

How to become a cyber
security expert


The Future of Cybersecurity

IT and Security Career Outlook **INFOSEC**
INSTITUTE

The Future of Cybersecurity

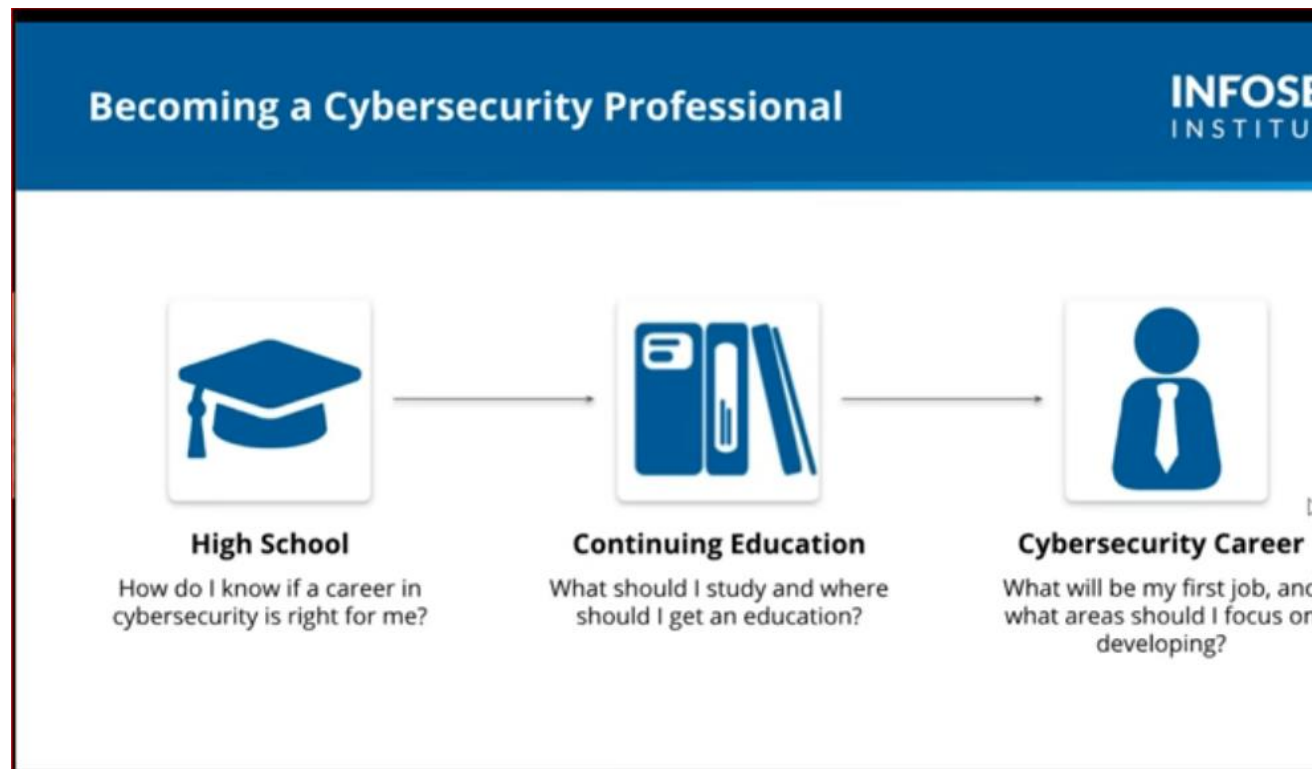
- Cybersecurity workforce shortage expected to hit **1.8 million by 2022**
- 52% of cybersecurity professionals said they had a difficult time finding qualified personnel
- 87% of cybersecurity workers did not start in cybersecurity (e.g. IT, business, marketing, finance, accounting, military)

Source: Global Information Security Workforce Study



- <https://www.infosecinstitute.com/>

Becoming a Cybersecurity Professional



- <https://www.infosecinstitute.com/>

Getting your first Security Certification

Getting Your First Security Certification

INFOSEC
INSTITUTE

Getting Started with Certifications

- Popular entry-level IT certifications (A+, Network+, CCNA)
- IT vs. Security certifications
- What questions do you have about certifications?



- <https://www.infosecinstitute.com/>

Train When, Where and How you want



The graphic features a blue header with the text "Train When, Where and How You Want" and the "INFOSEC INSTITUTE" logo. Below the header are four white boxes with orange headers, each representing a different training option. The first box is "Flex Pro" with the description "Immersive, live-streamed instruction. Our most popular option!". The second is "Flex Classroom" with "Public training boot camps held nationwide". The third is "Flex Basic" with "Self-paced, computer-based courses". The fourth is "Flex Enterprise" with "Tailored training at your location". At the bottom center is the "INFOSEC INSTITUTE" logo.

Train When, Where and How You Want INFOSEC INSTITUTE


- Flex Pro**
Immersive, live-streamed instruction. Our most popular option!
- Flex Classroom**
Public training boot camps held nationwide
- Flex Basic**
Self-paced, computer-based courses
- Flex Enterprise**
Tailored training at your location

INFOSEC INSTITUTE

- <https://www.infosecinstitute.com/>

Training with InfoSec

Why Train with InfoSec Institute



Benefits of Flex Pro:

- Expert instruction from industry professionals like Keatron Evans
- Industry-Leading Exam Pass Rates — 93%
- Personalized InfoSec Flex Center:
 - Pre-course study materials
 - Digital courseware and reinforcement materials throughout your course
 - Detailed reporting on Exam readiness
 - And more!
- 100% Satisfaction Guarantee
- **Exam Pass Guarantee!**

FREE Video Replays!

Get 90-day access to video replays of your daily lessons — a **\$699 value!**

When you enroll in an upcoming live online Flex Pro boot camp **before October 31**

5 cybersecurity roles

Cyber Operator



DEGREE REQUIRED?

Yes

Bachelor's in Computer Science/Engineering
Certification(s) recommended

MEDIAN SALARY

+\$100,000

JOB GROWTH

20%

SOFT SKILLS

Critical Thinking
Excellent Communication
(written and verbal)
Analytical

COMMON JOB DUTIES

- Analyze network architecture, tools and procedures for ways to improve performance
- Identify potential points of strength and vulnerability within a network
- Collect and process information on wireless networks and connected devices
- Deploy, test, and utilize network tools
- Monitor and track diagnostic information on network health
- Operate and maintain automated systems for gaining access to networks
- Collaborate with development organizations to create and deploy the tools needed to achieve objectives
- Conduct exploitation testing of devices and networks

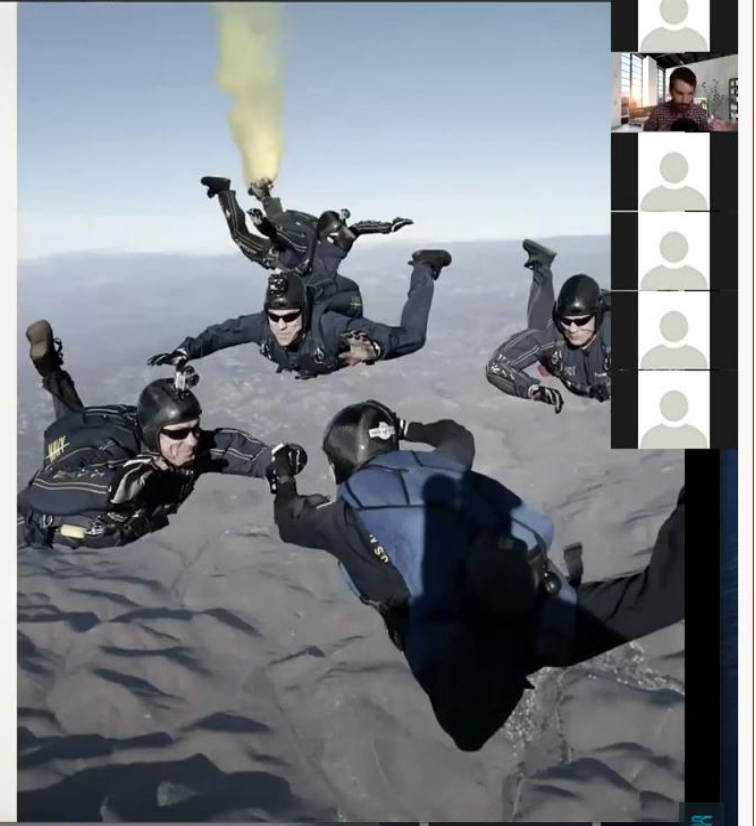


<https://nicerc.org/2019/03/connecting-cyber-education-to-cyber-careers/>

“This is me!”


-Your inner monologue

- Metasploit Training (Hackersplit Playlist)
https://youtu.be/8IR27r8Y_ik
- Hack the Box
<https://www.hackthebox.eu/home>
- Hacking 101 - 6 hours of free training -
<https://cyber.fullstackacademy.com/prepare/hacking-101>
- ELI5: x86_64 Exploit Development Fundamentals w/ John Ryan & Adrian Abdala (2-Hours) - Wed, Oct 14, 2020 12:30 PM - 3:00 PM EDT



EARLY CLOUD

2. Cyber Defense Incident Responder



CYBER DEFENSE INCIDENT RESPONDER

DEGREE REQUIRED?
No
Bachelor's Degree in Cybersecurity or Computer Science is a plus though

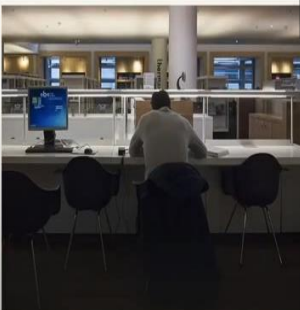

MEDIAN SALARY
+\$80,000

JOB GROWTH
+20%

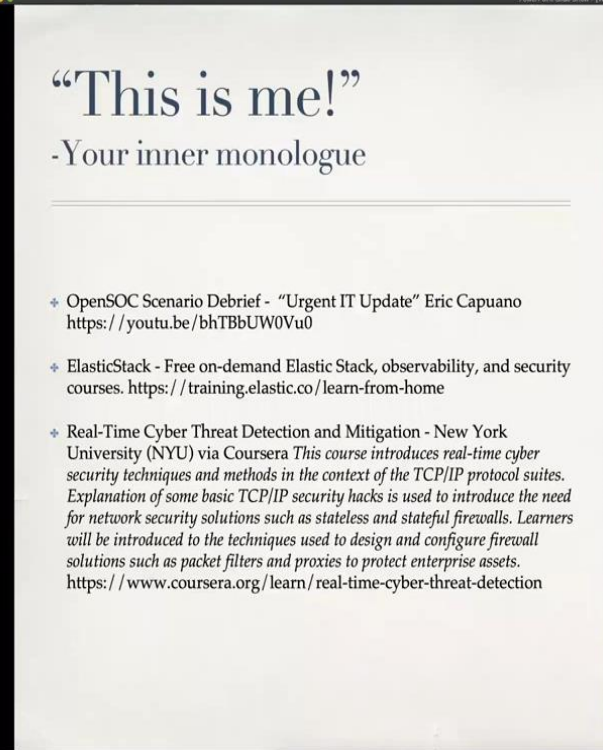
SOFT SKILLS
Capable of Handling Stress
Flexible
Problem-Solving
Analytical
Good Communication

COMMON JOB DUTIES

- ▶ Actively monitor systems and networks for intrusions
- ▶ Identify security flaws and vulnerabilities
- ▶ Perform security audits, risk analysis, network forensics and penetration testing
- ▶ Perform malware analysis and reverse engineering
- ▶ Develop a procedural set of responses to security problems
- ▶ Establish protocols for communication within an organization and dealings with law enforcement during security incidents
- ▶ Create a program development plan that includes security gap assessments, policies, procedures, playbooks, training and tabletop testing
- ▶ Produce detailed incident reports and technical briefs for management, admins and end-users
- ▶ Liaison with other cyber threat analysis entities




<https://nicerc.org/2019/03/connecting-cyber-education-to-cyber-careers/>

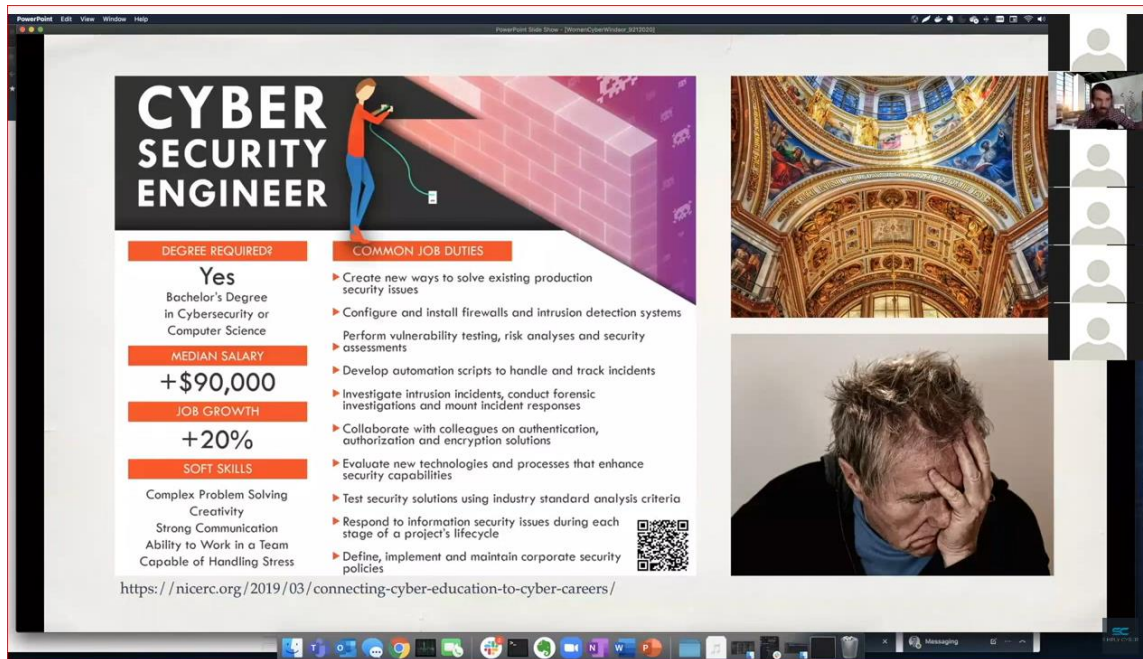


“This is me!”
-Your inner monologue

- ✦ OpenSOC Scenario Debrief - “Urgent IT Update” Eric Capuano
<https://youtu.be/bhTBbUW0Vu0>
- ✦ ElasticStack - Free on-demand Elastic Stack, observability, and security courses. <https://training.elastic.co/learn-from-home>
- ✦ Real-Time Cyber Threat Detection and Mitigation - New York University (NYU) via Coursera *This course introduces real-time cyber security techniques and methods in the context of the TCP/IP protocol suites. Explanation of some basic TCP/IP security hacks is used to introduce the need for network security solutions such as stateless and stateful firewalls. Learners will be introduced to the techniques used to design and configure firewall solutions such as packet filters and proxies to protect enterprise assets.*
<https://www.coursera.org/learn/real-time-cyber-threat-detection>



3. Cyber Security Engineer



CYBER SECURITY ENGINEER

DEGREE REQUIRED?
Yes
Bachelor's Degree in Cybersecurity or Computer Science

MEDIAN SALARY
+\$90,000

JOB GROWTH
+20%

SOFT SKILLS
Complex Problem Solving
Creativity
Strong Communication
Ability to Work in a Team
Capable of Handling Stress

COMMON JOB DUTIES

- ▶ Create new ways to solve existing production security issues
- ▶ Configure and install firewalls and intrusion detection systems
- ▶ Perform vulnerability testing, risk analyses and security assessments
- ▶ Develop automation scripts to handle and track incidents
- ▶ Investigate intrusion incidents, conduct forensic investigations and mount incident responses
- ▶ Collaborate with colleagues on authentication, authorization and encryption solutions
- ▶ Evaluate new technologies and processes that enhance security capabilities
- ▶ Test security solutions using industry standard analysis criteria
- ▶ Respond to information security issues during each stage of a project's lifecycle
- ▶ Define, implement and maintain corporate security policies

<https://nicerc.org/2019/03/connecting-cyber-education-to-cyber-careers/>

The infographic includes an illustration of a person climbing a wall, a photograph of a grand, ornate interior dome, and a photograph of a man holding his head in his hand, suggesting stress or frustration.

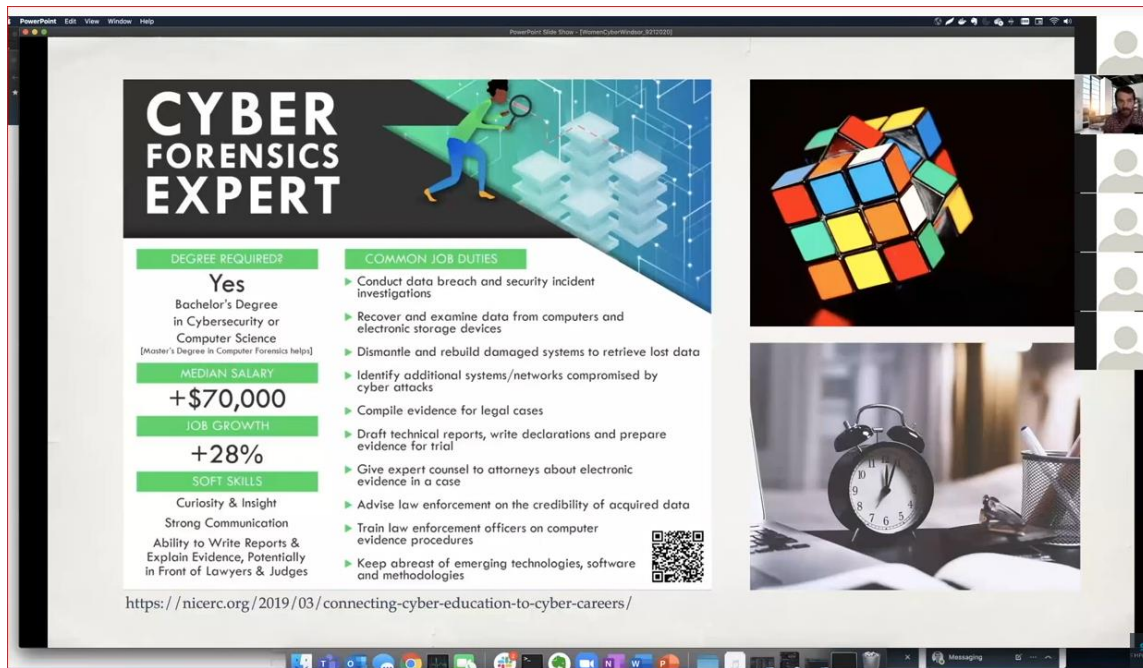


"This is me!"
-Your inner monologue

- ❖ Using ATT&CK for Cyber Threat Intelligence Training" - 4 hour training
<https://attack.mitre.org/resources/training/cti/>
- ❖ Fortinet Security Appliance Training - Free access to the FortiGate Essentials Training Course and Network Security Expert courses 1 and 2
<https://www.fortinet.com/training/cybersecurity-professionals.html>
- ❖ AWS Cloud Security (Free)
<https://aws.amazon.com/training/path-security/>

The slide features a photograph of three construction workers in hard hats and safety vests looking at a large set of blueprints on a construction site.

4. Cyber Forensics Expert



CYBER FORENSICS EXPERT

DEGREE REQUIRED?
Yes
Bachelor's Degree in Cybersecurity or Computer Science
(Master's Degree in Computer Forensics helps)

MEDIAN SALARY
+\$70,000

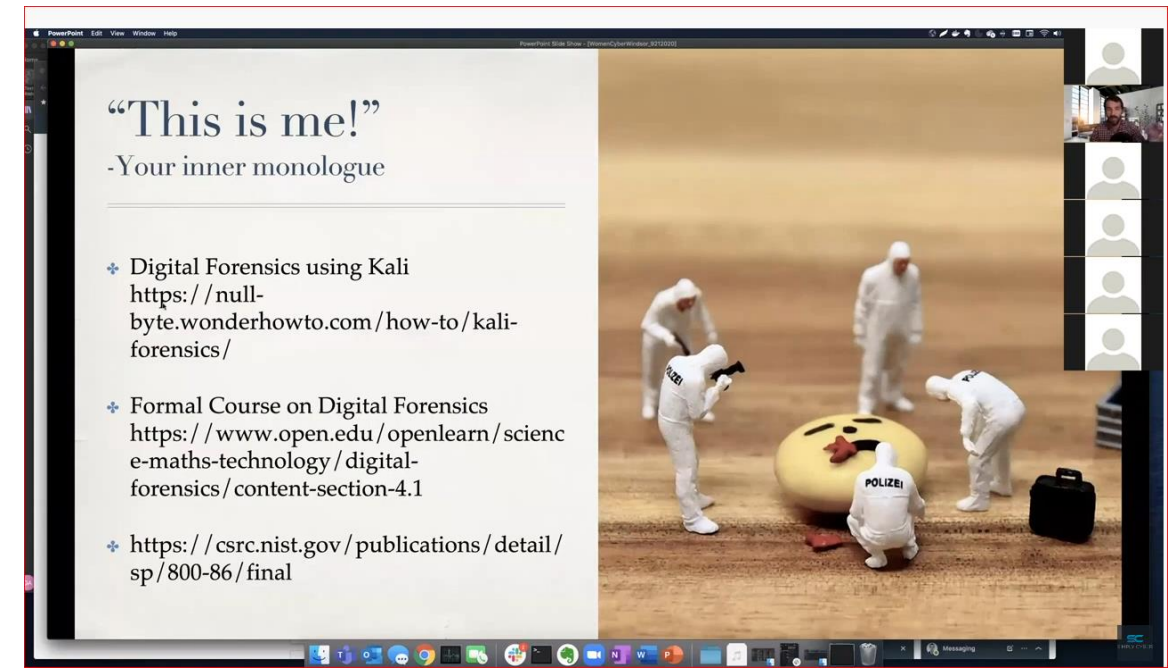



JOB GROWTH
+28%

SOFT SKILLS
Curiosity & Insight
Strong Communication
Ability to Write Reports & Explain Evidence, Potentially in Front of Lawyers & Judges

COMMON JOB DUTIES


- ▶ Conduct data breach and security incident investigations
- ▶ Recover and examine data from computers and electronic storage devices
- ▶ Dismantle and rebuild damaged systems to retrieve lost data
- ▶ Identify additional systems/networks compromised by cyber attacks
- ▶ Compile evidence for legal cases
- ▶ Draft technical reports, write declarations and prepare evidence for trial
- ▶ Give expert counsel to attorneys about electronic evidence in a case
- ▶ Advise law enforcement on the credibility of acquired data
- ▶ Train law enforcement officers on computer evidence procedures
- ▶ Keep abreast of emerging technologies, software and methodologies

<https://nicerc.org/2019/03/connecting-cyber-education-to-cyber-careers/>



“This is me!”
-Your inner monologue

- ✦ Digital Forensics using Kali
<https://null-byte.wonderhowto.com/how-to/kali-forensics/>
- ✦ Formal Course on Digital Forensics
<https://www.open.edu/openlearn/scienc-e-maths-technology/digital-forensics/content-section-4.1>
- ✦ <https://csrc.nist.gov/publications/detail/sp/800-86/final>



5. Vulnerability Assessment Analyst

VULNERABILITY ASSESSMENT ANALYST AKA VULNERABILITY ASSESSOR



DEGREE REQUIRED?

No

Real-world experience is much more valued than a degree, though a degree won't hurt

MEDIAN SALARY

\$75,000

JOB GROWTH

+20%

SOFT SKILLS

Alternative Problem Solving
Curious & Creative
Attention to Detail
Strong Communication
Interest in Hacking

COMMON JOB DUTIES

- Identify critical flaws in applications and systems that cyber attackers could exploit
- Conduct vulnerability assessments for networks, applications and operating systems
- Conduct network security audits and scanning on a predetermined basis
- Use automated tools (e.g. Nessus) to pinpoint vulnerabilities and reduce time-consuming tasks
- Use manual testing techniques and methods to gain a better understanding of the environment and reduce false negatives
- Develop, test and modify custom scripts and applications for vulnerability testing
- Compile and track vulnerabilities over time for metrics purposes
- Write and present a comprehensive Vulnerability Assessment and maintain a database
- Supply hands-on training for network and systems administrators



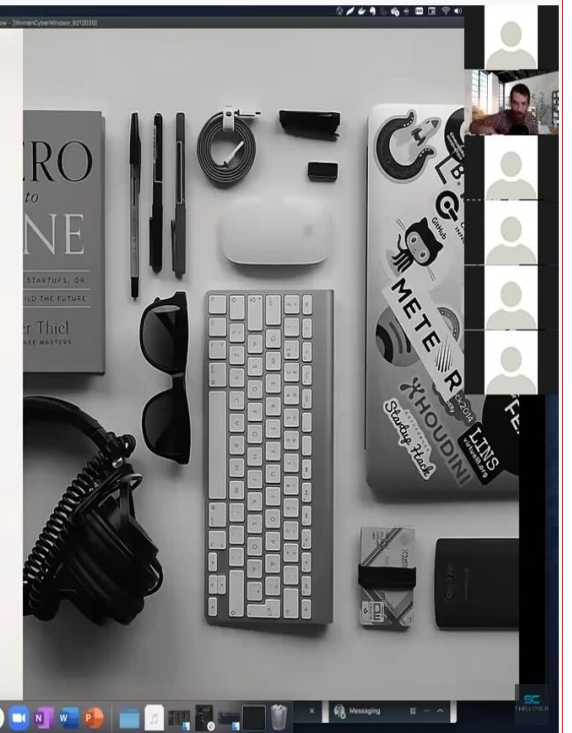
<https://nicerc.org/2019/03/connecting-cyber-education-to-cyber-careers/>



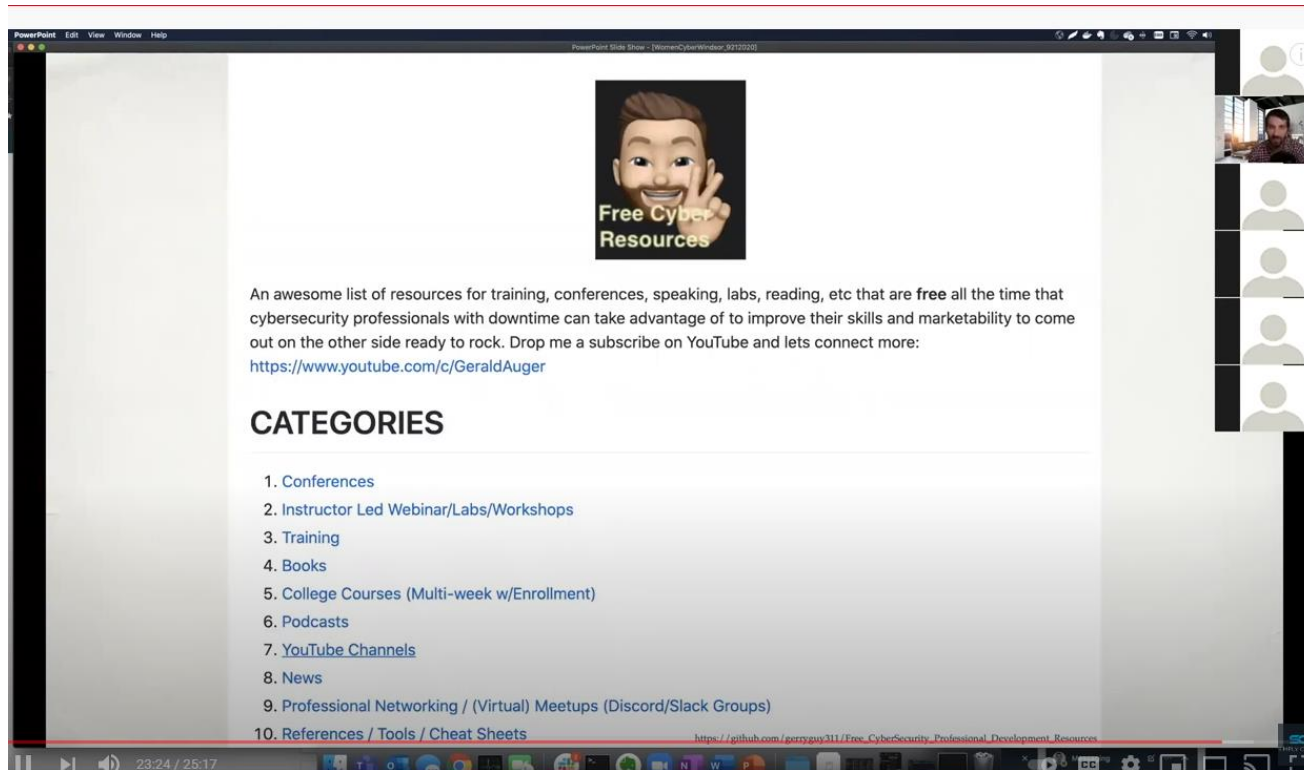
“This is me!”

-Your inner monologue

- ✦ Nessus
<https://www.tenable.com/education/on-demand-courses>
- ✦ Guide to Enterprise Patch Management Technologies
<https://csrc.nist.gov/v/publications/detail/sp/800-40/rev-3/final>
- ✦ US-CERT - Current state threat awareness
<https://us-cert.cisa.gov>



Free Cyber Resources



The screenshot shows a PowerPoint presentation slide with the following content:

- Free Cyber Resources** (with a cartoon character icon)
- An awesome list of resources for training, conferences, speaking, labs, reading, etc that are **free** all the time that cybersecurity professionals with downtime can take advantage of to improve their skills and marketability to come out on the other side ready to rock. Drop me a subscribe on YouTube and lets connect more:
<https://www.youtube.com/c/GeraldAuger>
- CATEGORIES**
 1. Conferences
 2. Instructor Led Webinar/Labs/Workshops
 3. Training
 4. Books
 5. College Courses (Multi-week w/Enrollment)
 6. Podcasts
 7. [YouTube Channels](#)
 8. News
 9. Professional Networking / (Virtual) Meetups (Discord/Slack Groups)
 10. References / Tools / Cheat Sheets
- Footer: https://github.com/gerryguy311/Free_CyberSecurity_Professional_Development_Resources

The slide is displayed in a window titled 'PowerPoint Slide Show - WomenCyberWindow.9212220'. On the right side of the window, there is a vertical stack of six icons representing participants in a video conference. The top icon shows a person's video feed, while the others are generic person icons. At the bottom of the window, a Windows taskbar is visible with the time 23:24 / 25:17.

Security + course

No matter what preparation materials you are using to study, the [Security+ Last Minute Review Guide](#) is something you need in your learning toolkit.

You'll find the most important points that you need to know from each of the six Security+ domains. This [13-page guide](#) covers:

Domain 1: Threats, Attacks, and Vulnerabilities

Domain 2: Technologies and Tools

Domain 3: Architecture and Design

Domain 4: Identity and Access Management

Domain 5: Risk Management

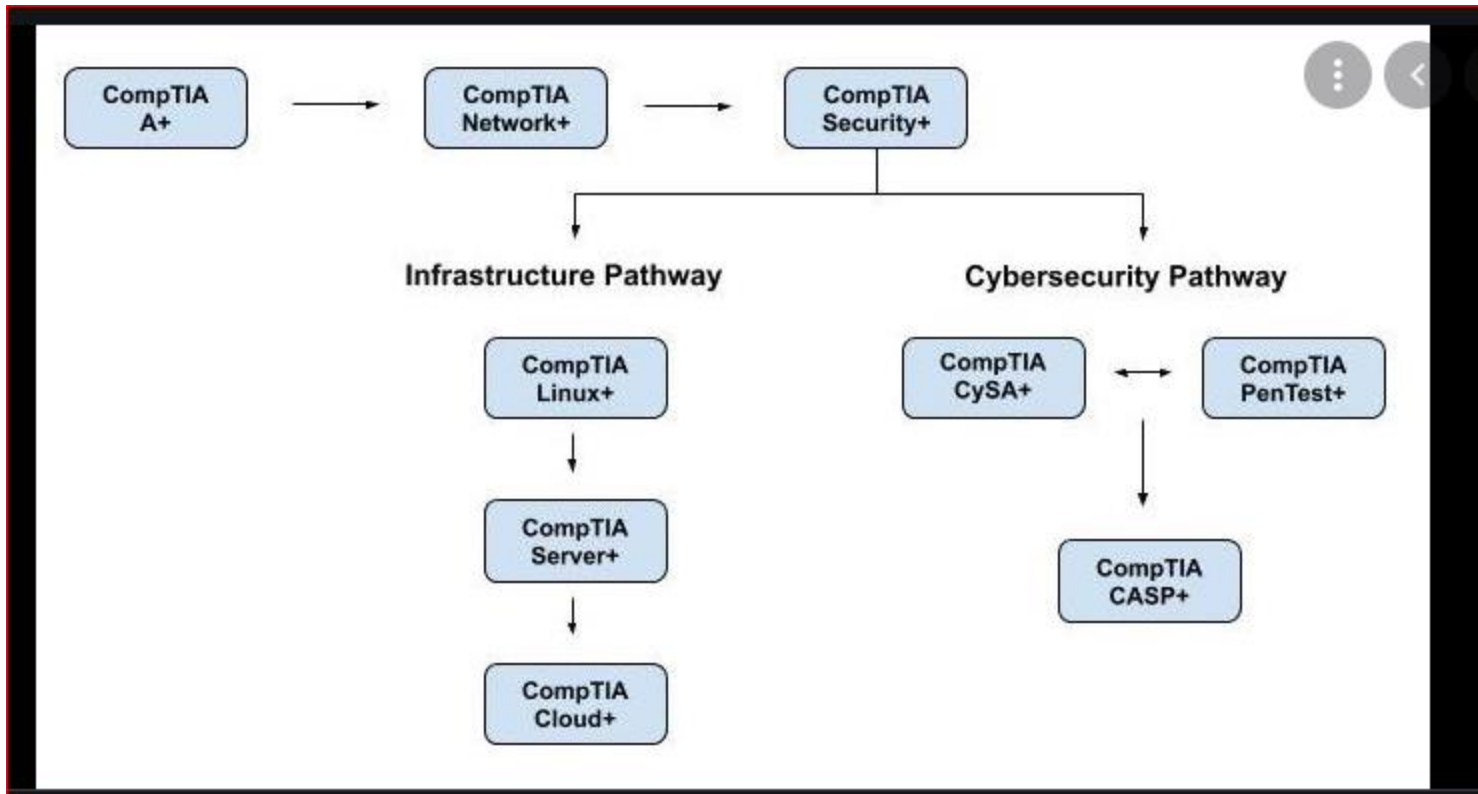
Domain 6: Cryptography and PKI

You can get your copy of the [Security+ Last Minute Review Guide](#) as an immediate digital download for only \$9.99.

Best regards,
Mike

[Get the Guide!](#)

Comptia + Certificate Path



CompTia Security+ Exam Syllabus

WWW.EDUSUM.COM

PDF

Introduction to CompTIA Security+ Exam

The CompTIA SY0-501 Exam is challenging and thorough preparation is essential for success. This exam study guide is designed to help you prepare for the Security+ certification exam. It contains a detailed list of the topics covered on the Professional exam, as well as a detailed list of preparation resources. These study guide for the CompTIA Security+ will help guide you through the study process for your certification.



SY0-501 CompTIA Security+ Exam Summary

- **Exam Name:** CompTIA Security+
- **Exam Code:** SY0-501
- **Exam Price:** \$339 (USD)
- **Duration:** 90 mins
- **Number of Questions:** 90
- **Passing Score:** 750 / 900
- **Schedule Exam:** [CompTIA Marketplace](#)
- **Sample Questions:** [CompTIA Security+ Sample Questions](#)
- **Recommended Practice:** [CompTIA SY0-501 Certification Practice Exam](#)

WWW.EDUSUM.COM

PDF

Exam Syllabus: SY0-501 CompTIA Security+

1. Threats, Attacks and Vulnerabilities 21%

Given a scenario, analyze indicators of compromise and determine the type of malware.
Compare and contrast types of attacks.
Explain threat actor types and attributes.
Explain penetration testing concepts.
Explain vulnerability scanning concepts.
Explain the impact associated with types of vulnerabilities.

2. Technologies and Tools 22%

Install and configure network components, both hardware and software-based, to support organizational security.
Given a scenario, use appropriate software tools to assess the security posture of an organization.
Given a scenario, troubleshoot common security issues.
Given a scenario, analyze and interpret output from security technologies.
Given a scenario, deploy mobile devices securely.
Given a scenario, implement secure protocols.

3. Architecture and Design 15%

Explain use cases and purpose for frameworks, best practices and secure configuration guides.
Given a scenario, implement secure network architecture concepts.
Given a scenario, implement secure systems design.
Explain the importance of secure staging deployment concepts.
Explain the security implications of embedded systems.
Summarize secure application development and deployment concepts.
Summarize cloud and virtualization concepts.
Explain how resiliency and automation strategies reduce risk.
Explain the importance of physical security controls.

4. Identity and Access Management 16%

Compare and contrast identity and access management concepts.
Given a scenario, install and configure identity and access services.
Given a scenario, implement identity and access management controls.
Given a scenario, differentiate common account management practices.

CompTia Security+ Exam Syllabus

WWW.EDUSUM.COM

PDF

5. Risk Management 14%

Explain the importance of policies, plans and procedures related to organizational security

Summarize business impact analysis concepts.

Explain risk management processes and concepts.

Given a scenario, follow incident response procedures.

Summarize basic concepts of forensics.

Explain disaster recovery and continuity of operation concepts.

Compare and contrast various types of controls.

Given a scenario, carry out data security and privacy practices.

6. Cryptography and PKI 12%

Compare and contrast basic concepts of cryptography.

Explain cryptography algorithms and their basic characteristics.

Given a scenario, install and configure wireless security settings.

Given a scenario, implement public key infrastructure.

CompTIA SY0-501 Certification Sample Questions and Answers

To make you familiar with CompTIA Security+ (SY0-501) certification exam structure, we have prepared this sample question set. We suggest you to try our Sample Questions for [Security Plus SY0-501 Certification](#) to test your understanding of CompTIA SY0-501 process with real CompTIA certification exam environment.

SY0-501 CompTIA Security+ Sample Questions:-

01. Which of the following reduces the effectiveness of a good password policy?

- a) Account lockout
- b) Password recovery
- c) Account disablement
- d) Password reuse

02. You identify a system that becomes progressively slower over a couple days until it is unresponsive. Which of the following is most likely the reason for this behavior?

- a) Improper error handling
- b) Race condition

WWW.EDUSUM.COM

PDF

- c) Memory leak
- d) Untrained user

03. Which one of the following best provides an example of detective controls versus prevention controls?

- a) IDS/camera versus IPS/guard
- b) IDS/IPS versus camera/guard
- c) IPS/camera versus IDS/guard
- d) IPS versus guard

04. An organization is implementing a server-side application using OAuth 2.0. Which of the following grant types should be used?

- a) Implicit
- b) Authorization code
- c) Password credentials
- d) Client credentials

05. Which of the following is associated with certificate issues?

- a) Unauthorized transfer of data
- b) Release of private or confidential information
- c) Algorithm mismatch error
- d) Prevention of legitimate content

06. Eliminating email to avoid the risk of email-borne viruses is an effective solution but is not likely to be a realistic approach for which of the following?

- a) Risk avoidance
- b) Risk transference
- c) Risk acceptance
- d) Risk mitigation

07. Which of the following best describes a biometric false acceptance rate (FAR)?

- a) The point at which acceptances and rejections are equal
- b) Rejection of an authorized user
- c) Access allowed to an unauthorized user
- d) Failure to identify a biometric image

08. Advanced malware tools use which of the following analysis methods?

- a) Static analysis
- b) Context based
- c) Signature analysis
- d) Manual analysis

Cyber Security Tools - Fortinet

<https://www.fortinet.com/>

FORTINET ENTERPRISE SMALL MID-SIZED BUSINESSES SERVICE PROVIDERS PARTNERS

SECURITY-DRIVEN NETWORKING CLOUD SECURITY **SECURITY OPERATIONS** ZERO TRUST ACCESS THREAT INTELLIGENCE

SECURITY OPERATIONS

- SOC PLATFORM**
 - Analytics, Reporting & Response
 - SIEM
 - SOAR
 - XDR
 - Artificial Intelligence for IT Operations
- ADVANCE THREAT PROTECTION**
 - Sandboxing
 - Deception
 - UEBA
 - Virtual Security Analyst
- ENDPOINT SECURITY**
 - FortiClient Fabric Agent
 - Endpoint Protection with EDR
- USE CASES**
 - Insider Risk
 - Automate Security
- QUICK LINKS**
 - Products A-Z
 - Resource Center
 - Request a Quote

FortiGuard Outbreak Alerts: what you need to know about the latest cybersecurity attacks

FORTINET ENTERPRISE SMALL MID-SIZED BUSINESSES SERVICE PROVIDERS PARTNERS

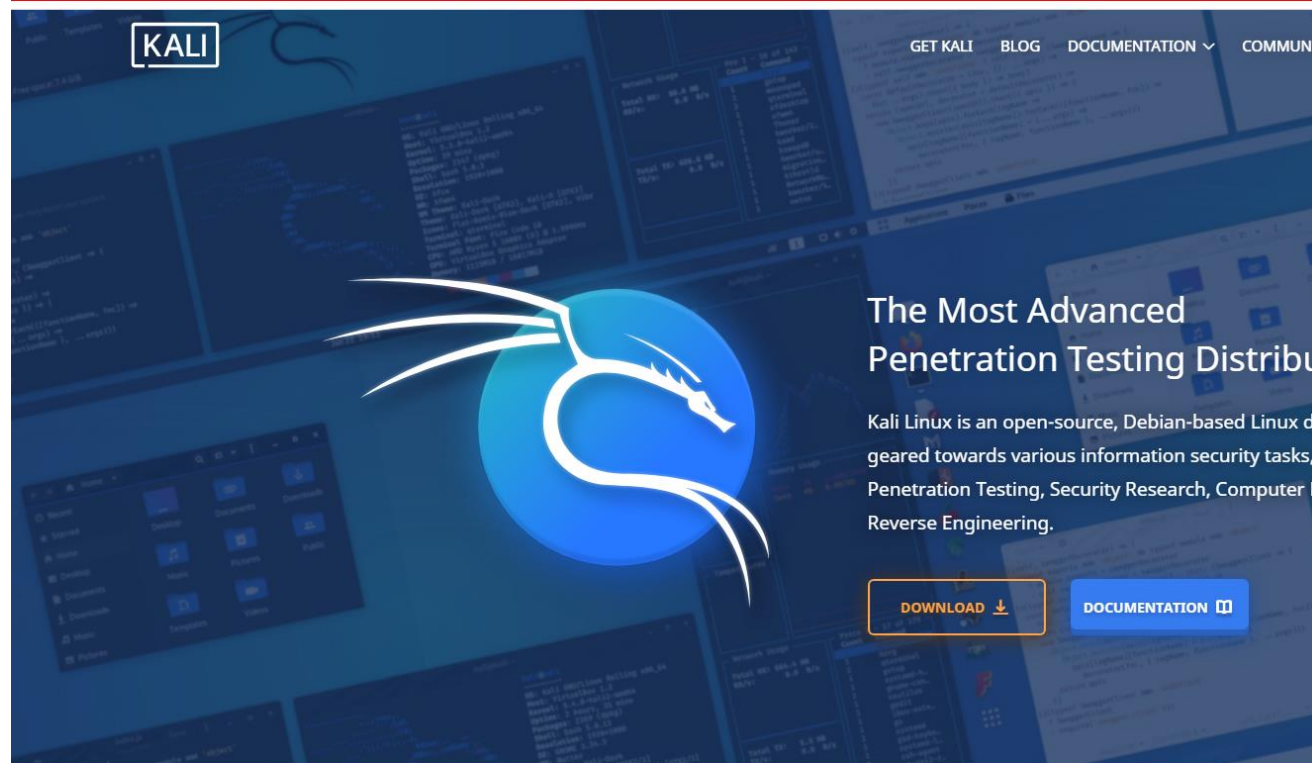
SECURITY-DRIVEN NETWORKING CLOUD SECURITY SECURITY OPERATIONS ZERO TRUST ACCESS **THREAT INTELLIGENCE** DISCOVER MORE

THREAT INTELLIGENCE

- FORTIGUARD LABS**
 - Threat Intelligence and research fueling AI-enabled autonomous security, providing a real-time coordinated response to attacks across endpoints, networks, and clouds.
 - LEARN MORE** →
- WEB SECURITY**
 - Web & Video Filtering
 - CONTENT SECURITY**
 - Realtime AV
 - Cloud Sandbox
- DEVICE SECURITY**
 - IPS & Vulnerability Scanning
 - IoT & OT
 - APPLICATION SECURITY**
 - Web Applications
 - Cloud Access Security Broker
 - FORTIGUARD LAB CONSULTING**
 - Overview
- USE CASES**
 - Network Security
 - Endpoint Security
 - Cloud Security
 - Hybrid worker security
 - FortiGuard Outbreak Alerts
- QUICK LINKS**
 - Products A-Z
 - Resource Center
 - Request a Quote

FortiGuard Outbreak Alerts: what you need to know about the latest cybersecurity attacks

Kali Penetration testing tool



- <https://www.kali.org/>

Hack the Box - tool

The screenshot shows the Hack the Box website homepage. The navigation bar includes links for HACKER, BUSINESS, UNIVERSITY, and Sign In. The main header features the HACKTHEBOX logo, navigation links for Products, Resources, and Company, and a JOIN NOW button. A promotional banner for a new HTB Business CTF competition is visible. The main content area features a large heading 'A Massive Hacking Playground' and a subheading 'Join a dynamically growing hacking community and take your cybersecurity skills to the next level through the most captivating, gamified, hands-on training experience!'. A cookie consent banner is at the bottom, with options to 'Use necessary cookies only', 'Allow selection', or 'Allow all cookies', and a list of categories: Necessary, Preferences, Statistics, Marketing, and Show details.

HACKER BUSINESS UNIVERSITY Sign In >

HACKTHEBOX Products Resources Company JOIN NOW

NEW HTB Business CTF: A hacking competition for companies | £20,000 worth of prizes! >

A Massive Hacking Playground

Join a dynamically growing hacking community and take your cybersecurity skills to the next level through the most captivating, gamified, hands-on training experience!

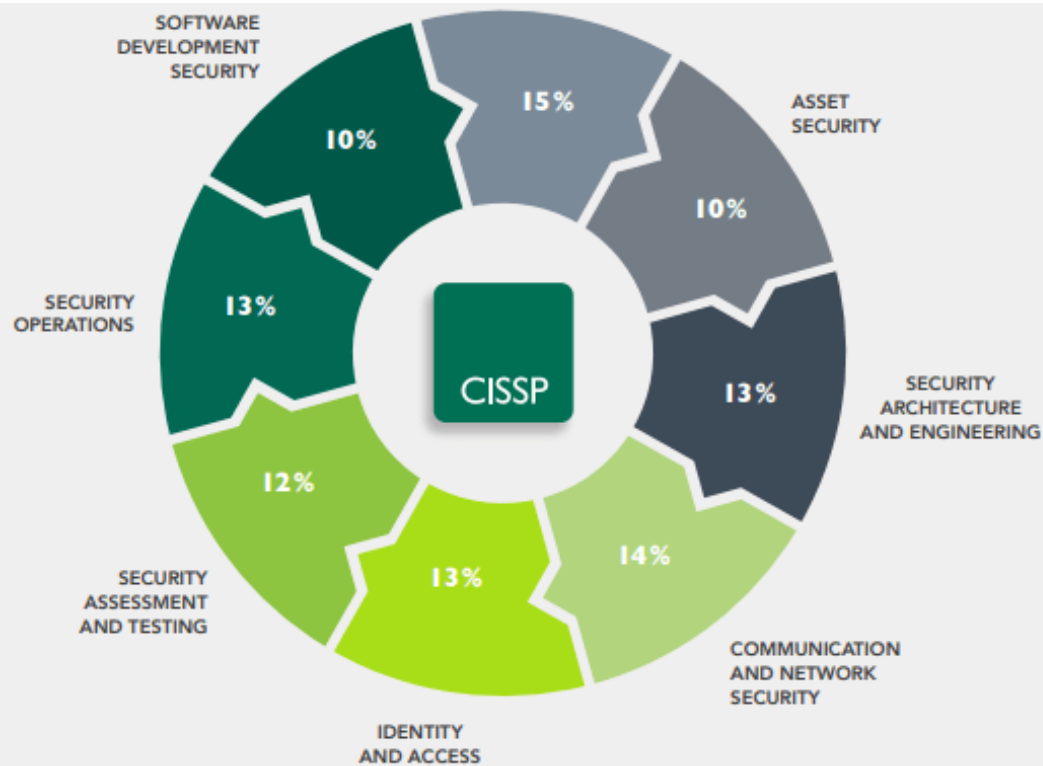
This website uses cookies
We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

Use necessary cookies only Allow selection Allow all cookies

Necessary Preferences Statistics Marketing Show details

- <https://www.hackthebox.eu/>

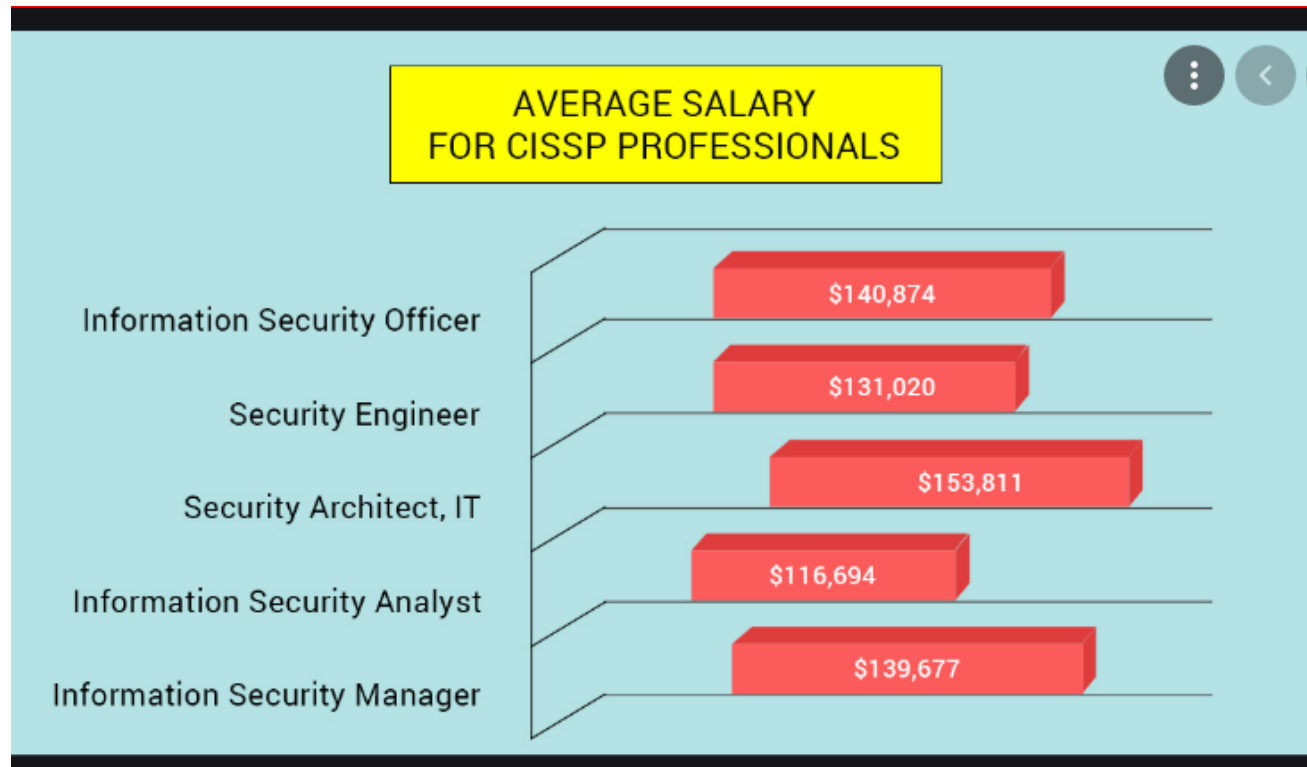
CISSP



CISSP

- ✓ Security and Risk Management
- ✓ Asset Security
- ✓ Security Engineering
- ✓ Communication and Network Security
- ✓ Identity and Access Management
- ✓ Security Assessment and Testing
- ✓ Security Operations

CISSP Salary



Useful Links

- <https://www.youtube.com/watch?v=xzDKM7eEweI>
- <https://www.youtube.com/watch?v=iW5UitULXLY>
- <https://www.youtube.com/watch?v=EwpcwMz1c0Qv>
- https://www.youtube.com/watch?v=2H9_I3yXhcx
- <https://www.youtube.com/watch?v=EtVTPonfm6Q>
-
- https://danielmiessler.com/study/infosec_interview_questions/
-
- <https://www.itjobswatch.co.uk/contracts/uk/cyber%20security.do>
- <https://www.itjobswatch.co.uk/contracts/uk/it%20strategy.do>
-
- <https://www.itjobswatch.co.uk/contracts/uk/itsm.do>

Cyber Job titles

- Internet management
- Stock Analyst
- IT audit role
- SOC analyst
- SOC analyst one
- Risk assessment specialist analyst
- Vulnerability analyst
- Policy and standard specialist

Buzz words

- Management skills using Nexpose, Qualys and Nexus
- Good understanding of Firewall: Cisco ASA and Palo Alto
- Knowledge of IPS/IDS: Checkpoint, Snort and security onion, Disk Encryption i.e Bitlocker/MBAM
- Good knowledge of GRC frameworks - ISO27001, PCI-DSS, ISO27002, GDPR and NIST
- Networking Skills (TCP IP, DNS, DHCP,VPN)
- Good communication and documentation skills
- Knowledge of Antivirus: Sophos and Symantec

Powershell Tool

```
Administrator: Windows PowerShell
PS C:\Windows\system32> get-help get-service

NAME
----
Get-Service

SYNOPSIS
-----
Gets the services on a local or remote computer.

SYNTAX
-----
Get-Service [-ComputerName <String[]> [-DependentServices] -DisplayName <String[]> [-Exclude <String[]>]
[-Include <String[]>] [-RequiredServices] [<CommonParameters>]

Get-Service [-ComputerName <String[]> [-DependentServices] [-Exclude <String[]>] [-Include <String[]>]
[-InputObject <ServiceController[]>] [-RequiredServices] [<CommonParameters>]

Get-Service [[-Name] <String[]>] [-ComputerName <String[]>] [-DependentServices] [-Exclude <String[]>] [-Include
<String[]>] [-RequiredServices] [<CommonParameters>]

DESCRIPTION
-----
The Get-Service cmdlet gets objects that represent the services on a local computer or on a remote computer,
including running and stopped services.

You can direct this cmdlet to get only particular services by specifying the service name or display name of the
services, or you can pipe service objects to this cmdlet.

RELATED LINKS
-----
Online Version: http://go.microsoft.com/fwlink/?LinkId=821593
New-Service
Restart-Service
Resume-Service
Set-Service
Start-Service
Stop-Service
Suspend-Service

REMARKS
-----
To see the examples, type: "get-help Get-Service -examples".
For more information, type: "get-help Get-Service -detailed".
For technical information, type: "get-help Get-Service -full".
For online help, type: "get-help Get-Service -online".

PS C:\Windows\system32>
```

--- The Solving
A Guide to PowerShell - part 1 | The Solving [Visit](#)

Images may be subject to copyright. [Learn More](#)

Related images [See more](#)

<https://www.pdq.com/powershell/>

Amazon AWS


<https://aws.amazon.com/>

The screenshot shows the AWS website homepage. At the top left is the AWS logo. To its right is a navigation bar with links for Products, Solutions, Pricing, Documentation, Learn, Partner Network, AWS Marketplace, Customer Enablement, Events, and Explore More. Further right are links for Contact Us, Support, English, and My Account, followed by a prominent orange button labeled 'Create an AWS Account'. Below the navigation bar is a large heading 'Explore Our Solutions'. Under this heading, there are two main sections: 'By Industry' and 'By Technology Category'. Each section contains four cards with icons, titles, brief descriptions, and 'Learn More' links. A 'View All Industries' link is also present.

aws [Products](#) [Solutions](#) [Pricing](#) [Documentation](#) [Learn](#) [Partner Network](#) [AWS Marketplace](#) [Customer Enablement](#) [Events](#) [Explore More](#) [Contact Us](#) [Support](#) [English](#) [My Account](#) [Create an AWS Account](#)

Explore Our Solutions


By Industry



Advertising & Marketing

Achieve cost-efficiency for petabyte-scale analytics and single-digit millisecond latency workloads.


[Learn More](#)



Financial Services

Less cost. More resiliency. Explore AWS solutions across banking, payments, capital markets, and insurance.


[Learn More](#)



Game Tech

Create computationally ridiculous games across all genres and platforms.

[Learn More](#)




Media & Entertainment

From content creation to distribution, purpose-built media solutions so you can move faster, smarter, and more efficiently.

[Learn More](#)

[View All Industries »](#)


By Technology Category



Analytics & Data Lakes

Securely store, categorize, and analyze all your data in one, centralized repository.


[Learn More](#)



Machine Learning

Build with powerful services and platforms, and the broadest machine learning framework support anywhere.


[Learn More](#)



Serverless Computing

Build and run applications and services without thinking about servers.

[Learn More](#)



Storage

Durable, cost-effective options for backup, disaster recovery, and data archiving at petabyte scale.

[Learn More](#)

Python

https://edube.org/?gclid=Cj0KCQjwlMaGBhD3ARIsAPvWd6iejHxfXWKrqy1GdeagH8dG0mOJYbqVbHzq0U8V3rAQU52oF4ay1eYaAo5OEALw_wcB

The screenshot displays the OpenEdg Learning & Assessment website. At the top, the OpenEdg logo is on the left, and 'Log in' and 'Sign up' buttons are on the right. A large banner features a green Python snake in a jungle setting with the text 'PYTHON ESSENTIALS COURSE' and 'Sign up today!'. Below the banner, there are filter buttons for 'Courses' (selected), 'Certifications', 'Level', 'Category', 'Technology', and 'Clear'. A grid of course cards is shown, including 'Python Essentials 1', 'Python Essentials 2', 'Advanced OOP', 'Best Practices and Standardization', 'GUI Programming', 'Working with RESTful APIs', 'File Processing', and 'C++ Essentials 1'. Each card includes the course title, Python Institute logo, course ID, level, and alignment with industry standards.

Course Title	Course ID	Level	Alignment
Python Essentials 1	PYTHON ESSENTIALS 1 Python 101 (PE1)	BEGINNER	Aligned with PCEP-30-01/PCEP-30-02
Python Essentials 2	PYTHON ESSENTIALS 2 Python 102 (PE2)	INTERMEDIATE	Aligned with PCAP-31-02/PCAP-31-03
Advanced OOP	PYTHON ADVANCED 1 Python 201 (Advanced OOP)	ADVANCED	Aligned with PCPP-32-101
Best Practices and Standardization	PYTHON ADVANCED 2 Python 202 (PEPs)	ADVANCED	Aligned with PCPP-32-101
GUI Programming			
Working with RESTful APIs			
File Processing			
C++ Essentials 1			

Security information and event management (SIEM)

- [Datadog Security Monitoring](#) EDITOR'S CHOICE A cloud-native network monitoring and management system that includes real-time security monitoring and log management.
- [SolarWinds Security Event Manager](#) (FREE TRIAL) One of the most competitive
- [ManageEngine EventLog Analyzer](#) (FREE TRIAL) A SIEM tool that manages, protects, and mines log files. This system installs on Windows, Windows Server, and Linux.

Security information and event management (SIEM)

- [Splunk Enterprise Security](#) This tool for Windows and Linux is a world leader because it combines network analysis with log management together with an excellent analysis tool.
- [OSSEC](#) The Open-source HIDS Security system that is free to use and acts as a Security Information Management service.
- [LogRhythm NextGen](#) SIEM Platform Cutting-edge AI-based technology underpins this traffic and log analysis tool for Windows and Linux.

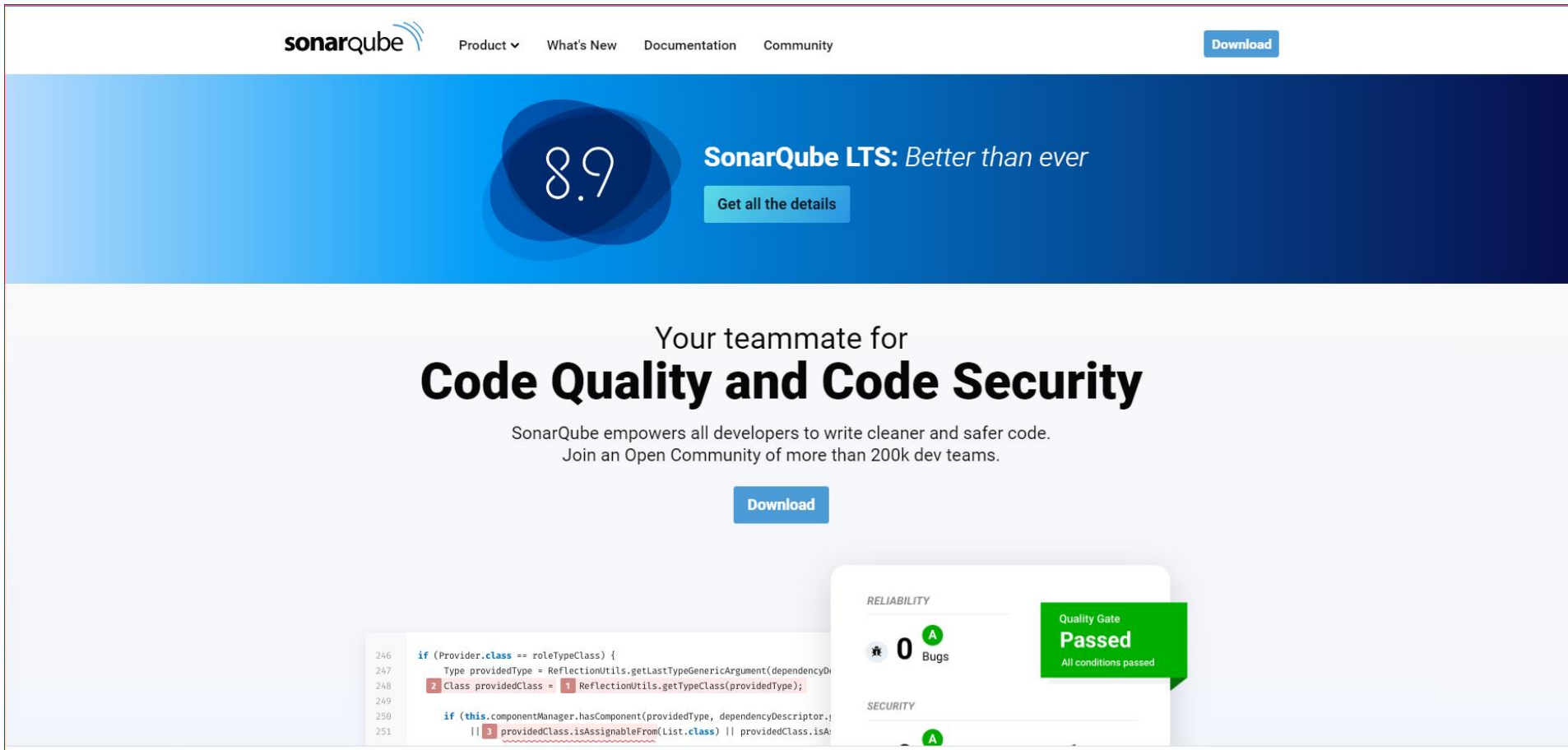
Security information and event management (SIEM)

- [AT&T Cybersecurity](#) AlienVault Unified Security Management Great value SIEM that runs on Mac OS as well as Windows.
- [RSA NetWitness](#) Extremely comprehensive and tailored towards large organizations but a bit too much for small and medium-sized enterprises. Runs on Windows.
- [IBM QRadar](#) Market-leading SIEM tool that runs on Windows environments.
- [McAfee Enterprise Security Manager](#) Popular SIEM tool that runs through your Active Directory records to confirm system security. Runs on Mac OS as well as Windows.
- [ArcSight Intelligence](#) - World-Class Threat Hunting Combine endpoint data with UEBA to unlock world-class threat intelligence. Request a demo. Detect insider threats & bad actors faster using ArcSight Intelligence UEBA. Get started. Detect Insider Threats. Use Behavior Analytics. Prioritize Threat Leads.

Network Security

- Palo Alto Networks - Leader in Global Cybersecurity
- <https://www.paloaltonetworks.com/>
- Palo Alto Networks Protects Millions of Remote Workers with Next-Generation Cybersecurity. Rapidly Onboard Remote Users at Scale with Prisma Access & Next-Generation Firewall.
- BlueCoat system [Symantec](#)
- Blue Coat Systems was a company that provided hardware, software, and services designed for cybersecurity and network management. In 2016, it was acquired by and folded into Symantec.
- The appliance sat behind corporate firewalls to filter website traffic for viruses, worms and other harmful software.
- It had a custom operating system called Security Gateway and provided many of its security features through partners, like Symantec and Trend Micro.
- The Blue Coat Secure Web Gateway solution provides a layered defense system that includes next-generation URL filtering, central policy management and the WebPulse cloud defense that provides 24/7 security against the latest malware attacks.

SonarQube LTS - <https://www.sonarqube.org/>



The screenshot shows the SonarQube website homepage. At the top, there is a navigation bar with the SonarQube logo, a dropdown menu for 'Product', links for 'What's New', 'Documentation', and 'Community', and a 'Download' button. The main banner features a large blue circle with the number '8.9' and the text 'SonarQube LTS: Better than ever' with a 'Get all the details' button. Below this, the text reads 'Your teammate for Code Quality and Code Security' and 'SonarQube empowers all developers to write cleaner and safer code. Join an Open Community of more than 200k dev teams.' with another 'Download' button. At the bottom, there is a code editor snippet showing Java code with SonarQube annotations and a 'Quality Gate Passed' badge.

sonarqube Product What's New Documentation Community [Download](#)

8.9 **SonarQube LTS: Better than ever** [Get all the details](#)

Your teammate for
Code Quality and Code Security

SonarQube empowers all developers to write cleaner and safer code.
Join an Open Community of more than 200k dev teams.

[Download](#)

```
246 if (Provider.class == roleTypeClass) {
247     Type providedType = ReflectionUtils.getLastTypeGenericArgument(dependencyDe
248     2 class providedClass = 1 ReflectionUtils.getTypeClass(providedType);
249
250     if (this.componentManager.hasComponent(providedType, dependencyDescriptor.)
251         || 3 providedClass.isAssignableFrom(List.class) || providedClass.isA
```

RELIABILITY
0 Bugs

SECURITY
A

Quality Gate
Passed
All conditions passed

NMAP Tool

- 1. Nmap
- The Network Mapper (Nmap) is a tool for exploring a target network or system. Nmap has a great deal of built-in knowledge in the form of a wide variety of different scan types. These different types of scans are designed to evade defenses or detect unique features that can be used to identify particular operating systems or applications.
- Nmap balances usability and configurability. For novice users, the Zenmap GUI provides a point-and-click interface for performing simple scans. However, both Nmap and Zenmap also allow more advanced users to apply a range of flags to precisely configure the details of their network scan.
- Nmap and Zenmap both provide a running commentary on the state of the scan and the tests performed. At the end, both a text-based and visual (in Zenmap) result is presented that outlines the detected systems, ports and protocols identified by the scan.
- Nmap and Zenmap are available [here](#).

NESSUS Tool

- Nessus
- Nessus is the only commercial tool on this list. It is available from Tenable under multiple different licensing models. A free version limits the number of IPs that can be scanned, while paid licenses allow unlimited scans and deployment of multiple scanners.
- Nessus is the most popular vulnerability scanner due to its extensive library of vulnerability signatures. A Nessus scan will examine the target machine, identify running services and provide a list of detected vulnerabilities along with additional information for exploitation and remediation. These scans provide a penetration tester with a list of potential attack vectors for gaining access to a target network or system.
- Nessus is available from Tenable's website [here](#)

Wireshark Tool

- Wireshark
- For network sniffing, Wireshark is by far the best tool available. Wireshark provides a large number of built-in protocol dissectors, enabling it to identify a range of different types of network traffic and break them down into an easily readable format. The Wireshark GUI labels each field of a network packet and provides built-in traffic coloring, filtering and connection following to help with identifying packets of interest.
- Under the hood, Wireshark is much more than just a pretty packet dissector. It includes a great deal of built-in functionality for network traffic analysis and is extensible to allow analysis of custom traffic. This makes it invaluable for penetration testing, since it allows testers to easily and rapidly extract features of interest from a network traffic capture.
- Wireshark can be downloaded [here](#).

Burp Suite Tool

- Burp Suite
- Burp Suite is a collection of application security testing tools developed by Portswigger. Of these tools, the most famous is likely Burp Proxy, their web proxy.
- Burp Proxy makes it possible for a penetration tester to perform a man-in-the-middle (MitM) attack, sitting between a webserver and a browser (their own or someone else's). This enables them to examine and modify network traffic en route, making it possible to detect and exploit vulnerabilities or data leakages within a web application.
- Burp Proxy — and the rest of Burp Suite — can be found [here](#).

John the Ripper Tool

- John the Ripper
- John the Ripper is a well-known and widely-used password cracking tool. It is designed primarily for use on CPUs, but it also supports GPUs for faster cracking.
- John the Ripper supports all of the most common cracking techniques (brute-force, dictionary and hybrid) and has a large library of supported hash formats. It is also a highly-flexible and configurable tool, allowing users to specify unique combinations of hash functions and generate custom candidate password formats for dictionary attacks.
- To learn more about and download John the Ripper, visit [here](#).

More useful Links

- <https://www.brighttalk.com/webcast/18576/452328>
- Top Considerations When Auditing Cloud Computing Systems

- Understanding Modern Software Development with i3 Secure & Veracode
- https://www.brighttalk.com/webcast/12807/452288?utm_source=i3Secure&utm_medium=brighttalk&utm_campaign=452288

- <https://www.youtube.com/c/knowledgeindia>

- [https://www.the-center.org/Blog/October-2020/ISO-9001-%E2%80%93-A-Key-to-Cybersecurity-\(Part-1\)](https://www.the-center.org/Blog/October-2020/ISO-9001-%E2%80%93-A-Key-to-Cybersecurity-(Part-1))

- [https://www.the-center.org/Blog/November-2020-\(1\)/ISO-9001-%E2%80%93-A-Key-to-Cybersecurity-\(Part-2\)](https://www.the-center.org/Blog/November-2020-(1)/ISO-9001-%E2%80%93-A-Key-to-Cybersecurity-(Part-2))

- https://www.youtube.com/watch?v=_nVq7f26-Uo&feature=youtu.be

Other things to know

- Email security , PGP
- Email Phishing
- Data security
- Vendor security