

The Value of Cybersecurity Certifications

Alex Ivkin, CISSP, CISM





Who am I

CISSP since 2006, CISM from 2014, one of the authors of the ISACA CSXP certification.

Hiring manager in IT Security for many years, former cert junkie.

CompTIA Security+ Certified Professional, IBM Security Champion, IBM Certified Deployment Professional - Security QRadar SIEM, Security Access Manager for Web, Identity Manager, IBM Certified Advanced Deployment Professional, IBM Certified Solution Advisor - Security and Compliance Management Solutions, IBM Certified Advanced Deployment Professional - Security Management Solutions, IBM Certified Specialist - Identity Manager, IBM Certified System Administrator WebSphere Application Server, IBM InfoSphere Guardium Technical Professional, IBM DB2 UDB Database Administrator for Linux, Unix and Windows, HP OpenView Certification Program Accredited Integration Specialist (Network Services), HP Accredited Sales Consultant, Cisco Unified Communications for System Engineer, Oracle Certified Partner, Microsoft Certified Systems Engineer: Messaging, Microsoft Certified Systems Engineer: Security, Microsoft Certified Systems Administrator Messaging, Microsoft Certified Systems Administrator: Security, Microsoft Certified Professional



Agenda

Disclaimer

- This is my personal take from the practical standpoint.
- IT Security certs only, no IIA or IAPP CIPP
- All great views and opinions in this presentation are my own, everything else is not my own.

The talk

- What are the IT security certs?
- Which one do I get?
- What does it take to get one?



Security industry certifications

Non-profit



CISSP, CISSP-with-a-twist, other stuff no one knows with C, S and P in the name (CSSLP, CCSP, SSCP, CCFP)



CISA, CISM, CRISC, CGEIT

For-profit



An alphabet soup of over 20 different certs with four letters in the name

Go for the one with 3 letters (GSE), but brace for the ride.

Practical certifications



OSCP - Offensive Security Certified Professional



CSXF - CyberSecurity Fundamentals

CSXP - CyberSecurity Practitioner



GSE - GIAC Security Expert

ISACA CSX Cybersecurity Nexus



[MY PROFILE](#) [MY TRAINING](#) [MY LABS](#) [FAQS](#) [SIGN OUT](#)



MY PROFILE



MY TRAINING



MY LABS



EDIT ACCOUNT



FORUMS



SIGN OUT

CSX VOLUME 1

▶ Lost Web Server [LAUNCH CONTENT](#)

🔧 Finding the Lost Web Server (Beginner) [LAUNCH LAB](#)

Students will leverage network discovery and diagnostic capabilities to identify what happened to a corporate webserver which was severely damaged during an attack.

▶ Scanning [LAUNCH CONTENT](#)

🔧 Network Scanning (Beginner) [LAUNCH LAB](#)

Students will leverage network scanning tools to identify nodes and services on an internal network. The end goal is to create an up to date network map of their company's internal network for troubleshooting, analysis, and future reference.

▶ HTTP Packet Analysis [LAUNCH CONTENT](#)

🔧 HTTP Packet Analysis (Beginner) [LAUNCH LAB](#)

ISACA CSX Practitioner

The screenshot displays the ISACA CSX Practitioner interface. At the top, the CSX logo and navigation links (MY PROFILE, MY TRAINING, MY LABS, FAQs, SIGN OUT) are visible. The main area shows a virtual machine environment with a Kali Linux desktop. The desktop has a blue background with a white dragon logo. The taskbar on the left includes icons for applications like Firefox, Nautilus, and various system utilities. The top status bar of the VM shows 'Sat 13:08' and '59 Minutes Remaining'. On the right side, a sidebar titled 'Content' and 'Machines' lists tasks. The 'Tasks' section includes 'Part one: Copy and Confirm' with sub-tasks '1. Secure Copy' and '2. Check file integrity', and 'Part Two: Malware Analysis'. At the bottom, a 'Secure Copy' window is open, displaying instructions to copy files from a server to the current working directory. The server details are: Server: 192.168.4.2, Username: lt-backup, Password: isaca. A 'Done' button is present next to the instructions.

CSX
CYBERSECURITY NEXUS

17: Challenge 2: Challenge 2 Volume 1 (Advanced)

MY PROFILE MY TRAINING MY LABS FAQs SIGN OUT

Sat 13:08 59 Minutes Remaining

Applications Places

Eval8 malware

Content Machines

Exercise Summary

Tasks

- Part one: Copy and Confirm
 - 1. Secure Copy
 - 2. Check file integrity
- Part Two: Malware Analysis

Secure Copy

Utilizing `scp` copy the files: `/home/lt-backup/backup.bak` and `/home/lt-backup/backup.md5` to your current working directory.

Server: 192.168.4.2
Username: lt-backup
Password: isaca

Done

Task 1 of 5
Exercise 1, Task 1 of 2



Vendor certifications

Many big security vendors have them

- Cloud Security - AWS Certified Security
- Network Security - CCIE Security
- Host Security - MCSE Security, RHCS Security
- DB - Oracle DB Security Certified
- IBM, DELL/EMC/RSA - IBM Security Solution Advisor, RSA Security



Junk certifications

Nobody really cares about, except the companies pushing them*

- EC-Council - C|EH, CCISO and a ton
- Mile2 - C|PEH and other C)* stuff
- CompTIA - Security+

** Some may be included as prerequisites for vendor certifications*





Why certify

Career

- Up - most sr. level security positions now list CISSP for general and/or CISM/CISA/CRISC for more specific (director/auditor/analyst) roles
- Lateral movements - CISA, GIAC certs

Deep technical knowledge in IT Security

- OSCP, GSE (which requires 4-5 from the SANS portfolio), CSXP

Employer

- Vendor certs for channel status for resellers
- CISSP, CRISC, CGEIT for PS firms



Certified Information
Security Manager®
An ISACA® Certification





Pay out. Sort of.

Global Knowledge List

- CGEIT & AWS Certified Solution Architect - 1st&2nd - \$121k
- PMP & AWS Certified Developer - 3rd & 4th - \$114k
- CISSP & CRISK - 5&6th - \$111k
- CISM - 7th - \$108k
- MCSE & CISA - 12&13th \$100k



What do they cost

Money. Ask your employer to pay for it.

- CISSP - \$600-700 + \$85/yr + 40cpe/yr
- ISACA - \$500-600 + \$205/yr + 40cpe/yr
- OSCP - \$800-\$1150
- GIAC GSE - arm+leg

Time (you pay)

- CISSP - 2-6 months
- CISA, CISM - 2-6 months, CRISC, CGEIT - more
- OSCP - 6+ months
- GIAC GSE - years

CISSP and ISACA certs require 5 years of relevant infosec experience



How to train

Industry certs

- Books and official training materials
- Online trainings, Linkedin learning, Youtube etc
- SANS and ISACA CISSP Instructor led trainings.
 - Derek Hill <derek@dh-solutions.com> is teaching one soon with SANS

Practical exams

- Get the lab subscription for longer than you think you'll need it

Vendor certs

- Get braindumps



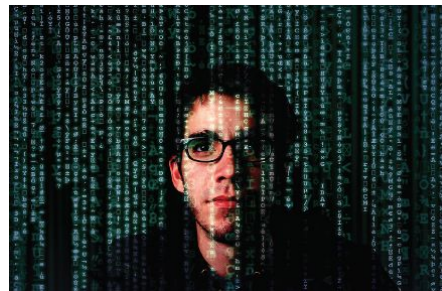
Conclusions

Serious about being in the industry - **CISSP**



Want to be an 31337 h4x0r - **OSCP**

Certification junkie - go **SANS!**



Thank you

Questions?

<https://securedmind.com>