Customer 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 analyze.
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 behavior.
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

2. Introduction to Darktrace
   • Darktrace overview

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 subnet
- 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
- Darktrace 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 AI company for cyber defense. With thousands of customers worldwide, the Enterprise Immune System is relied on to detect and fight back against cyber-attacks in real time. The self-learning AI protects the cloud, SaaS, corporate networks, IoT and industrial systems against cyber-threats and vulnerabilities, from insider threats and ransomware, to stealthy and silent attacks. Darktrace has over 800 employees and 40 offices worldwide. It is headquartered in San Francisco, and Cambridge, UK.

Contact Us
Europe: +44 (0) 1223 394 100
North America: +1 (415) 229 9100
Latin America: +55 11 97242 2011
Asia Pacific: +65 6804 5010
training@darktrace.com
darktrace.com