YOU BELONG AT THE TABLE:

Finding your voice in cybersecurity

Opinions are my own & do not represent my employer.

https://github.com/S1lv3rL10n/Talks

THIS TALK IS FOR YOU IF:

- Many ways into cybersecurity
- We need greater diversity
  - of People
  - of Thought
- Keep Learning

- Find Your Community
- Work Your Plan
- Find Your Voice

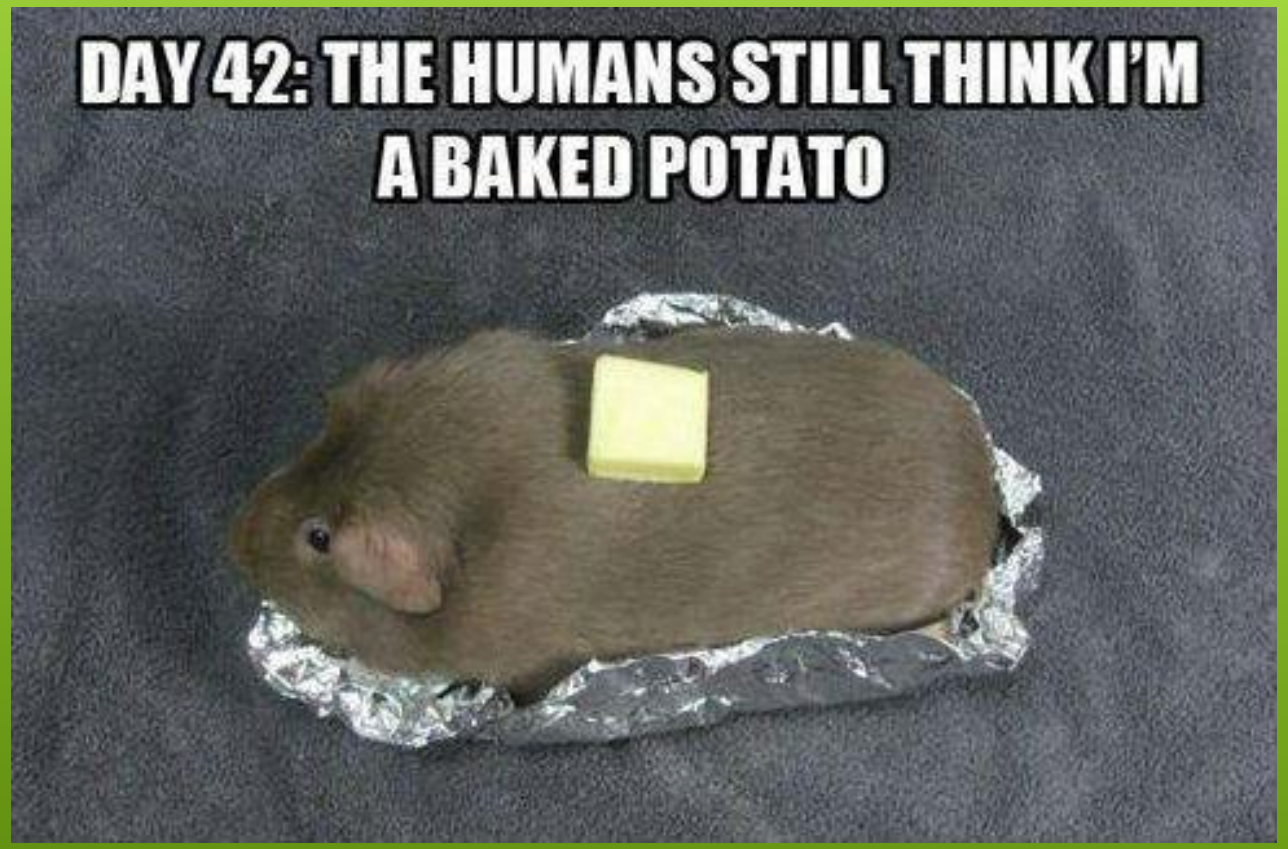
YOU BELONG AT THE TABLE

FIND YOUR COMMUNITY

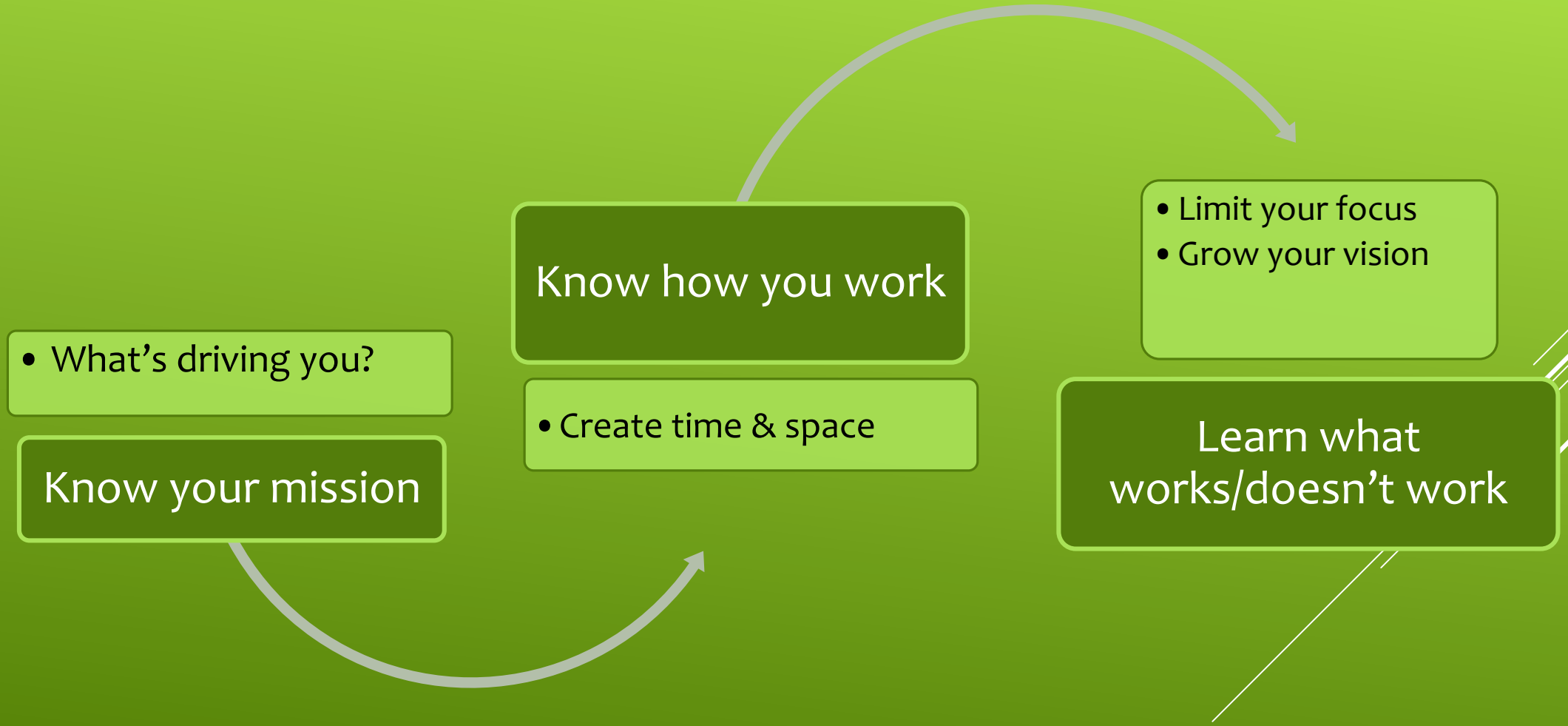
FIND YOUR COMMUNITY

- Conferences
- Groups

BE YOURSELF



BE YOURSELF


• What's driving you?
Know your mission
Know how you work
• Create time & space
• Limit your focus
• Grow your vision
Learn what works/doesn't work

Know your mission

Know how you work

Learn what works/ doesn't work


WHAT YOU KNOW
WHAT YOU ARE DOING
WHAT YOU ARE LOOKING FOR
HOW YOU CAN HELP
imgflip.com

WORK YOUR PLAN

STUDY PLAN

- U.S. Bureau of Labor Statistics
- Certification roadmaps
- Cyberseek
- NICCS
- 5 Year Plan
- Books
- And more (Podcasts, Webcasts, etc.)

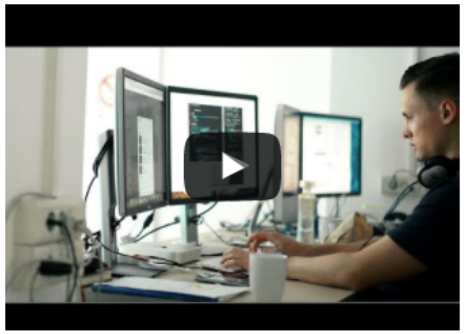
STUDY PLAN

- U.S. Bureau of Labor Statistics
- Certification roadmaps
- Cyberseek
- NICCS
- 5 Year Plan
- Books
- And more (Podcasts, Webcasts, etc.)

Information Security Analysts

Summary

Quick Facts: Information Security Analysts	
2019 Median Pay	$99,730 per year $47.95 per hour
Typical Entry-Level Education	Bachelor's degree
Work Experience in a Related Occupation	Less than 5 years
On-the-job Training	None
Number of Jobs, 2019	131,000
Job Outlook, 2019-29	31% (Much faster than average)
Employment Change, 2019-29	40,900



What Information Security Analysts Do

Information security analysts plan and carry out security measures to protect an organization's computer networks and systems.

Work Environment

Most information security analysts work for computer companies, consulting firms, or business and financial companies.

How to Become an Information Security Analyst

Most information security analyst positions require a bachelor's degree in a computer-related field. Employers usually prefer to hire analysts with experience in a related occupation.

STUDY PLAN

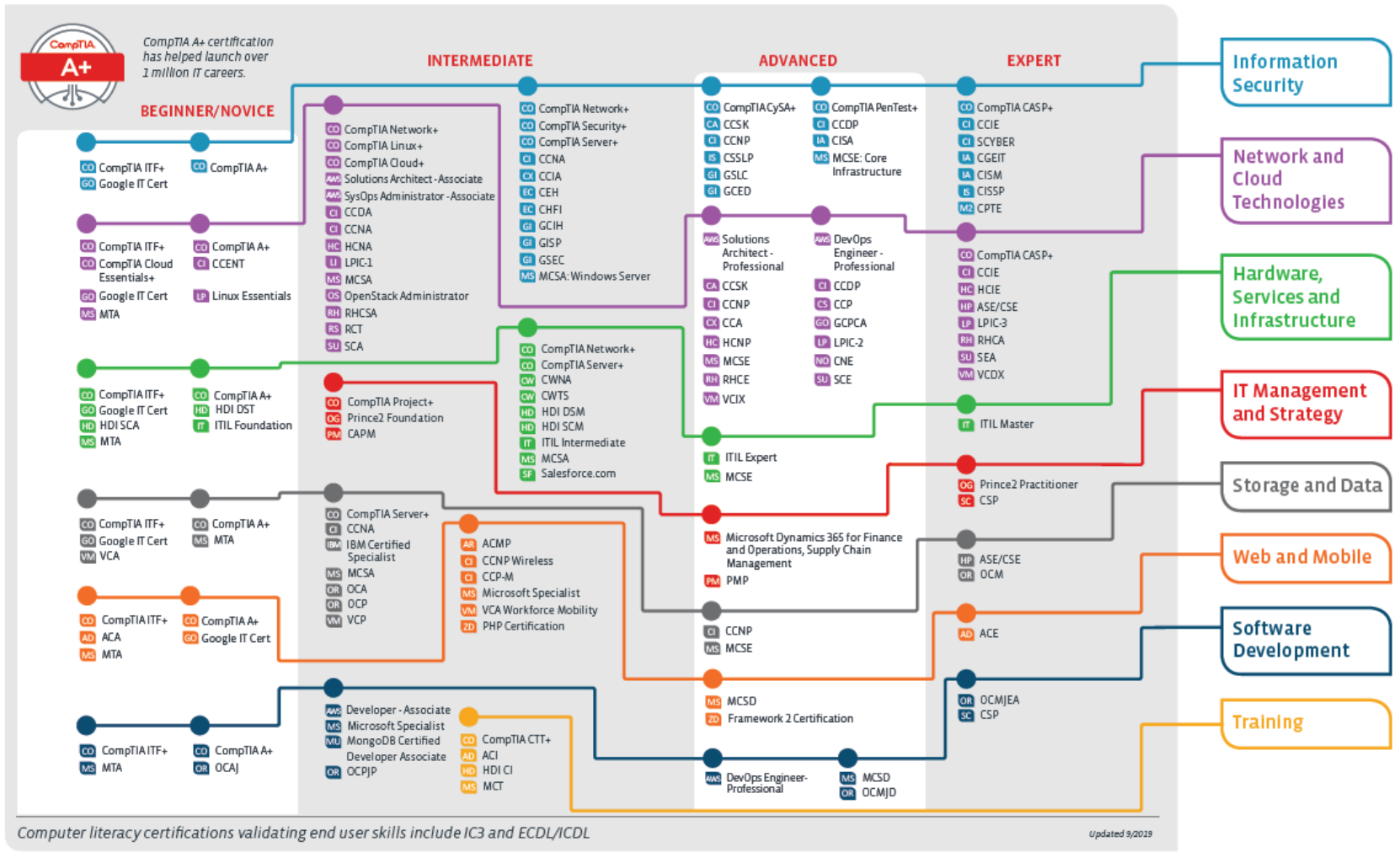
- U.S. Bureau of Labor Statistics
- Certification roadmaps
- Cyberseek
- NICCS
- 5 Year Plan
- Books
- And more (Podcasts, Webcasts, etc.)

IT Certification Roadmap

Explore the possibilities with the CompTIA Interactive IT Roadmap at: CompTIA.org/CertsRoadmap

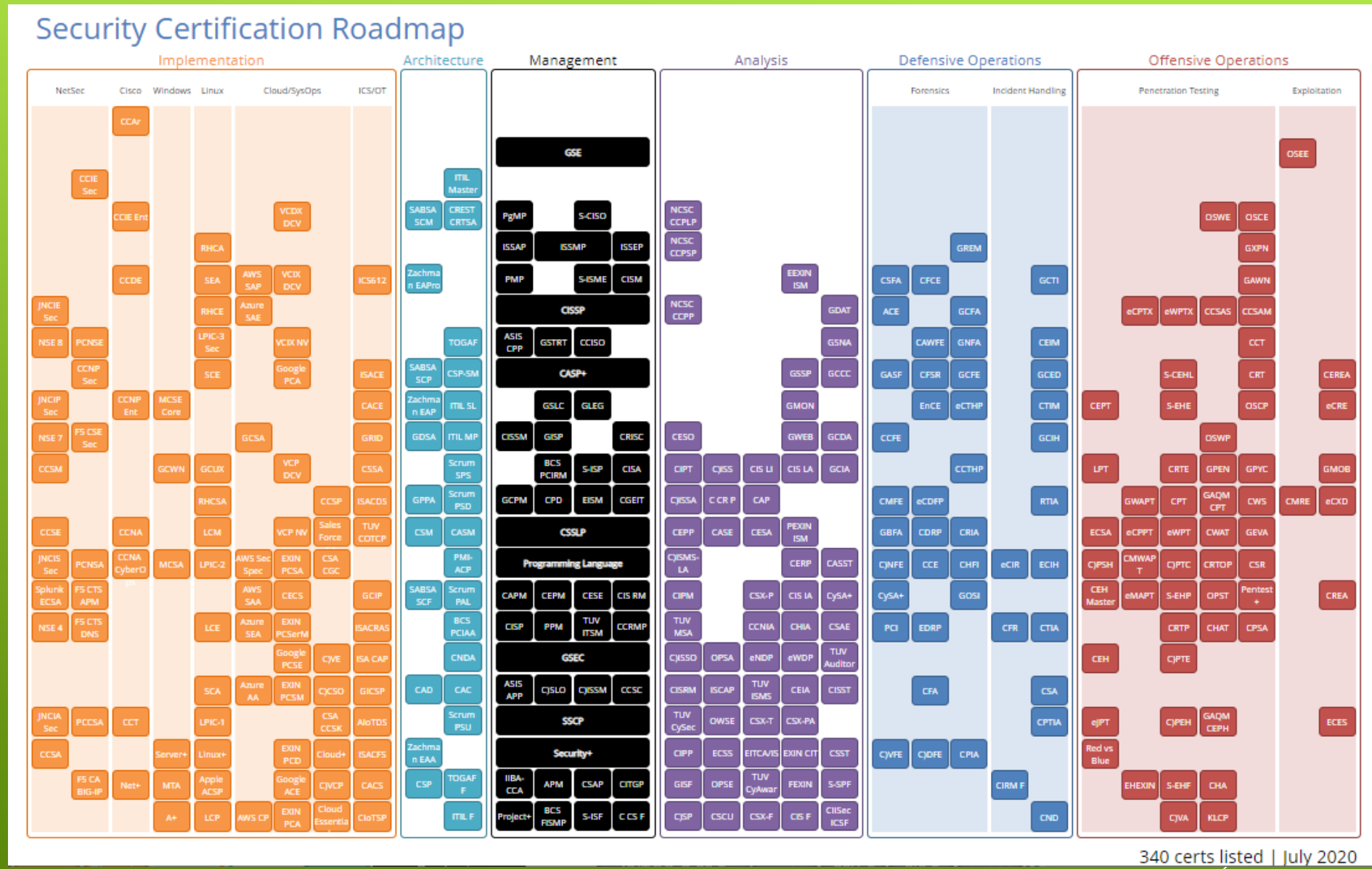
CompTIA

Certifications validate expertise in your chosen career.

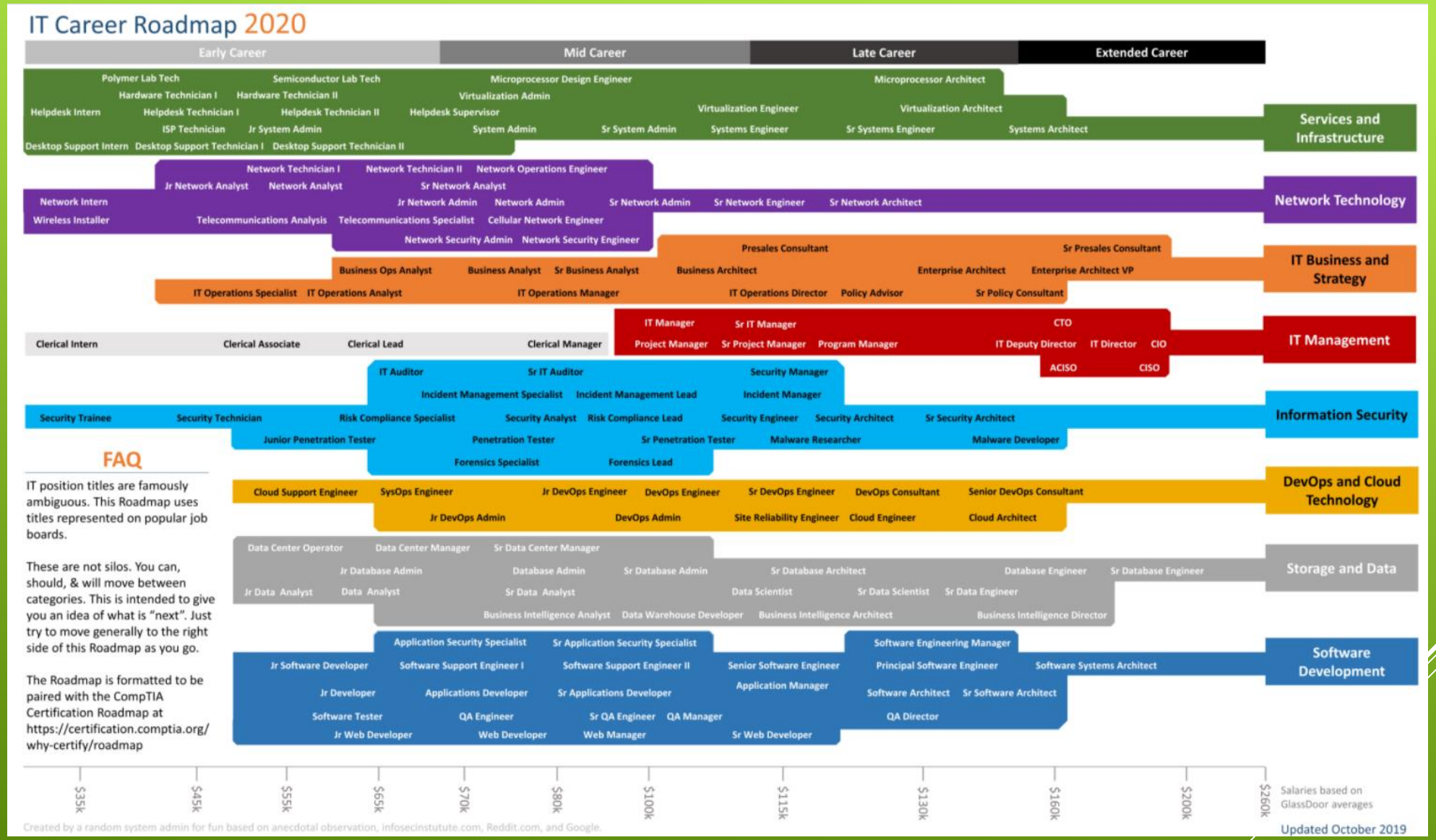


Computer literacy certifications validating end user skills include IC3 and ECDL/ICDL

Updated 9/2019



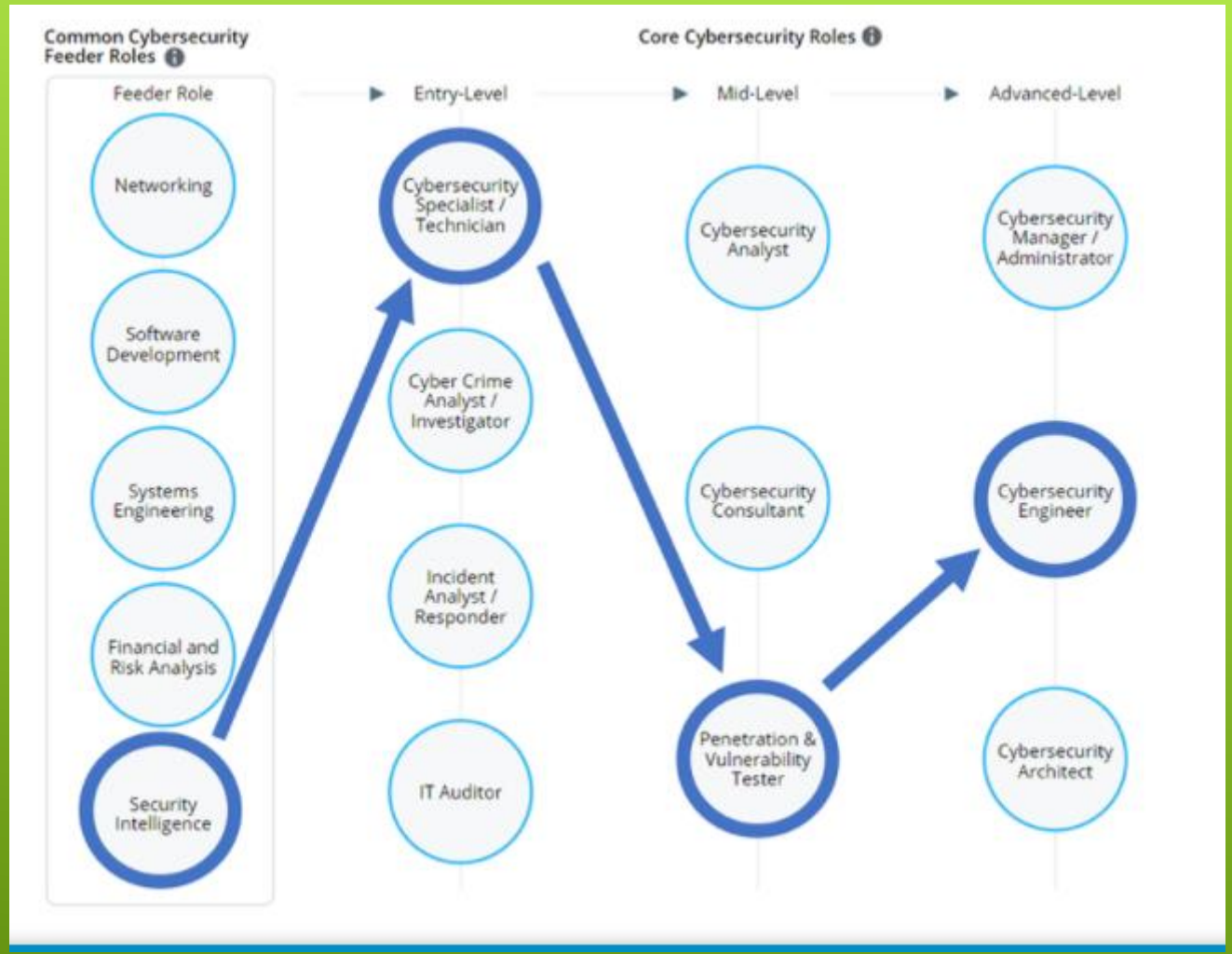
https://pauljerimy.com/security-certification-roadmap/



https://pauljerimy.com/wp-content/uploads/2020/03/IT_CareerRoadmap2020smol.png

STUDY PLAN

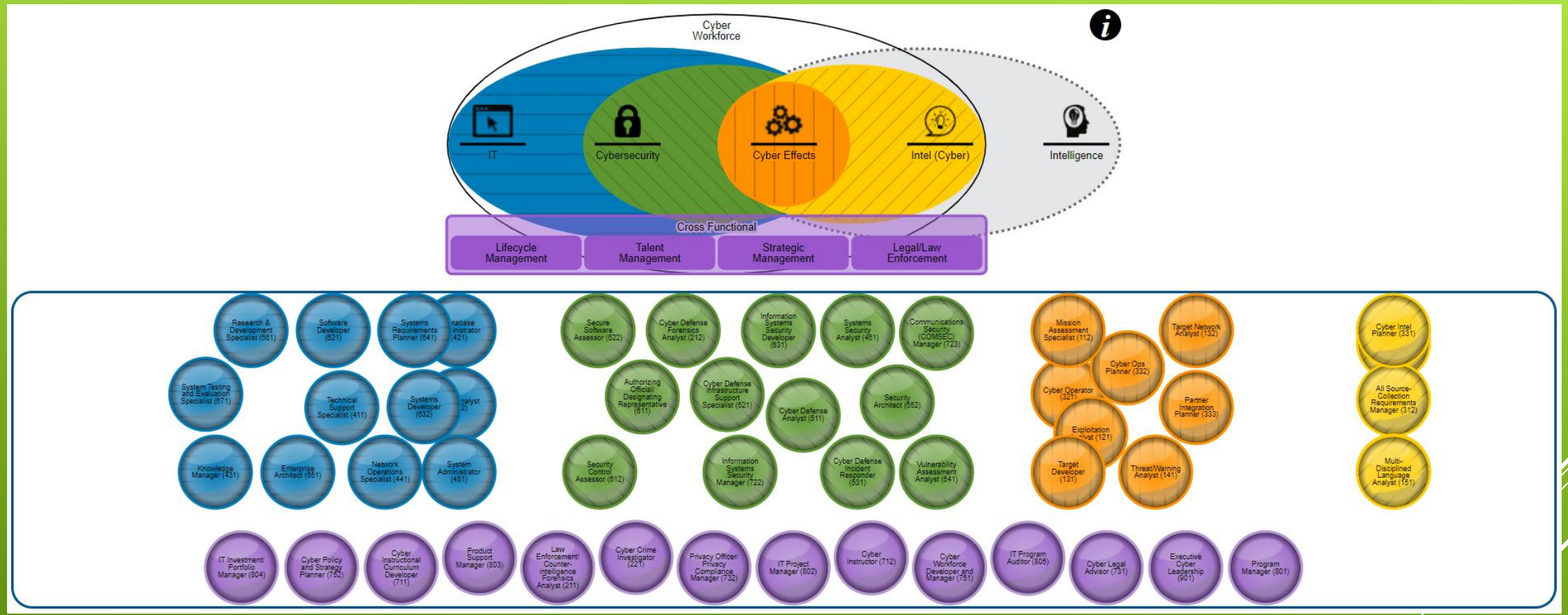
- U.S. Bureau of Labor Statistics
- Certification roadmaps
- Cyberseek
- NICCS
- 5 Year Plan
- Books
- And more (Podcasts, Webcasts, etc.)



https://www.cyberseek.org/

STUDY PLAN

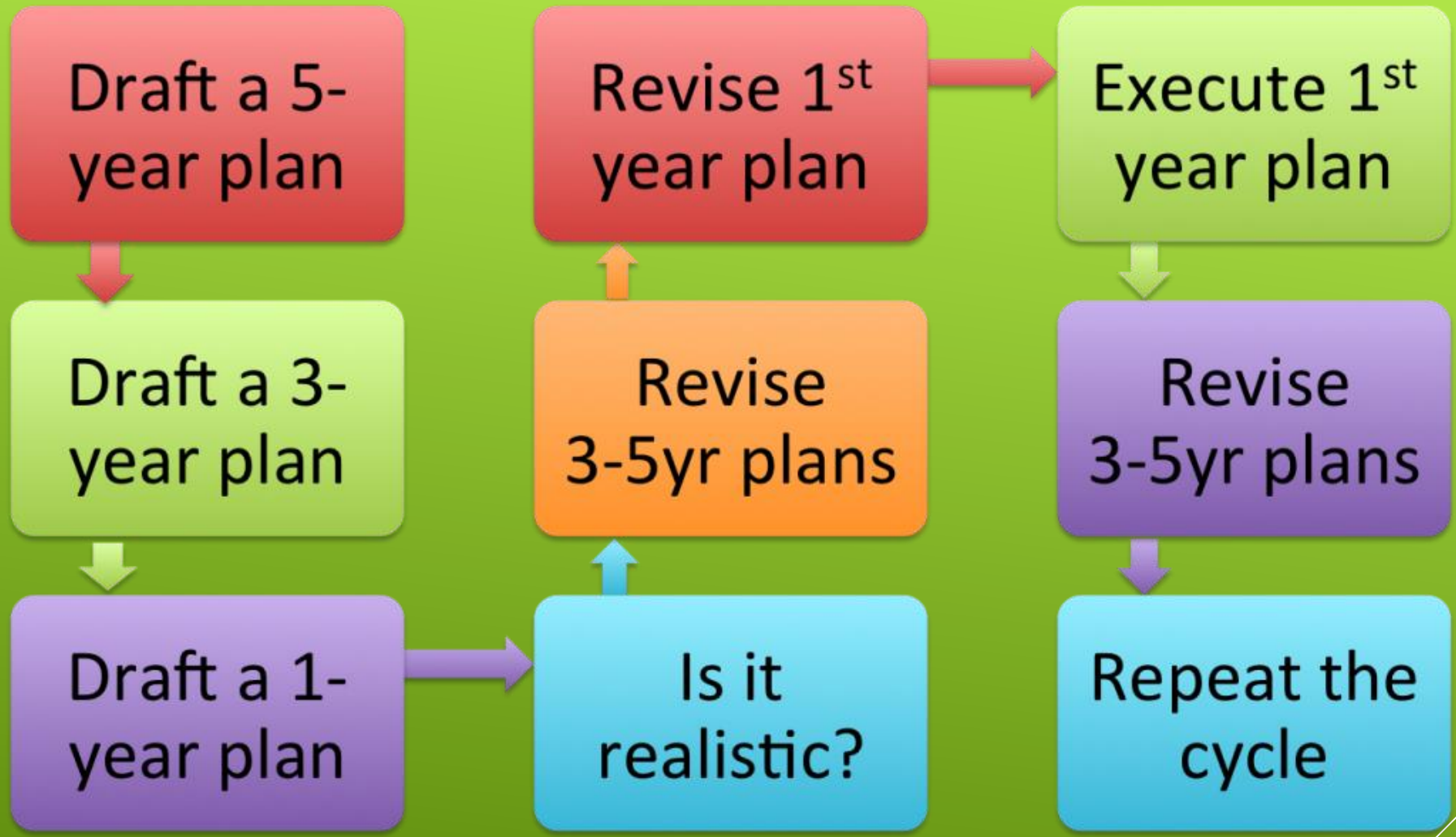
- U.S. Bureau of Labor Statistics
- Certification roadmaps
- Cyberseek
- NICCS
- 5 Year Plan
- Books
- And more (Podcasts, Webcasts, etc.)



https://niccs.us-cert.gov/workforce-development/cyber-career-pathways

STUDY PLAN

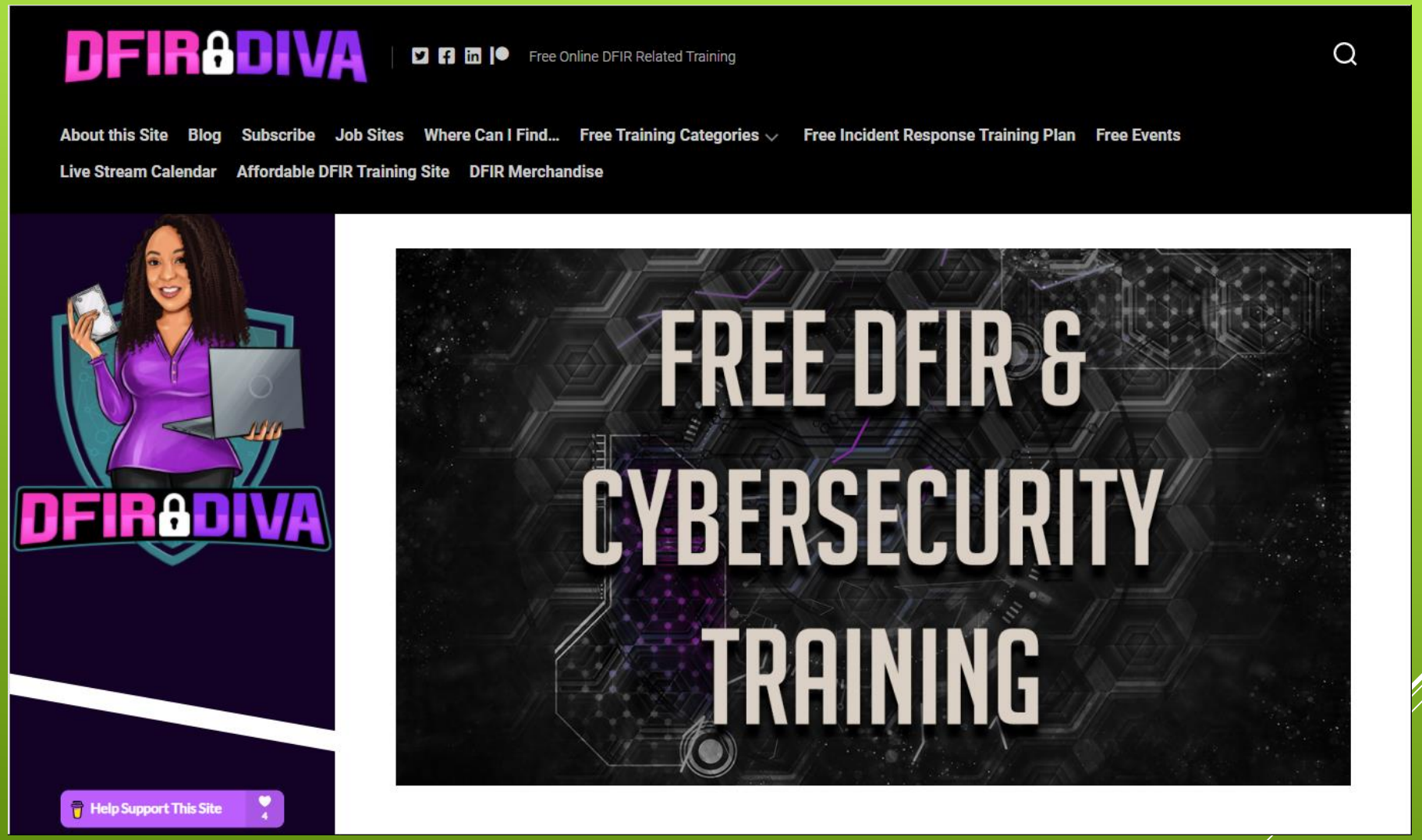
- U.S. Bureau of Labor Statistics
- Certification roadmaps
- Cyberseek
- NICCS
- 5 Year Plan
- Books
- And more (Podcasts, Webcasts, etc.)



https://thinkocrats.net/holistic-life-plans/

STUDY PLAN

- U.S. Bureau of Labor Statistics
- Certification roadmaps
- Cyberseek
- NICCS
- 5 Year Plan
- Books
- And more (Podcasts, Webcasts, etc.)



https://freetraining.dfirdiva.com/

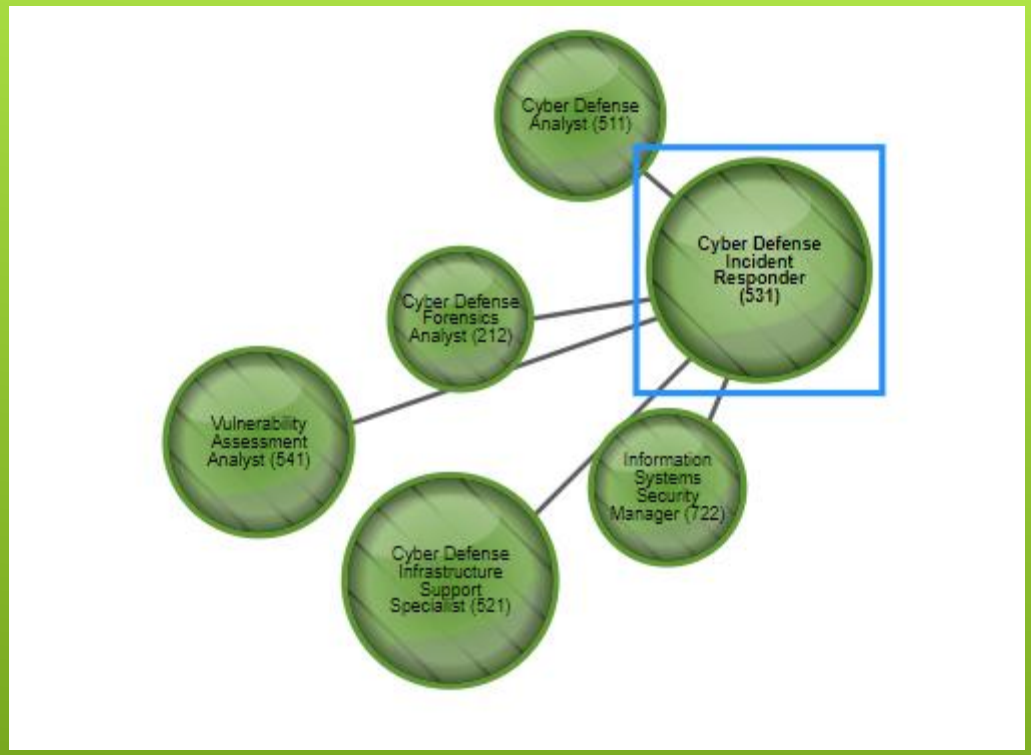
README.md

An awesome list of resources for training, conferences, speaking, labs, reading, etc that are **free** all the time that cybersecurity professionals with downtime can take advantage of to improve their skills and marketability to come out on the other side ready to rock. Drop me a subscribe on YouTube and lets connect more: https://www.youtube.com/c/GeraldAuger

CATEGORIES

1. Conferences
2. Instructor Led Webinar/Labs/Workshops
3. Training
4. Books
5. College Courses (Multi-week w/Enrollment)
6. Podcasts
7. YouTube Channels
8. News
9. Professional Networking / (Virtual) Meetups (Discord/Slack Groups)
10. References / Tools / Cheat Sheets

https://github.com/gerryguy311/Free_CyberSecurity_Professional_Development_Resources



EXAMPLE: CYBER DEFENSE INCIDENT RESPONDER

Details | Tasks | Knowledge | Skills | Abilities | Capability Indicators

Cyber Defense Incident Responder

Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.

Community: Cybersecurity

Category: Protect and Defend

Specialty Area: Incident Response

OPM ID: 531

Top 5 roles related by shared tasks, knowledge, skills and abilities:

- Cyber Defense Infrastructure Support Specialist (29.73%)
- Vulnerability Assessment Analyst (22.64%)
- Cyber Defense Analyst (16.81%)
- Information Systems Security Manager (13.21%)
- Cyber Defense Forensics Analyst (9.8%)

Details | **Tasks** | Knowledge | Skills | Abilities | Capability Indicators

Legend

C - Core Tasks A - Additional Tasks A* - Not included in the initial analysis to determine whether it is Core or Additional to the work role.

C	**T0041**	Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents.
A	**T0047**	Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.
A	**T0161**	Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security.
A	**T0163**	Perform cyber defense incident triage, to include determining scope, urgency, and potential impact, identifying the specific vulnerability, and making recommendations that enable expeditious remediation.
C	**T0164**	Perform cyber defense trend analysis and reporting.
C	**T0170**	Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems.
A	**T0175**	Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs)

Details | Tasks | **Knowledge** | Skills | Abilities | Capability Indicators

Legend

C - Core Knowledge

A - Additional Knowledge

A* - Not included in the initial analysis to determine whether it is Core or Additional to the work role.

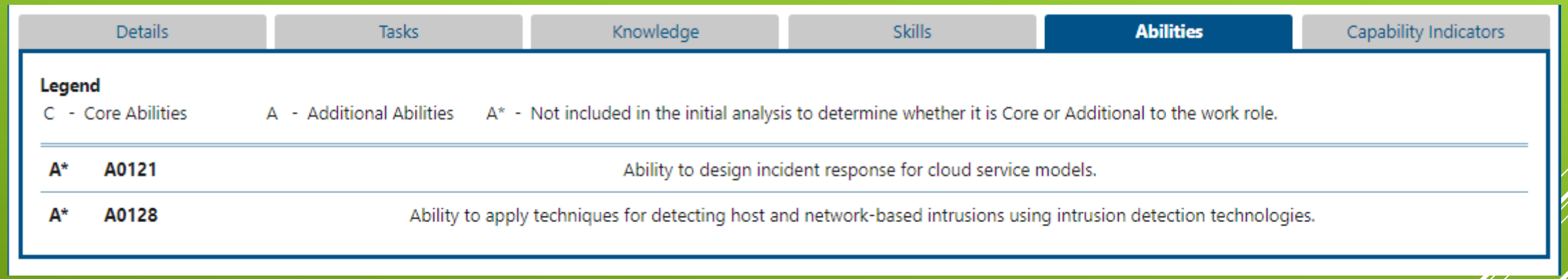
C	**K0001**	Knowledge of computer networking concepts and protocols, and network security methodologies.
C	**K0002**	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
C	**K0003**	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
C	**K0004**	Knowledge of cybersecurity and privacy principles.
C	**K0005**	Knowledge of cyber threats and vulnerabilities.
C	**K0006**	Knowledge of specific operational impacts of cybersecurity lapses.
A	**K0021**	Knowledge of data backup and recovery.
C	**K0026**	Knowledge of business continuity and disaster recovery continuity of operations plans.

Details | Tasks | Knowledge | **Skills** | Abilities | Capability Indicators

Legend

C - Core Skills A - Additional Skills A* - Not included in the initial analysis to determine whether it is Core or Additional to the work role.

C	**S0003**	Skill of identifying, capturing, containing, and reporting malware.
C	**S0047**	Skill in preserving evidence integrity according to standard operating procedures or national standards.
C	**S0077**	Skill in securing network communications.
C	**S0078**	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.
C	**S0079**	Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).
C	**S0080**	Skill in performing damage assessments.
C	**S0173**	Skill in using security event correlation tools.
A*	**S0365**	Skill to design incident response for cloud service models.



Details | Tasks | Knowledge | Skills | **Abilities** | Capability Indicators

Legend

C - Core Abilities A - Additional Abilities A* - Not included in the initial analysis to determine whether it is Core or Additional to the work role.

A*	**A0121**	Ability to design incident response for cloud service models.
A*	**A0128**	Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.

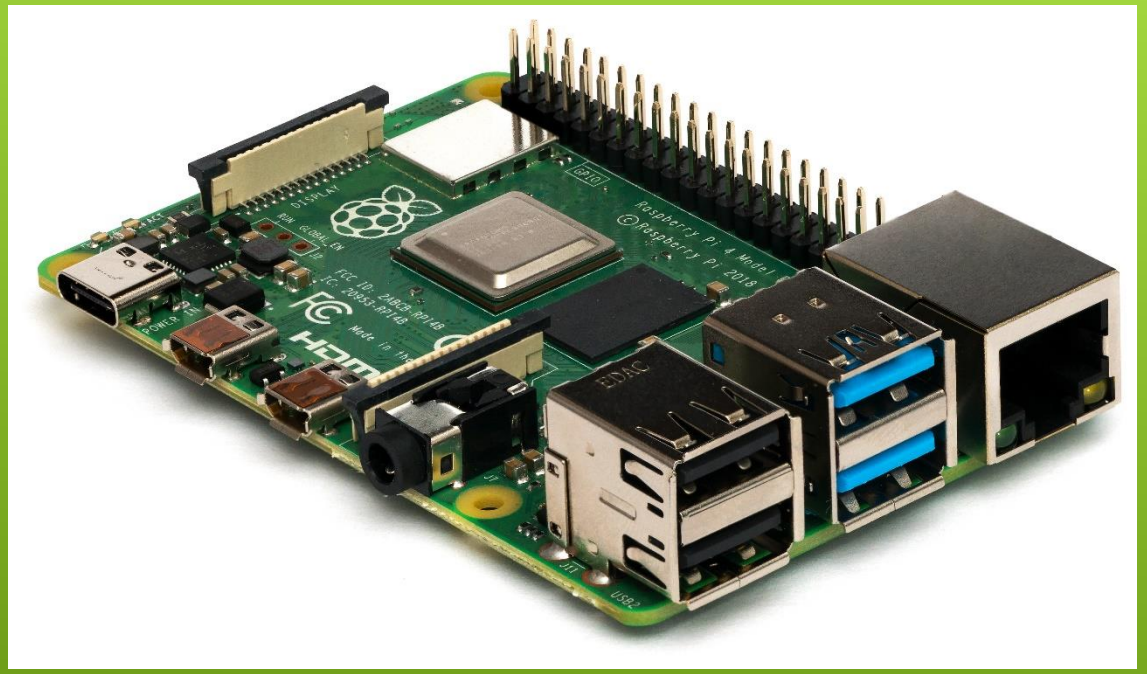
EXAMPLE: CYBER DEFENSE INCIDENT RESPONDER

Details | Tasks | Knowledge | Skills | Abilities | **Capability Indicators**

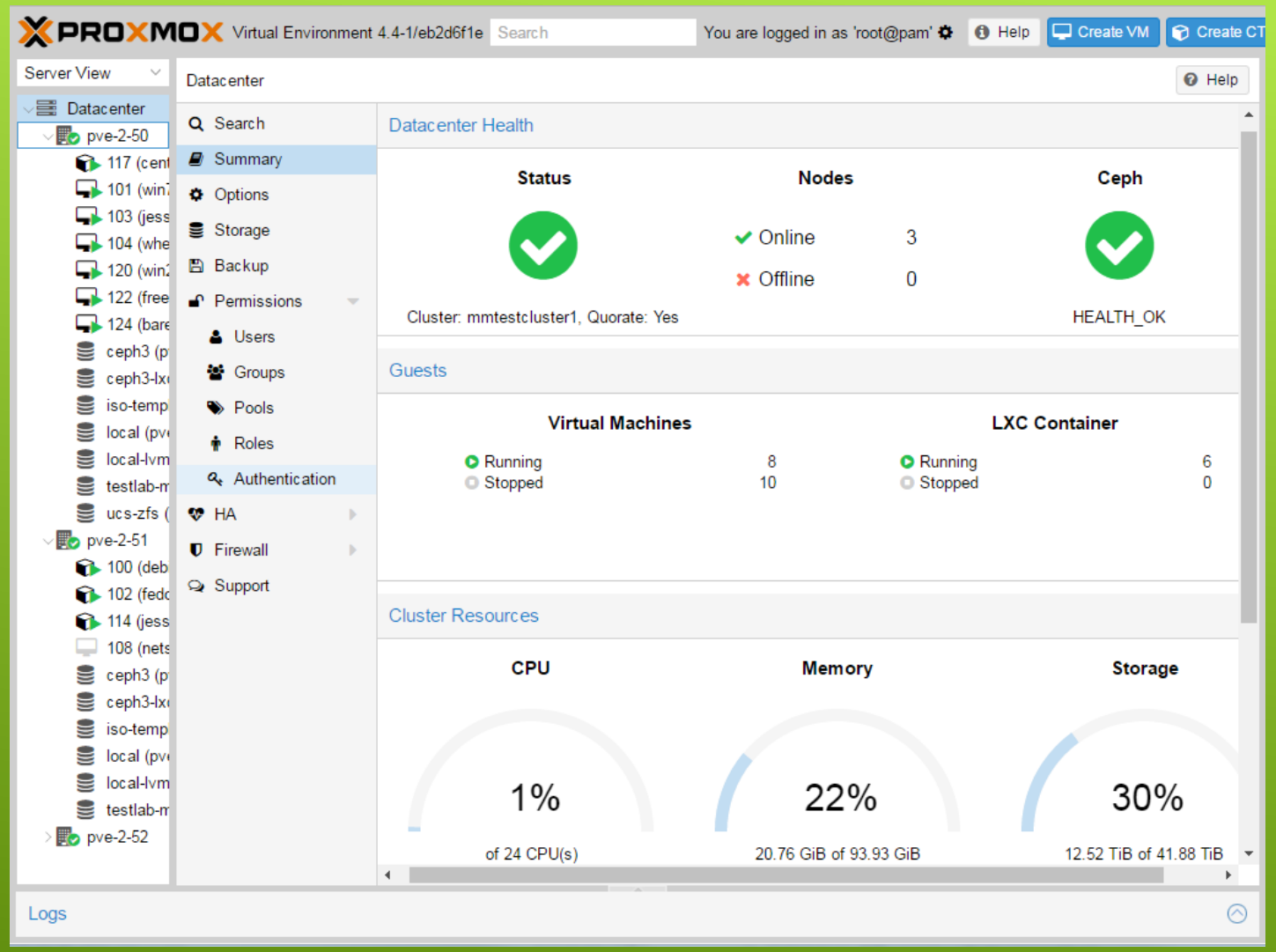
	Entry	Intermediate	Advanced
Credentials/Certifications	**Recommended:** Yes **Example Types:** N/A **Example Topics:** Certifications addressing new attack vectors (emphasis on cloud computing technology, mobile platforms and tablet computers), new vulnerabilities, existing threats to operating environments, advanced IDS concepts, applications protocols, concepts of TCP/IP and the link layer, DNS, fragmentation, IDS fundamentals and initial deployment (e.g., snort, bro), IDS rules (e.g., snort, bro), IPv6, network architecture and event correlation, network traffic analysis and forensics, packet engineering, silk and other traffic analysis tools, TCP, Tcpdump filters, UDP and ICMP, Wireshark fundamentals	**Recommended:** Yes **Example Types:** N/A **Example Topics:** Certifications addressing incident handling (identification, overview and preparation) buffer overflow, client attacks, covering tacks (networks, systems), denial of service attaches, network attacks, password attacks, reconnaissance, scanning (discovery and mapping, techniques, and defense), session hijacking and cache poisoning, techniques for maintaining access, web applications attacks, worms, bots, and bot-nets	**Recommended:** Yes **Example Topics:** Certifications addressing identification of malicious system and user activity, incident response in an enterprise environment, incident response process and framework, timeline artifact analysis, timeline collection, timeline processing, volatile data collection, filesystem structure and analysis, artifact analysis
Continuous Learning	**Recommended:** Yes **Examples:** 40 hours annually (may include participation in annual security conferences)	**Recommended:** Yes **Examples:** 40 hours annually (may include participation in annual security conferences)	**Recommended:** Yes **Examples:** 40 hours annually (may include participation in annual security conferences)

- Networking
- System Administration
  - Linux
    - Raspberry Pi
  - Virtual Machines
    - Proxmox VE
    - VMWare
    - Virtual Box
  - CLOUD
    - Linode
    - AWS
    - Github
  - Windows

- Networking
- System Administration
  - Linux
    - Raspberry Pi
  - Virtual Machines
    - Proxmox VE
    - VMWare
    - Virtual Box
  - CLOUD
    - Linode
    - AWS
    - Github
  - Windows



https://projects.raspberrypi.org/en/projects

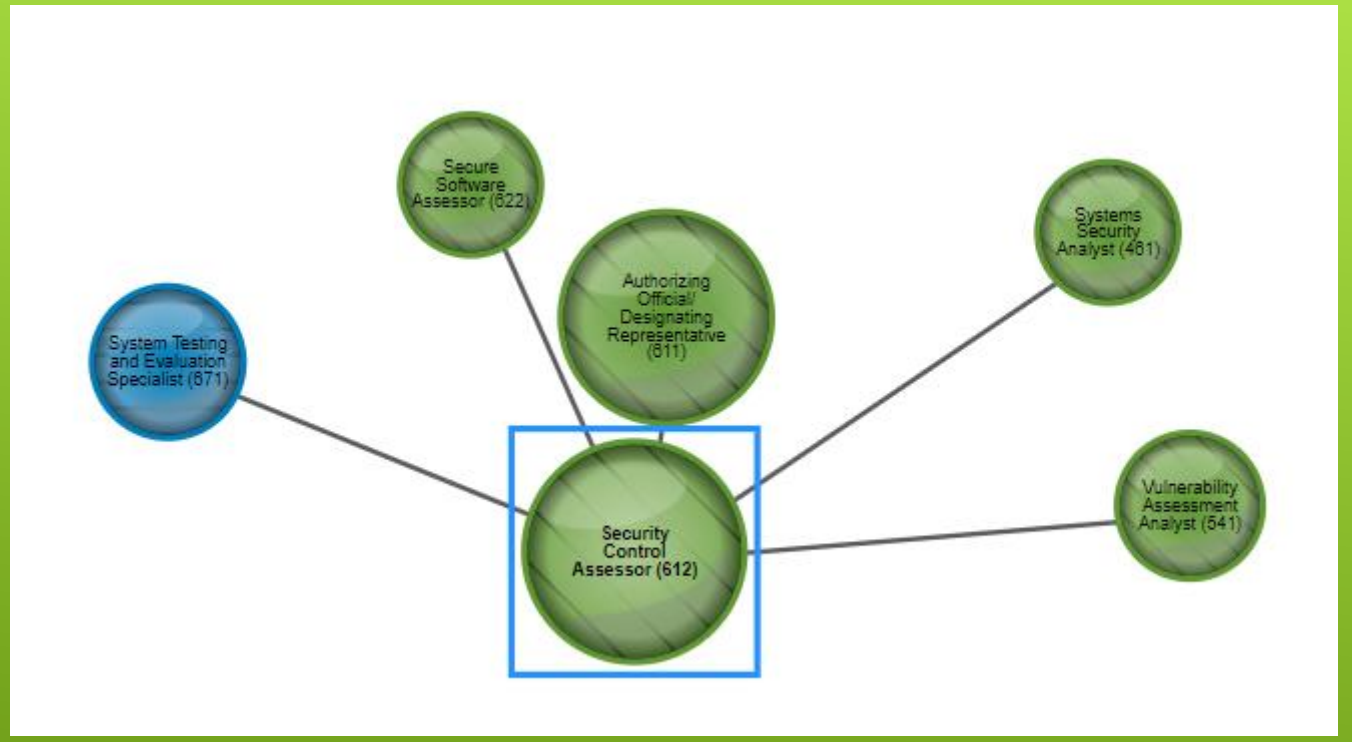


https://pve.proxmox.com/wiki/Main_Page

- Networking
- System Administration
  - Linux
    - Raspberry Pi
  - Virtual Machines
    - Proxmox VE
    - VMWare
    - Virtual Box
  - CLOUD
    - Linode
    - AWS
    - Github
  - Windows

https://blog.scottlogic.com/2019/07/03/getting-started-with-aws.html

- Networking
- System Administration
  - Linux
    - Raspberry Pi
  - Virtual Machines
    - Proxmox VE
    - VMWare
    - Virtual Box
  - CLOUD
    - Linode
    - AWS
    - Github
  - Windows



EXAMPLE: SECURITY CONTROL ASSESSOR

Details | Tasks | Knowledge | Skills | Abilities | Capability Indicators

Security Control Assessor

Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).

Community: Cybersecurity

Category: Securely Provision

Specialty Area: Risk Management

OPM ID: 612

Top 5 roles related by shared tasks, knowledge, skills and abilities:

- Authorizing Official/Designating Representative (92%)
- System Testing and Evaluation Specialist (40.74%)
- Vulnerability Assessment Analyst (35.85%)
- Systems Security Analyst (31.71%)
- Secure Software Assessor (31.58%)

Details | **Tasks** | Knowledge | Skills | Abilities | Capability Indicators

Legend

C - Core Tasks A - Additional Tasks A* - Not included in the initial analysis to determine whether it is Core or Additional to the work role.

A*	**T0145**	Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2).
A*	**T0177**	Perform security reviews, identify gaps in security architecture, and develop a security risk management plan.
A*	**T0178**	Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy.
A*	**T0181**	Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.
A	**T0184**	Plan and conduct security authorization reviews and assurance case development for initial installation of systems and networks.
A*	**T0205**	Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).
A	**T0221**	Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.
A*	**T0243**	Verify and update security documentation reflecting the application/system security design features.

Details | Tasks | **Knowledge** | Skills | Abilities | Capability Indicators

Legend

C - Core Knowledge

A - Additional Knowledge

A* - Not included in the initial analysis to determine whether it is Core or Additional to the work role.

C	**K0001**	Knowledge of computer networking concepts and protocols, and network security methodologies.
C	**K0002**	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
C	**K0003**	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
C	**K0004**	Knowledge of cybersecurity and privacy principles.
C	**K0005**	Knowledge of cyber threats and vulnerabilities.
C	**K0006**	Knowledge of specific operational impacts of cybersecurity lapses.
A*	**K0007**	Knowledge of authentication, authorization, and access control methods.
A*	**K0008**	Knowledge of applicable business processes and operations of customer organizations.

Details | Tasks | Knowledge | **Skills** | Abilities | Capability Indicators

Legend

C - Core Skills A - Additional Skills A* - Not included in the initial analysis to determine whether it is Core or Additional to the work role.

A	**S0001**	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.
A	**S0006**	Skill in applying confidentiality, integrity, and availability principles.
C	**S0027**	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.
C	**S0034**	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.
A	**S0038**	Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance, relative to the goals of the system.
A*	**S0073**	Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.).
A*	**S0078**	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.
A*	**S0097**	Skill in applying security controls.

Details | Tasks | Knowledge | Skills | **Abilities** | Capability Indicators

Legend

C - Core Abilities A - Additional Abilities A* - Not included in the initial analysis to determine whether it is Core or Additional to the work role.

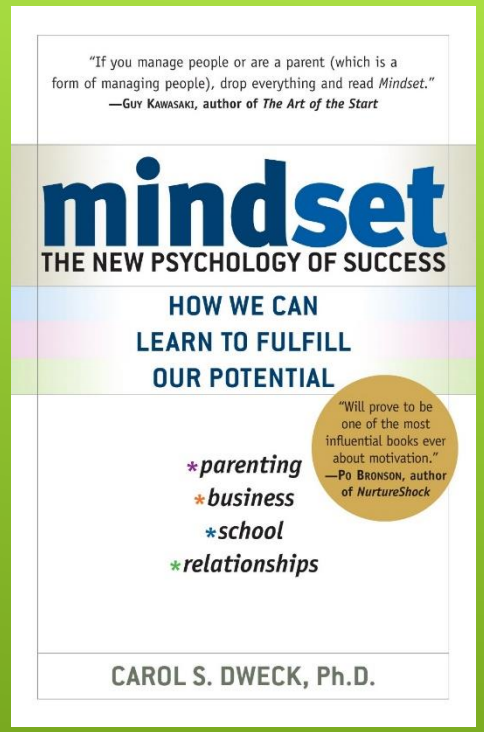
A*	**A0001**	Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.
A*	**A0011**	Ability to answer questions in a clear and concise manner.
A*	**A0012**	Ability to ask clarifying questions.
A*	**A0013**	Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.
A*	**A0014**	Ability to communicate effectively when writing.
A*	**A0015**	Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.
A*	**A0016**	Ability to facilitate small group discussions.
A*	**A0018**	Ability to prepare and present briefings.

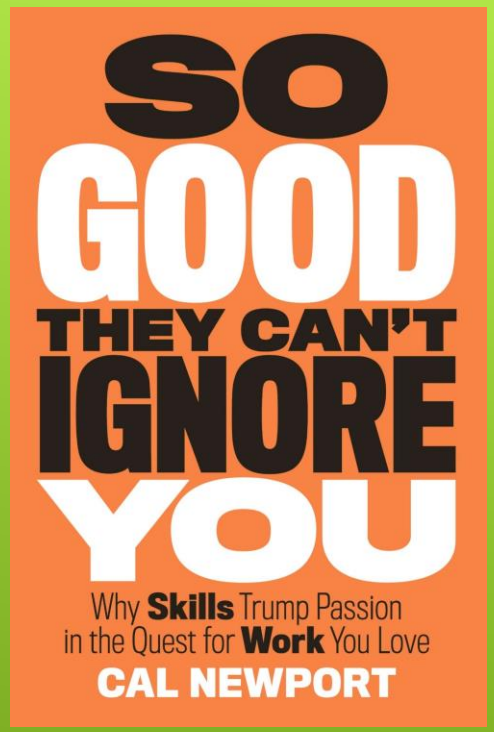
Details | Tasks | Knowledge | Skills | Abilities | **Capability Indicators**

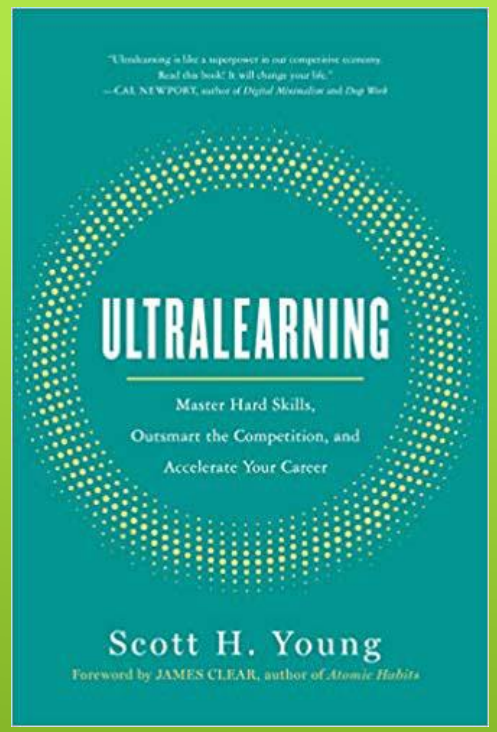
	Entry	Intermediate	Advanced
Credentials/Certifications	**Recommended:** Yes **Example Types:** N/A **Example Topics:** Certifications that address managing, maintaining, troubleshooting, installing, configuring basic network infrastructure, mobile device integration, hardware evaluation, operating systems, technical support, authentication, security testing, intrusion detection/prevention, incident response and recovery, attacks and countermeasures, and cryptography	**Recommended:** Yes **Example Types:** N/A **Example Topics:** Certifications that address network types, network media, switching fundamentals, TCP/IP, IP addressing and routing, WAN technologies, operating and configuring IOS devices, managing network environments, risk management, categorization of information systems, selection of security controls, security control implementation and assessment, information system authorization, monitoring of security controls, system security, network infrastructure, access control, cryptography, and organizational security	**Recommended:** Yes **Example Topics:** Certifications that address security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, incident management, integration of computing/ communications/business disciplines and enterprise components, change management/incident handling for managers, common attacks and malware, security policy, disaster recovery and contingency planning, total cost of ownership, physical security and facility safety, privacy and web security, risk and ethics, protecting intellectual property, network infrastructure, quality and growth of the security organization, wireless security, network and endpoint security technologies, network protocols for managers, project management, managing the mission
Continuous Learning	**Recommended:** Yes **Examples:** 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)	**Recommended:** Yes **Examples:** 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)	**Recommended:** Yes **Examples:** 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)

FIND YOUR VOICE

- Build a Home Lab
- Use a cloud hosted server
- Work with a nonprofit business
- Be active in a community
- Ask questions
- Synthesize Concepts
- Mentor







SUGGESTED READING


YOU DESERVE
TO BE HERE
CHANGE MY MIND
imgflip.com

YOU BELONG AT THE TABLE:

Finding your voice in cybersecurity

https://github.com/S1lv3rL10n/Talks