Google Cloud

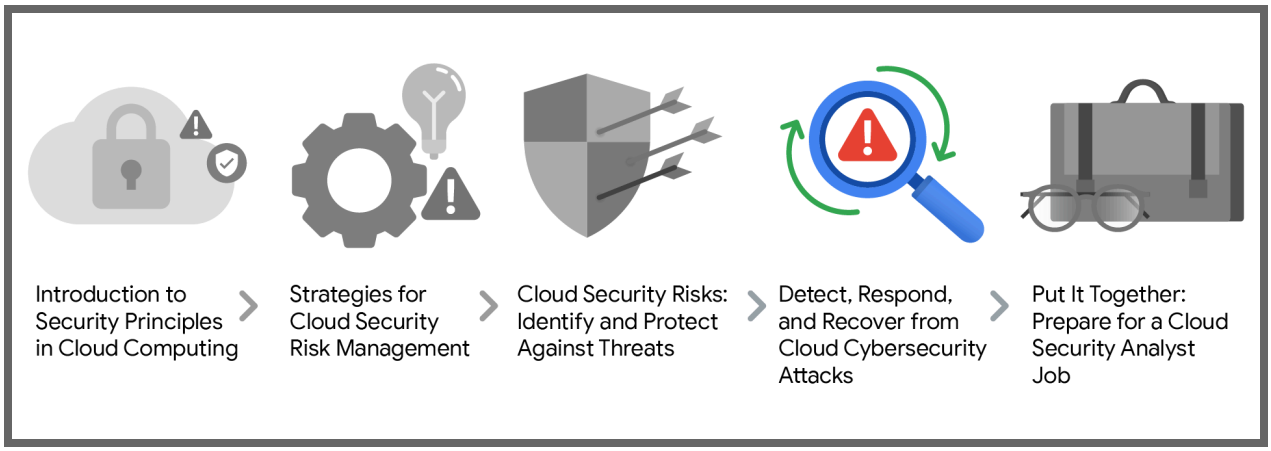
Course 4 overview

Hello and welcome to **Detect, Respond, and Recover from Cloud Cybersecurity Attacks**, the fourth course in the Google Cloud Cybersecurity Certificate. You're on an exciting journey!

In this course, you'll develop a well-rounded understanding of logging and monitoring fundamentals for incident detection, including documentation, evidence preservation, and automation for incident response. You'll also learn more about business continuity and disaster recovery for incident recovery.

Certificate program progress

The Google Cloud Cybersecurity Certificate program has five courses. **Detect, Respond, and Recover from Cloud Cybersecurity Attacks** is the fourth course.



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 — 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** (current course) — 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 All 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 4 content

Each course in this certificate program is broken into modules. You can complete courses at your own pace, but the module breakdowns are designed to help you finish the entire Google Cloud Cybersecurity Certificate in about 3-6 months if you complete about 1-2 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: Detection foundations

In this module, you'll explore essential topics for detecting activity like log retention policies, intrusion detection and prevention systems, monitoring and alerting systems, incident management, and attack mitigation.

Module 2: Detection in practice

In this module, you'll learn about Lockheed Martin's Cyber Kill Chain®, false positive analysis, and threat hunting techniques. You'll also learn how to create detection rules, use query tools, analyze logs, and identify indicators of compromise.

Module 3: Incident response management and attack mitigation

In this module, you'll explore the incident response process, including essential skills in documenting information for stakeholders, conducting post-mortem analysis, and developing and executing automated playbooks.

Module 4: Incident recovery

In this module, you'll learn about the critical aspects of business continuity and disaster recovery (BCDR). You'll also practice using BCDR tools and recovery metrics to restore compromised virtual machines to a specified point in time and maintain normal business operations.

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 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.