Training: Threat Visualizer

The Threat Visualizer course is an essential training program that enables you to get the most out of Darktrace's Enterprise Immune System software. Darktrace's training course ensures that you can maximize the Threat Visualizer's full potential and apply best practice methods that lead to successful deployments.

Combining both theory with practical lessons, the Darktrace training program makes sure the user fully understands the capabilities and features of the software before configuring and running the technology during training.

Darktrace training courses are heavily oriented toward hands-on practical experience to reinforce formal classroom instruction. Using fast-track training methods, the majority of the training will take place in a workshop environment following lessons that will challenge the trainee and aid them during the learning process.

Duration: 1 day

Audience: Network Security Professionals, Cybersecurity Analysts

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

Course Outline: The Threat Visualizer course has been designed to provide you with a comprehensive guide to using Darktrace's award winning Threat Visualizer interface. In just one day, network security professionals will feel empowered to use this fully featured application and gain unprecedented real-time visibility of their network.

Training Objectives: Threat Visualizer is a concise course that introduces Cybersecurity professionals to the key features of the Darktrace Threat Visualizer. Key objectives include:

1. Gain an understanding of Darktrace solutions & architectures.
2. Understand what data Darktrace can capture and analyse.
3. Discover how Darktrace identifies anomalies.
4. Familiarize yourself with the Threat Visualizer interface.
5. Perform investigations using Advanced Search.
6. View and edit Darktrace Models to detect anomalous behaviour.
7. Learn how Darktrace conducts Deep Packet Inspections.
8. Understand the nature of Darktrace Threat Intelligence Reports.

Course Agenda

A fully documented training manual is provided for each participant which set out the tasks and lessons planned.

1. Learning Objectives

Introduction and welcome
Darktrace Overview

2. Introduction to Darktrace

3. Architecture Overview

The Darktrace Appliance
Methods of Ingestion
Ports
Data Flows

Data Mapping
Deployment Types
Darkflow
Connection Metadata
Real-time Metric Collection
Model Blurring
Unidirectional Traffic

4. Threat Visualizer navigation

Threat Visualizer Introduction
Navigation Familiarization
Network Visualizer

5. Subnet View

Viewing a Subnets
Time Selector Overview
Date and Time Options
Adjusting Time Ranges

6. Device View

Viewing devices on a subnet
Interactive Summary

7. Investigating Alerts

Using the Threat Tray
Viewing Alerts
Customizing the Alert View
Viewing Model Breaches
Exploring detailed behaviors
Using the Device Event Log
Visualizing the behavior of peers

8. Device details

Device Summary
Editing device information
Viewing Metrics in graphs
Exploring Similar devices
Navigation exercise

9. Advanced Search

Searching Advanced Metadata
Overview
Launching Advanced Search
Common Columns
Common fields
Frequently used types and their fields
Filtering
Boolean Search
Regular Expressions
Exercises
Export and API functions
TCP Connection States

10. Creating and editing Models

Da rktrace Model Overview
Starting the Model Editor
Viewing Models
A Weighted Model example
Creating a new Model
Adding components to the model
Adding a metric to a component
Adding filters to a metric
Finalizing the new Model
Saving the new Model
Exercise to create a new Model
Model tuning

11. Creating a Packet Capture

Packet Capture Overview
Creating Packet Captures
Viewing and Analyzing Packet Captures

12. Tags

Tag Overview

13. Additional Tools

RegEx Tester
Base64 Converter
PunyCode
Epoch Converter

14. Analyst Workflow

Investigating Breaches

15. Threat Intelligence Reports

TIR Overview

16. Review Learning outcomes

About Darktrace

Darktrace is the world's leading machine learning company for cyber security. Created by mathematicians from the University of Cambridge, the Enterprise Immune System uses AI algorithms to automatically detect and take action against cyber-threats within all types of networks, including physical, cloud and virtualized networks, as well as IoT and industrial control systems. A self-configuring platform, Darktrace requires no prior set-up, identifying advanced threats in real time, including zero-days, insiders and stealthy, silent attackers. Headquartered in San Francisco and Cambridge, UK, Darktrace has 23 offices worldwide.

Contact Us

North America: +1 415 229 9100
Europe: +44 (0) 20 7925 3551
Asia Pacific:+65 6248 4516

Email: info@darktrace.com

www.darktrace.com