Google Career Certificates

Cybersecurity

Course Readings: Course 8

Table of Contents

Table of Contents continued

Course 8_ Module 5

Google

Course 8 - module 1

Hello, and welcome to **Put It to Work: Prepare for Cybersecurity Jobs**, the eighth and final course in the Google Cybersecurity Certificate. You've made such great progress, and you're almost ready to complete your journey!

By the end of this course, you will be able to understand the importance of incident escalation, classify data and assets, and recognize the impact security incidents can have on an organization. You will also be able to define stakeholders, describe their security roles, and learn strategies for communicating with them. Additionally, you will learn about resources that will help you stay current on what's happening in the security field, as well as how to engage with the security community. Finally, you will learn how to find, apply for, and prepare for a job as a security analyst.

Certificate program progress

The Google Cybersecurity Certificate program has eight courses. **Put It to Work: Prepare for Cybersecurity Jobs** is the eighth and final 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 — 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 — *(current course)* 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 8 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: Protect data and communicate incidents

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

Week 2: Escalate incidents

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

Week 3: Communicate effectively to influence stakeholders

You will learn about important stakeholders in cybersecurity. In addition, you'll create clear and concise communications to stakeholders.

Week 4: Engage with the cybersecurity community

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

Week 5: Find and apply for cybersecurity jobs

You will prepare for your job search. You will explore career readiness techniques, such as creating a resume, developing an elevator pitch, and preparing for the interview process. Finally, you'll use career resources that can help you find and apply for jobs in cybersecurity.

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.

Google

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.

Helpful resources and tips

As a learner, you can choose to complete one or multiple courses in this program. However, to obtain the Google Cybersecurity Certificate, you must complete all the courses. This reading describes what is required to obtain a certificate and best practices for you to have a good learning experience on Coursera.

Course completion to obtain a certificate

To submit graded assignments and be eligible to receive a Google Cybersecurity Certificate, you must:

- Pay the course certificate fee or apply and be approved for a Coursera scholarship.
- Pass all graded quizzes in the eight courses with a score of at least 80%. Each graded quiz in a course is part of a cumulative grade for that course.

Healthy habits for course completion

Here is a list of best practices that will help you complete the courses in the program in a timely manner:

- **Plan your time:** Setting regular study times and following them each week can help you make learning a part of your routine. Use a calendar or timetable to create a schedule, and list what you plan to do each day in order to set achievable goals. Find a space that allows you to focus when you watch the videos, review the readings, and complete the activities.
- **Work at your own pace:** Everyone learns differently, so this program has been designed to let you work at your own pace. Although your personalized deadlines start when you enroll, feel free to move through the program at the speed that works best for you. There is no penalty for late assignments; to earn your certificate, all you have to do is complete all of the work. You can extend your deadlines at any time by going to **Overview** in the navigation panel and selecting **Switch Sessions**. If you have already missed previous deadlines, select **Reset my deadlines** instead.
- **Be curious:** If you find an idea that gets you excited, act on it! Ask questions, search for more details online, explore the links that interest you, and take notes on your discoveries. The steps you take to support your learning along the way will advance your knowledge, create more opportunities in this high-growth field, and help you qualify for jobs.
- **Take notes:** Notes will help you remember important information in the future, especially as you're preparing to enter a new job field. In addition, taking notes is an effective way to make connections between topics and gain a better understanding of those topics.
- **Review exemplars:** Exemplars are completed assignments that fully meet an activity's criteria. Many activities in this program have exemplars for you to validate your work or check for errors. Although there are often many different ways to complete an assignment, exemplars offer you guidance and inspiration as you progress through the program.
- **Chat (responsibly) with other learners:** If you have a question, chances are, you're not alone. Use the discussion forums to ask for help from other learners taking this program. You can also visit Coursera's Global Online Community. Other important things to know while learning with others can be found in the Coursera Honor Code and Code of Conduct.
- **Update your profile:** Consider updating your profile on Coursera with your photo, career goals, and more. When other learners find you in the discussion forums, they can click on your name to access your profile and get to know you better.

Documents, spreadsheets, presentations, and labs for course activities

To complete certain activities in the program, you will need to use digital documents, spreadsheets, presentations, and/or labs. Security professionals use these software tools to collaborate within their teams and organizations. If you need more information about using a particular tool, refer to these resources:

- Microsoft Word: Help and learning: Microsoft Support page for Word
- Google Docs: Help Center page for Google Docs
- Microsoft Excel: Help and learning: Microsoft Support page for Excel
- Google Sheets: Help Center page for Google Sheets
- Microsoft PowerPoint: Help and learning: Microsoft Support page for PowerPoint
- How to use Google Slides: Help Center page for Google Slides
- Common problems with labs: Troubleshooting help for Qwiklabs activities

Weekly, course, and certificate glossaries

This program covers a lot of terms and concepts, some of which you may already know and some of which may be unfamiliar to you. To review terms and help you prepare for graded quizzes, refer to the following glossaries:

- **Weekly glossaries**: At the end of each week's content, you can review a glossary of terms from that week. Each week's glossary builds upon the terms from the previous weeks in that course. The weekly glossaries are not downloadable; however, all of the terms and definitions are included in the course and certificate glossaries, which are downloadable.
- **Course glossaries**: At the end of each course, you can access and download a glossary that covers all of the terms in that course.
- **Certificate glossary**: The certificate glossary includes all of the terms in the entire certificate program and is a helpful resource that you can reference throughout the program or at any time in the future.

You can access and download the certificate glossaries and save them on your computer. You can always find the course and certificate glossaries through the course's Resources section. To access the **Cybersecurity Certificate glossary**, click the link below and select *Use Template*.

- Cybersecurity Certificate glossary OR
- If you don't have a Google account, you can download the glossary directly from the attachment here.

Course feedback

Providing feedback on videos, readings, and other materials is easy. With the resource open in your browser, you can find the thumbs-up and thumbs-down symbols.

- Click **thumbs-up** for materials you find helpful.
- Click **thumbs-down** for materials that you do not find helpful.

If you want to flag a specific issue with an item, click the flag icon, select a category, and enter an explanation in the text box. This feedback goes back to the course development team and isn't visible to other learners. All feedback received helps to create even better certificate programs in the future.

For technical help, visit the Learner Help Center.

Data and asset classification

Protecting an organization's business operations and assets from security threats, risks, and vulnerabilities is important. You previously learned what it means to have a security mindset. That mindset can help you identify and reduce security risks and potential incidents.

In this reading, you will learn about key data classification types and the difference between the low-level and high-level assets of an organization.

Classifying for safety

Security professionals classify data types to help them properly protect an organization from cyber attacks that negatively impact business operations. Here is a review of the most common data types:

- **Public data**
- **Private data**
- **Sensitive data**
- **Confidential data**

Public data

This data classification does not need extra security protections. **Public data** is already accessible to the public and poses a minimal risk to the organization if viewed or shared by others. Although this data is open to the public, it still needs to be protected from security attacks. Examples of public data include press releases, job descriptions, and marketing materials.

Private data

This data classification type has a higher security level. **Private data** is information that should be kept from the public. If an individual gains unauthorized access to private data, that event has the potential to pose a serious risk to an organization.

Examples of private data can include company email addresses, employee identification numbers, and an organization's research data.

Sensitive data

This information must be protected from everyone who does not have authorized access. Unauthorized access to sensitive data can cause significant damage to an organization's finances and reputation.

Sensitive data includes personally identifiable information (PII), sensitive personally identifiable information (SPII), and protected health information (PHI). Examples of these types of sensitive data are banking account numbers, usernames and passwords, social security numbers (which U.S. citizens use to report their wages to the government), passwords, passport numbers, and medical information.

Confidential data

This data classification type is important for an organization's ongoing business operations. **Confidential data** often has limits on the number of people who have access to it. Access to confidential data sometimes involves the signing of non-disclosure agreements (NDAs)— legal contracts that bind two or more parties to protect information—to further protect the confidentiality of the data.

Examples of confidential data include proprietary information such as trade secrets, financial records, and sensitive government data.

Asset classification

Asset classification means labeling assets based on sensitivity and importance to an organization. The classification of an organization's assets ranges from low- to high-level.

Public data is a low-level asset. It is readily available to the public and will not have a negative impact on an organization if compromised. Sensitive data and confidential data are high-level assets. They can have a significantly negative impact on an organization if leaked publicly. That negative impact can lead to the loss of a company's competitive edge, reputation, and customer trust. A company's website address is an example of a low-level asset. An internal email from that company discussing trade secrets is an example of a high-level asset.

Key takeaways

Every company has their own data classification policy that identifies what type of data is in each category. It will be important to your success as a security professional to familiarize yourself with that policy. Understanding different data and asset classification types is important. It helps you prioritize what data needs to be protected most. It also helps you recognize what assets need higher levels of security and what assets need minimal security.

Disaster recovery and business continuity

The role of a security professional is to ensure a company's data and assets are protected from threats, risks, and vulnerabilities. However, sometimes things don't go as planned. There are times when security incidents happen. You've already learned that security breaches can lead to financial consequences and the loss of credibility with customers or other businesses in the industry.

This reading will discuss the need to create business continuity and disaster recovery plans to minimize the impact of a security incident on an organization's business operations. Analysts need to consider the sequence of steps to be taken by the security team before business continuity and disaster recovery plans are implemented.

Identify and protect

Creating business continuity and disaster recovery plans are the final steps of a four-part process that most security teams go through to help ensure the security of an organization.

First, the security team identifies the assets that must be protected in the organization. Next, they determine what potential threats could negatively impact those assets. After the threats have been determined, the security team implements tools and processes to detect potential threats to assets. Lastly, the IT or appropriate business function creates the business continuity and disaster recovery plans. These plans are created in conjunction with one another. The plans help to minimize the impact of a security incident involving one of the organization's assets.

Business continuity plan

The impact of successful security attacks on an organization can be significant. Loss of profits and customers are two possible outcomes that organizations never want to happen. A **business continuity plan** is a document that outlines the procedures to sustain business operations during and after a significant disruption. It is created alongside a disaster recovery plan to minimize the damage of a successful security attack. Here are four essential steps for business continuity plans:

- **Conduct a business impact analysis.** The business impact analysis step focuses on the possible effects a disruption of business functions can have on an organization.
- **Identify, document, and implement steps to recover critical business functions and processes.** This step helps the business continuity team create actionable steps toward responding to a security event.
- **Organize a business continuity team.** This step brings various members of the organization together to help execute the business continuity plan, if it is needed. The members of this team are typically from the cybersecurity, IT, HR, communications, and operations departments.
- **Conduct training for the business continuity team**. The team considers different risk scenarios and prepares for security threats during these training exercises.

Disaster recovery plan

A **disaster recovery plan** allows an organization's security team to outline the steps needed to minimize the impact of a security incident, such as a successful ransomware attack that has stopped the manufacturing team from retrieving certain data. It also helps the security team resolve the security threat. A disaster recovery plan is typically created alongside a business continuity plan. Steps to create a disaster recovery plan should include:

- Implementing recovery strategies to restore software
- Implementing recovery strategies to restore hardware functionality
- Identifying applications and data that might be impacted after a security incident has taken place

Key takeaways

Disaster recovery and business continuity plans are important for an organization's security posture. It's essential that the security team has plans in place to keep the organization's business operations moving forward in case a security incident does occur.

Google

Juliana's story: Asset protection

Meet Juliana Soto, who recently completed an online cybersecurity certificate program and was hired as a cybersecurity analyst for Right-On-Time Payment Solutions, a fictional payment processing company allowing individuals to transfer money to friends and family. Right-On-Time also allows companies to accept payments from customers or organizations.

In this reading, you will begin a three-part journey that follows Juliana as she takes on new roles and responsibilities within the cybersecurity team of her new company.

Juliana decides that one of her first objectives is to gain a better understanding of the most important assets to the company by reviewing various company reading materials that will help her learn what is most valuable to them. On her first day, she is given reading materials to help her familiarize herself with the company. She learns that customers must create unique usernames and passwords and provide their full name or company name to sign up for the service as an individual. Business customers can also sign up for the service if they provide their employee identification number (EIN). Finally, customers must enter their bank account information or debit card number for payments to be accepted.

Juliana discovers that this company handles a lot of personally identifiable information (PII) from its customers. This kind of information is considered sensitive data. Unauthorized access to it can lead to significant damage to the organization's finances, its customers, and its reputation. Juliana realizes that the most important asset to this company is customer data.

After finishing the required onboarding materials, she decides to put together an information lifecycle strategy. She learned about this when completing her online cybersecurity certificate program.

Information lifecycle strategy

Juliana recalls the following steps of the information lifecycle:

- The first step in the information lifecycle is to identify the important assets to the company, including sensitive customer information such as PII, financial information, social security numbers, and EINs.
- The second step is to assess the security measures in place to protect the identified assets and review the company's information security policies. There are different components to this step, ranging from vulnerability scanning to reviewing processes and procedures that are already in place. Juliana is new to the company and might not be ready to conduct vulnerability scans.
- The third step of the information lifecycle is to protect the identified assets of the organization. Once again, this is only Juliana's first day on the job. She asks her supervisor if she can observe a more senior security analyst for a day. This will give her the opportunity to learn how the security team monitors the company's systems and network.
- The last step of the security lifecycle is to monitor the security processes that have been implemented to protect the organization's assets. She contacts her supervisor and gives them a detailed report of what she has learned on her first day. She requests to finish her day by monitoring a few of the systems that are in place. Her supervisor is impressed with her initiative and prepares Juliana to monitor the security systems. What a great first day for Juliana!

Google

Key takeaways

Identifying the important assets of a company is a key security analyst responsibility. Once you identify the assets, it can be helpful to follow the information lifecycle strategy to help ensure those assets are being protected effectively. Reviewing a company's security policies will also help an analyst understand what is important to the company and how the analyst should be protecting that data.

Google

Course 8 - module 2

Escalate with a purpose

You previously learned about security incident escalation and the skills needed to help you escalate incidents. In this reading, you'll learn the importance of escalating security issues and the potential impact of failing to escalate an issue.

Incident escalation

Security incident escalation is the process of identifying a potential security incident. During this process, potential incidents are transferred to a more experienced department or team member. As a security analyst, you'll be expected to recognize potential issues, such as when an employee excessively enters the wrong credentials to their account, and report it to the appropriate person. When you join a new organization, you'll learn about the specific processes and procedures for escalating incidents.

Notification of breaches

Many countries have breach notification laws, so it's important to familiarize yourself with the laws applicable in the area your company is operating in. Breach notification laws require companies and government entities to notify individuals of security breaches involving personally identifiable information (PII). PII includes personal identification numbers (e.g., Social Security numbers, driver's license numbers, etc.), medical records, addresses, and other sensitive customer information. As an entry-level security analyst, you'll need to be aware of various security laws, especially because they are regularly updated.

Low-level security issues

Low-level security issues are security risks that do not result in the exposure of PII. These issues can include the following and other risks:

- An employee having one failed login attempt on their account
- An employee downloading unapproved software onto their work laptop

These issues are not significant security challenges, but they must be investigated further in case they need to be escalated. An employee typing in a password two to three times might not be of concern. But if that employee types in a password 15 times within 30 minutes, there might be an issue that needs to be escalated. What if the multiple failed login attempts were a malicious actor attempting to compromise an employee's account? What if an employee downloads an internet game or software on their work laptop that is infected with malware? You previously learned that malware is software designed to harm devices or networks. If malware is downloaded onto an organization's network, it can lead to financial loss and even loss of reputation with the organization's customers. While low-level security issues are not considered significant security threats, they should still be investigated to ensure they result in minimal impact to the organization.

The escalation process

Every company has different protocols and procedures, including unique escalation policies. These policies detail who should be notified when a security alert is received and who should be contacted if the first responder is not available. The policy will also determine how someone should specifically escalate an incident, whether it's via the IT desk, an incident management tool, or direct communication between security team members.

Key takeaways

Incident escalation is essential for protecting an organization's data. Every organization might have a different way of escalating security incidents. A security analyst should be aware of the escalation protocols that are in place at their organization. Both small and large security issues should be escalated to the appropriate team or team member.

Recognize roles and responsibilities during escalation

You previously learned about various incident classification types and how those incidents can impact an organization.

This reading will discuss the roles of the various team members who are a part of the incident escalation process. Keep in mind that not all organizations are alike, and some roles and responsibilities may be identified using different terminology and definitions.

Data owners

A data owner is the person that decides who can access, edit, use, or destroy their information. Data owners have administrative control over specific information hardware or software and are accountable for the classification, protection, access, and use of company data. For example, consider a situation where an employee gains unauthorized access to software they do not need to use for work. This kind of security event would be escalated to the data owner of that software.

Data controllers

Data controllers determine the procedure and purpose for processing data. This role largely focuses on collecting the personal information of customers. The data controller determines how that data is used. The data controller also ensures that data is used, stored, and processed in accordance with relevant security and privacy regulations. If sensitive customer information was at risk, that event would be escalated to data controllers.

Data processors

Data processors report directly to the data controller and are responsible for processing the data on behalf of the data controller. The data processor is typically a vendor and is often tasked with installing security measures to help protect the data. Data processing issues are typically escalated to the individual who oversees the third-party organization responsible for data processing.

Data custodians

Data custodians assign and remove access to software or hardware. Custodians are responsible for implementing security controls for the data they are responsible for, granting and revoking access to that data, creating policies regarding how that data is stored and transmitted, advising on potential threats to that data, and monitoring the data. Data custodians are notified when data security controls need to be strengthened or have been compromised.

Data protection officers (DPOs)

Data protection officers are responsible for monitoring the internal compliance of an organization's data protection procedures. These individuals advise the security team on the obligations required by the organization's data protection standards and procedures. They also conduct assessments to determine whether or not the security measures in place are properly protecting the data as necessary. DPOs are notified when set standards or protocols have been violated.

Key takeaways

Incident escalation requires various members of a security team to act as one. Entry-level analysts should be familiar with the roles and responsibilities of different team members on the security team. As an entry-level analyst, you will typically escalate incidents to your direct supervisor. However, it's still important to have an understanding of the different team members as you move forward in your security career because it will help you recognize which incidents should be reported to whom.

Escalation timing

You previously learned about the potential impact even the smallest incident can have on an organization if the incident is not escalated properly. You also discovered just how important your role as an entry-level analyst will be to the effectiveness of an organization's escalation process.

This reading will go into more detail about the role you'll play in protecting an organization's data and assets when it comes to escalating incidents.

Your decisions matter

Security is a fast-paced environment with bad actors constantly trying to compromise an organization's systems and data. This means security analysts must be prepared to make daily decisions to help keep a company's data and systems safe. Entry-level security analysts help the security team escalate potential security incidents to the right team members. A big part of your role as a security analyst will be making decisions about which security events to escalate before they become major security incidents.

Trust your instincts and ask questions

Confidence is an important attribute for a security analyst to have, especially when it comes to the escalation process. The security team will depend on you to be confident in your decision-making. You should be intentional about learning the organization's escalation policy. This will help you gain confidence in making the right decisions when it comes to escalating security events. But remember to ask questions when necessary. It shows that you're committed to constantly learning the right way to do your job.

All security events are not equal

An important part of escalation is recognizing which assets and data are the most important for your organization. You can determine this information by reading through your onboarding materials, asking your supervisor directly about which assets and data are most important, and reviewing your company's security policies. When you have that type of understanding, it allows you to recognize when one incident should be given a higher priority over others. You previously learned about the following incident classification types:

- **Malware infections:** Occur when malicious software designed to disrupt a system infiltrates an organization's computers or network
- **Unauthorized access:** Occurs when an individual gains digital or physical access to a system, data, or application without permission
- **Improper usage:** Occurs when an employee of an organization violates the organization's acceptable use policies

Identifying a specific incident type allows you to properly prioritize and quickly escalate those incidents. Remember, an incident which directly impacts assets that are essential to business operations should always take priority over incidents that do not directly impact business operations. For example, an incident where unauthorized access has been gained to a manufacturing application should take priority over an incident where malware has infected a legacy system that does not impact business operations. As you gain experience in the cybersecurity field, you will learn how to quickly assess the priority levels of incident types.

Quick escalation tips

A big part of your role in cybersecurity will be determining when to escalate a security event. Here are a few tips to help with this:

- Familiarize yourself with the escalation policy of the organization you work for.
- Follow the policy at all times.
- Ask questions.

Key takeaways

Incident escalation will be an important part of your role within a security team. Entry-level analysts are expected to identify and escalate incidents related to their daily work. Reading and understanding your organization's escalation policy will be helpful in this responsibility. The escalation policy will describe how and to whom you should escalate incidents. When in doubt, never be afraid to ask a supervisor about the escalation process. This will help you stay knowledgeable about your job and make informed decisions.

Juliana's story: Attention to detail

This is the second reading in the scenario about Juliana Soto, a cybersecurity analyst who was recently hired by Right-On-Time Payment Solutions. In the reading about asset protection, Juliana identified important assets to her organization and came up with a plan for how to protect them. In this reading, you will review how Juliana used her company's escalation policy and her attention to detail to deal with security issues she encountered on the job.

Focus on the details

As she prepares to go into the office this morning, Juliana reflects on the previous day's accomplishments:

- Read through company information to learn about the most important assets she is tasked with protecting
- Learned that her company deals with PII data from customers
- Put together an information security lifecycle strategy for the organization's data
- Began monitoring security systems on her work laptop

It was an exciting first day full of new information for Juliana! She wonders what today will bring.

Juliana is at her desk monitoring data logs and responding to emails. Suddenly, her system alerts her of suspicious log activity. It appears that an employee's account has been locked due to 10 failed login attempts. She finds this concerning because the escalation policy states that 10 failed login attempts should be escalated to the password protection team.

Juliana is excited about her first chance to escalate a security event. As she prepares to go through the escalation process, she is suddenly alerted to another event that has happened. She clicks on the alert and learns that an unknown source has attempted to compromise a system that stores bank account information for the company's customers. She views this as a major concern. She recalls the importance of sensitive financial information from her previous security training. She learned the previous day that her company stores a large amount of sensitive customer data. Hundreds of customers will be impacted if a system storing this kind of important data is compromised.

Juliana decides that the unknown source attempting to compromise the system that stores the bank information of customers is the more urgent of the two events and needs to be handled immediately. She references the company's escalation policy to find the best way to handle the escalation process for this type of incident.

Juliana carefully follows the process outlined in the escalation policy, making sure to be attentive to all of the details in the process. This allows her to notify the appropriate team members of what has happened. She completes all the steps outlined in the escalation policy for an event dealing with customer PII.

Next, she decides to escalate the lower-priority event. Once again, she follows the company guidelines to escalate that event.

Juliana's supervisor is impressed with her initiative and ability to follow the escalation guidelines. Juliana is off to a great start in her security career!

Key takeaways

Attention to detail is important for an entry-level security analyst. It helps the analyst monitor data logs and effectively follow an escalation policy. It's also critical for the analyst to recognize what assets are most important to an organization. This helps the analyst prioritize how quickly certain incidents should be escalated.

Google

Course 8 - module 3

The purpose and impact of stakeholders

You previously learned about incident escalation and the various security incident classification types. You also learned about the impact these incidents can have on an organization's business operations.

This reading will explore the individuals who have a significant interest in those business operations: stakeholders.

Who are stakeholders?

A **stakeholder** is defined as an individual or group that has an interest in any decision or activity of an organization. A big part of what you'll do as a security analyst is report your findings to various security stakeholders.

Levels of stakeholders

There are many levels of stakeholders within larger organizations. As an entry-level analyst, you might only communicate directly with a few of them. Although you might not communicate with all of the security stakeholders in an organization, it's important to have an understanding of who key stakeholders are:

- A Chief Information Security Officer, also known as the CISO, is the highest level of security stakeholder. You are unlikely to communicate directly with this stakeholder as an entry-level analyst.
- A Chief Financial Officer, also known as the CFO, is another high-level stakeholder that you're unlikely to communicate with directly.
- An operations manager oversees the day-to-day security operations. These individuals lead teams related to the development and implementation of security strategies that protect an organization from cyber threats.
- A cybersecurity risk manager is a professional responsible for leading efforts to identify, assess, and mitigate security risks within an organization.

CFOs and CISOs are focused on the big picture, like the potential financial burden of a security incident, whereas other roles like operations managers are more focused on the impact on day-to-day operations. Although you will rarely interact directly with high-level security stakeholders, it's still important to recognize their relevance.

Stakeholder communications for entry-level analysts

Two examples of security stakeholders with whom you might regularly communicate are operations managers and risk managers. When you report to these stakeholders, you'll need to clearly communicate the current security issue and its possible causes. The operations managers will then determine next steps and coordinate other team members to remediate or resolve the issue.

For example, you might report multiple failed login attempts by an employee to your operations manager. This stakeholder might contact the employee's supervisor to ensure the occurrence is a genuine issue of entering the wrong password or determine if the account has been compromised. The stakeholder and supervisor might also need to discuss the consequences for day-to-day operations if genuine failed login attempts can lead to account lockouts that might impact business operations. As an entry-level security analyst, you might play a role in implementing preventative measures once next steps have been determined.

From one stakeholder to the next

Operations managers and risk managers are stakeholders who rely on entry-level analysts and other team members to keep them informed of security events in day-to-day operations. These stakeholders commonly report back to the CISOs and CFOs to give a broader narrative of the organization's overall security picture. Although you won't regularly communicate with high-level stakeholders, it's important to recognize that your efforts still reach the highest levels of security stakeholders in the organization. These other members of your team keep those top-level stakeholders informed on the security measures and protocols in place that are continuously helping to protect the organization.

Key takeaways

Stakeholders play a major role in ensuring the security of an organization. Entry-level analysts should have a foundational understanding of the different levels of security stakeholders within an organization. Entry-level analysts will not communicate with every security stakeholder in a company, but there are certain stakeholders that the analyst will need to provide updates to. Those updates will eventually be reported up to the more senior-level stakeholders, such as the CISO and the CFO.

Communicate effectively with stakeholders

You previously learned about security stakeholders and their significance in an organization. In this reading, you'll learn the importance of clearly communicating to stakeholders to ensure they have a thorough understanding of the information you're sharing and why it's meaningful to the organization.

Get to the point

Security stakeholders have roles and responsibilities that are time sensitive and impact the business. It's important that any communications they receive, and the actions they need to take, are clear. To get to the point in your communications, ask yourself:

- What do I want this person to know?
- Why is it important for them to know it?
- When do they need to take action?
- How do I explain the situation in a nontechnical manner?

Follow the protocols

When you first join a security team, you'll want to learn about the different protocols and procedures in place for communicating with stakeholders and other members of the organization. It's important to make sure you know what applications and forms of communications are acceptable before you begin communicating with stakeholders, such as in-person meetings, video-conferencing, emails, or company chat applications.

Communicate with impact

You previously learned about the different stakeholders within an organization and what specific areas they're focused on. When you first begin your career in the cybersecurity field, you're more likely to interact with lower-level stakeholders, like operations managers or security risk managers, who are interested in the day-to-day operations, such as logging. Senior-level stakeholders might be more interested in the underlying risks, such as the potential financial burden of a security incident—as opposed to the details around logs.

When you communicate with an operations manager, make sure you address relevant information that relates to their daily responsibilities, such as anomalies in data logs that you are escalating. Concentrating on a manager's daily responsibilities will help you communicate the need-to-know information to that individual.

Communication methods

Your method of communication will vary, depending on the type of information you're sharing. Knowing which communication channels are appropriate for different scenarios is a great skill to help you communicate effectively with stakeholders. Here are a few ways you might choose to communicate:

- Instant messaging
- Emailing
- Video calling
- Phone calls
- Sharing a spreadsheet of data
- Sharing a slideshow presentation

If your message is straightforward, an instant message or phone call might be the route to take. If you have to describe a complex situation with multiple layers, an email or in-person meeting might be the better option. If you're providing a lot of data and numbers, sharing a graph might be the best solution. Each situation helps you determine the best means of communication.

Key takeaways

Stakeholders are busy people who have very specific interests within the organization. Therefore, it's important to only communicate information that is specific to their interests and impacts their role in the company.

Be mindful of the kind of information you're communicating because that will help determine what method of communication you should use.

Create visual dashboards for impactful cybersecurity communications

You previously learned about security stakeholders, the people responsible for protecting the data and systems of various departments of an organization. An entry-level analyst might communicate directly or indirectly with these individuals. If you do end up communicating with a stakeholder, it's important to use the right method of communication. This reading will further elaborate on the significance of using visual dashboards to communicate information to stakeholders. Dashboards can include charts, graphs, and even infographics. You'll learn more about when to use visual communication strategies in this reading.

Using visuals to communicate effectively

Security is about protecting a company from threats that can affect its reputation and finances. Oftentimes, responding to threats quickly and effectively depends on clear communications between the stakeholders who are involved.

In the cybersecurity field, the stakeholders you'll deal with will often be busy with other responsibilities. Showing them important information visually is a great way to gain their input and support to address security challenges that arise. Visuals help provide these decision-makers with actionable information that can help them identify potential risks to the organization's security posture.

Visual dashboards

A **visual dashboard** is a way of displaying various types of data quickly in one place. Visual dashboards are useful tools that can be used to communicate stories to stakeholders about security events—especially when they involve numbers and data.

Dashboards can be simple or complex depending on the information you're communicating. A simple dashboard might contain a single chart, while a complex one can include multiple detailed charts, graphs, and tables. Deciding which type to use will depend on the situation and story you are telling. However, attention to detail and accurately representing information is important anytime you're communicating data to stakeholders.

Pro tip: Programs like Google Sheets and Apache OpenOffice are tools that can be used to create visual dashboards.

When to use visual communication

Security is often a team effort. Everyone must work together to ensure an organization is properly protected from bad actors. Knowing how to communicate with your colleagues is a big part of the team-focused aspect.

Sometimes it's enough to send a simple email update. Other times you might want to include a document attachment that further elaborates on a specific topic. A simple phone call can also be valuable because it allows you to quickly communicate the necessary information without having to wait for a response to an email or message. Other times, the best way to communicate is through visuals.

For example, consider a situation where your supervisor has asked you to provide them with results from a recent internal audit of five different departments within the organization. The audit gathered data showing how many phishing emails each department clicked over the last five months. This is an ideal opportunity to tell this story using visualization tools. Instead of sending an email that simply describes what the findings are, a graph or chart will clearly illustrate those findings, making them easier for the stakeholder to understand quickly and easily.

Key takeaways

Stakeholders, like the rest of the security team, are busy. With that in mind, be clear and concise any time you communicate with them. This makes everyone's job easier! It's important to recognize when visual dashboards are the most effective communication method. A visual dashboard is often best to use when you're communicating information that involves numbers and data.

Juliana's story: Effective communication

Throughout this course, you've been following the story of Juliana Soto. Juliana was recently hired as a cybersecurity analyst by Right-On-Time Payment Solutions, a payment processing company that handles sensitive customer information. In the reading about attention to detail, Juliana had to deal with two different types of security incidents, and she used her company's escalation policy to properly escalate the two incidents. Now you will review how Juliana handled communication with stakeholders after escalating the incidents.

Communicating with stakeholders after an incident

Days after escalating the two incidents, Juliana's manager asks her to communicate information about the incidents to stakeholders.

Communicating about incident #1

One of the incidents dealt with an employee being locked out of their account due to multiple failed login attempts. Juliana's manager was recently asked to provide a report that reviews how many departments have experienced locked employee accounts due to failed login attempts over the last month. The security team shared data that details the number of locked employee accounts due to multiple failed login attempts from five different departments.

Juliana's manager will report the information to the senior executives of each of the five departments. The manager asks Juliana to display the data in a way that communicates the incident clearly to these stakeholders. For this task, Juliana decides to put together a visual dashboard to represent the data because the communication is primarily focused on numbers. Her dashboard will use charts and graphs to relay important information, like the number of employees who have been locked out of their accounts in the last month. Juliana's visual dashboard makes it easier for the high-level stakeholders to review incident #1 and determine a course of action.

Communicating about incident #2

Juliana's manager has also been informed that the Chief Information Security Officer (CISO) wants more information about what took place during the second incident, which involved an attacker almost compromising a system that stores customers' private data. This communication will include a more detailed report that establishes what processes and procedures worked well during attackers' attempts to compromise the system and what processes and procedures might need to be revised. Because this is a more detailed communication, Juliana decides to put together a detailed document with timelines that clearly explain what happened. The document also includes her thoughts on what the security team, data owners, and data processors could have done differently to protect the system in question. She shares the report with her manager so they can review it.

Key takeaways

Communications for stakeholders should always be focused on what matters to them most. Some stakeholders will be more focused on the data and numbers, and other stakeholders will be more focused on how policies and procedures are working to prevent cyber attacks. Recognizing what's important to each stakeholder will help an analyst decide what method of communication is best to use.

Google

Course 8 - module 4

Strategies for engaging with the cybersecurity community

You have learned a lot about the security field, from the origins of security and its importance to organizations around the world to recognizing security incidents and communicating with stakeholders.

Security is a rapidly evolving industry, so it's important to stay up-to-date on the latest news and trends. This reading will focus on how to stay engaged with the cybersecurity community after completing this program.

Security organizations and conferences

Attending security conferences and joining organizations gives you the opportunity to gain knowledge from seasoned professionals who are constantly seeking out new ways to improve on their security strategies and techniques.

Find the right organization

What security organization should you join? This question depends on your specific interest in security. Are you someone who wants to focus on reacting to security incidents or preventing them from happening? Are you interested in forensic security or data logging? Do you have aspirations of being a CISO one day? It's important to have a clear understanding of what your interests are before you narrow down your search for a cybersecurity organization or conference.

Begin the search

Once you understand what your interests are, do a web search for organizations or conferences in your area. For example, you can type in "incident response cybersecurity conferences in my area." This search will give you a list of cybersecurity conferences focused on incident response. If you're interested in forensic security, you can type "forensic security organizations in my area" or a similar phrase into your web search engine. No matter what your interests are, you can do a web search online to find a cybersecurity organization or conference focused on that area.

Use social media

Social media is another great way to find cybersecurity organizations or conferences. LinkedIn®, for example, is a social media platform that connects business professionals with one another. You can use LinkedIn® to find security groups or organizations to join. In the LinkedIn® search bar, you can try search queries such as:

- "Incident response cybersecurity groups"
- "Organizations for cybersecurity analysts"

Be aware of social engineering

While social media is a good way to connect with other professionals in the security industry, it's also important to be mindful that hackers use social media to trick users into giving up private information. You've previously learned that social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. To protect yourself from social engineering when using social media to find resources, always remember not to click on unexpected links or attachments sent from unfamiliar users on social media.

Mailing lists for security

Another great way to stay connected with the security industry is to sign up for different cybersecurity mailing lists. These mailing lists send out information periodically on various security topics. The Cybersecurity & Infrastructure Security Agency (CISA) offers two cybersecurity mailing lists for you to join:

- A list focused on security threat information, best practices for cybersecurity, and analysis from CISA's domestic and international security partners
- A list providing weekly summaries of new vulnerabilities that might pose a risk to an organization's network

Key takeaways

Attackers are always developing new ways to compromise corporate and personal data from users. Cybersecurity organizations and conferences are a great way for security professionals to stay up-to-date on the latest news, tools, and trends in the industry. Be sure to find organizations that align with your security interests.

Connect with other cybersecurity professionals

You've learned the importance of staying engaged with the cybersecurity community after completing this certificate program. The security industry is always evolving, so it's important that security professionals continue to learn about the field.

This reading will focus on providing more tips to help you stay engaged with the security community and advance your career by engaging with the cybersecurity community.

LinkedIn® with CISOs

Earlier in the program, you learned about Chief Information Security Officers, also known as CISOs. It's their job to be up-to-date on every aspect of security, including all of the latest trends and news in the security world. With this in mind, it's a great idea to follow CISOs on LinkedIn® professional networking services. When you follow a CISO on social media, you'll have an opportunity to discover the kinds of information they share with their audience. That information might provide you with useful tips and relevant news. Staying informed about security news and trends can help progress your cybersecurity career because it helps sharpen your security mindset.

Finding other security professionals on LinkedIn®

Whether you'd like to connect with other entry-level analysts or more seasoned professionals, LinkedIn® is a great way to connect with others. When connecting with others, it's important to send a well-written message. This message can help the person understand your intentions. It also helps people determine that you're not a scammer looking to exploit them. Here are a few tips to help you write your first message in a way that engages and interests the recipient:

- Use a conversational tone.
- Provide a clear reason for wanting to connect.
- Avoid spelling and grammatical errors.

Here is an example of an effective LinkedIn® message to send to a security professional:

"Hi, Tim. I recently completed the Google Cybersecurity Certificate program, and I'd like to connect with other security professionals. It seems like you have a lot of experience in the security industry that I can learn from. Let's keep in touch!"

This example provides a clear reason for why you want to connect with this person and is presented in a conversational tone. You also did not give the impression that you are a scammer by asking the person to do something suspicious to connect with you, like downloading an unusual file attachment.

Key takeaways

Attackers are always developing new ways to compromise corporate and personal data. Connecting with other cybersecurity professionals on social media is a great way to stay ahead of the latest trends in security. CISOs are great professionals to connect with because they are responsible for all aspects of an organization's security. Because of that, CISOs tend to share important security tips, news, and trends on their social media pages that could be valuable to you as a newcomer to the industry.

Google

Course 8 - module 5

Tips for finding and applying for a job

As you learned previously, connecting with security professionals on social media and joining different cybersecurity conferences and organizations are two ways to use your network to find job opportunities. You were also introduced to a few online resources to help you find jobs in the security field. In this reading, you'll learn about specific sites and resources you can use to apply for jobs.

ZipRecruiter

ZipRecruiter is a popular website for job seekers and employers worldwide; the website helps connect job seekers with available roles in their industry. When you enter the site, you're asked to fill out specific geographical and work preference questions to help ZipRecruiter match you with opportunities in your field. Then you can upload your resume on the platform and search for jobs in your industry. Employers can reach out to you directly, too, based on your profile and responses.

Indeed

Indeed is another popular website that helps connect job seekers with available roles in their industry. When you first enter the site, search for jobs using the job title, a keyword, or a company that you're interested in working at. Then, specify your preferred job location. You can also upload your resume on Indeed, which allows recruiters to reach out to you if your resume is a match for a job opportunity.

Monster®

Monster is a frequently used website in both the United States and internationally that helps connect job seekers with available roles in their industry. Similar to the other job search sites, search for a role using the job title, keyword, or company you're interested in working at, as well as your preferred working location. If you upload your resume to Monster, recruiters might reach out to you if your resume is a match for a job opportunity.

LinkedIn®

LinkedIn® professional services is a social networking site where you can also find jobs in the cybersecurity field. When you first enter LinkedIn®, click on the "jobs" tab. From here, enter the location where you'd want to work and the particular job title that you'd be interested in. LinkedIn is also a great way to learn about a company's culture, values, and even community initiatives. This can help you determine if the company is the right fit for you.

Key takeaways

Building a network of security professionals, viewing and applying for jobs on various sites, and using professional networking applications like LinkedIn are great ways to find a job in the cybersecurity profession. So, use all of these resources to your advantage!

The interview process

You previously learned how to create a resume and cover letter to apply for security jobs. In this reading, you'll concentrate on how to prepare for the interview process. Although the interview process can vary widely from one company to another, most companies follow the steps described in this reading.

Getting contacted by a recruiter

After you apply for a job, you might receive a call, an email, or a message from a recruiter expressing interest in your application and asking to schedule a call or meeting. Reply as soon as possible to show that you're responsive and interested in the position.

Preliminary interview or phone screening

In most cases, the first step in the interview process is a preliminary interview, sometimes referred to as a phone screening. This usually involves a conversation with a recruiter over the phone, in person, or on a video call.

The preliminary interview is typically shorter than a regular interview. The recruiter will share information about the company and the job opening. Then they'll ask you questions to get to know you and your work experience better. The recruiter will also provide time for you to ask questions about the role and the company, so be sure to prepare a few questions before the interview. For example, you might ask: "What is the work culture like at the company?" or "What will my average day be like in this role?" Asking questions helps demonstrate your interest and will help you determine whether the job will be a good fit for you.

After the interview, send a thank-you email to the recruiter within 24 hours. Express your gratitude for their time and briefly restate why you would be a good fit for the position.

Additional interviews

Once you've passed the preliminary interview, you might be invited for multiple additional interviews. These interviews are typically with the hiring manager. You might also meet with other individuals on the team and be required to go through a technical interview. You'll learn more about technical interviews in a later reading.

This interview is often longer than the preliminary interview. It could be in person, over the phone, or on a video call.

The interview usually opens with introductions and a brief description of the company and job position. Then, the interviewer will ask you questions about your background, skills, and experience. Next, you'll have an opportunity to ask questions about the company, the role, and job expectations.

Finally, you'll learn about next steps in the hiring process.

There might be multiple rounds of interviews, depending on how the company's interview process works. These additional interviews could be longer, include future teammates or other employees at the company, and feature questions that take more time and thought to answer.

As with the preliminary interview, send a thank-you note to the people you interviewed with after each round of interviews.

Final offer

Now comes the exciting part: Receiving a job offer. The company might reach out to you by phone or email. After the company extends their initial offer, you'll need to decide whether or not to accept it or negotiate for a higher salary or other benefits. Feel free to ask for a day or two to make your decision.

Building perseverance

If the company lets you know that you didn't get the job, take a moment to process your emotions. If you'd like, you can let the company know that you appreciate the opportunity to be considered and that you'd be interested in any future roles that might be a good fit. You can also ask for feedback on what you could do better next time.

Key takeaways

Interviews are a great opportunity to learn more about a job and the company you'd be working for. By preparing for the interview process and continuing to persevere in your job search, you'll be well on your way to building a career in cybersecurity.

Prepare for technical interviews

You previously learned about the interview process, which generally consists of an introductory interview, a second interview with a hiring manager, and a panel interview. In this reading, you'll focus more on the technical interviews that take place during the interview process. Although technical interviews can vary from one company to another, the concepts covered in this reading will help prepare you for any technical interview.

What are technical interviews?

After you've applied for a job in cybersecurity and receive interest from a recruiter, you might be invited to an introductory interview, a second interview with a hiring manager, and a panel interview. Additionally, you might be asked to participate in a technical interview. The main difference between technical interviews and other interviews is the focus on required knowledge of specific tools.

Python

Python is a programming language that serves as an important tool in security, and you might be asked about it during a technical interview. It will be important to mention your basic knowledge of Python. You might recall from this program that Python is popular for its ease of use as well as its extensive libraries and integrations. It can be applied to various security tasks that require automation. During your interview, you might be asked to whiteboard a pseudo code in Python. Being able to confidently use Python terminology during an interview can help you stand out as a potential candidate. This will let the interviewer know that you have a solid understanding of what Python is and what it can be used for.

General techniques

During your technical interview, you might be expected to demonstrate basic knowledge of various general security concepts. For example, you might need to show familiarity with **security frameworks**, which are guidelines used for building plans to help mitigate risk and threats to data and privacy. When discussing security frameworks, it would be helpful to mention your knowledge of specific NIST frameworks, such as the Cybersecurity Framework (CSF). Another technical concept for you to discuss during a technical interview is network security. You might recall that **network security** is the practice of keeping an organization's network infrastructure secure from unauthorized access. Reviewing the different technical concepts you've learned throughout this program is a good way to prepare for a technical interview. It will sharpen your skills and help you leave a good impression on the interviewer.

Additionally, it may be a good idea to write the entire question down on paper before answering. Often, technical interview questions have multiple parts to cover. People sometimes rush to give an answer and show their knowledge but not fully cover everything that the question asks. Writing down the question can help you ensure you have the question right and are able to provide a structured response.

Possible technical interview questions

Every technical interview will be different, depending on the company and the interviewers. But here are a few possible technical interview questions to help you prepare:

- What is the TCP/IP model?

  The TCP/IP model is a framework used to visualize how data is organized and transmitted across a network.

- What is the OSI model?

  The OSI model stands for open systems interconnection (OSI) model. It is a standardized concept that describes the seven layers computers use to communicate and send data over the network.

- What are SIEM tools and what are they used for?

  SIEM tools are security information and event management tools that are used by security professionals to identify and analyze security threats, risks, and vulnerabilities.

Key takeaways

Technical interviews are a great opportunity to show your potential employer your technical cybersecurity skills, such as coding, during the interview. Even if you have no prior security experience, you can take this time to share what you've learned in the Google Cybersecurity Certificate program and express your excitement to put that learning into action. By preparing for the technical interview process, you'll be well on your way to building a career in cybersecurity.

Google

Apply the STAR method during interviews

You've been learning about different techniques and strategies to use during future interviews for jobs in the cybersecurity field. In this reading, you'll learn more details about the STAR method for answering interview questions. Implementing this strategy will help you answer interview questions with confidence and clarity.

The STAR method

When interviewing for a job, it can be challenging to convey the right details about your professional history and skills to your interviewers. Using the STAR method can help you share your success stories effectively and strategically. STAR stands for Situation, Task, Action, and Result. Using this method enables you to describe potential challenges you faced in previous roles and gives you the opportunity to show how you thoughtfully approached solving those problems from start to finish.

Situation

The **situation** is the project you worked on or a challenge that you had to overcome. For example, perhaps you had to manage a disgruntled customer's negative feedback about your company, a system error on your work device that slowed down a customer transaction, or being left alone in the office for an extended period of time. Fully describing the situation allows the interviewer to gain a clear understanding of the challenge you had to overcome.

Task

The **task** outlines the key responsibilities or role you played in solving the challenge described in the situation phase of the STAR method. Specifying what the task is provides clarity about what your objectives were in this scenario.

Action

The **action** describes the exact steps you took to resolve the challenging situation you described in the beginning of the STAR method. The action is crucial to the STAR method because it allows the employer to understand what choices you made to achieve your desired outcome during a real conflict or challenge. Employers want employees who can think fast and make decisions that help solve problems.

Result

Finally, sharing the **result** of your challenge or example shows the employers how the situation was resolved as a direct result of the actions you took. When participating in an interview, you want to make sure that any example you give with the STAR method ends in a positive result. Positive results show an employer that you are someone who has demonstrated an ability to successfully resolve issues and may lead an employer to offer you a job. Of course, not all situations have completely positive outcomes; if an employer asks you about a situation that didn't have a positive outcome, try to focus on what you learned from the situation and how that experience helped you become a better employee.

Key takeaways

The STAR method stands for Situation, Task, Action, and Result. Following this method helps you communicate to an employer an example of a challenge you faced in the workplace. Remember to use one of your success stories when using the STAR method on an interview. Challenges arise all the time in the security world, so being able to demonstrate an ability to overcome any type of challenge is a great trait to show off during an interview. Plus, since cybersecurity is such a team-driven industry, being able to communicate effectively to an interviewer will help you be a competitive applicant.

Prepare for interviews

Great news! You've submitted your application and received a follow-up email requesting an interview. The work isn't over yet, though—you still have a lot of preparation to do. That's what you're going to learn about in this reading!

Prepare for the introductory call

It's important to showcase your best self in the introductory phone call. In this conversation, you'll talk with the recruiter or hiring manager about yourself, the kind of work or training you have, and why you want the job. You might also be asked specifically about your salary requirements. For this question, it's a good idea to prepare in advance and conduct an internet search for "average salary for entry-level security analysts."

Do your research

Make sure you've done your research on the company. When the interviewer asks why you'd be a good fit for the job, they want to learn why you're interested in cybersecurity and why you want to work at that company specifically.

Prepare for the second round

Your second-round interview will focus more on what you can offer as an entry-level security analyst. You'll likely discuss yourself here, too, but you'll also be going into detail about your knowledge of the profession. You'll want to cover the same material you prepared for your introductory call, but you'll also need to fully review your accomplishments in the security industry. Don't worry if you have no prior professional cybersecurity experience. You can discuss the information you've learned in this certificate program.

Depending on where you and your interviewer are located, the second-round interview might be over the phone, via video conference, or in person. In-person interviews often last an hour or so, but if you traveled for your interview or the company likes to bring candidates in for all of the remaining interview stages at once, you might complete your panel interview with a group that day as well.

Panel interview

During the panel interview, you'll meet with two or more people and discuss yourself and your ability to contribute to the organization. If you're nervous about this, remind yourself that the team brought you in for the interview for a reason. When you feel confident in your abilities, you're better able to showcase your knowledge about the security industry and demonstrate your ability to work well with a team.

Be sure to engage with each panelist by giving them your full attention during the interview. Maintaining eye contact can help you express confidence, but for those who cannot do so, actively engaging with each panelist in your own way is just as important.

It's likely that each panelist will ask you at least one question during the interview. It's okay to address the whole panel when answering a question, rather than only directing your response to the person who asked the question.

More resources to help you prepare

There's an endless supply of job-preparation resources available to you. Here are some great ones to get you started:

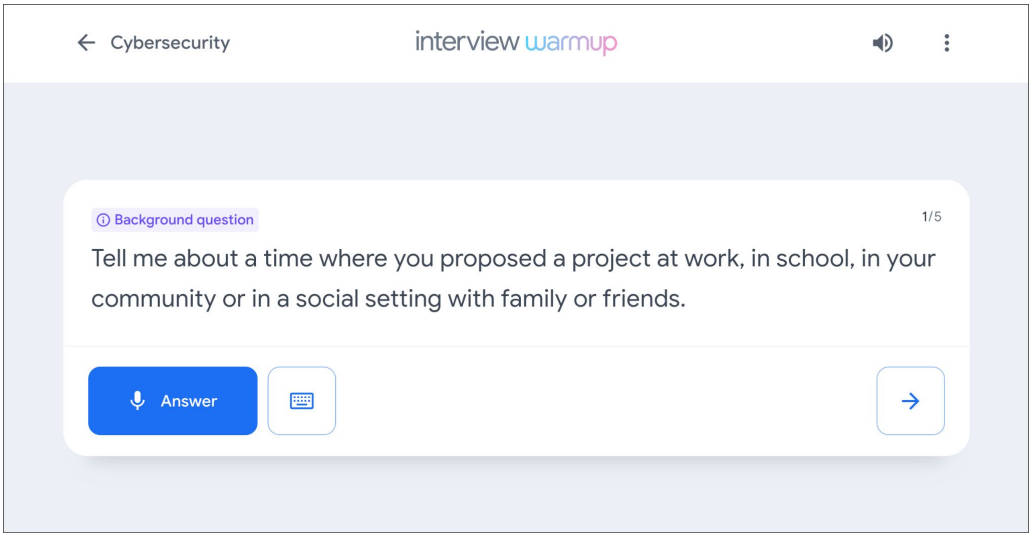
- Interview tips from Google. This resource from the Google Careers team provides best practices and advice on how to prepare and ace your interviews at Google, but of course these tips will work at any company!
- Interviewing techniques for persons with disabilities. This resource from the Job Accommodation Network (JAN) offers helpful advice on navigating the interview process for individuals with disabilities.

Key takeaways

Preparation for your first interview is very important, so be sure to do your research and practice for the introductory call. Don't worry if you don't have prior security experience. Instead, you can rely on the information and skill sets you've gained from completing this certificate program.

Prepare for interviews with Interview Warmup

Now that you have developed new skills and knowledge in cybersecurity, it's time to start preparing for interviews. Interview Warmup is a tool that helps you practice answering questions to become more confident and comfortable throughout the interview process.



Get started

Follow these steps to start a five-question practice interview related to cybersecurity:

1. Go to grow.google/interview-warmup.
2. Click **Start practicing**.
3. Select **Cybersecurity** to open an additional menu.
4. Click **Start**.

The interview lasts about 10 minutes, and the questions will vary with each attempt. During each interview session, you will be asked two background questions, one behavioral question, and two technical questions. You are encouraged to try as many practice interviews as you want.

You can also review complete lists of cybersecurity interview questions or general interview questions if you'd like to focus on a particular topic.

How it works

Interview Warmup asks you interview questions to practice answering verbally. Your answers will be transcribed in real time, allowing you to review how you responded. In addition, Interview Warmup's machine learning algorithm can detect insights that can help you learn more about your answers and improve the way you communicate.

Here are a few examples of questions Interview Warmup might ask:

- What are your career goals for the next five years?
- What processes can you use to ensure user data is protected?
- Name two types of common cybersecurity attacks?
- What are two internal factors that can increase the chances of security risks?
- What do security information and event management tools enable security analysts to do?
- In Python, what's the difference between break and continue?

Here are some of the insights that Interview Warmup provides:

- **Talking points:** The tool lets you know which topics you covered in your answer, such as your experience, skills, and goals. You'll also be able to view other topics that you might want to consider covering.
- **Most-used words:** The tool highlights the words you used most often and suggests synonyms to broaden your word choices.
- **Job-related terms:** The tool highlights the words you used that are related to the role or industry in which you are preparing to work. You'll also be able to view an entire list of job-related terms that you might want to consider including in your answer.

Interview Warmup gives you the space to practice and prepare for interviews on your own. Your responses will be visible only to you, and they won't be graded or judged.

Key takeaways

Practicing for interviews is an important skill for your career in cybersecurity. Using Interview Warmup can help you practice interview questions and receive feedback in real time. As you practice, you will gain confidence and be able to prepare more polished responses for common interview questions.

Learn more about developing an elevator pitch

When interviewing with potential employers, it's important to communicate who you are, your value as a security professional, and what qualities you're searching for in a potential job. A simple way to deliver this information succinctly is with an elevator pitch. An **elevator pitch** is a brief summary of your experience, skills, and background that should be communicated in 60 seconds or fewer.

Although an elevator pitch is often specific to an idea or a product, you can also use it to sell yourself as a professional to potential employers. In an interview, a strong elevator pitch can be used to stand out to your interviewer. It can be used to help explain why you're a good fit for the role or to answer the popular interview question "tell me about yourself." This reading helps you prepare your elevator pitch to express the value you can provide as an entry-level security analyst or a more experienced cybersecurity professional.

Provide an introduction

Start by providing an introduction. Introduce yourself and give a brief overview of your professional background. Explain some job roles you've had, your years of work experience, and the types of industries you've worked in. If this is your first job in security, mention some of your past roles and skills used for those roles that can translate to success in the security field. Some of these skills can include attention to detail, goal-orientedness, and good collaboration skills.

Describe your career interests and transferable skills

Even if you're interviewing for your first internship or job in security, it's important to clarify that this is your desired career. For example, you could say, "I want to apply my excellent skills for collaborating with others, and my attention to detail, to help the security team protect company data and assets." To determine which transferable skills to highlight in your elevator pitch, consider ones that you have already developed and how they might apply to your goals as a security professional, such as problem-solving, communication, and time management.

Express your excitement

This is where you share your passion for the field and why you want to work in the industry. If you're motivated to help an organization defend itself against hackers, mention that. This is also a good time to talk about your goals.

For example, you could say, "I love security because it gives me the opportunity to safeguard valuable information from malicious actors attempting to cause unnecessary harm to people and organizations. Long term, I'd love to develop a security and hacker mindset to play my part in defending against the constantly evolving threat actor tactics and techniques."

Communicate your interest in the company

Communicating why you are interested in the company—and not just the role—is a great way to help the interviewer recognize that you are knowledgeable about the company. This helps you to establish a rapport with the interviewer and shows that you've done your due diligence before coming to the interview.

For example, if you were interviewing for a position for Google's security team, you could say, "Being a member of Google's security team helps protect millions of people's private and sensitive information. As a long-time Google products user, I'm looking forward to the opportunity to be able to help safeguard those products and ensure customers have the best experience possible."

Key takeaways

Creating an elevator pitch that's 60 seconds or fewer is a great tool to use to quickly share who you are. Use an elevator pitch to introduce yourself to career and business connections in the future. You can even use your elevator pitch in other types of situations, like meeting new friends or colleagues.

Tips for interviewing remotely

A remote interview is an interview conducted virtually using video platform software. This type of interview provides an opportunity to connect with hiring managers and recruiters, even if you are not able to meet with them in person. Remote interviews also present challenges that in-person interviews do not, such as issues related to technology, lighting, and sound.

In this reading, you will learn tips to successfully prepare for a remote interview.

Test your technology

The first tip is to test the technology you'll be using for the video. Different companies use different video platform software to host their remote interviews. Typically, the recruiter or hiring manager will reach out to you over the phone or email to share information about which software will be used for the interview.

Once you find out which software the company you're interviewing with uses, you should download that software, if you don't have it already. Next, it's important to test your computer's camera and microphone to ensure they work well with the video platform software a day or two before the interview. This allows you to resolve any technical issues you might have. Be mindful of how to mute and unmute your microphone, just in case there is noise in your environment that you do not want the interviewer to hear. It's also important to talk with the recruiter or hiring manager about a backup plan if the technology does not cooperate when it's time for the interview.

You'll also want to test any technologies you need to use to ensure you are ready to interview, such as the closed caption feature on the app. Employers are typically happy to accommodate your needs if you're using assistive technology or need specific accommodations. If your internet service is not fast enough to allow for a video interview, you can request a phone interview instead.

Practice communicating through video

Communicating through video can be a challenge because there is a slight sound delay. The sound delay can make it difficult to know how long to wait for someone to stop speaking and for you to start. If you don't have experience communicating through video, consider practicing with friends and family before the remote interview. This will help you learn how pauses affect video communication.

Create a professional background

Review your video background before the interview. Typically, you should avoid having an unorganized background or any objects that might distract the interviewer. When interviewing remotely, ensure that your area is well lit. You might want to rearrange your desk or furniture to ensure good lighting.

Always try to have light behind your camera so that it will shine on your face. If you can't position your desk next to a window or don't have enough light coming from the window, consider using artificial light.

Additionally, you should do your best to limit background noise and use a headset, if possible.

Dress appropriately

It's a good idea to research the company you're interviewing with to determine which type of interview outfit is suitable. You might need to wear formal business attire during your remote interview for a particular role and company, whereas for another position, more casual clothing might be appropriate. Typically, it is better to overdress than to underdress, especially for more traditional businesses.

Look at the interviewer when speaking

When communicating through video, try to look at the interviewer when speaking instead of at the camera. Looking at the interviewer can give them the feeling that you're engaged in the conversation and focused on what they're saying.

Sign in early

Before the interview, test your technology. This will help you feel confident that everything will work. However, technology and software can be unpredictable. If possible, sign in to your remote interview early to ensure everything is working properly.

Signing in early also indicates to your interviewer that you respect their time and are a punctual person.

Key takeaways

Follow the tips in this reading to become more confident with the remote interviewing process. Always test your technology before the interview to ensure it works well with the video platform software being used for the interview.

Showcase your work

Congratulations on earning your Google Cybersecurity Certificate! Now it's time to let the world know about the skills you've gained to help advance your career. We recommend adding the completion of this certificate program to your resume and LinkedIn® profile. Read on and follow these tips to get started.

Add the Google Cybersecurity Certificate to your resume and LinkedIn® profile

You may have already started on a cybersecurity resume earlier in the program. If not, there are a variety of digital templates for creating your resume available at Enhancv, Big Interview, Google Docs, or Microsoft Word. You can find additional resume creation guidance in this lesson from Google Applied Digital Skills: Start a Resume.

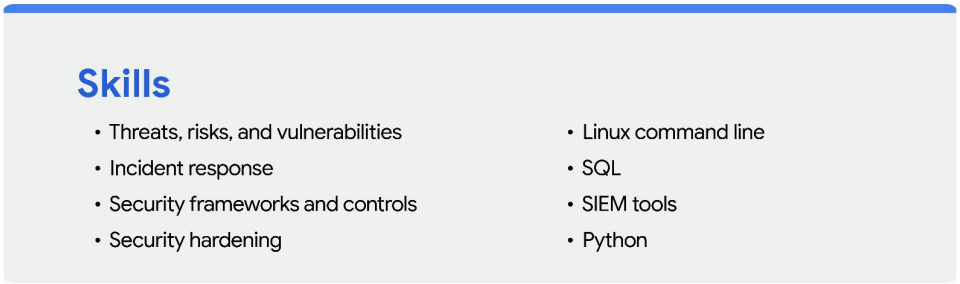
Update your Education or Licenses and Certifications section

- To add the completion of this certificate to your resume, update your ***Education*** or ***Licenses & Certifications*** section.
- To add the completion of this certificate to the ***Licenses & Certifications*** section of your LinkedIn® profile, follow the steps listed in this LinkedIn® Help article.

Update your Skills section

If applicable, update the ***Skills*** section of your resume. Following is a comprehensive list of skills that this certificate was designed to help you develop that you could potentially add.

To update the ***Skills & Endorsements*** section of your LinkedIn® profile, follow the steps listed in this LinkedIn® Help article.



Update your Summary or About section

- If your resume has a ***Summary*** section, you can include this certification as a qualification.
- To include a summary that mentions this certification in your LinkedIn® profile, update your ***About*** section by following the steps listed in this Linkedin® Help article.

Here is an example of a professional summary:

Professional Summary

Detail-oriented cybersecurity professional dedicated to protecting organizations and the people they serve. Knowledgeable about NIST frameworks and able to implement security controls to ensure compliance with international regulations related to data protection. Experience with identifying threats, risks, and vulnerabilities; security hardening; threat modeling; and incident escalation and response. Proficient in the use of Linux command line, SQL, and Python. Strong communication and problem-solving skills. Recently completed the Google Cybersecurity Certificate, a rigorous, skills-based program that covers key cybersecurity knowledge and skills.

Add your badge

Check out the next course item to learn how to claim your Google Cybersecurity Certificate completion badge and add it to your LinkedIn® profile!

Claim your Google Cybersecurity certificate badge!

Learners who complete all eight courses of the Google Cybersecurity certificate are eligible to earn a digital badge from Credly and Google! A badge is a visual representation of a verified credential that you've earned. In this case, your credential is the Google Cybersecurity Certificate. You can share your badge on platforms like LinkedIn® to draw the attention of potential employers.

More details are in the FAQ below. For any other questions, including issues with your certificate, please reach out to Coursera Learner Services.

About badges

What are Credly and Acclaim?

- Acclaim is a badging platform that's part of Credly, a leading digital credential service provider. Acclaim provides badges so that you can easily share your achievements to online destinations like LinkedIn®, and employers can instantly verify your skills.

About the Google badge

How do I claim my badge for completing the Google Cybersecurity Certificate?

- When you complete the Google Cybersecurity Certificate, **you will receive an email from Credly** (admin@credly.com) with instructions about claiming your badge and setting up your account.

- Claim your badge on Credly's Acclaim platform using the email address linked to your Coursera account. You'll need to opt in to share your information and receive your badge
- Please allow at least one week from your date of completion for the system to update. Remember to check your spam folder.

I completed the Google Cybersecurity Certificate. What should I do if I have not received an email invite to claim my badge?

- If you've waited a week since you completed the certificate and haven't received an email, please submit a request through the Credly Help Center.

How do I add my badges to my LinkedIn® profile?

Follow the steps in this Credly article to add your badge to your LinkedIn® profile. You can also check out this YouTube video.

Want to solve a puzzle from Google?

We invite you to stretch your skills in a new way! This puzzle isn't part of passing the certificate program or getting a job, just a fun way to challenge yourself.

01100110 01101001 01101110 01100100 00101110 01100110 01101111 01101111 00101111 00110010 00110000 00110010 00110011 01000111 01101111 01101111 01100111 01101100 01100101 01000011 01100101 01110010 01110100 01110011