

## The Underlying Challenge

To combat the growing number, frequency, and sophistication of malicious attacks, enterprises have made large investments in security technologies. Collectively these devices generate a flood of raw security information, literally billions of events per day. Security analysts and SOC/NOC operators are then tasked with monitoring the sea of alerts and false positives generated by devices like IDS, IPS, routers, and switches to qualify and detect incidents that warrant further investigation. However, given the different consoles, logging standards, and log access protocols, any manual approach at log monitoring, threat detection and response becomes an exercise in futility. Effectively most real threats go unnoticed and the large security investments made by enterprises remains largely untapped.

These challenges are only compounded by a growing regulatory landscape and the increased incidence of and concern around insider threats. Regulatory mandates and insider threats have necessitated the addition of operating systems, databases, and a slew of applications to the existing roster of log sources that need to be monitored and analyzed. Audit, compliance and IT governance are major requirements for all enterprises and the need to centrally collect, monitor, respond and report on security event data is now more important than ever. Enterprises need an effective solution that can provide a single, integrated solution enabling them to collect, correlate and manage massive amounts of security data across heterogeneous sources for real-time monitoring and real time response.

While SIM (Security Information Management) solutions automate event data consolidation and correlation across security event data sources, targeted investigation of hosts is often accomplished through forensic tools that support broad credentialed scanning capabilities. The collaboration between ArcSight and Guidance combines the leading solutions across Enterprise Security Management and forensics investigation, enabling a stronger and more integrated approach to automated threat detection and response.

## ArcSight ESM

ArcSight ESM (Enterprise Security Management) provides real time visualization and monitoring of security events across security devices, network devices, operating systems, databases, and application. ESM includes a host of tools, features and functions to enable:

- Optimized collection of event data from over 140 distinct products out of the box
- SDK driven connectors to incorporate in-house or non-traditional data sources
- Real time cross device and device independent correlation and threat visualization
- Incorporation of vulnerability scanner data to account for threat relevance and asset susceptibility
- Rapid investigation for root cause analysis of security issues and breaches
- Workflow and remediation for reduced response time and minimization of damage
- Packaged and ad hoc role based reports for security and compliance stakeholders
- High-availability and scalability in event monitoring for the largest of environments

## Guidance EnCase Enterprise

Guidance EnCase Enterprise enables computer investigations by providing immediate response and thorough analysis of servers and workstations anywhere on a wide area network. EnCase Enterprise provides a scaleable integrated platform to immediately respond to and investigate computer-related incidents through:

- Capture and analysis of volatile data, including active network sessions, open files and running processes
- A single tool to investigate and analyze computers running on Windows, Linux and Solaris
- Secure analysis of machines over the LAN/WAN from a central location
- Investigation and analysis of multiple machines simultaneously at a disk level

- Acquisition and preservation of data in a forensically sound manner
- Auditing of machines to detect whether they have been compromised by malicious attacks
- Identification and remediation of Windows-based kernel rootkits

## The ArcSight ESM & Guidance EnCase AIRS Integrated Solution

ArcSight ESM gathers security related events from network devices, security devices, operating systems, databases, and applications in real time. This information is normalized and categorized as it is collected and then processed by the rules engine within the ArcSight ESM Manager. Events within and across devices are correlated to detect perimeter threats, compliance violations, as well as insider threats. Suspicious activity is triggered when the conditions of a rule are met, in turn generating a correlated event and alert. The user has various interactive visual views into such security activity, ranging from live grids, graphs, monitors, dashboards, and maps.

Guidance EnCase AIRS, an add-on module to Guidance EnCase Enterprise, provides the ability to bring additional information stored in the volatile RAM memory of investigated hosts, into the overall threat detection and response process in real time. This is facilitated by EnCase AIRS' ability to take ad hoc or interval based snapshots of target and/or attacker machines. The snapshot contents reveal details of known, unknown and hidden processes, TCP network socket information, open files and other threat relevant data.

By dynamically exposing this information in the ArcSight console for correlated events, ArcSight users have greater knowledge on the live state of the source and target machines involved in an impending threat. Combining such state related information in real time with the details of the correlated event from ArcSight enables greater reduction of false positives and accuracy in tracking compromised hosts.

For example, information on active processes is critical when trying to identify whether rogue, unknown or unauthorized processes, services or

drivers are active and running on a system. Similarly, knowing all files that are open can reveal the information an application or suspect is accessing. In some cases, malicious applications hide information about running processes and network connections, but cannot conceal open files which are stored in RAM. Registry information can provide relevant details on auto-run keys, devices, installed software, build information, networking details, user information and hardware. And active user information provides details on all users who have logged onto a machine.

## Benefits of an Integrated ArcSight ESM & Guidance EnCase AIRS Solution

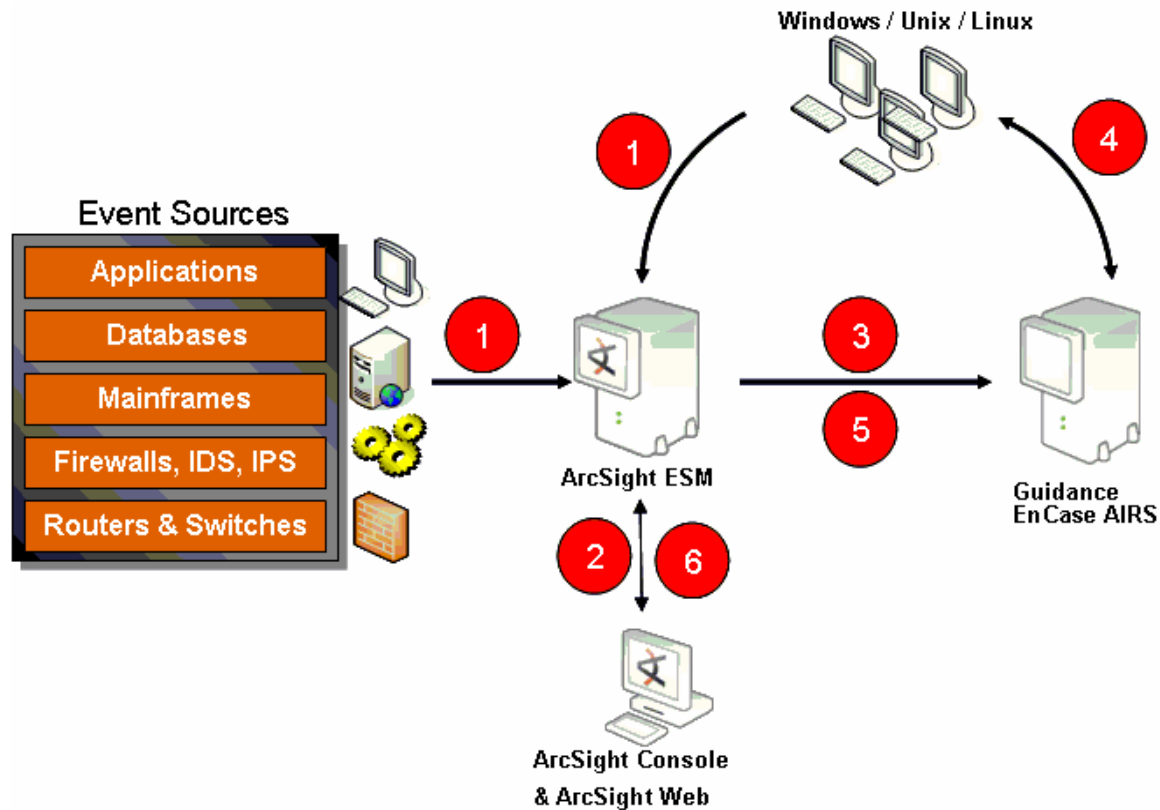
Integrating the ArcSight ESM and Guidance EnCase AIRS solutions brings together the world's leading Enterprise Security Management and Enterprise Investigative Infrastructure solutions. The integrated solution allows organizations to automate the self-learning process of detecting, resolving and preventing threats to the network.

The collaboration between ArcSight and Guidance Software Inc. minimizes human intervention for organizations, since they can now automate and expedite the time sensitive incident response and evidence collection phases. Additionally, the self-learning aspect of this integrated solution provides a closed-loop process that allows organizations to look for an ever-increasing number of anomalies and threats when monitoring the security events across their enterprise.

## Summary

The ArcSight – Guidance collaboration leverages the strengths of both offerings to provide greater intelligence in threat detection and future prevention. With the integrated offering, ArcSight can invoke EnCase to investigate specific hosts and EnCase in turn automatically injects the added intelligence regarding impacted hosts in real time into ArcSight's monitoring data stream, reducing false positives further and enhancing the accuracy in detecting compromised hosts and the extent of threat propagation without added human intervention.

The flow of information between ArcSight and EnCase AIRS is depicted and described below:



1. ArcSight ESM monitors enterprise wide security event data from a wide variety of sources including hosts, periodically triggering and displaying correlated events that suggest suspicious activity or an impending threat.
2. To gather more information on attacking or targeted hosts, the ArcSight user can trigger an investigation to be performed by EnCase - directly from within the ArcSight interface. These investigations can be triggered based on rule violations or based on IP addresses.
3. ArcSight exports information regarding the hosts that need to be investigated into a database, including: IP addresses, name of the triggered rule, event time, offending ports, and file names that might have been involved in the violation.
4. EnCase monitors the database for new events and upon seeing an event of interest, a snapshot is taken of the target host/s specified. The snapshot captures threat relevant volatile data in real time, including: open files, open ports, active processes, drivers and services, active (logged on) users, active registry hives, and NIC information (IP, MAC, subnet mask, NIC manufacturer)
5. EnCase writes the snapshot data to a database for retrieval by the ArcSight Manager
6. ArcSight picks up the investigation results from the database and displays them to the requesting user. Going forward, these anomalies will now be part of the ArcSight rules library, so that they can be identified across the system before a forensic investigation is needed.