

CSIS Academy

Be Better



Course overview

August 19, 2011

Indhold

1	The Courses	3
2	CSIS Security Analyst	4
2.1.1	Module 1: Threat assessment & Information gathering	4
2.1.2	Module 2: Attack techniques	5
2.1.3	Module 3: Identify and exploit vulnerabilities	5
2.1.4	Duration	5
2.1.5	Price	5
3	CSIS Forensic & Incident Response	6
3.1.1	Module 1: Detect & react	6
3.1.2	Module 2: Analyze file system, registry and memory	7
3.1.3	Module 3: Malware analysis	8
3.1.4	Duration	8
3.1.5	Price	8
4	CSIS Secure Web Programming	9
5	Instructors	10
6	Course facilities	11
7	Registration	11

1 The Courses

CSIS Academy offers three different courses, which can be taken independently:

- **CSIS Security Analyst**
- **CSIS Incident Response & Forensic**
- **CSIS Secure Web Programming**

After each course, the participant can take an exam. In case the participant passes all exams, he/she gets the title of 'CSIS Security Expert'.

The different courses are carefully selected based on the current threat assessment followed closely by CSIS in many years. Thus, the content is adapted to the threats faced by most companies.

CSIS has emphasized the following characteristics in the educational programs:

- Theory is fine, but practice is better
- Our instructors have a minimum of five years hands-on experience
- Course material includes completely up-to-date information

2 CSIS Security Analyst

The student will achieve following skills:

- Able to sanitize the massive amount of IT security information relevant to his/her company
- Understand what the current threat landscape looks like, and the development of it
- Able to identify and mitigate IT security threats
- Understand the most common security issues and exposes within a company
- Able to make a security audit on a system/network/infrastructure

2.1.1 Module 1: Threat assessment & Information gathering

- Who are the hackers?
 - How are they organized?
 - How do they operate?
 - How can they earn money on your business?

- How to prepare an attack?
 - Social engineering
 - Fingerprinting
 - Port scanning
 - Banner grabbing
 - Meta data
 - Google hacking
 - Website searching

- How do we find and prioritize our threats?
 - Business Impact Analysis (BIA)
 - Risk analysis

Finally, all participants create an information gathering report on their own company.

2.1.2 Module 2: Attack techniques

- Website hacking
 - Cross-site scripting
 - Cross-site request-forgery
 - SQL injection
 - Cookie manipulation
 - Etc.
- Password cracking
 - Brute forcing
 - Rainbow tables
- Drive-by hacking
 - Advance social engineering
 - Attacking the browser
- Insight into tools and frameworks freely available

Finally, all participants make a security audit of a website and a Windows PC.

2.1.3 Module 3: Identify and exploit vulnerabilities

- What is fuzzing?
- What is a debugger?
- How to find vulnerabilities in software
- How to write an exploit

Finally, all participants will learn to find vulnerabilities in a piece of software and write their own exploit.

2.1.4 Duration

Module 1:	2 days	(8-15.30)
Module 2:	2 days	(8-15.30)
Module 3:	2 days	(8-15.30)
Exam:	½ day	(8-12)

2.1.5 Price

Per module:	12.000 DKK excl. VAT
Exam:	6.000 DKK excl. VAT
Full package (3 modules & exam):	30.000 DKK excl. VAT

3 CSIS Forensic & Incident Response

The student will achieve following skills:

- Learn how to detect and react when an incident happens
- Learn how to analyze different types of security incidents
- Get to know the different file systems
- Understand the complexity of malware and how to detect

3.1.1 Module 1: Detect & react

- The five steps to IR
 - Preparation
 - Response kit
 - Cabels
 - Tools
 - Hard disks
 - Detection
 - IPS/IDS
 - Logs
 - SIEM
 - Users
 - Understand the threat
 - Verify an incident
 - Containment
 - Pull the plug
 - Segmentation
 - IDS/IPS
 - Custom signatures
 - Removal
 - Know the cause
 - Understand the risks
 - Getting back in business
 - Reinstall
 - Restore
 - Re-establish processes
 - Lessons learned
 - Feeds Preparation

- Defining the terms
 - Events
 - Incident
 - When does an event become an incident
- Acquisition
 - Memory
 - Hard disks
 - Parts of file system
 - Documentation
 - Evidence handling
 - Virus detection
 - Limitations in anti-virus
 - Secure DNS & Heimdal
 - Network analysis
 - Netstat
 - Firewall logs
 - IDS/IPS
 - Custom signatures
 - Abnormal behaviour
 - Process lists
 - Usefulness
 - Root kits
 - Detection

3.1.2 Module 2: Analyze file system, registry and memory

- Understand file systems
 - File system/metadata and data
 - NTFS
 - Ext3
- Understand registry
- Understand memory
- Time lining
 - File system timeline
 - Registry timeline
 - Logs
 - Super time lining
- Sleuth and Autopsy
 - Sleuth set of commands
 - Use autopsy

3.1.3 Module 3: Malware analysis

- Behavioural analysis
 - Environment
 - System changes
 - Network changes
- Code analysis
 - Olly Debugger
 - Detect and identify packers
 - Unpack packed code

Finally, all participants will do an acquisition on a Windows OS and analyze the incident.

3.1.4 Duration

Module 1:	2 days	(8-15.30)
Module 2:	2 days	(8-15.30)
Module 3:	2 days	(8-15.30)
Exam:	½ day	(8-12)

3.1.5 Price

Per module:	12.000 DKK excl. VAT
Exam:	6.000 DKK excl. VAT
Full package (3 modules & exam):	30.000 DKK excl. VAT

4 CSIS Secure Web Programming

Contact CSIS for details

5 Instructors

The same consultants who carry out tasks for large Danish and foreign organizations share their knowledge with you in an open environment*. The consultants are working on a daily basis with everything from investigation of computer crimes to security audits and malware analysis. Due to their background and experience, the instructors make the course programs interesting, challenging and inspiring.

A selection of the instructors' certifications:

- GIAC Reverse Engineering Malware (GREM)
- Certified Expert Penetration Tester (CEPT)
- Certified Penetration Tester (CPT)
- EC-Council Certified Security Analyst (ECSAv4)
- Certified Ethical Hacker (CEHv6)
- Certified Information Systems Auditor (CISA)
- GIAC Certified Firewall Analyst (GCFW)
- GIAC Certified Forensics Analyst (GCFA)
- GIAC Information Security Professional (GISP)
- Certified Information Systems Security Professional (CISSP)

In addition, some of CSIS' instructors were on the winning team, European Nopsled Team, in the Defcon Competition 2011: Capture The Flag; <https://www.csis.dk/da/csis/news/3299/>

* CSIS always respects and protects our customer's privacy and therefore all examples taken from real life are completely anonymised

6 Course facilities

The courses are held in exclusive facilities with space for up to 12 students:

Institut for Selskabsledelse
Olof Palmes Gade 8
2100 København Ø

Breakfast, before lunch snacks, lunch, after lunch snacks is included and Coffee and soda is available all day long.

Hard copy of course material is available.

Laptop during the course is available.

7 Registration

Send an e-mail to academy@csis.dk or give us a call: +45 60 11 55 09.

Please don't hesitate calling us if you have questions.

We hope to see you soon!

Regards,
CSIS Academy Team