Cyberdefense

TRAINING SCHEDULE - S2 2024

TUESDAY, SEPTEMBER 3, 2024 - DURATION: 1/2 DAY (MORNING)

INCIDENT RESPONSE MANAGEMENT – TRAINER : FRÉDÉRIC BOURLA

This training course is ideal for embarking on the long journey of incident response, which is not just about acquiring the tools and techniques you'll need to use in the heat of the moment. A major part of the process is preparing in advance, and establishing procedures you can rely on when the time comes. This half-day training course is therefore an introduction to the concept of incident management, as well as to the underlying best practices, norms and standards. It will enable you to lay the foundations of your defensive strategy in terms of preparedness.

WEDNESDAY, SEPTEMBER 4, 2024 - DURATION: 1 DAY

WEB APPLICATION ATTACK PART 1 - TRAINER: ALAIN MOWAT

The aim of this course is to prepare participants not only to test the security of a Web application, but also to correct the most commonly encountered vulnerabilities. The methodology for analyzing a Web site is developed, focusing first on identifying systems and entry points, then on exploiting vulnerabilities such as SQL injections or Cross-Site Scripting. Above all, this is a practical course in which participants can exploit the vulnerabilities discussed in order to fully understand how they work, and how best to protect their own applications.

THURSDAY, SEPTEMBER 5, 2024 - DURATION: 1 DAY

WEB APPLICATION ATTACK PART 2 - TRAINER: ALAIN MOWAT

This course is a logical continuation of the “HA1.01 - Attacking web applications - Level 1” course. It takes certain concepts and pushes them further to show that exploiting a vulnerability can often compromise not only an application, but in some cases the entire infrastructure hosting it. The course analyzes server-side attacks such as XML eXternal Entites, Local File Inclusion and other weak encryption problems, as well as client-side attacks aimed at bypassing the browser's “Same Origin Policy”.

TUESDAY, SEPTEMBER 10, 2024 - DURATION: 1 DAY

LOG MANAGEMENT – TRAINER: FRÉDÉRIC BOURLA

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 the ideal complement to the “INCIDENT RESPONSE MANAGEMENT” training course, and aims to provide a clearer picture of what needs to be logged and how, so that you can improve your security incident response capabilities.

THURSDAY, SEPTEMBER 19, 2024 – DURATION: 1/2 DAY (MORNING)

DEVELOPER AWARENESS (OWASP TOP 10) - TRAINER: ALAIN MOWAT

Discover the TOP10 OWASP risks, advice and solutions for reducing them, as well as a series of examples and advice adapted to the languages used by your teams (PHP, Java, C, etc.).

TUESDAY, SEPTEMBER 24, 2024 - DURATION: 1 DAY

INCIDENT RESPONSE & FORENSIC ANALYSIS (L1) - TRAINER: FRÉDÉRIC BOURLA

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

TUESDAY, OCTOBER 1, 2024 - DURATION: 1 DAY

INCIDENT RESPONSE & FORENSIC ANALYSIS (L2) - TRAINER: FRÉDÉRIC BOURLA

This intensive one-day course builds on FOR1.01 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 (such as FDE and SDD) and will enable you to delve into the heart of the NTFS file system to exploit its main metadata. You'll also learn how to make direct acquisitions of the operating system to extract valuable information from its many artifacts.

TUESDAY, OCTOBER 8, 2024 - DURATION: 1 DAY

INCIDENT RESPONSE & FORENSIC ANALYSIS (L3) – TRAINER: FRÉDÉRIC BOURLA

This intensive one-day course complements FOR1.01 and FOR1.02 by covering the fundamentals of Windows malware analysis. It aims to provide you with the methods and tools you need to carry out basic analyses, using both static and dynamic approaches. You'll learn how to quickly assess the threat level of executable files and other Office documents.

TUESDAY, NOVEMBER 5, 2024 - DURATION: 1 DAY

ATTACKING WINDOWS ENVIRONMENTS WITH METASPLOIT - TRAINER: JULIEN OBERSON

This training course presents the characteristics of the Windows security model, as well as the most common attacks against corporate environments. Demonstrations and exercises enable participants to better understand how these attacks work and - by extension - how to protect themselves effectively.

THURSDAY, NOVEMBER 7, 2024 - DURATION: 1 DAY

DARKNET AWARENESS - TRAINER: FRÉDÉRIC BOURLA

This one-day training course will introduce you to the concepts of the Darknet and take you step by step into the darkest corners of the Internet. Its aim is to improve your monitoring and proactive security skills. In particular, you'll learn how to search and communicate on the TOR network, as well as how to assess the impact of a third-party leak on your business.

TUESDAY, NOVEMBER 19, 2024 - DURATION: 1 DAY

MOBILE APPLICATION ATTACK - TRAINER: FABRICE CARALINDA

This course aims to share experience and knowledge in auditing mobile applications on Android and iOS. The course presents auditing processes and techniques to help participants prepare an ideal test environment for assessing the security of an application. Among other things, it presents several methodologies for security testing, from local analysis to inspection of an application's network traffic. The course also provides several examples of how to automate the tedious tasks involved in most mobile security audits (root bypass/jailbreak detection or certificate pinning).

CONDITIONS AND PRICES

“A la carte” training

CHF 2,000 valid for one day of specific training for one participant
(CHF 1,000 for ½ day).

“Training Pass”

CHF 8,000 valid for one calendar year from the date of registration and including all training courses offered, for one participant. The pass is transferable and non-nominative; it is therefore possible to register a different person for each course.

Payable within 30 days of registration.

Group courses are non-refundable, even if the participant is unable to attend. However, another person may replace the participant.

info@ch.orangecyberdefense.com
www.orangecyberdefense.com/ch
+41 (0)21 802 64 01
Rue du Sablon 4
1110 Morges, Switzerland