Course 3 overview
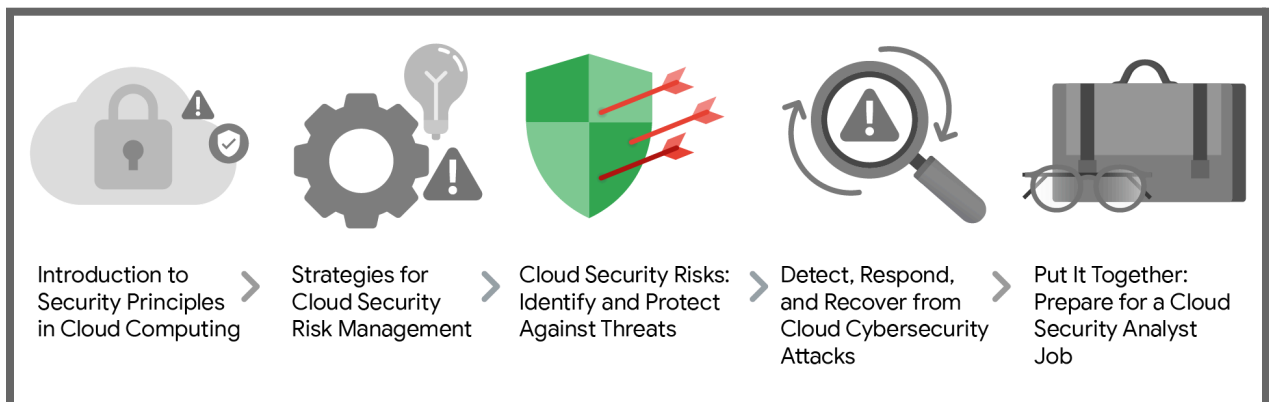

Hello and welcome to **Cloud Security Risks: Identify and Protect Against Threats**, the third course in the Google Cloud Cybersecurity Certificate!

In this course, you'll explore methods cloud security analysts use to protect the confidentiality, integrity, and availability of cloud data. Then, you'll learn the principles of identity management and access control in the cloud, including how authentication, authorization, and auditing (AAA), credential handling, and certificate management help to protect information stored in the cloud. You'll also explore the cloud-native concepts of ephemerality and immutability, and learn how cloud security analysts use policy automation to securely configure cloud resources.

Certificate program progress

The Google Cloud Cybersecurity Certificate program has four courses. **Cloud Security Risks: Identify and Protect Against Threats** is the third course.

| Introduction to Security Principles in Cloud Computing | Strategies for Cloud Security Risk Management | Cloud Security Risks: Identify and Protect Against Threats | Detect, Respond, and Recover from Cloud Cybersecurity Attacks | Put It Together: Prepare for a Cloud Security Analyst Job |

1. Introduction to Security Principles in Cloud Computing — In this course, you'll explore the fundamentals of cloud computing, learn how security principles apply to cloud products and services, and investigate Google Cloud tools.

2. Strategies for Cloud Security Risk Management — In this course, you'll learn about risk management frameworks used to secure cloud resources. You'll also be introduced to tools, regulations, and industry standards that cloud security analysts follow on the job.

3. **Cloud Security Risks: Identify and Protect Against Threats** (current course) — In this course, you'll gain experience with tools and techniques used to protect cloud resources from threats. You'll also explore threat and vulnerability management, cloud native principles, and data protection.

4. Detect, Respond, and Recover from Cloud Cybersecurity Attacks — In this course, you'll learn how cloud security professionals use logging and monitoring systems to identify and mitigate attacks. You'll also explore techniques used to detect, respond to, and recover from a security incident.

5. Put It Together: Prepare for a Cloud Security Analyst Job — In this course, you'll add your new skills to your resume and explore job search tips. Then, you'll apply concepts like risk management, identifying vulnerabilities, incident management, and crisis communications in a capstone project.

Course 3 content

Each course in this certificate program is broken into modules. You can complete courses at your own pace, but the weekly breakdowns are designed to help you finish the entire Google Cloud Cybersecurity Certificate in about 3-6 months if you complete one-two modules per week.

What's to come? Here's a quick overview of the skills you'll learn in each module of this course.

Module 1: Access control and identity management

In this module, you'll discover how identity management principles align with the security concepts of least-privilege and separation-of-duties. Then, you'll learn the key elements of authentication, authorization, and auditing (AAA), and explore implementing access control methods within cloud deployments. You'll also explore how perimeter protection concepts apply to cloud environments, and identify common attack vectors that impact boundary protection.

Module 2: Threat and vulnerability management

In this module, you'll learn to identify threats and vulnerabilities in cloud resources, and how to remediate vulnerabilities using patching or rehydration. You'll also explore cloud asset management tools and best practices. Next, you'll learn to improve security posture using secure configuration best practices.

Module 3: Cloud-native principles and automation

In this module, you'll learn the cloud-native principles of ephemerality and immutability and explore what they mean to cloud security. You'll also explore infrastructure as code (IaC), a form of policy automation cloud security analysts use to efficiently secure cloud resources, and gain experience with the tools used to design IaC. Then, you'll learn the importance of containers, orchestrators, and serverless functions, and explore how cloud security analysts secure these resources.

Module 4: Data protection and privacy

In this module, you'll learn to secure sensitive data stored and used in the cloud. You'll also learn encryption concepts and gain experience with the encryption techniques cloud security analysts use to protect data. Then, you'll explore the concepts of data sovereignty, data governance, and applying compliance controls to different data retention levels. Finally, you'll explore cloud security's role in business continuity planning.

What to expect

Each course offers many types of learning opportunities:

- **Videos** led by Google instructors teach new concepts, introduce the use of relevant tools, offer career support, and provide inspirational personal stories.
- **Readings** build on the topics discussed in the videos, introduce related concepts, share useful resources, and describe case studies.
- **Activities** and **labs** give you hands-on practice in applying the skills you're learning, and allow you to assess your own work by comparing it to a completed example.
- **Glossaries** provide a list of key terms for you to review to prepare for quizzes.
- **Practice quizzes** allow you to check your understanding of key concepts, and provide you with valuable feedback.
- **Graded quizzes** allow you to demonstrate your understanding of the main concepts of a course. You must score 80% or higher on each graded quiz to obtain a certificate. You can take a graded quiz multiple times to achieve a passing score.

Note: Some learning item types may not be included in every course.

Tips for success

- It's strongly recommended that you go through the items in each lesson in the order they appear because new information and concepts build on previous knowledge.
- Participate in all learning opportunities to gain as much knowledge and experience as possible.
- If something is confusing, don't hesitate to replay a video, review a reading, or repeat an activity.
- When you encounter useful links in this course, bookmark them so you can refer to the information later for study or review.