Finding Your Place in Today's Cybersecurity Landscape

DJ Hovermale

Is a widely-recognized expert in military cyber exercises. While working for the National Security Agency, Johns Hopkins Applied Physics Laboratory, and Science Applications International Corporation he has been instrumental in the development of capstone-level cyber exercises for United States Cyber Command, the Army National Guard, and the United States Army Reserve.

Who is this guy?

- PhD in computational linguistics, Ohio State 2011

- National Security Agency, 2012-2014

- Johns Hopkins APL, 2014-2016

- SAIC, 2016- present

- University of Alabama in Huntsville, 2019-present

TestOut®
CYBERSECURITY
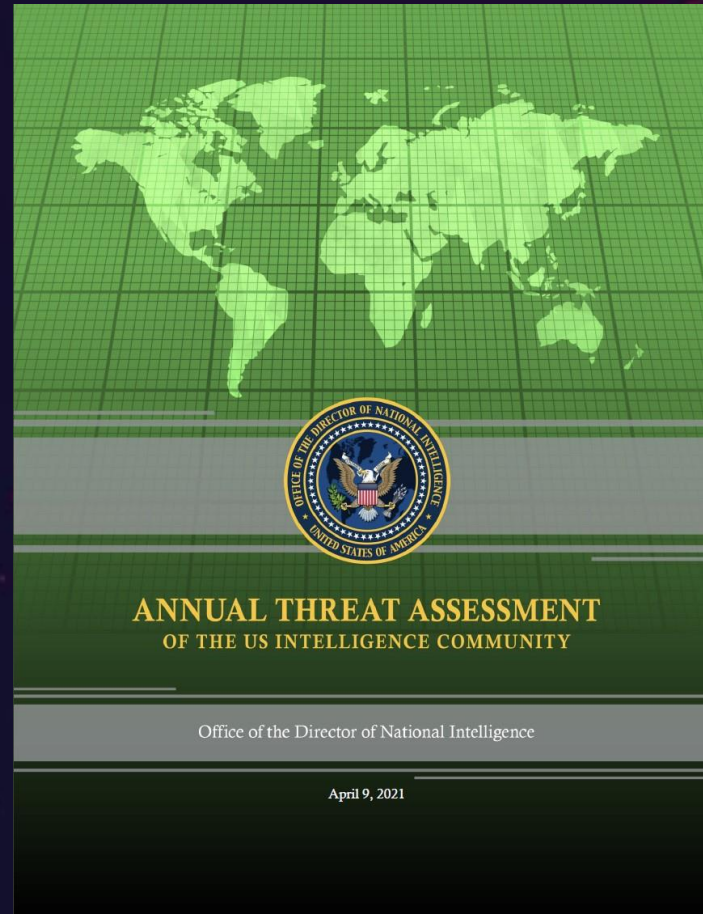AWARENESS MONTH

What is he going to talk about?

I.   Cyber Threat Landscape
   a.   Threats Against U.S. govt
   b.   Threats Against Industry
   c.   Questions (can type in chat during presentation)

II.   Cybersecurity Jobs
   a.   Job Shortage
   b.   Resume
   c.   Certifications
   d.   Self-Learning
   e.   Networking
   f.   Questions

TestOut®
CYBERSECURITY
AWARENESS MONTH

Cyber Threat Landscape

What are current cyber threats to govt. agencies?

https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf

TestOut®
CYBERSECURITY AWARENESS MONTH

What are current cyber threats to govt. agencies?

- We continue to assess that China can launch cyber attacks that, at a minimum, can cause localized, temporary disruptions to critical infrastructure within the United States.

- China's cyber-espionage operations have included compromising telecommunications firms, providers of managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack, or influence operations.

TestOut®
CYBERSECURITY
AWARENESS MONTH

What are current cyber threats to govt. agencies?

- Russia continues to target critical infrastructure, including underwater cables and industrial control systems, in the United States and in allied and partner countries, as compromising such infrastructure improves—and in some cases can demonstrate—its ability to damage infrastructure during a crisis.

- intent to target and potentially disrupt public and private organizations in the United States

- Russia almost certainly considers cyber attacks an acceptable option to deter adversaries, control escalation, and prosecute conflicts.

TestOut®
CYBERSECURITY
AWARENESS MONTH

What are current cyber threats to govt. agencies?

- Iran was responsible for multiple cyber attacks between April and July 2020 against Israeli water facilities that caused unspecified short-term effects, according to press reporting.

- Iran attempted to influence dynamics around the 2020 US presidential election by sending threatening messages to US voters, and Iranian cyber actors in December 2020 disseminated information about US election officials to try to undermine confidence in the US election.

TestOut®
CYBERSECURITY
AWARENESS MONTH

What are current cyber threats to govt. agencies?

- Pyongyang probably possesses the expertise to cause temporary, limited disruptions of some critical infrastructure networks and disrupt business networks in the United States, and it may be able to conduct operations that compromise software supply chains.

- North Korea has conducted cyber theft against financial institutions and cryptocurrency exchanges worldwide, potentially stealing hundreds of millions of dollars, probably to fund government priorities, such as its nuclear and missile programs.

TestOut®
CYBERSECURITY
AWARENESS MONTH

What are current cyber threats to industry?

Active Industry Threats in 2020

- 246 Groups

- 6 Advanced Persistent Threat Groups

- 4 Financial Threat Groups

- 236 Uncategorized Groups

THREAT GROUPS, 2020

2 Active FIN Groups From These Geolocations • Russia • Ukraine

4 Active FIN Groups

55 Active UNC Groups From These Geolocations • China • Iran • Nigeria • North Korea • Russia • Sweden • Switzerland • Slovenia • Uganda • Ukraine • Vietnam

236 Active UNC Groups

6 Active APT Groups From These Nation-States • China • Iran • Vietnam

11 FIN Groups (1 Graduated)

6 Active APT Groups

652 UNC Groups Identified in 2020 (75 Merged)

41 APT Groups

FIN

UNC

APT

1900+ Total Groups

2020 Active Geolocations

2020 Activity

Total Tracked Efforts

TestOut®
CYBERSECURITY AWARENESS MONTH

https://www.fireeye.com/current-threats/annual-threat-report.html

What are current cyber threats to industry?

Most Targeted Industries

- Business and Professional Services

- Retail and Hospitality

- Financial

- Healthcare

- High Technology

TestOut®
CYBERSECURITY
AWARENESS MONTH

What are current cyber threats to industry?

Ransomware

- $20 billion in global damage (2020)
    - Average cost $83k
    - Baltimore spent $18 million recovering from an attack that asked for $76k
- First death related to a cyberattack
- Free kits available online to would-be attackers
- Professional organizations for-hire
- 75% of victims had up-to-date software

What are current cyber threats to industry?

Supply Chain Attacks

- SolarWinds

- Kaseya VSA

- Xiaomi's Mi 10T 5G phone

- Lenovo

- Huawei

Expected to increase 400% in next 12 months

58% of attacks aimed to access data

62% of the attacks exploit the trust of customers in their supplier

66% OF ATTACKS FOCUS ON THE SUPPLIER'S CODE

62% OF ATTACKS RELY ON MALWARE

SUPPLY CHAIN ATTACKS ON THE RISE

ENISA Threat Landscape for Supply Chain Attacks

What are current cyber threats to industry?

Critical Infrastructure

- Mirai Botnet

- Colonial Pipeline

- Estonia

- Stuxnet

- Ukraine (Electrical Grid)

Image credit: CNN

TestOut

CYBERSECURITY
AWARENESS MONTH

Dangerous attack combinations

Cyber/Physical

- Georgia/South Ossetia

- Ukraine

Supply Chain/ Ransomware

- Kaseya VSA

- Accellion

What's Next?

Image credit: Atlantic Council

TestOut®
CYBERSECURITY
AWARENESS MONTH

Questions

Cyber Job Landscape

Where do you fit in?

You can make a difference!

Good Progress

- Global median dwell time reduced to 24 days in 2020 from more than one year in 2011

- Internal detection rates up to 61%

Room for Improvement

- Non-ransomware dwell time 45+ days

- 2/5 attacks not detected internally

TestOut®
CYBERSECURITY
AWARENESS MONTH
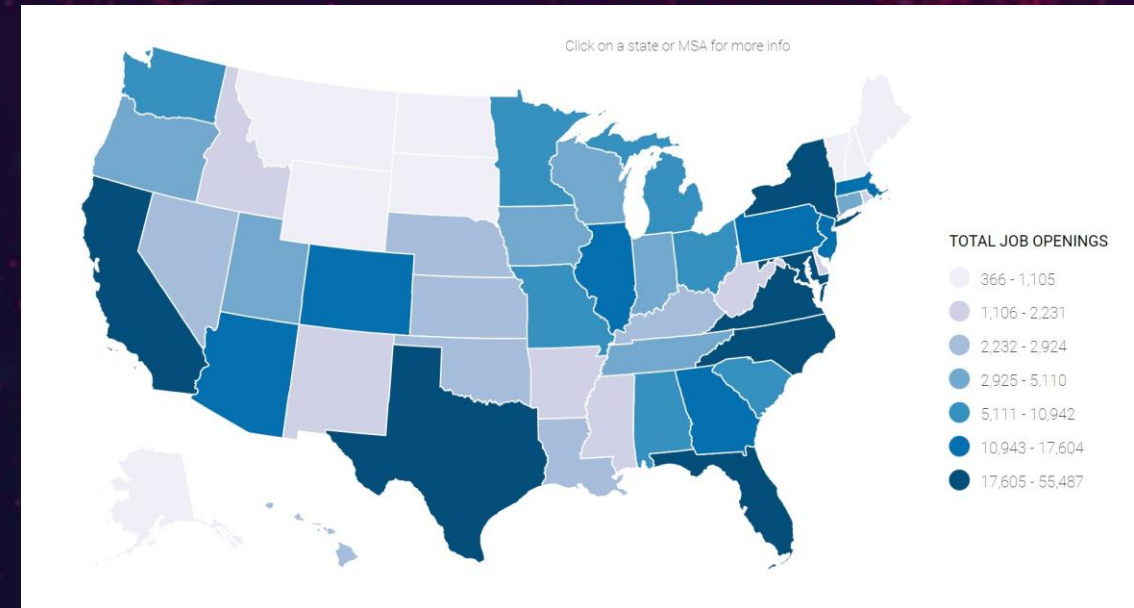
Cybersecurity Job Shortage

Government

- 1700 cyber vacancies at DHS alone

- 36,000 vacancies across federal, state, and local governments

- There are 16 times more federal IT workers older than 50 than there are younger than 30

Industry

- 465,000 total vacancies

This is a threat to our national security!
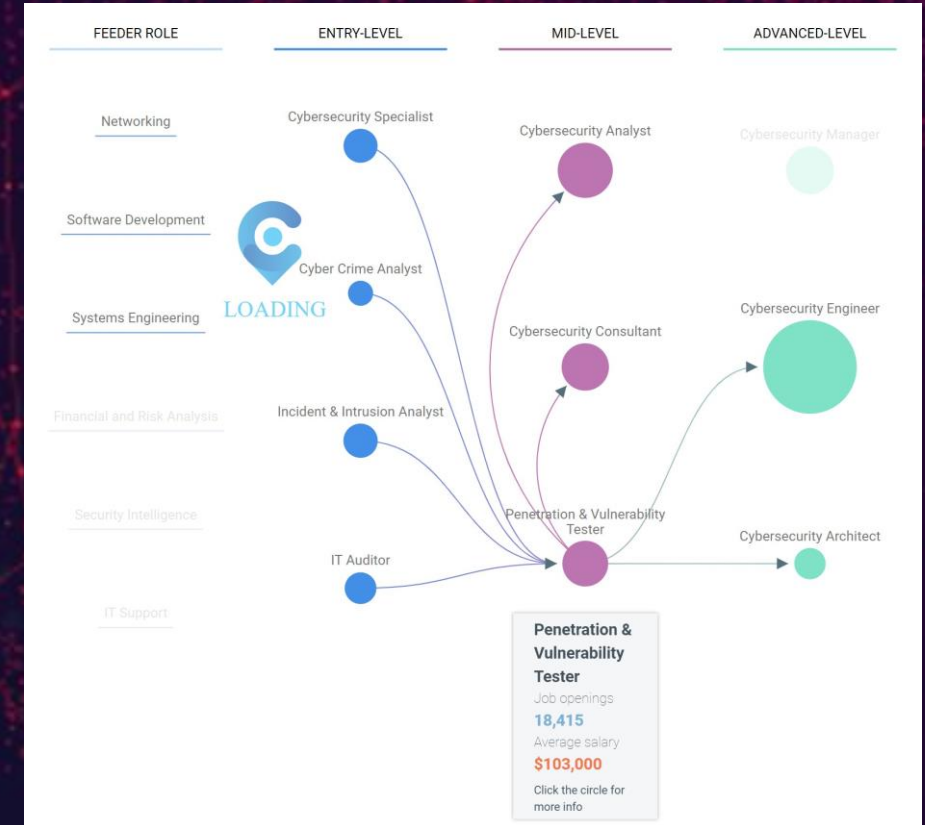

Click on a state or MSA for more info

TOTAL JOB OPENINGS

- 366 - 1,105
- 1,106 - 2,231
- 2,232 - 2,924
- 2,925 - 5,110
- 5,111 - 10,942
- 10,943 - 17,604
- 17,605 - 55,487

TestOut®
CYBERSECURITY
AWARENESS MONTH

Image credit: CyberSeek

Cybersecurity Job Shortage

Top In-Demand Cybersecurity Job Titles

- Cybersecurity Analyst
- Cybersecurity Consultant
- Cybersecurity Manager
- Software Developer
- Systems Engineer
- Network Engineer
- Penetration & Vulnerability Tester
- Cybersecurity Specialist
- Incident & Intrusion Analyst

FEEDER ROLE	ENTRY-LEVEL	MID-LEVEL	ADVANCED-LEVEL
Networking	Cybersecurity Specialist	Cybersecurity Analyst	Cybersecurity Manager
Software Development	Cyber Crime Analyst	Cybersecurity Consultant	Cybersecurity Engineer
Systems Engineering	LOADING		
Financial and Risk Analysis	Incident & Intrusion Analyst		
Security Intelligence		Penetration & Vulnerability Tester	Cybersecurity Architect
	IT Auditor		
IT Support			

Penetration & Vulnerability Tester
Job openings
18,415
Average salary
$103,000
Click the circle for more info

TestOut®
CYBERSECURITY
AWARENESS MONTH

Image credit: CyberSeek

Make Your Resume Stand Out

- **Focus on Relevant Skills**
  - Certifications
  - Degrees
  - Outside activities
  - Don't forget soft skills
- **Get referred by Current Employee**
  - Associations
  - LinkedIn
  - Former classmates, alumni

TestOut®
CYBERSECURITY
AWARENESS MONTH

Image credit: CyberSeek

Where do I start?: Certifications
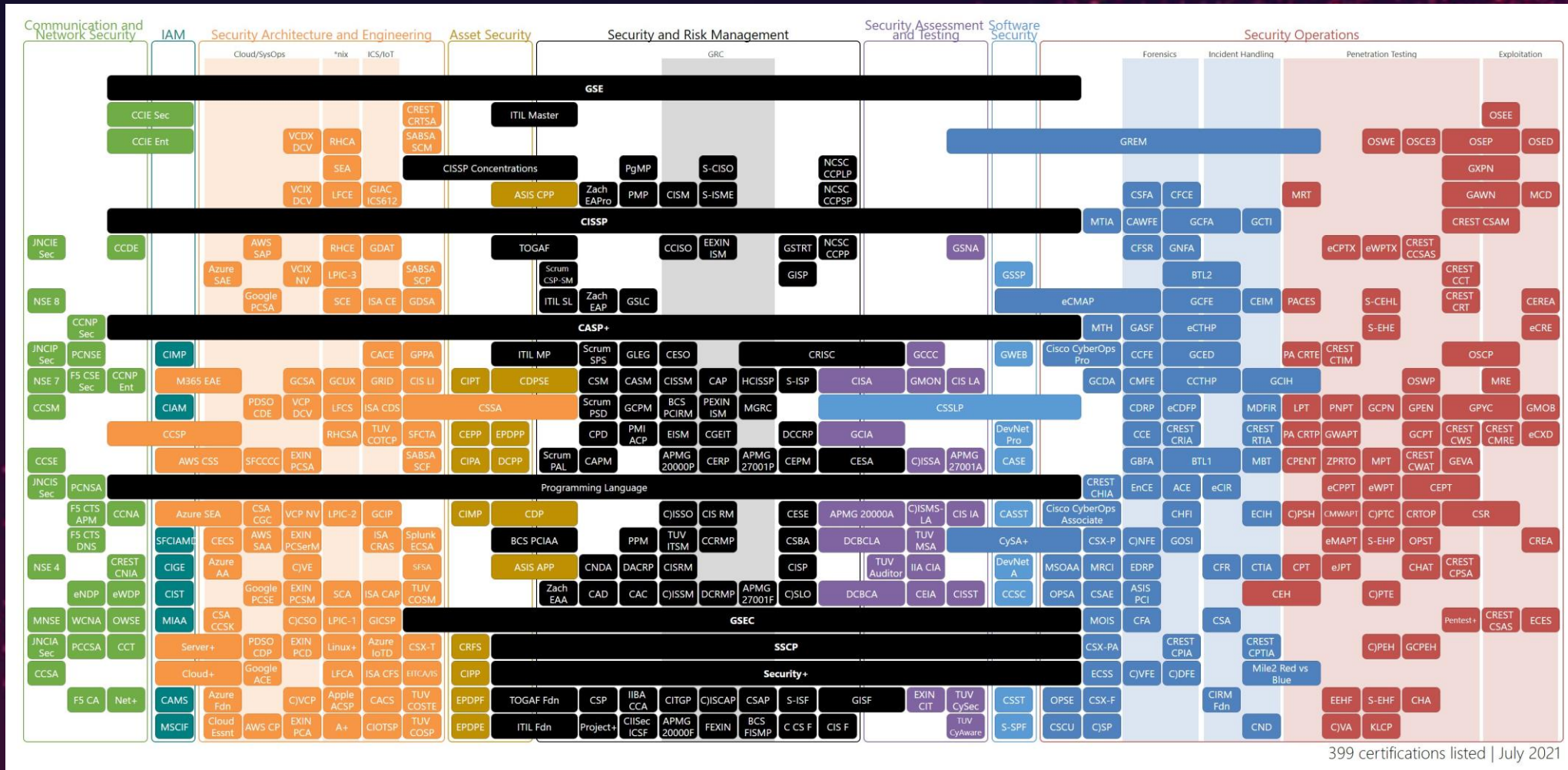
399 certifications listed | July 2021

TestOut®
CYBERSECURITY AWARENESS MONTH

Image credit: https://pauljerimy.com/security-certification-roadmap/

What certifications should I get?

- What do you want to do?

- What level of job are you targeting?

- What resources do you have?
  - Can your school help?
  - Will your employer pay for the training/exam?

- What level of effort does the certification take?
  - Don't look for easy wins (bootcamps, crash courses, etc.), instead find resources that allow adequate preparation and time to actually learn material
  - Look for certifications that are hands-on, not just memorize and regurgitate

TestOut®
CYBERSECURITY
AWARENESS MONTH

Image credit: CyberSeek

What certifications should I get?

IAT Level 1 (Network Specialist, HelpDesk Technician, IS Security Specialist)
A+ CE, CCNA-Security, CND, Network+ CE, SSCP

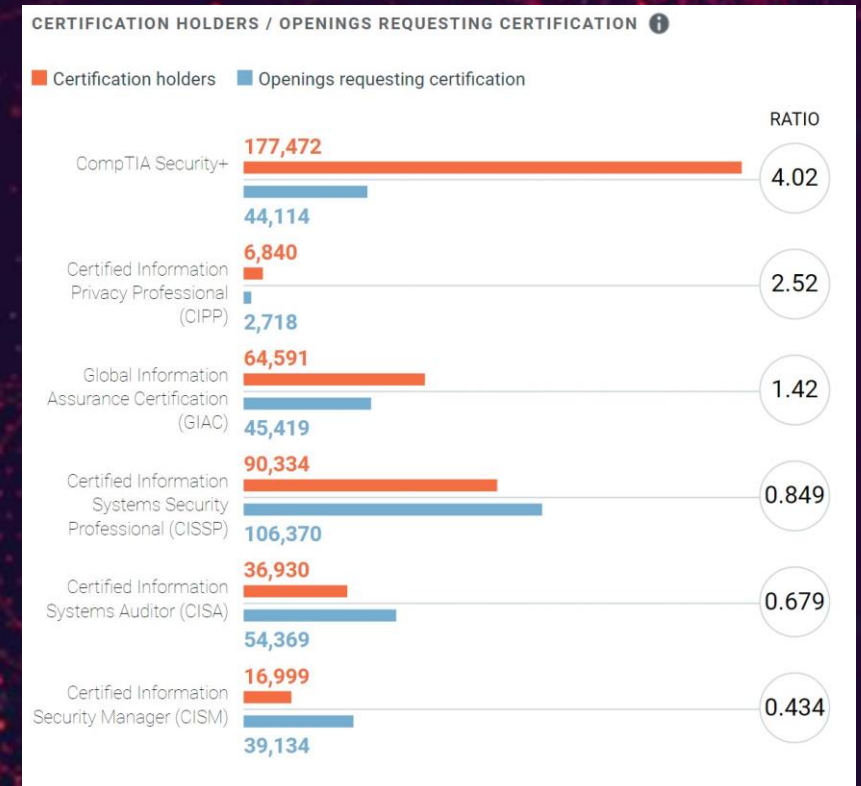**IAM Level 1 (System Administrator, Network Engineer)**
CAP, CND, Cloud+, GSLC, Security+ CE, HCISSP

IASAE 1 (Network Specialist, Auditor, Cyber Security Engineer)
CASP+ CE, CISSP, CSSLP

CSSP Analyst (Cyber Defense Analyst, Monitoring Specialist)
CEH, CFR, CCNA Cyber Ops, CCNA Security, CySA+, GCIA, GCIH, GICSP, Cloud+

https://public.cyber.mil/cw/cwmp/dod-approved-8570-baseline-certifications/

CERTIFICATION HOLDERS / OPENINGS REQUESTING CERTIFICATION ⓘ

■ Certification holders   ■ Openings requesting certification

		RATIO
CompTIA Security+	177,472 / 44,114	4.02
Certified Information Privacy Professional (CIPP)	6,840 / 2,718	2.52
Global Information Assurance Certification (GIAC)	64,591 / 45,419	1.42
Certified Information Systems Security Professional (CISSP)	90,334 / 106,370	0.849
Certified Information Systems Auditor (CISA)	36,930 / 54,369	0.679
Certified Information Security Manager (CISM)	16,999 / 39,134	0.434

TestOut®
CYBERSECURITY AWARENESS MONTH

Where do I start?: Self-Learning

Resources to Learn Skills

- malware-traffic-analysis.net
- hackthebox.eu
- tryhackme.com
- Web Security Academy (portswigger)
- Cybrary
- Cisco Packet Tracer (NetAcad)
- SANS Cyber Aces
- https://www.nist.gov/itl/applied-cybersecurity/nice/resources/online-learning-content

TestOut®
CYBERSECURITY
AWARENESS MONTH

Where do I start?: Networking

Organizations

- National Cybersecurity Student Association

- Information Systems Security Association

- ISACA

- National Cyber Security Alliance

- Women in CyberSecurity

- Blacks in Cybersecurity

- Minorities in Cybersecurity

- School Clubs

TestOut®
CYBERSECURITY
AWARENESS MONTH

Image credit: CyberSeek

Questions