FILIGRAN TRAINING COURSE

OpenCTI Analyst Essentials

Course Summary

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

½ 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 on-demand (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
    - Notes
    - Opinions
    - External references
- 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 Us

Filigran provides cyber threat intelligence, knowledge subsystems and crisis response solutions to thousands of cybersecurity and crisis management teams across the world. By developing open source platforms such as OpenCTI, OpenEx, OpenCrisis, HackMeIfUcan, Filigran actively participates in the defense and the preparation of organizations against the threats and events they fear. Find more information at www.filigran.io, follow us on LinkedIn and Twitter.

FILIGRAN TRAINING COURSE

OpenCTI Analyst Advanced

Course Summary

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

Filigran provides cyber threat intelligence, knowledge subsystems and crisis response solutions to thousands of cybersecurity and crisis management teams across the world. By developing open source platforms such as OpenCTI, OpenEx, OpenCrisis, HackMeIfUcan, Filigran actively participates in the defense and the preparation of organizations against the threats and events they fear. Find more information at www.filigran.io, follow us on LinkedIn and Twitter.

FILIGRAN TRAINING COURSE

OpenCTI Administrator Essentials

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). Students 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

½ 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 on-demand (online e-learning platform) or instructor-led (remote or on-site).

Topics

Platform architecture and data ingestion

- What is OpenCTI?
- 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 Us

Filigran provides cyber threat intelligence, knowledge subsystems and crisis response solutions to thousands of cybersecurity and crisis management teams across the world. By developing open source platforms such as OpenCTI, OpenEx, OpenCrisis, HackMeIfUcan, Filigran actively participates in the defense and the preparation of organizations against the threats and events they fear. Find more information at www.filigran.io, follow us on LinkedIn and Twitter.

FILIGRAN TRAINING COURSE

OpenCTI Administrator Advanced

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. Students 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 on-demand (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 Us

Filigran provides cyber threat intelligence, knowledge subsystems and crisis response solutions to thousands of cybersecurity and crisis management teams across the world. By developing open source platforms such as OpenCTI, OpenEx, OpenCrisis, HackMeIfUcan, Filigran actively participates in the defense and the preparation of organizations against the threats and events they fear. Find more information at www.filigran.io, follow us on LinkedIn and Twitter.