+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated 04/30/2024

Sign up

Adversary emulation training with MITRE ATT&CK

3 days (21 hours)

Presentation

Our Adversary emulation training with MITRE ATT&CK will teach you to understand the importance of adversary emulation for the security of information systems. You'll be able to truly understand the scenario of a cyber attack, and be prepared to respond and prevent them.

Our program will enable you to understand all the key principles related to adversary simulation as well as advanced persistent threats (APTs) and their impact on security. You'll also learn about the importance of visualization in understanding attacks.

Our training course will teach you how to emulate opponents as close to reality as possible: researching hacker methods and planning operations will be on the agenda to create the most realistic scenarios possible.

Like all our training courses, this one runs on the latest version of the tool: Att&ck V15.

Objectives

- Understanding the importance of opponent simulation
- Efficiently simulate cyber attacks
- Analyze simulation results

Target audience

- Ethical Hacker
- Cybersecurity Experts
- Pentester

Prerequisites

- Cybersecurity/pentesting experience
- Basic IT knowledge

Adversary emulation with MITRE ATT&CK training program

INTRODUCTION TO OPPONENT EMULATION WITH MITRE ATT&CK

- Understanding the importance of adversary emulation to enhance security
- Introducing the MITRE ATT&CK framework
- Distinction between opponent emulation and threat simulation
- Overview of advanced persistent threats (APTs) and their impact
- Introduction to TTPs (Tactics, Techniques, and Procedures)

UNDERSTANDING OPPONENTS' MODUS OPERANDI

- Analysis of frameworks and strategies used by opponents
- Learn more about groups of notorious adversaries
- Study of real use cases for ATT&CK framework TTPs
- The importance of visualization in attack analysis
- Introduction to Cyber Threat Intelligence

PLANNING AND RESEARCH FOR OPPONENT EMULATION

- Definition of specific emulation objectives
- Research techniques on opponents' operating methods
- Detailed planning of opponent emulation engagements
- Selection of tools and resources required for emulation
- Discussion of ethics and legality in emulation operations

IMPLEMENTING TTPs WITH MITRE ATT&CK

- Building a test environment for emulation
- Practical implementation of TTPs based on case studies
- Techniques for realistically simulating attacks
- Measuring the effectiveness of existing safety controls
- Feedback and adjustment of emulation strategies

PRACTICAL EXERCISES IN OPPONENT EMULATION

- Drawing up an emulation plan

- Creating an emulation scenario
- Attack simulation
- Analysis of results and identification of safety gaps
- Techniques for documenting and reporting emulation results

DEFENSIVE STRATEGIES AND CONTINUOUS IMPROVEMENT

- Using emulation results to reinforce safety posture
- Development of defensive recommendations based on emulation data
- Importance of integrating emulation into the security lifecycle
- Planning emulation program updates and evolution
- Engaging with the ATT&CK community and sharing knowledge

CONCLUSION AND EVALUATION

- Summary of key training points
- Assessment of acquired skills through practical tests
- Discussion of next steps and learning opportunities

Companies concerned

This training course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire is used to check correct acquisition.

skills.

Sanction

A certificate will be issued to each trainee who completes the course.