

Google Cybersecurity Certificate



Key Competencies & Job Mapping

Developing talent for in-demand jobs

GOOGLE CAREER CERTIFICATES

Google Career Certificates give learners the skills they need to apply for more than 2.4 million in-demand jobs with a median salary of \$76,000+¹ across the fields of cybersecurity, data analytics, digital marketing & e-commerce, IT support, project management, and user experience (UX) design.

Google Career Certificates are taught and developed by Google employees working in these fields; they are hands-on, practical, and rigorous. A Google Career Certificate can be completed in under 6 months at a suggested pace of 10 hours a week or less. 75% of certificate graduates report a positive career outcome (e.g., new job, promotion, or raise) within six months of completion.²

GOOGLE CYBERSECURITY CERTIFICATE

The Google Cybersecurity Certificate teaches learners how to identify common cybersecurity risks, threats, and vulnerabilities, as well as the techniques to mitigate them.

This certificate program is for anyone who wants to enter the field of cybersecurity; no prior experience or specific knowledge is required. All you need is an interest in solving puzzles and helping others.

213K+

open jobs in
cybersecurity³

\$100K+

median salary in
cybersecurity (0-5 years
experience)³

THE GOOGLE CYBERSECURITY CERTIFICATE PREPARES LEARNERS FOR IN-DEMAND JOBS SUCH AS:

- Cybersecurity analyst
- Security analyst
- Security operations center (SOC) analyst
- Information security analyst
- IT security analyst
- Cyber defense analyst

¹ Lightcast™ US Job Postings (2022: Jan. 1, 2022 - Dec. 31, 2022).

² Based on program graduate survey, United States 2022

³ Lightcast™ US Job Postings (2022: Jan. 1, 2022 - Dec. 31, 2022).

Program Overview

Upon completing the **Google Cybersecurity Certificate**, graduates will:

- Understand the importance of cybersecurity practices and their impact for organizations.
- Identify common risks, threats, and vulnerabilities, as well as techniques to mitigate them.
- Gain hands-on experience with Python, Linux, and SQL.
- Protect networks, devices, people, and data from unauthorized access and cyber attacks using Security Information Event Management (SIEM) tools, Intrusion Detection Systems (IDS), and network protocol analyzers (packet sniffing).



Python



Linux



SQL



SIEM tools



IDS



Network security



Information security



NIST Cybersecurity Framework

Course 1

Foundations of Cybersecurity

Course 2

Play It Safe: Manage Security Risks

Course 3

Connect and Protect: Networks and Network Security

Course 4

Tools of the Trade: Linux and SQL

Course 5

Assets, Threats, and Vulnerabilities

Course 6

Sound the Alarm: Detection and Response

Course 7

Automate Cybersecurity Tasks with Python

Course 8

Put It to Work: Prepare for Cybersecurity Jobs

CONTENT BREAKDOWN:



314

Videos



252

Readings



157

Quizzes



125

Hands-on activities

PORTFOLIO ACTIVITY:

Each course in the Google Cybersecurity Certificate has activities where learners create artifacts for a professional portfolio, which can be shared with employers when applying for jobs.

Course 1 — Foundations of Cybersecurity

In this course, learners will be introduced to the world of cybersecurity through an interactive curriculum developed by Google. Learners will identify significant events that led to the development of the cybersecurity field, explain the importance of cybersecurity to today's business operations, and explore the job responsibilities and skills of an entry-level cybersecurity analyst.

By the end of this course, learners will:

- Identify how security attacks impact business operations.
- Explore the job responsibilities and core skills of an entry-level cybersecurity analyst.
- Recognize how past and present attacks on organizations led to the development of the cybersecurity field.
- Learn the CISSP eight security domains.
- Identify security domains, frameworks, and controls.
- Explain security ethics.
- Recognize common tools used by cybersecurity analysts.

Portfolio activity: In course 1, learners will draft a professional statement to include in their portfolio.





SKILLS ACQUIRED:

- ❑ Introduction to cybersecurity concepts
- ❑ Historical attacks, such as the Brain virus and the Morris worm
- ❑ Ethics in cybersecurity
- ❑ Workplace skills like communication and collaboration

TOPICS:

- ★ Introduction to the exciting world of cybersecurity
- ★ The evolution of cybersecurity
- ★ Protect against threats, risks, and vulnerabilities
- ★ Cybersecurity tools and programming languages

CONTENT BREAKDOWN:

	29	Videos
	21	Readings
	13	Quizzes
	10	Hands-on activities

Course 2 — Play It Safe: Manage Security Risks

In this course, learners will take a deeper dive into concepts introduced in the first course, with an emphasis on how cybersecurity professionals use frameworks and controls to protect business operations. In particular, they'll identify the steps of risk management and explore common threats, risks, and vulnerabilities. Additionally, they'll explore Security Information and Event Management (SIEM) data and use a playbook to respond to identified threats, risks, and vulnerabilities. Finally, they will take an important step towards becoming a cybersecurity professional by practicing performing a security audit.

By the end of this course, learners will:

- Identify the common threats, risks, and vulnerabilities to business operations.
- Understand the threats, risks, and vulnerabilities that entry-level cybersecurity analysts are most focused on.
- Comprehend the purpose of security frameworks and controls.
- Describe the confidentiality, integrity, and availability (CIA) triad.
- Explain the National Institute of Standards and Technology (NIST) framework.
- Explore and practice conducting a security audit.
- Use a playbook to respond to threats, risks, and vulnerabilities.

Portfolio activity: In course 2, learners will complete a security audit to include in their portfolio.





SKILLS ACQUIRED:

- ❑ CIA triad
- ❑ NIST Cybersecurity Framework (CSF)
- ❑ NIST Risk Management Framework (RMF)
- ❑ Security audits
- ❑ Incident response playbooks
- ❑ Workplace skills like critical thinking and analysis

TOPICS:

- ★ Security domains
- ★ Security frameworks and controls
- ★ Explore cybersecurity tools
- ★ Use playbooks to respond to incidents

CONTENT BREAKDOWN:

	35	Videos
	21	Readings
	15	Quizzes
	7	Hands-on activities

Course 3 — Connect and Protect: Networks and Network Security

In this course, learners will explore how networks connect multiple devices and allow them to communicate. They'll start with the fundamentals of modern networking operations and protocols. For example, they'll learn about the Transmission Control Protocol / Internet Protocol (TCP/IP) model and how network hardware, like routers and modems, allow computers to send and receive information on the internet. Then, they'll learn about network security. Organizations often store and send valuable information on their networks, so networks are common targets of cyber attacks. By the end of this course, learners will be able to recognize network-level vulnerabilities, and explain how to secure a network using firewalls, system hardening, and virtual private networks.

By the end of this course, learners will:

- Describe the structure of different computer networks.
- Illustrate how data is sent and received over a network.
- Recognize common network protocols.
- Identify common network security measures and protocols.
- Explain how to secure a network against intrusion tactics.
- Compare and contrast local networks to cloud computing.
- Explain the different types of system hardening techniques.

Portfolio activity: In course 3, learners will complete a network structure and security analysis to include in their portfolio.





SKILLS ACQUIRED:

- ❑ Network architecture
- ❑ Cloud networks
- ❑ Network security
- ❑ The Transmission Control Protocol / Internet Protocol (TCP/IP)
- ❑ Security hardening
- ❑ Workplace skills like problem solving and conceptualization

TOPICS:

- ★ Network architecture
- ★ Network operations
- ★ Secure against network intrusions
- ★ Security hardening

CONTENT BREAKDOWN:

	37	Videos
	32	Readings
	19	Quizzes
	10	Hands-on activities

Course 4 — Tools of the Trade: Linux and SQL

In this course, learners will explore computing skills that they'll use on-the-job as a cybersecurity analyst. First, they'll practice using Linux, an operating system commonly used by cybersecurity professionals. For example, they will use the Linux command line through the Bash shell to navigate and manage the file system and authenticate users. Then, they will use SQL to communicate with a database.

By the end of this course, learners will:

- Explain the relationship between operating systems, applications, and hardware.
- Compare a graphical user interface to a command line interface.
- Identify the unique features of common Linux distributions.
- Navigate and manage the file system using Linux commands via the Bash shell.
- Use Linux commands via the Bash shell to authenticate and authorize users.
- Describe how a relational database is organized.
- Use SQL to retrieve information from a database.
- Apply filters to SQL queries and use joins to combine multiple tables.

Portfolio activity: In course 4, learners will use Linux commands to manage file permissions and apply filters to SQL queries to include in their portfolio.





SKILLS ACQUIRED:

- ❑ Command line interface (CLI)
- ❑ Linux
- ❑ Bash
- ❑ SQL
- ❑ Workplace skills like research and organization

TOPICS:

- ★ Introduction to operating systems
- ★ The Linux operating system
- ★ Linux commands in the Bash shell
- ★ Databases and SQL

CONTENT BREAKDOWN:

	42	Videos
	35	Readings
	21	Quizzes
	26	Hands-on activities

Course 5 — Assets, Threats, and Vulnerabilities

In this course, learners will explore the concepts of assets, threats, and vulnerabilities. First, they'll build an understanding of how assets are classified. Next, they will become familiar with common threats and vulnerabilities, and the security controls used by organizations to protect valuable information and mitigate risk. Learners will develop an attacker mindset by practicing the threat modeling process, and learn tactics for staying ahead of security breaches.

By the end of this course, learners will:

- Learn effective data handling processes.
- Discuss the role of encryption and hashing in securing assets.
- Describe how to effectively use authentication and authorization.
- Explain how common vulnerability exposures are identified by MITRE.
- Analyze an attack surface to find risks and vulnerabilities.
- Identify threats, such as social engineering, malware, and web-based exploits.
- Summarize the threat modeling process.

Portfolio activity: In course 5, learners will identify vulnerabilities for a small business to include in their portfolio.





SKILLS ACQUIRED:

- ❑ Asset classification
- ❑ Threat analysis
- ❑ Vulnerability assessment
- ❑ Authentication
- ❑ Cryptography
- ❑ Workplace skills like strategic planning and prioritization

TOPICS:

- ★ Introduction to asset security
- ★ Protect organizational assets
- ★ Vulnerabilities in systems
- ★ Threats to asset security

CONTENT BREAKDOWN:

	43	Videos
	40	Readings
	26	Quizzes
	18	Hands-on activities

Course 6 — Sound the Alarm: Detection and Response

In this course, learners will focus on incident detection and response. They'll define a security incident and explain the incident response lifecycle, including the roles and responsibilities of incident response teams. They'll analyze and interpret network communications to detect security incidents using packet sniffing tools to capture network traffic. By assessing and analyzing artifacts, they'll explore the incident investigation and response processes and procedures. Additionally, they will practice using Intrusion Detection Systems (IDS) and Security Information Event Management (SIEM) tools.

By the end of this course, learners will:

- Explain the lifecycle of an incident.
- Describe the tools used in documentation, detection, and management of incidents.
- Analyze packets to interpret network communications.
- Perform artifact investigations to analyze and verify security incidents.
- Identify the steps to contain, eradicate, and recover from an incident.
- Determine how to read and analyze logs during incident investigation.
- Interpret the basic syntax and components of signatures and logs in IDS and Network Intrusion Detection Systems (NIDS) tools.
- Perform queries in SIEM tools to investigate an event.

Portfolio activity: In course 6, learners will develop an incident handlers journal to include in their portfolio.





SKILLS ACQUIRED:

- ❑ Splunk
- ❑ Chronicle
- ❑ Suricata
- ❑ Packet capture
- ❑ Packet analysis
- ❑ Workplace skills like escalation and documentation

TOPICS:

- ★ Introduction to detection and incident response
- ★ Network monitoring and analysis
- ★ Incident investigation and response
- ★ Network traffic and logs using IDS and SIEM tools

CONTENT BREAKDOWN:

	46	Videos
	35	Readings
	26	Quizzes
	18	Hands-on activities

Course 7 — Automate Cybersecurity Tasks with Python

In this course, learners will be introduced to the Python programming language and apply it in a cybersecurity setting to automate tasks. They'll start with foundational Python programming concepts, including data types, variables, conditional statements, and iterative statements. They'll also learn to work with Python effectively by developing functions, using libraries and modules, and making code readable. In addition, they'll work with string and list data, and learn how to import, parse, and debug files.

By the end of this course, learners will:

- Explain how the Python programming language is used in cybersecurity.
- Write conditional and iterative statements in Python.
- Create new, user-defined Python functions.
- Use Python to work with strings and lists.
- Use regular expressions to extract information from text.
- Use Python to open and read the contents of a file.
- Identify best practices to improve code readability.
- Practice debugging code.

Portfolio activity: In course 7, learners will update files using Python algorithms to include in their portfolio.





SKILLS ACQUIRED:

- ❑ Python
- ❑ Coding skills
- ❑ PEP 8 style guide
- ❑ Workplace skills like analytical thinking and attention to detail

TOPICS:

- ★ Introduction to Python
- ★ Write effective Python code
- ★ Work with strings and lists
- ★ Python in practice

CONTENT BREAKDOWN:

	40	Videos
	32	Readings
	17	Quizzes
	18	Hands-on activities

Course 8 — Put It to Work: Prepare for Cybersecurity Jobs

In this course, learners will focus on making decisions and escalating incidents to stakeholders. They'll develop the communication and collaboration skills needed to inform and influence stakeholders within an organization. In addition, they'll explore how to ethically operate as a cybersecurity professional. They will discover how to engage with the cybersecurity community, explore jobs in the cybersecurity field, and complete practice interviews. They'll also write a resume and cover letter to prepare for applying and interviewing for jobs in cybersecurity.

By the end of this course, learners will:

- Determine when and how to escalate a security incident.
- Explain how having an ethical mindset supports a cybersecurity professional's ability to protect assets and data.
- Communicate sensitive information with care and confidentiality.
- Use reliable sources to remain current on the latest cybersecurity threats, risks, vulnerabilities, and tools.
- Engage with the cybersecurity community.
- Find and apply for cybersecurity jobs.
- Prepare for job interviews.

Portfolio activity: In course 8, learners will create or update their resume.





SKILLS ACQUIRED:

- ❑ Stakeholder communication
- ❑ Escalation
- ❑ Job preparedness like resume and portfolio preparation
- ❑ Workplace skills like integrity and discretion

TOPICS:

- ★ Protect data and communicate incidents
- ★ Escalate incidents
- ★ Communicate effectively to influence stakeholders
- ★ Engage with the cybersecurity community
- ★ Find and apply for cybersecurity jobs

CONTENT BREAKDOWN:

	42	Videos
	36	Readings
	20	Quizzes
	15	Hands-on activities