Roadmap

Getting Started In Cybersecurity

Do Things DFIRINTLY

A message from MyDFIR.

Thank you for the support. Cybersecurity is a field that is difficult in getting started, as it should be. You no longer have to walk this journey alone. My sole mission is to help you wherever you are in the world and in your career.

Lets get started.

About This Roadmap

This roadmap focuses on **how to get started into cybersecurity** and was created for individuals who are hoping to **transition into this field**. I will walk through the steps on where to begin, what to focus on, and what to do next. There are 5 pillars listed below that you will need to keep in mind to **be successful** in the field of cybersecurity and I will go over them, one by one.

- Time
- Dedication
- Commitment
- Purpose
- Curiosity

Do Things DFIRINTLY

5 Pillars Of Success

Getting Started In Cybersecurity

Time

You will need to be patient to excel in this field as it will take a lot of **time** in the beginning to get started. There is a lot to learn.

Cybersecurity is a marathon and not a sprint.

Dedication

Cybersecurity requires focus and attention.

Be ready to **dedicate** your time to this field, specially in a domain of interest.

Commitment

Cybersecurity is not easy.

A **commitment** to really understand and learn the concepts of cybersecurity will go a long way.

Purpose

Understand your **purpose** into why cybersecurity.

If it is only about money, this field may burn you out quicker than you would like.

If it is about passion and interest, strap in and get ready.

Curiosity

Always be cat. Focus on understanding the “why”.

Curiosity will help you in cybersecurity by asking the right questions to getting answers to the “why”.

Roadmap

Cybersecurity Journey

Some IT Experience

Create a cover letter and resume which includes the skills you had learned during hands-on labs & blog posts.

Create a blog and each lab you have completed, write a blog post to demonstrate your skills.

Look for hands-on labs to gain relevant experience in tools and develop a methodology

Study and obtain Security+. Obtain Network+ (Optional) for better knowledge of networks.

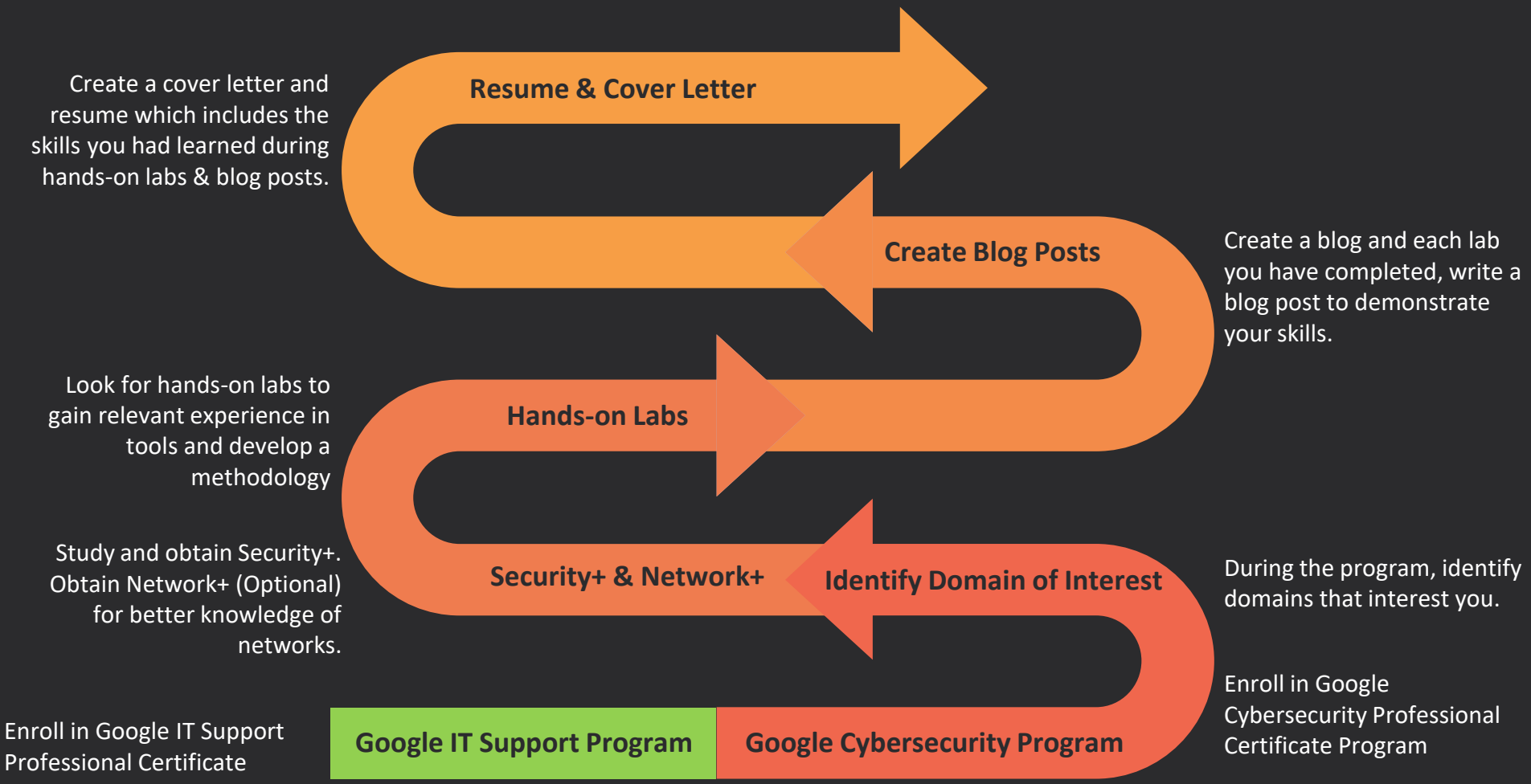
During the program, identify domains that interest you.

Enroll in Google Cybersecurity Professional Certificate Program

Roadmap

Cybersecurity Journey

No IT Experience



Create a cover letter and resume which includes the skills you had learned during hands-on labs & blog posts.

Create a blog and each lab you have completed, write a blog post to demonstrate your skills.

Look for hands-on labs to gain relevant experience in tools and develop a methodology

Study and obtain Security+. Obtain Network+ (Optional) for better knowledge of networks.

During the program, identify domains that interest you.

Enroll in Google IT Support Professional Certificate Program

Enroll in Google Cybersecurity Professional Certificate Program

Google Cybersecurity Professional Certificate

Google

Google Cybersecurity Professional Certificate

This is your path to a career in cybersecurity. In this certificate program, you'll learn in-demand skills that can have you job-ready in less than 6 months. No degree or experience required.

(Affiliate) Enroll Here: Google Cybersecurity Professional Certificate

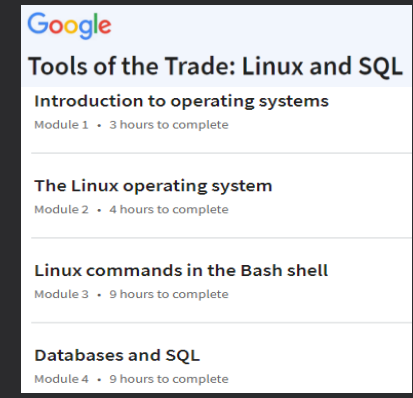
Professional Certificate - 8 course series
Earn a career credential that demonstrates your expertise

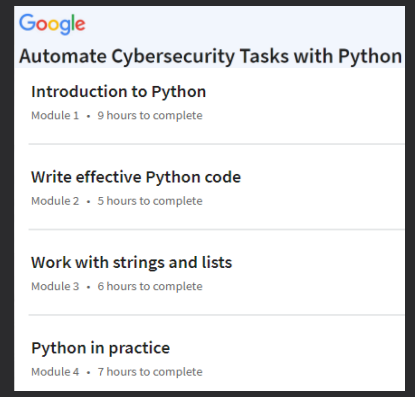
4.9 ★ (3,569 reviews)

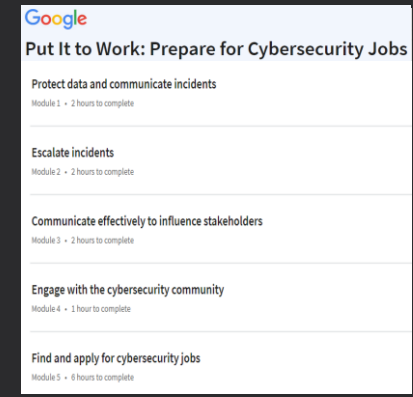
Beginner level
No previous experience necessary

6 months at 7 hours a week

Flexible schedule
Learn at your own pace







Identify domains that interest you the most

Google IT Support Professional Certificate

Google

Google IT Support Professional Certificate

This is your path to a career in IT. In this program, you'll learn in-demand skills that will have you job-ready in less than 6 months. No degree or experience required.

(Affiliate) Enroll Here: Google IT Support Professional Certificate

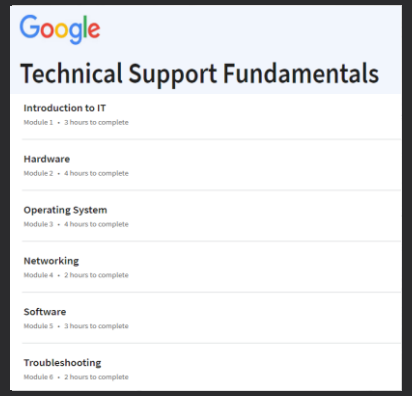
Professional Certificate - 5 course series
Earn a career credential that demonstrates your expertise

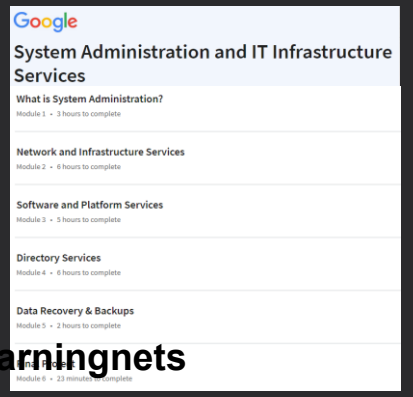
4.8 ★ (163,915 reviews)

Beginner level
Recommended experience ⓘ

6 months at 10 hours a week

Flexible schedule
Learn at your own pace





Supplement your studies with books in IT

CompTIA Security+

Comptia Security+

COMPTIA SECURITY+ VALIDATES CERTIFIED PROFESSIONALS HAVE THE SKILLS REQUIRED TO BE MORE PROACTIVE IN PREVENTING THE NEXT ATTACK

What Skills Will You Learn?

Attacks, Threats and Vulnerabilities

More threats, attacks and vulnerabilities from newer custom devices that must be mitigated, such as IoT and embedded devices, newer DDoS attacks and social engineering attacks based on current events

Architecture and Design

Enterprise environments and reliance on the cloud, which is growing quickly as organizations transition to hybrid networks

Implementation

Administering identity, access management, PKI, basic cryptography, wireless and end-to-end security

Operations and Incident Response

Organizational security assessment and incident response procedures, such as basic threat detection, risk mitigation techniques, security controls and basic digital forensics

Governance, Risk and Compliance

Organizational risk management and compliance with regulations, such as PCI-DSS, SOX, HIPAA, GDPR, FISMA, NIST and CCPA

Get Training Here: CBTNuggets Security+ Training

CompTIA Network+

Comptia Network+

(Optional)

COMPTIA NETWORK+ PROVES YOU HAVE THE SKILLS REQUIRED TO MANAGE TODAY'S NETWORKS

What Skills Will You Learn?

Networking Fundamentals
Explain basic networking concepts including network services, physical connections, topologies and architecture, and cloud connectivity

Network Implementations
Explain routing technologies and networking devices; deploy ethernet solutions and configure wireless technologies

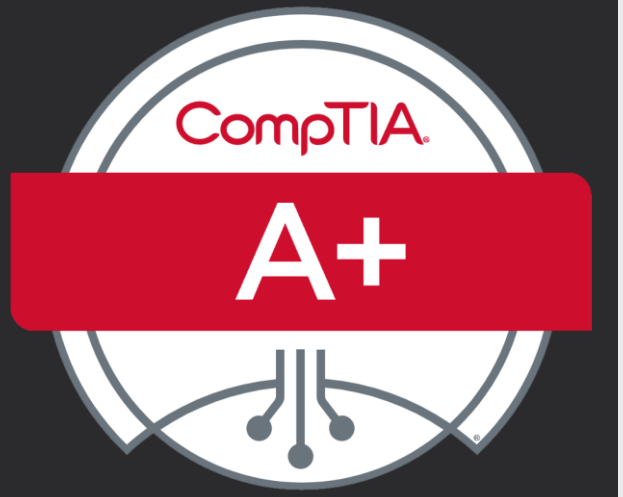
Network Operations
Monitor and optimize networks to ensure business continuity

Network Security
Explain security concepts and network attacks in order to harden networks against threats

Network Troubleshooting
Troubleshoot common cable, connectivity and software issues related to networking

Get Training Here: CBTNuggets Network+ Training

CompTIA A+



Comptia A+

(Optional)

COMPTIA A+ VALIDATES CERTIFIED PROFESSIONALS HAVE THE SKILLS REQUIRED TO SUPPORT TODAY'S DIGITAL WORLD

What Skills Will You Learn?

Hardware
Identifying, using and connecting hardware components and devices, including the broad knowledge about different devices that is now necessary to support the remote workforce

Operating Systems
Install and support Windows OS including command line and client support, system configuration imaging and troubleshooting for Mac OS, Chrome OS, Android and Linux OS

Software Troubleshooting
Troubleshoot PC and mobile device issues including common OS, malware and security issues

Networking
Explain types of networks and connections including TCP/IP, WIFI and SOHO

Troubleshooting
Troubleshoot real-world device and network issues quickly and efficiently

Security
Identify and protect against security vulnerabilities for devices and their network connections

Mobile Devices
Install and configure laptops and other mobile devices and support applications to ensure connectivity for end users

Virtualization and Cloud Computing
Compare and contrast cloud computing concepts and set up client-side virtualization

Operational Procedures
Follow best practices for safety, environmental impacts, and communication and professionalism

Get Training Here: CBTNuggets A+ Training

Hands-On Labs

All about gaining practical experience

TryHackMe

Hands-on Cyber security training through real-world scenarios

HackTheBox

Software platform to sharpen offensive and defensive security expertise.

CyberDefenders

Training platform focused on the defensive side of cybersecurity to learn, validate, and advance CyberDefense skills.

Blue Team Level One

A gamified platform for defenders to practice their skills in security investigations and challenges

LetsDefend

Hands-on experience by investigating real cyber attacks inside a simulated SOC.

OverTheWire

Learn and practice security concepts in the form of fun-filled games.

UnderTheWire

PowerShell Training for the People

picoCTF

The largest high school hacking competition now provides year-round cyber security education content for learners of all skill levels.

Hands-On Labs

All about gaining practical experience

TryHackMe

Site: https://tryhackme.com

LetsDefend

Site: https://letsdefend.io

HackTheBox

Site: https://www.hackthebox.com

OverTheWire

Site: https://overthewire.org

CyberDefenders

Site: https://cyberdefenders.org

UnderTheWire

Site: https://underthewire.tech

Blue Team Level One

Site: https://blueteamlabs.online

picoCTF

Site: https://picoctf.org

Creating A Blog Post

The main purpose of a blog post is to demonstrate both your technical and written skills. This will allow you to stand out and have something interesting to talk about during an interview.

Free Blog Sites

Resources to create your FREE blog

Wix

Create a free website without limits.
Site: https://www.wix.com/

LinkedIn

Free to publish articles about your expertise and interest
Site: https://www.linkedin.com/

Medium

Create a blog for free to have a personalized home for your writing.
Site: https://medium.com/

Weebly

Suitable for all categories business and personal presentation
Site: https://www.weebly.com/

Blogger

Create a unique and beautiful blog easily.
Site: https://www.blogger.com

Name

City,State ▪ Phone Number ▪ Email

SUMMARY OF QUALIFICATIONS

- Add 5 to 10 qualifications on why you are qualified for this job

AREAS OF EXPERTISE

- **Category** – List tools, see below for example
- **SIEM** – LogRhythm, Splunk/Splunk SOAR, IBM QRadar

EDUCATION

What you majored in, diploma, degree etc. Begin Date – End Date
School, City, State

RELATED WORK EXPERIENCE

Current Position Month Year – Present
Company

- List relevant work experience tied to the job positing

Previous Position Month Year – Month Year
Company

- List relevant work experience tied to the job posting

CERTIFICATIONS

Certificate **Month Obtained Year**
Vendor

<Below is optional>

WEBSITE

Title of site
Website URL

- List what the site is about

TRAININGS

Title of training **Month Year Completion**
Vendor

- List what the training was about and make sure its related to the job

Resume Template

Download the template here

Cover Letter Template

Download the template here

[Your Name]
[City, State]
[Email Address]
[Phone Number]
[Today's Date]

[Recipient's Name]
[Recipient's Job Title]
[Company Name]
[Company Address]
[City, State, ZIP Code]

Dear [Recipient's Name],

First Paragraph: Introduction
Introduce yourself and state your intention to apply for the position. Show enthusiasm for the opportunity and mention where you learned about the job opening.

Second Paragraph: Relevant Skills and Experience
Highlight your relevant skills, certifications, and experience (including lab experience) in the field of cybersecurity. Provide specific examples of projects or achievements that demonstrate your ability to secure information systems, mitigate risks, and respond to incidents.

Third Paragraph: Company Fit and Interest
Show your knowledge of the company's initiatives and explain why you are interested in working for them. Highlight specific aspects of the company's reputation, client base, or industry focus that resonate with you. This demonstrates your genuine interest and dedication to contributing to their goals.

Fourth Paragraph: Closing and Next Steps
Express gratitude for considering your application and reiterate your interest in the position. State that you are eager to discuss your qualifications further and provide your availability for an interview. Mention that you have attached your resume and any other relevant documents for their review. If you have a website/blog, list it here.

Sincerely,

[Your Name]

1-Year Timeline (12 Months)

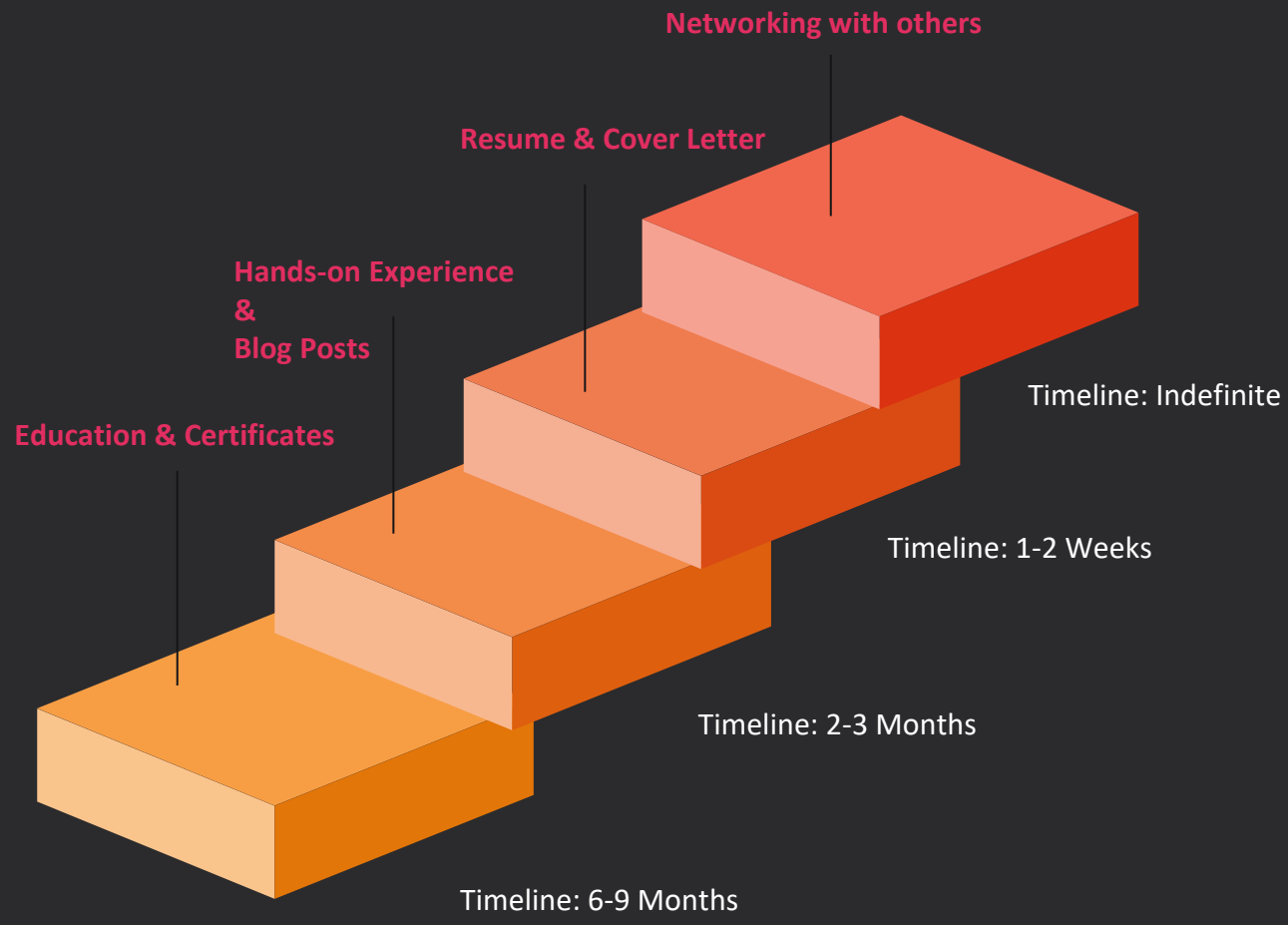
Cybersecurity Journey

Here is an ambitious timeline to transition into cybersecurity within 1 year assuming **you have some prior IT experience**.

I strongly believe people who put in the work and follow the 5 pillars can achieve this.

Be true to yourself and don't try to rush the process.

"More haste, less speed"



Do Things DFIRINTLY

1.5-Year Timeline (18 Months)

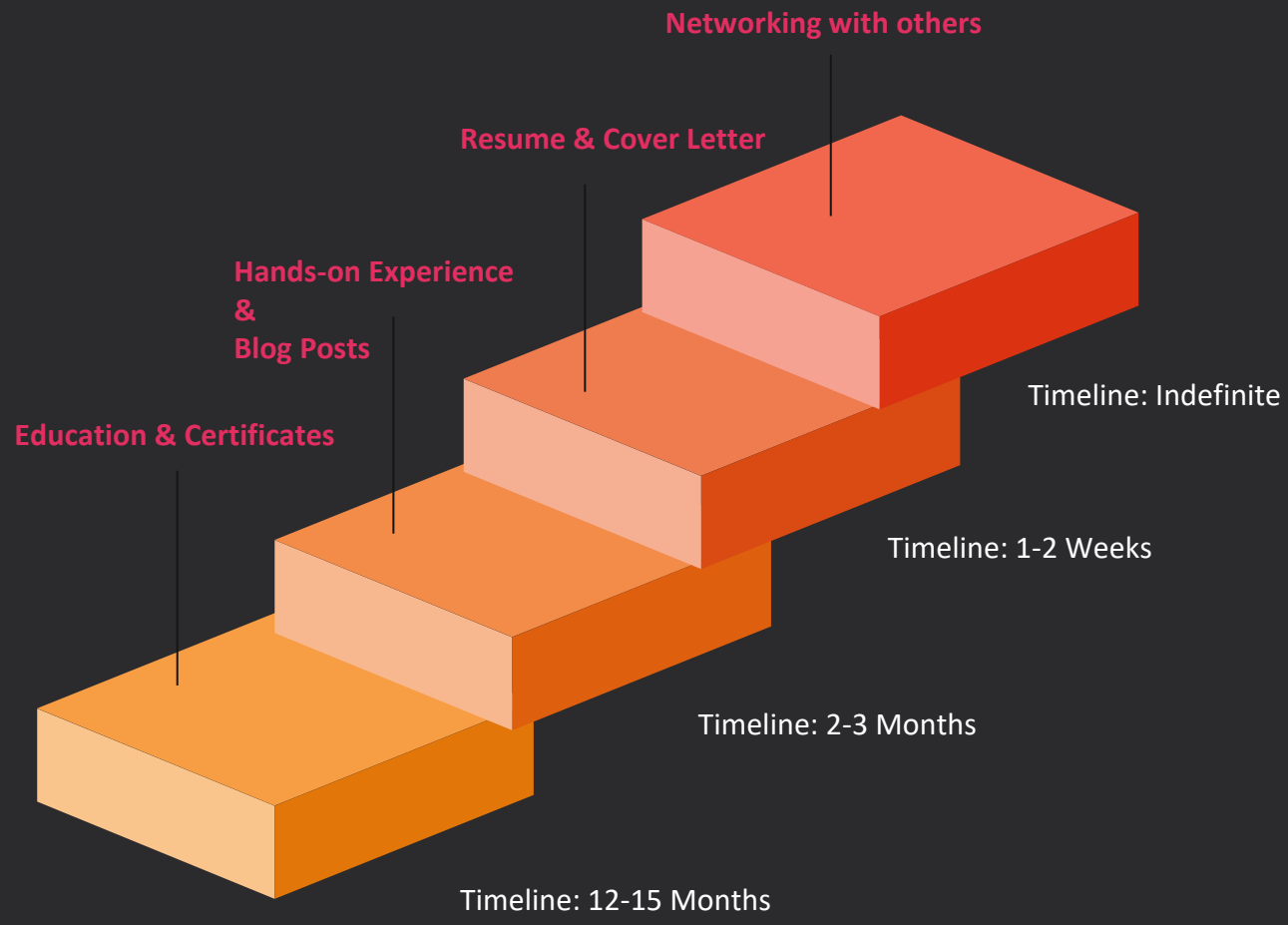
Cybersecurity Journey

Here is an ambitious timeline to transition into cybersecurity within 1.5 years assuming **you have no prior IT experience**.

I strongly believe people who put in the work and follow the 5 pillars can achieve this.

Be true to yourself and don't try to rush the process.

"More haste, less speed"

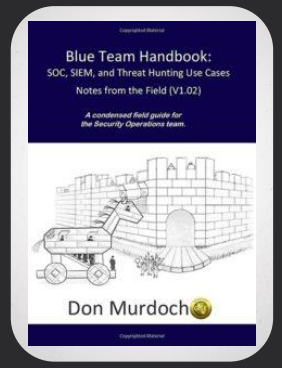


Do Things DFIRINTLY

Recommended Books

Resources specific to Security Operations & DFIR Analysts

These are all affiliate links



Blue Team Handbook: SOC, SIEM,& Threat Hunting

BTHb:SOCTH is the go to guiding book for new staff at a top 10 MSSP, integrated into University curriculum, and cited in top ten courses from a major information security training company.

Purchase

Blue Team Handbook: Incident Response

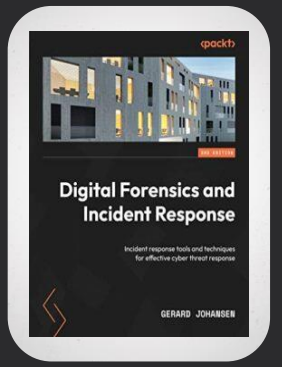
The Blue Team Handbook is a “zero fluff” reference guide for cyber security incident responders, security engineers, and InfoSec pros alike.

Purchase

Applied incident Response

Incident response is critical for the active defense of any network, and incident responders need up-to-date, immediately applicable techniques with which to engage the adversary.

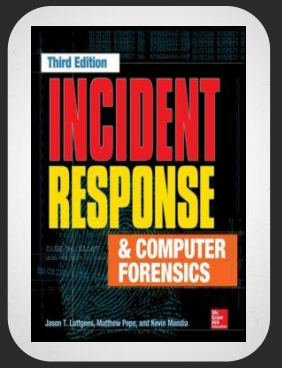
Purchase



DFIR - Incident response tools and techniques for effective cyber threat response, 3rd Edition

An understanding of how digital forensics integrates with the overall response to cybersecurity incidents is key to securing your organization’s infrastructure from attacks.

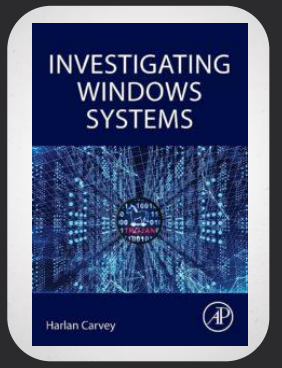
Purchase



Incident Response & Computer Forensics, Third Edition

Thoroughly revised to cover the latest and most effective tools and techniques, Incident Response & Computer Forensics, Third Edition arms you with the information you need to get your organization out of trouble when data breaches occur.

Purchase



Investigating Windows Systems

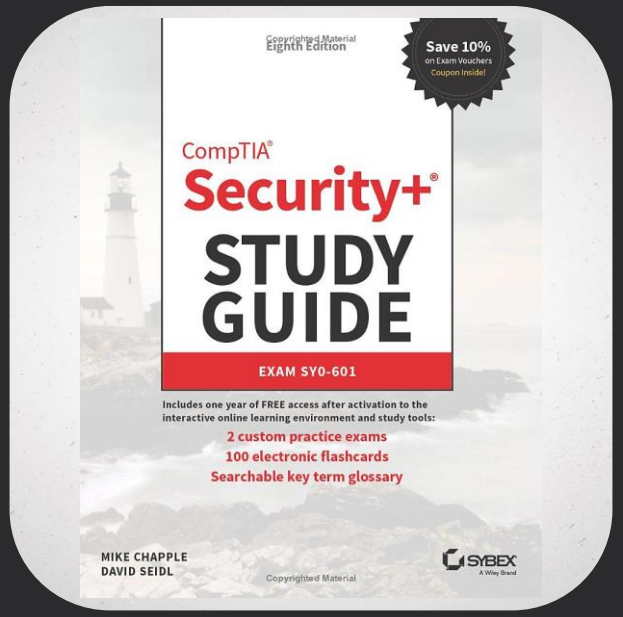
Unlike other books, courses and training that expect an analyst to piece together individual instructions into a cohesive investigation, Investigating Windows Systems provides a walk-through of the analysis process, with descriptions of the thought process and analysis decisions along the way.

Purchase

Study Guides

Resources to help with certifications

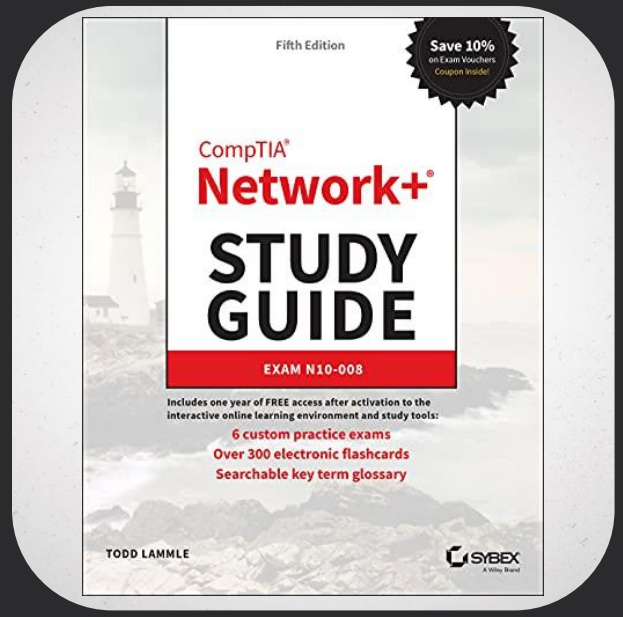
These are all affiliate links



CompTIA Security+ Study Guide: SY0-601

The Eighth Edition of the CompTIA Security+ Study Guide Exam SY0-601 efficiently and comprehensively prepares you for the SY0-601 Exam.

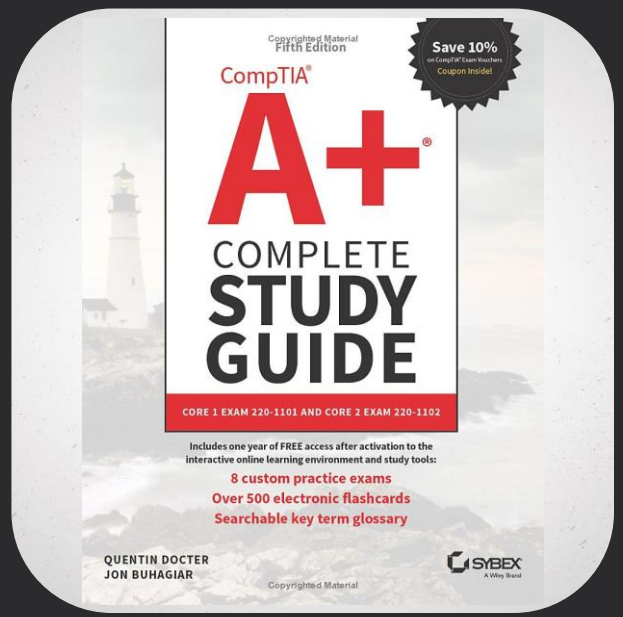
Purchase



CompTIA Network+ Study Guide: Exam N10-008

In the newly revised Fifth Edition of CompTIA Network+ Study Guide Exam N10-008, bestselling author and network expert Todd Lammle delivers thorough coverage of how to install, configure, and troubleshoot today's basic networking hardware peripherals and protocols.

Purchase



CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam 220-1102

The Fifth Edition of the CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam 220-1102 offers accessible and essential test preparation material for the popular A+ certification.

Purchase

Next Steps

Thank you for the support. I hope you have learned something new and are excited to get started on your journey into cybersecurity.

Sign up for **FREE** mentorship if you haven't already on my site: MyDFIR.com and keep me updated in your progress.

You Got This.