OpenCTI Administrator Essentials

Filigran training course

COURSE SUMMARY

Filigran's OpenCTI Administrator Essentials training is tailored for system administrators, infrastructure owners and technical departments, responsible of maintaining and operating on-premise platform(s).

Trainees will learn how to install, configure and maintain OCTI components and connectors with the aim of maintaining an ecosystem corresponding to the requirements of the teams of analysts and other users of the platform.

LENGTH

1/2 Day

TARGET AUDIENCE

This is an essentials course and is recommended for administrators who are starting deploying and operating OpenCTI and wish to learn the basic installation process and maintenance best practices.

DELIVERY OPTIONS

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

TOPICS

Platform architecture and data ingestion

- Platform architecture overview
- Technical dependencies and databases
  - ElasticSearch
  - Redis
  - S3 bucket / MinIO
  - RabbitMQ
- Internal components
  - Application manager
  - Expiration manager
  - Tasks scheduler
  - Rules engine
  - Synchronization manager
  - Retention manager
  - History manager

Static configuration and parameters

- Platform configuration
- Dependencies configuration
- Internal stream and Redis trimming

Connectors configuration and workers

- Connectors basic configuration
- Specific parameters for connectors
- Workers best practices

Installation and production deployment

- Docker installation
- Manual installation overview
- Production architecture recommendations

Platform runtime configuration and maintenance

- Global parameters
- Roles and capabilities
- Other configurations
- Data management
- Engines management

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 Administrator Advanced

Filigran training course

COURSE SUMMARY

Filigran's OpenCTI Administrator Advanced training is tailored for system administrators, infrastructure owners and technical departments, responsible of maintaining and operating on-premise platform(s) with high value knowledge or important volume of data.

Trainees will learn how to manually install OpenCTI on large-scale architectures, fine tune platform and dependencies configurations as well as handle integration with third parties and troubleshoot data management issues.

LENGTH

1 Day

TARGET AUDIENCE

This is an advanced course and is recommended for administrators who already know OpenCTI basic components behaviors or technical team would like to be able to use deeply integrate OpenCTI with third parties.

DELIVERY OPTIONS

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

TOPICS

Architecture and base code deep dive

- Advance architecture understanding
- Data structure and schema
- Data ingestion mechanisms
  - Connectors data generation
  - Locking and overlaps
  - De-duplication and resolution

Cluster deployment

- Multi-nodes platform
  - Components behavior
  - Workers / frontend load balancing
- Dependencies
  - ElasticSearch
  - RabbitMQ
  - MinIO / S3 buckets
  - Redis

Dependencies configuration

- ElasticSearch optimization
  - Indices configuration
  - Rollover policies
- RabbitMQ tuning
- Redis parameters

Integration with third parties

- Stateless feeds
  - TAXII collections
  - CSV feeds
- Streams
  - Live streams
  - Raw stream

Troubleshooting and data management

- Common errors
- Handling knowledge issues
  - Duplicates and merging
  - Troubleshoot consistency

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