CIRCL - Computer Incident Response Center Luxembourg

# *TRAINING AND TECHNICAL COURSES CATALOGUE 2023*

*from Incident Response to Operational Security*

*TLP:CLEAR - version 202301*

CIRCL
Computer Incident
Response Center
Luxembourg

# *INTRODUCTION*

CIRCL offers courses to its members and organizations based in Luxembourg and worldwide.

In their mission to improve information security, CIRCL is sharing its field experience through a set of training or technical courses. Due to diversity of competences within the team, CIRCL is able to provide a large diversity of information security trainings. Courses target technical experts but also non-technical staff in the topics of incident handling, malware analysis, operational security and system forensics.

CIRCL sees the trainings and technical course as a great opportunity to learn from their partners, too, and to improve the security handling procedures. By attending the courses, partners are not only helping their own organization but also the overall security in Luxembourg (i.e. it is beneficial for both the organization and CIRCL if the technical staff is prepared for Incident Response).

Courses can be held at CIRCL's training room or virtually in Video Teleconferencing unless specific requirements are noted.

Courses however have specific requirements in terms of technical equipment or preliminary knowledge. These requirements are specified in the course description or will be specified before the course starts.

CIRCL provides these courses under tailored terms and conditions in order to fit your organizational structure. Don't hesitate to Contact us for more information.

CIRCL
Computer Incident
Response Center
Luxembourg

# Contents



CIRCL
Computer Incident
Response Center
Luxembourg

# *INTRODUCTION TO INCIDENT RESPONSE*

| | |
|---|---|
| **Title** | Introduction to Incident Response |
| **Abstract** | Incident detection and response introduction theory and practical examples from concrete incidents. The training includes an overview of the most common types of incidents encountered in Luxembourg. |
| **Goals** | How are the majority of security incidents detected<br>- How to secure evidences after detecting an incident<br>- How to perform acquisition of evidences (file-system, memory and network)<br>- How to interact with local CERTs and/or international CERTs<br>- How to balance remediation with incident response<br>- How to communicate an incident in the public |
| **Who** | IT department staff and manager - Local Incident Response Team |
| **Level** | IT support - basic knowledge of operating systems is required |
| **Duration** | 3 hours |
| **Language** | English, French, German or Luxembourgish |

CIRCL
Computer Incident
Response Center
Luxembourg

# *FILE-SYSTEM POST-MORTEM FORENSIC ANALYSIS*

| | |
|---|---|
| **Title** | File-system Post Mortem Forensic Analysis |
| **Abstract** | Forensic Analysis is based on the assumption that everything leaves a trace behind. A trace in an information system can be any data that helps to identify space and time actions. Post mortem analysis is a key tool to discover and analyse security incidents.<br><br>This course will teach the participant on how to find answers to what has happened by analysing different layers from the physical medium, the file system up to application level. |
| **Goals** | - Perform disk acquisition the right way<br>- Introduction to file system analysis (NTFS/FAT)<br>- Analysis of operating system artifacts (MS Windows)<br>- Find evidences in communication applications (e.g. browser or chat history) |
| **Who** | IT department staff - Local Incident Response Team |
| **Level** | Knowledge of operating systems and IT security is required |
| **Duration** | 8 hours |
| **Language** | English, German |

CIRCL
Computer Incident
Response Center
Luxembourg

# *INTRODUCTION TO PENETRATION TESTING*

| | |
|---|---|
| **Title** | Introduction to Penetration Testing |
| **Abstract** | Besides classical security techniques like firewalls, VPN, Antivirus among many others, offensive security is also a mandatory ability nowadays. This course gives an overview on how attackers prepare and execute a targeted attack.<br><br>APT - Advanced Persistent Threats turn into the most critical risk for companies today. This course will help the security responsible to see their corporate network from the attackers point of view and choose the necessary security mechanisms. |
| **Goals** | Learn to attack your network before others do |
| **Who** | IT security teams and administrators |
| **Level** | Good level of IT security |
| **Duration** | 8 hours |
| **Language** | English, German |

CIRCL
Computer Incident
Response Center
Luxembourg

# *INTRODUCTION TO (MALWARE) REVERSE ENGINEERING*

| | |
|---|---|
| **Title** | Introduction to (Malware) Reverse Engineering |
| **Abstract** | It is not unusual to detect unknown software on computer systems. Identifying if the software is malicious or benign is a critical (and expensive) task. This course aims to develop skills to perform basic Malware Reverse Engineering.<br>The goal of this course is to set up a malware laboratory for each student and to get introduced into the most successful malware reverse engineering strategies. |
| **Goals** | - Get an overview of malware analysis techniques<br>- Create a custom lab environment<br>- Be able to collect indicators if a file is malicious or benign<br>- Develop strategies to collect Indicators of Compromise (IOCs)<br>- Build-up some solid grounds for further studies |
| **Not in scope** | - Learn x86 assembler<br>- Get deep into reverse engineering |
| **Who** | Security Engineers, Administrators, Managers |
| **Prerequisites** | - Linux/UNIX experience<br>- Good knowledge of Windows internals<br>- Knowledge about control flows in programming languages<br>- Understanding of TCP/IP networks, DNS, proxy, firewall<br>- Very basic x86 assembler understanding is an advantage |
| **Duration** | 16 hours or 24 hours |
| **Language** | English, German |

CIRCL
Computer Incident
Response Center
Luxembourg

# *MISP - THREAT INTELLIGENCE AND INFORMATION SHARING*

| | |
|---|---|
| **Title** | MISP Threat Intelligence |
| **Abstract** | MISP is an advanced open source platform for sharing cyber threat intelligence, storing and correlating cyber threat intelligence (CTI) from attacks and cyber security threats.<br>MISP is a full-feature information and threat sharing platform to support operational and tactical cyber security intelligence.<br>The training will show the platform, its functionalities and demonstrate how to benefit most from sharing, commenting and contributing on it. Custom MISP training or workshop can be also organised based on the MISP training materials produced by CIRCL. |
| **Sections** | - (3 hours) MISP usage and how it can be used to support your operational cyber security intelligence. A practical overview of MISP and how to use it from a user perspective.<br>- (3 hours) MISP interfaces and API. How to use and extend MISP to support your information security operational teams using programmatic interfaces.<br>- Timetable which can be adapted following specific needs or requirements. |
| **Who** | Security Engineers, ICT Administrators, Analysts |
| **Prerequisites** | - Good knowledge of information security fundamentals. |
| **Duration** | 6:00 |
| **Language** | English |

CIRCL
Computer Incident
Response Center
Luxembourg

# *TRAINING MATERIALS FREELY AVAILABLE*

| | |
|---|---|
| **Title** | Training Materials Freely Available |
| **Background** | At CIRCL, we create trainings in order to improve the state of information security in Luxembourg and abroad.<br><br>We strongly believe that sharing the training materials can significantly help organizations, private companies and training centers to improve the overall shape in IT security. Reusing our material is strongly encouraged.<br><br>This is the reason why we publish a significant part of our trainings including slides and additional material under open source licenses. |
| **Available materials** | |
| **MISP** | https://github.com/misp/misp-training |
| **MISP LEA** | https://github.com/MISP/misp-training-lea |
| **AIL** | https://github.com/ail-project/ail-training |
| **Forensic** | https://www.circl.lu/services/forensic-training-materials/ |
| **Penetration testing** | https://www.circl.lu/services/pentest-training-materials/ |

CIRCL
Computer Incident
Response Center
Luxembourg

# *CONTACT*

## Postal Address

CIRCL - Computer Incident Response Center Luxembourg
c/o "Luxembourg House of Cybersecurity" g.i.e.
122, rue Adolphe Fischer
L-1521 Luxembourg
Grand-Duchy of Luxembourg

## Telephone

(+352) 247 88444

## Email

info@circl.lu
PGP Fingerprint: CA57 2205 C002 4E06 BA70 BE89 EAAD CFFC 22BD 4CD5

CIRCL
Computer Incident
Response Center
Luxembourg