Google Cybersecurity Certificate

The Google Cybersecurity Certificate is a skills-based, online program designed to prepare learners for entry-level jobs in cybersecurity upon completion of the certificate. Google developed this program, and it covers fundamentals of the cybersecurity field, including roles and responsibilities of cybersecurity analysts; the Certified Information Systems Security Professional (CISSP) security domains; frameworks and controls; security hardening; Linux® command line and SQL; asset protection; log analysis; Python™ for automating security-related tasks, and more. Learners in the Google Cybersecurity Certificate will:

- Define the field of security and recognize core skills and knowledge needed to become a security analyst.
- Explain the focus of CISSP's eight security domains and define the primary threats, risks, and vulnerabilities to business operations.
- Recognize network-level vulnerabilities, explain network architecture, and describe how to secure a network.
- Describe the main functions of an operating system, and understand foundational computing skills related to the use of Linux and SQL.
- Learn how to classify and protect assets, manage cybersecurity risk, and identify threats, risks, and vulnerabilities.
- Explore the processes and procedures used in incident detection and response, and analyze artifacts with various cybersecurity tools.
- Use the Python programming language to complete security-related tasks.
- Determine ways to engage with the cybersecurity community, and describe how to find, apply for, and prepare for a job as a security analyst.

Equipment Needed: All learners must have a computer with reliable internet to access course content. Reliable internet access is necessary to complete hands-on course activities. Headphones are also a good option for a noisy environment.

SEMESTER PLAN:

Below includes a detailed guide for you to follow as you complete the course work. The goal is to keep you on track to finish your certificate within the allotted timeframe.

Expectations and Best Practices

Online learning allows for the flexibility of working at your own pace to meet a deadline, but it's helpful to establish a routine to stay on target and remember when work is due! Here's one that has worked well for students previously:

- **Monday/Tuesday**: Review all new material for the week and watch all assigned videos by end of day on Tuesday.

- **Rest of the week:** Complete work at your own pace. Aim to complete at least one task each day, no matter how large or small. With work, you may complete core coursework on Saturdays and

Sundays. ***Reminder:*** To ensure you are actively participating, discussion posts may require you to post multiple times throughout the week.

- **Sunday:** Typically, weekly assignments are due at the end of the day on Sunday. Review that you have completed each assignment for that week.

Now that you have reviewed the coursework guidelines, please take a moment to review a general breakdown of each course, including estimates of how much time each may take based on the quantity and difficulty of the content. As you work though this plan, reach out to you professor with questions, concerns, and if you need clarifications.

COURSE 1: Foundations of Cybersecurity

In this course, learners will be introduced to the cybersecurity profession, including the primary job responsibilities and core skills of entry-level analysts; significant events that led to the development of the cybersecurity field; and security's continued importance to organizational operations. Learners will also explore the Certified Information Systems Security Professional (CISSP) eight security domains, common security frameworks and controls, as well as the confidentiality, integrity, and availability (CIA) triad. This course covers a wide variety of cybersecurity topics to provide an overview of what's to come in this certificate program.

Week 1

MODULE 1: Welcome to the exciting world of cybersecurity!

Begin the journey into cybersecurity! Learners will explore the cybersecurity field, and learn about the job responsibilities of cybersecurity professionals.

Module items

- 9 videos
- 8 readings
- 1 interactive plug-in
- 2 discussion prompts
- 2 practice quizzes
- 1 graded quiz

MODULE 2: The evolution of cybersecurity

Learners will explore how cybersecurity threats have appeared and evolved alongside the adoption of computers. They will also understand how past and present cyber-attacks have influenced the development of the security field. In addition, learners will get an overview of the CISSP eight security domains.

Module items

- 7 videos
- 4 readings
- 1 interactive plug-in
- 2 practice quizzes
- 1 graded quiz

MODULE 3: Protect against threats, risks, and vulnerabilities

Learners will be introduced to security frameworks and controls, which are used to mitigate organizational risk. They will also explore principles of the CIA triad and specific NIST frameworks. In addition, learners will explore security ethics.

Module items

- 7 videos
- 3 readings
- 1 interactive plug-in
- 1 discussion prompt
- 2 practice quizzes
- 1 graded quiz

MODULE 4: Cybersecurity tools and programming languages

Learners will discover common tools used by cybersecurity analysts to identify and mitigate risk. They will learn about security information and event management (SIEM) tools, network protocol analyzers, and the value of programming languages for completing cybersecurity-related tasks.

Module items

- 5 videos
- 6 readings
- 1 interactive plug-in
- 1 self-review activity
- 1 discussion prompt
- 2 practice quizzes
- 1 graded quiz

COURSE 2: Play it Safe: Manage Security Risks

This course offers a closer examination of concepts introduced in the first course, with an emphasis on recognizing the focus of the Certified Information Systems Security Professional (CISSP) eight security domains, steps of risk management, specific security frameworks and controls, as well as common security threats, risks, and vulnerabilities. Learners are also provided with an opportunity to explore common cybersecurity tools such as security Information and event management (SIEM) tools and playbooks to respond to identified threats, risks, and vulnerabilities.

WEEK 2

MODULE 1: Security domains (3 hours, 28 minutes total module time)

Learners will gain a greater understanding of the CISSP eight security domains. Then, they'll learn about primary threats, risks, and vulnerabilities to business operations. In addition, learners will explore the NIST Risk Management Framework (RMF) and the steps of risk management.

Module items

- 10 videos
- 5 readings
- 1 interactive plug-in
- 1 discussion prompt
- 2 practice quizzes
- 1 graded quiz

MODULE 2: Security frameworks and controls (4 hours, 52 minutes total module time)

Learners will focus on specific security frameworks and controls, along with the core components of the confidentiality, integrity, and availability (CIA) triad. They will also learn about Open Web Application Security Project, recently renamed Open Worldwide Application Security Project® (OWASP), security principles and security audits.

Module items

- 11 videos
- 5 readings
- 1 interactive plug-in
- 2 self-review activities
- 4 practice quizzes
- 1 graded quiz

WEEK 3

MODULE 3: Introduction to cybersecurity tools (2 hours, 31 minutes total module time)

Learners will explore industry-leading SIEM tools that are used by security professionals to protect business operations. They will also learn how entry-level security analysts use SIEM dashboards as part of their everyday work.

Module items

- 7 videos

- 4 readings
- 2 practice quizzes
- 1 graded quiz

MODULE 4: Use playbooks to respond to incidents (3 hours, 16 minutes total module time)

Learners will gain an understanding of the purposes and common uses of playbooks. They'll also explore how cybersecurity professionals use playbooks to respond to identified threats, risks, and vulnerabilities.

Module items

- 7 videos
- 5 readings
- 2 interactive plug-ins
- 1 discussion prompt
- 2 practice quizzes
- 1 graded quiz

COURSE 3: Connect and Protect: Networks and Network Security

This course introduces network architecture, operations, intrusion tactics, common network vulnerabilities and attacks, and how to secure networks. Learners will also gain an understanding of common network protocols, firewalls, virtual private networks (VPNs), and system hardening practices.

Week 4

MODULE 1: Network architecture (4 hours, 20 minutes total module time)

Learners will be introduced to network security and explain how it relates to ongoing security threats and vulnerabilities. They will also learn about network architecture and mechanisms to secure a network.

Module items

- 13 videos
- 8 readings
- 2 interactive plug-ins
- 1 discussion prompt
- 3 practice quizzes
- 1 graded quiz

MODULE 2: Network operations (2 hours, 55 minutes total module time)

Learners will explore network protocols and how network communication can introduce vulnerabilities. In addition, learners will gain an understanding of common security measures, like firewalls, that help network operations remain safe and reliable.

Module items

- 8 videos
- 7 readings
- 2 practice quizzes
- 1 graded quiz

Week 5

MODULE 3: Secure against network intrusions (4 hours, 11 minutes total module time)

Learners will understand types of network attacks and techniques used to secure compromised network systems and devices. They will explore the many ways that malicious actors exploit vulnerabilities in network infrastructure and how cybersecurity professionals identify and close potential loopholes.

Module items

- 7 videos
- 5 readings
- 1 interactive plug-in
- 2 self-review activities
- 2 practice quizzes
- 1 graded quiz

MODULE 4: Security hardening (6 hours, 33 minutes total module time)

Learners will become familiar with network hardening practices that strengthen network systems. Additionally, learners will explain how security hardening helps defend against malicious actors and intrusion methods. They will also learn how to use security hardening to address the unique security challenges posed by cloud infrastructures.

Module items

- 8 videos
- 8 readings
- 1 lab
- 3 self-review activities
- 1 discussion prompt
- 3 practice quizzes
- 1 graded quiz

COURSE 4: Tools of the Trade: Linux and SQL

This course focuses on foundational computing skills that support the work of cybersecurity analysts. Learners will be introduced to operating systems and explore how to communicate with the Linux operating system via commands entered through the Bash shell. They will also practice using Structured Query Language (SQL) to query databases and filter results.

Week 6

MODULE 1: Introduction to operating systems (4 hours, 5 minutes total module time)

Learners will examine the relationship between operating systems, hardware, and software, and become familiar with the primary functions of an operating system. They will also recognize common operating systems in use today and understand how the graphical user interface (GUI) and command-line interface (CLI) both allow users to interact with the operating system.

Module items

- 9 videos
- 7 readings
- 1 interactive plug-in
- 1 self-review activity
- 2 discussion prompts
- 3 practice quizzes
- 1 graded quiz

MODULE 2: The Linux operating system (5 hours, 1 minute total module time)

Learners will be introduced to the Linux operating system and explore how it is commonly used in cybersecurity. They will also learn about Linux architecture and common Linux distributions. In addition, learners will be introduced to the Linux shell and understand how it allows users to communicate with the operating system.

Module items

- 9 videos
- 6 readings
- 1 interactive plug-in
- 2 labs
- 1 discussion prompt
- 3 practice quizzes
- 1 graded quiz

Week 7

MODULE 3: Linux commands in the Bash shell (10 hours, 54 minutes total module time)

Learners will be introduced to Linux commands as entered through the Bash shell. They will then use the Bash shell to navigate and manage the file system and to authorize and authenticate users. Learners will also understand where to go for help when working with new Linux commands.

Module items

- 12 videos
- 8 readings

- 1 interactive plug-in
- 6 labs
- 1 self-review activity
- 1 discussion prompt
- 4 practice quizzes
- 1 graded quiz

Week 8

MODULE 4: Databases and SQL (10 hours, 55 minutes total module time)

Learners will practice using SQL to communicate with databases. They will also learn how to query a database and filter the results. Additionally, learners will understand how SQL can join multiple tables together in a query.

Module items

- 12 videos
- 12 readings
- 1 interactive plug-in
- 5 labs
- 1 self-review activity
- 2 discussion prompts
- 4 practice quizzes
- 1 graded quiz

COURSE 5: Assets, Threats, and Vulnerabilities

Learners will further explore the importance of protecting organizational assets from threats, risks, and vulnerabilities. They will also continue to develop an understanding of asset classification and how to use the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF), as well as security controls, to protect assets and mitigate risk. Additionally, learners will gain an understanding of how to develop a threat actor mindset to help protect assets from ever-evolving threat actor tactics and techniques.

Week 9

MODULE 1: Introduction to asset security (5 hours, 20 minutes total module time)

Learners will be introduced to how organizations determine what assets to protect. They'll learn about the connection between managing risk and classifying assets by exploring the unique challenge of securing physical and digital assets. Learners will also continue to explore the NIST CSF, as well as other guidelines and best practices to manage cybersecurity risk.

Module items

- 10 videos

- 7 readings
- 1 interactive plug-in
- 2 self-review activities
- 2 discussion prompts
- 3 practice quiz/quizzes
- 1 graded quiz

MODULE 2: Protect organizational assets (7 hours, 39 minutes total module time)

Learners will focus on security controls that protect organizational assets. They'll explore how privacy impacts asset security and understand the role that encryption plays in maintaining the privacy of digital assets. Learners will also explore how authentication and authorization systems help verify a user's identity.

Module items

- 11 videos
- 9 readings
- 2 labs
- 2 self-review activities
- 3 practice quizzes
- 1 graded quiz

Week 10

MODULE 3: Vulnerabilities in systems (7 hours, 31 minutes total module time)

Learners will build an understanding of the vulnerability management process. They will also learn about common vulnerabilities and develop an attacker mindset by examining the ways vulnerabilities can become threats to asset security if they are exploited.

Module items

- 10 videos
- 9 readings
- 2 self-review activities
- 3 practice quizzes
- 1 graded quiz

MODULE 4: Threats to asset security (6 hours, 50 minutes total module time)

Learners will explore common types of threats to digital asset security. They will also examine the tools and techniques used by cybercriminals to target assets. In addition, learners will be introduced to the threat modeling process and examine the ways that security professionals stay ahead of security breaches.

Module items

- 12 videos
- 8 readings
- 2 interactive plug-ins
- 2 self-review activities
- 2 discussion prompts
- 4 practice quizzes
- 1 graded quiz

COURSE 6: Sound the Alarm Detection and Response

Learners will focus on incident detection and response by understanding the incident response lifecycle and the roles and responsibilities of incident response teams. Learners will also practice using resources like network protocol analyzers (packet sniffers), intrusion detection systems (IDS), and security information event management (SIEM) tools to capture network packets and analyze log data. Additionally, learners will have an opportunity to explore incident investigation and response processes and procedures by assessing and analyzing artifacts.

Week 11

MODULE 1: Introduction to detection and incident response (4 hours, 29 minutes total module time)

Detection and incident response are an important part of a cybersecurity analyst's work. Learners will explore how cybersecurity professionals verify and respond to malicious threats and become familiar with the steps involved in incident response.

Module items

- 12 videos
- 6 readings
- 1 interactive plug-in
- 1 self-review activity
- 1 discussion prompt
- 4 practice quizzes
- 1 graded quiz

MODULE 2: Network monitoring and analysis (5 hours, 36 minutes total module time)

Learners will explore network analysis tools, commonly referred to as packet sniffers. In particular, they will sniff the network and analyze packets for malicious threats. Learners will also craft filtering commands to analyze the contents of captured packets.

Module items

- 9 videos
- 6 readings
- 2 labs
- 1 self-review activity
- 3 practice quizzes
- 1 graded quiz

Week 12

MODULE 3: Incident investigation and response (6 hours, 12 minutes total module time)

Learners will focus on the various processes and procedures in the stages of incident detection, investigation, analysis, and response. Then, they'll analyze the details of suspicious file hashes. They will also learn about the importance of documentation and evidence collection during the detection and response stages. Finally, learners will approximate an incident's chronology by mapping artifacts to reconstruct an incident's timeline.

Module items

- 11 videos
- 8 readings
- 2 interactive plug-ins
- 3 self-review activities
- 1 discussion prompt
- 3 practice quiz/quizzes
- 1 graded quiz

MODULE 4: Network traffic and logs using IDS and SIEM tools (8 hours, 9 minutes total module time)

Learners will explore logs and their role in IDSs and SIEM systems. They'll learn how these systems detect attacks. Learners will also be introduced to some IDS and SIEM products. In addition, they will have an opportunity to write basic IDS rules to provide alerts for malicious network traffic.

Module items

- 13 videos
- 9 readings
- 1 interactive plug-in
- 1 lab
- 3 self-review activities
- 1 discussion prompt
- 4 practice quizzes
- 1 graded quiz

COURSE 7: Automate Cybersecurity Tasks with Python

In this course, learners will be introduced to the Python programming language and how it can be used to automate cybersecurity-related tasks. First, learners will focus on foundational concepts of Python, including data types, variables, conditional statements, and iterative statements. Then, learners will develop functions in Python and work with string and list data. Finally, learners will explore algorithms that involve importing and parsing files.

Week 13

MODULE 1: Introduction to Python (12 hours, 5 minutes total module time)

Learners will get an introduction to the Python programming language and how Python is used in cybersecurity. They will also explore foundational Python concepts including data types, variables, conditional statements, and iterative statements.

Module items

- 12 videos
- 13 readings
- 1 interactive plug-in
- 8 labs
- 1 discussion prompt
- 3 practice quizzes
- 1 graded quiz

Week 14

MODULE 2: Write effective Python code (6 hours, 23 minutes total module time)

Learners will expand their ability to work with Python. They'll learn about pre-built and user-defined Python functions. Learners will also explore how modules help provide access to reusable code. Finally, they will make code readable.

Module items

- 10 videos
- 7 readings
- 2 labs
- 3 practice quizzes
- 1 graded quiz

MODULE 3: Work with strings and lists (8 hours, 38 minutes total module time)

Learners will explore more options for working with strings and lists in Python, and discover methods that can be applied to these data types. They will apply this knowledge to write a short algorithm. Finally, learners will use regular expressions to search for patterns in strings.

Module items

- 7 videos
- 7 readings
- 1 interactive plug-in
- 5 labs
- 3 practice quizzes
- 1 graded quiz

Week 15

MODULE 4: Python in practice (9 hours, 28 minutes total module time)

Learners will put Python into practice and focus on automating cybersecurity-related tasks, which requires working with files. They'll be introduced to opening and reading files. Then, they will learn to parse files and structure their contents. Finally, learners will focus on strategies for debugging code.

Module items

- 11 videos
- 9 readings
- 4 labs
- 1 self-review activity
- 2 discussion prompts
- 3 practice quizzes
- 1 graded quiz

COURSE 8: Put it to Work: Prepare for Cybersecurity Jobs

In this final course of the certificate program, learners will further develop their understanding of the importance of incident escalation, data and asset classification, and the impact cybersecurity incidents have on organizations and the people those organizations serve. Learners will also explore the role of stakeholders and develop strategies for effective stakeholder communications. Additionally, learners will be provided with resources to help them stay up-to-date on the latest cybersecurity news and to engage with the larger cybersecurity community. Finally, learners will receive guidance related to how to find, apply for, and prepare for a job as a cybersecurity analyst.

Week 16

MODULE 1: Protect data and communicate incidents (2 hours, 49 minutes total module time)

Learners will recognize the importance of security professionals in the workplace. They will also discover how proper detection and escalation can impact an organization's security posture.

Module items

- 6 videos
- 6 readings
- 1 interactive plug-in

- 2 discussion prompts
- 2 practice quizzes
- 1 graded quiz

MODULE 2: Escalate incidents (2 hours, 35 minutes total module time)

Learners will explore the importance of incident prioritization and escalation. Additionally, they'll learn how the decisions security professionals make help to keep business operations safe.

Module items

- 7 videos
- 5 readings
- 1 interactive plug-in
- 1 discussion prompt
- 2 practice quizzes
- 1 graded quiz

MODULE 3: Communicate effectively to influence stakeholders (2 hours, 49 minutes total module time)

Learners will examine the importance of stakeholders in cybersecurity. In addition, they will create clear and concise communications to stakeholders.

Module items

- 7 videos
- 5 readings
- 1 interactive plug-in
- 2 practice quizzes
- 1 graded quiz

MODULE 4: Engage with the cybersecurity community (2 hours, 25 minutes total module time)

Learners will prepare to stay up-to-date on the latest cybersecurity trends and explore how to engage with the security community.

Module items

- 6 videos
- 3 readings
- 1 self-review activity
- 1 practice quiz
- 1 graded quiz

MODULE 5: Find and apply for cybersecurity jobs (8 hours total module time)

Learners will prepare to search for jobs in the field of cybersecurity. They'll explore career readiness techniques, such as creating a resume, developing an elevator pitch, and preparing for the interview process. In addition, learners will have an opportunity to use career resources that can help them find and apply for jobs in cybersecurity.

Module items

- 18 videos
- 13 readings
- 3 self-review activities
- 5 discussion prompts
- 4 practice quizzes
- 1 graded quiz