Cyberdefense

Training Catalogue 2026

Knowledge is power

AW 1.01 | Cybersecurity Awareness for Users

Overview

Complex security measures can often be foiled by attacking the users of your information system. This training, based on demonstrations and concrete examples, aims to provide end users with the correct tools and knowledge to respond to common threats such as social engineering, malicious software or the interception of communications.

Who should attend

- End-users
- CISO

Skills you'll learn

N/A

Level 1

2 hours

French or English

Course Modules

- Introduction
  - Rationale
  - Hacker types
  - Employee role in security
- Passwords
  - Attack types & examples
  - Password manager
  - Multi-factor authentication
- Social engineering
  - Concept
  - Attack vectors
  - Emails
  - Phishing
  - Others
- Malicious software
  - Anti-virus
  - Infection vectors
  - Mobile malware
- Remote working
  - Concepts
  - Attack vectors
  - Mobile devices
  - Collaboration tools
- Conclusion & Takeaways

For more information check
www.orangecyberdefense.com/ch

Orange Cyberdefense Switzerland
Rue du Sablon 4, 1110 Morges

training@ch.orangecyberdefense.com
+41 21 802 64 01

Cyberdefense

Training Catalogue 2026

Knowledge is power

AW 2.01 | Cybersecurity Awareness for Developers

Overview

This training is aimed at raising awareness towards security issues for developers. It starts by presenting an attacker's methodology before turning towards the OWASP Top 10. Each category from the Top 10 is explained and demonstrated so that the participants properly understand the consequences of each issue. Remediation options are also proposed for each subject. Additional topics are covered based on current trendy vulnerabilities if they are not already covered by the Top 10.

Who should attend

- Developers

Skills you'll learn

N/A
Level 1
4 hours
French or English

Course Modules

- Introduction
  - Secure Development Life Cycle
  - OWASP
- Attacker methodology
  - Information gathering
  - Entry point analysis
  - Parameter fuzzing
  - Automation
- Top 10 vulnerabilities
  - Broken access control
  - Cryptographic failures
  - Injection
  - Insecure Design
  - Security misconfiguration
  - Vulnerable and outdated components
  - Identification and Authentication failures
  - Software and Data Integrity failures
  - Security Logging and Monitoring failures
  - Server-Side Request Forgery
- Conclusions
  - Most reported vulnerabilities
  - Key takeaways

For more information check
www.orangecyberdefense.com/ch

Orange Cyberdefense Switzerland
Rue du Sablon 4, 1110 Morges

training@ch.orangecyberdefense.com
+41 21 802 64 01

Cyberdefense

Training Catalogue 2026

Knowledge is power

AW 3.01 | Darknet Awareness

Overview

This one-day course will introduce you to the concepts of the Darknet and allow you to delve deeper into the darkest corners of the Internet. The aim is to help you improve your monitoring and proactive security skills. In particular, you will learn how to search and communicate on the TOR network, and how to assess the impact of a leak from a third-party company on your business.

Who should attend

- End-users
- Developers
- Ethical hackers, incident responders
- IT system & network admins
- CISO

Skills you'll learn

N/A

Level 1

1 day

French or English

Course Modules

- Introduction
  - History
  - Hidden service examples
  - Privacy and anonymity
  - The good and bad sides of TOR
  - Golden rules on TOR
- How does TOR work?
  - Onion routing fundamentals
  - Guard, middle and exit relays
  - Nodes particularities
- About the toolkit
  - Occasional proxy
  - Basic routing
  - TOR Browser
  - Live OS
- Lab 1: Create your toolkit
  - Go back home with a portable TAILS
- Finding entry points
  - Search engines
  - Onion services lists
  - Hacking forums
  - Whistleblowers
  - Ransomware groups
- Lab 2: Find the leak
  - Find the leaks which may have an impact on your business
- How to communicate?
  - The various types of email services
  - Instant messaging and file sharing over TOR
  - Signing and encryption
- Lab 3: Play with XMPP
  - Create your account and chat with the classroom over TOR
- Monitoring automation
  - The various ways to monitor the surface web and hidden services

Cyberdefense

Training Catalogue 2026

Knowledge is power

HA 1.01 | Web Application Security

Overview

Hands-on training which covers a broad scope of vulnerabilities that can be found in Web applications. The objective is to provide participants with the methodology and tools required in order to assess a Web application. It is tailored for developers or junior security engineers who want to start their journey in attacking and compromising Web applications. It does not dive in-depth into specific vulnerabilities, but rather covers a broad spectrum of issues to provide the participants with a basic understanding of all the relevant topics.

Who should attend

- Developers
- Ethical hackers, incident responders
- IT system & network admins

Skills you'll learn

Basic understanding of Web technologies

Level 2

2 days

French or English

Course Modules

- **Introduction**
  - Overview of technologies in use
  - Encodings
  - Introduction to BurpSuite
- **Information gathering**
  - Generic information gathering
  - Specific information gathering
- **Entry point analysis**
  - Identifying entry points
  - Analysing entry points
  - Fuzzin entry points
- **Authentication & Authorisations**
  - Session issues
  - Authentication issues
  - Delegating authentication
  - SAML
  - Oauth2/OIDC
  - JWT
  - Access control
    - Function
    - Resource-based
- **Server-side attacks**
  - Injections
  - XML
  - Path traversal
  - Server-Side Request Forgery
  - Deserialization
  - Race conditions
- **Client-side attacks**
  - Same Origin Policy
  - Cross-Origin Resource Sharing
  - PostMessage API
  - JSONP
  - Cross-Site Scripting
  - Cross-Site Request Forgery
  - Websockets
- **Infrastructure attacks**
  - Attacking encryption mechanisms
  - Request smuggling
  - Cache poisoning

Cyberdefense

Training Catalogue 2026

Knowledge is power

HA 2.01 | Attacking Windows environments with Metasploit Frameworks

Overview

This training presents the characteristics of the Windows security model as well as the most common attacks against corporate environments. Demonstrations and hands-on exercises allow participants to better understand how these attacks work and how to protect these systems effectively.

Course Modules

- Offensive frameworks & tools
- Network discovery
- Vulnerability Exploitation
- Implant Deployment
- Windows Authentication Workflow
- Password theft & Lateral movements

Who should attend

- Ethical hackers, incident responders
- IT system & network admins

Skills you'll learn

N/A
Level 2
1 day
French or English

For more information check
www.orangecyberdefense.com/ch

Orange Cyberdefense Switzerland
Rue du Sablon 4, 1110 Morges

training@ch.orangecyberdefense.com
+41 21 802 64 01

Cyberdefense

Training Catalogue 2026

Knowledge is power

HA 3.01 | Attacking Mobile Applications Android Edition

Overview

This mobile training (designed for mobile developers or security engineers) covers common vulnerabilities that can be discovered in Android mobile applications. The participants will discover the methodology, and the tools used to attack and exploit mobile applications as well as apply them in diverse lab scenarios. This includes reverse engineering vulnerable applications and crafting malicious applications that exploit security vulnerabilities.

Who should attend

- Developers
- Ethical hackers, incident responders

Skills you'll learn

- **Comfortable with command line (Linux)**
- **Some experience with reverse engineering**

Level 3

1 day

French or English

Course Modules

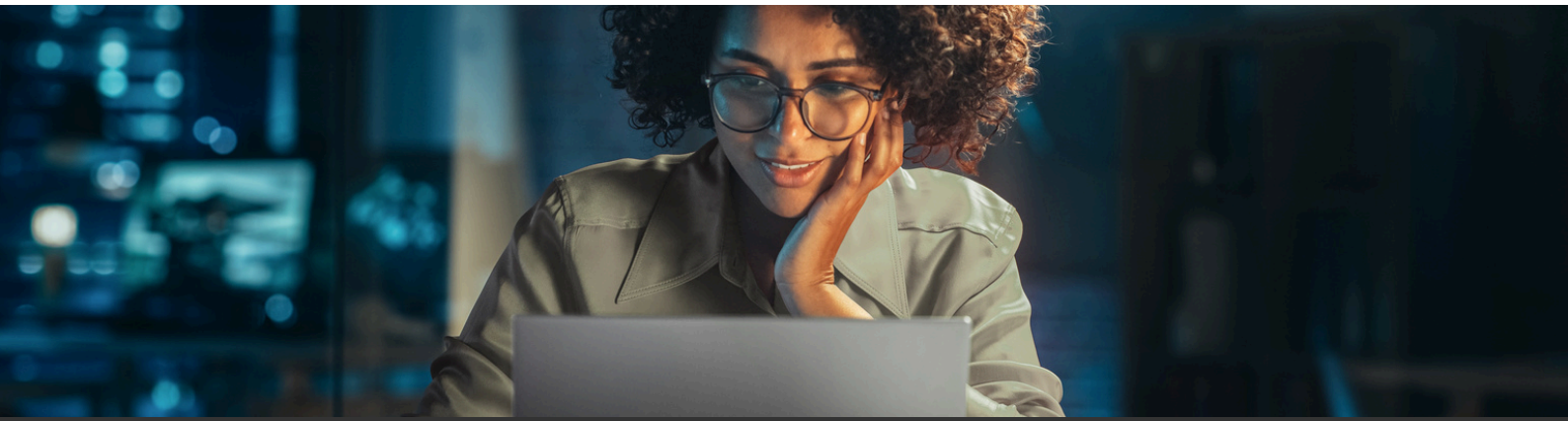
Module 01 – Android testing methodology

- Part 1: Creating an Android application testing environment
- Part 2: Attack surface and testing methodology

Module 02 – Exploiting vulnerabilities in Mobile Applications

- Part 1: High-level IPC issues.
- Part 2: Common permission issues.
- Part 3: Accessing Content providers.
- Part 4: Attacking Webviews.

Bonus 1: Memory corruptions bugs.



For more information check
www.orangecyberdefense.com/ch

Orange Cyberdefense Switzerland
Rue du Sablon 4, 1110 Morges

training@ch.orangecyberdefense.com
+41 21 802 64 01

Cyberdefense

Training Catalogue 2026

Knowledge is power

HA 3.02 | Attacking Mobile Applications iOS Edition

Overview

This mobile training (designed for mobile developers or security engineers) covers common vulnerabilities that can be discovered in iOS mobile applications. The participants will discover the methodology, and the tools used to attack and exploit mobile applications as well as apply them in diverse lab scenarios. This includes reverse engineering vulnerable applications and crafting malicious applications that exploit security vulnerabilities.

Who should attend

- Developers
- Ethical hackers, incident responders

Skills you'll learn

- **Comfortable with command line (Linux)**
- **Some experience with reverse engineering**

Level 3

1 day

French or English

Course Modules

Module 03 – iOS testing methodology

- Part 1: Creating an iOS application testing environment
- Part 2: Attack surface and testing methodology

Module 04 – Exploiting vulnerabilities in Mobile Applications

- Part 1: Local Data Storage
- Part 2: Broken Cryptography
- Part 3: Local Authentication
- Part 4: iOS Platform

Bonus 2: Mobile resilience

For more information check
www.orangecyberdefense.com/ch

Orange Cyberdefense Switzerland
Rue du Sablon 4, 1110 Morges

training@ch.orangecyberdefense.com
+41 21 802 64 01

Cyberdefense

Training Catalogue 2026

Knowledge is power

HA 4.01 | Windows Attack & Defense

Overview

This training will familiarize system administrators and security professionals with modern Windows attacks and best security practices, such as Windows security components, network interception, Active Directory mapping, privilege escalation, lateral movements, credentials theft and common persistence techniques. After covering a large attack overview, the course introduces associated counter-measures such as credentials protection and much more. After the workshop, members will understand how to protect their infrastructure against modern attacks. Hands-on: This class is practice-oriented, lectures present realworld attacks that participants put into practice in various labs.

Who should attend

- Ethical hackers, incident responders
- IT system, networks admins

Skills you'll learn

- **Comfortable with command line (Linux)**
- **Some experience with Windows environments**
- **Some experience with pentesting & hacking tools**

Level 3

2 days

French or English

Course Modules

Network access to initial account
- Windows network protocols poisoning (LLMNR, NetBIOS, DHCPv6)
- Initial network discovery (nmap port scan)

Active Directory mapping
- Active directory enumeration (Bloodhound, PingCastle)
- Kerberos authentication
- Common domain password extraction techniques (GPP passwords, Kerberoast, ASREPRoast)

Lateral movement
- Kerberos delegation (Unconstrained, constrained, ressource-based)
- NTLM authentication and cross-protocol relay attacks
- Ways to coerce a machine account NTLM authentication and abuse it (Printer Bug, PetitPotam, ntlmrelayx)

Windows credentials dumping
- Windows credentials storage (SAM, LSA secrets, LSASS, etc.)

Getting access to a key asset
- From RDP access to administrator
- Abusing impersonation privileges in Windows services

Domain compromise and persistence
- Domain credentials storage
- Kerberos Silver/Golden tickets

Bonus
- Physical device security (BitLocker and known attacks)
- LSA protection (how it works and how it can be bypassed)
- Credential Guard (how it works and how it can be bypassed)

For more information check
www.orangecyberdefense.com/ch

Orange Cyberdefense Switzerland
Rue du Sablon 4, 1110 Morges

training@ch.orangecyberdefense.com
+41 21 802 64 01

Cyberdefense

Training Catalogue 2026

Knowledge is power

IR 1.01 | Incident Response Management

Overview

This course is ideal for embarking on the long journey of incident response. Most of the process involves preparing in advance, and establishing procedures that you can rely on when the time comes. This halfday course is therefore an introduction to the concept of incident management, as well as the underlying best practices, norms and standards. It will enable you to lay the foundations of your defensive strategy from the point of view of preparedness.

Who should attend

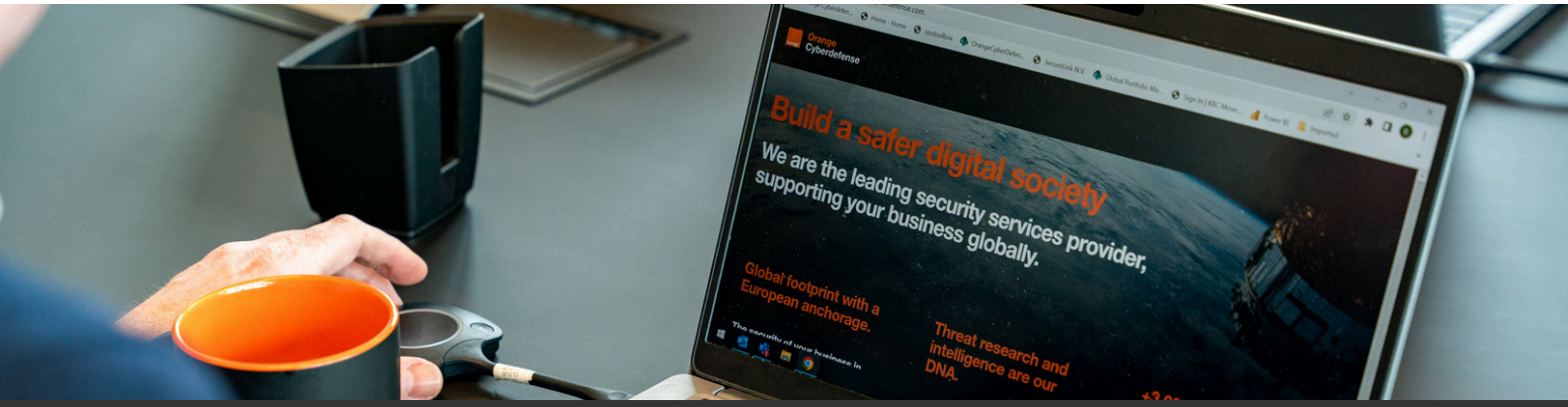
- Ethical hackers, incident responders
- IT system, networks admins
- CISO

Skills you'll learn

N/A
Level 2
4 hours
French or English

Course Modules

- **Introduction**
  - Prepare for the war
  - Recognize security incidents
  - Risk exposure
- **Standards and norms**
- **Incident handling**
  - Attack phases
  - Defender's view
  - Incident Response steps and best practices
  - Documentation and communication
- **Introduction to Forensic Analysis**
  - Avoiding mistakes
  - General principles
  - A few words on how to collect, handle and analyze digital evidence



For more information check www.orangecyberdefense.com/ch
Orange Cyberdefense Switzerland
Rue du Sablon 4, 1110 Morges
training@ch.orangecyberdefense.com
+41 21 802 64 01

Cyberdefense

Training Catalogue 2026

Knowledge is power

IR 2.01 | Log Management

Overview

This one-day course covers the fundamentals of event logging on Windows and Linux, the different types of log, and the management and analysis of these logs. It is an ideal complement to the IR1.01 course and aims at examining what needs to be logged and how, so that you can improve your ability to respond to security incidents.

Who should attend

- Ethical hackers, incident responders
- IT system, networks admins
- CISO

Skills you'll learn

N/A
Level 2
1 day
French or English

Course Modules

- **Log fundamentals**
  - The good and the bad logs
  - Benefits from the cyber-security point of view
- **Log types**
  - Pros and cons of the various types of logs
- **Log management**
  - Policy definition
  - Compliance requirements
  - Aspects to consider for a strong audit policy
  - Best practices
  - Infrastructure
  - Challenges and common mistakes
  - Logs centralization on Windows and Unix
- **Lab 1 - Data sources identification**
- **Logs analysis**
  - Handling Windows logs
  - Handling Linux logs
  - Rotation and permissions
- **Log management tools**
- **Lab 2 - Logs manipulation on Windows and Linux**

For more information check
www.orangecyberdefense.com/ch

Orange Cyberdefense Switzerland
Rue du Sablon 4, 1110 Morges

training@ch.orangecyberdefense.com
+41 21 802 64 01

Cyberdefense

Training Catalogue 2026

Knowledge is power

IR 3.01 | Incident Response & Forensic Analysis (Level 1)

Overview

This intensive hands-on one-day course is designed to introduce you to the investigation methods and tools you can rely on in the event of a security incident. It will take you into the world of incident response and forensic analysis, covering the different scenarios for acquiring RAM and hard disks, then focusing on triage through live analysis, as well as in-depth investigation through offline analysis.

Who should attend

- Ethical hackers, incident responders
- IT system, networks admins

Skills you'll learn

N/A
Level 2
1 day
French or English

Course Modules

- **Introduction to DFIR**
  - The pillars of incident response
  - A few words on digital forensics
  - Tactics, techniques and procedures
  - Incident response phases and common mistakes
  - Incident response lifecycle and success factors
- **Some words on incident response procedures**
  - The importance of documentation
  - Chain of custody
- **Acquisition**
  - Objectives, common pitfalls and data volatility
  - RAM acquisition on Windows
  - RAM acquisition on Linux
  - RAM acquisition on virtual machines
  - Disk acquisition
    - Various scenarios depending on conditions like physical access to the host, availability considerations, and disk extraction
    - Image file formats
    - Slack space
    - A few words on SSDs (interfaces and carving issues)
- **Analysis**
  - Bad VS good starts
  - Live analysis
    - Objective and drawbacks
    - What to look for?
  - Offline analysis
    - Advantages and prerequisites
    - Memory analysis
    - Filesystem analysis
- **Lab - Investigate an Active Directory compromise**
  - Triage
  - Memory analysis
  - Disk analysis
- **Small game to remember the most important points of the day with fun**

For more information check
www.orangecyberdefense.com/ch

Orange Cyberdefense Switzerland
Rue du Sablon 4, 1110 Morges

training@ch.orangecyberdefense.com
+41 21 802 64 01

Cyberdefense

Training Catalogue 2026

Knowledge is power

IR 3.02 | Incident Response & Forensic Analysis (Level 2)

Overview

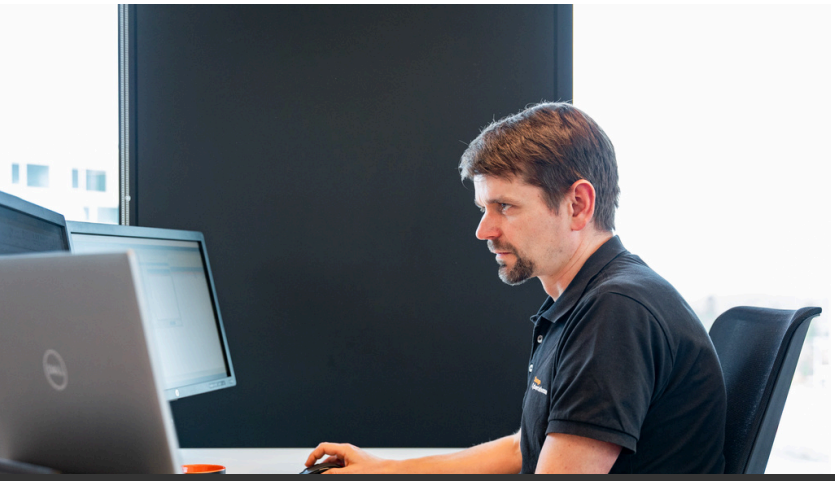
This intensive hand-om one-day course expands on the content of IR3.01 and introduces all the basic concepts you need to understand incident response and forensic analysis in a Windows environment. It covers advanced disk acquisition scenarios and will enable you to delve into the heart of the NTFS file system. You will also learn how to perform direct acquisitions of the operating system to extract valuable information from its many artefacts.

Who should attend

- Ethical hackers, incident responders
- IT system, networks admins

Skills you'll learn

IR 3.01
Level 3
1 day
French or English



Course Modules

- **Introduction**
  - Objectives
  - Quick reminder of the IR3.01 takeaways
- **Advanced disk acquisition scenarios**
  - Encrypted media
  - BitLocker case
  - A few words on flash memories
  - SSD vs HDD
  - SSD acquisition
- **NTFS artifacts**
  - Overview of the MFT and MBR
  - The MFT metadata from a DFIR perpective
    - $MFT metadata ($SI, $FN, $DATA, $I30)
    - Transaction log ($LogFile)
    - Change log ($UsnJrnl)
  - Metadata parsing and limitations
- **Windows artifacts**
  - Registry artifacts
  - File-based artifacts
  - Event logs
- **Live acquisition**
- **Lab - Further investigate the Active Directory compromise**
  - Understanding live acquisition principles
  - Analyzing the output of a live acquisition
  - Parsing the acquired event logs
  - File-based artifacts analysis
  - Network and files deletion artifacts
- **Small game to remember the most important points of the day with fun**

For more information check
www.orangecyberdefense.com/ch

Orange Cyberdefense Switzerland
Rue du Sablon 4, 1110 Morges

training@ch.orangecyberdefense.com
+41 21 802 64 01

Cyberdefense

Training Catalogue 2026

Knowledge is power

IR 3.03 | Incident Response & Forensic Analysis (Level 3)

Overview

This intensive hands-on one-day course complements the IR3.01 and IR3.02 courses by covering the fundamentals of mal- ware analysis on Windows. It aims to provide you with the methods and tools you need to carry out basic analyses, using both static and dynamic approaches. You will learn how to quickly assess the threat level of executable files and other Office documents.

Who should attend

- Ethical hackers, incident responders
- IT system, networks admins

Skills you'll learn

IR 3.02
Level 3
1 day
French or English

Course Modules

- **Introduction**
  - Objectives
  - Quick reminder of the IR3.02 takeaways
- **Malware Analysis fundamentals**
  - Purpose of malware analysis in the incident response phases
  - Various approaches to malware analysis
  - The main types of malwares
  - Anatomy of sophisticated attacks
- **Basic Static Analysis**
  - Signature-based scan, hashes and IOCs
  - PE analysis
  - Linked libraries and functions
  - Packed and obfuscated malware
  - Office documents
- **Basic Dynamic Analysis**
  - Advantages of controlled environments
  - Sandbox limitations
  - The DIY approach
- **Lab**
  - Understanding the types of malwares and the analysis techniques
  - Playing with a PE through Basic Static Analysis
  - Office document analysis
- **Small game to remember the most important points of the day with fun**

For more information check
www.orangecyberdefense.com/ch

Orange Cyberdefense Switzerland
Rue du Sablon 4, 1110 Morges

training@ch.orangecyberdefense.com
+41 21 802 64 01

Find our more about our training courses on:
orangecyberdefense.com/ch

Pricing

Standard Pricing Model

All trainings except AW 1.01		
1 - 2 seats	3 + seats	5 + seats
CHF 1'500	CHF 1'275	CHF 1'050
	- 15%	- 30%

The price is per day and per person.

Training Pass

Training pass	
Price	Description
CHF 6'000	Allow access to a total of 5 seats on shared training sessions.

Cybersecurity Awareness for Users

AW 1.01	
Base price (incl. 1 session)	Additional sessions (on same day)*
CHF 2'000	CHF 300

*A maximum of 3 AW 1.01 sessions can be organised on the same day.