Datasheet

# Stamus ND/NDR Capture-the-Flag Training

This course uses a scavenger hunt - style capture-the-flag (CTF) exercise to teach the fundamentals of the Stamus Network Detection and Response (NDR) and Stamus Network Detection (ND) solutions.

The exercise takes place over a 30-day period during which participants are provided with instructor-led training on the Stamus Security Platform (SSP) and given remote access to an SSP system populated with training data. Throughout the 30-day exercise, participants are presented with several challenges that will test their skills while teaching them to use the system.

## Learning Objectives

After completing this course, participants should be able to:

- Comfortably navigate among the various functional elements of the SSP user interface
- Use the SSP cyber kill chain display to identify any assets that may be under attack
- Drill down and pivot on the initial clues to fully investigate a suspected incident, view the timeline of the attack, identify potential offender(s), and set a follow up course of action
- Understand the various asset types (IP, e-mail, or username) and offenders
- Create filters - both include and exclude - based on extensive metadata
- Use filters to tag items as “Informational” and “Relevant” to aid workflow
- Use predefined filters to start a proactive threat hunting session, formulating a hypothesis and investigating
- Understand signatures, IOCs, alerts, Stamus Events and Stamus Threats and how they are used in detection
- Navigate the fields of the host display, where related metadata data associated with a host are collected and presented
- Create custom threat detection logic using filters
- Add new sources of threat intelligence and rulesets

## Who Should Attend

Network security professionals and incident response personnel who expect will use Stamus ND/NDR to detect, investigate, and respond to cyber threats.

## Prerequisites

- A working understanding of networking and network security
- Ability to dedicate at least 2 hours per week for working through the self-paced CTF exercises
- Ability to attend introductory training and weekly team review sessions
- Internet access to connect with the remote Stamus Security Platform
- Positive and curious attitude.

## What's Included

- 30-day access for up to ten (10) users to a hosted Stamus Security Platform
- Industry-appropriate simulated threat data, customized for your environment and preloaded into the CTF-specific SSP system
- Two (2) introductory 1-hour instructor-led training sessions
- Customized set of self-paced CTF questions designed to teach SSP basics and rapid navigation for threat triage, incident response, and proactive threat hunting
- Three (3) weekly 1-hour CTF team review sessions to support the self-paced learning
- Email and/or messaging channel access to Stamus Networks technical support

### ABOUT STAMUS NETWORKS

Stamus Networks believes in a world where defenders are heroes, and a future where those they protect remain safe. As defenders face an onslaught of threats from well-funded adversaries, we relentlessly pursue solutions that make the defender's job easier and more impactful. A global provider of high-performance network-based threat detection and response systems, Stamus Networks helps enterprise security teams accelerate their response to critical threats with solutions that uncover serious and imminent risk from network activity. Our advanced network detection and response (NDR) solutions expose threats to critical assets and empower rapid response.

5 Avenue Ingres
75016 Paris
France

450 E 96th St. Suite 500
Indianapolis, IN 46240
United States

contact@stamus-networks.com
www.stamus-networks.com

 