

Leveling-up your workforce for cloud enablement

pathways to total pwnage

@aarondlancaster



Who Am I?

@aarondlancaster

```
>>> dir(aaron_d_lancaster)
['___init__',
 '__followChrist__',
 '__loveWife__',
 '__raiseKids__',
 '__flyHelos__',
 '__flyDrones__',
 'assess_environments',
 'call_CQ',
 'defend_networks',
 'handle_incidents',
 'mentor_infosec',
 'write_python']
```



Aaron Lancaster

Business Information
Security Manager

Masters Student
@SANS_EDU



WARNING: Several PEPs were broken in the making of this slide... sorry.

Agenda

1. Where we are
2. Where we need to go
3. How we get there
4. Q&A

NO LEGAL ADVICE INTENDED

OPINIONS ARE MY OWN

DISCLAIMER:

The materials available herein and via linked websites are for informational purposes only and not for the purpose of providing legal advice. You should contact your attorney to obtain advice with respect to any particular issue or problem. The opinions expressed here or through linked sites are the opinions of the individual authors and may not reflect the opinions of their respective organizations, employers, or any individual attorney.

Link to slides and references will be provided at the end :-)

Rule #1: Know your audience



BEING
A CLOUD WAS
SUCH A CAREFREE
EXISTENCE - NOW
PEOPLE EXPECT SO
MUCH FROM US!

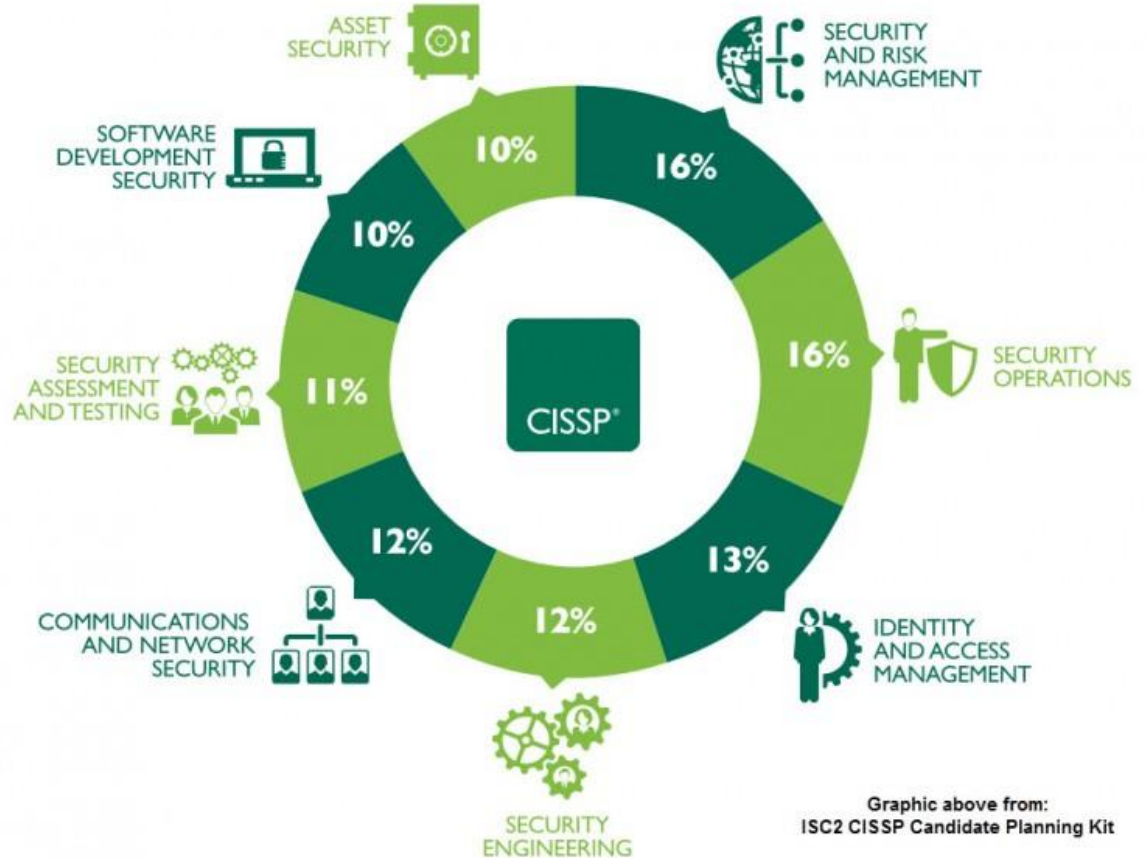
Where we are

Cyber Domains

Red,
Blue,
or
Purple

Common Body of Knowledge (CBK)

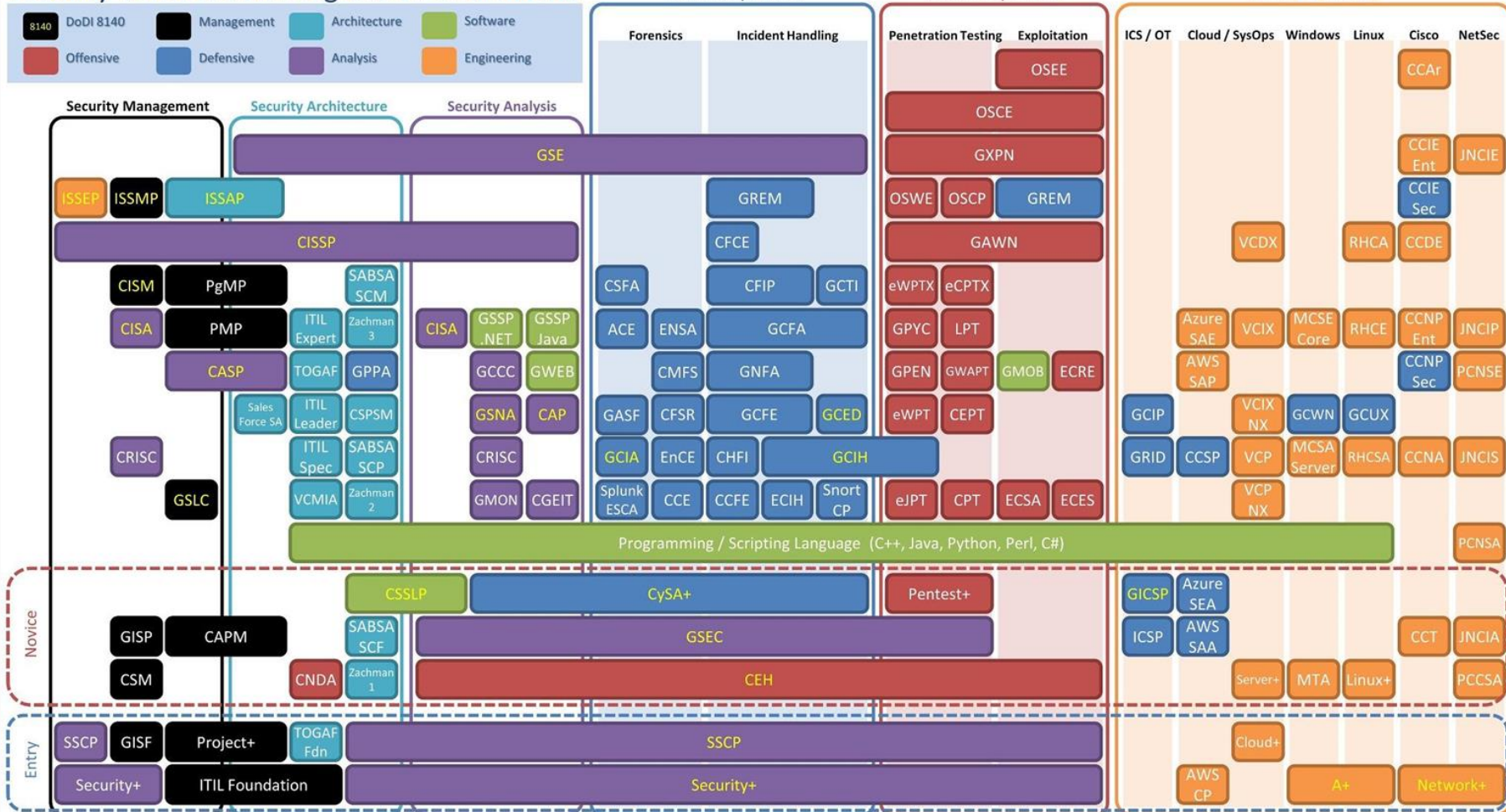
Weight of each of the domain on the exam. You MUST master the top 4.



Cyber Security Career Lifecycle®



Security Certification Progression Chart 2020



Where we need to go



Networking

Development

SysAdmin

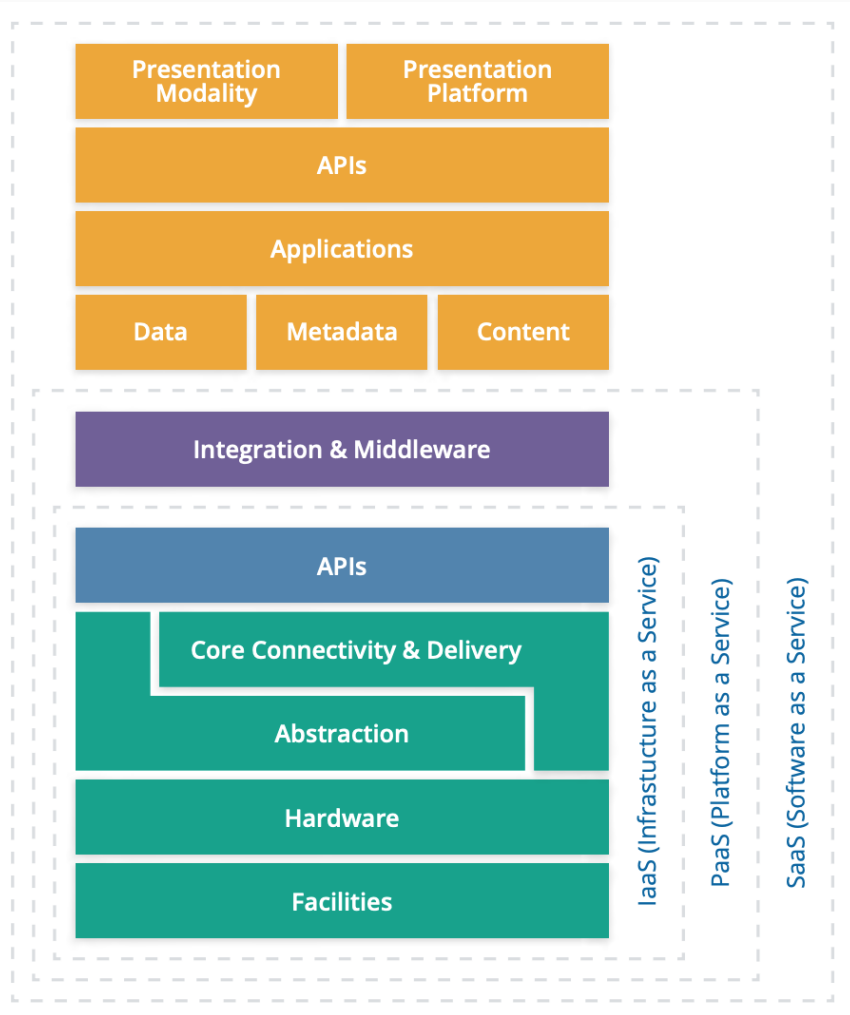


Image credit: CSA

DevOps

- Scripting - Python, Powershell, etc.
- Chaos Engineering

Systems

- Server vs. serverless
- Software Defined Networking

Architecture

- Functional & Security Requirements
- ID necessary pieces

Management

- Cost Opt
- Portfolio
- Business Requirements

DevSecOps

How we get there



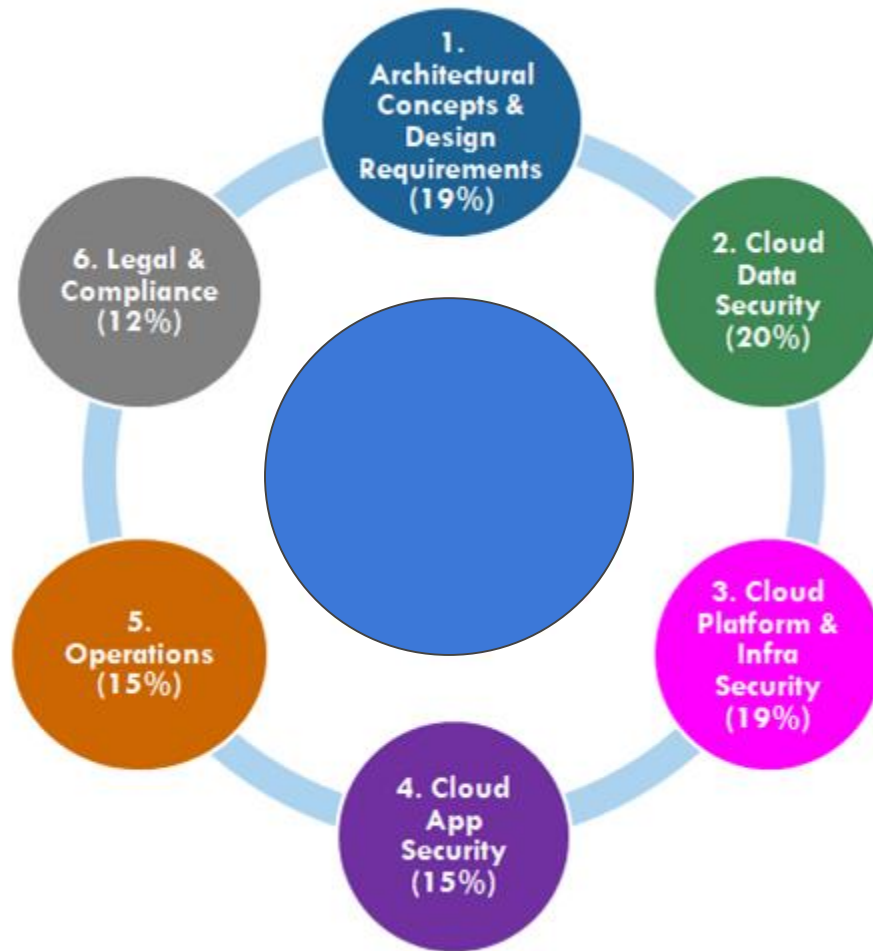
“

**AT LEAST 40% OF ALL BUSINESSES
WILL DIE IN THE NEXT 10 YEARS... IF
THEY DON'T FIGURE OUT HOW TO
CHANGE THEIR ENTIRE COMPANY TO
ACCOMMODATE NEW
TECHNOLOGIES**

JOHN CHAMBERS, EXECUTIVE CHAIRMAN, CISCO SYSTEM

TechsmartDigital





Credit: (ISC)2 CCSP CBK

Certifications

Roles



Information
Security



Consultant



Manager



Security
Architect

Senior

Engineer

Security

SR Cloud

Architect

Director

Solutions Architect

Analyst

Security Analyst

Specialist

Lead

Compliance

Image Credit: CSA

CCSK

Two different formats:

- CCSK Foundation (1 or 2-day course)
- CCSK PLUS (2 or 3-day course)

CCSK PLUS = CCSK Foundation + AWS labs (Dashboard sec., IAM, Mon. & Alert, VPCs and GW, Instances & Immut., VA, S3 & Encrypt., Federation)

New in v4:
containers, CI/CD toolchains, DevOps, Chaos engineering and even more Software Defined Networking (SDN) security

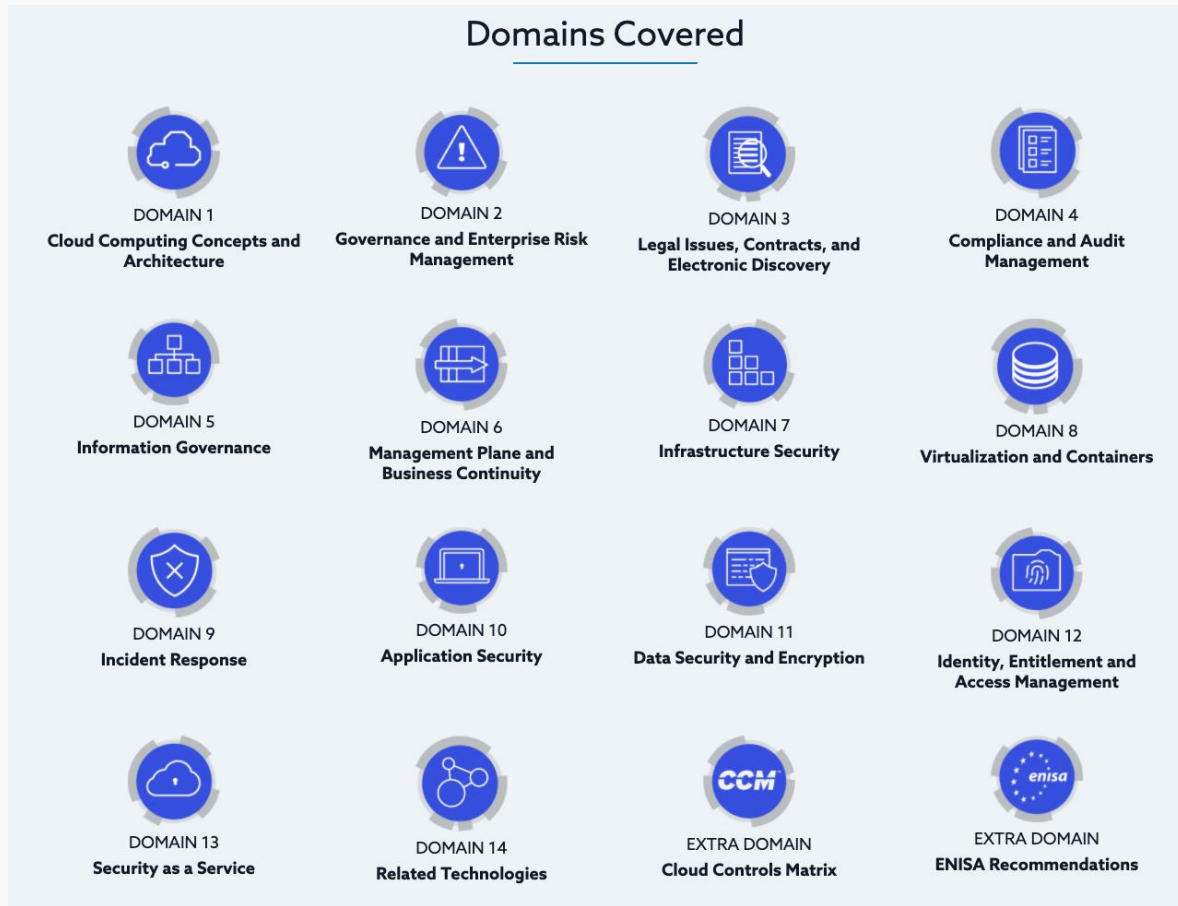


Image Credit: CSA

CCSP

CCSP = CCSK + Expanded
Governance Items +
Traditional Security +
Privacy

NO labs

More suitable for CISSP
holders (assumes you know
that CBK) - ex. OSI model &
encapsulation



Credit: (ISC)2 CCSP CBK

AWS

- CSA-A
- Security Specialty

Professional

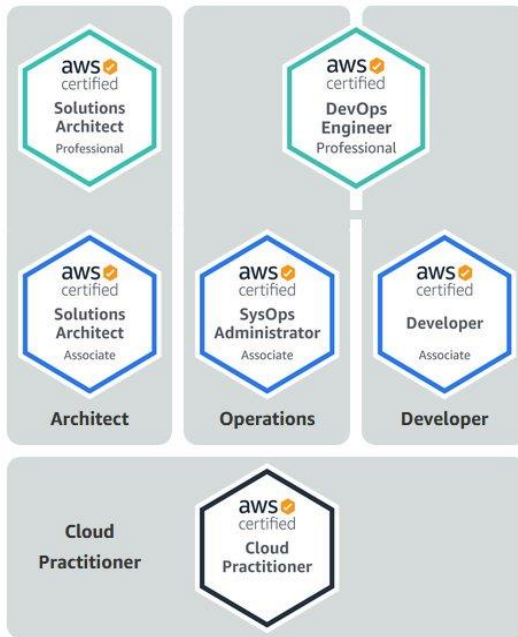
Two years of comprehensive experience designing, operating, and troubleshooting solutions using the AWS Cloud

Associate

One year of experience solving problems and implementing solutions using the AWS Cloud

Foundational

Six months of fundamental AWS Cloud and industry knowledge



Specialty

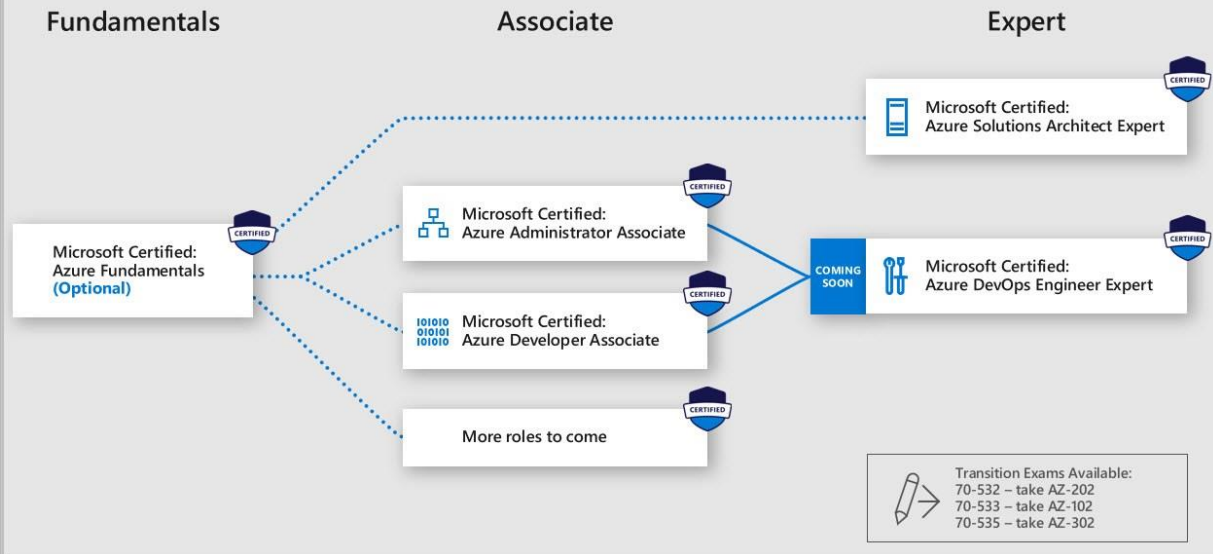
Technical AWS Cloud experience in the Specialty domain as specified in the **exam guide**



Azure

- Role based
- Architect (AZ300) -> Security Engineer (AZ500)

Azure Apps and Infrastructure certifications



<https://docs.microsoft.com/en-us/learn/certifications/posts/new-role-based-certification-and-training-is-here>

SANS

- Integrated approach
- Even baseline classes such as Sec. Essent. (SEC401), Leadership Essent. (MGT512) address cloud topics, and Mgt. Sec. Vulns (MGT516)

SEC540: Cloud Security and DevOps Automation

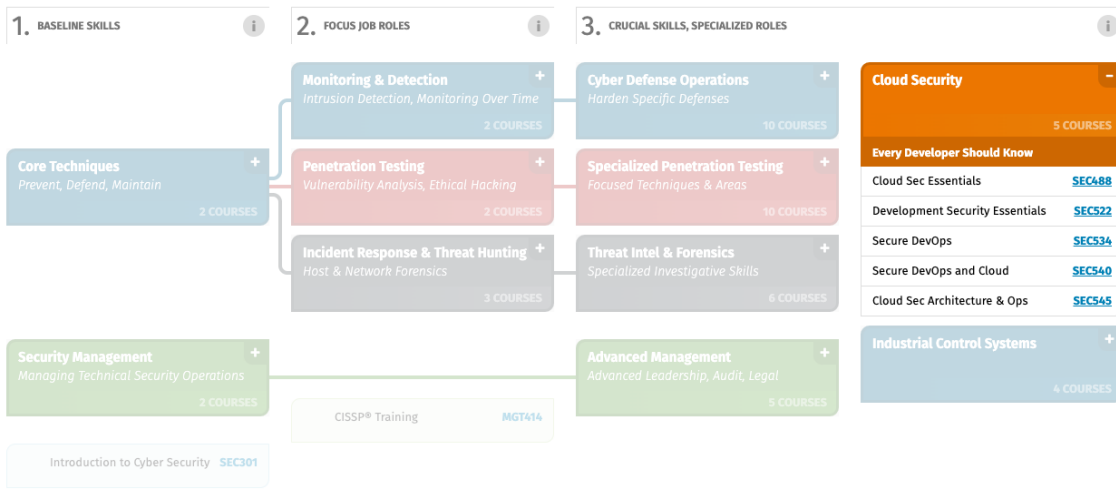
Associated Certification: [GIAC Cloud Security Automation \(GCSA\)](#)

SEC488: Cloud Security Essentials (Beta)

SEC588: Cloud Penetration Testing (Beta)

Cyber Security Skills Roadmap

Explore this interactive training roadmap to find the courses for your immediate cyber security skill development and for your long-term career goals. More than 60 courses deliver critical skills in the cyber defense operations, digital forensics, software development, and management practice areas of cyber security.



<https://www.sans.org/cyber-security-skills-roadmap>

Q&A

Resources

Thanks for listening!

What's your approach?

What did you think of mine?

<https://bit.ly/2L90YYM>

<https://blog.casterlan.com/2020/05/cloud-pro-dev-resource-leveling-up.html>

