Cyber Security Career In Blue Team

CyberFest 2022

Digit Oktavianto
@digitoktav
https://threathunting.id

Who Am I

- Infosec Consulting Manager at Mitra Integrasi Informatika
- Co-Founder BlueTeam.ID (https://blueteam.id)
- Born to be DFIR Team
- Community Lead @ Cyber Defense Community Indonesia (https://cdef.id)
- Member of Indonesia Honeynet Project
- Opreker and Researcher

Agenda

- Introduction to Career in Cyber Security
- Cyber Security Certification
- Cyber Security Career Path Step by Step

Introduction to Career in Cyber Security Industry

Intermezzo

"Cybersecurity is all about people, not just the processes and technology."

INTRODUCTION

Important Question for All of You :

Do you want career or just a job?

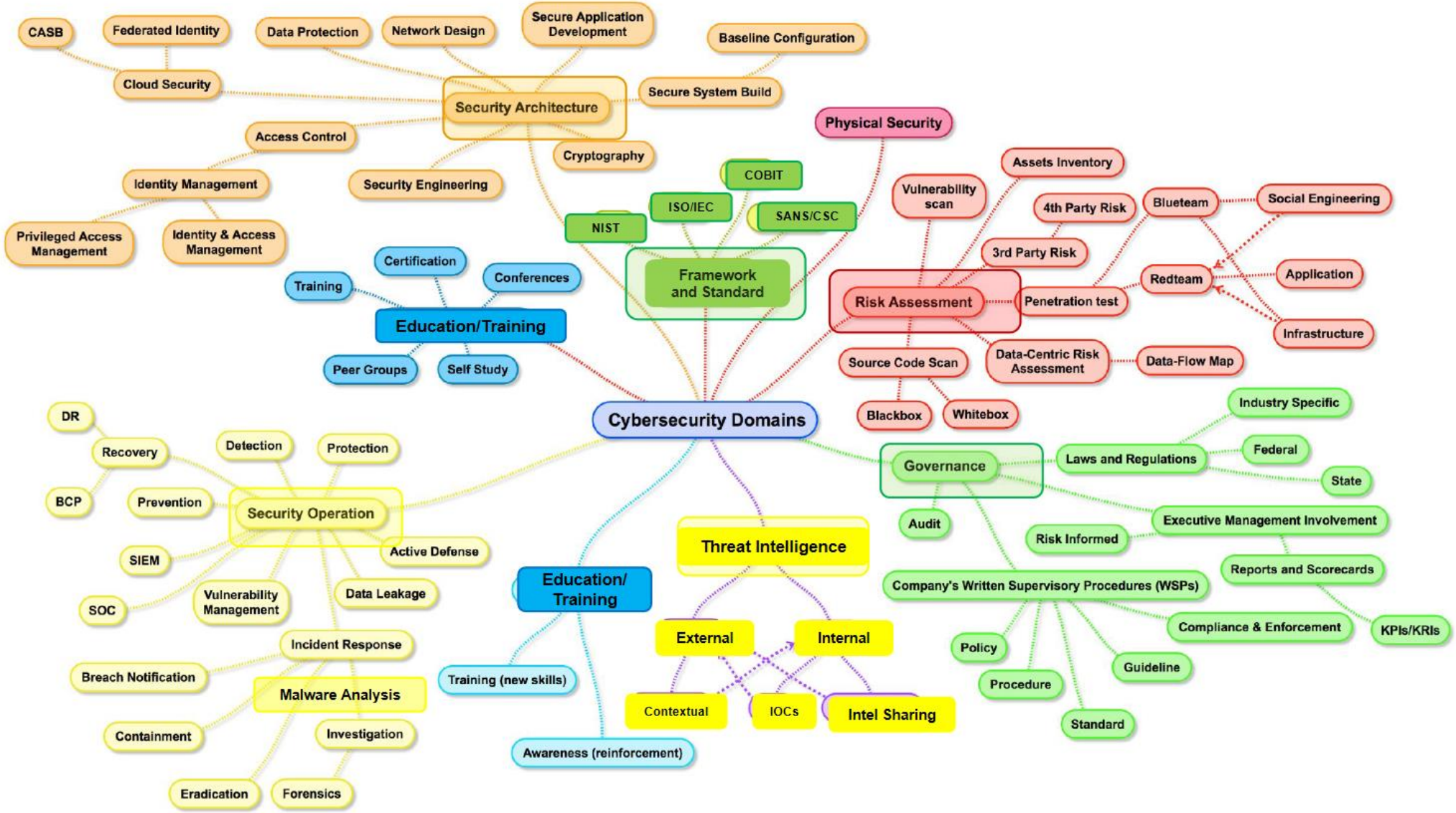
FAQ About Career in Cyber Security :

What does a cyber security career look alike?

Is it really different from normal IT Career?

What is short / long term in cyber security career?

Cyber Security Domain



Cyber Security Professional

WHAT DO CYBER SECURITY PROFESSIONALS DO?

The great part about cyber security is that it encompasses many different fields. Yes, there are the extremely technical roles. But there are also many different fields that contribute to a business's security posture (how good their cyber defences are).

As today's companies do more of their business online, the need for cyber security professionals continues to grow.

Job roles can be separated into four basic categories. Let your interests guide you when choosing a career path.

Cyber security professionals work in diverse fields and perform important roles, such as:

- Defending our nation
- Securing our telecommunications infrastructure
- Safeguarding our money
- Protecting our electrical distribution systems
- Protecting our identities
- Ensuring our medical information remains private
- Stopping ransomware attacks
- And many more

Cyber Security Roles (1)

Govern and Support

Manage and provide direction and support to ensure an organization conducts effective cyber security work. Roles include cyber legal advisor, policy analyst, privacy officer, and risk analyst

Protect, Detect, and Respond

Detect, prevent, respond to, and recover from cyber incidents and threats. Roles include cyber threat assessor, data scientist/modeler, big data analyst, cyber security analyst, information security analyst, DFIR (digital Forensic and Incident Responder), vulnerability assessment analyst, and penetration tester.

Cyber Security Roles (2)

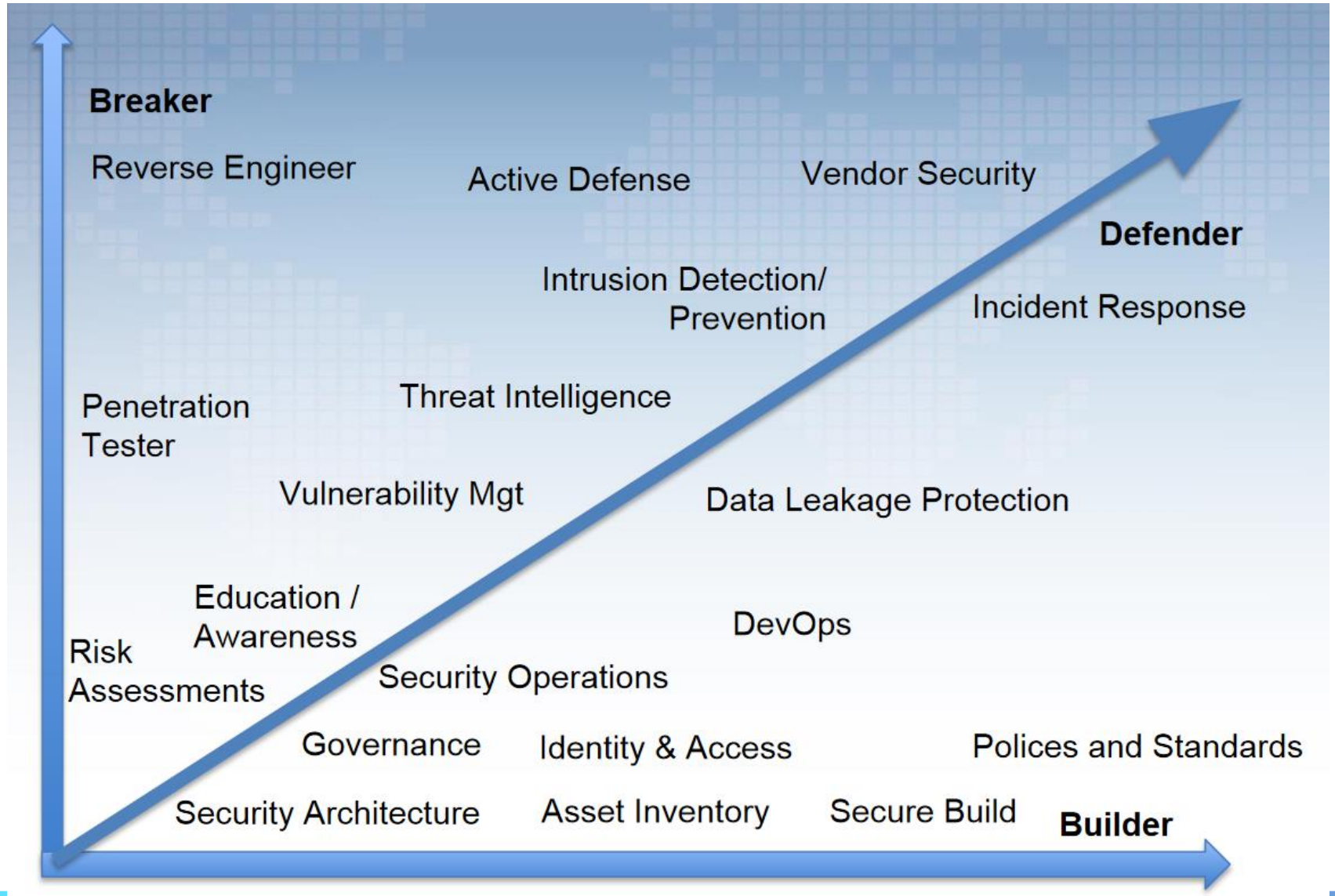
Design and Develop

Develop, secure, test, and integrate hardware, software, and systems throughout a product's life cycle. Roles include security architect, security engineer, application developer, and secure software developer.

Operate and Maintain

Administer, maintain, and support to ensure effective and efficient performance and cyber security. Roles include network security operator, security operation center analyst, cryptanalyst, and technical support specialist

Cyber Security Roles



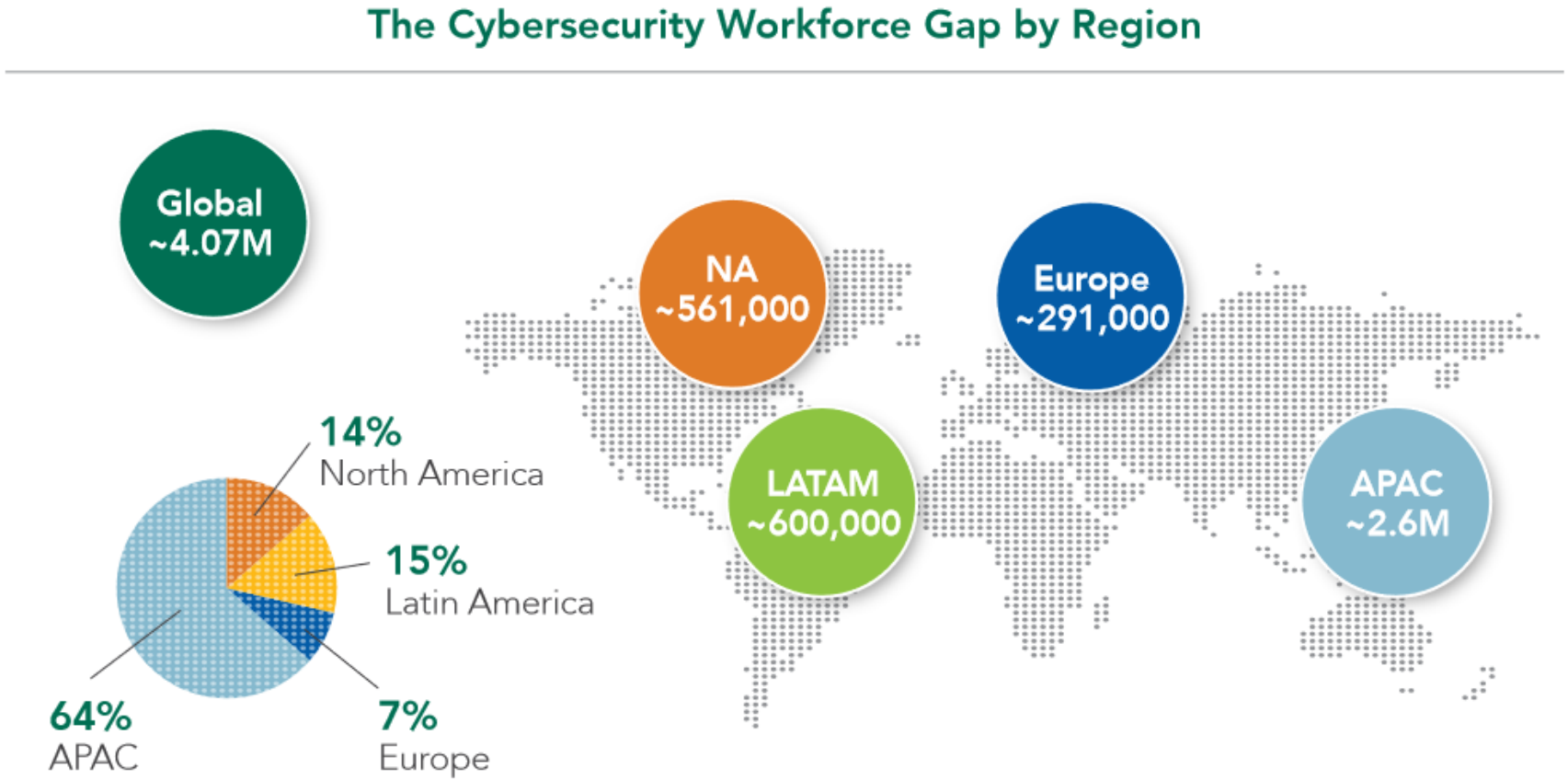
Cyber Security Roles

Average Number of Employees in Each Role (Across All Company Sizes)

Cybersecurity team roles	Total	NA	LATAM	EUR	APAC
Security Operations	22	23	19	22	22
Security Administration	15	16	15	15	15
Risk Management	13	13	13	13	13
Compliance	12	13	10	12	11
Operational Technology Security	11	11	14	11	12
Secure Software Development	10	9	12	9	11
Penetration Testing	8	8	9	9	9
Forensics	8	8	8	9	8

https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=D087F6468B4991E0BEFFC017BC1ADF59CD5A2EF7

Cyber Security Workforce Gap



https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=D087F6468B4991E0BEFFC017BC1ADF59CD5A2EF7

Peta Okupasi Cyber Security

PETA OKUPASI NASIONAL DALAM KERANGKA KUALIFIKASI NASIONAL INDONESIA PADA AREA FUNGSI KEAMANAN SIBER

KKNI		STRATA JABATAN	
LEVEL	KATEGORI	PEMERINTAH	INDUSTRI
9	AHLI	AHLI UTAMA	DIREKTUR UTAMA, PRESIDEN DIREKTUR, CXO, MANAGING DIRECTOR
8	AHLI	AHLI SENIOR	DIREKTUR; VICE PRESIDENT; GENERAL MANAGER; SCIENTIST
7	AHLI	AHLI PERDANA	MANAGER; EXPERT
6	TEKNISI/ANALIS	TEKNISI/ ANALIS MADYA	ASISTEN MANAGER; DEPUTY MANAGER; ADVISOR
5	TEKNISI/ANALIS	TEKNISI/ ANALIS MUDA	SUPERVISOR; PENYELIA

BEFORE				DURING		AFTER	
100904,07	CHIEF OF INFORMATION SECURITY OFFICER (CISO)						
100805,04	CYBER RISK SPECIALIST					100808,01	CYBER INCIDENT INVESTIGATION MANAGER
100806,04	SECURITY ARCHITECT					100809,01	CYBER FORENSIC SPECIALIST
100807,04	CRYPTOGRAPHIC SPECIALIST						
100723,04	CRYPTOGRAPHIC ENGINEER	100704/ 100704.07	MANAJER CYBERSECURITY/CYBERSECURITY MANAGER				
100724,04	ICT SECURITY PRODUCT LEAD EVALUATOR	100701/ 100701.04	MANAJER KEAMANAN JARINGAN/ NETWORK SECURITY MANAGER			100728,07	DIGITAL FORENSIC ANALYST
		100720,04	CYBERSECURITY AWARENESS LEAD OFFICER				
		100721,07	INCIDENT RESPONSE TEAM MANAGER				
		100722,04	AUDITOR KEAMANAN INFORMASI				
		100725,06	THREAT HUNTER				
		100726,04	PENETRATION TESTER				
		100727,07	CYBERSECURITY GOVERNANCE OFFICER				
100608,04	ICT SECURITY PRODUCT EVALUATOR	100605,04	CYBERSECURITY AWARENESS OFFICER	100601/ 100601.03	CYBERSECURTY ANALYST/ CYBERSECURITY INCIDENT ANALYST		
100610,04	CRYPTOGRAPHIC ANALYST	100606,04	VULNERABILITY ASSESSMENT ANALYST			100612	DIGITAL EVIDENCE FIRST RESPONDER
100611,04	CRYPTOGRAPHIC MODULE ANALYST	100607,04	NETWORK SECURITY ADMINISTRATOR				
		100609,04	CYBERSECURITY ADMINISTRATOR				
		100508,06	CYBERSECURITY OPERATOR				
		100501/ 100501.04	JUNIOR CYBER SECURITY				
		100509,04	TEKNISI PERANGKAT KERAS KRIPTOGRAFI				
		100510,04	CRYPTOGRAPHIC ADMINISTRATOR				

UNIT KOMPETENSI TELAH DILENGKAPI
SEBAGIAN UNIT KOMPETENSI TELAH DILENGKAPI
UNIT KOMPETENSI BELUM DILENGKAPI

LAUNCHING PETA OKUPASI NASIONAL KEAMANAN SIBER

Peta Okupasi Cyber Security

CAREER PATH

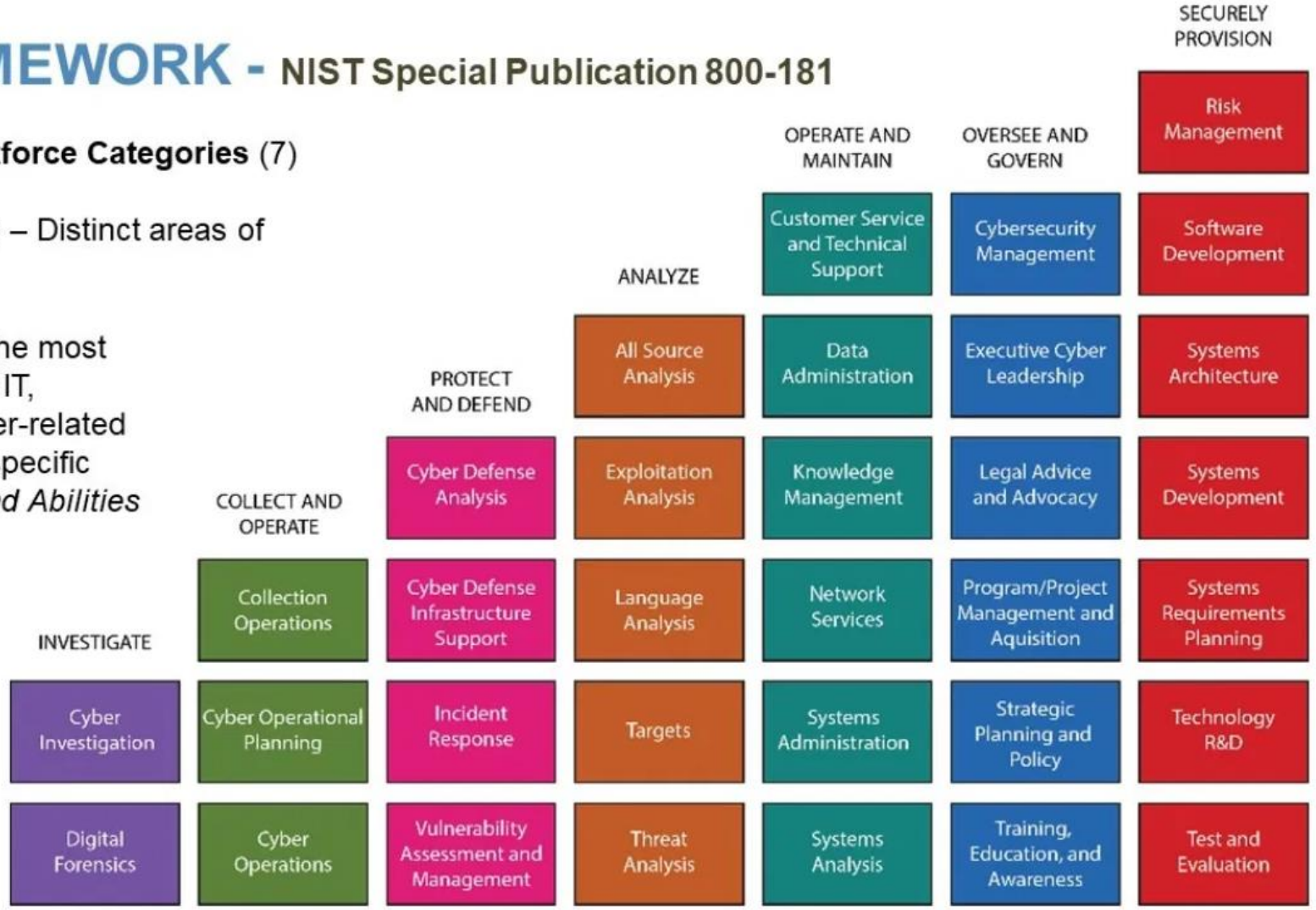
NICE Framework

NICE FRAMEWORK - NIST Special Publication 800-181

Cybersecurity Workforce Categories (7)

Specialty Areas (33) – Distinct areas of cybersecurity work

Work Roles (52) – The most detailed groupings of IT, cybersecurity, or cyber-related work, which include specific *Knowledge, Skills, and Abilities*



Cyber Security Training and Certification

Do We Need to Take Certification Program?

- Yes, Of Course. But Why?
- What Kind of Certification Should I Take?
  - **Vendor Based :**

  CISCO, F5, Checkpoint, Palo Alto, Microsoft, Juniper, etc
  - **Non-Vendor Based :**

  Offensive Security : OSCP, OSWE, OSCE, OSEP, OSEE
  EC-Council : CEH, ECSA, CHFI, ECIH, CHFI
  GIAC : GCIH, GPEN, GCFA, GSEC
  ISC2 : CISSP, SSCP
  ISACA : CISA, CISM, CRISC

Why Do You Need Certifications?

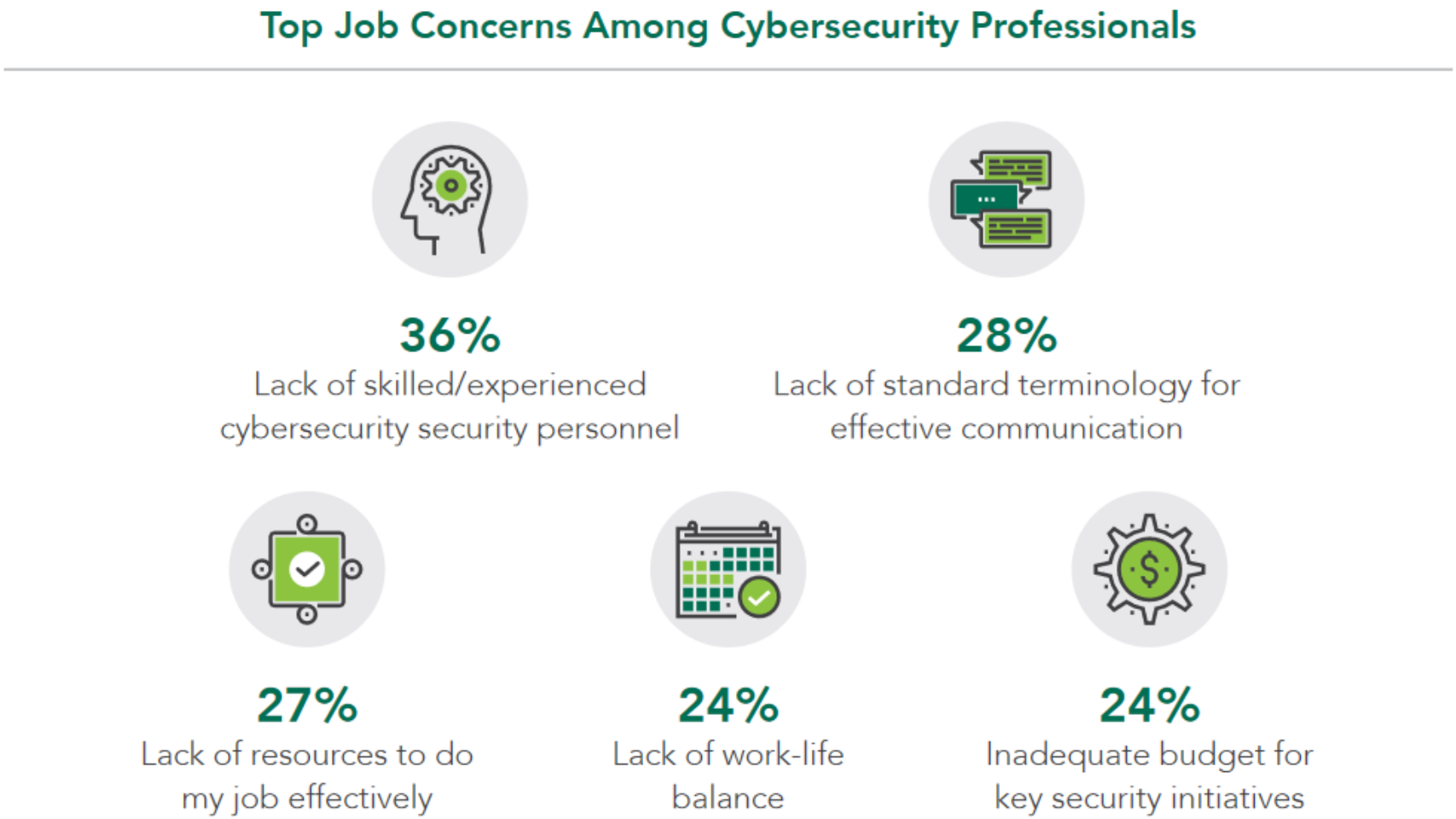
- The global cyber security market is forecast to expand at a compound rate of 10% a year through 2027, and that means new jobs — and fierce competition for those high-paying jobs as more and more people try to get into cyber security
- In the cyber security industry, certifications show the cyber security skill you have and can be absolutely critical to your cyber security career trajectory.
- Keep in mind that some certifications are for the beginning of your career while others are more important later on. Often, there are multiple certifications for a specific path. Depending on your interest, there's a different certification that fits your path. So let's figure out what certifications you need for your cyber security path.

Job Search and Certification Statistics

Certification	LinkedIn	Indeed	Simply Hired	Total
CISSP	30,857	11,630	7,756	50,243
CISA	7,262	5,432	3,485	16,179
CISM	5,173	3,779	2,488	11,440
CEH	4,179	2,717	1,858	8,754
Security+	3,618	2,933	2,202	8,753
GSEC	3,039	1,873	1,521	6,433
SSCP	2,908	1,850	1,490	6,248
CCSK	5,466	264	151	5,881
CCNA Security	2,879	1,566	1,034	5,479
CASP	2,342	1,556	1,208	5,106

Number of US job search results for each certification when searched on December 22, 2020

Job Concern Among Cyber Security Professional



https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=D087F6468B4991E0BEFFC017BC1ADF59CD5A2EF7

What Specific Area of Certification ???

Fundamental Cyber Security Certification

CEH, GSEC, CompTIA Security+, ISACA CSX Fundamental, ISC2 SSCP

Higher Level Cyber Security Certification

CISSP, CCISO, CISM, GSE,

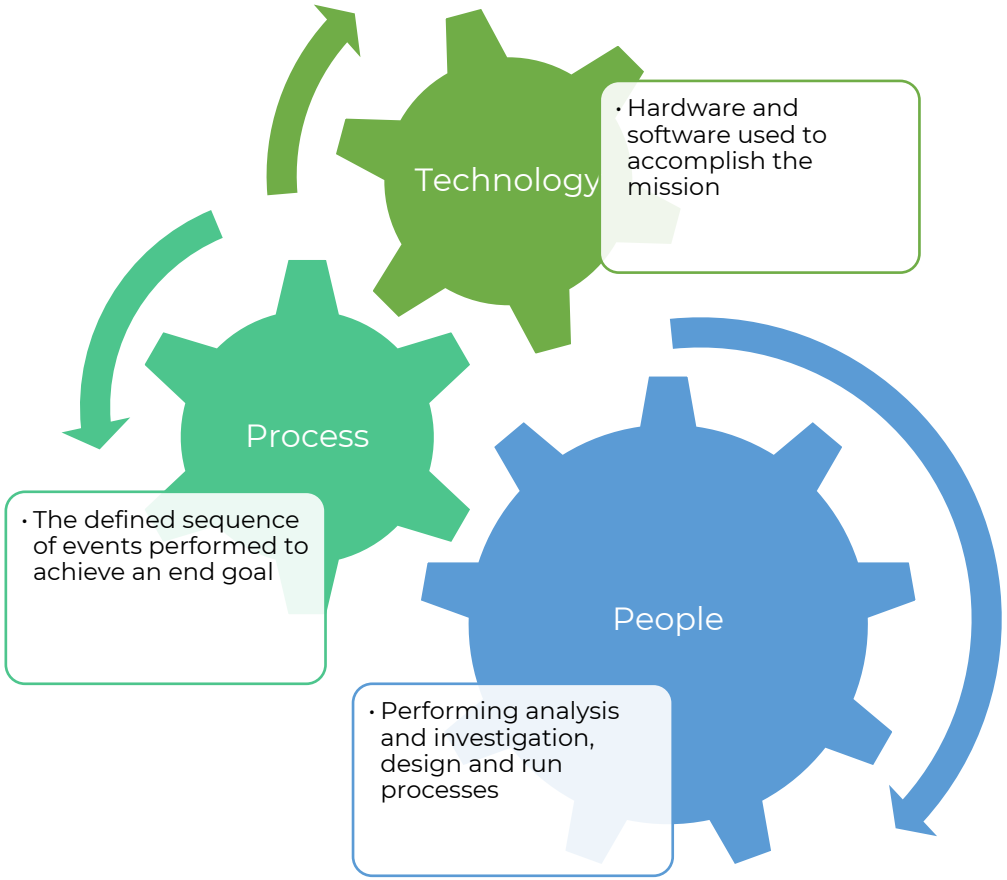
Cyber Security Career in Blue Team

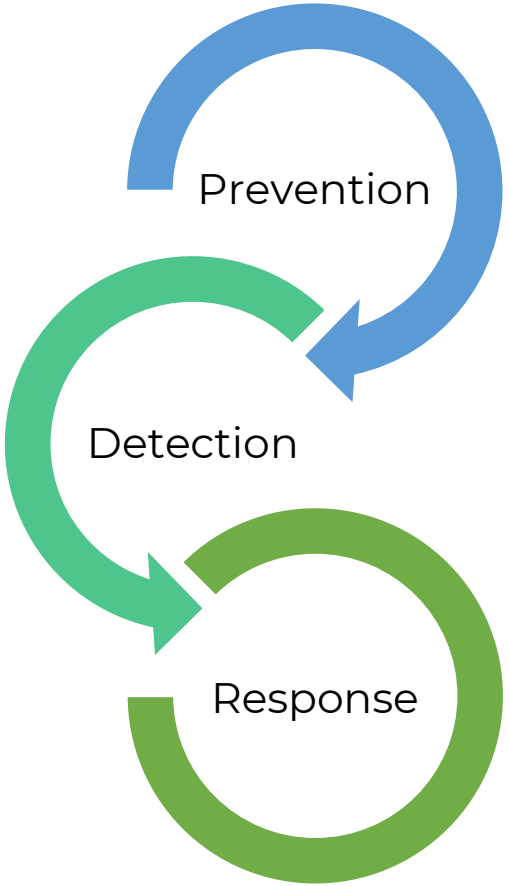

PROTECT
DETECT
RESPOND

NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Awareness Control	Anomalies and Event	Response Planning	Recovery Planning
Business Environment	Awareness and training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Process	Analysis	Communications
Risk Assessment	Info Protection and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	

Defensive Capabilities in Organization





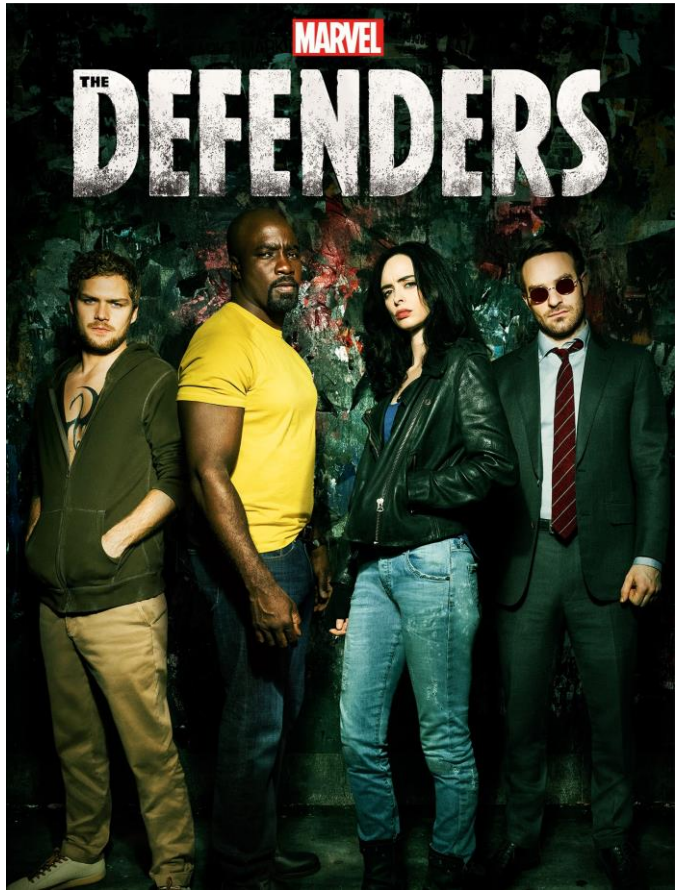
Ensure security has been implemented

Ensure the team capable to detect known threat.

Ensure the team capable to response security incident

Organizations Need Some Heroes

- The Defenders
- A **Blue Team** is a group of individuals who perform an analysis of information systems to:
  - Identify and give some recommendation for critical assets & systems
  - Ensure security has been implemented
  - Identify security flaws and inform into system owners
  - Verify the effectiveness of each security measure
  - Make certain all security measures will continue to be effective after implementation.
- Example : **Security Analyst, Security Engineer, Incident Responder, Threat Hunter, Digital Forensic Investigator, Malware Analyst**



Career Focus Area for Blue Team in Cyber Security

- SOC Analyst
- Threat Hunter
- Detection Engineer
- Incident Response / Incident Handler
- Digital Forensic
- Malware Analysis
- Reverse Engineering
- Security Engineer
- Security Architect

What Specific Area of Certification ???

Defensive Security Certification Example :

- GIAC : GCIH, GMON, GCFA, GCFE, GDSA
- EC Council : ECIH, CHFI, CSA, CTIA, CND
- Comptia : CySA+
- ElearnSecurity : eCTHP, eCIR, eDFP, eMAP, etc

But, I don’t have Experience.....

So, you’ve decided to make the jump and enroll in a cyber security program. Now what, you ask? “Will I be able to find a job in the field after school if I have no work experience in cyber security?

The odds are in your favour. Consider this: graduates of cyber security programs tend to be quickly recruited by public and private sector organizations.

In fact, **the shortage of cyber security professionals** is so pronounced that organizations are retraining employees in basic cyber security skills on the job! **As a skilled graduate of a cyber security program, you are sure to be an attractive candidate for many employers.**

FAQ

Most common questions from college student in their last year of uni : what should I do to improve the chance getting hired from the employer in cyber security roles?

- Understand the Basic of IT

  Understanding the fundamentals of IT, such as administering & configuring systems, networks, database management and coding will go a long way towards getting your first job.

- Networking

  Get a LinkedIn account and start connecting with people in the industry. Businesses post jobs there and recruiters use it as a tool to find candidates. Join local community in cyber security, attend the meetup, discuss with the community, getting involved in conference, event, CTF competition.

FAQ

- Focus on your Interests

  It is impossible to be an expert in all categories. Focus on an area (e.g. offensive security, cloud security, blue team, etc) and understand it well. Think ahead 5-10 years to your dream job, then look for an entry-level position that will give you the right skills.

- Gain Practical Experience

  Gain as much hands-on experience as possible. A co-op position or internship will help you get a sense of IT procedures and real-world business operations. Even if you’re not in a program that offers these types of positions, you can accomplish a lot with self-directed learning. Many universities or certification authorities offer free online resources. Take cyber security online learning platform such as TryHackMe, Hack The Box, RangeForce, CyberDefenders.org, LetsDefend.io, AttackIQ, etc.

How to Prepare Cyber Security Career Path

- **Education**
  - Learn and study the basic knowledge
  - Develop hard skill and soft skill from college
- **Networking**
  - Build relationship from Local Community.
  - Build your profile in Networking Site (LinkedIn, Twitter, Medium, etc)
- **Experience**
  - Practice. Practice. Practice.
  - Build your Own Lab in your Home
  - Involve in many Projects. (e.g open Source Projects)
  - Joining in a competition (e.g CTF Competition)
- **Seek for Mentorship**
  - Find the right mentor to guide you in cyber security industry
  - Find a partner to discuss all things related cyber security
- **Training and Certification**
  - Getting the right training from the industry
  - Getting acknowledgement from industry

Step by Step

1. Creating Your Goals
2. Know Your Skill
3. Skill Self-Assessment
4. Developing Your Career Plan
5. A Short Career Plan
6. Effective Career Investment

Creating Effective Plan

- **The Best Plan**
  – Ties long-term career strategy to short-term activities
  – Matches your skills, aptitudes and potential
  – Allows you to move forward daily.
  – Deals with more than just your career - your career should be a part of your overall life plan.
- **How do you do that?**
  – Go beyond Job Descriptions
  – The importance of Mentoring and having good models
- **Every Plan Has a Risk**
  – You can do anything you want, but you can't do everything that you want.

TOP NEWS | LATEST NEWS | PRESS RELEASE

Antaranews.com

About Us

ANTARANEWS.com

Friday, 11th June 2021

HOME CURRENT ISSUE WORLD BUSINESS & INVESTMENT EXPLORE INDONESIA ARTICLE PHOTO PRESS RELEASE BAHASA

Legislator calls for good cyber security to protect citizens' data

23rd May 2021

POPULAR

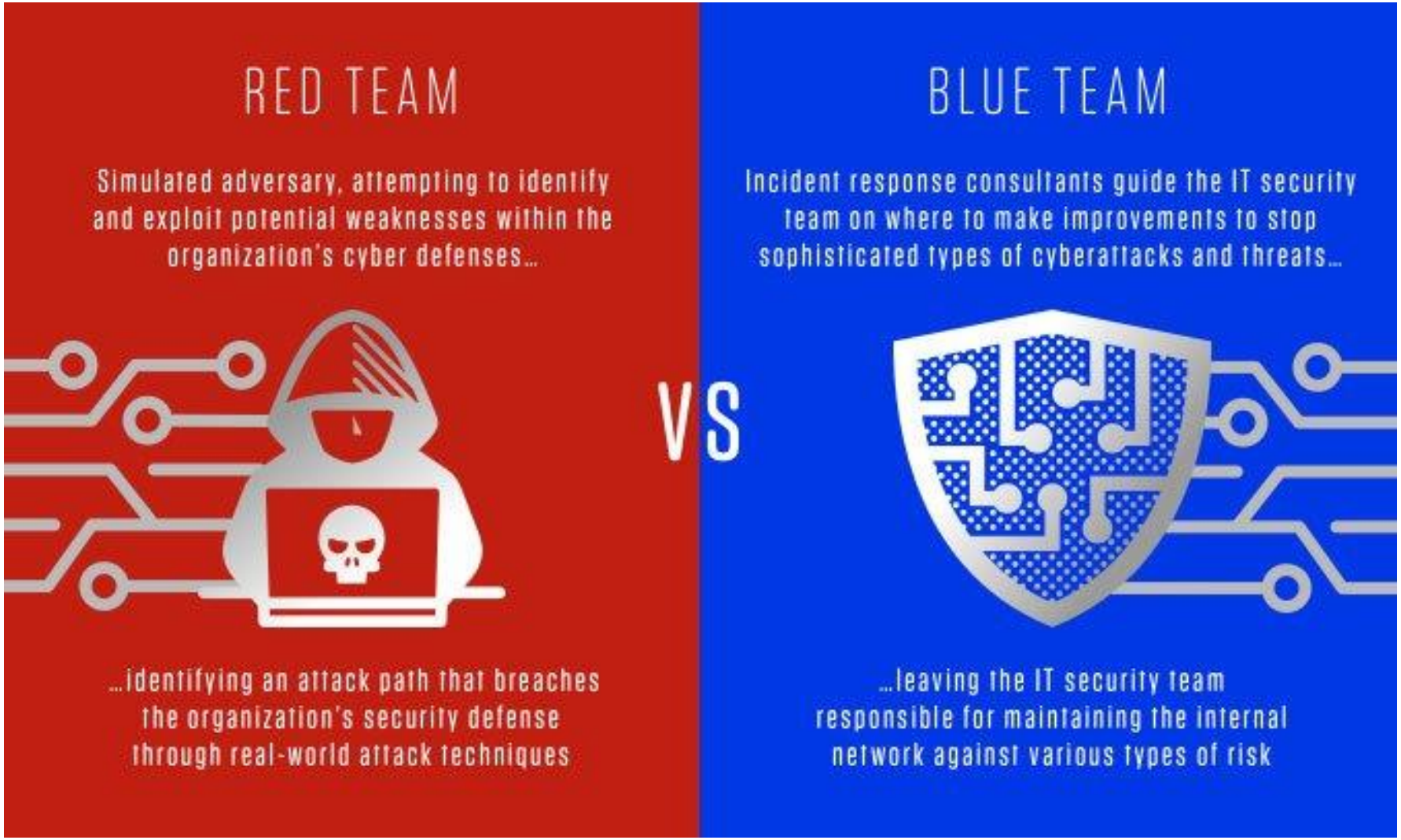
Govt plans 14-day quarantine for travelers from abroad

4th June 2021

Dilema Pekerja Keamanan Siber, Banyak Dicari tapi Syarat Berlebihan

Kompas.com - 04/12/2020, 20:09 WIB

Knowledge Gaps Between Blue Team and Red Team


RED TEAM
Simulated adversary, attempting to identify and exploit potential weaknesses within the organization's cyber defenses...
...identifying an attack path that breaches the organization's security defense through real-world attack techniques
VS
BLUE TEAM
Incident response consultants guide the IT security team on where to make improvements to stop sophisticated types of cyberattacks and threats...
...leaving the IT security team responsible for maintaining the internal network against various types of risk

Gaps Between Blue Team and Red Team

- The blue team are the good folks that often do not get enough praise, they are the real heroes in this story. The blue team are the front line defenders who work at all levels to protect a network from nefarious activity and help to secure businesses day in day out. Their primary role is to act as the varying lines of defense of companies' networks, similar to the offensive side of security blue teamers come in many flavours.
- Red Team (and also threat Actor) Leverage many Open source tools to perform the infiltration into the organization, but blue team knowledge is not expanding much since they already have a lot of daily task.
- Less research time in Blue team side
- Less training provided (and also the provider / training materials) for Blue Team

Refreshment

Dino A. Dai Zovi
@dinodaizovi

We overly celebrate offense in InfoSec, but we don't get more secure by finding and fixing bugs one-by-one. We get more secure by building systems that obliterate entire bug classes.

We need to shift focus to celebrating the defenders who build scalable and effective defenses.

11:20 PM · Dec 16, 2020 · Twitter Web App

176 Retweets **27** Quote Tweets **833** Likes

Dino A. Dai Zovi @dinodaizovi · Dec 16

Replying to @dinodaizovi

I did pen-testing when I was young because it was easy and I had no real experience. It took me almost twenty years of being in security to get any good at thinking about building defenses in a way that works, actually gets deployed, and gets deployed in enough places to matter.

3 9 111

THANK YOU
Q & A