CISSP: Not Just for Squares

DMITRIY BERYOZA

OWASP Ottawa, October 2021

About me

Dmitriy Beryoza

@0xd13a on Discord/Twitter

https://www.linkedin.com/in/beryozad

VECTRA®
SECURITY THAT THINKS

- Senior Security Researcher at *Vectra AI*
- Prior to that - Pentester/Secure Software Development Advocate with X-Force Ethical Hacking Team at *IBM Security*
- 25+ years in software design and development
- Ph.D. in Computer Science, OSCP, CISSP, CCSP, CEH
- Presented at BSides LV, HackFest, Global AppSec, BSides Ottawa, and others
- *Interests*: reverse engineering, binary exploitation, secure software development, and CTFs

Agenda

- What is CISSP?
- Requirements, CBK domains, costs, test prep
- Who is CISSP for? Is it right for red-teamers?
- 4 reasons for pursuing CISSP

Disclaimer

- This is not a promotional talk for CISSP, $(ISC)^2$ did not sponsor me
  - …although I will consider offers ;-)
- I advocate not for CISSP specifically, but rather for the body of knowledge that this certification represents
- Views expressed here represent my subjective opinions, YMMV

What is CISSP?

- ***Certified Information Systems Security Professional***
  - Comprehensive coverage of various InfoSec domains
- Established in 1994 (!)
- Granted by $(ISC)^2$ - *International Information System Security Certification Consortium, Inc.*
- Accredited by ANSI ISO; approved by DoD; NSA baseline
- ~150K certification holders globally (~6500 in Canada)

Test Requirements

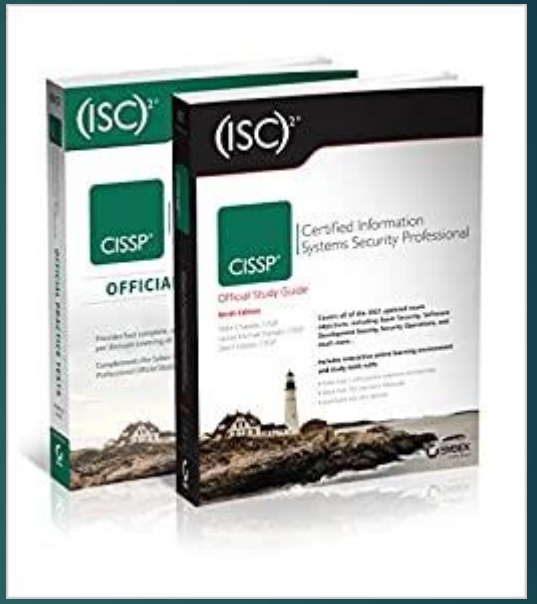
- Work experience:
  - 5 years of work in two or more of the CISSP *domains* (described later)
    - A bit of a Catch-22 - may be hard to be hired without certification
  - College degree or some other certs count for 1 year
  - Can get "Associate" certification without work experience (and then work to gain the experience)
- Accept Code of Ethics canons:
  - *Protect society, the common good, necessary public trust and confidence, and the infrastructure.*
  - *Act honorably, honestly, justly, responsibly, and legally.*
  - *Provide diligent and competent service to principals.*
  - *Advance and protect the profession.*

Test Requirements (cont.)

- Answer questions about your background
  - Separate question about blackhat activities
- Get endorsed by another CISSP holder

- Costs:
  - Currently - US$749 (employers may help cover)
  - Retake - full cost
- Maintenance:
  - Annual fee of US$125 (employers may help cover that too)
  - Earn Continuing Professional Education (CPE) credits (120 in 3 years)

Test Prep



- Buy a study guide (employer may reimburse you)
- Take several months to study
  - Material is massive - Official Study Guide is 1000+ pages long

- You could:
  - Study on your own
  - Join a study group
  - Take a prep course
  - Wing it (not recommended - even if you know everything about security)

- Do multiple tests (online tests available with some guides)
- There are cheat sheets available - great for refreshing your memory before exam

On Test Date

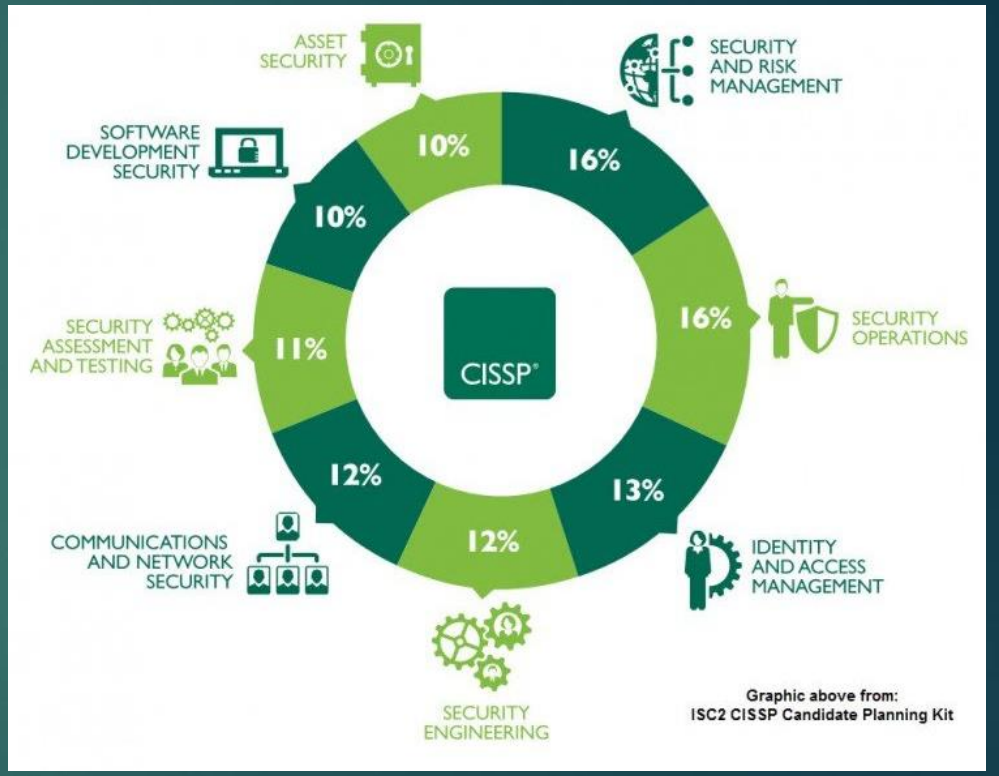
- Tests conducted by Pearson VUE (3 locations in Ottawa)
- Tight security - you will be asked to show your pockets, glasses, etc.
  - Lockers provided for your belongings
- 3 hours, 125 questions (100 of them count)
- 70% passing score
- Only given pass/fail, exact score unknown
- Results may be held up for a period of time for auditing

Questions

- Computer-based, multiple choice
- Multiple flavors:
  - Simple questions
  - Match pairs
  - Scenario with multiple associated questions
  - Some calculations may be required
- Questions could be harder than what is in the official test prep guide

Common Body of Knowledge

- Domain 1. Security and Risk Management
- Domain 2. Asset Security
- Domain 3. Security Architecture and Engineering
- Domain 4. Communication and Network Security
- Domain 5. Identity and Access Management (IAM)
- Domain 6. Security Assessment and Testing
- Domain 7. Security Operations
- Domain 8. Software Development Security



Common Body of Knowledge (cont.)

- Domain 1. Security and Risk Management
  - General concepts in information security; security governance; compliance; legal/regulatory; investigations; BC/BIA; security policies; risk management; supply chains; threat modeling; security education, training, and awareness
- Domain 2. Asset Security
  - Collection, storage, maintenance, retention and destruction of data; roles in data handling (owner, controller and custodian); data protection methods/states; resource provisioning; asset classification; data lifecycle management
- Domain 3. Security Architecture and Engineering
  - Security engineering plans, designs and principles; security models and architectures in access control; cryptography + attacks; ICS/cloud/IoT/containers/microservices/virtual; site and facility design and security controls

Common Body of Knowledge (cont.)

- Domain 4. Communication and Network Security
  - Secure communication channels and networks; secure protocols; OSI; IP networking; converged protocols (e.g. VoIP); micro-segmentation (e.g. SDN); cellular/wireless/CDN networks
- Domain 5. Identity and Access Management (IAM)
  - Physical/logical controls; identification and authentication (IdM, MFA, SSO); federation; authorization (RBAC/DAC/MAC/…); ID and access provisioning lifecycle; authentication systems (OIDC/OAuth/SAML/Kerberos/…)
- Domain 6. Security Assessment and Testing
  - Assessment, test, audit strategies; vulnerability testing; pentests attacks simulations; collection of security process data; DR/BC; analyze test output; conduct/validate audits

Common Body of Knowledge (cont.)

- Domain 7. Security Operations
  - Security investigations/forensics; logging/monitoring (SIEM/threat intel/UEBA/…); configuration management; security operations; incident management; detective/preventive measures (IDS/IPS/sandboxing/honeypots/…); patch and vuln management; change management; recovery strategies; DR; DRP testing; BC; physical security; personnel safety
- Domain 8. Software Development Security
  - SDLC; maturity models (CMM/SAMM); SD ecosystems (tools, CI/CD, security testing - SAST/DAST); supply chain security; managed services; secure software development

Do You Need This Certification?

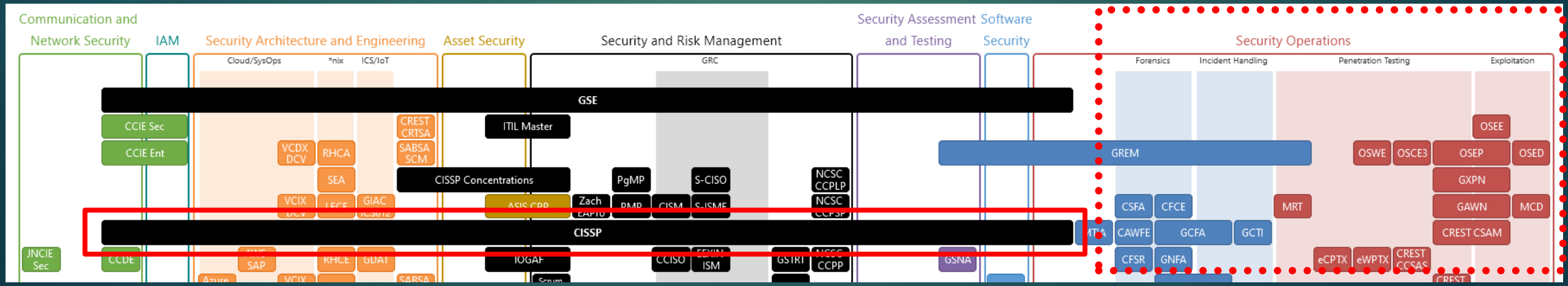
- Overall this is a big undertaking
  - Expensive, takes a long time, you have to pass a tough exam
- So the most important question is:
  - *Is this certification right for you?*
- Judging by CBK content it is more appropriate for certain specific roles in security

Who is CISSP For?

- According to CISSP:

• Chief Information Security Officer	• Security Systems Engineer	• Security Architect
• Chief Information Officer	• Security Analyst	• Security Consultant
• Director of Security	• Security Manager	• Network Architect
• IT Director/Manager	• Security Auditor	

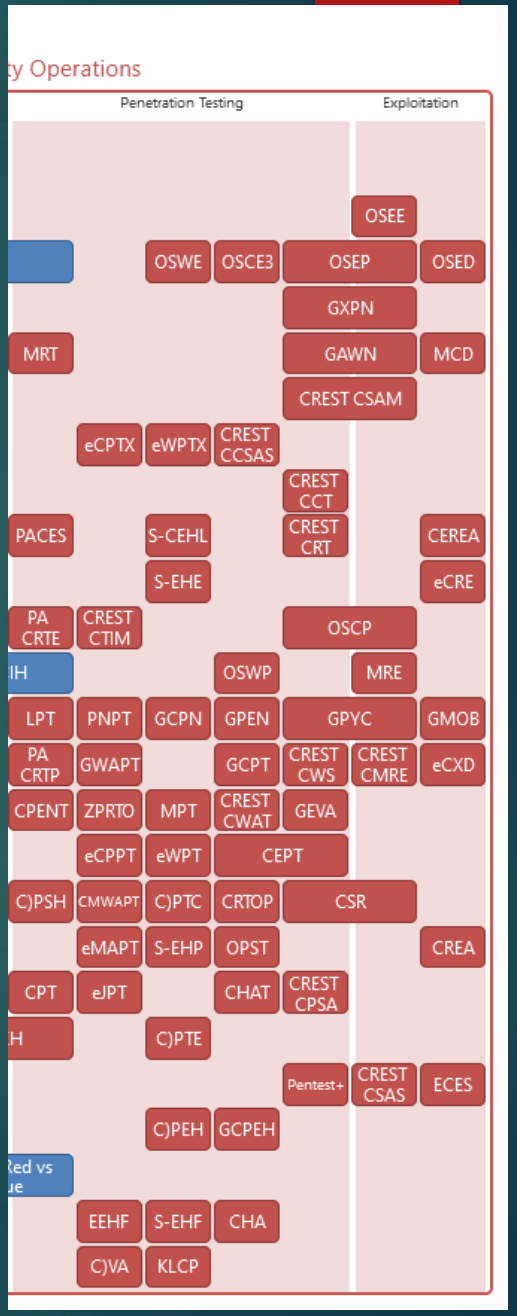
- Primarily geared towards:
  - Blue teams - SecSDLC - Management - Consulting



(Source: https://pauljerimy.com/security-certification-roadmap/)

Who is CISSP For? (cont.)

- It seems that CISSP is not for offensive side
  - I heard that opinion expressed more than once
  - There are many topics in the CBK that just don't apply:
    - Legislation and regulations
    - Risk management and analysis
    - Admin controls
    - BC/DR
    - Evidence collection
    - Datacenter setup
    - DLP
- There are more appropriate certs for "breakers":
  - Offensive Security
  - Some GIAC
  - CREST
  - eLearnSecurity



Who is CISSP For? (cont.)

- My interests are in that camp:
  - Red-teaming
  - Pentesting
  - Exploit development
- I just want to break stuff ☺
- My big dilemma was - is the exercise of this magnitude actually worth it?
- But after studying the exam outline and thinking about the big picture I decided to pursue it
- Here are my reasons…

Reason #1 - Fill Your Knowledge Gaps

- Thought experiment - if you work in cyber security, take an inventory of your colleagues' education backgrounds
- Here's mine:
  - Computer Science
  - Quality Assurance
  - Information Technology
  - Customer Support
- Even some exotic ones:
  - Real Estate
  - Music
  - Drama
- Is something missing?
  - **Cyber Security**

Reason #1 - Fill Your Knowledge Gaps (cont.)

- Of course this is just one person's experience, but the trend is there
- Many cyber security practitioners did not study it formally
  - The field is too young
- Most of us learned on the job; reading books, articles and blogs; watching presentations…
- Absence of formal education is bound to leave gaps in your knowledge (that was my case)
- Gaps are dangerous, and may be contributing to ongoing cybersecurity disasters we are having…

Reason #1 - Fill Your Knowledge Gaps (cont.)

- I went to university in the '90s, Cyber Security was not a widely available track then
  - We had bits and pieces of it taught in Computer Science and InfoTech classes
- Situation is much better now
  - 70+ universities and colleges have cybersecurity programs in Canada *(Source: https://cyber.gc.ca/en/guidance/where-go-school)*
- If you don't have an option of going back to school, CISSP is comprehensive enough to be treated as a Security 101 course (and beyond)
  - UK NARIC (agency for recognition and comparison of credentials) recognized it at Level 7 - "*comparable to Masters degree standard*" *(Source: https://www.infosecurity-magazine.com/news/cissp-equal-masters-degree/, May 2020)*

Reason #1 - Fill Your Knowledge Gaps (cont.)

- Crazy idea:
  - Don't go through the CISSP CBK with the sole purpose of passing the exam
  - Consider going *slower* to thoroughly take in the material and make sense of how it all fits together
- I think it will give you a more complete "big picture" of security field
- And you will then be able to draw on that knowledge in all kinds of roles, whether you are and attacker or a defender

Reason #2 - Know Your "Opponent"

- If you are in the offensive camp you need to know how the systems that you are attacking were built
- I'm a big believer in:
  - *"You cannot exploit what you don't understand"*
- CISSP CBK describes industry guidelines most players are following
- Studying it will give you a better idea of what to expect in the environment you are attacking, and where the weak spots could be

Reason #2 - Know Your "Opponent" (cont.)

Knowledge of…	Will help you…
Investigative procedures	Hide your tracks in a red-team engagement
Data classification	Know what assets to go after during assessments
Authorization mechanisms	Find weak spots in specific method used in customer environment
SIEM/UEBA guidelines	Bypass monitoring
SecSDLC gudelines	Poison the supply chain
Datacenter setup guidelines and physical protections	Perform physical security testing

Reason #3 - Know Your Colleagues

- If you are in the offensive camp you may occasionally work alone:
  - Bounty hunter
  - Security researcher
- But most other times you will interact with others:
  - Coworkers
  - Managers
  - Customers
- Most of those people operate in "CISSP world"
  - Having similar knowledge will help you empathize, communicate in the same terms, be aware of their needs, requirements, and challenges

Reason #3 - Know Your Colleagues (cont.)

- Knowing legislation/regulation expectations you can both find the deficiencies in customer implementations and propose ways of mitigating that that will bring customers into compliance
- Knowing pentest policies and recommendations will help you conduct tests legally and without jeopardizing your customer environment
- Knowing your specific customer needs, and corresponding CISSP guidelines you can tailor your security assessment and recommend appropriate access control mechanisms in case of deficiencies

Reason #4 - Help Your Career

- *I would caution everyone not to make this the primary reason for getting certified*
  - *Acquiring knowledge and skills should trump mere career advancement*

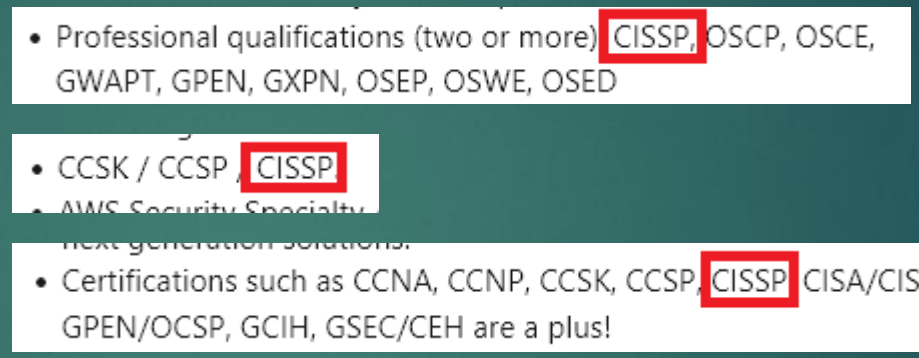
- CISSP is in highest demand across InfoSec job listings

(Source: https://www.coursera.org/articles/popular-cybersecurity-certifications , August 2021)

Certification	LinkedIn	Indeed	Simply Hired	Total
CISSP	48,711	13,499	9,333	71,543
CISA	12,466	6,138	3,859	22,463
CISM	8,860	4,064	2,806	15,730
Security+	5,371	3,583	2,698	11,652
CEH	5,894	2,401	1,697	9,992
GSEC	3,623	2,515	1,807	8,045

Reason #4 - Help Your Career (cont.)

- In demand even for red team jobs *(Source: LinkedIn job listings, October 2021)*
  - Ethical Hacker
  - Penetration Tester
  - Ethical Hacker



- CISSP may become more useful as your career progresses
  - Even if you are a red-teamer now you could move to consulting or management eventually

Reason #4 - Help Your Career (cont.)

- Among the top-paying IT certifications

(Source: https://www.globalknowledge.com/us-en/resources/resource-library/articles/top-paying-certifications/, August 2021)

Wrap-up

- CISSP is one of the longest running and most respected InfoSec cert
- Comprehensively covers information security field
- Not an easy undertaking: large CBK, difficult test preparation, tough exam, sizeable upfront and maintenance costs
- Geared more towards development, blue team and management roles
- Yet I believe it's useful for red teamers:
  - Fills in your knowledge gaps
  - Gives you better knowledge of your targets
  - Puts you on the same page with colleagues and clients
  - Helps advance your career

Q&A

@0xd13a on Discord/Twitter https://www.linkedin.com/in/beryozad

Slides can be found at https://github.com/0xd13a/presentations

Thank you!