Course 6 overview

Hello, and welcome to **Sound the Alarm: Detection and Response**, the sixth course in the Google Cybersecurity Certificate. You're on an exciting journey!

By the end of the course, you will have hands-on practice using resources like network protocol analyzers, intrusion detection systems (IDS), and security information event management (SIEM) tools to capture network packets and analyze log data.

Certificate program progress

The Google Cybersecurity Certificate program has eight courses. **Sound the Alarm: Detection and Response** is the sixth course.

1. **Foundations of Cybersecurity** — Explore the cybersecurity profession, including significant events that led to the development of the cybersecurity field and its continued importance to organizational operations. Learn about entry-level cybersecurity roles and responsibilities.
2. **Play It Safe: Manage Security Risks** — Identify how cybersecurity professionals use frameworks and controls to protect business operations, and explore common cybersecurity tools.
3. **Connect and Protect: Networks and Network Security** — Gain an understanding of network-level vulnerabilities and how to secure networks.
4. **Tools of the Trade: Linux and SQL** — Explore foundational computing skills, including communicating with the Linux operating system through the command line and querying databases with SQL.
5. **Assets, Threats, and Vulnerabilities** — Learn about the importance of security controls and developing a threat actor mindset to protect and defend an organization's assets from various threats, risks, and vulnerabilities.
6. **Sound the Alarm: Detection and Response** — *(current course)* Understand the incident response lifecycle and practice using tools to detect and respond to cybersecurity incidents.
7. **Automate Cybersecurity Tasks with Python** — Explore the Python programming language and write code to automate cybersecurity tasks.
8. **Put It to Work: Prepare for Cybersecurity Jobs** — Learn about incident classification, escalation, and ways to communicate with stakeholders. This course closes out the program with tips on how to engage with the cybersecurity community and prepare for your job search.

Course 6 content

Each course of this certificate program is broken into weeks. You can complete courses at your own pace, but the weekly breakdowns are designed to help you finish the entire Google Cybersecurity Certificate in about six months.

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

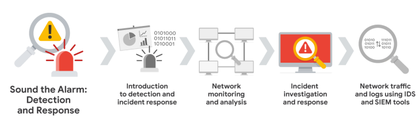
Week 1: Introduction to detection and incident response

You will be introduced to detection and incident response, and the steps involved in the incident response process. You'll also explore how cybersecurity professionals verify and respond to malicious threats.

Week 2: Network monitoring and analysis

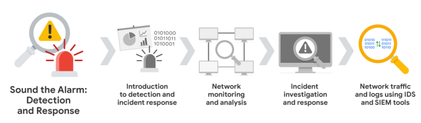
You will learn the importance of network monitoring, and how to understand network traffic. Then, you'll explore how to use network protocol analyzer tools, commonly referred to as packet sniffers. In particular, you'll sniff the network and analyze packets for malicious threats. You'll also craft filtering commands to analyze the contents of captured packets.

Week 3: Incident investigation and response



You will learn about the various processes and procedures in the stages of incident detection, investigation, analysis, and response. Then, you'll analyze the details of suspicious file hashes using investigative tools. You'll also learn about the importance of documentation, evidence collection, the triage process, and more.

Week 4: Network traffic and logs using IDS and SIEM tools



You will explore logs and their role in IDS and SIEM tools. You'll learn how these systems work to help cybersecurity teams monitor systems and detect malicious activity. You'll also be introduced to some IDS and SIEM products, and practice using tools to perform queries.

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.
- **Discussion prompts** explore course topics for better understanding and allow you to chat and exchange ideas with other learners in the discussion forums.
- **Self-review activities** and **labs** give you hands-on practice in applying the skills you are learning and allow you to assess your own work by comparing it to a completed example.
- **Interactive plug-ins** encourage you to practice specific tasks and help you integrate knowledge you have gained in the course.
- **In-video quizzes** help you check your comprehension as you progress through each video.
- **Practice quizzes** allow you to check your understanding of key concepts and provide valuable feedback.
- **Graded quizzes** demonstrate your understanding of the main concepts of a course. You must score 80% or higher on each graded quiz to obtain a certificate, and you can take a graded quiz multiple times to achieve a passing score.

Tips for success

- It is 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 a self-review activity.
- Use the additional resources that are referenced in this course. They are designed to support your learning. You can find all of these resources in the Resources tab.
- When you encounter useful links in this course, bookmark them so you can refer to the information later for study or review.
- Understand and follow the Coursera Code of Conduct to ensure that the learning community remains a welcoming, friendly, and supportive place for all members.

Mark as completed