

EnCase[®] Automated Incident Response Solution

Complete your IR process by automating response,
enabling razor-sharp diagnosis and achieving thorough remediation...

“*EnCase Enterprise is the best out there for incident response and compromise assessments. Before we deployed EnCase Enterprise, it took 2 hours to review a workstation during a security incident. Now it only takes 15 minutes. You can find out where they've been and what they did. You can determine the origin of a malicious incident immediately. I can scan my entire network for malicious processes in about 6.5 seconds.*”

*Deputy Director, IRM Office and ISSO
U.S. Federal Agency*

Integrate with these
alerting technologies:

Snort[®]

Vontu[®]

Vericept

ArcSight

ISS

and more...

Intrusion detection systems (IDS), security information management tools (SIM), content monitoring systems (CMS) and other alerting technologies kick out hundreds to thousands of alerts each day. Yet, no organization has the resources to track and diagnose every high-priority alert or employee policy violation. That interval of time between an event's occurrence and your response is when vital information becomes stale and real damage occurs. With manual procedures and tools that aren't integrated, by the time you determine which alerts are meaningful, it's often too late.

How quickly can you
identify meaningful alerts?

How long does it take you to
zero in on the origin
of the incident?

Are you able to **pinpoint all**
affected machines across your network?

Are you able to **diagnose an incident** to
determine exactly what happened?

How confident are you in your ability to
remediate thoroughly?

EnCase[®] Automated Incident Response Solution (AIRS) integrates with your existing alerting systems to deliver real-time response, diagnosis and remediation...

Alerting System Integration

AIRS automates the incident response process by allowing you to define custom logic to query a wide variety of event response repositories at given intervals and for specific types of events. This gives you the flexibility to define specific event attributes that are often found in high-priority events or policy violations, thereby optimizing your ability to defend against them.

Dynamic Forensic Analysis

Content Monitoring Systems identify policy violations and unapproved-user activity from a network perspective. That is only part of the picture, as analysts are often left to follow up on user-policy infractions manually. AIRS triages CMS alerts and automatically kick-starts the investigation process by analyzing suspect machines to eliminate false positives or locate and preserve temporary artifacts. Examples of these events include email attachments containing intellectual property, unapproved applications and URLs of inappropriate websites.



The web interface delivers unprecedented visibility and analysis:

- Identify the machines running unapproved, malicious or hidden processes
- Identify all open ports and the associated processes
- Identify injected DLLs
- Associate DLLs with the relevant load process
- Filter snapshots to display the state of a machine over the course of time
- Conduct differential snapshot reporting on the fly
- Perform web searches to investigate unknown processes
- Conduct IANA port searches to identify common protocols that run over a given port

Automated Incident Response

As alerts from security monitoring systems are created, AIRS automatically takes snapshots of all hosts involved in the event. Immediate analysis from the “machine’s” view provides deep visibility into a machine’s state, revealing known, unknown and hidden processes, as well as running DLLs and network socket information — automatically delivering the critical data you need.

Incident Impact Analysis and System Baseline

AIRS has the unique ability to take multiple snapshots and correlate a system’s data across time, providing a detailed analysis of an attack against a machine or set of machines. Additionally, you can snapshot machines (usually servers) in their pristine state to capture normal running behavior. Then, during an investigation, AIRS provides quick differential analysis to deliver relevant information about the compromised machine. This significantly decreases the amount of time required for investigations, as a server’s volatile data does not deviate much during normal operations.

DEPTH OF ANALYSIS	EnCase IR/ Compromise Assessment	Typical Auditing Tools
Detect Running Processes	✓	✓
Detect Hidden Processes	✓	✗
Detect Renamed Processes or Drivers	✓	✗
Detect Running Services	✓	✓
Detect Malicious Injected DLLs	✓	✗
Detect Rootkits	✓	✗
Identify Current Logged-on User	✓	✓
Enumerate Autostart Registry Keys	✓	✗
Detect Hidden Ports	✓	✗
Identify Hidden Registry Keys	✓	✗
Map Ports to Processes	✓	✗
Provide Detailed Reporting	✓	✗
Create Machine Profiles	✓	✗

Web-based Incident Analysis

AIRS’ web-based investigative console provides an easy-to-use interface to correlate real-time, dynamic investigative information, which includes volatile data, forensic analysis and alerting system data. This allows you to quickly and effectively drill down into specific events to determine which are most critical, without bouncing between multiple security tools and logs or having to visit suspect machines. The web interface also provides information on historical events, snapshot data and dynamic forensic analysis for reference during investigations.

Web-based Workflow Management

Work flow management is provided in the web interface to allow the assignment of EnCase Enterprise investigations to specific individuals. Groups and users can be defined by administrative or user level and with jurisdiction over certain portions of the network.

About Guidance Software

Guidance Software is recognized worldwide as the industry leader in digital investigative solutions. Its EnCase® platform provides the foundation for government, corporate and law enforcement organizations to conduct thorough and effective computer investigations of any kind, such as intellectual property theft, incident response, compliance auditing and responding to eDiscovery requests—all while maintaining the forensic integrity of the data. There are more than 20,000 licensed users of the technology, and thousands of investigators and corporate security personnel attend Guidance Software’s forensic methodology training annually. Validated by numerous courts worldwide, EnCase software is also frequently honored with top security awards and recognition from eWEEK, SC Magazine and Network Computing, as well as the Socha-Gelbmann survey.

©2007 Guidance Software, Inc. All Rights Reserved. EnCase and Guidance Software are registered trademarks or trademarks owned by Guidance Software in the United States and other jurisdictions and may not be used without prior written permission. All other marks and brands may be claimed as the property of their respective owners.