opentext™

Training overview

IR280 EnCase Endpoint Security Training

Training facilities

Ondata International SL
Avenida de Brasil 17, planta 3
28020, Madrid
Tel. 91 417 4468
sales@ondata.es
https://www.ondata.es

Syllabus

Day 1

This course begins with an introduction to OpenText™ EnCase™ Endpoint Security and how it is used in today's business environment. During day one activities, students will walk through the components of the product and begin studying how to use EnCase Endpoint Security to conduct a network-enabled incident response.

On day one, students will learn:

- About the course and course goals and be guided through an introduction to EnCase Endpoint Security.
- How EnCase Endpoint Security benefits corporations and government agencies.
- Current cybersecurity trends and how EnCase Endpoint Security works within a security infrastructure.
- The planning and methodology necessary for network-enabled incident response.
- EnCase Endpoint Security terminology, infrastructure and definitions of included program components and how to create an investigation using the EnCase Endpoint Security web interface and desktop client.

Day 2

Day two begins with a practical exercise on adding groups and targets, creating a new investigation and snapshots and then reviewing the reports. After the practical exercise, the students will learn how to use EnCase Endpoint Security to create Enterprise Scans and the resultant files. Students will then learn how to create a snapshot from within an investigation and navigate both the web and desktop interfaces used in an EnCase Endpoint Security investigation.

The day concludes with a lesson on how to detect questionable activity using preconfigured and custom rules and how to create and import whitelists and blacklists.

On day two, students will:

- Navigate the EnCase Endpoint Security investigation interfaces—web and desktop client.
- Prepare data for escalation to Tier 2 and Tier 3 investigators.
- Use preconfigured and customized rules to detect malicious or suspicious activity.
- Import whitelists and blacklists into EnCase Endpoint Security for use with current and future investigations.
- Add items of interest to the whitelists and blacklists.

opentext™

Day 3

Day three begins with a practical exercise on the skills learned to create and import white and blacklists. Following this, students will learn how to create a job in EnCase Endpoint Security to acquire RAM and then examine the importance of data contained in the Windows® Registry and how to search and acquire that data. Next, the students will be taught how to create conditions to examine compound files. The day will close with a practical exercise on creating conditions.

On day three, students will learn how to:

- Examine and acquire data in RAM.
- Use the Registry Search module of EnCase Endpoint Security.
- Create custom conditions that are not part of the pre-packaged conditions, keywords or matching files conditions.

Day 4

Day 4 begins with instruction on how to use the tools included in EnCase Endpoint Security to conduct a timeline analysis, after which students will learn to identify and address indicators of compromise (IOC) and conduct searches for specific items of interest (IoI). Students will compare two different snapshots and create custom rules for data collection. To close the course, the students will learn how to collect data from multiple targets and remediate known malware and corresponding registry keys and participate in a practical exercise.

On day four, students will learn how to:

- Use the tools included with EnCase Endpoint Security to identify changes to files, processes and ports over a set amount of time.
- Conduct a search to find specific items of interest (IOI) and build a case from the responses.
- Determine an indicator of compromise and create custom IOC rules and an IOC search.
- Compare snapshots with EnCase Endpoint Security and determine what can be accomplished by comparing snapshots at different points in time.
- Create custom data collection rules and collect data from different targets.
- Remediate known malware and registry keys.