GUIDANCE SOFTWARE

From beginning to endpoint

EnCase® Endpoint Security

INTEGRATED OPEN-SOURCE TOOL KIT

for Incident Responders

We've enhanced EnCase Endpoint Security to strengthen and centralize the incident response process with a robust set of integrations to various open source software, combining the leading forensics and endpoint response platform with powerful, freely available, tools.

The EnCase Integrated Threat Toolkit improves the productivity and speed of your incident response by providing integrations to open source tools in a centralized user console without the burden of having to remember every command line parameter.

EnCase Endpoint Security with open-source tools help speed incident response workflows by:

- Streamlining and optimizing your unique processes
- Organizing incident response analysis and reporting through one central user interface
- Maximizing the capability of each open-source tool by extending reach to all endpoints
- Reducing the learning curve for incident responders by replacing command line operations with "point and click" functionality

experts@guid.com

guidancesoftware.com/endpointsecurity

Incident Responders can be confident in their analysis of ALL endpoint data with EnCase Endpoint Security and its integration with these 16 open source tools:

CYBER ANALYSIS MODULES:

RAM Dump

The acquisition of memory from a target machine. This module will launch EnCase Basic in the background and acquire the image, placing it in a Logical Evidence File (LEF) for future use.

Strings

Uses the System Internals (owned by Microsoft) strings.exe that parses through any file to provide a resulting text file with any ASCII character located in the target file.

MD5 Module

Searches for any MD5 value that is provided individually or in a text file.

RegRipper Module

Allows the user to process multiple Registry Hive files across an endpoint. The Registry hives will be copied into the output folder as native files as well as contained in a LEF for future use. Each "plugin" or "Profile" will be processed against the required hive file, and an output result will be placed in the ToolLogs subfolder for review.

PDF Parser

Uses PDFID to run the Triage, Name Obfuscation and Embedded File plugins—identifying the fundamental elements of PDF files.

Volatility for Windows, Linux and Mac

Uses the Open Source Volatility Framework to parse and analyze memory dumps from the respective systems.

Reverse Shell Module

Provides the ability to create an embedded command shell onto the EITT from a target machine.

Plaso (Log2Timeline and Psort)

Incorporates the Super Timeline Analysis functionality into a GUI Interface.

INVESTIGATIVE SCRIPT MODULES:

MFT Parser

Parses the $MFT on any Windows OS.

MWD Registry Parser

Looks for any type of binary value located in the Windows Registries. It will use a "Blacklist Path" file if provided and will ignore any "Whitelist Path" files.

Prefetch Parser

Parses the Prefetch folder located on Windows OS and looks for any file with the extension of ".pf."

UsnJrnl Parser

Parses the $UsnJrnl on any Windows OS.

Find Temp Executable Search

Searches an Operating System looking for any executables located in any temp directory on the system.

PST Timeline

Gives the ability to process a timeline from a provided PST file.

Malware Entropy Date Range Search

Searches a target system for any file that has an entropy value above the value provided in the Entropy field.

Known Malware Paths

Searches a target system for any file path/extension that is contained in a provided "Blacklist" and/or has an entropy value above the value provided in the Entropy field.

GUIDANCE SOFTWARE

From beginning to endpoint.

ABOUT GUIDANCE

Guidance exists to turn chaos and the unknown into order and the known-so that companies and their customers can go about their daily lives as usual without worry or disruption, knowing their most valuable information is safe and secure. The makers of EnCase®, the gold standard in forensic security, Guidance provides a mission-critical foundation of market-leading applications that offer deep 360-degree visibility across all endpoints, devices and networks, allowing proactive identification and remediation of threats. From retail to financial institutions, our field-tested and court-proven solutions are deployed on an estimated 33 million endpoints at more than 70 of the Fortune 100 and hundreds of agencies worldwide, from beginning to endpoint.