Training in CYBERSECURITY

LEARNING AND BUILDING CYBERSECURITY

HOUSE OF TRAINING

SECURITY MADEIN.LU

aware.lu circl.lu cases.lu

INFORMATIQUE

LEARNING AND BUILDING CYBERSECURITY

Keeping information safe is a priority that concerns all areas of economic activity and all employees have a stake in safeguarding their companies' and institutions' data. This is a considerable challenge across the globe including Luxembourg. Indeed, attacks are becoming more frequent and need to be managed. With this in mind, a partnership between Security Made in Lëtzebuerg GIE, commissioned by the Ministry of Economy to promote and reinforce information security in Luxembourg, and House of Training has been established. The main objective of this collaboration is to offer targeted training options.

HOUSE OF TRAINING

Formally established in 2015, the House of Training brings together, under a single roof, the training institutes of both the Chamber of Commerce and the Luxembourg Bankers' Association (ABBL), who are renowned for their expertise and their vast offerings in the field of continued vocational training in Luxembourg. The Financial Technology Transfer Agency (ATTF) also joined the House of Training on 1st January 2016, bringing a significant international dimension.

www.houseoftraining.lu

SECURITYMADEIN.LU is the main platform for cybersecurity in Luxembourg. Its goal is to provide news, tools, information as well as cybersecurity solutions for private users, organisations and the ICT community. Its stakeholders are the Ministry of Family, Integration and the Greater Region, Ministry of Education, Childhood and Youth, Ministry of the Economy, as well as local government federations SIGI (Syndicat Intercommunal de Gestion Informatique) and SYVICOL (Syndicat des Villes et Communes du Luxembourg).

www.securitymadein.lu

SERIOUS GAME - RED / BLUE TEAM (FOR TECHNICAL STAFF)

Objectives

Based on a realistic and operational IT infrastructure, we offer to your teams the opportunity to expose themselves to real scenarios in the field of cybersecurity / cyber defence. Beyond learning by doing, the objective is to test the skills of your teams and their operational capacities in terms of reaction and defensive struggle.

- Learning how to detect an attack
- Evaluate the severity of an attack quickly
- Determine the appropriate level of countermeasures
- Maintain the availability of services during an attack
- Search for evidence
- Reporting an attack
- Learn or refine techniques
- Adopting reflex acts

Programme

This activity is intended for any organisation wishing to realistically train their teams involved in the cyber chain, without exposing its own infrastructure.

Target audience

- Technical teams (SOC operators, CERT experts ...)
- Management teams (RSSI, DSI, General Management, Communication Department, ...)

Duration

3 hours

Languages

French / English

MIX OF ROOM 42/SERIOUS GAME (TECHNICAL AND NON-TECHNICAL STAFF – CUSTOMISED)

Objectives

We suggest that you involve each department of your organisation in a real cyber crisis management exercise. Under the guidance of our experts, we will analyse the reaction of your teams to our multiple attacks. We offer you a real cyber defence training during which you can:

- Test your own defensive procedures
- Confront the reflexivity of your decision-makers in stressful situations
- Immersing your staff in a major IT crisis close to reality
- Analyse inter-team collaborative capacities

Programme

Based on a mix of room 42 and serious game activities, we propose to simulate an

- environment modelled on your organisation and expose it to a cyber-attack.

Target Audience

C' level, Management, CIO, CISO, Technical People, Technical teams (SOC operators, CERT experts...)

Duration

8 hours

Languages

French / English

MISP – MALWARE INFORMATION SHARING PLATFORM - THREAT SHARING

Sharing is caring

Objectives

- MISP usage: how it can be used to support your operational cybersecurity intelligence. A practical overview of MISP and how to use it from a user's perspective
- MISP interfaces and API. How to use and extend MISP to support your operational security information teams using programmatic interfaces
- Be part of the MISP future, how to contribute to MISP not only as a developer but as an active contributor (from documentation to taxonomies)

Programme

MISP is an advanced platform for sharing, storing and correlating Indicators of Compromise (IOCs) from attacks and cybersecurity threats. Today, MISP is used in multiple organisations to store, share, collaborate on malware, and also to use the IOCs to detect and prevent attacks. The aim of this trusted platform is to help to improve the countermeasures used against targeted attacks and set up preventive actions. MISP becomes a full-featured information and threat sharing platform to support operational and tactical cybersecurity intelligence.

The training will introduce the platform's functionalities and demonstrate how to benefit most from sharing, commenting and contributing on it. At the end of the day, every participant will be knowledgeable in information sharing about cybersecurity threats and become a proficient MISP user and threat intel handler.

Target Audience

Security Engineers, ICT Administrators, Analysts

Prerequisites

Good knowledge of information security fundamentals

Duration

6 hours

Language

English

Training materials freely available on:
www.circl.lu

Simulation: acquire know-how and practical competencies

ROOM 42 – DO(N'T) PANIC (FOR NON-TECHNICAL STAFF)

The day after: check how long you will survive after a major cyber-attack...

Objectives

Break the complexity of cybersecurity tasks and create motivation for collective efforts to deal with the rising challenges.

Programme

The simulation environment creates a realistic experience where all participants are required to make quick, high-impact decisions with real-time but - also often - minimal information.

The "Room 42" is a cyber-attack simulation game. It is an innovative and unique concept in Luxembourg, during which "players" will be completely immersed - for a maximum of 1 to 2 hours - in a cyber-attack and will be requested to react to it. The way the participants react, interact and behave will be scrutinized and analysed throughout the game.

Target Audience

C' level, Management, CIO, CISO, Technical people

Duration

3 hours

Languages

French / English

Programme overview

The first category of training courses (TRAINING) aims to provide a sound theoretical and practical knowledge on different subjects related to Cybersecurity, whereas the second category (SIMULATION) is designed to strengthen practical know-how by creating realistic scenarios for participants.

All training and simulation modules can be booked separately.

TRAINING: increase skills and knowledge

	Hours	FR	EN	DE	LU	P.
Awareness for everyone	3h	✓	✓	✓	✓	4
Cybersecurity for managers	2h	✓	✓	✓	✓	5
Security elixir for IT managers	3h	✓	✓	✓	✓	5
Cybersecurity for trainers	8h	✓	✓	✓	✓	6
Ethical hacking	8h	✓	✓			6
MONARC - Optimised **method for risk analysis**	8h	✓	✓			7
File-System Post-Mortem Forensic Analysis	8h		✓	✓		8
Digital Privacy Salon	2h	✓	✓	✓	✓	8
Introduction to Penetration Testing	8h		✓	✓		9
Introduction to (Malware) Reverse Engineering	16 or 24h		✓	✓		9
MISP - Malware Information Sharing Platform - Threat Sharing	6h		✓			10

SIMULATION: acquire know-how and practical competencies

	Hours	FR	EN	DE	LU	P.
Room 42 – Do(n't) Panic (For Non-Technical Staff)	3h	✓	✓			10
Serious Game - Red / Blue Team (For Technical Staff)	3h	✓	✓			11
Mix of Room 42/Serious Game (Technical and Non-Technical Staff – Customised)	8h	✓	✓			11

Training: increase skills and knowledge

AWARENESS FOR EVERYONE

Don't suffer in silence

Objectives

- Understanding the basics of information security
- Acquiring the right reflexes
- Learning how to protect information assets (private or professional)

Programme

- Introduction
    - Invisible danger, unbelievable threats and optical illusions
    - Identify threats and vulnerabilities
    - Protect yourself
- Basics
    - Wear helmet and shield
    - Keep secrets
    - Build battlements
- Protection
    - Human factor: the weak link
    - Human factor: the strong link
    - Social engineering: some gifts are poisoned
    - Message in a bottle: do you know where it comes from?
- Watch the enemy
    - Dealing with incidents: malicious acts, attacks, negligent actions, accidents, impacts, etc
    - Prevention and protection: how to organise and strengthen your defences
    - Protect your life. Protect your data
    - Safely fly over the cloud and online services
    - Mobile devices: weaker and stronger

Target Audience

Employees, self-employed or private individuals

Duration

3 hours

Languages

French / English / German / Luxembourgish

INTRODUCTION TO PENETRATION TESTING

Is your protection strong enough?

Objectives

Learn to attack your network before others do

Programme

Besides classical security techniques like firewalls, VPN, AV among many others, offensive security is also a mandatory ability nowadays. This course gives an overview on how attackers prepare and execute targeted attacks. APT - Advanced Persistent Threats turn into the most critical risk for companies, today. This course will help the security managers to see their corporate network from the attackers' point of view and choose the necessary security mechanisms.

Target audience

IT security teams and administrators

Level

Good level of IT security

Duration

8 hours

Languages

English / German

Training materials freely available on:
www.circl.lu

INTRODUCTION TO (MALWARE) REVERSE ENGINEERING

Undress the malware to strengthen your shield

Objectives

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.

The goal of this course is to set up a malware laboratory for each student and to introduce the most successful malware reverse engineering strategies.

Programme

- Get an overview of malware analysis techniques
- Create a custom lab environment
- Be able to collect indicators if a file is malicious or benign
- Develop strategies to collect Indicators of Compromise (IOCs)
- Build-up some solid grounds for further studies
    - Not in scope
    - Learn x86 assembler
    - Get deep into reverse engineering

Target Audience

Security Engineers, Administrators, Managers

Prerequisites

- Linux/UNIX experience
- Good knowledge of Windows internals
- Knowledge about control flows in programming languages
- Understanding of TCP/IP networks, DNS, proxy, firewall
- Very basic x86 assembler understanding is an advantage

Duration

16 hours or 24 hours

Languages

English / German

FILE-SYSTEM POST-MORTEM FORENSIC ANALYSIS

What has happened to your corrupted system ?

Objectives

- Perform disk acquisition the right way
- Introduce to file system analysis (NTFS/FAT)
- Analyse operating system artefacts (MS Windows)
- Find evidence in communication applications (e.g. browser or chat history)

Programme

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. This course will teach the participants how to find answers to what has happened by analysing different layers from the physical medium to the file system up to the application level.

Target audience

IT department staff - Local Incident Response Team

Level

Knowledge of operating systems and IT security is required

Duration

8 hours

Languages

English / German

DIGITAL PRIVACY SALON

A smart chat without a smartphone

Objectives

A digital privacy salon presents and explains how to use secure communication tools along with good Internet hygiene and understanding the associated risks.

Programme

- Learning how to securely use:
- Browsers (e.g. HTTPS, plugins, passwords, tracking, phishing)
- Instant messaging (e.g. OTR, Cryptocat)
- E-mails (e.g. virus, spam, encryption (PGP - GnuPG))
- Mobile devices (e.g. tracking, secure communication)
- Disk encryption (e.g. FireVault, Bitlocker, LUKS, truecrypt)
- Online and offline exchange of data (e.g. USB, Sharing platforms)
- Network encryption (e.g. VPN, Tor)

Target Audience

Citizens using IT equipment

Level

Beginner or Advanced

Duration

2 hours

Languages

English / French / German / Luxembourgish

CYBERSECURITY FOR MANAGERS

When cybersecurity means efficiency and performance

Objectives

- Understanding what information security involves:
  - in economic terms
  - in legal terms
  - in terms of image and reputation
- Making information security a strategic element for the organisation
- Protecting every component of an organisation (people, clients and assets)

Programme

- Identifying strategic data and understanding the value of the organisation's information assets (patents, skills, confidential information, etc.)
- Protecting the organisation
- Understanding basic vulnerabilities and how to mitigate them
- Knowing the most frequent threats: the human factor, piracy, negligent behaviours, etc.
- Taking the new risks into account: social networks, mobility, cloud computing, BYOD
- Adopting minimal security measures: charter, increasing awareness among staff, updates
- Foreseeing the impacts of a security incident
- Facing a crisis: disaster response plan, business continuity, crisis communication
- Respecting the legislation on information security

Target audience

Managers and decision-makers

Duration

Two-hour training course delivered by a security expert

Languages

French / English / German / Luxembourgish

SECURITY ELIXIR FOR IT MANAGERS

Analyse, Detect, React

Objectives

- Making IT teams feel responsible for what information security involves
- Positioning information security at the heart of IT activity
- Learning (or re-learning) good practices in information security

Programme

- Safe development
- Code revision
- Pen testing
- Maintaining an information system safely
- Knowing the usual threats and vulnerabilities
- Adding security within the IT management routine
- Knowing the framework of regulations and obligations incumbent on IT personnel in terms of information security
- Knowing how to report a security incident or the detection of a vulnerability

Target audience

IT personnel, IT managers, safety and security managers

Duration

Three-hour training course delivered by a security expert

Languages

French / English / German / Luxembourgish

CYBERSECURITY FOR TRAINERS

Become a guru. Show the right way

Teaching your colleagues is the best way to maintain your knowledge and stay in touch with the problems they are facing in their everyday work.

Objectives

- Training the trainers in order to improve in-house awareness of information security
- Building in-house competencies to strengthen the cybersecurity maturity of the organisation

Programme

- Reminder and continuation of introduction programmes
- Teaching methods
    - Increasing awareness without imposing guilt
    - Highlighting the ROI (return on investment) of security
    - Using everyday examples
    - Organising situation-staging / Role-playing
    - Adapting courses to the maturity level of their target audience
- Educational tools
    - How to create a good password
    - How to manage passwords
    - How to test a URL
    - How to make your browser safe
    - How to configure a Facebook and an e-mail account
    - How to encrypt data
    - How to keep mobile interfaces safe
    - How to keep your Wi-Fi connection safe
    - How to set up a coherent security strategy
    - Introduction to risk analysis

Target audience

IT personnel, trainers, etc.

Prerequisites

Participants must have completed the Awareness for everyone and Cybersecurity for managers training courses.

Duration

Eight-hour training course delivered by a security expert

Languages

French / English / German / Luxembourgish

ETHICAL HACKING

Don't be evil!

Discover the other side of the scenery by putting yourself in the shoes of an "ethical hacker".

Wake the coding daemon inside of you and start coding to break through the networks…. legally.

Objectives

Understand how hackers can use the vulnerabilities of our infrastructure and information systems to achieve their goals.

Programme

- Introduction
    - The basics of ethical hacking
    - Objectives, practices and rules
    - The strategies of the ethical hacker
- The preparatory phase
    - Prepare an attack
    - Hacker tools and techniques
- The enforceable phases
    - Recognition: Finding a victim and detecting vulnerabilities
    - Intrusion: Successfully enter the victim's computer
    - Operation: Divert a system or retrieve data
- Finalisation: Remove the traces
- The terminal phase
    - Exploit the product of the attack
- Reminder to the law

Target audience

For all

Duration

8 hours

Languages

French / English

MONARC - OPTIMISED METHOD FOR RISK ANALYSIS

Don't be afraid of risk. Manage it.

Objectives

Master the risk analysis with the MONARC tool.

Programme

Raising awareness among the employees is absolutely necessary to improve the security of your company. Necessary but not sufficient. You need to manage the risk by using a systematic method that will help you to identify and mitigate every single risk.

This training teaches you to use the assessment tool MONARC, to understand and master its main functionalities and the different steps of the associated method. At the end of the training, people will be able to conduct a risk analysis using MONARC as described in the ISO 27005.

Target Audience

Risk managers

Duration

8 hours

Languages

French / English

HOUSE OF TRAINING

More information

More information about the course content and objectives, the target audience, the exact schedule, etc. can be found on our website www.houseoftraining.lu

Registrations

Registrations for the training modules are to be made online via our website. They have to be made at least 5 days before the beginning of the training course.

Registration fees

The fees indicated in this flyer represent the basic fees. These can vary, depending on several options chosen by the participant (training material, exam fees, etc.). All prices are indicated without VAT (3%).

Training location

Unless otherwise indicated in the registration confirmation, all courses take place at the:

Chamber of Commerce
Training Centre
7 rue Alcide de Gasperi
L-1615 Luxembourg

C3 - Cybersecurity Competence Center Luxembourg
16 boulevard d'Avranches
L-1160 Luxembourg
Tel.: +352 274 00 98

Contact

House of Training - Customer Service
customer@houseoftraining.lu
BP 490 L- 2014 Luxembourg
Tel.: +352 46 50 16 – 1

www.houseoftraining.lu

Terms and conditions as stated on our website www.houseoftraining.lu are applicable.