**Certificado de Carreira do Google: Focado em Segurança Cibernética**

**Visão geral do Certificado de segurança cibernética do Google**

Olá, bem-vindo ao **Certificado de Segurança Cibernética do Google**! Neste programa, você explorará o crescente campo da segurança cibernética, aprenderá como a segurança cibernética é crucial para as organizações e as pessoas que elas atendem e desenvolverá habilidades relevantes para uma futura carreira no Campo. Ao concluir os oito cursos desse programa de certificação, você se preparará para empregos de nível básico em segurança cibernética, como analista de segurança cibernética, analista de segurança e analista do Centro de operações de segurança (SOC). Não é necessário ter experiência prévia em segurança cibernética para concluir este programa.

**Entre em um campo em crescimento**

Por que as habilidades em segurança cibernética são tão demandadas? O mundo está passando por uma transformação digital. Todos os dias, a globalização do acesso à Internet está se expandindo, introduzindo mais dispositivos, mais aplicativos e uma quantidade ainda maior de dados na World Wide Web. AS como resultado, as ameaças, os riscos e as vulnerabilidades estão se expandindo e causando uma quantidade significativa de danos às organizações e às pessoas. Os profissionais de segurança cibernética estão em alta demanda para ajudar a manter as organizações, as pessoas e os dados seguros.

Ao longo do programa, você terá várias oportunidades de desenvolver seus conhecimentos e habilidades de segurança cibernética. Você explorará conceitos e cenários para aprender o que um analista de segurança cibernética de nível básico deve saber e ser capaz de fazer para prosperar na profissão de segurança cibernética.

**Cursos do Certificado de segurança cibernética do Google**

O Certificado de segurança cibernética do Google tem oito cursos que se concentram e se baseiam nos principais conceitos e habilidades relacionados ao trabalho diário dos profissionais de segurança cibernética, incluindo modelos e frameworks fundamentais de segurança cibernética usados para reduzir riscos, proteger redes e dados, usar programação para automatizar tarefas, identificar e responder a incidentes de segurança e comunicar e colaborar com as partes interessadas. Além disso, você aplicará o que aprendeu em cada curso ao concluir projetos de Portfólio que podem ser usados para mostrar sua compreensão dos conceitos essenciais de segurança cibernética a possíveis empregadores. Os cursos do programa são os seguintes:

1. [**Fundamentos de segurança c**](https://www.coursera.org/learn/foundations-of-cybersecurity/home/week/1)ibernética *(curso atual)*
2. [**Play It Safe: Gerenciamento de riscos de segurança**](https://www.coursera.org/learn/manage-security-risks/home/week/1)
3. [**Conectar e proteger: Redes de computadores e segurança de rede**](https://www.coursera.org/learn/networks-and-network-security/home/week/1)
4. [**Ferramentas do comércio: Linux e SQL**](https://www.coursera.org/learn/linux-and-sql/home/week/1)
5. [**Recursos, ameaças e vulnerabilidades**](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/home/week/1)
6. [**Soe o alarme: Detecção e resposta**](https://www.coursera.org/learn/detection-and-response/home/week/1)
7. [**Automatize as tarefas de segurança cibernética com Python**](https://www.coursera.org/learn/automate-cybersecurity-tasks-with-python/home/week/1)
8. [**Coloque-o em prática: Prepare-se para**](https://www.coursera.org/learn/prepare-for-cybersecurity-jobs/home/week/1) **empregos**[**na**](https://www.coursera.org/learn/prepare-for-cybersecurity-jobs/home/week/1) área de[**segurança c**](https://www.coursera.org/learn/prepare-for-cybersecurity-jobs/home/week/1)ibernética



**Benefícios para quem procura emprego**

Depois de concluir os oito cursos, os formandos do Certificado de segurança cibernética do Google têm acesso a recursos de busca de emprego, cortesia do Google. Você terá a oportunidade de:

* Elaborar seu currículo, participar de entrevistas simuladas e receber dicas de busca de emprego por meio da Big Interview, uma plataforma de treinamento para empregos gratuita para os formandos do programa.
* Aprimorar sua técnica de entrevista com o Interview Warmup, uma ferramenta criada pelo Google pensando nos formandos do certificado. Acessível a perguntas práticas específicas de segurança cibernética, transcrições de suas respostas e insights automáticos que o ajudam a aumentar suas habilidades e confiança.
* Acesse milhares de ofertas de emprego e Coaching individual gratuito com o Career Circle. (Para participar, você deve estar qualificado para trabalhar nos EUA)
* Reivindique seu emblema do Certificado de Segurança Cibernética do Google e compartilhe sua conquista nos serviços de rede de computadores profissionais do LinkedIn® para se destacar entre outros candidatos para possíveis empregadores.
* Prepare-se para o exame CompTIA Security+, a certificação líder do setor para funções de segurança cibernética. Você receberá uma credencial dupla ao concluir o Certificado de segurança cibernética do Google e o exame CompTIA Security+.

Parabéns por ter dado o primeiro passo para desenvolver suas habilidades para uma carreira em segurança cibernética. Aproveite a jornada!

**Visão geral do curso 1**

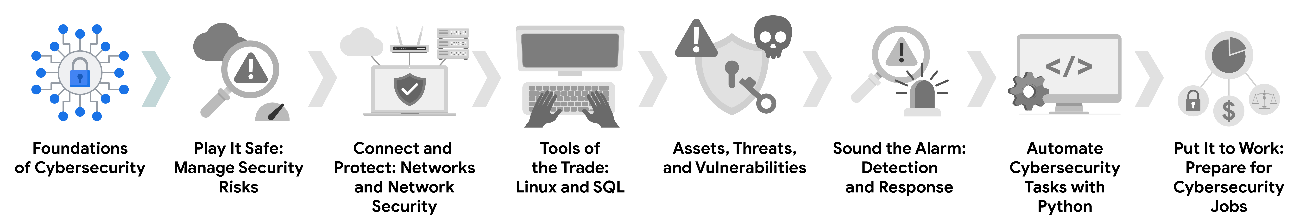


Olá, bem-vindo ao **Foundations of Cybersecurity (Fundamentos de segurança cibernética**), o primeiro curso do Certificado de segurança cibernética do Google. Você começou uma jornada emocionante!

Neste curso, você conhecerá as principais responsabilidades profissionais e as habilidades essenciais de quem trabalha na área de segurança cibernética. Você explorará os oito domínios de segurança do Certified Information Systems Security Professional (CISSP), várias estruturas e controles de segurança, bem como um modelo de segurança fundamental chamado de tríade Confiança, integridade e disponibilidade (CIA). Você também será apresentado a algumas ferramentas comuns usadas por analistas de segurança que ajudam a proteger organizações e pessoas.

**Evolução do programa de certificação**

O programa de certificação em segurança cibernética do Google tem oito cursos. **Fundamentos de segurança cibernética** é o primeiro curso.



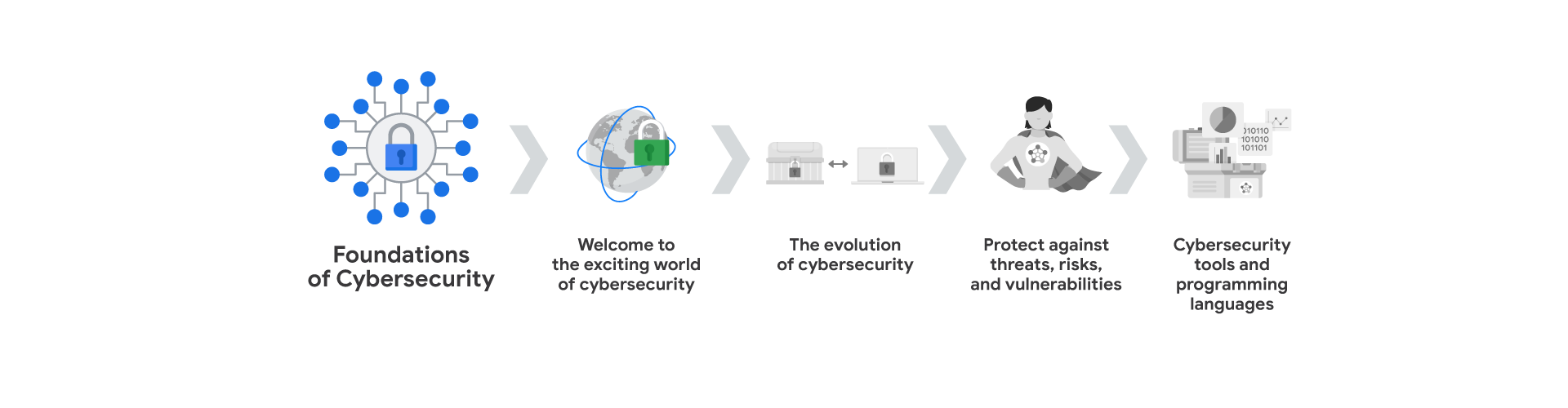
1. [**Fundamentos de segurança cibernética**](https://www.coursera.org/learn/foundations-of-cybersecurity/home/week/1)- *(curso atual)* Explore a profissão de segurança cibernética, incluindo eventos significativos que levaram ao desenvolvimento do campo de segurança cibernética e sua importância contínua para as operações organizacionais. Conheça as funções e responsabilidades de segurança cibernética de nível básico.
2. [**Play It Safe: Gerencie os riscos de segurança**](https://www.coursera.org/learn/manage-security-risks/home/week/1)- Identifique como os profissionais de segurança cibernética usam estruturas e controles para proteger as operações comerciais e explore as ferramentas comuns de segurança cibernética.
3. [**Connect and Protect (Conectar e Proteger): Networks and Network Security**](https://www.coursera.org/learn/networks-and-network-security/home/week/1)- Compreenda as vulnerabilidades em nível de rede e como protegê-las.
4. [**Tools of the Trade: Linux e SQL**](https://www.coursera.org/learn/linux-and-sql/home/week/1)- Explore as habilidades básicas de computação, incluindo a comunicação com o sistema operacional Linux por meio da linha de comando e a consulta a bancos de dados com SQL.
5. [**Assets, Threats, and Vulnerabilities (Ativos, ameaças e vulnerabilidades**](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/home/week/1))- Aprenda sobre a importância dos controles de segurança e do desenvolvimento de uma mentalidade de ator de ameaças para proteger e defender os ativos de uma organização contra várias ameaças, riscos e vulnerabilidades.
6. [**Soe o Alarme: Detecção e resposta**](https://www.coursera.org/learn/detection-and-response/home/week/1)- Entenda o ciclo de vida da resposta a incidentes e pratique o uso de ferramentas para detectar e responder a incidentes de segurança cibernética.
7. [**Automate Cybersecurity Tasks with Python**](https://www.coursera.org/learn/automate-cybersecurity-tasks-with-python/home/week/1)- Explore a linguagem de programação Python e escreva códigos para automatizar tarefas de segurança cibernética.
8. [**Coloque-a em prática: Prepare-se para empregos de segurança cibernética**](https://www.coursera.org/learn/prepare-for-cybersecurity-jobs/home/week/1)- Aprenda sobre classificação de incidentes, escalonamento e maneiras de se comunicar com as partes interessadas. Este curso encerra o programa com dicas sobre como se envolver com a comunidade de segurança cibernética e se preparar para sua busca de emprego.

**Conteúdo do curso 1**

Cada curso deste programa de certificação é dividido em módulos. Você pode concluir os cursos no seu próprio ritmo, mas a divisão em módulos foi criada para ajudá-lo a concluir todo o Certificado de segurança cibernética do Google em cerca de seis meses.

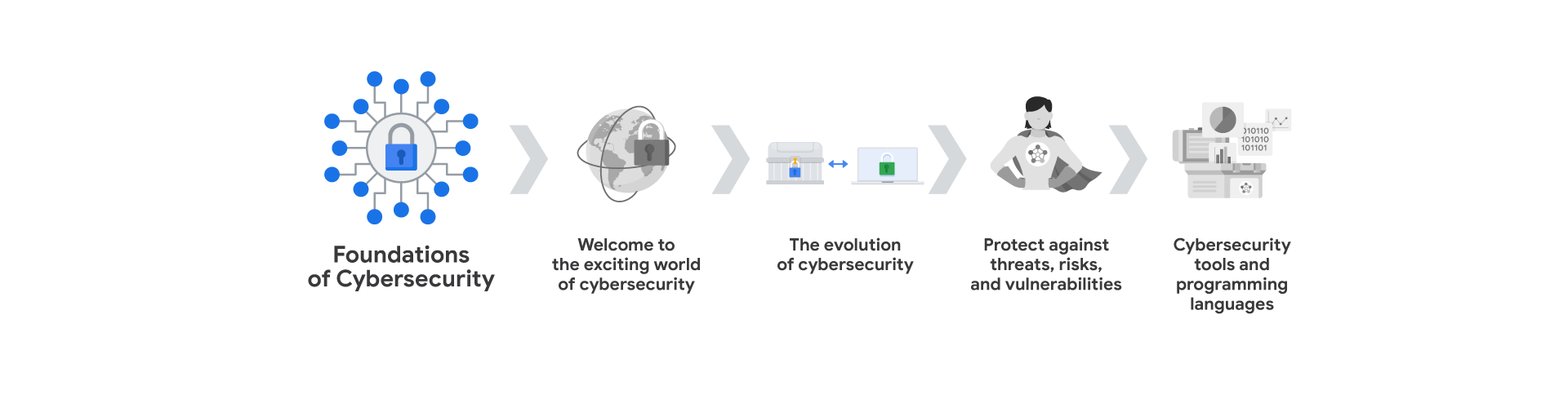
O que está por vir? Aqui está uma rápida visão geral das habilidades que você aprenderá em cada módulo deste curso.

**Módulo 1: Bem-vindo ao empolgante mundo da segurança cibernética**



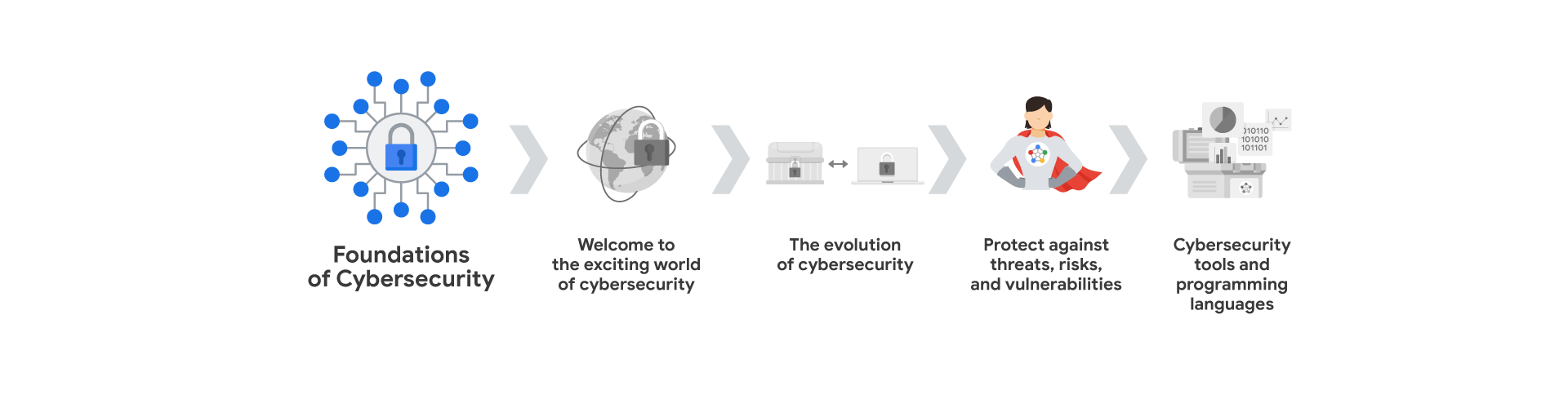
Comece sua jornada na segurança cibernética! Você explorará o campo da segurança cibernética e aprenderá sobre as responsabilidades do trabalho dos profissionais de segurança cibernética.

**Módulo 2: A evolução da segurança cibernética**



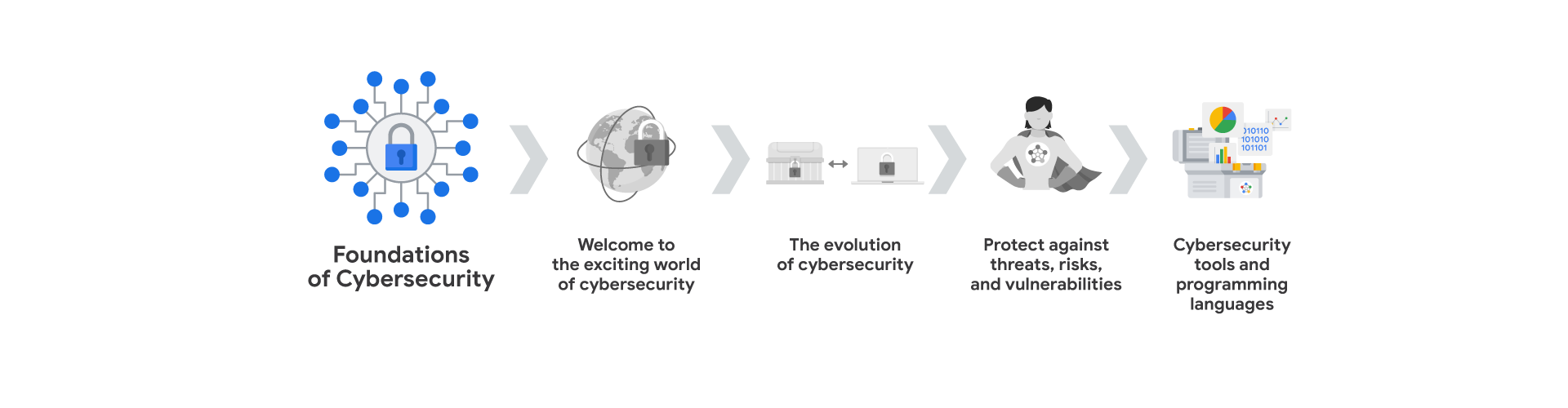
Você explorará como as ameaças à segurança cibernética surgiram e evoluíram junto com a adoção de computadores. Também entenderá como os ataques cibernéticos do passado e do presente influenciaram o desenvolvimento do campo de segurança. Além disso, você terá uma visão geral dos oito domínios de segurança.

**Module 3: Proteger-se contra ameaças, riscos e vulnerabilidades**



Você aprenderá sobre estruturas e controles de segurança, que são usados para reduzir os riscos organizacionais. Você abordará os princípios da tríade CIA e várias estruturas do National Institute of Standards and Technology (NIST). Além disso, você explorará a ética de segurança.

**Módulo 4: Ferramentas de segurança cibernética e linguagens de programação**



Você descobrirá as ferramentas comuns usadas pelos analistas de segurança cibernética para identificar e eliminar riscos. Você aprenderá sobre ferramentas de gerenciamento de eventos e informações de segurança (SIEM), analisadores de protocolo de rede e linguagens de programação, como Python e SQL.

**O que esperar**

Cada curso oferece vários tipos de oportunidades de aprendizado:

* **Vídeos** conduzidos por instrutores do Google ensinam novos conceitos, introduzem o uso de ferramentas relevantes, oferecem suporte à carreira e fornecem histórias pessoais inspiradoras.
* **As leituras** se baseiam nos tópicos discutidos nos vídeos, apresentam conceitos relacionados, compartilham recursos úteis e descrevem estudos de caso.
* **Conecte-se com outros alunos**: Se tiver alguma dúvida, é provável que você não esteja sozinho. Visite a [comunidade](http://www.coursera.support/s/group-invite?id=MEY5VkgwMDAwMDAwMWMxMEFB) privada de [segurança cibernética](http://www.coursera.support/s/group-invite?id=MEY5VkgwMDAwMDAwMWMxMEFB) do Coursera para expandir sua rede de contatos, discutir jornadas de carreira e compartilhar experiências. Confira o [guia de início rápido](https://www.coursera.support/s/article/Community-Quick-Start-Guide).
* **As atividades de autoavaliação** e **os laboratórios** oferecem prática na aplicação das habilidades que você está aprendendo e permitem que você avalie seu próprio trabalho comparando-o com um exemplo concluído.
* **Os plug-ins interativos** o incentivam a praticar tarefas específicas e o ajudam a integrar o conhecimento adquirido no curso.
* **Os testes em vídeo** o ajudam a verificar sua compreensão à medida que avança em cada vídeo.
* **Os testes práticos** permitem que você verifique sua compreensão dos principais conceitos e fornecem feedback valioso.
* **Os testes com notas** demonstram sua compreensão dos principais conceitos de um curso. Você deve obter uma pontuação de 80% ou mais em cada teste avaliado para obter um certificado, e pode fazer um teste avaliado várias vezes para obter uma pontuação de aprovação.

**Dicas para o sucesso**

* É altamente recomendável que você leia os itens de cada lição na ordem em que aparecem, pois as novas informações e conceitos se baseiam no conhecimento anterior.
* Participe de todas as oportunidades de aprendizado para obter o máximo possível de conhecimento e experiência.
* Se algo estiver confuso, não hesite em reproduzir um vídeo, revisar uma leitura ou repetir uma atividade de auto-revisão.
* Use os recursos adicionais mencionados neste curso. Eles foram criados para apoiar seu aprendizado. Você pode encontrar todos esses recursos na guia [Recursos](https://www.coursera.org/learn/foundations-of-cybersecurity/resources/L1aML).
* Quando encontrar links úteis neste curso, marque-os como favoritos para que você possa consultar as informações posteriormente para estudo ou revisão.
* Entenda e siga o [Código de Conduta da Coursera](https://www.coursera.support/s/article/208280036-Coursera-Code-of-Conduct?) para garantir que a comunidade de aprendizagem permaneça um lugar acolhedor, amigável e de apoio para todos os membros.

**Seu Roteiro para o Certificado de Segurança Cibernética do Google**

* **Which course?**

For details on topics covered, tools used, and skills you will gain, select the course you’d like to learn more about.

* **What tools, solutions, or platforms are included in the curriculum?**The curriculum includes SIEM tools, playbooks, network and cloud security, network protocol analyzers, and programming languages.
* **Doo i need to take the courses in a certain order?** We highly recommend completing the courses in the order presented. The content in each course builds on information from previous lessons.
* **Do i need to have a background in cybersecutiry?**

This certificate program is for learners with little to no experience in the cybersecurity field.

**Foundations in cybersecurity**

**In this course, you will:**

* Define the field of security
* Recognize core skills and knowledge needed to become a security analyst
* Identify how security attacks impact business operations
* Identify eight security domains
* Define security frameworks and controls

**Skill sets:**

* Communicating effectively
* Collaborating with others
* Identifying threats, risks, and vulnerabilities
* Problem-solving

**Play it Safe: Manage Security Risks**

In this course, you will:

* Recognize and explain the focus of eight security domains
* Identify the steps of risk management
* Describe the CIA triad
* Identify security principles
* Define and describe the purpose of a playbook
* Explain how entry-level security analysts use SIEM dashboards

Skill sets:

* Applying the CIA triad to workplace situations
* Analyzing log data
* Identifying the phases of an incident response playbook

**Connect and Project: Networks and Network Security**

In this course, you will:

* Define types of networks
* Explain how data is sent and received over a network
* Recognize common network protocols
* Compare and contrast local networks to cloud computing
* Explain how to secure a network against intrusion tactics

Skill sets:

* Configuring a firewall
* Recognizing components of computer networks and cloud computing
* Analyzing threats
* Implementing security hardening

**Tools of the Trade: Linux and SQL**

In this course, you will:

* Describe the main functions of an operating system
* Explain the relationship between operating systems, applications, and hardware
* Compare a graphical user interface to a command line interface
* Navigate the file system using Linux commands via the Bash shell
* Use SQL to retrieve information from a database

Skill sets:

* Interacting with both a graphical user interface (GUI) and command line interface (CLI)
* Querying a database with SQL
* Filtering on a particular word with the Linux command line
* Authenticating and authorizing users with the Linux command line

**Assets, Threats, and Vulnerabilities**

In this course, you will:

* Explain security’s role in mitigating organizational risk
* Describe the defense in depth strategy
* Explain how vulnerability assessments are used to assess potential risk
* Develop an attacker mindset to recognize threats
* Discuss the role encryption and hashing play in securing assets
* Identify forms of social engineering, malware, and web-based exploits

Skill sets:

* Classifying assets
* Decrypting a message
* Searching the CVE database for vulnerable applications
* Analyzing attack surfaces
* Applying the PASTA threat modeling framework

**Sound the Alarm: Detection and Response**

In this course, you will:

* Explain the lifecycle of an incident
* Use packet sniffing tools to capture and view network communications
* Perform artifact investigations to analyze and verify security incidents
* Identify the steps to contain, eradicate, and recover from an incident
* Interpret the basic syntax and components of signatures and logs in IDS and NIDS tools

Skill sets:

* Capturing, viewing, and analyzing a packet
* Investigating a suspicious hash file
* Following a playbook
* Examining alerts, logs, and rules
* Performing queries with SIEM tools

**Automate Cybersecurity Tasks with Python**

In this course, you will:

* Explain how the Python programming language is used in security
* Write a simple algorithm
* Use regular expressions in Python to extract information from text
* Use Python to automate tasks performed by security professionals
* Use Python to parse a file

Skill sets:

* Working with strings and their index values
* Applying regular expressions (regex)
* Importing and parsing a file
* Debugging code

**Put It to Work: Prepare for Cybersecurity Jobs**

In this course, you will:

* Define stakeholders and describe their security roles
* Communicate sensitive information with care and confidentiality
* Identify reliable sources within the security community
* Determine opportunities to become engaged with the security community
* Determine ways to establish and advance a career in security, by engaging with the security community
* Find, apply for, and prepare for job interviews

Skill sets:

* Creating a dashboard
* Creating or updating a resume
* Using the STAR method for interview questions
* Drafting an elevator pitch

**Módulo I**

**Bem vindo a certificação de cibersegurança do Google**

Olá e bem-vindo ao Certificado de Carreira do Google focado em segurança cibernética. Estou tão animada que você esteja aqui! Meu nome é Toni e sou gerente de engenharia de segurança no Google. Serei seu instrutor no primeiro curso deste programa de certificação. Ao iniciar este curso, você já deu um grande passo para desenvolver novas habilidades que o ajudarão em sua carreira.

Segurança cibernética pode parecer assustadora no início, mas você ficaria surpreso com as diferentes experiências que muitos de nós temos. Trabalhei como analista de inteligência antes de conseguir meu primeiro emprego no setor de segurança e estou empolgado em ser seu instrutor ao iniciar sua jornada rumo à segurança.

A demanda por profissionais de segurança está crescendo a um ritmo incrível. Em 2030, o Bureau of Labor Statistics dos EUA espera que as funções de segurança cresçam em mais de 30%, o que é superior à taxa média de crescimento de outras ocupações. O acesso global à Internet está se expandindo. Todos os dias, mais pessoas e organizações estão adotando novas tecnologias digitais. Ter uma comunidade diversificada de profissionais de segurança com origens, perspectivas e experiências únicas é essencial para proteger e atender diferentes mercados.

Trabalhar com segurança me permitiu trabalhar com pessoas de todo o mundo. Trabalhar com pessoas com experiências diversas garante que nossas equipes façam muitas perguntas e criem soluções mais criativas.

O principal objetivo em segurança é proteger organizações e pessoas. Essa linha de trabalho permite que você apoie e interaja com pessoas em todo o mundo.

Há muitas vagas abertas para analistas de segurança iniciantes, e os empregadores estão tendo dificuldades para encontrar candidatos suficientes com a experiência certa. Este programa foi desenvolvido para fornecer o conhecimento e as habilidades necessárias para iniciar ou avançar na profissão de segurança. Independentemente do seu nível de habilidade atual, ao concluir este programa de certificação, você estará preparado para encontrar um emprego relacionado à segurança ou expandir sua carreira em segurança.

Você pode estar se perguntando: o que os profissionais de segurança realmente fazem? Você já precisou atualizar sua senha on-line para incluir um número ou um símbolo especial? Se sim, então você já está familiarizado com as medidas básicas de segurança, como o gerenciamento de senhas. E se você já recebeu uma notificação de um provedor de serviços sobre dados roubados ou uma invasão de software, então você tem experiência em primeira mão com o impacto de uma violação de segurança. Se você já se perguntou como as organizações protegem os dados, então você já tem duas características importantes que são necessárias para prosperar nesse setor: curiosidade e entusiasmo.

Os analistas de segurança ajudam a minimizar os riscos para organizações e pessoas. Os analistas trabalham para se proteger proativamente contra incidentes enquanto monitoram continuamente os sistemas e as redes. E, se ocorrer um incidente, eles investigam e relatam suas descobertas. Eles estão sempre fazendo perguntas e procurando soluções.

Uma das melhores coisas sobre o setor de segurança são os muitos caminhos e opções de carreira aos quais ele expõe você. Cada opção envolve um conjunto exclusivo de habilidades e responsabilidades. Não importa qual seja sua formação, você provavelmente descobrirá que já tem alguma experiência relevante. Se você gosta de colaborar e ajudar outras pessoas, resolver quebra-cabeças e é motivado por desafios, essa é a carreira para você.

Por exemplo, minha experiência como analista de inteligência não tinha nada a ver com segurança cibernética. No entanto, ter fortes habilidades de pensamento crítico e comunicação forneceu uma base sólida para meu sucesso quando decidi seguir uma carreira em segurança.

Se você não tem certeza de qual direção deseja seguir no setor de segurança, tudo bem. Este programa lhe dará uma visão geral de muitos tipos diferentes de empregos disponíveis. Também permitirá que você explore certos conjuntos de habilidades especializadas para ajudá-lo a descobrir para onde deseja levar sua carreira.

Os Certificados de Carreira do Google são elaborados por profissionais do setor com décadas de experiência aqui no Google. Você terá um especialista diferente do Google para guiá-lo em cada curso do certificado. Compartilharemos nosso conhecimento em vídeos, ofereceremos oportunidades práticas com atividades práticas e mostraremos cenários reais que você pode encontrar no trabalho.

Ao longo deste programa, você obterá prática na detecção e resposta a ataques, monitoramento e proteção de redes, investigação de incidentes e criação de código para automatizar tarefas.

O programa é composto por vários cursos elaborados para ajudá-lo a conseguir um emprego de nível básico. Você aprenderá sobre tópicos como: conceitos básicos de segurança; domínios de segurança; segurança de rede; noções básicas de computação, incluindo Linux e SQL; além de entender ativos, ameaças e vulnerabilidades. Nosso objetivo é ajudar você a alcançar sua meta de ingressar no setor de segurança.

Você aprenderá sobre detecção e resposta a incidentes, além de como usar linguagens de programação, como Python, para realizar tarefas comuns de segurança. Você também obterá estratégias valiosas de busca de emprego que o beneficiarão quando você começar a encontrar e se candidatar a empregos na profissão de segurança.

A conclusão deste Certificado de Carreira do Google ajudará você a desenvolver habilidades e aprender a usar ferramentas para se preparar para um emprego em um campo de rápido crescimento e alta demanda.

O certificado foi elaborado para prepará-lo para um emprego em 3 a 6 meses, se você trabalhar com o certificado em tempo parcial. Depois de se formar, você pode se conectar com mais de 200 empregadores interessados em contratar graduados do Certificado de Carreira do Google, como você. Se você deseja trocar de emprego, começar uma nova carreira ou aprimorar suas habilidades, este certificado de carreira do Google pode abrir portas para novas oportunidades de emprego.

Você não precisa de experiência ou conhecimento prévio na área de segurança, pois esse programa de certificação começará com o básico. Estarei ao seu lado durante este primeiro curso, garantindo que você esteja aprendendo o conhecimento básico necessário para ter sucesso na área. Esse programa também é flexível. Você pode concluir todos os cursos deste certificado em seus próprios termos e no seu próprio ritmo, on-line.

Reunimos alguns instrutores incríveis para apoiá-lo em sua jornada, e eles gostariam de se apresentar agora:

* **Ashley**: Líder de Capacitação de Engenharia de Clientes para Vendas de Operações de Segurança no Google. Mostrará os domínios, estruturas e controles de segurança, bem como ameaças, riscos e vulnerabilidades comuns à segurança.
* **Chris**: Diretor de Segurança de Informações do Google Fiber. Falará sobre a estrutura de uma rede, protocolos de rede, ataques comuns à rede e como proteger uma rede.
* **Kim**: Gerente de programas técnicos no Google. Guiará por meio de habilidades básicas de computação que apoiam o trabalho de um analista de segurança, como sistemas operacionais, linha de comando Linux e SQL.
* **Da'Queshia**: Engenheira de segurança no Google. Explorará a proteção dos ativos organizacionais por meio de controles de segurança.
* **Dave**: Estrategista principal de segurança no Google. Ensiná-lo-á como detectar e responder a incidentes de segurança.
* **Angel**: Engenheiro de segurança no Google. Explorará os conceitos básicos de programação em Python para ajudar a automatizar tarefas comuns de segurança.
* **Dion**: Gerente de Programas no Google. Será seu instrutor na primeira parte do curso final, discutindo como escalar incidentes e se comunicar com as partes interessadas.
* **Emily**: Gerente de Programas no Google. Guiará pela parte final do programa e compartilhará maneiras de interagir com a comunidade de segurança e se preparar para sua próxima busca de emprego.

E, como você já sabe, eu, Toni, vou guiá-lo pelo primeiro curso deste programa. Este é um ótimo momento para desenvolver sua carreira na área de segurança. Vamos começar!

Here is the translated text in English:

Hello and welcome to the Google Career Certificate focused on cybersecurity. I’m so excited that you’re here! My name is Toni and I’m a security engineering manager at Google. I’ll be your instructor for the first course in this certification program. By starting this course, you’ve already taken a big step towards developing new skills that will help you in your career.

Cybersecurity may seem intimidating at first, but you’d be surprised by the different experiences many of us have had. I worked as an intelligence analyst before landing my first job in the security field, and I’m excited to be your instructor as you begin your journey into security.

The demand for security professionals is growing at an incredible rate. By 2030, the U.S. Bureau of Labor Statistics expects security jobs to grow by more than 30%, which is higher than the average growth rate for other occupations.

Global internet access is expanding. Every day, more people and organizations are adopting new digital technologies. Having a diverse community of security professionals with different backgrounds, perspectives, and experiences is essential to protect and serve different markets.

Working in security has allowed me to work with people from all over the world. Working with people with diverse experiences ensures that our teams ask a lot of questions and come up with more creative solutions.

The main goal in security is to protect organizations and people. This line of work allows you to support and interact with people all around the world.

There are many open positions for entry-level security analysts, and employers are struggling to find enough candidates with the right experience. This program has been designed to provide the knowledge and skills needed to get started or advance in the security profession. Regardless of your current skill level, by completing this certification program, you will be prepared to find a security-related job or further your career in security.

You may be wondering: What do security professionals actually do? Have you ever needed to update your online password to include a number or special symbol? If so, then you are already familiar with basic security measures like password management. And if you’ve ever received a notification from a service provider about stolen data or a software breach, then you have firsthand experience with the impact of a security breach. If you’ve ever wondered how organizations protect their data, then you already have two important traits needed to thrive in this field: curiosity and enthusiasm.

Security analysts help minimize risks to organizations and people. They work proactively to protect against incidents while continuously monitoring systems and networks. If an incident occurs, they investigate and report their findings. They are always asking questions and seeking solutions.

One of the best things about the security field is the many career paths and options it exposes you to. Each option involves a unique set of skills and responsibilities. No matter what your background is, you’ll likely find that you already have some relevant experience. If you enjoy collaborating and helping others, solving puzzles, and are motivated by challenges, this is the career for you.

For example, my experience as an intelligence analyst had nothing to do with cybersecurity. However, having strong critical thinking and communication skills provided a solid foundation for my success when I decided to pursue a career in security.

If you’re not sure which direction you want to take in the security field, that’s okay. This program will give you an overview of many different jobs available. It will also allow you to explore certain specialized skill sets to help you figure out where you want to take your career.

The Google Career Certificates are designed by industry professionals with decades of experience here at Google. You’ll have a different Google expert guiding you through each course of the certification. We’ll share our knowledge in videos, provide hands-on opportunities with practical activities, and showcase real-world scenarios you might encounter on the job.

Throughout this program, you will practice detecting and responding to attacks, monitoring and protecting networks, investigating incidents, and writing code to automate tasks.

The program consists of several courses designed to help you land an entry-level job. You’ll learn about topics like: security fundamentals; security domains; network security; computing basics, including Linux and SQL; and understanding assets, threats, and vulnerabilities. Our goal is to help you achieve your goal of entering the security field.

You’ll learn about incident detection and response, as well as how to use programming languages like Python to perform common security tasks. You’ll also gain valuable job-search strategies that will benefit you as you begin finding and applying for jobs in the security profession.

The conclusion of this Google Career Certificate will help you develop skills and learn to use tools to prepare for a job in a fast-growing and high-demand field.

The certificate is designed to prepare you for a job in 3 to 6 months, if you work on it part-time. After graduation, you can connect with over 200 employers interested in hiring Google Career Certificate graduates like you. Whether you want to change jobs, start a new career, or improve your skills, this Google Career Certificate can open doors to new job opportunities.

You don’t need prior experience or knowledge in security, as this certification program will start with the basics. I’ll be with you throughout this first course, ensuring that you learn the basic knowledge needed for success in the field. This program is also flexible. You can complete all the courses in this certification on your own terms and at your own pace, online.

We’ve gathered some amazing instructors to support you on your journey, and they’d like to introduce themselves now:

Hello! My name is Ashley, and I’m a Customer Engineering Training Lead for Security Operations Sales at Google. I’ll guide you through security domains, frameworks, and controls, as well as common security threats, risks, and vulnerabilities. You’ll also learn about the common tools used by security analysts. I can’t wait to get started!

Hello! My name is Chris, and I’m the Director of Information Security at Google Fiber. I’m excited to talk to you about network architecture, network protocols, common network attacks, and how to protect a network.

Hello! My name is Kim, and I’m a Technical Program Manager at Google. I’ll guide you through the basic computing skills that support the work of a security analyst. We’ll also learn about operating systems, the Linux command line, and SQL.

Hi! My name is Da'Queshia, and I’m a Security Engineer at Google. Together, we’ll explore how to protect organizational assets through a variety of security controls and develop a deeper understanding of risks and vulnerabilities.

Hi! My name is Dave, and I’m a Senior Security Strategist at Google. During our time together, we’ll learn how to detect and respond to security incidents. You’ll also get the chance to monitor and analyze network activity using powerful security tools.

Hello! I’m Angel, and I’m a Security Engineer at Google. We’ll explore the basics of programming in Python to help you automate common security tasks.

Hello! I’m Dion. I’m a Program Manager at Google. I’m your instructor for the first part of the final course of the program. We’ll discuss how to scale incidents and communicate with stakeholders.

And my name is Emily. I’m a Program Manager at Google. I’ll guide you through the final part of the program and share ways to interact with the security community and prepare for your next job search.

And, as you already know, I’ll be guiding you through the first course in this program. This is a great time to develop your career in security. Sounds exciting? Let’s get started!

**Módulo I - Vídeo – Bem vindo a primeira semana**

Oi de novo! Agora que você tem uma ideia do que esperar do programa como um todo, vamos falar mais sobre o que você aprenderá neste curso.

Este curso apresentará o mundo da segurança e como ela é usada para proteger operações comerciais, usuários e dispositivos, para que você possa contribuir para a criação de uma Internet mais segura para todos.

Nesta seção, abordaremos os conceitos básicos de segurança. Primeiro, definiremos o que é segurança. Em seguida, exploraremos as responsabilidades profissionais comuns dos analistas de segurança. Com base nisso, discutiremos as principais habilidades que um analista de segurança pode ter. Por fim, discutiremos o valor da segurança para proteger organizações e pessoas.

Em seguida, abordaremos oito domínios de segurança. Depois, abordaremos frameworks e controles de segurança comuns. Por fim, encerraremos o curso discutindo ferramentas e linguagens de programação comuns que os analistas de segurança iniciantes podem usar.

A seguir, analisaremos alguns recursos que permitirão que você aproveite ao máximo esse programa. Estou muito animada para que você comece essa jornada — vamos começar!

Here is the translated text in English:

Hi again! Now that you have an idea of what to expect from the program as a whole, let's talk more about what you’ll learn in this course.

This course will introduce the world of security and how it’s used to protect business operations, users, and devices so that you can contribute to creating a safer Internet for everyone.

In this section, we’ll cover the basics of security. First, we’ll define what security is. Then, we’ll explore the common professional responsibilities of security analysts. Based on that, we’ll discuss the key skills a security analyst may have. Finally, we’ll talk about the value of security in protecting organizations and people.

Next, we’ll cover eight security domains. Then, we’ll look at common security frameworks and controls. Finally, we’ll wrap up the course by discussing tools and programming languages that beginner security analysts can use.

Next, we’ll look at some resources that will help you make the most of this program. I’m really excited for you to begin this journey — let’s get started!

Eu me comprometo com meu objetivo de completar o Certificado Profissional em Cibersegurança do Google.  
Eu escolhi completar o Certificado Profissional em Cibersegurança do Google.  
**O que motivou você a fazer este programa?**  
R: Meu interesse em segurança cibernética e o desejo de adquirir habilidades valiosas para proteger dados e sistemas, além de expandir minhas oportunidades profissionais.

**Quando eu encontrar obstáculos ou perder a motivação em algum momento durante o programa, eu vou...**  
R: Relembrar meus objetivos de longo prazo e os benefícios que essa qualificação trará para minha carreira, além de buscar apoio em comunidades e fóruns para superar dificuldades.

**O que você fará ou dirá para motivar seu futuro eu?**  
R: Vou lembrar a mim mesmo do impacto positivo que concluir este programa terá na minha trajetória profissional e como isso pode abrir portas para novos desafios e oportunidades.

Here are the responses in English:

I commit to my goal of completing the Google Cybersecurity Professional Certificate.  
I chose to complete the Google Cybersecurity Professional Certificate.  
**What motivated you to take this program?**  
R: My interest in cybersecurity and the desire to acquire valuable skills to protect data and systems, as well as expand my professional opportunities.

**When I run into obstacles or lack motivation at some point during the program, I will...**  
R: Remind myself of my long-term goals and the benefits this qualification will bring to my career, as well as seek support from communities and forums to overcome difficulties.

**What will you do or say to motivate your future self?**  
R: I will remind myself of the positive impact completing this program will have on my career path and how it can open doors to new challenges and opportunities.

Modulo I – Introdução a cibersegurança

Imagine que você está se preparando para uma tempestade. Você recebeu uma notificação de que uma tempestade está chegando. Você se prepara reunindo as ferramentas e os materiais necessários para se manter seguro. Você garante que suas janelas e portas estejam seguras. Você monta um kit de primeiros socorros, ferramentas, comida e água. Você está preparado. A tempestade chega e há ventos fortes e chuvas fortes. A tempestade está usando sua força para tentar invadir sua casa. Você percebe alguns vazamentos de água e começa a corrigi-los rapidamente para minimizar qualquer risco ou dano potencial.

Lidar com um incidente de segurança não é diferente. As organizações devem se preparar para a tempestade, garantindo que tenham as ferramentas para mitigar e responder rapidamente às ameaças externas. O objetivo é minimizar riscos e possíveis danos.

Como analista de segurança, você trabalhará para proteger sua organização e as pessoas que ela atende de uma variedade de riscos e ameaças externas. E se uma ameaça passar, você e sua equipe fornecerão uma solução para remediar a situação.

Para ajudar você a entender melhor o que isso significa, definiremos a segurança e discutiremos as funções dos profissionais de segurança nas organizações.

Vamos começar com algumas definições: Cibersegurança, ou segurança, é a prática de garantir a confidencialidade, a integridade e a disponibilidade das informações protegendo redes, dispositivos, pessoas e dados contra acesso não autorizado ou exploração criminosa.

Por exemplo, exigir senhas complexas para acessar sites e serviços melhora a confidencialidade ao tornar muito mais difícil para um agente de ameaças comprometê-las. Um agente de ameaça é qualquer pessoa ou grupo que apresente um risco de segurança.

Agora que você conhece a definição de segurança, vamos discutir o que as equipes de segurança fazem por uma organização.

A segurança protege contra ameaças externas e internas. Uma ameaça externa é alguém de fora da organização tentando obter acesso a informações, redes ou dispositivos privados.

Uma ameaça interna vem de funcionários atuais ou antigos, fornecedores externos ou parceiros confiáveis. Muitas vezes, essas ameaças internas são acidentais, como um funcionário clicando em um link comprometido em um e-mail. Outras vezes, o ator interno se envolve intencionalmente em atividades como acesso não autorizado a dados ou abuso de sistemas para uso pessoal.

Profissionais de segurança experientes ajudarão as organizações a mitigar ou reduzir o impacto de ameaças como essas.

As equipes de segurança também garantem que uma organização atenda à conformidade regulatória, ou às leis e diretrizes, que exigem a implementação de padrões de segurança específicos.

Garantir que as organizações estejam em conformidade pode permitir que elas evitem multas e auditorias, ao mesmo tempo em que cumprem sua obrigação ética de proteger os usuários.

As equipes de segurança também mantêm e melhoram a produtividade dos negócios. Ao estabelecer um plano para a continuidade dos negócios, as equipes de segurança permitem que as pessoas façam seu trabalho, mesmo no caso de algo como uma violação de dados.

Estar preocupado com a segurança também pode reduzir as despesas associadas aos riscos, como a recuperação da perda de dados ou do tempo de inatividade operacional e, potencialmente, evitar multas. O último benefício da segurança que discutiremos é manter a confiança na marca. Se os serviços ou os dados do cliente forem comprometidos, isso pode diminuir a confiança na organização, prejudicar a marca e prejudicar os negócios a longo prazo. A perda da confiança do cliente também pode resultar em menos receita para a empresa.

Agora, vamos examinar algumas funções comuns baseadas em segurança. Depois de concluir este programa de certificação, aqui estão alguns cargos que você pode procurar: analista ou especialista em segurança, analista ou especialista em cibersegurança, analista de centro de operações de segurança ou SOC, analista de segurança de informações.

Você também aprenderá mais sobre as responsabilidades associadas a alguns desses cargos posteriormente no programa.

Como você pode perceber agora, o campo da segurança inclui muitos tópicos e conceitos e cada atividade que você realiza neste programa o aproxima um passo de um novo emprego. Vamos continuar aprendendo juntos.

Here is the translated text in English:

Imagine you're preparing for a storm. You received a notification that a storm is coming. You prepare by gathering the tools and materials needed to stay safe. You make sure your windows and doors are secure. You assemble a first aid kit, tools, food, and water. You are prepared. The storm arrives with strong winds and heavy rain. The storm is using its force to try to invade your house. You notice some water leaks and quickly start fixing them to minimize any potential risk or damage.

Dealing with a security incident is no different. Organizations must prepare for the storm by ensuring they have the tools to mitigate and respond quickly to external threats. The goal is to minimize risks and potential damage.

As a security analyst, you will work to protect your organization and the people it serves from a variety of risks and external threats. And if a threat gets through, you and your team will provide a solution to remedy the situation.

To help you better understand what this means, we’ll define security and discuss the roles of security professionals in organizations.

Let's start with a few definitions: Cybersecurity, or security, is the practice of ensuring the confidentiality, integrity, and availability of information by protecting networks, devices, people, and data from unauthorized access or criminal exploitation.

For example, requiring complex passwords to access sites and services improves confidentiality by making it much harder for a threat agent to compromise them. A threat agent is any person or group that poses a security risk.

Now that you know the definition of security, let's discuss what security teams do for an organization.

Security protects against both external and internal threats. An external threat is someone from outside the organization attempting to access private information, networks, or devices.

An internal threat comes from current or former employees, external vendors, or trusted partners. Often, these internal threats are accidental, like an employee clicking on a compromised link in an email. Other times, the internal actor intentionally engages in activities like unauthorized data access or system abuse for personal use.

Experienced security professionals help organizations mitigate or reduce the impact of these types of threats.

Security teams also ensure that an organization complies with regulatory requirements, or laws and guidelines, that mandate the implementation of specific security standards.

Ensuring that organizations comply can help them avoid fines and audits while fulfilling their ethical obligation to protect users.

Security teams also maintain and improve business productivity. By establishing a business continuity plan, security teams ensure that people can continue working, even in the event of something like a data breach.

Worrying about security can also reduce costs associated with risks, such as recovering from data loss or downtime and potentially avoiding fines. The last benefit of security we’ll discuss is maintaining brand trust. If customer services or data are compromised, it can decrease trust in the organization, damage the brand, and harm long-term business. The loss of customer trust can also result in less revenue for the company.

Now, let’s look at some common security-based roles. After completing this certification program, here are some positions you might look for: security analyst or specialist, cybersecurity analyst or specialist, security operations center (SOC) analyst, information security analyst.

You’ll also learn more about the responsibilities associated with some of these roles later in the program.

As you can see now, the field of security includes many topics and concepts, and every activity you engage in during this program brings you one step closer to a new job. Let’s continue learning together.

Olá, sou Toni, sou gerente de engenharia de segurança. Nossas equipes protegem o Google e seus usuários contra ameaças graves.

Geralmente atacantes apoiados pelo governo, operações de influência coordenadas e agentes graves de ameaças de crimes cibernéticos. Eu cresci como um pirralho do exército. Meu pai era militar e nos mudávamos muito. Em geral, sempre tive interesse em segurança. Eu fiquei muito viciado em relações internacionais quando estava no ensino médio. Eu fiz muitos Model United Nations. E isso realmente uniu essas duas coisas para mim, a forma como a segurança funciona no mundo.

Eu venho de uma família grande. Eu sabia que precisaria de ajuda financeira para ir para a faculdade. E o Departamento de Defesa oferece muitas oportunidades educacionais vinculadas ao serviço. Então, esse foi um ajuste natural para mim. Eu sabia que estava interessado nessa área e isso proporcionaria um caminho de carreira para algo pelo qual eu era apaixonado.

Comecei como analista de inteligência, mas não me concentrei na cibersegurança. Trabalhei na contra-insurgência por vários anos e em questões de inteligência geopolítica. Por fim, ao observar e ver que a forma como a segurança cibernética estava começando a ter um impacto em nossas vidas diárias e no mundo das relações internacionais, fiquei cada vez mais atraída por ela.

A transição para a cibersegurança foi uma grande mudança para mim. Entrei sem uma sólida formação técnica, tive que aprender muito disso no trabalho e, por meio do aprendizado individualizado em diferentes tipos de cursos, precisei aprender linguagens de programação como Python e SQL, duas das coisas que abordamos neste certificado. Eu precisava aprender uma linguagem totalmente nova sobre o vocabulário das ameaças e os diferentes componentes e como elas se manifestam tecnicamente.

Uma das coisas que eu tive que descobrir logo no início dessa jornada é que tipo de aluno eu era. Eu trabalho melhor com um estilo de aprendizado estruturado. Então, recorrer a muitos desses cursos e recursos on-line que pegaram esse material e o estruturaram, desde os primeiros princípios até o aplicativo, ressoou muito bem para mim.

Muito disso também foi aprendido no trabalho por colegas de trabalho que estavam dispostos a compartilhar e investir tempo para me ajudar a entender isso. Eu fiz muitas perguntas e ainda faço. A maior parte do trabalho de segurança cibernética será aprendida no trabalho, no ambiente específico que você está protegendo. Portanto, você precisa trabalhar bem com seus colegas de equipe para poder construir essa base de conhecimento.

Meu conselho seria manter a curiosidade e continuar aprendendo, especialmente focando em suas habilidades técnicas e desenvolvendo-as ao longo de sua carreira. É muito fácil contrair a síndrome do impostor na segurança cibernética porque ela é muito ampla e o domínio de todas essas áreas diferentes é um trabalho para toda a vida. E às vezes essa síndrome do impostor pode nos paralisar e fazer com que pareça: por que se preocupar em tentar continuar crescendo. Eu nunca vou ser capaz de dominar isso em vez de nos motivar. Então continue aprendendo, supere esse medo. Os esforços sempre serão recompensados.

Here is the translated text in English:

Hello, I’m Toni, and I’m a security engineering manager. Our teams protect Google and its users from serious threats.

Usually, these include government-backed attackers, coordinated influence operations, and major cybercrime threat actors. I grew up as an army brat. My father was in the military, and we moved around a lot. In general, I’ve always been interested in security. I became very passionate about international relations when I was in high school. I participated in many Model United Nations events. And that really brought these two things together for me—the way security works in the world.

I come from a large family. I knew I would need financial assistance to go to college. And the Department of Defense offers many educational opportunities tied to service. So, that was a natural fit for me. I knew I was interested in this field, and it would provide a career path for something I was passionate about.

I started as an intelligence analyst, but I didn’t initially focus on cybersecurity. I worked in counterinsurgency for several years and dealt with geopolitical intelligence issues. Eventually, as I observed how cybersecurity was beginning to impact our daily lives and the world of international relations, I became increasingly drawn to it.

Transitioning to cybersecurity was a big shift for me. I entered the field without a strong technical background, so I had to learn a lot on the job and through self-paced learning in various courses. I needed to learn programming languages like Python and SQL, two of the topics covered in this certificate. I also had to learn a whole new language—the vocabulary of threats, their different components, and how they manifest technically.

One of the first things I had to figure out on this journey was what kind of learner I was. I work best with a structured learning style. So, turning to many of these online courses and resources that structured the material from first principles to application resonated well with me.

A lot of my learning also came from colleagues who were willing to share their knowledge and invest time in helping me understand things. I asked a lot of questions—and I still do. Most of the work in cybersecurity will be learned on the job, in the specific environment you are protecting. So, you need to work well with your teammates to build that knowledge base.

My advice would be to stay curious and keep learning, especially by focusing on and developing your technical skills throughout your career. It’s very easy to experience imposter syndrome in cybersecurity because the field is so vast, and mastering all its different areas is a lifelong endeavor. Sometimes, imposter syndrome can paralyze us, making us feel like, “Why even bother trying to grow? I’ll never be able to master this,” instead of motivating us. So, keep learning, push through that fear. Your efforts will always be rewarded.

**Responsabilidades de um Analista de Segurança Cibernética de nível básico**

A tecnologia está mudando rapidamente, assim como as táticas e técnicas que os atacantes utilizam. Com a evolução da infraestrutura digital, espera-se que os profissionais de segurança aprimorem continuamente suas habilidades para proteger informações confidenciais. Neste vídeo, discutiremos algumas das responsabilidades de um analista de segurança iniciante.

Os analistas de segurança são responsáveis por monitorar e proteger informações e sistemas. Suas principais responsabilidades incluem:

1. **Proteção de computadores e sistemas de rede**  
   Isso envolve monitorar a rede interna da organização. Se uma ameaça for detectada, o analista geralmente é o primeiro a responder. Além disso, eles participam de exercícios para identificar vulnerabilidades nos sistemas da empresa.
2. **Testes de penetração e hacking ético**  
   Os analistas de segurança podem contribuir para testes de penetração, tentando hackear a própria rede da organização para identificar falhas e sugerir melhorias.
3. **Prevenção de ameaças**  
   Trabalham proativamente para evitar que ameaças aconteçam, colaborando com equipes de TI para instalar softwares de prevenção e identificar riscos.
4. **Desenvolvimento de software e hardware**  
   Auxiliam as equipes de desenvolvimento na implementação de processos e sistemas que garantam a segurança dos produtos e a proteção de dados da organização.
5. **Auditorias de segurança**  
   Realizam revisões periódicas dos registros e atividades de segurança da empresa. Isso pode incluir verificar se informações sensíveis, como senhas, estão devidamente protegidas e acessíveis apenas a pessoas autorizadas.

Os analistas de segurança são fundamentais para qualquer organização. Suas tarefas diárias protegem desde pequenas empresas até grandes corporações, além de organizações sem fins lucrativos e agências governamentais, garantindo a segurança das pessoas atendidas por essas instituições.

Here is the translated text in English:

Technology is rapidly changing, as are the tactics and techniques used by attackers. As digital infrastructure evolves, security professionals are expected to continuously enhance their skills to protect sensitive information. In this video, we will discuss some of the responsibilities of a junior security analyst.

Security analysts are responsible for monitoring and protecting information and systems. Their main responsibilities include:

1. **Protection of computers and network systems**  
   This involves monitoring the organization's internal network. If a threat is detected, the analyst is usually the first to respond. Additionally, they participate in exercises to identify vulnerabilities in the company’s systems.
2. **Penetration testing and ethical hacking**  
   Security analysts can contribute to penetration testing by attempting to hack the organization’s own network to identify flaws and suggest improvements.
3. **Threat prevention**  
   They work proactively to prevent threats from occurring, collaborating with IT teams to install prevention software and identify risks.
4. **Software and hardware development**  
   They assist development teams in implementing processes and systems that ensure product security and protect the organization’s data.
5. **Security audits**  
   They conduct periodic reviews of the company's security records and activities. This may include verifying that sensitive information, such as passwords, is properly secured and accessible only to authorized personnel.

Security analysts are essential to any organization. Their daily tasks help protect small businesses, large corporations, nonprofit organizations, and government agencies, ensuring the safety of the people they serve.

**Nikki: Um dia na vida de um engenheiro de segurança**

Meu nome é Nikki e sou engenheira de segurança no Google. Faço parte da equipe de detecção de ameaças internas, focando na identificação de atividades suspeitas dentro da empresa.

Minha primeira experiência com cibersegurança foi durante um estágio em um aquário. Lá, aprendi muito sobre segurança de rede, pois havia muitas tentativas de phishing. Meu gerente estava extremamente focado em garantir a segurança das redes, e essa experiência despertou meu interesse pela área.

O principal motivo pelo qual escolhi seguir uma carreira em segurança cibernética foi a flexibilidade desse campo. Há diversas áreas para explorar, seja na equipe azul, protegendo os usuários, ou na equipe vermelha, testando defesas e identificando falhas.

A rotina de um profissional de segurança iniciante pode variar, mas geralmente envolve duas partes principais. O lado operacional consiste em responder a detecções e conduzir investigações. Já o lado estratégico envolve colaborar com outras equipes para criar novas detecções ou aprimorar as existentes.

A principal diferença entre um analista de segurança cibernética e um engenheiro de segurança cibernética no nível inicial é o foco das atividades. O analista se concentra mais em operações, enquanto o engenheiro, além de atuar nas operações, desenvolve detecções e trabalha em projetos.

Minha parte favorita do trabalho é a investigação, pois me permite analisar atividades suspeitas e determinar se há realmente uma ameaça ou apenas um falso positivo.

Uma das maiores contribuições que fiz como profissional iniciante foi o desenvolvimento de manuais para minha equipe. Esses manuais detalham como realizar detecções e quais aspectos analisar durante uma investigação. Fiquei muito orgulhosa desse trabalho, pois meus colegas destacaram o quanto essas documentações foram úteis.

Se você gosta de resolver problemas, proteger dados dos usuários e atuar na linha de frente da cibersegurança, essa pode ser a carreira ideal para você.

Here is the translated text in English:

My name is Nikki, and I am a security engineer at Google. I am part of the internal threat detection team, focusing on identifying suspicious activities within the company.

My first experience with cybersecurity was during an internship at an aquarium. There, I learned a lot about network security since there were many phishing attempts. My manager was highly focused on ensuring the security of our networks, and that experience sparked my interest in the field.

The main reason I chose a career in cybersecurity was the flexibility it offers. There are many different areas to explore, whether in the blue team, protecting users, or the red team, testing defenses and identifying vulnerabilities.

The daily routine of an entry-level security professional can vary, but it generally consists of two main parts. The operational side involves responding to detections and conducting investigations. The strategic side involves working with other teams to create new detections or improve existing ones.

The key difference between an entry-level cybersecurity analyst and a security engineer is their focus. Analysts concentrate more on operations, while engineers, in addition to working on operations, develop detections and work on projects.

My favorite part of the job is investigation because it allows me to analyze suspicious activities and determine whether there is an actual threat or just a false positive.

One of the biggest contributions I have made as a junior security professional was developing manuals for my team. These manuals outline how to perform detections and what to analyze during an investigation. I am very proud of this work because my colleagues have highlighted how useful these documents have been for them.

If you love solving problems, protecting user data, and being on the front lines of cybersecurity, this could be the perfect career for you.

**Terminologia comum de segurança cibernética**

ASegundo você aprendeu, **a segurança cibernética** (também conhecida como security) é a prática de garantir a confidencialidade, integridade e disponibilidade das informações, protegendo redes de computadores, dispositivos, pessoas e dados contra o acesso não autorizado ou a exploração criminosa. Nesta leitura, você será apresentado a alguns termos-chave usados na profissão de segurança cibernética. Em seguida, você receberá um recurso útil para se manter informado sobre as mudanças na terminologia de segurança cibernética.

**Principais termos e conceitos de segurança cibernética**

Há muitos termos e conceitos que são importantes para os profissionais de segurança conhecerem. Estar familiarizado com eles pode ajudá-lo a identificar melhor as ameaças que podem prejudicar organizações e pessoas. Um analista de segurança ou analista de segurança cibernética concentra-se no monitoramento de redes de computadores em busca de violações. Ele também ajuda a desenvolver Estratégias para proteger uma organização e pesquisa tendências de segurança de tecnologia da informação (TI) para permanecer alerta e informado sobre possíveis ameaças. Além disso, o analista trabalha para evitar incidentes. Para que os analistas realizem esses tipos de tarefas com eficácia, eles precisam desenvolver conhecimentos sobre os seguintes conceitos-chave.

**Conformidade** é o processamento de adesão a padrões internos e regulamentos externos e permite que as organizações evitem multas e violações de segurança.

**Frameworks de segurança** são diretrizes usadas para criar planos que ajudem a reduzir os riscos e as ameaças aos dados e à privacidade dos dados.

**Controles de segurança** são salvaguardas projetadas para reduzir riscos de segurança específicos. Eles são usados com os frameworks de segurança para estabelecer uma postura de segurança forte.

**A postura de segurança** é a capacidade da organização de gerenciar a defesa de recursos e dados críticos e reagir a mudanças. Uma postura de segurança forte leva a um risco menor para a organização.

Um **agente de ameaça**, ou atacante mal-intencionado, é qualquer pessoa ou grupo que represente um risco à segurança. Esse risco pode estar relacionado a computadores, aplicativos, redes e dados.

Uma **ameaça interna** pode ser um funcionário ou ex-funcionário, um fornecedor externo ou um parceiro confiável que represente um risco à segurança. Às vezes, uma ameaça interna é acidental. Por exemplo, um funcionário que clica acidentalmente em um link de e-mail malicioso seria considerado uma ameaça acidental. Outras vezes, o agente da ameaça interna se envolve *intencionalmente* em atividades de risco, como o acesso não autorizado a dados.

**Segurança de rede** é a prática de manter a infraestrutura de rede de uma organização protegida contra acesso não autorizado. Isso inclui dados, serviços, sistemas e dispositivos armazenados na rede de computadores de uma organização.

**Segurança na nuvem** é o processamento para garantir que os recursos armazenados na nuvem sejam configurados ou definidos corretamente, e que o acesso a esses recursos seja limitado a usuários autorizados. A Nuvem é uma rede composta por um conjunto de servidores ou computadores que armazenam recursos e dados em locais físicos remotos, conhecidos como data centers, que podem ser acessados pela Internet. A Segurança na nuvem é um subcampo crescente da segurança cibernética que se concentra especificamente na proteção de dados, aplicativos e infraestrutura na nuvem.

**Programação** é um processamento que pode ser usado para criar um conjunto específico de instruções para um computador executar tarefas. Essas tarefas podem incluir:

* Automação de tarefas repetitivas (por exemplo, pesquisar uma lista de domínios maliciosos)
* Análise do Tráfego da Web
* Alerta de atividades suspeitas

**Principais lições**

Compreender as chaves dos termos e conceitos técnicos usados no Campo de Segurança ajudará a prepará-lo para sua função de analista de segurança. O conhecimento desses termos pode ajudá-lo a identificar ameaças, riscos e vulnerabilidades comuns. Para explorar uma variedade de termos de segurança cibernética, visite o [glossário do National Institute of Standards and Technology](https://csrc.nist.gov/glossary). Ou use seu navegador para pesquisar glossários de segurança cibernética confiáveis e de alta qualidade de institutos de pesquisa ou autoridades governamentais. Os glossários estão disponíveis em vários idiomas.

**Habilidades Essenciais para Profissionais de Segurança Cibernética**

Para qualquer trabalho, certas habilidades são necessárias para o sucesso, e muitas dessas habilidades são transferíveis de uma função para outra. Independentemente do trabalho atual, você provavelmente já possui diversas habilidades essenciais. Ter uma formação diversificada aprimora essas habilidades, tornando suas experiências e perspectivas pessoais especialmente valiosas.

Neste vídeo, serão discutidas tanto as habilidades transferíveis quanto as habilidades técnicas que são particularmente úteis para um analista de segurança.

**Habilidades Transferíveis**

Habilidades transferíveis são competências adquiridas em outras áreas que podem ser aplicadas a diferentes carreiras.

Uma dessas habilidades é a comunicação. Analistas de segurança frequentemente precisam descrever ameaças, riscos ou vulnerabilidades para pessoas que podem não ter um conhecimento técnico. Eles também podem ser responsáveis por interpretar e comunicar políticas e procedimentos a outros funcionários ou por relatar descobertas aos seus supervisores para que as ações apropriadas sejam tomadas.

Outra habilidade essencial é a colaboração. Analistas de segurança costumam trabalhar em equipes com engenheiros, investigadores forenses digitais e gerentes de projetos. Por exemplo, ao implementar um novo recurso de segurança, é comum trabalhar com um gerente de projeto, um engenheiro e um hacker ético.

A capacidade de analisar cenários complexos também é fundamental. Um analista de segurança pode precisar recomendar como diferentes ferramentas podem aumentar a eficiência e proteger a rede interna de uma organização.

Por fim, a resolução de problemas é uma habilidade essencial. Identificar um problema de segurança, diagnosticá-lo e propor soluções são passos necessários para manter as operações comerciais seguras. Entender os agentes de ameaças e identificar padrões pode ajudar a lidar com ameaças futuras.

**Habilidades Técnicas**

Agora que as habilidades transferíveis foram abordadas, é importante discutir algumas habilidades técnicas que os analistas de segurança devem desenvolver.

Uma compreensão básica de linguagens de programação é essencial, pois os analistas de segurança podem utilizá-las para automatizar tarefas e identificar mensagens de erro. Assim como aprender qualquer outro idioma, o aprendizado de uma linguagem de programação pode parecer desafiador no início. No entanto, este programa não exige experiência prévia em programação e oferece várias oportunidades de prática com linguagens como Python e SQL.

Outra habilidade técnica importante é o uso de ferramentas de gerenciamento de informações e eventos de segurança (SIEM). Profissionais de segurança utilizam essas ferramentas para identificar e analisar ameaças, riscos e vulnerabilidades. Por exemplo, uma ferramenta SIEM pode alertar sobre um usuário desconhecido acessando o sistema, e o analista pode usar a informática forense para investigar o incidente.

A informática forense é uma área essencial. Assim como um investigador e um cientista forense no sistema de justiça criminal, investigadores forenses digitais tentam identificar, analisar e preservar evidências criminais dentro de redes, computadores e dispositivos eletrônicos.

**Conclusão**

É importante lembrar que você pode já possuir algumas das habilidades essenciais discutidas. Se ainda não possui as habilidades técnicas, não há problema! Este programa foi projetado para ajudá-lo a desenvolvê-las.

Por exemplo, ao longo dos últimos sete anos trabalhando em segurança cibernética, aprendi que analistas de segurança precisam ter curiosidade intelectual e motivação para continuar aprendendo. Pessoalmente, dedico tempo regularmente para aprimorar minhas habilidades em Python e SQL, pois elas são fundamentais para os projetos em que estou envolvido. Você terá a oportunidade de aprender sobre essas linguagens ao longo deste programa.

À medida que avança nesta jornada, você desenvolverá os conhecimentos e habilidades necessários para ingressar na área de segurança cibernética.

**Essential Skills for Cybersecurity Professionals**

For any job, certain skills are necessary for success, and many of these core skills are transferable from one role to another. Regardless of your current job, you likely already have many essential skills. Having a diverse background enhances these skills, making your personal experiences and perspectives especially valuable.

In this video, we will discuss both transferable and technical skills that are particularly useful for a security analyst.

**Transferable Skills**

Transferable skills are competencies acquired in other areas that can be applied to different careers.

One such skill is communication. Security analysts often need to describe threats, risks, or vulnerabilities to people who may not have a technical background. They may also be responsible for interpreting and communicating policies and procedures to other employees or reporting findings to their supervisors so that appropriate actions can be taken.

Another essential skill is collaboration. Security analysts frequently work in teams with engineers, digital forensic investigators, and project managers. For example, when implementing a new security feature, it is common to work with a project manager, an engineer, and an ethical hacker.

The ability to analyze complex scenarios is also crucial. A security analyst may need to recommend how different tools can enhance efficiency and protect an organization's internal network.

Lastly, problem-solving is an essential skill. Identifying a security problem, diagnosing it, and proposing solutions are necessary steps to keep business operations secure. Understanding threat actors and identifying patterns can help address future threats.

**Technical Skills**

Now that we have covered transferable skills, it is important to discuss some technical skills that security analysts should develop.

A basic understanding of programming languages is essential, as security analysts can use programming to automate tasks and identify error messages. Just like learning any other language, learning a programming language may seem challenging at first. However, this program does not require prior programming experience and offers several opportunities for hands-on practice with languages such as Python and SQL.

Another important technical skill is using Security Information and Event Management (SIEM) tools. Security professionals use these tools to identify and analyze threats, risks, and vulnerabilities. For example, a SIEM tool may alert you that an unknown user has accessed the system, and the analyst can use computer forensics to investigate the incident.

Computer forensics is a crucial field. Similar to an investigator and forensic scientist in the criminal justice system, digital forensic investigators attempt to identify, analyze, and preserve criminal evidence within networks, computers, and electronic devices.

**Conclusion**

It is important to remember that you may already possess some of the essential skills discussed. If you do not yet have the technical skills, that is okay! This program is designed to help you develop them.

For example, over the past seven years working in cybersecurity, I have learned that security analysts need intellectual curiosity and the motivation to keep learning. Personally, I regularly dedicate time to improving my Python and SQL skills, as they are fundamental to the projects I am involved in. You will have the opportunity to learn about these languages throughout this program.

As you continue this journey, you will build the knowledge and skills needed to enter the cybersecurity field.

**Verônica: Meu caminho para trabalhar com segurança cibernética**

Oi, eu sou a Veronica e sou engenheira de segurança no Google.

**Minha Jornada na Cibersegurança**

Minha jornada na cibersegurança mudou minha vida para melhor de muitas formas. A parte mais importante é ter um trabalho gratificante. Eu posso fazer algo que amo e que realmente me interessa, e me sinto muito sortuda por esse ser o meu trabalho.

Antes de entrar nessa área, eu não fazia ideia do que era cibersegurança. Meu conhecimento se resumia a usar senhas seguras, e só. Se alguém tivesse me perguntado há cinco anos se eu trabalharia com cibersegurança, minha resposta teria sido: "O que é isso?"

**Entrando na Cibersegurança Sem um Background Técnico**

Alguém sem formação técnica pode, com certeza, ter sucesso na cibersegurança. Minha trajetória começou como residente de TI no Google, trabalhando no Techstop. Lá, desenvolvi habilidades de pensamento analítico enquanto solucionava problemas, depurava sistemas e dava suporte técnico.

No início, eu não percebia que possuía habilidades transferíveis. Mas, quando entrei na cibersegurança, tomei a iniciativa de conversar com engenheiros de segurança, entrevistá-los e aprender com suas experiências. Eu não cheguei aqui sozinha—foi preciso um grupo de mentores para me ajudar, então não tenha medo de pedir ajuda.

**A Importância da Educação e Superando o Perfeccionismo**

Eu não acho que um diploma universitário seja necessário para entrar na cibersegurança. Algumas das mentes mais brilhantes com quem trabalho não têm um diploma, e acho que isso é uma das melhores coisas dessa indústria.

Olhando para minha carreira, gostaria de ter sabido antes que eu não precisava preencher todos os requisitos ou ser uma especialista na área para tentar. Também gostaria de ter percebido mais cedo que o perfeccionismo pode, às vezes, atrapalhar a realização dos nossos objetivos.

Here is the translated text in English:

Hi, I'm Veronica, and I'm a security engineer at Google.

**My Journey into Cybersecurity**

My journey into cybersecurity has changed my life for the better in many ways. The most important part is having fulfilling work. I get to do something that I absolutely love and that I’m deeply interested in, and I feel very lucky that this is my job.

Before entering this field, I had no idea what cybersecurity was. My knowledge was limited to using secure passwords, and that was about it. If you had asked me five years ago if I would be in cybersecurity, I would have responded, "What is that?"

**Breaking into Cybersecurity Without a Technical Background**

Someone without a technical background can 100% be successful in cybersecurity. My journey began as an IT resident at Google, working in Techstop. There, I developed analytical thinking skills while troubleshooting, debugging, and providing help desk support.

At first, I didn’t realize I had transferable skills. But once I got into cybersecurity, I took the initiative to connect with security engineers, interview them, and learn from their experiences. I didn’t get here alone—it took a village of mentors to help me, so don’t be afraid to ask for help.

**The Importance of Education and Overcoming Perfectionism**

I don’t believe a college degree is necessary to enter cybersecurity. Some of the brightest professionals I work with don’t have a degree, and I think that’s one of the best aspects of this industry.

Looking back at my career, I wish I had known that I didn’t have to check all the boxes or be an expert in the field before taking my shot. I also wish I had realized earlier that perfectionism can sometimes stand in the way of achieving your goals.

**Habilidades transferíveis e técnicas de segurança cibernética**

Anteriormente, você aprendeu que os analistas de segurança cibernética precisam desenvolver certas habilidades essenciais para serem bem-sucedidos no trabalho. **Habilidades transferíveis** são habilidades de outras áreas de estudo ou prática que podem ser aplicadas a diferentes carreiras. **As habilidades técnicas** também podem se aplicar a várias profissões; entretanto, elas normalmente exigem conhecimento de ferramentas, procedimentos e políticas específicos. Nesta leitura, você explorará mais a fundo as habilidades transferíveis e as habilidades técnicas.

**Habilidades transferíveis**

Você provavelmente desenvolveu muitas habilidades transferíveis por meio de experiências de vida; algumas dessas habilidades o ajudarão a prosperar como profissional de segurança cibernética. Entre elas estão:

* **Comunicação:** Como analista de segurança cibernética, você precisará se comunicar e colaborar com outras pessoas. Compreender as dúvidas ou preocupações dos outros e comunicar as informações com clareza a pessoas com conhecimento técnico e não técnico o ajudará a mitigar rapidamente os problemas de segurança.
* **Resolução de problemas:** Uma de suas principais tarefas como analista de segurança cibernética será identificar e resolver problemas de forma proativa. Você pode fazer isso reconhecendo padrões de ataque e, em seguida, determinando a solução mais eficiente para minimizar os riscos. Não tenha medo de correr riscos e tentar coisas novas. Além disso, entenda que é raro encontrar uma solução perfeita para um problema. Provavelmente, você precisará fazer concessões.
* **Gerenciamento de tempo:** Ter um senso de urgência elevado e priorizar as tarefas adequadamente é essencial no Campo da segurança cibernética. Portanto, o gerenciamento eficaz do tempo o ajudará a minimizar os possíveis danos e riscos aos recursos e dados críticos. Além disso, será importante priorizar as tarefas e manter o foco no problema mais urgente.
* **Mentalidade de crescimento:** Este é um setor em evolução, portanto, uma importante Habilidade transferível é a disposição para aprender. A tecnologia avança rapidamente, e isso é ótimo! Isso não significa que você precisará aprender tudo, mas sim que precisará continuar aprendendo ao longo de sua carreira. Felizmente, você poderá aplicar muito do que aprendeu neste programa ao seu desenvolvimento profissional contínuo.
* **Diversidade de perspectivas:** A única maneira de ir longe é juntos. Respeitando uns aos outros e incentivando perspectivas diversas e respeito mútuo, sem dúvida, você encontrará várias e melhores soluções para os problemas de segurança.

**Habilidades técnicas**

Há muitas habilidades técnicas que o ajudarão a ter sucesso no Campo da segurança cibernética. Você aprenderá e praticará essas habilidades à medida que avança no programa de certificação. Algumas das ferramentas e conceitos que você precisará usar e entender incluem

* **Linguagens de programação:** Ao compreender como usar linguagens de programação, os analistas de segurança cibernética podem automatizar tarefas que, de outra forma, seriam muito demoradas. Exemplos de tarefas em que a programação pode ser usada incluem a pesquisa de dados para identificar possíveis ameaças ou a organização e análise de informações para identificar padrões relacionados a problemas de segurança.
* **Ferramentas de gerenciamento de eventos e informações de segurança (SIEM):** As ferramentas SIEM coletam e analisam dados de registros, ou registros de eventos, como comportamento incomum de login, e dão suporte à capacidade dos analistas de monitorar atividades críticas em uma organização. Isso ajuda os profissionais de segurança cibernética a identificar e analisar possíveis ameaças à segurança, Riscos e vulnerabilidades com mais eficiência.
* **Sistemas de detecção de intrusão (IDSs):** Os analistas de segurança cibernética usam IDSs para monitorar a atividade do sistema e alertas de possíveis intrusões. É importante familiarizar-se com os IDSs porque eles são uma ferramenta chave que toda organização usa para proteger recursos e dados. Por exemplo, você pode usar um IDS para monitorar as redes em busca de sinais de atividade mal-intencionada, como acesso não autorizado a uma rede.
* **Conhecimento do cenário de ameaças:** É fundamental estar ciente das tendências atuais relacionadas a agentes de ameaças, malware ou metodologias de ameaças. Esse conhecimento permite que as Equipes de segurança criem defesas mais fortes contra táticas e técnicas de agentes de ameaças. Ao se manterem atualizados sobre as tendências e os padrões de ataque, os profissionais de segurança são mais capazes de reconhecer quando surgem novos tipos de ameaças, como uma nova variante de ransomware.
* **Resposta a incidentes:** Os analistas de segurança cibernética precisam ser capazes de seguir políticas e procedimentos estabelecidos para responder a incidentes de forma adequada. Por exemplo, um analista de segurança pode receber um alerta sobre um possível ataque de malware e, em seguida, seguir os procedimentos delineados pela organização para iniciar o processamento de resposta a incidentes. Isso pode envolver a realização de uma investigação para identificar a raiz do problema e estabelecer maneiras de corrigi-lo.

**CompTIA Security+**

Além de adquirir habilidades que o ajudarão a ter sucesso como profissional de segurança cibernética, o Certificado de segurança cibernética do Google ajuda a prepará-lo para o [exame CompTIA Security+](https://www.comptia.org/certifications/security), a certificação líder do setor para funções de segurança cibernética. Ao concluir ambos os cursos, você receberá uma credencial dupla, que poderá ser compartilhada com possíveis empregadores. Após concluir todos os oito cursos do Certificado de segurança cibernética do Google, você receberá um desconto de 30% para o exame CompTIA Security+ e materiais práticos adicionais.

**Principais lições**

Compreender os Benefícios das principais Habilidades transferíveis e técnicas pode ajudar a prepará-lo para entrar com sucesso na força de trabalho de segurança cibernética. Ao longo deste programa, você terá várias oportunidades de desenvolver essas e outras habilidades chave de analista de segurança cibernética.

**A importância da segurança cibernética**

Aqui está o texto organizado e sem os números:

**A Importância da Segurança Cibernética**

Profissionais de segurança protegem diversos ativos físicos e digitais. Essas habilidades são valorizadas por organizações e entidades governamentais porque a gestão de riscos é essencial. Vamos continuar explorando por que a segurança é tão importante.

A segurança é fundamental para garantir a continuidade dos negócios e a integridade ética das organizações. Existem implicações legais e considerações morais na manutenção da segurança. Uma violação de dados, por exemplo, afeta todos os envolvidos com a organização, prejudicando sua reputação e a confiança de clientes e usuários. Medidas de segurança eficazes aumentam a confiança do usuário, o que pode levar ao crescimento financeiro e à fidelização de clientes.

As organizações não são as únicas prejudicadas em caso de vazamento de dados. Proteger as informações de usuários, clientes e fornecedores é essencial para evitar a exposição de informações pessoais identificáveis.

Informações pessoais identificáveis (PII) são qualquer dado que possa ser usado para identificar uma pessoa, como nome completo, data de nascimento, endereço, telefone, e-mail e endereço de IP.

Informações pessoais identificáveis sensíveis (SPII) são um tipo específico de PII que exige diretrizes mais rigorosas de proteção. Isso inclui números de segurança social, dados médicos ou financeiros e biometria, como reconhecimento facial. O roubo de SPII pode causar danos ainda mais graves do que o de PII comum.

PII e SPII são alvos prioritários para invasores durante uma violação de dados. Quando essas informações são comprometidas, vazadas ou roubadas, o risco principal é o roubo de identidade.

O roubo de identidade consiste no uso indevido de informações pessoais para cometer fraudes, geralmente com o objetivo de obter ganhos financeiros.

Exploramos várias razões pelas quais a segurança cibernética é essencial. Empresas precisam de analistas de segurança para proteger dados, produtos e pessoas, garantindo a confidencialidade, integridade e acesso seguro às informações. Por isso, o Bureau de Estatísticas do Trabalho dos EUA prevê que a demanda por profissionais de segurança crescerá mais de 30% até 2030.

Continue aprendendo e, com o tempo, você poderá contribuir para um ambiente mais seguro para organizações e pessoas!

Security professionals protect various physical and digital assets. These skills are valued by organizations and government entities because risk management is essential. Let’s continue exploring why security is so important.

Security is crucial for ensuring an organization’s business continuity and ethical standing. There are legal implications and moral considerations in maintaining security. A data breach, for example, affects everyone associated with the organization, damaging its reputation and the trust of clients and users. Effective security measures increase user trust, which can lead to financial growth and customer loyalty.

Organizations are not the only ones harmed in a data breach. Protecting user, customer, and vendor information is crucial to prevent the exposure of personally identifiable information.

Personally identifiable information (PII) is any data used to identify a person, such as full name, date of birth, address, phone number, email address, and IP address.

Sensitive personally identifiable information (SPII) is a specific type of PII that requires stricter handling guidelines. This includes social security numbers, medical or financial data, and biometric information like facial recognition. The theft of SPII can cause significantly more harm than the theft of regular PII.

PII and SPII are key targets for attackers during a data breach. When this information is compromised, leaked, or stolen, identity theft becomes the primary concern.

Identity theft is the act of stealing personal information to commit fraud, typically with the goal of financial gain.

We have explored several reasons why security matters. Employers need security analysts to protect data, products, and people while ensuring confidentiality, integrity, and secure access to information. This is why the U.S. Bureau of Labor Statistics expects the demand for security professionals to grow by more than 30% by 2030.

Keep learning, and over time, you’ll be able to contribute to a safer and more secure environment for organizations and people alike!

**Aprenda a manter as organizações seguras**  
Selecione o rótulo em cada infográfico para aprender sobre as habilidades que um analista de segurança pode usar no trabalho para ajudar a manter uma organização segura.

**Pensamento Analítico**  
Os analistas de segurança frequentemente usam o pensamento analítico, que significa pensar de forma cuidadosa e detalhada. Eles aplicam essa habilidade ao monitorar e proteger sistemas de computador e redes, responder a ameaças potenciais, definir privilégios de sistema e determinar maneiras de mitigar riscos.

**Colaboração**  
Colaboração significa trabalhar com partes interessadas e outros membros da equipe. Os analistas de segurança frequentemente usam essa habilidade ao responder a uma ameaça ativa. Eles trabalham com outros para bloquear acessos não autorizados e garantir que sistemas comprometidos sejam restaurados.

**Prevenção de Malware**  
Quando uma ameaça ou vulnerabilidade específica é identificada, um analista pode instalar um software de prevenção, que é um software que trabalha para prevenir proativamente que uma ameaça aconteça. Como o malware é projetado para prejudicar dispositivos ou redes, a prevenção de malware é essencial.

**Comunicação**  
À medida que o analista previne e encontra ameaças, riscos ou vulnerabilidades, ele documenta e relata suas descobertas. Um relatório pode detalhar tentativas de proteger sistemas, testar pontos fracos ou oferecer soluções para melhoria de sistemas. Habilidades de comunicação fortes são importantes ao relatar as descobertas.

**Compreensão de Linguagens de Programação**  
Os analistas podem, às vezes, trabalhar com equipes de desenvolvimento de software para analisar e apoiar a segurança, instalar software e configurar processos apropriados. Quando envolvidos em projetos de desenvolvimento de software, pode ser útil para um analista entender linguagens de programação.

**Uso de Ferramentas SIEM**  
Quando os analistas de segurança precisam revisar vulnerabilidades, eles realizam uma auditoria de segurança periódica. Isso envolve a revisão dos registros, atividades e documentos relacionados de uma organização. Durante as auditorias, as ferramentas de Gerenciamento de Informações e Eventos de Segurança (SIEM) ajudam os analistas a entender melhor as ameaças, riscos e vulnerabilidades de segurança.

**Você Concluiu!**  
Analistas de segurança iniciantes executarão uma variedade de tarefas no trabalho, e várias habilidades transferíveis podem ajudar um analista a concluir com sucesso essas tarefas.

**Aprenda a manter as organizações seguras**  
Selecione o rótulo em cada infográfico para aprender sobre as habilidades que um analista de segurança pode usar no trabalho para ajudar a manter uma organização segura.

**Learn to Keep Organizations Secure**  
Select the label in each infographic to learn about the skills a security analyst may use on the job to help keep an organization secure.

**Analytical Thinking**  
Security analysts often use analytical thinking, which involves thinking carefully and thoroughly. Analysts apply this skill when monitoring and securing computer and network systems, responding to potential threats, defining system privileges, and determining ways to mitigate risks.

**Collaboration**  
Collaboration means working with stakeholders and other team members. Security analysts often use this skill when responding to an active threat. They work with others to block unauthorized access and ensure any compromised systems are restored.

**Malware Prevention**  
When a specific threat or vulnerability is identified, an analyst might install prevention software to proactively prevent a threat. Since malware is designed to harm devices or networks, malware prevention is essential.

**Communication**  
As an analyst encounters and prevents threats, risks, or vulnerabilities, they document and report their findings. A report might detail attempts to secure systems, test weak points, or suggest solutions for system improvement. Strong communication skills are important when reporting findings.

**Understanding Programming Languages**  
Analysts may sometimes work with software development teams to analyze and support security, install software, and set up appropriate processes. An understanding of programming languages is helpful when involved with software development projects.

**Using SIEM Tools**  
When security analysts need to review vulnerabilities, they conduct periodic security audits. These reviews examine an organization’s records, activities, and related documents. During audits, Security Information and Event Management (SIEM) tools help analysts better understand security threats, risks, and vulnerabilities.

You’re Done!  
Entry-level security analysts will perform a range of tasks on the job. Several transferable skills can help an analyst successfully complete these tasks.

**Finalização**

Parabéns por concluir a primeira seção deste curso! Vamos revisar rapidamente o que cobrimos até agora, antes de seguir em frente.

Definimos segurança e apresentamos os benefícios de implementar segurança em uma organização. Em seguida, discutimos diferentes responsabilidades de trabalho, como gerenciar ameaças e instalar software de prevenção. Também introduzimos algumas habilidades essenciais, como colaboração e forense computacional. Terminamos discutindo o valor da segurança e como ela apoia funções críticas de negócios.

Espero que você tenha adquirido uma maior compreensão sobre segurança. Se achar necessário, pode sempre voltar e revisar qualquer conteúdo com o qual não esteja totalmente seguro.

Ao aprender o básico, você está estabelecendo a base para o restante da sua carreira em segurança.

A seguir, exploraremos alguns ataques bem conhecidos que moldaram a indústria de segurança. Estou empolgado para continuar essa jornada com você!

**Termos do glossário do Módulo 1**

**Termos e definições do Curso 1, Módulo 1**

**Segurança cibernética (ou segurança): A prática de garantir a confidencialidade, a integridade e a disponibilidade das informações, protegendo redes, dispositivos, pessoas e dados contra o acesso não autorizado ou a exploração criminosa**

**Segurança na nuvem: O processamento para garantir que os recursos armazenados na Nuvem sejam configurados adequadamente e que o acesso a esses recursos seja limitado a usuários autorizados**

**Ameaça interna: Um funcionário ou ex-funcionário, um fornecedor externo ou um parceiro confiável que represente um Risco à segurança**

**Segurança de rede: A prática de manter a infraestrutura de rede de uma organização protegida contra acesso não autorizado**

**Informações de identificação pessoal (PII): Qualquer informação usada para inferir a identidade de um indivíduo**

**Postura de segurança: A capacidade de uma organização de gerenciar sua defesa de recursos e dados críticos e reagir a mudanças**

**Informações sensíveis de identificação pessoal (SPII): Um tipo específico de PII que se enquadra em diretrizes de manuseio mais rigorosas**

**Habilidades técnicas: Habilidades que exigem conhecimento de ferramentas, procedimentos e políticas específicas.**

**Ameaça: Qualquer circunstância ou evento que possa afetar negativamente os recursos**

**Ator da ameaça: Qualquer pessoa ou grupo que apresente um Risco à segurança**

**Habilidades transferíveis: Habilidades de outras áreas que podem ser aplicadas a diferentes carreiras**

**Módulo 2**

Congratulations on completing the first section of this course! Let's quickly review what we've covered so far, before moving on.

We defined security and introduced the benefits of implementing security in an organization. Then, we discussed different job responsibilities, such as managing threats and installing prevention software. We also introduced some important core skills, like collaboration and computer forensics. We finished by discussing the value of security and how it supports critical business functions.

I hope you've gained a greater understanding of security. If you feel like you need a refresher before moving on, you can always go back and review any content you're unsure about.

By learning the basics, you are laying the foundation for the rest of your security career.

Coming up, we'll explore some well-known attacks that shaped the security industry. I'm excited to continue this journey with you!

**Bem-vindo ao Módulo 2**

Bem-vindo de volta! Quando se trata de segurança, há muito o que aprender, e estou empolgado por fazer parte da sua jornada profissional.

Este é um momento incrível para aprender sobre segurança! Quando soube de ataques internacionais que impactaram tanto empresas privadas quanto organizações governamentais, fiquei inspirado a trabalhar com segurança porque percebi o quão dinâmica e importante essa área é.

Um dos motivos pelos quais há tantas vagas na área de segurança atualmente é devido a ataques que ocorreram nas décadas de 1980 e 1990. Décadas depois, os profissionais de segurança ainda trabalham ativamente para proteger organizações e pessoas contra variações desses primeiros ataques cibernéticos.

Nesta seção do curso, discutiremos vírus e malware e apresentaremos o conceito de engenharia social. Em seguida, falaremos sobre como a era digital inaugurou uma nova geração de agentes de ameaça. Conhecer a evolução de cada ataque é essencial para se proteger contra futuras ameaças. Por fim, forneceremos uma visão geral de oito domínios de segurança.

A seguir, voltaremos no tempo para explorar alguns dos vírus, vazamentos de dados e ataques de malware que ajudaram a moldar a indústria como a conhecemos hoje.

Welcome back! When it comes to security, there is so much to learn, and I'm thrilled to be part of your career journey.

This is such an exciting time to be learning about security! When I learned about international hacks that impacted both private companies and government organizations, I was inspired to want to work in security because I realized how dynamic and important this field is.

One reason there are so many jobs in the security field today is because of attacks that happened in the 1980s and 1990s. Decades later, security professionals are still actively working to protect organizations and people from variations of these early computer attacks.

In this section of the course, we'll discuss viruses and malware and introduce the concept of social engineering. Then, we'll discuss how the digital age ushered in a new era of threat actors. Knowing the evolution of each attack is key to protecting against future attacks. Lastly, we'll provide an overview of eight security domains.

Next up, we'll travel back in time to explore some of the viruses, data breaches, and malware attacks that have helped shape the industry as we know it today.

**Ataques anteriores de segurança cibernética**

A indústria de segurança está em constante evolução, mas muitos ataques atuais não são totalmente novos. Os invasores frequentemente modificam ou aprimoram métodos anteriores. Compreender ataques do passado pode fornecer direções sobre como lidar com incidentes ou investigá-los no seu trabalho como analista de segurança.

Primeiro, vamos revisar alguns termos essenciais que ajudarão no entendimento dos ataques que discutiremos. Um vírus de computador é um código malicioso escrito para interferir nas operações do computador e causar danos a dados e softwares. Ele se anexa a programas ou documentos em um computador, espalhando-se e infectando outras máquinas em uma rede. Atualmente, os vírus são mais comumente chamados de malware, que é um software projetado para prejudicar dispositivos ou redes. Dois exemplos iniciais de ataques de malware que abordaremos são o vírus Brain e o worm Morris.

Esses programas foram criados por desenvolvedores de malware para realizar tarefas específicas. No entanto, os criadores subestimaram o impacto que seu malware teria e a quantidade de computadores que seriam infectados. Vamos examinar esses ataques mais de perto e discutir como eles ajudaram a moldar a segurança como a conhecemos hoje.

Em 1986, os irmãos Alvi criaram o vírus Brain. Embora a intenção fosse rastrear cópias ilegais de um software médico e impedir licenças pirateadas, o que o vírus realmente fez foi inesperado. Quando alguém usava uma cópia pirata do software, o computador era infectado. Qualquer disco inserido nessa máquina também era contaminado. Assim, toda vez que um desses discos infectados era usado em outro computador, o vírus se espalhava. Sem ser detectado, ele se disseminou globalmente em poucos meses. Apesar de não ter sido criado para destruir dados ou hardware, o vírus reduziu a produtividade e impactou significativamente as operações empresariais.

O vírus Brain mudou fundamentalmente a indústria da computação, destacando a necessidade de um plano para manter a segurança e a produtividade. Como analista de segurança, você seguirá e manterá estratégias para garantir que sua organização tenha um plano eficaz para proteger seus dados e funcionários. Outro ataque de grande impacto foi o worm Morris.

Em 1988, Robert Morris desenvolveu um programa para avaliar o tamanho da internet. Esse programa percorria a web e se instalava em outros computadores para contar quantas máquinas estavam conectadas. Parece simples, certo? No entanto, o programa não conseguia rastrear os computadores já comprometidos e continuava a se reinstalar até que os sistemas ficassem sem memória e travassem. Aproximadamente 6.000 computadores foram afetados, representando 10% da internet da época. Esse ataque causou milhões de dólares em prejuízos devido à interrupção dos negócios e aos esforços necessários para remover o worm.

Após o ataque do worm Morris, foram criadas as Equipes de Resposta a Emergências Computacionais, conhecidas como CERTs®, para responder a incidentes de segurança. Hoje, os CERTs ainda existem, mas suas funções foram ampliadas para incluir mais responsabilidades no setor de segurança. Mais adiante neste programa, você aprenderá mais sobre as funções essenciais dessas equipes e terá a oportunidade de praticar com ferramentas de detecção e resposta.

Os primeiros ataques desempenharam um papel fundamental na formação da indústria de segurança como a conhecemos. A seguir, discutiremos como os ataques evoluíram na era digital.

The security industry is constantly evolving, but many present-day attacks are not entirely new. Attackers often modify or enhance previous methods. Understanding past attacks can provide guidance on how to handle or investigate incidents in your role as a security analyst.

First, let's review some key terms that will help you understand the attacks we will discuss. A computer virus is malicious code designed to interfere with computer operations and cause damage to data and software. It attaches itself to programs or documents on a computer, spreading and infecting other machines in a network. Today, viruses are more commonly referred to as malware, which is software designed to harm devices or networks. Two early examples of malware attacks that we will cover are the Brain virus and the Morris worm.

These programs were created by malware developers to perform specific tasks. However, the creators underestimated the impact their malware would have and the number of computers that would be infected. Let's take a closer look at these attacks and discuss how they helped shape security as we know it today.

In 1986, the Alvi brothers created the Brain virus. Although the intention was to track illegal copies of medical software and prevent pirated licenses, the actual effect of the virus was unexpected. When someone used a pirated copy of the software, their computer became infected. Any disk inserted into that machine was also contaminated. As a result, every time one of these infected disks was used in another computer, the virus spread. Undetected, it disseminated globally within a few months. Although it was not designed to destroy data or hardware, the virus reduced productivity and significantly impacted business operations.

The Brain virus fundamentally changed the computing industry, highlighting the need for a plan to maintain security and productivity. As a security analyst, you will follow and implement strategies to ensure your organization has an effective plan to protect its data and employees. Another highly impactful attack was the Morris worm.

In 1988, Robert Morris developed a program to assess the size of the internet. This program crawled the web and installed itself on other computers to count how many machines were connected. Sounds simple, right? However, the program failed to track the computers it had already compromised and continued reinstalling itself until systems ran out of memory and crashed. Approximately 6,000 computers were affected, representing 10% of the internet at the time. This attack caused millions of dollars in damages due to business disruptions and the efforts required to remove the worm.

Following the Morris worm attack, Computer Emergency Response Teams, known as CERTs®, were established to respond to security incidents. Today, CERTs still exist, but their role in the security industry has expanded to include more responsibilities. Later in this program, you will learn more about the core functions of these security teams and gain hands-on experience with detection and response tools.

Early attacks played a key role in shaping the security industry as we know it. Up next, we will discuss how attacks have evolved in the digital age.

**Ataques na era digital**

Onel De Guzman criou o malware LoveLetter para roubar credenciais de login na internet. Esse ataque se espalhou rapidamente e explorou pessoas que não tinham o hábito de desconfiar de e-mails não solicitados. Os usuários recebiam um e-mail com o assunto **"I Love You"**, contendo um anexo chamado **"Love Letter For You"**. Ao abrir o anexo, o malware escaneava o catálogo de endereços do usuário e se enviava automaticamente para todos os contatos da lista. Além disso, ele instalava um programa para coletar informações e senhas. As vítimas acreditavam estar recebendo um e-mail de um amigo, mas, na realidade, tratava-se de um ataque. O LoveLetter acabou infectando 45 milhões de computadores no mundo todo, causando um prejuízo estimado em mais de 10 bilhões de dólares. Esse ataque foi um dos primeiros exemplos de **engenharia social**.

A **engenharia social** é uma técnica de manipulação que explora o erro humano para obter informações privadas, acesso indevido ou bens valiosos. Após o LoveLetter, os invasores perceberam o poder da engenharia social. Com o crescimento das redes sociais e o compartilhamento de informações públicas, os ataques desse tipo se tornaram ainda mais comuns. Muitas pessoas priorizam a conveniência em vez da privacidade, tornando-se mais vulneráveis a ataques se não utilizarem essas ferramentas com cautela.

Como profissional de segurança, sua função será identificar e gerenciar o uso inadequado da tecnologia, que pode colocar sua organização e seus membros em risco. Uma das formas de proteger a empresa é realizar treinamentos internos regulares, nos quais você, como futuro analista de segurança, pode ser chamado a liderar ou participar.

Hoje em dia, é comum que funcionários sejam treinados para identificar ataques de engenharia social, principalmente **phishing** em e-mails. O **phishing** consiste no uso de comunicações digitais para enganar as pessoas e fazê-las revelar dados sensíveis ou instalar software malicioso.

Outro ataque marcante foi a **violação de dados da Equifax**. Em 2017, hackers invadiram a agência de crédito Equifax, resultando em um dos maiores vazamentos de informações sensíveis da história. Mais de 143 milhões de registros de clientes foram roubados, afetando aproximadamente 40% da população dos Estados Unidos.

Os dados comprometidos incluíam informações pessoais como números de seguridade social, datas de nascimento, números de carteira de motorista, endereços residenciais e informações de cartões de crédito. Do ponto de vista da segurança, a invasão ocorreu devido a múltiplas falhas por parte da Equifax. Os invasores exploraram diversas vulnerabilidades que a empresa não corrigiu nos meses anteriores ao ataque.

No final, a Equifax fechou um acordo com o governo dos Estados Unidos e pagou mais de 575 milhões de dólares em multas e indenizações aos clientes afetados. Esse caso alertou empresas sobre o impacto financeiro de uma violação de dados e a necessidade de implementar medidas preventivas.

Esses são apenas alguns exemplos de incidentes que moldaram a indústria da segurança. Conhecê-los ajudará em sua carreira. Compreender diferentes tipos de malware e ataques de engenharia social permitirá que você se comunique melhor sobre riscos de segurança durante entrevistas de emprego.

Como futuro profissional da área, adaptar-se constantemente e aprender sobre novas táticas de ameaças será parte do seu trabalho. Ao identificar padrões e metodologias semelhantes, você poderá prever possíveis violações e minimizar danos futuros.

Por fim, entender como a segurança afeta a vida das pessoas reforça a importância do trabalho que você fará!

Onel De Guzman created the LoveLetter malware to steal internet login credentials. This attack spread rapidly and exploited people who were not accustomed to suspecting unsolicited emails. Users received an email with the subject **"I Love You"**, containing an attachment labeled **"Love Letter For You"**. When the attachment was opened, the malware scanned the user's address book and automatically sent itself to every contact on the list. Additionally, it installed a program to collect user information and passwords. Victims believed they were receiving an email from a friend, but in reality, it was an attack. The LoveLetter ended up infecting 45 million computers worldwide, causing an estimated loss of over 10 billion dollars. This attack was one of the first examples of **social engineering**.

**Social engineering** is a manipulation technique that exploits human error to gain private information, unauthorized access, or valuables. After the LoveLetter, attackers understood the power of social engineering. With the rise of social media and the public sharing of personal information, these attacks have become even more common. Many people prioritize convenience over privacy, making them more vulnerable to attacks if they do not use these tools cautiously.

As a security professional, your role will be to identify and manage the improper use of technology that may put your organization and its members at risk. One way to protect your company is to conduct regular internal training sessions, which you, as a future security analyst, may be asked to lead or participate in.

Nowadays, employees are commonly trained to recognize social engineering attacks, especially **phishing** through emails. **Phishing** involves the use of digital communications to deceive people into revealing sensitive data or installing malicious software.

Another significant attack was the **Equifax data breach**. In 2017, hackers successfully infiltrated the credit reporting agency Equifax, resulting in one of the largest breaches of sensitive information in history. Over 143 million customer records were stolen, affecting approximately 40% of the U.S. population.

The compromised data included personally identifiable information such as Social Security numbers, birth dates, driver’s license numbers, home addresses, and credit card details. From a security standpoint, the breach occurred due to multiple failures on Equifax’s part. The attackers exploited several vulnerabilities that the company had failed to fix in the months leading up to the attack.

In the end, Equifax settled with the U.S. government and paid over 575 million dollars in fines and customer compensations. This case alerted companies to the financial impact of a data breach and the necessity of implementing preventive measures.

These are just a few examples of incidents that have shaped the security industry. Understanding them will benefit your career. Knowing different types of malware and social engineering attacks will help you communicate about security risks during job interviews.

As a future security professional, constantly adapting and learning about threat actors' evolving tactics will be a crucial part of your job. By recognizing similar patterns and methodologies, you may be able to identify potential breaches and minimize future damage.

Finally, understanding how security impacts people’s lives is a strong reminder of why the work you will do is so important!

**Ataques comuns e sua eficácia**

Anteriormente, você aprendeu sobre ataques do passado e do presente que ajudaram a moldar o setor de segurança cibernética. Entre eles estão o ataque LoveLetter, também chamado de vírus ILOVEYOU, e o worm Morris. Um dos resultados foi o estabelecimento de equipes de resposta, que agora são comumente chamadas de CSIRTs (Computer Security Incident Response Teams). Nesta leitura, você aprenderá mais sobre os métodos comuns de ataque. Familiarizar-se com os diferentes métodos de ataque *e* com a evolução das táticas e técnicas usadas pelos agentes de ameaças o ajudará a proteger melhor as organizações e as pessoas.

**Phishing**

**Phishing** é o uso de comunicações digitais para enganar as pessoas e fazê-las revelar dados confidenciais ou implantar software mal-intencionado.

Alguns dos tipos mais comuns de ataques de phishing atualmente incluem:

* **Business-to-business Compromise (BEC):** Um agente de ameaças envia uma mensagem de e-mail que parece ser de uma fonte conhecida para fazer uma solicitação aparentemente legítima de informações, a fim de obter uma vantagem financeira.
* **Spear phishing:** ataque de e-mail mal-intencionado que tem como alvo um usuário específico ou um grupo de usuários. O e-mail parece ter sido originado de uma fonte confiável.
* **Whaling:** Uma forma de spear phishing. Os agentes da ameaça têm como alvo os executivos da empresa para obter acesso a dados confidenciais.
* **Vishing:** o exploit da comunicação eletrônica de voz para obter informações confidenciais ou para se passar por uma fonte conhecida.
* **Smishing:** o uso de mensagens de texto para enganar os usuários, a fim de obter informações confidenciais ou se passar por uma fonte conhecida.

**Malware**

**Malware** é um software projetado para danificar dispositivos ou redes de computadores. Há muitos tipos de malware. O principal objetivo do malware é obter dinheiro ou, em alguns casos, uma vantagem de inteligência que pode ser usada contra uma pessoa, uma organização ou um território.

Alguns dos tipos mais comuns de ataques de malware atualmente incluem:

* **Vírus:** Código malicioso escrito para interferir nas operações do computador e causar danos aos dados e ao software. Um vírus precisa ser iniciado por um usuário (ou seja, um agente de ameaça), que transmite o vírus por meio de um anexo malicioso ou download de arquivo. Quando alguém abre o anexo malicioso ou o download, o vírus se esconde em outros arquivos no sistema agora infectado. Quando os arquivos infectados são abertos, o vírus pode inserir seu próprio código para danificar e/ou destruir os dados do sistema.
* **Worms:** Malware que pode se duplicar e se espalhar pelos sistemas por conta própria. Ao contrário de um vírus, um worm não precisa ser baixado por um usuário. Em vez disso, ele se auto-replica e se espalha de um computador já infectado para outros dispositivos na mesma rede.
* **Ransomware:** Ataque malicioso em que os agentes da ameaça criptografam os dados de uma organização e exigem pagamento para restaurar o acesso.
* **Spyware:** Malware usado para coletar e vender informações sem consentimento. O spyware pode ser usado para acessar dispositivos. Isso permite que os agentes de ameaças coletem dados pessoais, como e-mails particulares, textos, registros de voz e imagem e localizações.

**Engenharia social**

**A engenharia social** é uma técnica de manipulação que explora o erro humano para obter informações privadas, acesso ou objetos de valor. O erro humano geralmente é resultado de confiar em alguém sem questionar. A missão de um agente de ameaças, agindo como engenheiro social, é criar um ambiente de falsa confiança e mentiras para explorar o maior número possível de pessoas.

Alguns dos tipos mais comuns de ataques de engenharia social atualmente incluem:

* **Phishing de mídia social:** um agente de ameaças coleta informações detalhadas sobre seu alvo em sites de mídia social. Em seguida, ele inicia um ataque.
* **Ataque de watering hole:** Um agente de ameaças ataca um site frequentemente visitado por um grupo específico de usuários.
* **USB baiting:** Um agente de ameaças deixa estrategicamente um pendrive com malware para que um funcionário o encontre e instale, infectando uma rede sem saber.
* **Engenharia social física:** Um agente de ameaças se faz passar por um funcionário, cliente ou fornecedor para obter acesso não autorizado a um local físico.

**Princípios da engenharia social**

A engenharia social é incrivelmente eficaz. Isso ocorre porque as pessoas geralmente confiam e estão condicionadas a respeitar a Autoridade. O número de ataques de engenharia social está aumentando a cada novo aplicativo de mídia social que permite o acesso público aos dados das pessoas. Embora o compartilhamento de dados pessoais, como sua localização ou fotos, possa ser conveniente, também é um risco.

Os motivos pelos quais os ataques de engenharia social são eficazes incluem:

* **Autoridade:** Os agentes da ameaça se fazem passar por indivíduos com poder. Isso ocorre porque as pessoas, em geral, foram condicionadas a respeitar e seguir figuras de autoridade.
* **Intimidação:** Os agentes da ameaça usam táticas de intimidação. Isso inclui persuadir e intimidar as vítimas para que façam o que lhes é pedido.
* **Consenso/prova social:** Como as pessoas às vezes fazem coisas que acreditam que muitos outros estão fazendo, os agentes de ameaças usam a confiança dos outros para fingir que são legítimos. Por exemplo, um agente de ameaças pode tentar obter acesso a dados privados dizendo a um funcionário que outras pessoas da empresa lhe deram acesso a esses dados no passado.
* **Escassez:** Uma tática usada para sugerir que os bens ou serviços têm oferta limitada.
* **Familiaridade:** Os agentes da ameaça estabelecem uma falsa conexão emocional com os usuários que pode ser exploit.
* **Confiança:** Os agentes da ameaça estabelecem um relacionamento emocional com os usuários que pode ser explorado *ao longo do tempo*. Eles usam esse relacionamento para desenvolver a confiança e obter informações pessoais.
* **Urgência:** Um agente de ameaças persuade os outros a responder rapidamente e sem questionar.

**Principais lições**

Nesta leitura, você aprendeu sobre alguns ataques comuns e seus impactos. Você também aprendeu sobre engenharia social e por que ela é tão bem-sucedida. Embora esta seja apenas uma breve introdução aos tipos de ataque, você terá muitas oportunidades ao longo do programa para desenvolver ainda mais sua compreensão de como identificar e se defender contra ataques à segurança cibernética.

Identify: Methods of attack

Review the flashcards to become more familiar with common types of attacks and how they can impact business operations.

Term:

**Malware**

Definition

A software designed to harm devices or networks

Term:

**Virus**

A malware program that modifies other computer programs by inserting its own code to damage and/or destroy data  
  
Example of: Malware

Term:

**Worm**

Definition

Malware that self-replicates, spreading across the network and infecting computers  
  
Example of: Malware

Term:

**Ransomware**

Definition

A malicious attack during which threat actors encrypt an organization's data and demand payment to restore access  
  
Example of: Malware

Term:

**Spyware**

Definition

Malicious software installed on a user’s computer without their permission, which is used to spy on and steal user data  
  
Example of: Malware

Term:

**Phishing**

Definition

The use of digital communications to trick people into revealing sensitive data or deploying malicious software

Term:

**Spear phishing**

Definition

A malicious email attack targeting a specific user or group of users that appears to originate from a trusted source  
  
Example of: Phishing

Term:

**Whaling**

Definition

A form of spear phishing during which threat actors target executives in order to gain access to sensitive data  
  
Example of: Phishing

Term:

**Business email compromise (BEC)**

Definition

An attack in which a threat actor impersonates a known source to obtain a financial advantage  
  
Example of: Phishing

Term:

**Vishing**

Definition

The exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source  
  
Example of: Phishing

Term:

**Social engineering**

Definition

A manipulation technique that exploits human error to gain unauthorized access to sensitive, private, and/or valuable data

Term:

**Social media phishing**

Definition

An attack in which a threat actor collects detailed information about their target on social media sites before initiating an attack  
  
Example of: Social engineering

Term:

**Watering hole attack**

Definition

An attack in which a threat actor compromises a website frequently visited by a specific group of users  
  
Example of: Social engineering

Term:

**Physical social engineering**

Definition

An attack in which a threat actor impersonates an employee, customer, or vendor to obtain unauthorized access to a physical location  
  
Example of: Social engineering

Term:

**USB baiting**

Definition

An attack in which a threat actor strategically leaves a malware USB stick for an employee to find and unknowingly infect a network  
  
Example of: Social engineering

Term:

**Social engineering**

Definition

A manipulation technique that exploits human error to gain unauthorized access to sensitive, private, and/or valuable data

Term:

**Virus**

Definition

A malware program that modifies other computer programs by inserting its own code to damage and/or destroy data  
  
Example of: Malware

Term:

**Whaling**

Definition

A form of spear phishing during which threat actors target executives in order to gain access to sensitive data  
  
Example of: Phishing

**Malware**

Definition

A software designed to harm devices or networks

You’re done!

Recognizing various examples of malware, phishing, and social engineering attacks will help you better understand common security threats.

Identify: Methods of attack

Review the flashcards to become more familiar with common types of attacks and how they can impact business operations.

**Sean: Mantenha a calma durante uma violação de dados**

Olá, meu nome é Sean. Sou Gerente Técnico de Programas no Google Workspace. Tenho 30 anos de experiência na área de segurança, atuando em seis diferentes setores.

Durante sua primeira violação de dados, a coisa mais importante que você pode fazer é manter a calma. Todos ao seu redor estarão em pânico. Se você faz parte da equipe de segurança e está gerenciando o incidente, precisa ser a pessoa tranquila na sala. Seja aquele que faz uma pausa na conversa. Alguém pode perguntar: "Você sabe o que está acontecendo?" E você responde: "Sim, absolutamente".

A maior violação de dados que já enfrentei começou com um simples telefonema. Um engenheiro de uma instituição financeira comprou um servidor no eBay. Quando ligou o equipamento, descobriu que ele não havia sido formatado. Havia 20 milhões de registros de cartões de crédito nele. Isso desencadeou uma revisão completa dos nossos controles. Percebemos que não estávamos monitorando como terceiros lidavam com a remoção de dados, já que começamos a terceirizar data centers.

A primeira coisa a fazer em uma violação de dados é conter o incidente. Se os dados ainda estão vazando, é necessário seguir os procedimentos para interromper essa perda. Isso pode significar desligar um servidor, um data center ou até interromper comunicações. O mais importante é parar o vazamento de dados.

Seu trabalho como gestor de incidentes, ou como parte da equipe que lida com uma violação, é conter o incidente e depois investigá-lo. Executar seu plano de gerenciamento de incidentes corretamente é a lição mais valiosa para qualquer profissional iniciante na área.

Hi, my name is Sean. I'm a Technical Program Manager in Google Workspace. I have 30 years of experience in the security field, working across six different industries.

During your first data breach, the most important thing you can do is keep your cool. Everyone around you will be freaking out. If you are on the security team and managing the incident, you need to be the calm person in the room. Be the one who takes a pause in the conversation. Someone might ask, "Do you know what's going on?" And you respond, "Yes, absolutely."

The biggest breach I have ever handled started with a simple phone call. An engineer from a financial institution bought a server on eBay. When he powered it on, he found it hadn't been wiped. There were 20 million credit card records on it. This triggered a full review of our controls. We realized we weren’t monitoring how third parties handled data removal, as we had started outsourcing data centers.

The first thing to do in a data breach is to contain the incident. If data is still leaking, you must follow procedures to stop it. This might mean shutting down a server, a data center, or even cutting off communications. The top priority is to stop data loss.

Your job as an incident manager, or as part of the team handling a breach, is to contain the incident and then investigate it. Properly executing your incident management plan is the most important lesson for any entry-level professional in the field.

**Introdução aos oito domínios de segurança do CISSP, Parte 1**