DFIR130 OpenText Endpoint Investigator | Endpoint Forensics & Response Training

Syllabus

Training facilities

Los Angeles, CA (Pasadena, CA)
1055 East Colorado Boulevard
Suite 400
Pasadena, CA 91106-2375

Washington, DC (Gaithersburg, MD)
9711 Washingtonian Blvd
6th floor, Room 601 (Paris Room)
Gaithersburg, MD 20878

London, UK (Reading)
420 Thames Valley Park Drive
Earley, Reading
Berkshire RG6 1PT

Munich, Germany (Grasbrunn)
Werner-von-Siemens-Ring 20
85630 Grasbrunn/München
Germany

Day 1

Students will learn how to navigate, filter, sort, search, and process data presented to them in the OpenText™ Endpoint Investigator interface. Students will then look at the advantages of using filters and conditions followed by discussions on various acquisition options. Students will also participate in a practical exercise to reinforce new skills.

On day one, students can expect to:

- Get familiar with OpenText Endpoint Investigator software and its component parts.
- Log into the SAFE from the OpenText Endpoint Investigator desktop client for the first time.
- Learn how to install the OpenText Endpoint Investigator agent.
- Preview remote disks, volumes, and physical memory.
- Use the OpenText Endpoint Investigator Sweep Enterprise function to capture volatile data (running processes, open ports, etc.).
- Use Rapid Preview and the Universal Agent to collect data from endpoints.
- Create custom conditions to filter data.
- Learn how to identify and retrieve target files based on hash values or file system metadata.
- Practice previewing and acquiring endpoints.

Day 2

Students will learn how to perform raw searches. This will be followed by a discussion about how external viewers can be leveraged to view file content that is either not supported natively or viewed better in a third-party application. Students will then create bookmarks that can later be used for the final report.

Students will also discuss how to use the evidence processor and review the results, allowing them to perform index queries. They'll also discuss the use of signature and hash analysis.

The last lesson of the day demonstrates how case reports can be created using the different OpenText Endpoint Investigator bookmarking options. The day concludes with a final exercise.

On day two, students can expect to:

- Perform raw and indexed keyword searching.
- Use external viewers to view the content of files that can't be viewed inside of OpenText Endpoint Investigator.
- Bookmark case information, examination notes, folder structures, evidence items (files, internet artifacts, etc.), raw text, decoded data, transcript data, keyword hits, and tabular data.
- Determine file type using file extensions and file signature analysis.
- Locate files with hash analysis.
- Use the evidence processor to identify email and internet artifacts.
- Understand case and report templates.
- Move and order bookmarks and bookmark folders to create the final case report.

Day 3

On day three, students will be introduced to the OpenText™ Endpoint Forensics & Response web application and its component servers. This software works hand-in-hand with Open Text Endpoint Investigator and the SAFE.

Students will learn how to use the web application to perform tasks while investigating an incident involving onion sites as well as live malware. Instruction also includes acquisition of RAM and automated response tasks performed against collected data.

On day three, students can expect to:

- Manage web application user accounts.
- Download the Universal Agent.
- Manage groups of target (endpoints).
- Create an investigation with a snapshot.
- Navigate the web application.
- Compare point-in-time snapshots.
- Create an automated response task.
- Acquire RAM.

Day 4

On day four, students will focus on incident response as part of digital forensics. Instruction includes learning how to create filters to collect files across the entire environment from endpoints that are connected to the network or those that are not. Afterward, the students will perform a rapid preview of an endpoint and collect files for further analysis.

From the collected files, the students will create indicator-of-compromise filters that may also be run across the entire environment to locate any other endpoints that may contain the same data.

At the end of the course, the students will learn how to respond to endpoints deemed responsive to the filters. This response includes isolating endpoints from the network to prevent further spread of these files and ends with remediation of these files.

On day four, students can expect to:

- Create a filter to collect files based on findings in a snapshot or from a preview.
- Perform a rapid preview and collect data.
- Find items of interest based on the findings in a snapshot.
- Create a filter for indicators of compromise and perform a search using the filter.
- Perform a timeline analysis.
- Search and remediate from the Windows® Registry.
- Isolate an endpoint and remediate malicious processes.