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

Updated 03/15/2024

Sign up

# Huntress Managed Security Platform training

3 days (21 hours)

## PRESENTATION

Our Huntress training course will enable you to effectively protect your business by simulating the many cyber-attacks that occur throughout your organization.

Discover one of the most popular cybersecurity platforms. Gradually, we'll introduce you to its various features, so that you can use them to protect your infrastructure.

You'll know how to interpret the Huntress dashboard. Access real-time security alerts, manage incidents or investigations, and use remediation tools to solve problems efficiently.

In this course, we'll take a closer look at the phishing simulator. You'll learn how to set up a phishing campaign to test your organization's defenses. We'll also teach you how to use RMM (Remote Monitoring and Management) with ConnectWise and Datto.

We'll also teach you how to implement host isolation to isolate hosts en masse and autonomously, and how to apply Canaries ransomware, a perfect service for detecting potential incidents.

## Objectives

- Understanding Huntress' features and cybersecurity benefits
- Interpret and analyze dashboard figures
- Master remediation tools, including self-remediation, manual remediation and assisted remediation
- Familiarize yourself with phishing simulation, Canary Islands ransomware and antivirus management

## Target audience

- Infrastructure engineers
- System administrators
- Security administrators
- IT Security Managers
- Cybersecurity Analyst

# Prerequisites

Knowledge of cybersecurity.

# Huntress Managed Security Platform training program

## Introduction to Huntress

- Presentation
- Why choose a managed security platform?
- How does Huntress protect your business?
- Features presentation
- Add Huntress to exclusion lists
- Add Huntress to authorized lists
- Solving network problems
- Install Huntress agent

## Dashboard

- Dashboard overview
- Access to security alerts, active incidents and investigations
- Use of remediation tools
- Self-correction
  - Manual remediation
  - Assisted remediation
  - Real-time reporting
- Report presentation and settings
- Send reports to other departments
- Solving breakdown problems

## Administration

- Managing multiple organizations
- User management
- SAML SSO
- Implementation of MFA (Multi Factor Authentication)
- Identifier recovery methods

## Phishing simulation

- SAT presentation
- The benefits of a phishing simulator
- Presentation of different scenarios
- Create a phishing campaign
- The phishing report

## Antivirus management

- Can we use other antivirus programs with Huntress?
- Configuring Microsoft Defender for Huntress
- Complete scans

## RMM

- Introducing ConnectWise
- Automation with ConnectWise
  - Service Agent
  - Billing
  - Internal monitor
  - Remote monitor
- Installing policies with Datto

## Ransomware Canaries

- What you need to know before using Canaries ransomware
- Limitations and technical details
- Launching and disabling ransomware

## Host Isolation

- How insulation works
- Mass insulation
- Self managed isolation
- Sequence of events
- Exclusion

## Troubleshooting

- Check agent status
- Use safe mode
- Script errors
- Measuring disk performance
- Reinstall MFA without backup
- Remove third-party antivirus software

## Companies concerned

This 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 verifies the correct acquisition of skills.

## Sanction

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