**Google Cybersecurity Certificate overview**

Hello, and welcome to the **Google Cybersecurity Certificate**! In this program, you will explore the growing field of cybersecurity, learn how cybersecurity is crucial to organizations and the people they serve, and develop relevant skills for a future career in the field. By completing the eight courses in this certificate program, you'll prepare for entry-level jobs in cybersecurity, such as cybersecurity analyst, security analyst, and security operations center (SOC) analyst. No prior experience in cybersecurity is required to complete this program.

**Enter a growing field**

Why are skills in cybersecurity in such high demand? The world is undergoing a digital transformation. Every day, global access to the internet is expanding, introducing more devices, more applications, and an even larger amount of data to the World Wide Web. As a result, threats, risks, and vulnerabilities are expanding and causing a significant amount of harm to organizations and people. Cybersecurity professionals are in high demand to help keep organizations, people, and data safe.

Throughout the program, you will have multiple opportunities to develop your cybersecurity knowledge and skills. You will explore concepts and scenarios to learn what an entry-level cybersecurity analyst must know and be able to do to thrive in the cybersecurity profession.

**Google Cybersecurity Certificate courses**

The Google Cybersecurity Certificate has eight courses that focus and build upon core concepts and skills related to the daily work of cybersecurity professionals, including foundational cybersecurity models and frameworks that are used to mitigate risk; protecting networks and data; using programming to automate tasks; identifying and responding to security incidents; and communicating and collaborating with stakeholders. Additionally, you will apply what you’ve learned in each course by completing portfolio projects that can be used to showcase your understanding of essential cybersecurity concepts to potential employers. The courses of the program are as follows:

1. [**Foundations of Cybersecurity**](https://www.coursera.org/learn/foundations-of-cybersecurity/home/week/1)

 *(current course)*

 [**Play It Safe: Manage Security Risks**](https://www.coursera.org/learn/manage-security-risks/home/week/1)



 [**Connect and Protect: Networks and Network Security**](https://www.coursera.org/learn/networks-and-network-security/home/week/1)



 [**Tools of the Trade: Linux and SQL**](https://www.coursera.org/learn/linux-and-sql/home/week/1)



 [**Assets, Threats, and Vulnerabilities**](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/home/week/1)



 [**Sound the Alarm: Detection and Response**](https://www.coursera.org/learn/detection-and-response/home/week/1)

  [**Automate Cybersecurity Tasks with Python**](https://www.coursera.org/learn/automate-cybersecurity-tasks-with-python/home/week/1)



 [**Put It to Work: Prepare for Cybersecurity Jobs**](https://www.coursera.org/learn/prepare-for-cybersecurity-jobs/home/week/1)





**Benefits for job seekers**

After completing all eight courses, Google Cybersecurity Certificate graduates have access to job search resources, courtesy of Google. You’ll have the opportunity to:

* Build your resume, participate in mock interviews, and receive job search tips through Big Interview, a job-training platform that’s free for program graduates.
* Improve your interview technique with Interview Warmup, a tool built by Google with certificate graduates in mind. Access cybersecurity-specific practice questions, transcripts of your responses, and automatic insights that help you grow your skills and confidence.
* Access thousands of job postings and free one-on-one career coaching with Career Circle. (You must be eligible to work in the U.S. to join.)
* Claim your Google Cybersecurity Certificate badge, and share your achievement on LinkedIn® professional networking services to stand out among other candidates to potential employers.
* Prepare for the CompTIA Security+ exam, the industry-leading certification for cybersecurity roles. You’ll earn a dual credential when you complete both the Google Cybersecurity Certificate and the CompTIA Security+ exam.

Congratulations on taking this first step to build your skills for a career in cybersecurity. Enjoy the journey!

**Course 1 overview**

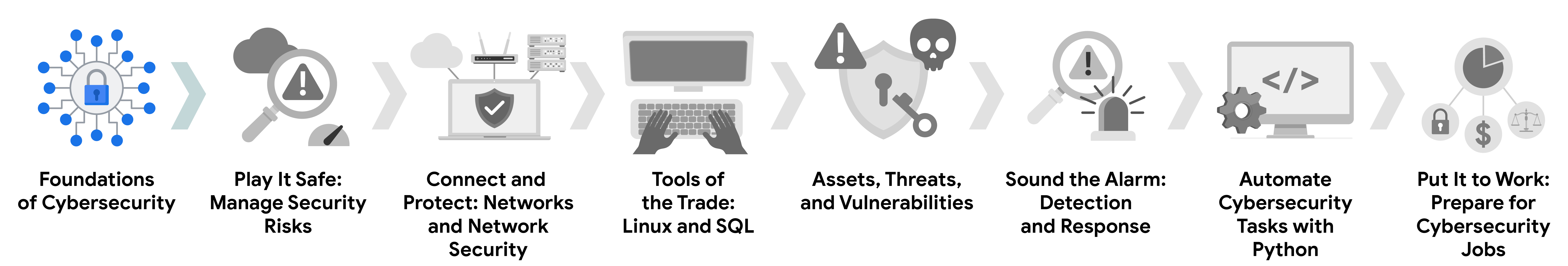


Hello, and welcome to **Foundations of Cybersecurity**, the first course in the Google Cybersecurity Certificate. You’ve begun an exciting journey!

In this course, you will learn the primary job responsibilities and core skills of those who work in the field of cybersecurity. You will explore the eight Certified Information Systems Security Professional (CISSP) security domains, various security frameworks and controls, as well as a foundational security model called the confidentiality, integrity, and availability (CIA) triad. You will also be introduced to some common tools used by security analysts that help protect organizations and people alike.

**Certificate program progress**

The Google Cybersecurity Certificate program has eight courses. **Foundations of Cybersecurity** is the first course.



1. [**Foundations of Cybersecurity**](https://www.coursera.org/learn/foundations-of-cybersecurity/home/week/1)

 — *(current course)* 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.

 [**Play It Safe: Manage Security Risks**](https://www.coursera.org/learn/manage-security-risks/home/week/1)

 — Identify how cybersecurity professionals use frameworks and controls to protect business operations, and explore common cybersecurity tools.

 [**Connect and Protect: Networks and Network Security**](https://www.coursera.org/learn/networks-and-network-security/home/week/1)

 — Gain an understanding of network-level vulnerabilities and how to secure networks.

 [**Tools of the Trade: Linux and SQL**](https://www.coursera.org/learn/linux-and-sql/home/week/1)

 — Explore foundational computing skills, including communicating with the Linux operating system through the command line and querying databases with SQL.

 [**Assets, Threats, and Vulnerabilities**](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/home/week/1)

 — 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.

 [**Sound the Alarm: Detection and Response**](https://www.coursera.org/learn/detection-and-response/home/week/1)

 — Understand the incident response lifecycle and practice using tools to detect and respond to cybersecurity incidents.

 [**Automate Cybersecurity Tasks with Python**](https://www.coursera.org/learn/automate-cybersecurity-tasks-with-python/home/week/1)

 — Explore the Python programming language and write code to automate cybersecurity tasks.

 [**Put It to Work: Prepare for Cybersecurity Jobs**](https://www.coursera.org/learn/prepare-for-cybersecurity-jobs/home/week/1)

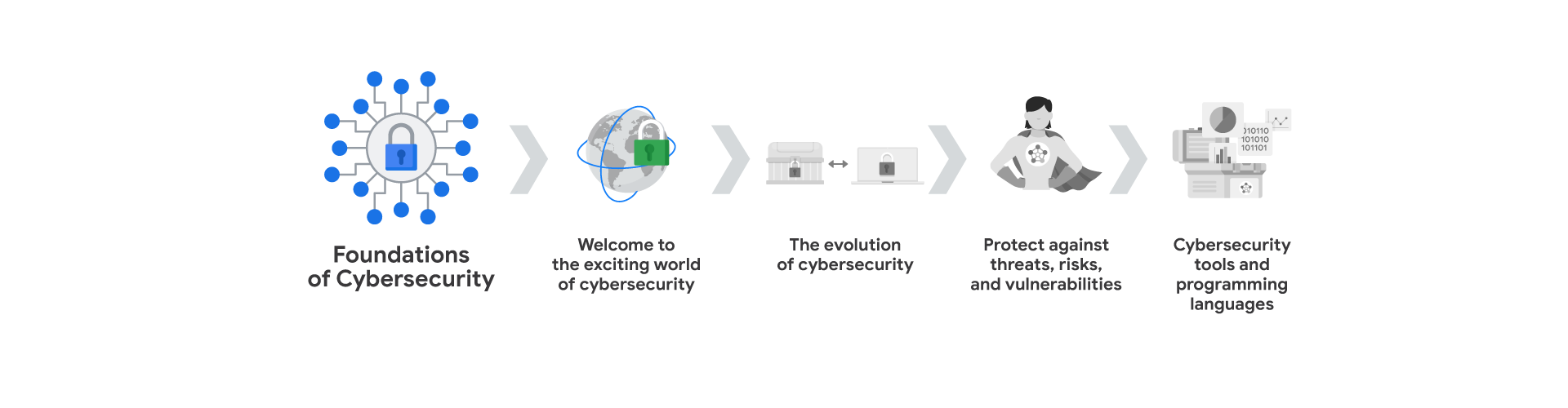
1. — Learn about incident classification, escalation, and ways to communicate with stakeholders. This course closes out the program with tips on how to engage with the cybersecurity community and prepare for your job search.

**Course 1 content**

Each course of 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 Cybersecurity Certificate in about six months.

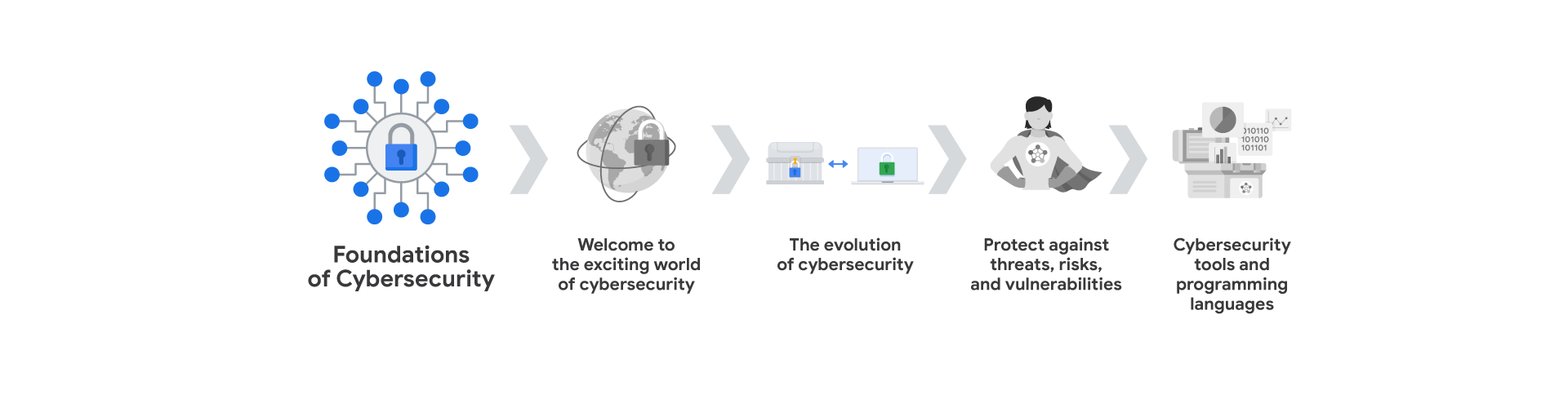
What’s to come? Here’s a quick overview of the skills you’ll learn in each module of this course.

**Module 1: Welcome to the exciting world of cybersecurity**



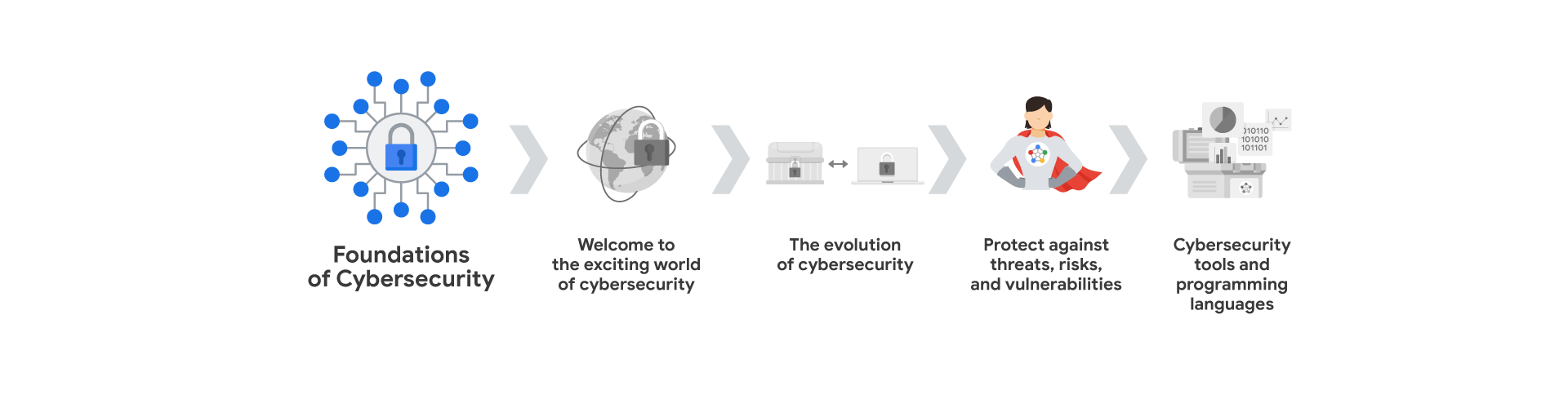
Begin your journey into cybersecurity! You'll explore the cybersecurity field, and learn about the job responsibilities of cybersecurity professionals.

**Module 2: The evolution of cybersecurity**



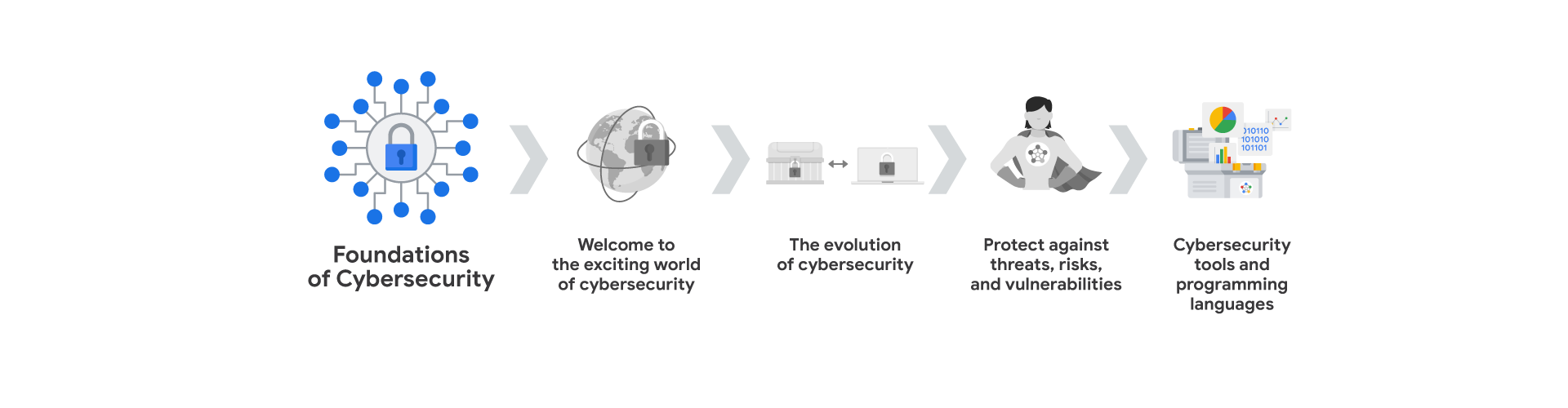
You will explore how cybersecurity threats have appeared and evolved alongside the adoption of computers. You will also understand how past and present cyber attacks have influenced the development of the security field. In addition, you'll get an overview of the eight security domains.

**Module 3: Protect against threats, risks, and vulnerabilities**



You will learn about security frameworks and controls, which are used to mitigate organizational risk. You'll cover principles of the CIA triad and various National Institute of Standards and Technology (NIST) frameworks. In addition, you'll explore security ethics.

**Module 4: Cybersecurity tools and programming languages**



You’ll discover common tools used by cybersecurity analysts to identify and eliminate risk. You'll learn about security information and event management (SIEM) tools, network protocol analyzers, and programming languages such as Python and SQL.

**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](https://www.coursera.org/learn/foundations-of-cybersecurity/discussions)
* .
* **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](https://www.coursera.org/learn/foundations-of-cybersecurity/resources/L1aML)

 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](https://www.coursera.support/s/article/208280036-Coursera-Code-of-Conduct?)

to ensure that the learning community remains a welcoming, friendly, and supportive place for all members.

# Common cybersecurity terminology

Informações:

Este item inclui conteúdo que ainda não foi traduzido para o idioma de sua preferência.

As you’ve learned, **cybersecurity** (also known as security) is the practice of ensuring confidentiality, integrity, and availability of information by protecting networks, devices, people, and data from unauthorized access or criminal exploitation. In this reading, you’ll be introduced to some key terms used in the cybersecurity profession. Then, you’ll be provided with a resource that’s useful for staying informed about changes to cybersecurity terminology.

## Key cybersecurity terms and concepts

There are many terms and concepts that are important for security professionals to know. Being familiar with them can help you better identify the threats that can harm organizations and people alike. A security analyst or cybersecurity analyst focuses on monitoring networks for breaches. They also help develop strategies to secure an organization and research information technology (IT) security trends to remain alert and informed about potential threats. Additionally, an analyst works to prevent incidents. In order for analysts to effectively do these types of tasks, they need to develop knowledge of the following key concepts.

**Compliance** is the process of adhering to internal standards and external regulations and enables organizations to avoid fines and security breaches.

**Security frameworks** are guidelines used for building plans to help mitigate risks and threats to data and privacy.

**Security controls** are safeguards designed to reduce specific security risks. They are used with security frameworks to establish a strong security posture.

**Security posture** is an organization’s ability to manage its defense of critical assets and data and react to change. A strong security posture leads to lower risk for the organization.

A **threat actor**, or malicious attacker, is any person or group who presents a security risk. This risk can relate to computers, applications, networks, and data.

An **internal threat** can be a current or former employee, an external vendor, or a trusted partner who poses a security risk. At times, an internal threat is accidental. For example, an employee who accidentally clicks on a malicious email link would be considered an accidental threat. Other times, the internal threat actor intentionally engages in risky activities, such as unauthorized data access.

**Network security** is the practice of keeping an organization's network infrastructure secure from unauthorized access. This includes data, services, systems, and devices that are stored in an organization’s network.

**Cloud security** is the process of ensuring that assets stored in the cloud are properly configured, or set up correctly, and access to those assets is limited to authorized users. The cloud is a network made up of a collection of servers or computers that store resources and data in remote physical locations known as data centers that can be accessed via the internet. Cloud security is a growing subfield of cybersecurity that specifically focuses on the protection of data, applications, and infrastructure in the cloud.

**Programming** is a process that can be used to create a specific set of instructions for a computer to execute tasks. These tasks can include:

* Automation of repetitive tasks (e.g., searching a list of malicious domains)
* Reviewing web traffic
* Alerting suspicious activity

## Key takeaways

Understanding key technical terms and concepts used in the security field will help prepare you for your role as a security analyst. Knowing these terms can help you identify common threats, risks, and vulnerabilities. To explore a variety of cybersecurity terms, visit the [National Institute of Standards and Technology glossary](https://csrc.nist.gov/glossary)

. Or use your browser to search for high-quality, reliable cybersecurity glossaries from research institutes or governmental authorities. Glossaries are available in multiple languages.

# Transferable and technical cybersecurity skills

Informações:

Este item inclui conteúdo que ainda não foi traduzido para o idioma de sua preferência.

Previously, you learned that cybersecurity analysts need to develop certain core skills to be successful at work. **Transferable skills** are skills from other areas of study or practice that can apply to different careers. **Technical skills** may apply to several professions, as well; however, they typically require knowledge of specific tools, procedures, and policies. In this reading, you’ll explore both transferable skills and technical skills further.

## Transferable skills

You have probably developed many transferable skills through life experiences; some of those skills will help you thrive as a cybersecurity professional. These include:

* **Communication:** As a cybersecurity analyst, you will need to communicate and collaborate with others. Understanding others’ questions or concerns and communicating information clearly to individuals with technical and non-technical knowledge will help you mitigate security issues quickly.
* **Problem-solving:** One of your main tasks as a cybersecurity analyst will be to proactively identify and solve problems. You can do this by recognizing attack patterns, then determining the most efficient solution to minimize risk. Don't be afraid to take risks, and try new things. Also, understand that it's rare to find a perfect solution to a problem. You’ll likely need to compromise.
* **Time management:** Having a heightened sense of urgency and prioritizing tasks appropriately is essential in the cybersecurity field. So, effective time management will help you minimize potential damage and risk to critical assets and data. Additionally, it will be important to prioritize tasks and stay focused on the most urgent issue.
* **Growth mindset:** This is an evolving industry, so an important transferable skill is a willingness to learn. Technology moves fast, and that's a great thing! It doesn't mean you will need to learn it all, but it does mean that you’ll need to continue to learn throughout your career. Fortunately, you will be able to apply much of what you learn in this program to your ongoing professional development.
* **Diverse perspectives:** The only way to go far is together. By having respect for each other and encouraging diverse perspectives and mutual respect, you’ll undoubtedly find multiple and better solutions to security problems.

## Technical skills

There are many technical skills that will help you be successful in the cybersecurity field. You’ll learn and practice these skills as you progress through the certificate program. Some of the tools and concepts you’ll need to use and be able to understand include:

* **Programming languages:** By understanding how to use programming languages, cybersecurity analysts can automate tasks that would otherwise be very time consuming. Examples of tasks that programming can be used for include searching data to identify potential threats or organizing and analyzing information to identify patterns related to security issues.
* **Security information and event management (SIEM) tools:** SIEM tools collect and analyze log data, or records of events such as unusual login behavior, and support analysts’ ability to monitor critical activities in an organization. This helps cybersecurity professionals identify and analyze potential security threats, risks, and vulnerabilities more efficiently.
* **Intrusion detection systems (IDSs):** Cybersecurity analysts use IDSs to monitor system activity and alerts for possible intrusions. It’s important to become familiar with IDSs because they’re a key tool that every organization uses to protect assets and data. For example, you might use an IDS to monitor networks for signs of malicious activity, like unauthorized access to a network.
* **Threat landscape knowledge:** Being aware of current trends related to threat actors, malware, or threat methodologies is vital. This knowledge allows security teams to build stronger defenses against threat actor tactics and techniques. By staying up to date on attack trends and patterns, security professionals are better able to recognize when new types of threats emerge such as a new ransomware variant.
* **Incident response:** Cybersecurity analysts need to be able to follow established policies and procedures to respond to incidents appropriately. For example, a security analyst might receive an alert about a possible malware attack, then follow the organization’s outlined procedures to start the incident response process. This could involve conducting an investigation to identify the root issue and establishing ways to remediate it.

## CompTIA Security+

In addition to gaining skills that will help you succeed as a cybersecurity professional, the Google Cybersecurity Certificate helps prepare you for the [CompTIA Security+ exam](https://www.comptia.org/certifications/security)

, the industry leading certification for cybersecurity roles. You’ll earn a dual credential when you complete both, which can be shared with potential employers. After completing all eight courses in the Google Cybersecurity Certificate, you will unlock a 30% discount for the CompTIA Security+ exam and additional practice materials.

## Key takeaways

Understanding the benefits of core transferable and technical skills can help prepare you to successfully enter the cybersecurity workforce. Throughout this program, you’ll have multiple opportunities to develop these and other key cybersecurity analyst skills.

# Glossary terms from module 1

## ****Terms and definitions from Course 1, Module 1****

**Cybersecurity (or security):** The practice of ensuring confidentiality, integrity, and availability of information by protecting networks, devices, people, and data from unauthorized access or criminal exploitation

**Cloud security:** The process of ensuring that assets stored in the cloud are properly configured and access to those assets is limited to authorized users

**Internal threat:** A current or former employee, external vendor, or trusted partner who poses a security risk

**Network security:** The practice of keeping an organization's network infrastructure secure from unauthorized access

**Personally identifiable information (PII):** Any information used to infer an individual’s identity

**Security posture:** An organization’s ability to manage its defense of critical assets and data and react to change

**Sensitive personally identifiable information (SPII):** A specific type of PII that falls under stricter handling guidelines

**Technical skills:** Skills that require knowledge of specific tools, procedures, and policies

**Threat:** Any circumstance or event that can negatively impact assets

**Threat actor:** Any person or group who presents a security risk

**Transferable skills:** Skills from other areas that can apply to different careers