Accelerating and Pivoting your Security Career

OWASP CT HARTFORD CHAPTER

bSidesCT 2017


DISCLAIMER

I am a Whitehat Illuminati Hacker. During the day I moonlight as a Research Director for Gartner. I am here because I love to give presentations. You can find me at @mcgoverntheory

HELLO!

I am James McGovern

OATH KEEPER
CUSTODES REI PUBLICAE
10
NOT ON OUR WATCH
OATH KEEPER

OWASP
Open Web Application Security Project

I am a “Breaker”. During the day I moonlight as a Principle Security Architect at Lodestone Security. I’m here because CT needs YOU to help save InfoSEC!

You can find me on Meetup and LinkedIn

My name is Alvin Fong

Oh Hai!

About OWASP

- The Open Web Application Security Project (OWASP) is a worldwide free and open community focused on improving the security of software software. Our mission is to make application security "visible," so that people and organizations can make informed decisions about application security risks. Everyone is free to participate in OWASP and all of our materials are available under a free and open software license. The OWASP Foundation is a 501c3 not-for-profit charitable organization that ensures the ongoing availability and support for our work

CORE VALUES

- OPEN: Everything at OWASP is radically transparent from our finances to our code
- INNOVATION: OWASP engoucrages and supports innovation and experiments for solutions to software security challenges.
- GLOBAL: Anyone around the world is encouraged to participate in the OWASP community.
- INTEGRITY: OWASP is an honest, truthful, vendor neutral, global community

Our core purpose is to be a thriving global community that drives visibility and evolution in the safety and security of the world's software.

Accelerating and Pivoting your Security Career

- Objectives
- State of Computer Security employment
- The Pipeline problem and potential solutions
- Visualizing career paths; common paths, technical and non-technical skills
- Common Computer Security tracks
- Industry “fit”
- Career Pipeline; Past, Present Future
- Learning Resources
- OWASP Mentorship Initiative

Objectives

Hiring managers/ recruiters/ HR	K-12 / Academic Institutions	New Professionals	Experienced Professionals
• Understand typical corporate barriers to entry • Framework for technical security skills • Break down security hiring barriers	• Understand academic barriers to entry • Understand security education needs • Develop/Modify curriculums	• Understand security career landscape • Determine interesting career paths • Focus on technical skills mapped to interested path • Plan for security skillset changes	• Understand alternative security career domains • Leverage skills commonalities to determine domains for career pivoting • Plan for security skillset changes • Mentorship

STATE OF COMPUTER SECURITY EMPLOYMENT

Marketplace Realities

Millennials are careless with passwords

- Just 33% of Millennials use secure passwords for all of their accounts, compared to 53% of baby boomers
- http://www.prnewswire.com/news-releases/millennial-travelers-more-vulnerable-to-cybersecurity-attacks-than-boomers-according-to-new-webroot-survey-300274423.html

Breaches are becoming commonplace.

- 32% of companies said they were the victims of cyber crime in 2016.
- http://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html

CIOs don't have much confidence in their efforts

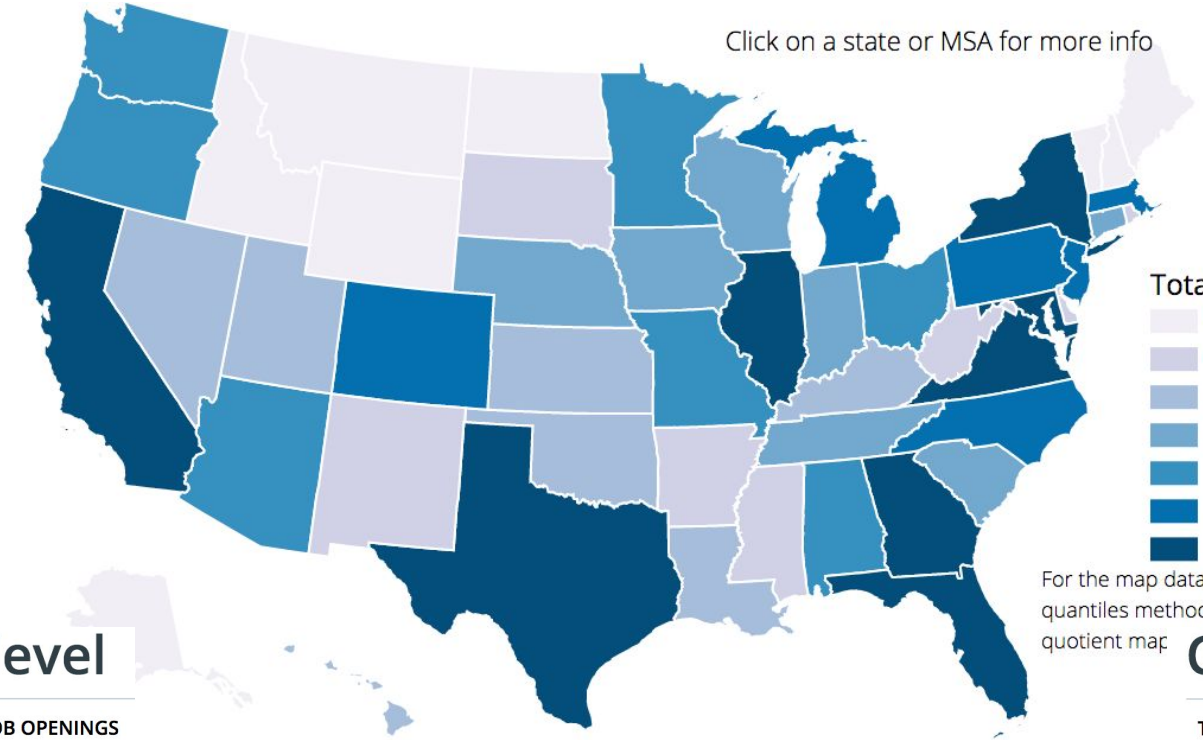
- 87% of CIOs believe their security controls are failing to protect their business.
- https://www.venafi.com/assets/pdf/wp/Venafi_2016CIO_SurveyReport.pdf

Human attack surface to reach 4 billion people by 2020

- Microsoft estimates that by 2020 4 billion people will be online—twice the number that are online now. The hackers smell blood now, not silicon.
- http://www.csoonline.com/article/3149510/security/the-human-attack-surface-counting-it-all-up.html

Economics


Adjusting Security Plans in 2017 for Cyber Attack Victims
52% have no changes planned
31% are making changes to their security plan
17% not sure
Barkly



National level

TOTAL CYBERSECURITY JOB OPENINGS

299,335

TOTAL EMPLOYED CYBERSECURITY WORKFORCE

746,858

http://cyberseek.org/heatmap.html

Connecticut

TOTAL CYBERSECURITY JOB OPENINGS

3,440

TOTAL EMPLOYED CYBERSECURITY WORKFORCE

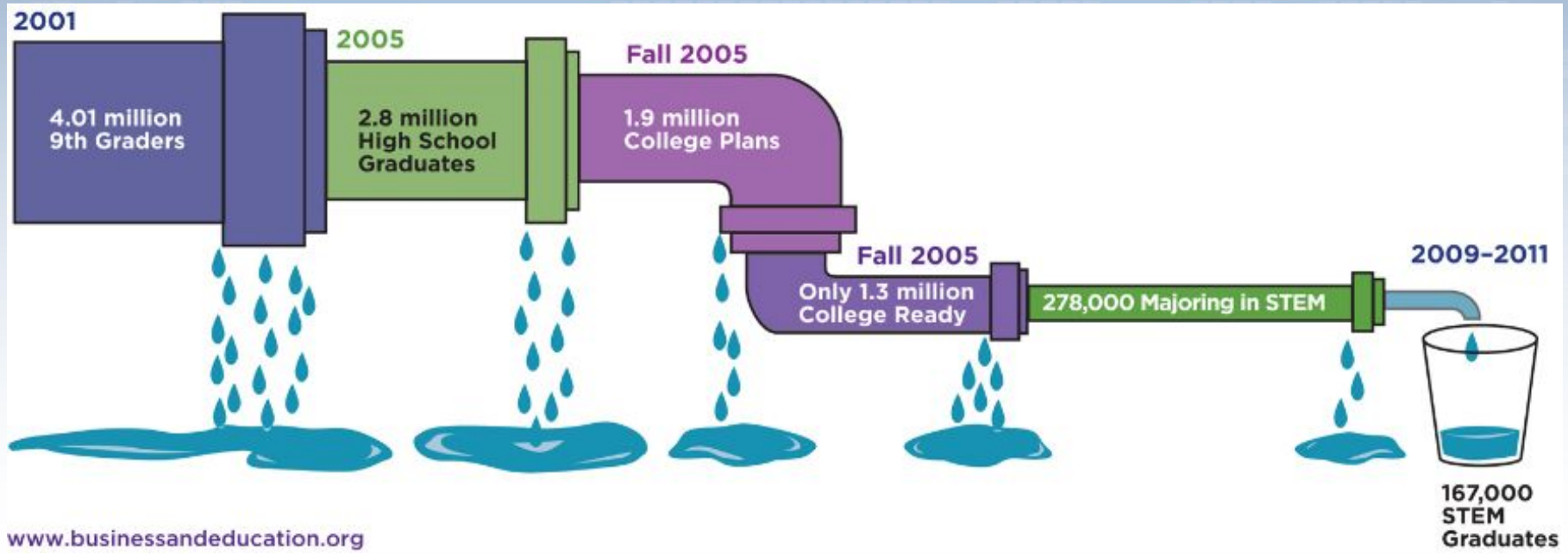
6,671

Top 10 Average Security Salaries

Dice

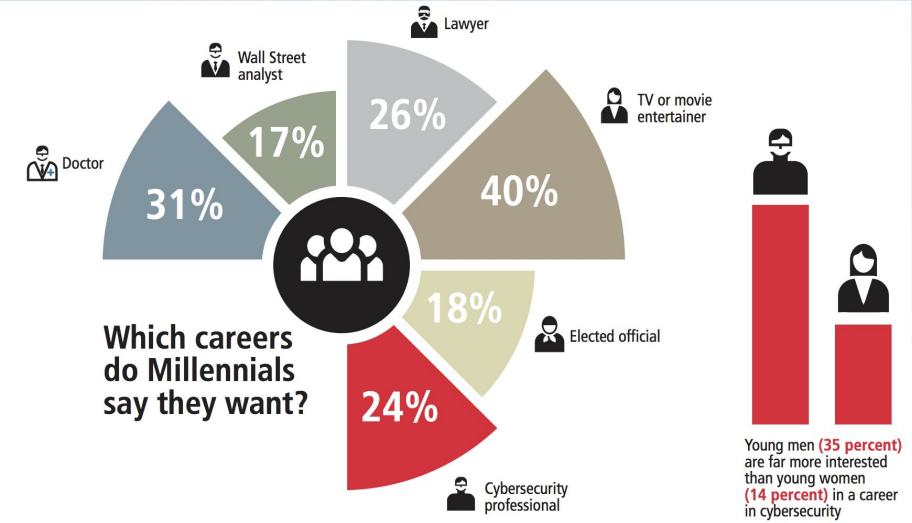
OWASP
Open Web Application Security Project

A Leaking STEM Pipeline



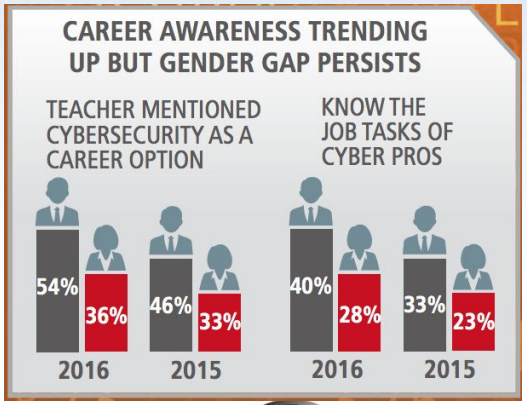
Millennials

Career opportunities in cybersecurity are increasing but it's not clear that Millennials are being coached to fill the need. Eighty-two percent say no high school teacher or guidance counselor ever mentioned to them the idea of a career in cybersecurity.

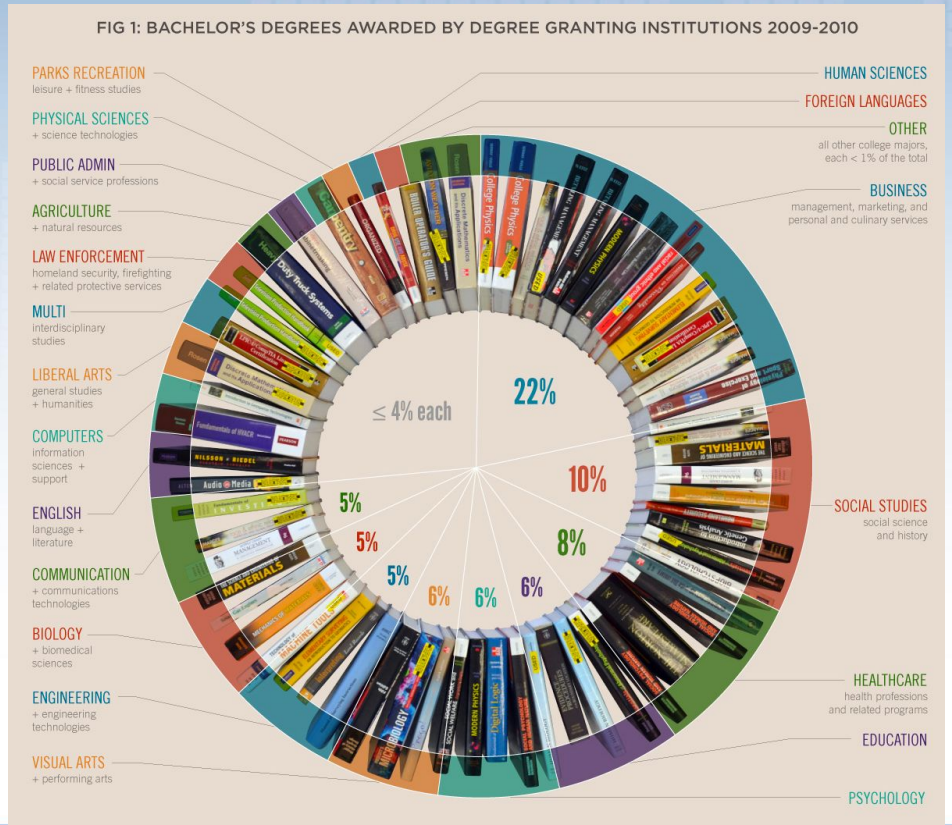


http://www.raytheon.com/capabilities/rtnwcm/groups/gallery/documents/digitalasset/rtn_158203.pdf

Starting to get better this past year…



If we limit Computer Security to only Computer-related majors…

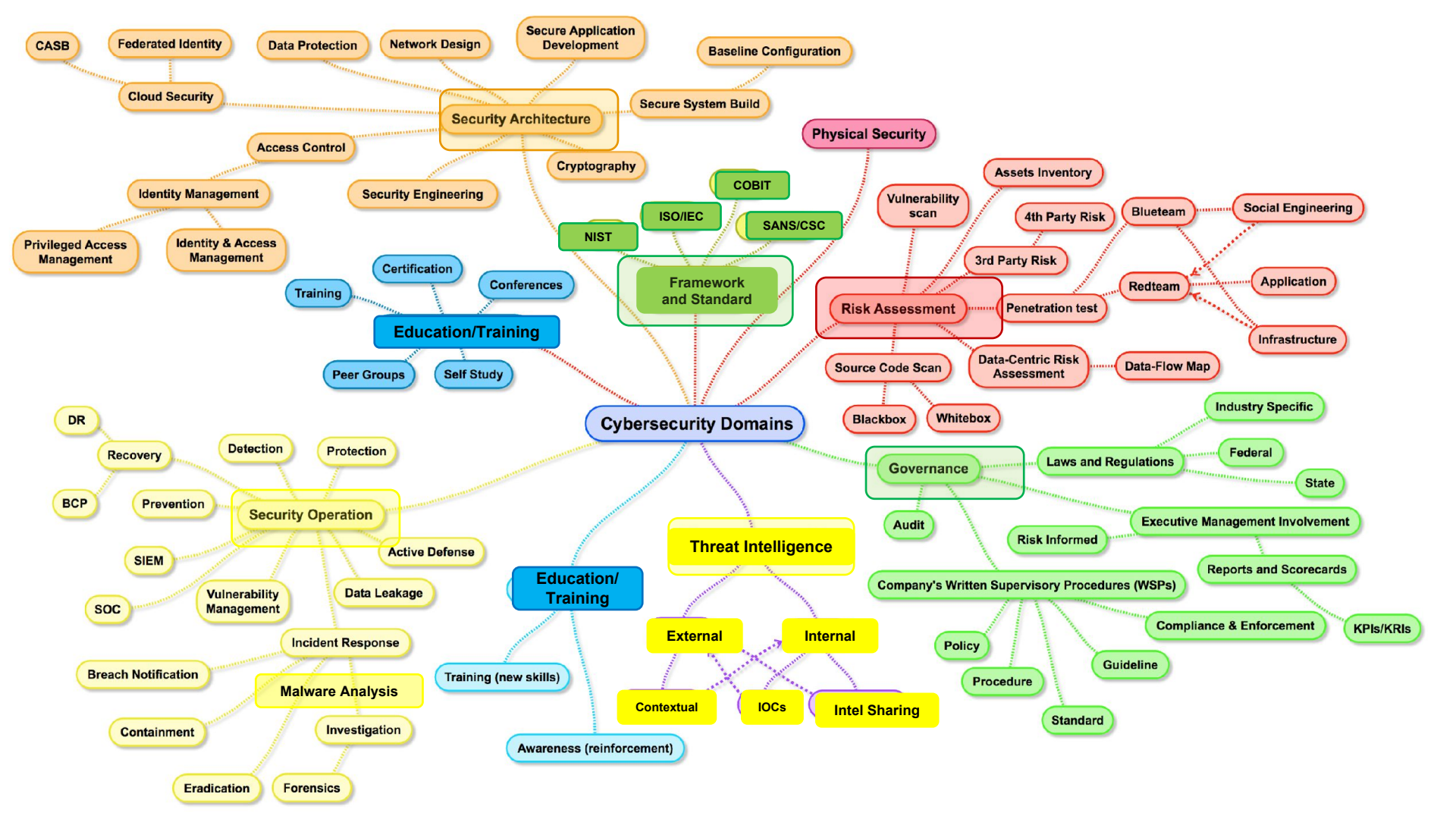


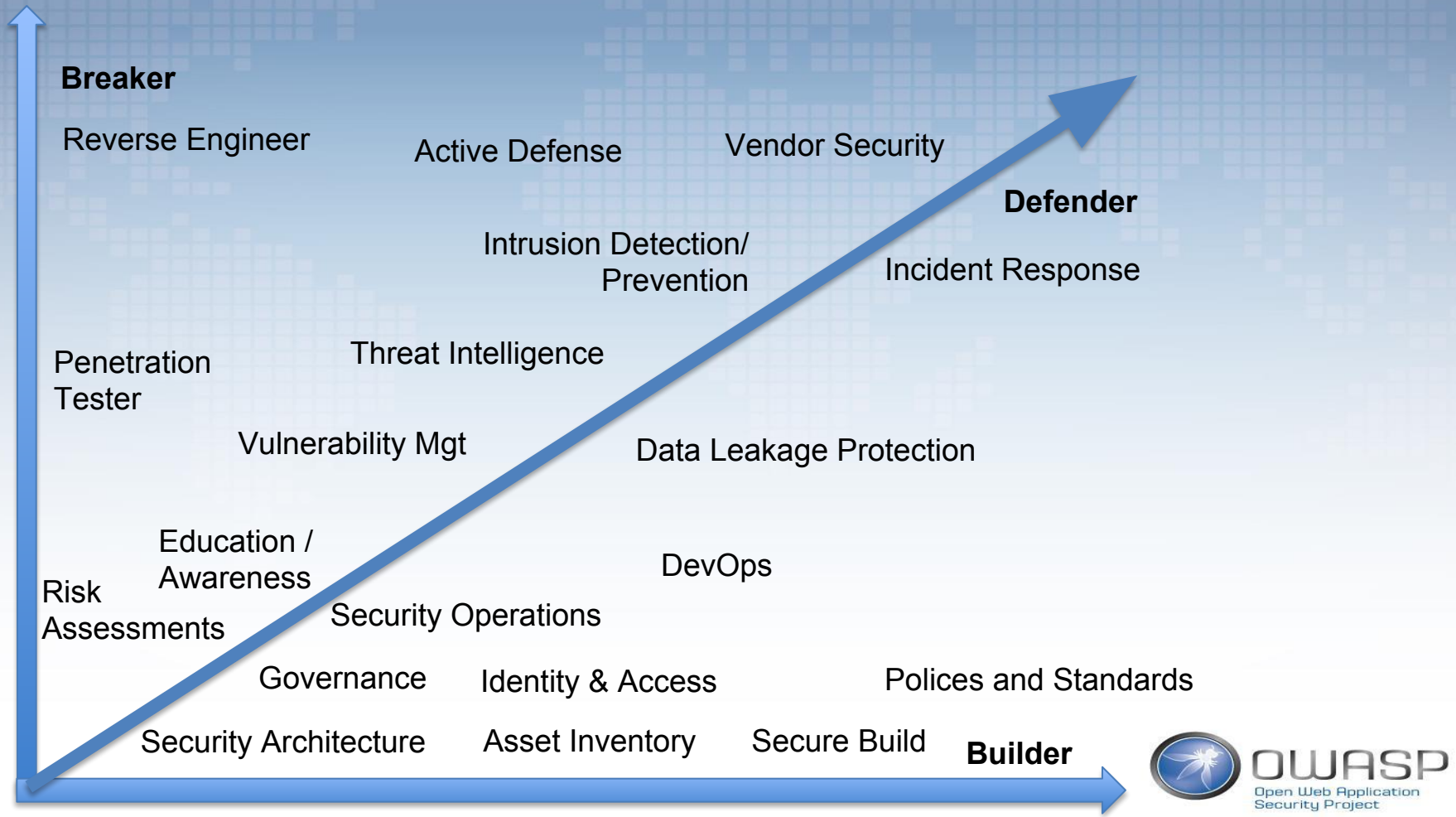
OWASP
Open Web Application Security Project

How to Fix

- K-12:
  - Increase computer security career awareness, r00tz asylum etc.
  - Apprenticeships
- Academic Institutions:
  - Interdisciplinary programs and Professional-oriented programs
  - Include computer security courses in non comp sci/engineering degrees
  - Having an environment where classes are taught by Practioners
- Hiring managers, Recruiters, HR:
  - Remove artificial barriers to entry; comp sci degree requirement
  - Establish non-technical security career tracks

Computer Security Career Paths


Cybersecurity Domains
Security Architecture
CASB
Federated Identity
Data Protection
Network Design
Secure Application Development
Baseline Configuration
Cloud Security
Secure System Build
Access Control
Cryptography
Identity Management
Security Engineering
Privileged Access Management
Identity & Access Management
Physical Security
Framework and Standard
COBIT
ISO/IEC
SANS/CSC
NIST
Education/Training
Certification
Conferences
Training
Peer Groups
Self Study
Risk Assessment
Assets Inventory
Vulnerability scan
4th Party Risk
Blueteam
Social Engineering
3rd Party Risk
Redteam
Application
Penetration test
Infrastructure
Source Code Scan
Data-Centric Risk Assessment
Data-Flow Map
Blackbox
Whitebox
Governance
Industry Specific
Laws and Regulations
Federal
State
Audit
Executive Management Involvement
Risk Informed
Reports and Scorecards
Company's Written Supervisory Procedures (WSPs)
Compliance & Enforcement
KPIs/KRIs
Policy
Guideline
Procedure
Standard
Threat Intelligence
External
Internal
Contextual
IOCs
Intel Sharing
Education/ Training
Training (new skills)
Awareness (reinforcement)
Security Operation
DR
Recovery
Detection
Protection
BCP
Prevention
SIEM
Active Defense
SOC
Vulnerability Management
Data Leakage
Incident Response
Breach Notification
Malware Analysis
Containment
Investigation
Eradication
Forensics

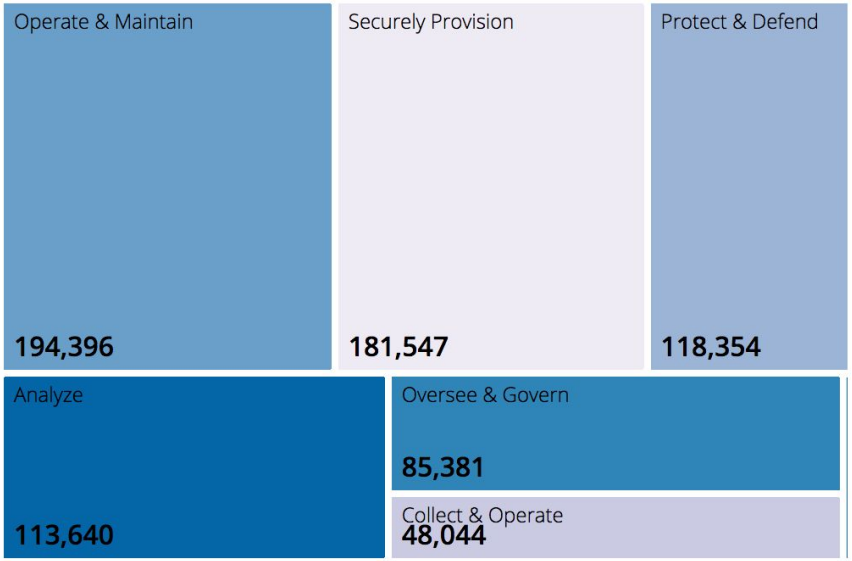


NIST 800-181

Categories	Descriptions
Securely Provision (SP)	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.
Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
Analyze (AN)	Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Collect and Operate (CO)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Investigate (IN)	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

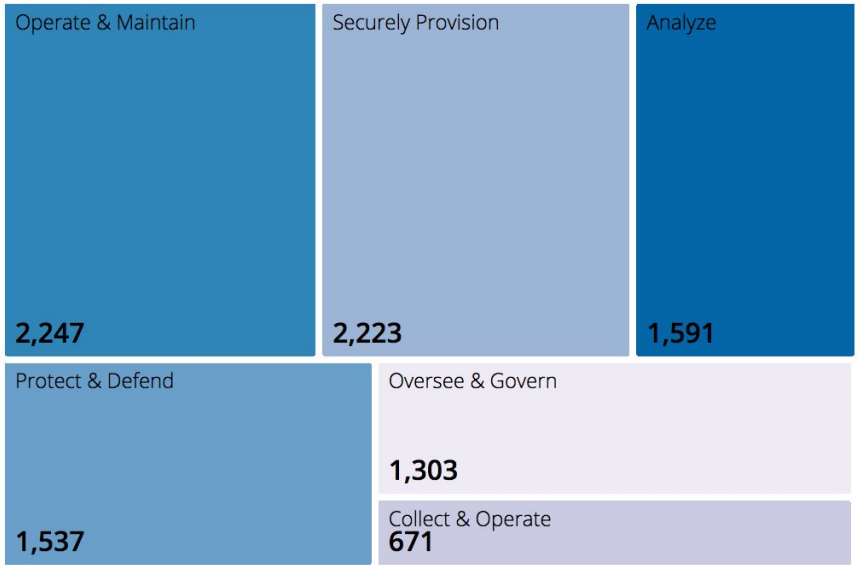
Work Role Name	**Security Architect**
Work Role ID	**SP-ARC-002**
Specialty Area	**Systems Architecture (ARC)**
Category	**Securely Provision (SP)**
Work Role Description	Ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes.
Tasks	T0050, T0051, T0071, T0082, T0084, T0090, T0108, T0177, T0196, T0203, T0205, T0268, T0307, T0314, T0328, T0338, T0427, T0448, T0473, T0484, T0542, T0556
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0009, K0010, K0011, K0012, K0013, K0015, K0018, K0019, K0024, K0026, K0027, K0030, K0035, K0036, K0037, K0043, K0044, K0052, K0055, K0056, K0057, K0059, K0060, K0061, K0063, K0071, K0074, K0082, K0091, K0092, K0093, K0102, K0170, K0180, K0198, K0200, K0202, K0211, K0212, K0214, K0227, K0240, K0260, K0261, K0262, K0264, K0275, K0277, K0286, K0287, K0291, K0293, K0320, K0322, K0323, K0325, K0326, K0332, K0333, K0336, K0374, K0565
Skills	S0005, S0022, S0024, S0027, S0050, S0059, S0061, S0076, S0116, S0122, S0138, S0139, S0152, S0168, S0170, S367, S0374
Abilities	A0008, A0014, A0015, A0027, A0038, A0048, A0049, A0050, A0061, A0123, A0148, A0149, A0170, A0172

National level



Connecticut

POSTINGS BY NICE CYBERSECURITY WORKFORCE FRAMEWORK CATEGORY



Common Careers Paths – Security Governance Track

Network Security Administrator -> Sr. Mgr Information Security Technical -> [SMB CISO]

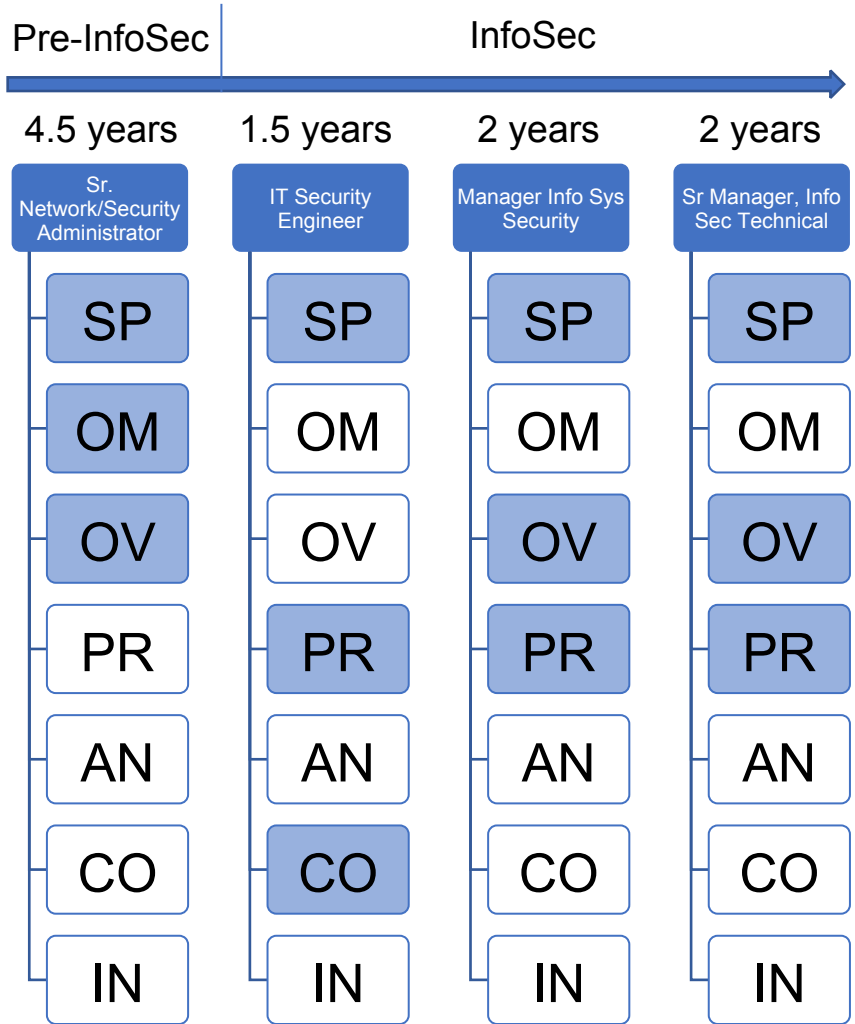
Entry path: System Administrator
BS Comp Sci

Technical Skills for the role:

- ✓ Securely Provision (SP)
  - Systems Architecture
  - Systems Requirements Planning
- ✓ Oversee and Govern (OV)
  - Strategic Planning & Policy
- ✓ Protect & Defend (PR)
  - Defense Infrastructure Support

Top Non-Tech Skills Required for the role

- ✓ Communication
- ✓ People Management
- ✓ Accountability



Common Careers Paths – Security Architect Track

InfoSec Identity Mgt -> Enterprise Security Architect ->

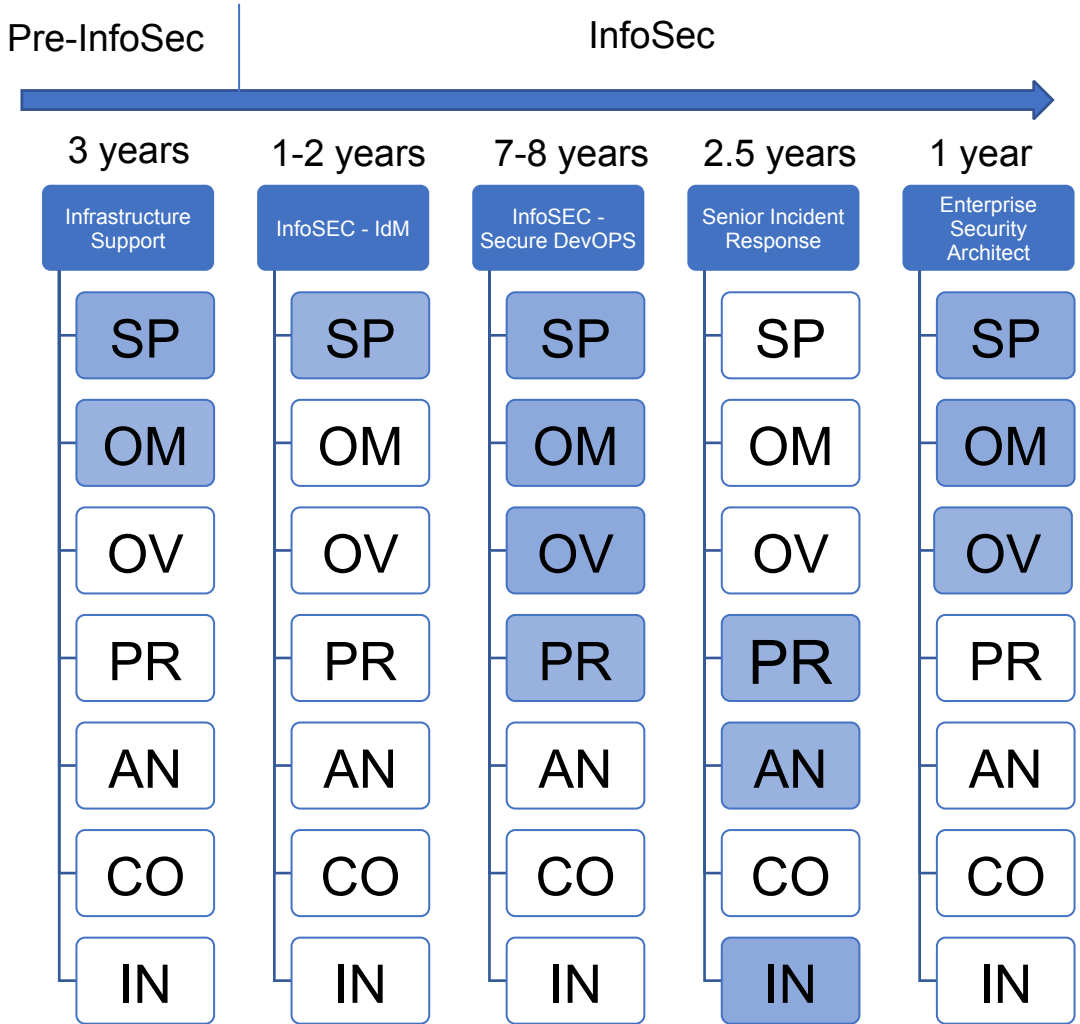
Entry path: Desktop/Server support
BA Information Technology

Technical Skills for the role:

- ✓ Securely Provision (SP)
  - Systems Architecture
  - Systems Requirements Planning
- ✓ Operate and Maintain (OM)
  - Customer Service and Technical Support
- ✓ Oversee and Govern (OV)
  - Strategic Planning & Policy

Top Non-Tech Skills Required for the role

- ✓ Communication
- ✓ Curiosity
- ✓ Willingness & ability to challenge status quo



Common Careers Paths – Security Operations Track

Software Eng-> Team Manager -> [Technical SME]

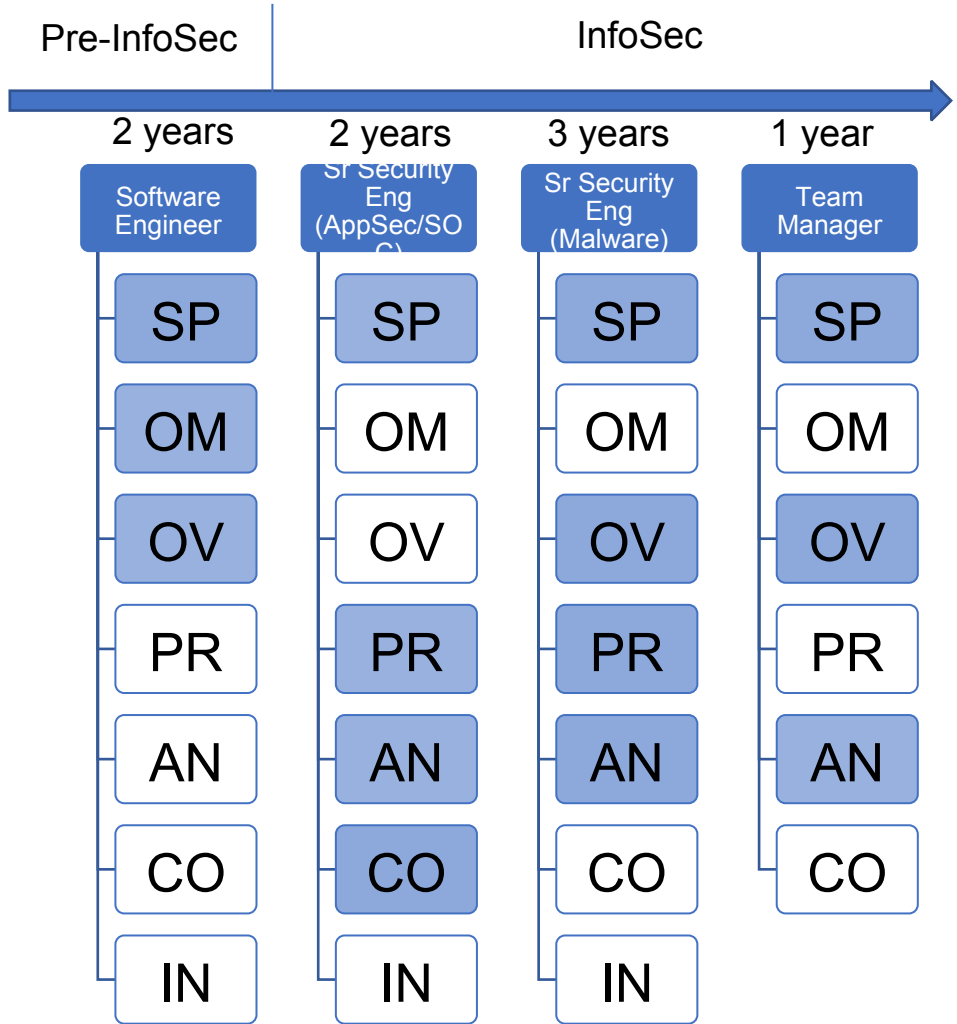
Entry path: Software Engineer
M.S. Electrical & Computer Engineering

Technical Skills focused on for the role:

- ✓ Securely Provision (SP)
  - Risk Management
  - Software Development
- ✓ Oversee and Govern (OV)
  - Advice and Advocacy
  - Cybersecurity Management
  - Strategic Planning & Policy
- ✓ Protect & Defend
  - Cybersecurity Defense Analysis
  - Cybersecurity Defense Infrastructure Support
- ✓ Analyze
  - Threat Analysis

Top Non-Tech Skills Required for the role

- ✓ Communication
- ✓ Networking
- ✓ Technical Mentorship



Common Careers Paths – Risk Assessment Track

InfoSEC Engineer -> Principle Security Consultant -> [Beach Bum]

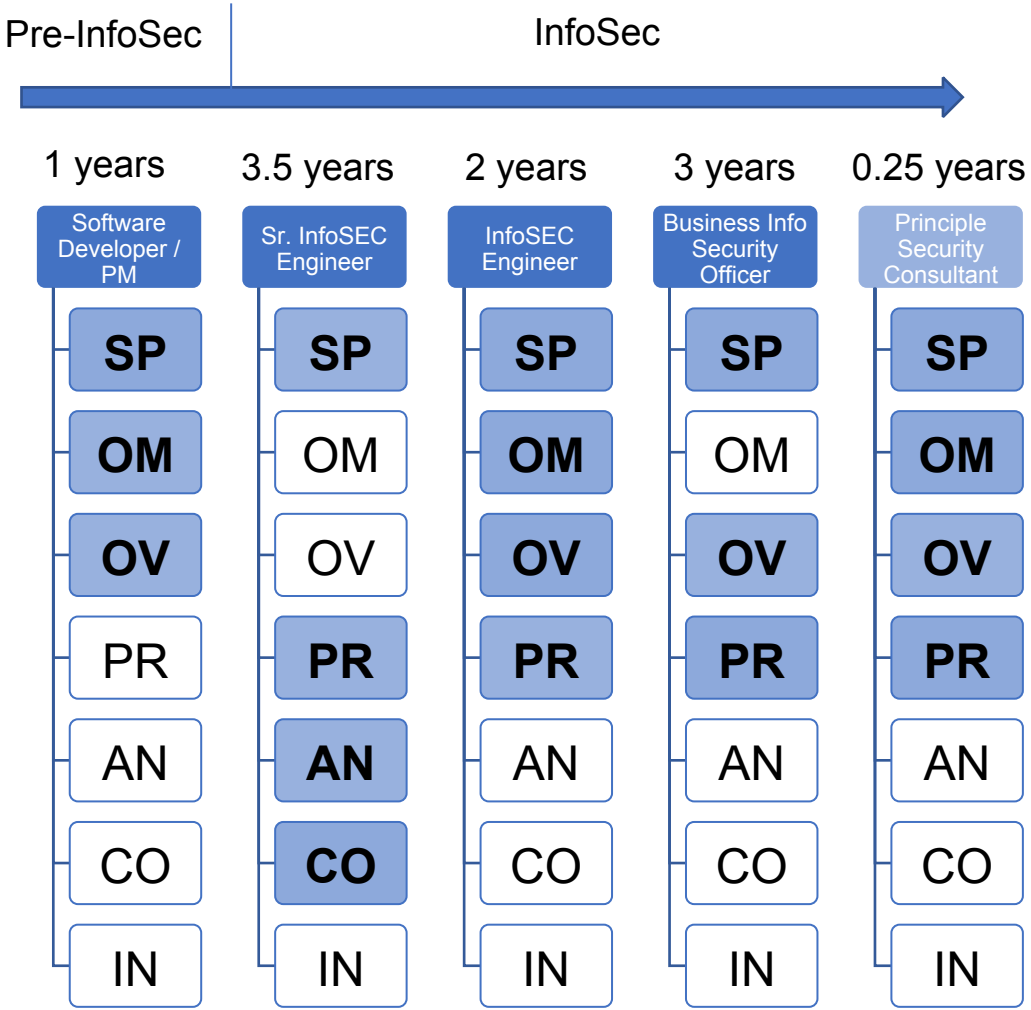
Entry path: MISM Info Sys Management
Internships: AppDev, IT Proj Mgt, Dev consulting

Technical Skills for the role:

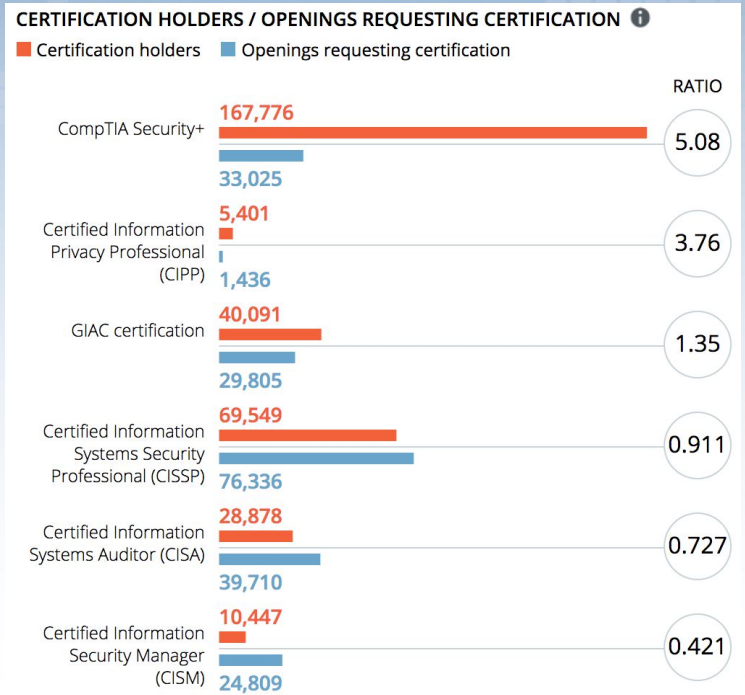
- ✓ Securely Provision (SP)
  - Risk Management
  - Systems Architecture
  - Development
- ✓ Oversee and Govern (OV)
  - Training, Education, and Awareness
  - Security Mgt & Executive Leadership
  - Strategic Planning & Policy
- ✓ Protect and Defend (PR)
  - Vulnerability Assessment & Management

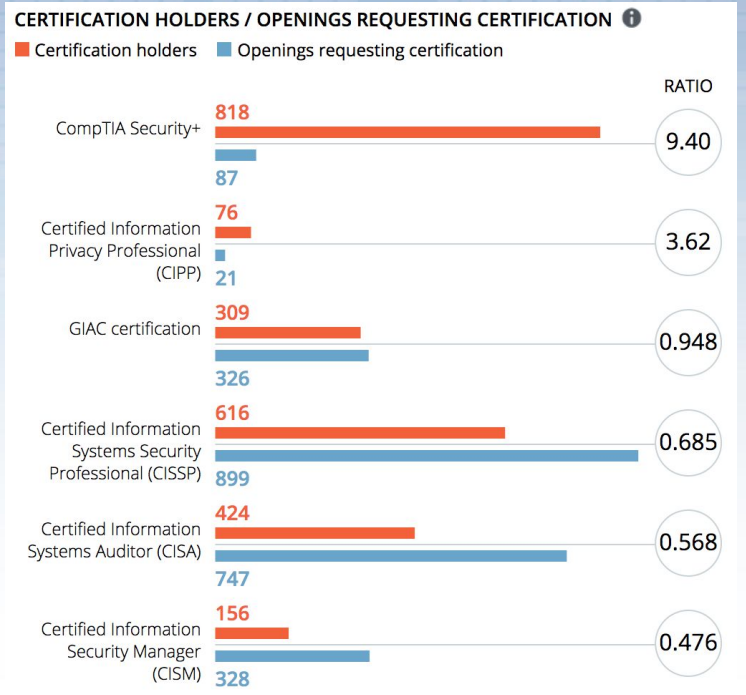
Top Non-Tech Skills Required for the role

- ✓ Communication (Presentations, verbal, written)
- ✓ Influence
- ✓ Negotiation

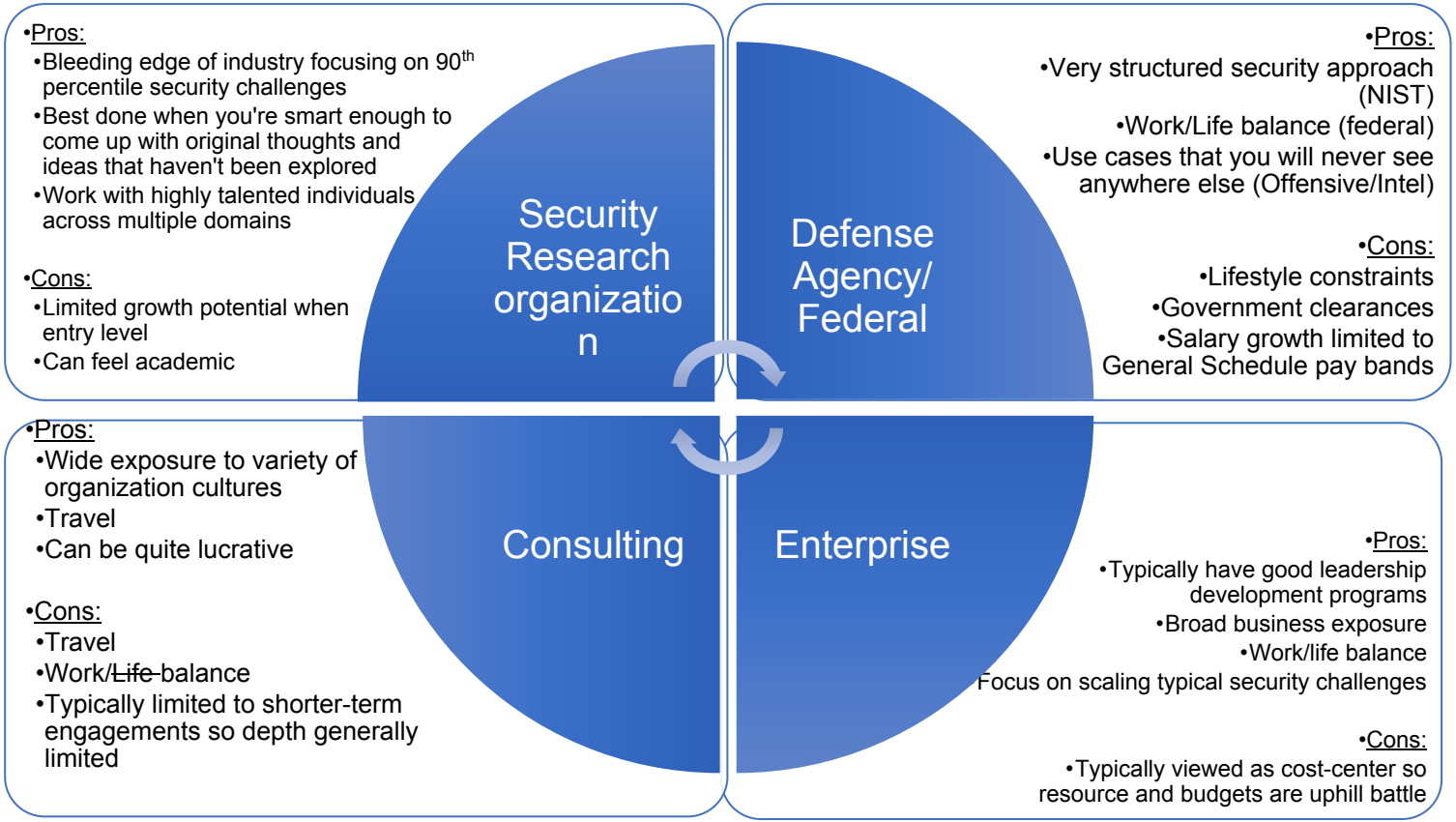


Certifications





Industry Fit



CAREER PIPELINE Entry Points

System Administrator

Software Developer

Network Administrator

IT Auditor

B.S. Computer Science

B.S. Information Systems

Risk Professional

Data Scientist

R00tz Asylum

BS/MS/PhD Computer Security

AI

Blockchain

IoT

PAST

Pre-2000 2000 2005

PRESENT

2010 2015 2020

FUTURE

2025 2030 2035

CYBERSECURITY VENTURES

THE LATEST CYBERSECURITY NUMBERS

$1,000,000,000,000
Cybersecurity spending to exceed 1 trillion between 2017 and 2021

1,500,000
Unfilled cybersecurity jobs will reach 1.5 million by 2019

$6,000,000,000,000
Cybercrime damages will cost the world 6 trillion by 2021

$221
The average cost per stolen record is $221 dollars

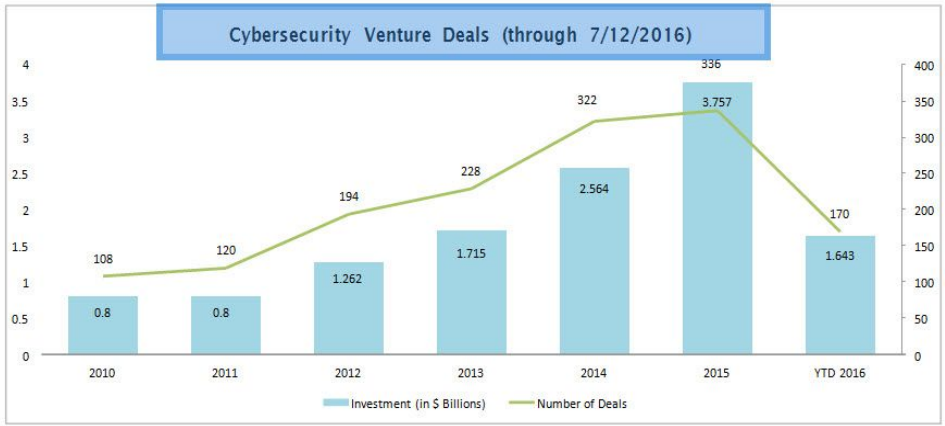
CSO FROM IDG

SC MEDIA

3.5M vacant cybersecurity roles by 2021, Cybersecurity Ventures report according to "The Cybersecurity Jobs Report," sponsored by Herjavec Group

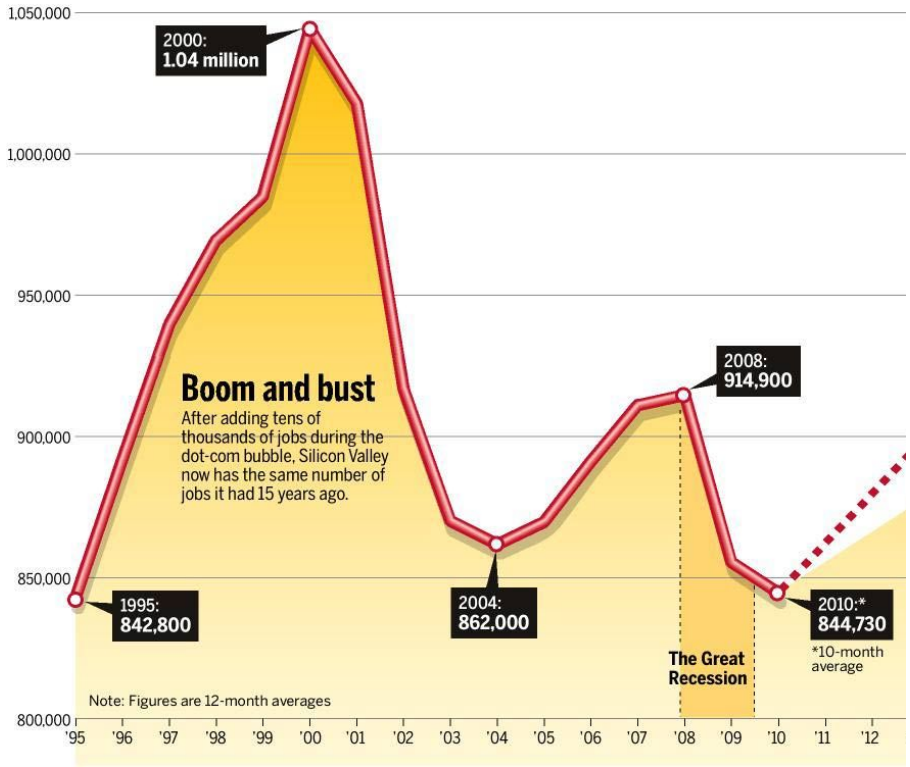
1 External spend based on forecasts to 2020 provided by Gartner, extrapolated to 2026 using the average growth rates from 2016-2020. Growth rates applied at the product segment level
2 Internal spend refers to the compensation of in-house FTEs. Estimated based on Gartner data on global internal spending. Internal spend grows more slowly than external spend, linked to the increasing adoption of external managed security services

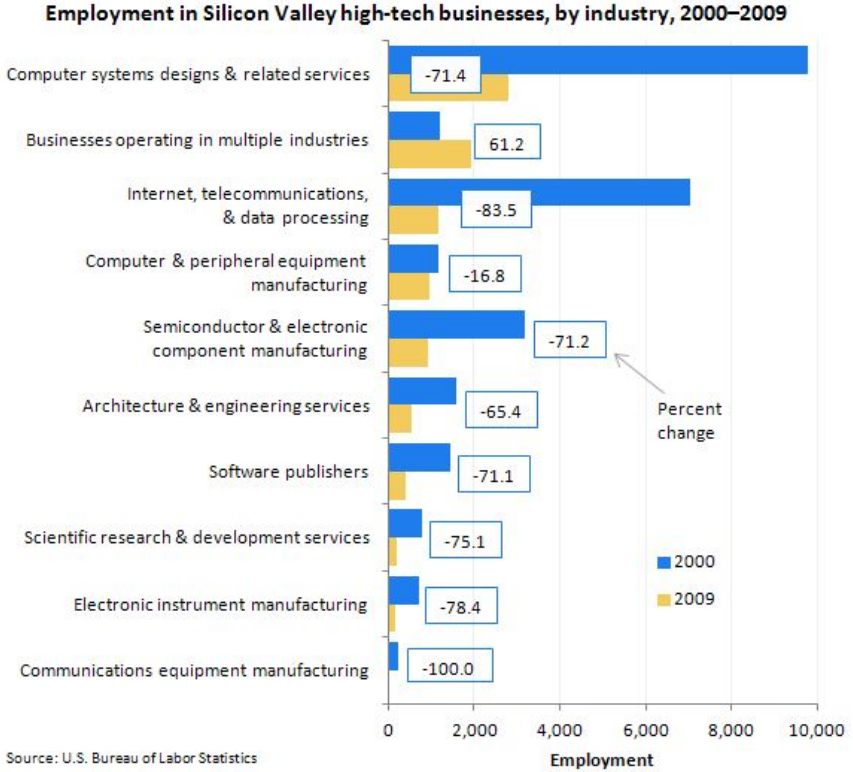
SOURCE: Gartner; ABS; Burning Glass; expert interviews; team analysis



Source: https://www.cbinsights.com/blog/cybersecurity-startups-funding-trends-q2-2016/

Wait…I've seen this before…





Identifying Critical New Skill Sets for Cybersecurity

Traditional Security Practices Are Shifting to:

Contextual Security Monitoring and Response

Data Classes, Data Governance

Embedded Security Programming

Ubiquitous Identity and Access Management

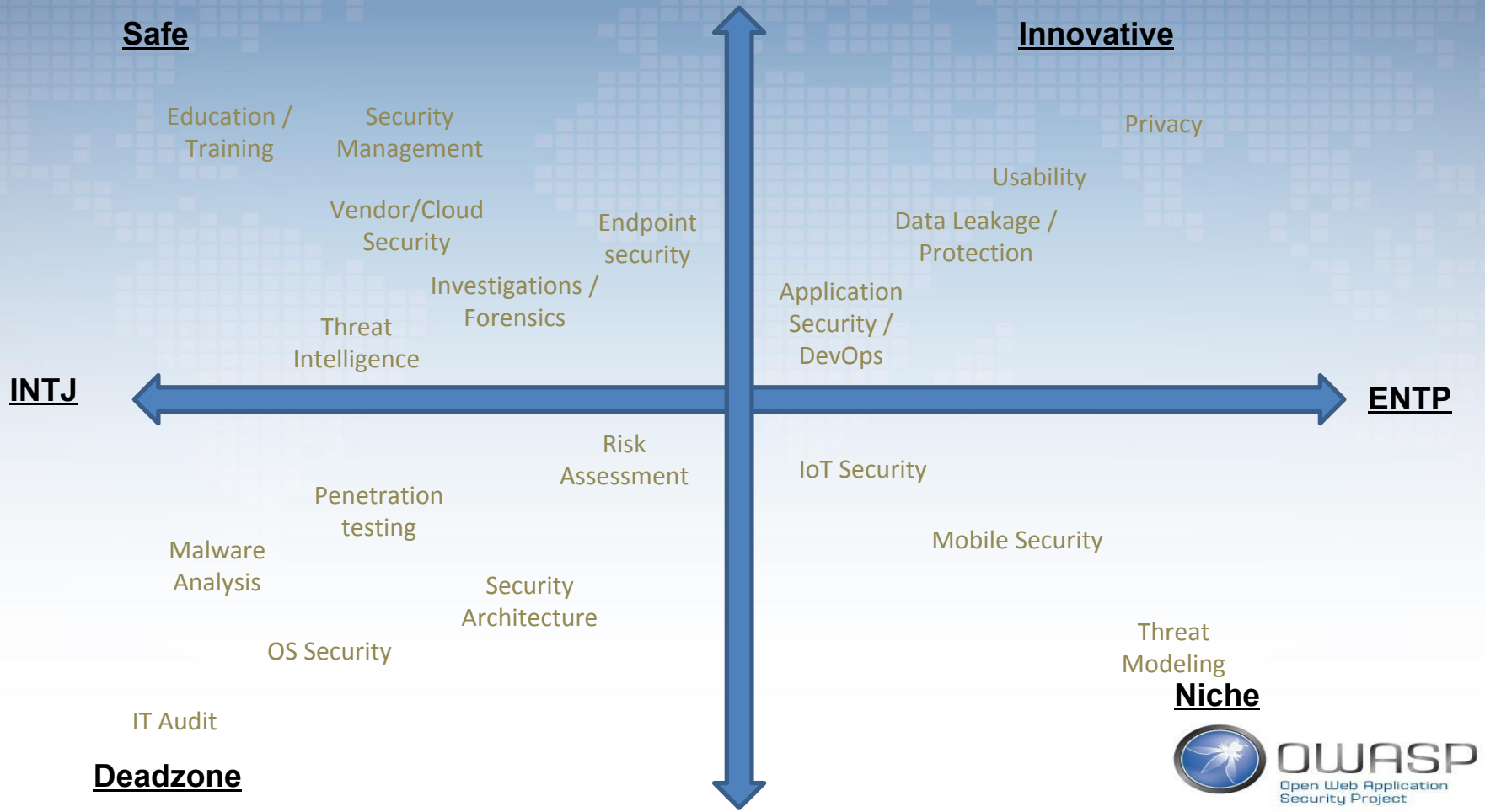
Security Awareness, Privacy and Behavior

Advanced Network Engineering

Physical Security Automation

Artificial Security Intelligence

Cloud and Service Center Expertise


Safe
Innovative
Education / Training
Security Management
Privacy
Usability
Vendor/Cloud Security
Endpoint security
Data Leakage / Protection
Investigations / Forensics
Application Security / DevOps
Threat Intelligence
INTJ
ENTP
Risk Assessment
IoT Security
Penetration testing
Mobile Security
Malware Analysis
Security Architecture
Threat Modeling
OS Security
Niche
IT Audit
Deadzone
OWASP
Open Web Application Security Project

Resources

- Opensecuritytraining.info
  - SP: x86, Trusted Computing, Understanding Cryptology, Life of Binaries
  - PR: Secure Coding, Vulnerability Assessment, Hacking Techniques
  - AN: Malware Analysis, Reverse Engineering Software/Malware, Rootkits, keylogging, Exploitation in Windows
  - IN: Android/Network Forensics, Flow Analysis

- Non-engineering security careers: BSides Boston 2017 panel
- Conference talks: OWASP BSides Defcon
- OWASP

Resources

- Cybrary
  - Securely Provision (SP)
    - Risk Management Framework
    - Secure Coding
    - NIST Controlled Unclassified Information
    - Enterprise Security Architecture
    - Intermediate Cloud Security
  - Operate & Maintain (OM)
    - Python for Security Pros
    - Virtualization Management
  - Oversee and Govern (OV)
    - Social Engineering & Manipulation
    - CISO
    - Corporate Cybersecurity Management
    - End User Security Training
  - Protect & Defend
    - Web Application Penetration Testing
    - Intro to Cyber Threat Intelligence
    - Post exploitation Hacking
    - Intro to Cyber Threat Intelligence
    - Security Operations
  - Analysis (AN)
    - Intro to Malware Analysis and Reverse Engineering
    - Dynamic Malware Analysis
  - Investigate (IN)
    - Computer and Hacking Forensics
    - Incident Response & Advanced Forensics

Mentorship Initiative

Provide professional development opportunities for future leaders of OWASP Hartford CT Community through mentoring relationships that enable the exchange of knowledge, leadership development, and career or professional development.

Takeaways

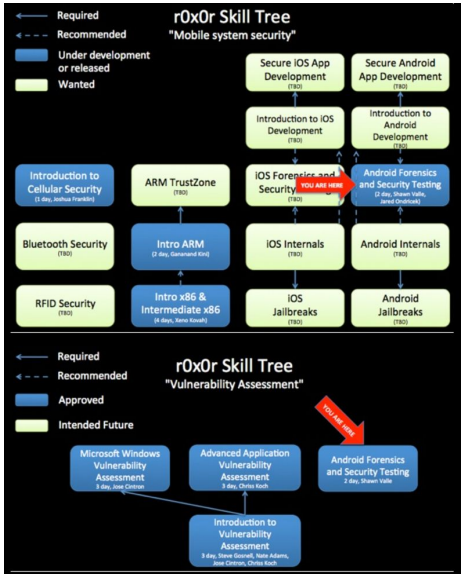
- State of Computer Security employment
- Solving the pipeline problem; academia, enterprise, industry
- Common Career Paths
- Technical/non-technical skills to focus on for new/experienced professionals
- Career pipeline is changing; how to evolve your security career and avoid the cliff
- Resources to develop technical skills
- OWASP Mentorship

Contributors

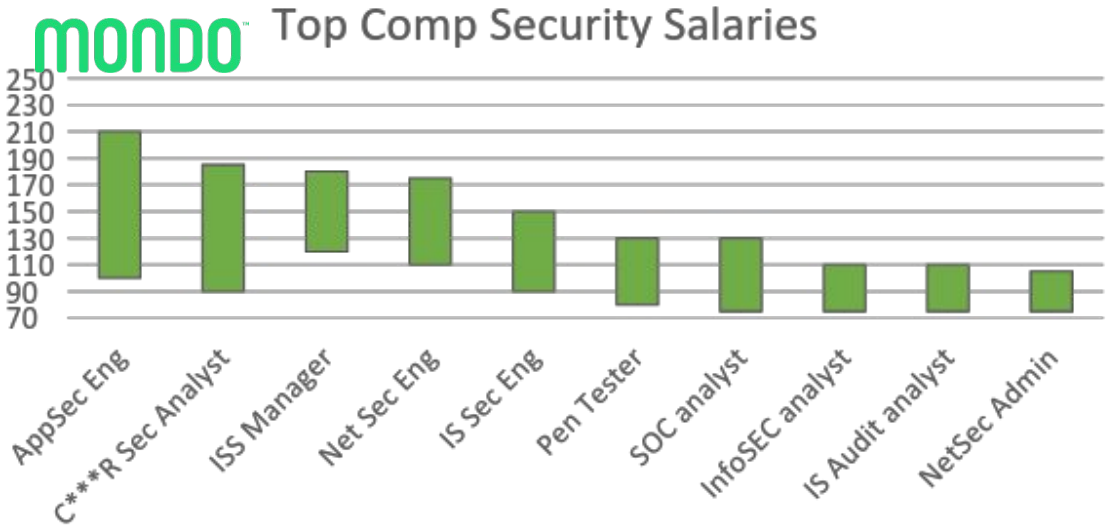
- Drew Hunt
- Emmanuel Enaohwo
- Giana Zeno-Munoz
- Jonathan Searles
- Nicole Becher
- Pierre Ernst

Acknowledgements

- Henry Jiang (Cybersecurity Domains)
- Xeno Kovah (opensecuritytraining.info)



Appendix



National level

CyberSeek™

Connecticut

TOP CYBERSECURITY JOB TITLES

- Cyber Security Engineer
- Cyber Security Analyst
- Network Engineer / Architect
- Cyber Security Manager / Administrator
- Software Developer / Engineer
- Systems Engineer
- Systems Administrator
- IT Auditor
- Vulnerability Analyst / Penetration Tester

TOP CYBERSECURITY JOB TITLES

- Cyber Security Engineer
- Cyber Security Analyst
- Cyber Security Manager / Administrator
- IT Auditor
- Network Engineer / Architect
- Internal Auditor
- Cyber Security Consultant
- Internal Audit Manager
- Cyber Security Architect