Darktrace Cyber Security Professional

Partner Training

As part of Darktrace's worldwide Partner Program, Darktrace Education has developed a fast-paced training program that empowers Darktrace Partners to deploy and support Darktrace solutions.

This program consolidates the vital learning objectives taken from our entire training portfolio and combines this with architectural design considerations, deployment and best practices in order to provide an end-to-end training course for security professionals.

Course name: Darktrace Cyber Security Professional

Duration: 2 days

Audience: Darktrace Partner Program Members

Skills: Networking, Network Security, Cyber Security Analytics

Prerequisites: Experience with Network Administration/ Network Security

Training Format: Practical Hand-on course 70%, Theory 30%

Course Outline: This course first examines architectural considerations, installation and best practices before moving on to detailed product training and workflow exercises. The final section of this course builds on the knowledge gained so far and focuses on how to conduct advanced threat hunting that enables security professionals to produce high quality Threat Intelligence Reports.

Course Agenda

Training material is provided for each participant which sets out the tasks and lessons planned. Key objectives include:

1. Learning Objectives

- Introduction and welcome

2. Module I: Installation & Configuration

The Installation and Configuration course covers architectural design considerations, deployment and best practices.

Topics include:

- Architecture
- Sizing
- Installation
- Darktrace Appliance Console Configuration
- Reviewing traffic status in the Threat Visualizer
- Setting up Call Home
- Configuring vSensor
- Configuring osSensor
- Creating Backups

- Restoring from Backups
- Upgrading Darktrace
- LDAP Authentication and Enrichment of User Details
- Configuring HTTPs Certification
- Email Alert Configuration
- User Administration
- Securely erasing captured data on your Darktrace appliance

3. Module II: Threat Visualizer

This module is designed to provide you with a comprehensive guide to using Darktrace's award-winning Threat Visualizer interface. Network security and compliance teams will feel empowered to use this fully featured application and gain unprecedented real-time visibility of networks.

Topics include:

- Threat Visualizer Overview
- Subnet View
- Device View
- Investigating Alerts
- Device details
- Navigation exercise
- Tags
- Advanced Search
- Advanced Search exercises
- TCP Connection States
- Export and API functions
- Creating and editing Models
- A Weighted Model
- Exercise: Creating a New Model
- Whitelisting Domains, IP Addresses and IP Address Ranges
- Watched domains
- Model Tuning
- Searching for Models
- Creating a Packet Capture
- Additional Tools
- RegEx Tester

4. Module III: Threat Intelligence Reporting

The Threat Intelligence Reporting course is designed for security professionals that need to learn how write and submit regular Threat Intelligence Reports (TIRs). Leveraging the Enterprise Immune System's powerful machine learning and AI algorithms, participants will use the Threat Visualizer as a platform to carry out detailed Threat Hunting techniques and learn the craft of creating TIRs that highlight prioritized risks to the organization.

Topics include:

- Darktrace Detection Capabilities
- Overview of latest Threat Visualizer updates and new functionality
- Examples of recent breaches and new threats
- Model changes and experimental Models
- Introduction to Threat Intelligence Report

Models

- Types of Models
- Process to create Models
- Model configuration
- Model Tuning
- Examine Key models, metrics and filters
- Exercise to explain how Models work
- Exercise to understand how different threats trigger differ Models
- Creating Advanced Models

Investigating Anomalies

- Explore the Analyst Workflow
- Threat Visualizer Analysis Levels
- Metadata Analysis in Advanced Search
- PCAP Analysis
- Analyst Toolset
- Exercise: Analyst questions
- Exercise: Anomalous File Investigation

Threat Intelligence Reports

- What is a TIR?
- Threat Indicators
- TIR Security
- TIR Format
- Executive Summary
- Incident Summary
- Incident Details
- Exercise: Create a TIR
- Present findings
- TIR Evaluation

Contact us

If you would like to inquire about our training services or schedule a training session, please do not hesitate to contact us at training@darktrace.com.