 courses

19 modules

212 videos

12 labs

154 readings

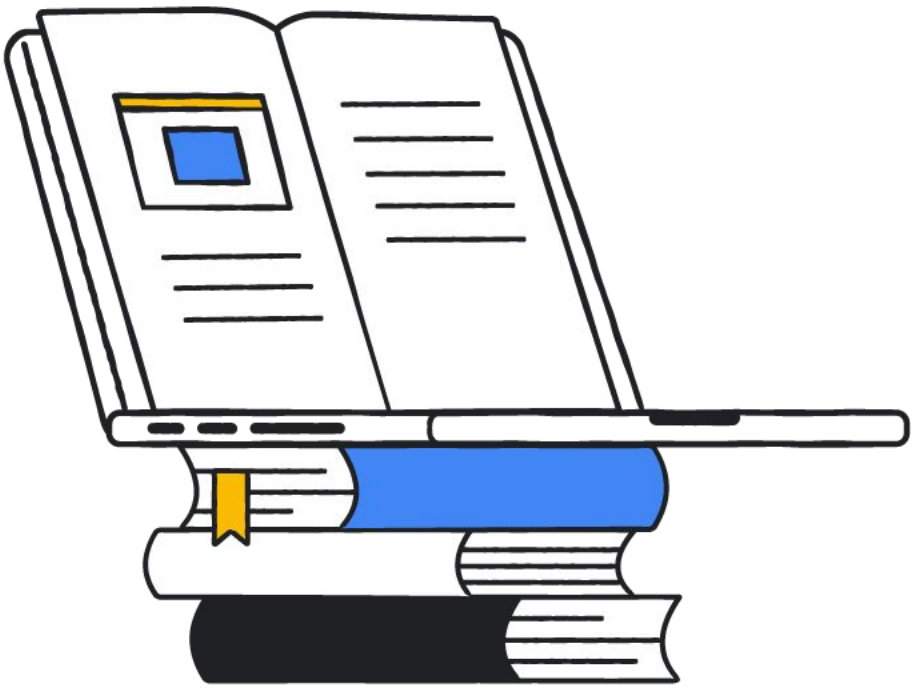
94 quizzes

1 capstone

~ 90 hours to complete

Google Cloud

Courses



Course 1

Introduction to Security Principles in Cloud Computing

Course Overview

This course introduces cloud security principles and outlines the goals of the Cloud Certificate program. It defines the field of cloud security, and describes primary roles and responsibilities for cloud computing. Learners will explore cloud fundamentals from digital transformation, to the security lifecycle, to an overview of cloud computing and key concepts, and then investigate Google Cloud tools, such as Google Cloud Console and Cloud Shell. Learners begin to prepare for the job application and interview process by updating resumes and practicing interview techniques.

By the end of this course, learners will:

- Explain how this certificate program will help prepare learners for a career in cloud security.
- Define Cybersecurity as it applies to cloud computing.
- Describe the common roles and responsibilities of an entry-level cloud security analyst.
- Identify common tools used by entry-level cloud security analysts.
- Explain the security lifecycle and key concepts in cloud security computing.
- Describe the fundamentals of digital transformation within the cloud.

Course Outline

Module 1: Introduction to cloud computing
Module 2: Security in the cloud
Module 3: The security lifecycle
Module 4: Cloud security analyst roles and responsibilities

~ 15 hours to complete

Course 2

Strategies for Cloud Security Risk Management

Course Overview

This course provides an introduction to the most widely used cloud risk management frameworks. It explores various security domains, encompasses the compliance lifecycle, and dives into some regulations and industry standards (e.g., HIPAA, NIST CSF, SOC) that cloud security analysts follow on the job. Learners will gain an understanding of how to identify risks, implement security controls to mitigate risks, evaluate compliance while managing data protection and privacy, and compare and adopt frameworks. Additionally, this course introduces learners to specific Google Cloud and multi-cloud tools used for risk and compliance management. Learners continue to apply job application and interview preparation techniques.

By the end of this course, learners will:

- Explain and analyze the risk management process and its main components and objects.
- Explain the process and frameworks of cloud security risk management.
- Define security controls and describe the control-to-risk mapping process.
- Explore the stages of the compliance lifecycle and discuss the roles of control mapping, auditing, regulatory compliance, and organizational impacts of non-compliance.
- Analyze how Google Cloud's Security Command Center (SCC) and Risk Manager monitor compliance and help you manage risk.
- Identify risk management regulations and industry standards.
- Compare and contrast the regulations and industry standards.
- Describe the rationale for compliance - how people, process, and technology play a part.
- Implement tools for compliance risk mitigation.

Course Outline

Module 1: Introduction to frameworks within security domains

Module 2: Risk management frameworks, regulations, and standards

Module 3: The compliance lifecycle

Module 4: Cloud tools for risk management and compliance

~ 20 hours to complete

Course 3

Cloud Security Risks: Identify and Protect Against Threats

Course Overview

This course covers identity management and access control principles in a cloud environment, including AAA elements, credential handling, and certificate management. Learners will also explore threat and vulnerability management, cloud native principles, and data protection measures. Upon completion, learners will possess the skills and knowledge to secure cloud-based resources and protect sensitive organizational information. Learners continue to apply job application and interview preparation techniques.

By the end of this course, learners will:

- Describe identity and access management concepts in the cloud.
- Identify elements of AAA (authentication, authorization, and auditing) for enhanced cloud security.
- Discuss the importance of credential handling and certificate management in cloud security.
- Explain capabilities and best practices that streamline asset and resource management.
- Identify common security vulnerabilities and assess their impact and risk.
- Define key implementations of cloud-native concepts, including containers, serverless functions, and orchestrators.
- Analyze effective practices for securing containers and Kubernetes.
- Describe the role of data protection and privacy in organizational security.
- Evaluate the significance of automation in cloud infrastructure.
- Identify emerging trends and technologies and their impact on threat and vulnerability management.

Course Outline

Module 1: Access control and identity management
Module 2: Threat and vulnerability management
Module 3: Cloud Native Principles of Ephemerality and Immutability
Module 4: Data Protection and Privacy

~ 22 hours to complete

Course 4

Detect, Respond, and Recover from Cloud Cybersecurity Attacks

Course Overview

This course emphasizes capabilities, logging, security and alert monitoring, and techniques for mitigating attacks. Additionally, learners gain knowledge in customizing threat feeds, incident management, crisis communications, root cause analysis, incident response, and post-event communications. Using Google Cloud tools, learners identify indicators of compromise and prepare for business continuity and disaster recovery. Learners continue to apply job application and interview preparation techniques.

By the end of this course, learners will:

- Identify logging systems in a cloud environment and how to aggregate, correlate, and identify security alerts.
- Compose custom queries using pattern matching techniques and system specific syntax against aggregated logs, limiting the scope to security related information.
- Explain how security monitoring systems are implemented and configured in a cloud computing environment.
- Configure security monitoring systems to identify and mitigate threats to a cloud environment.
- Define incident response and how this applies to a cloud computing environment.
- Define the lifecycle of a security incident and the process to identify, document, and prevent future incidents.
- Reference attack mitigation techniques using custom defined rules, security applications, and analysis of emerging threats.
- Explain the purpose of a Disaster Recovery Plan and how this affects data retention and recovery.

Course Outline

Module 1: Detection foundations
Module 2: Detection in practice
Module 3: Incident response management and attack mitigation
Module 4: Incident recovery

~ 22 hours to complete

Course 5

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

Course Overview

The final course combines and applies the material from courses 1-4 in an interactive capstone project. Concepts learners will apply in the project include cloud security principles, risk management, identifying vulnerabilities, incident management, and crisis communications. Learners will gain practice in detecting, responding to, and recovering from security threats and incidents, and security monitoring techniques. Learners will finalize their resume updates and apply all their new interview techniques in preparation for applying and interviewing for jobs.

By the end of this course, learners will:

- Explain IAM and the scope of permissions and roles, and the roles and responsibilities of a security organization.
- Identify the regulatory requirements and standards that apply to different industries.
- Interpret and identify risks and vulnerabilities.
- Develop a plan to protect an organization by detecting, responding and recovering from security threats and incidents.
- Develop career resources for a role in cloud security computing.
- Practice resume and interview techniques for a cloud security career.

Course Outline

Module 1: Cloud security-focused career resources

Module 2: The capstone project

Module 3: Congratulations on completing the Google Cloud Cybersecurity Certificate

~ 11 hours to complete

Google Cloud