

Career in cyber security, where to start ?

Jasmin Azemović

CISO – Head of SecOps | University Professor | Microsoft MVP

HTEC
GROUP



Lecturer



- University Professor
Since 2011
- CISO | Head of SecOps
Since 2019
- Award
Security Microsoft MVP
 - Since 2009



@JasminAzemovic

Agenda

- 01 | Why Careers in Cybersecurity?
- 02 | Current Market Needs
- 03 | Cybersecurity Job Categories
- 04 | Coolest Careers in Cybersecurity
- 05 | Q&A

Why Careers in Cybersecurity?

Cost of data breach

- Increase by 15 % in the last 3 years
- In 2023, the average cost of a data breach has reached a record high of **US\$4.45 million**, according to report by IBM and the Ponemon institute.

<https://www.ibm.com/reports/data-breach>

Johnson & Johnson discloses IBM data breach impacting

- The compromised data could support highly effective phishing, scamming, and social engineering attacks. Considering the value of medical data, there is a high chance they will be sold for a premium on darknet markets.
- Value of one medical record **100-500 USD** (**4,000,000** records)
 - Full name
 - Contact information
 - Date of birth
 - Health insurance information
 - Medication information
 - Medical condition information



Microsoft leaks 38TB (private data)



- The Microsoft AI research division accidentally leaked dozens of terabytes of sensitive data starting in July 2020 while contributing open-source AI learning models to a public GitHub repository.




Hacker leaks millions of new 23andMe genetic data profiles

- A hacker has leaked an additional 4.1 million stolen 23andMe genetic data profiles for people in Great Britain and Germany on a hacking forum.

DNA Data of Celebrities (1 million Ashkenazi REPOST!)

by Addka72424 - Monday October 2, 2023 at 03:12 PM



Addka72424

10-02-2023, 03:12 PM #1

Hello everyone, today i re-uploaded 1 million Ashkenazi database
Originally posted @Golem here - [REDACTED]
lines: 1kk
leak date: don't know
sample:

```
profile_id; account_id; first_name; last_name; sex; birth_year; has_health; ydna; mdna;  
current_location; region_1; region_2; region_3; region_4; region_5; subregion_1; subregion_2; subregion_3; subregion_4; subregion_5; population_id1; population_id2; population_id3
```


Fatal outcome

- The world crossed a red line this month when police directly tied a woman's death to a cyberattack in Germany on Sept. 10. 2020

NEWS



TECH



Report: Cyberattack on German hospital inadvertently causes patient's death



BY NIC KER 12:12 PM, 18 SEPTEMBER 2020 2 COMMENTS







Uber Breach

**Senior Security Engineer - Application Security**
Uber
Dallas, TX
 Actively recruiting
3 days ago

**Senior Security Engineer - Enterprise Security**
Uber
New York, NY
 Actively recruiting
3 days ago 19 applicants

**Senior Security Engineer - Enterprise Security**
Uber
Dallas, TX
 Actively recruiting
3 days ago 14 applicants

**Senior Threat Detection Engineer, Security Engineering (US Remote Available)**
Uber
Baltimore, MD
 Actively recruiting
3 days ago 7 applicants

**Sr Security Engineer - Investigations (US Remote Available)**
Uber
Chicago, IL
 You have a preferred skill badge
3 days ago

(I was spamming employee with push auth for over a hour) i then contacted him on WhatsApp and claimed to be from Uber IT, told him if he wants it to stop he must accept it

6:47 PM

And well, he accepted and I added my device

6:47 PM

“Our recommendation, first and foremost, is to delete your Uber account and create a new one with immediate effect. It might sound drastic but if you care about your personal information it is a small price to pay and can be done quickly. Then, as ever, we recommend setting passwords that are unique and hard for anyone to guess. When it comes to Uber accounts, we recommend people change any passwords that have been used elsewhere, to avoid a domino effect. Also, use this as an opportunity to set up two-factor authentication, something that is mandatory on some sites but voluntary on others.

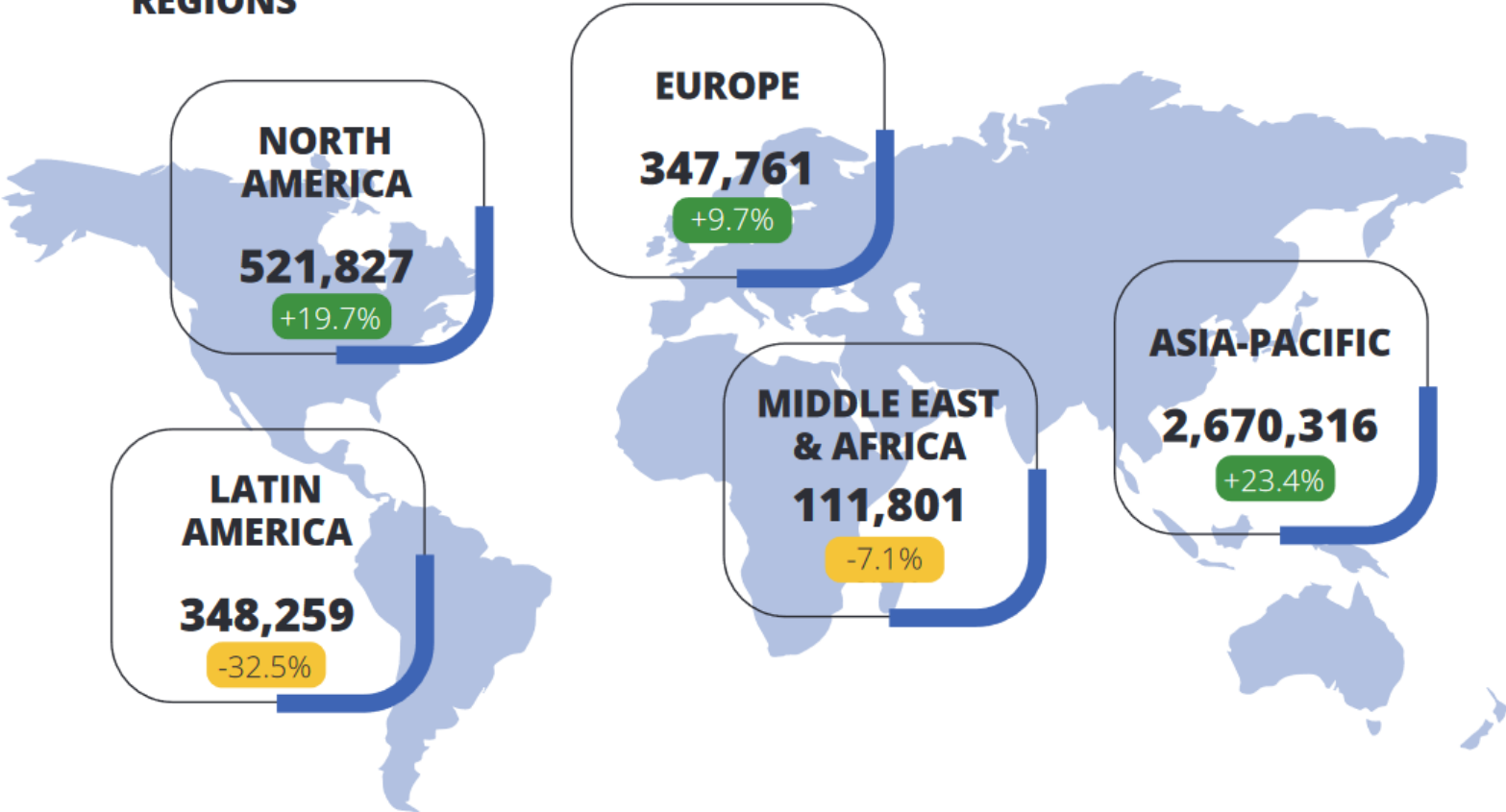
Current market needs

Global Cybersecurity Workforce Estimate (2023)

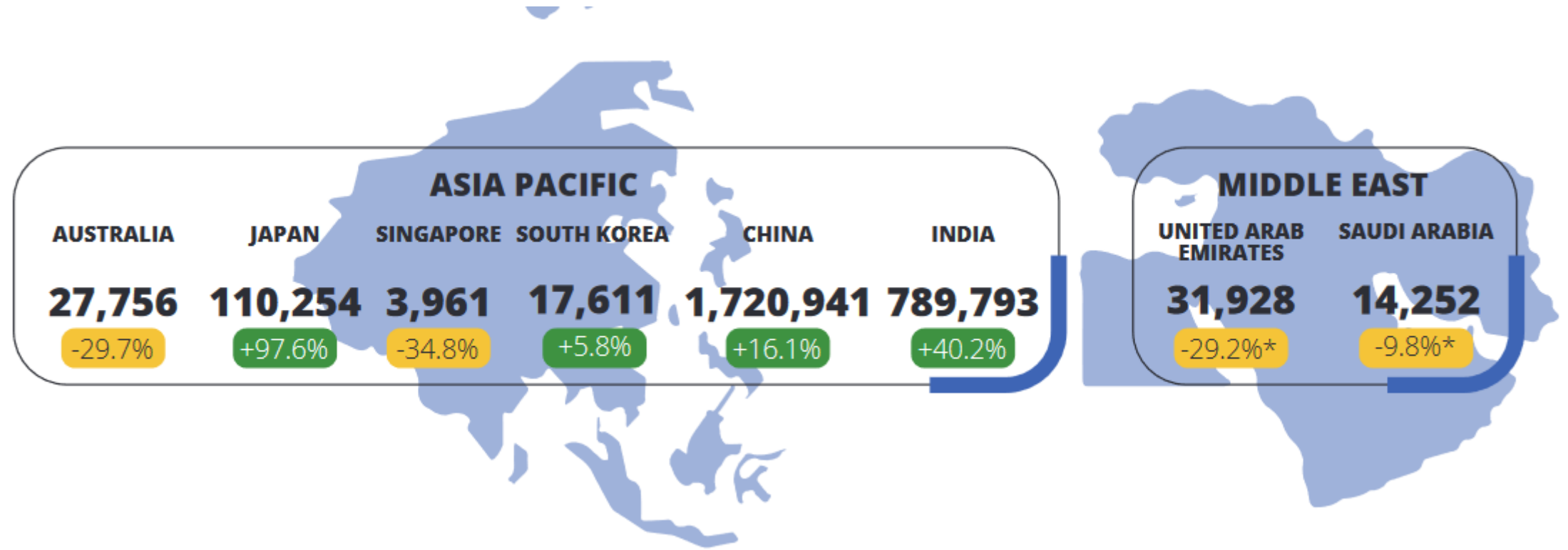
2023 Global Cybersecurity Workforce Gap

3,999,964 +12.6% YoY*

REGIONS

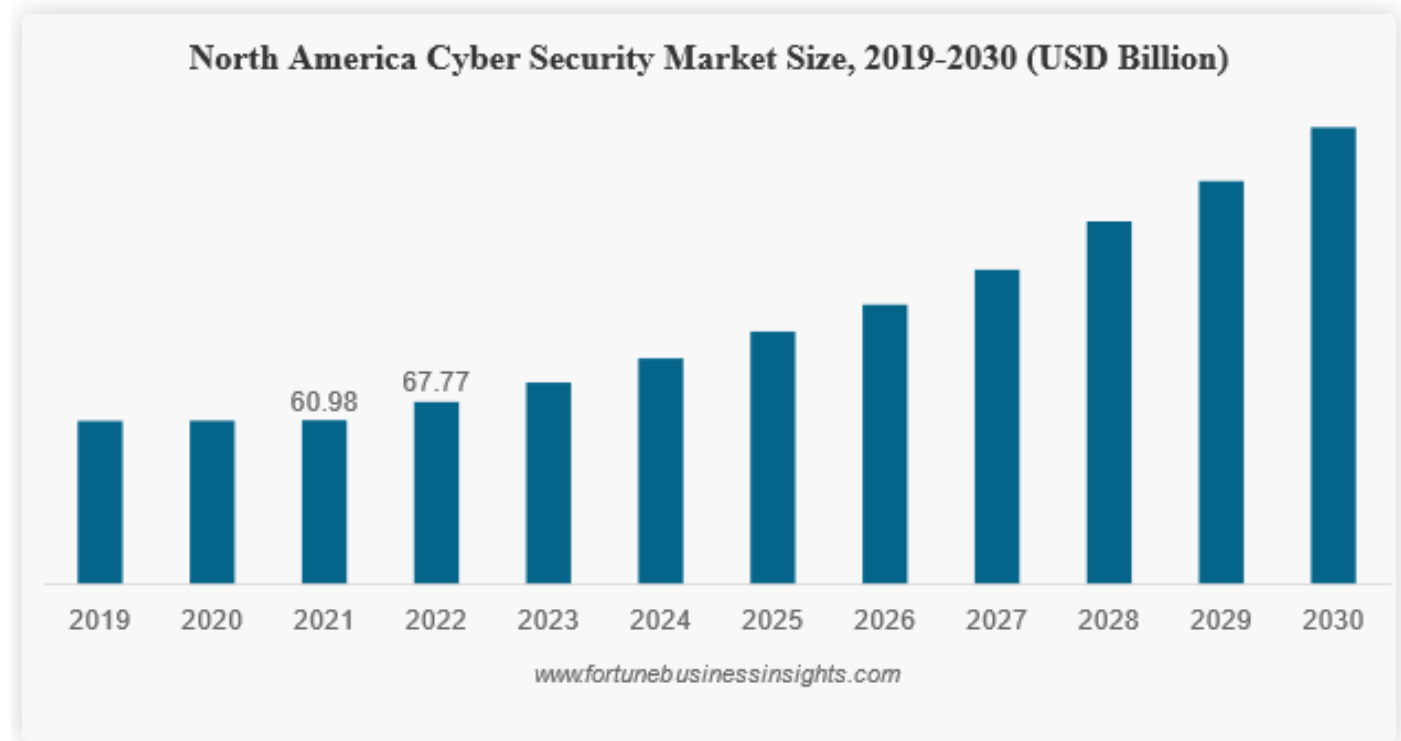


Middle East focus



Cybersecurity market size USA, 2019-2030

The global cyber security market size is projected to grow from \$172.32 billion in 2023 to \$424.97 billion in 2030



How much does a Cyber Security make?

Experience

All years of Experience

Industry

All industries

\$85,494 / yr

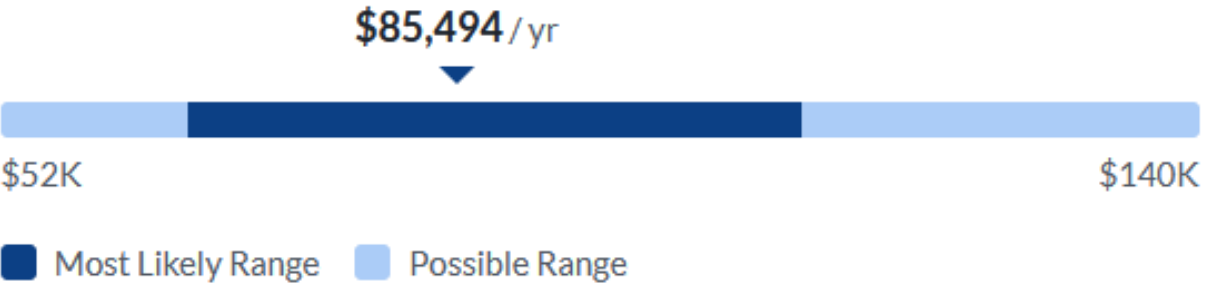
Total Pay

\$78,858 / yr


Base Pay

\$6,636 / yr

Additional Pay



LinkedIn (29.04.2024:17:00h)



Jobs ▾


Date posted ▾

Experience level ▾

Company ▾

cyber security in EMEA
47,332 results

Set alert ☐



Jobs ▾

Date posted ▾

Experience level ▾

Company ▾

Information Security Manager in EMEA
1,955 results

Set alert ☐

Cybersecurity job categories

Job Categories



Defensive
Security



Offensive
Security



Cloud
Security



Digital
Forensics



Leadership

Example

RED TEAM

OFFENSIVE ATTACK TEAM



Tasks include:

- Ethical hacking
- Penetration testing
- Black box testing
- Social engineering
- Web app scanning
- Vulnerability exploitation

PURPLE TEAM

DATA COLLECTION & IMPLEMENTATION TEAM



Tasks include:

- Improvement facilitation
- Data analytics
- Gap analysis
- Red vs Blue skill testing
- System improvements
- Collaborative security

BLUE TEAM

DEFENSIVE PROTECT TEAM



Tasks include:

- Infrastructure security
- Damage control
- Incident response (IR)
- Operational security
- Threat hunting
- Digital forensics



Cooler careers in Cybersecurity

10 COOLEST JOBS IN CYBERSECURITY

WHY THEY MAKE A
DIFFERENCE AND HOW
TO QUALIFY FOR THEM

Initial Jobs With Lots of Advancement Opportunities

1 DIGITAL FORENSIC ANALYST; INVESTIGATOR

"The thrill of the hunt! It's CSI for cyber geeks! You never encounter the same crime twice."

You are the detective in the world of cybersecurity - searching computers and networks for evidence in the wake of an incident.

2 PENETRATION TESTER FOR SYSTEMS AND NETWORKS

"Be a hacker, but do it legally and get paid a lot of money!"

You look for security vulnerabilities in target systems and networks to help enterprises improve their security.

3 APPLICATION PEN TESTER

"We desperately need more of this, application security has been such a black hole for so long."

You're a programming/security wizard - testing applications before deployment so they don't present opportunities for intruders.

4 SECURITY OPERATIONS CENTER (SOC) ANALYST

"The fire ranger. Better catch the initial blaze, or there goes the forest."

With an eye for detail and anomalies, you see things most others miss. You implement active prevention, active detection, active monitoring, active response.

5 CYBER DEFENDER; SECURITY ENGINEER (ENTERPRISE AND ICS)

"A leg up on your IT and engineering buddies; talk shop with them but you are saving the world from the bad guys, too."

You implement and tune firewalls, IPS/IDS, patching, admin rights, monitoring, application white listing, more.

More Advanced Jobs - Open After A Few Years of Great Performance and Specialized Training

6 HUNTER; INCIDENT RESPONDER

"The secret agent of geekdom. You walk in and say 'OK I'll take it from here.'"

While everyone else is running around shouting, "The system's dead!", you have the sense and skills to rationally figure out why.

7 SECURITY ARCHITECT

"You get to design the solution, and not just for the perimeter."

You are creative and on top of the game both technically and in business; You design and build defensible systems and are part of an adept team.

8 SECURE SOFTWARE DEVELOPMENT MANAGER

"Coolest software developers"

You protect the development team from making errors that will allow hackers to penetrate your organization and steal data. You are a programmer, but a programmer with special powers.

9 MALWARE ANALYST / REVERSE ENGINEER

"The technical elite! Only go here if you have been called. You know who you are."

You look deep inside malicious software to understand the nature of the threat - how it got in, what flaw it exploited, and what it is trying to do or has done.

10 TECHNICAL DIRECTOR / CISO

"Making decisions; making things happen. That's coolness."

You are at the top of the tech ladder. A strategic thinker, you're hands on the design and deployment of solutions. You hold the keys to tech infrastructure.

CYBER FAST TRACK

1



"I loved CyberStart challenges - the coolest game I ever played."

"Taught me a lot; proved cybersecurity wasn't too hard to learn."

"The most fun I have had learning."

DISCOVER IF YOU HAVE THE APTITUDE CYBERSTART: THE GAME

- No need for cyber or IT experience
- More than **250 fun challenges** protecting "real-world" bases
- Available **completely online** Everything you need is in the online Field Manual and hints.
- 19 U.S. Governors launched statewide programs for their students.

LEARN MORE AT [CYBERSTART.US](https://cyberstart.us)

2

CATEGORY/TO PIC	MODULES
Computer Hardware /Data	6
Linux and Windows	7
Networking	6
Programming	6
Common Attacks & Security	10
Others (Kali, Google, etc)	11

"We now hire cybersecurity grads only if they have 'hands-on mastery of these foundations' (CISO, multi \$billion Silicon Valley tech leader)"

MASTER THE FOUNDATIONS CYBERSTART: ESSENTIALS

- Core technologies: How they work and are attacked
- Online, hands-on immersion training, in **46 modules**
- Progress at your own pace. Quizzes and tests on each module
- **National exam** to reach silver or gold levels

3

EMPLOYER INTERVIEWS BEFORE ACCEPTANCE

GET SKILLS EMPLOYERS NEED AND A COOL JOB!

- Veterans' Academies, Women's Academies, and Open Academies
- Three SANS immersion courses and three high value GIAC certifications
- **%90 job placement** in 6 months
- Also available as Certificate in Applied Cyber Security (ACS) at SANS.edu and other accredited colleges and universities

LEARN MORE AT [USCYBERACADEMY.SANS.ORG](https://uscyberacademy.sans.org)

"Completing the SANS VetSuccess Academy not only influenced my career plans, it defined them - opening doors that were inaccessible to me otherwise. In fact, being selected into the VetSuccess program was a 'hitting the jackpot' moment for me."

Ed Russell, USAF (ret) NTT Security



Application Penetration Tester

Application penetration testers probe the security integrity of a company's applications and defenses by evaluating the attack.

Why is this role important?

Web applications are critical for conducting business operations, both internally and externally. These applications often use open-source plugins which can put these apps at risk of a security breach.



Programming background (web), TryHackMe, Ec-Council

Security operation center (SOC) Analyst

The person who may be a primary security contact for a small organization and must deal with engineering and architecture, incident triage and response, security tool administration, and more.

Why is this role important?

This job role is highly important as it often shows up in small to mid-size organizations that do not have budget for a full-fledged security team with dedicated roles for each function.



System/network/cloud services and administration skills

Incident Responder

This dynamic and fast-paced role involves identifying, mitigating, and eradicating attackers while their operations are still unfolding.

Why is this role important?

While preventing breaches is always the ultimate goal, one unwavering information security reality is that we must assume a sufficiently dedicated attacker will eventually be successful.

Cloud administration, Log analysis, organizational and soft skills

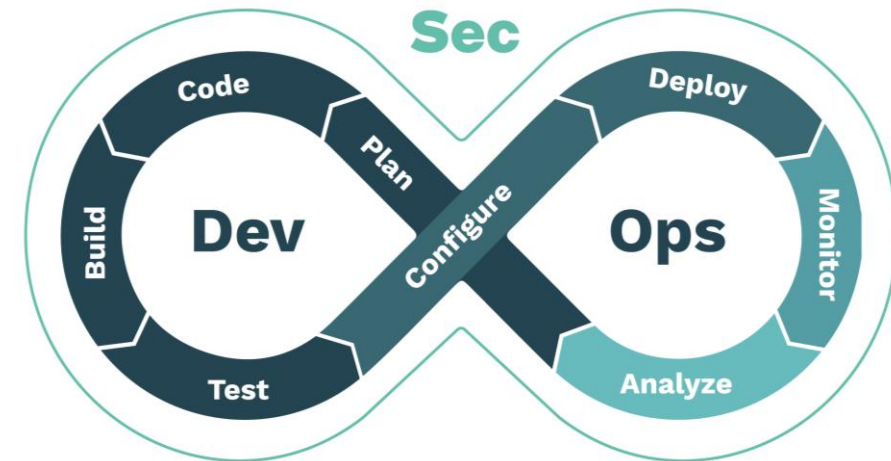


DevSecOps Engineer

Develop automated security capabilities leveraging best-of-breed tools and processes to inject security into the DevOps pipeline.

Why is this role important?

A natural and necessary response to the bottleneck effect of older security models on the modern continuous delivery pipeline.



Development, cloud services, app security

Digital Forensics Analyst

The practice of being a digital forensic examiner requires several skill sets, including evidence collection, computer, smartphone, cloud, and network forensics, and an investigative mindset.

Why is this role important?

These experts analyze compromised systems or digital media involved in an investigation that can be used to determine what really happened.

Skills from all IT areas with narrow specialization



Chief Information Security Officer - CISO

Works on strategy, financial framework and information security management at the company level. In charge of communication with the board of directors, analysis and mitigation of cyber risks.

Why is this role important?

The trend is for CISOs to have a strong balance of business acumen and technology knowledge in order to be up to speed on information security issues.

Information security, risk analysis, management, governance, leadership and strong technical background

Sleeping Positions



Academic vs. Industry

Academia

- Get Credit for Research
- More free time
- Generate new generations

Industry

- Rarely Get Credit for Work
- 9 to 5
- No time for mentoring



