OpenCTI Analyst Essentials

Filigran training course

COURSE SUMMARY

Filigran's OpenCTI Analyst Essentials training is tailored for Cyber Threat Intelligence practitioners and stakeholders, monitoring and investigating threat actors, intrusion sets and campaigns which may target their organization or vertical.

Trainees will learn how to leverage the OCTI platform to search, consult and browse available knowledge at their disposal in order to anticipate and assess the best courses of action needed to enhance their cybersecurity posture within their organization.

LENGTH

1/2 Day

TARGET AUDIENCE

This is a basic/essential course and is recommended for analysts starting to use OpenCTI or decision-makers who would like to be able to follow high level CTI trends in there are of interest.

DELIVERY OPTIONS

This course is available both self-service (online e-learning platform) or instructor-led (remote or on-site).

TOPICS

Introduction to OpenCTI

- What is OpenCTI?
- Approach and usage
- Data model

Platform Header

- Searching for specific information
- Custom dashboards
- Investigation overview
- User profile and subscriptions

Data Exploration and Pivots

- Organization and home dashboard
- Analysis
  - Reports
  - Grouping
  - Notes
  - Opinions
- External references
- Cases
- Events
  - Incidents
  - Knowledge relations and pivots
  - Sightings
  - Observed data
- Observations
  - Observables
  - Artifacts
  - Indicators
  - Infrastructures
- Threats
  - Threat Actors
  - Knowledge inferences
  - Intrusion Sets
  - Campaigns
- Arsenal
  - Malwares
  - Tools
  - Vulnerabilities
- Stakeholders
  - Sectors
  - Locations
  - Identities
- Use cases

ABOUT FILIGRAN

Filigran is a cybertech founded in 2022, providing open source cybersecurity solutions covering threat intelligence management, breach and attack simulation, and cyber risk management.

filigran.io

contact@filigran.io

OpenCTI Analyst Advanced

Filigran training course

COURSE SUMMARY

Filigran's OpenCTI Analyst Advanced training is tailored for Cyber Threat Intelligence practitioners, incident responders and cybersecurity stakeholders, investigating and producing data about threat actors, intrusion sets and campaigns which may target their organization or vertical.

Trainees will learn how to leverage the OCTI platform to capitalize, enrich and disseminate knowledge in order to detect and prepare their organizations to future incidents and large-scale attacks while improving the cybersecurity posture within their organization.

LENGTH

1 Day

TARGET AUDIENCE

This is an advanced course and is recommended for analysts who already know OpenCTI basics or CSIRT/SOC teams which would like to be able to use OpenCTI to handle incidents and threat knowledge.

DELIVERY OPTIONS

This course is available both self-service (online e-learning platform) or instructor-led (remote or on-site).

TOPICS

Ingestion and data management

- Deep understanding of the data ingestion process
  - Architecture and workers
  - De-duplication mechanisms
  - STIX model implementation
- Report construction and capitalization
  - Manual creation
  - Import using parsers / connectors
- Knowledge creation and update
  - Entities and relationships
  - Enrichment

Investigations, dashboards and pivots

- Workspaces
  - Custom dashboards
  - Investigation and pivots
- Complex queries
  - Relationships screen
  - GraphQL API usage

Technical elements

- Indicators versus observables
  - Modelization and extraction
  - Dependencies with rules
- Nested entities and relationships
- Artifacts management

Knowledge dissemination

- Feeds
  - TAXII collections
  - CSV feeds
  - Live and raw streams
- Export
  - Single entity
  - Lists

ABOUT FILIGRAN

Filigran is a cybertech founded in 2022, providing open source cybersecurity solutions covering threat intelligence management, breach and attack simulation, and cyber risk management.

filigran.io
contact@filigran.io