GUIDANCE SOFTWARE

From beginning to endpoint.

EnCase® Endpoint Security

IOC INVESTIGATIONS WITH ENCASE ENDPOINT SECURITY

Indicators of Compromise (IOCs) are forensic artifacts that reveal activity or the presence of factors that often indicate the compromise, or attempted compromise, of endpoint devices. Common IOCs include virus signatures, IP addresses, MD5 hashes of malware files, or domain names of botnet command and control servers. Scanning systems for the presence of IOCs is an effective way to identify any attempts to breech your enterprise.

"IOC support augmented by the depth and breadth of visibility provided by EnCase Endpoint Security enables us to locate IOCs in a more comprehensive manner than with any other solution on the market."

–Fortune 100 Global Automobile Manufacturer

experts@guid.com

guidancesoftware.com

Every action taken on a computer leaves forensic residue, and an IOC alert is often the first warning of a potential compromise on your system, making these analyses invaluable for incident response teams. The presence of IOCs doesn't necessarily mean compromise, but they should always be investigated promptly to help investigators understand if a breach has occurred. Databases and tools exist to support IOC detection, two of the most commonly leveraged are:

- Structured Threat Information Expression (STIX), a database of definitions of indicators of compromise
- YARA, a similar database that helps malware researchers and incident responders identify and classify malware samples

Effective, one-click IOC investigation

EnCase Endpoint Security ingests both STIX definitions and YARA rules as filtering criteria to detect and validate IOCs across the enterprise. With Endpoint Security, security teams can run a one-click query across the network, identify indicators on potentially infected hosts, and fully remediate threats.

EnCase Endpoint Security also locates known blacklisted items and employs behavior analysis to locate unknown and yet-to-be blacklisted items on the network.

Endpoint Security provides kernel-level visibility of all activity at the endpoint to dramatically increase the effectiveness of incident responders. Other, non-forensic security, solutions cannot identify IOCs located in unallocated disk space or areas of the disk outside of user space. When IOCs are found on the network, suspect endpoints can be easily investigated to verify malicious code. Security Teams can then locate other infected machines and surgically, and remotely, remediate the threat from endpoint devices.

EnCase Endpoint Security provides a complete set of tools to assist responders with threat hunting, detection, and complete remediation. Our solution empowers responders to successfully address any incident.

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.