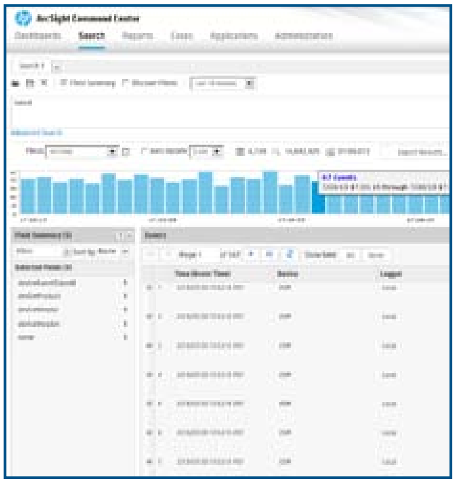
Solution Brief

Intelligent Incident Response System

ArcSight Express + EnCase® Cybersecurity
Prioritized Detection + Automated Response in a Single Package



ArcSight Express allows you to correlate events feeds across a wide variety of detection systems

Streamline your post-detection workflow with HP ArcSight Express and EnCase Cybersecurity:

- Prioritize alerts
- Eliminate False Positives
- Determine incident scope
- Assess sensitive data impact
- Zero in on the origin of an incident
- Remediate endpoints

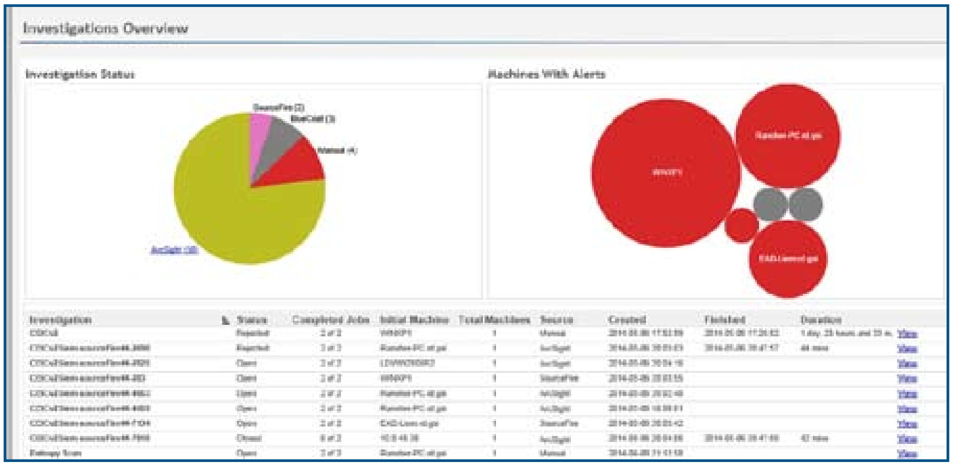
Your organization has invested in people, processes and technology designed to prevent malicious access to your network and endpoints — yet the volume of alerts generated from disparate point solutions calls for similar investments to manage, prioritize and respond to the deluge of alerts your limited security resources are responsible for analyzing every day.

This is an urgent problem where the existing approach is untenable — attacks continue to compromise the sensitive data of well-defended networks while security teams are overwhelmed with a backlog of countless alerts. To keep pace you need to:

- Quickly understand which alerts are meaningful
- Initiate automatic response actions for those deemed to pose the most risk to your valuable digital assets
- Address these threats without bringing down the very systems responsible for running your business.

HP and Guidance Software have combined forces to deliver a complete, best-of-breed post-event workflow designed to automatically prioritize and respond to the most critical alerts. The combined solution allows you to:

- Aggregate and correlate multiple event feeds to identify the most critical threats
- Validate the efficacy of threats
- Immediately understand impact to sensitive data
- Acurately assess the scope of the intrusion
- Remediate threat from affected endpoints with no disruption



Investigation	Status	Completed Jobs	Initial Machine	Total Machines	Source	Created	Finished	Duration	
[illegible]	Rejected	2 of 2	WINXP1	1	Manual	[illegible]	[illegible]	1 day, 23 hours and 33 m..	View
[illegible]	Rejected	3 of 3	Random-PC.et.gsi	1	ArcSight	[illegible]	[illegible]	44 mins	View
[illegible]	Open	2 of 2	[illegible]	1	ArcSight	[illegible]			View
[illegible]	Open	2 of 2	WINXP1	1	SourceFile	[illegible]			View
[illegible]	Open	2 of 2	Random-PC.et.gsi	1	ArcSight	[illegible]			View
[illegible]	Open	2 of 2	Random-PC.et.gsi	1	ArcSight	[illegible]			View
[illegible]	Open	2 of 2	EAD-Lion.et.gsi	1	SourceFile	[illegible]			View
[illegible]	Closed	[illegible]	[illegible]	1	ArcSight	[illegible]	[illegible]	42 mins	View
Entropy Scan	Open	2 of 3	Random-PC.et.gsi	1	Manual	[illegible]			View

Within EnCase Cybersecurity validate alerts and review endpoint data related to a alert

With this best-of-breed solution, organizations can respond quickly and effectively while reducing costs related to inefficient analysis of forensic data after a breach. Your ability to validate events, prioritize incidents and lower your response time is vital to keep related costs in check and ensure your ability to understand the scope and impact of any security incident before the trail runs cold or further damage is done.

How quickly can you respond to an incident?
How rapidly can you reduce false positives?
Can you immediately determine the impact to sensitive data?
How long does it take you to zero in on the origin of an incident?
Do you have the information you need to effectively prioritize alerts?

Integrating Event Management with Response

Guidance Software's EnCase Cybersecurity automates the incident response process by allowing you to augment rules in ArcSight with the ability to trigger a variety of response options based on specific alert criteria being met. For instance if an unauthorized user logs in to the network, EnCase Cybersecurity can be configured to capture relevant system information at the time the user logs in and correlate that back in the ArcSight user console, providing context around what was occurring at the time the unauthorized user was logged in.

Guided Forensics

Many perimeter solutions integrated with ArcSight identify policy violations and unapproved user activity from a network perspective. That is only part of the whole picture, as analysts are often left to follow up on user-policy infractions manually. ArcSight Express coupled with EnCase Cybersecurity idenfifies and triages the highest priority alerts — automatically kick starting an investigation process by analyzing suspect machines to eliminate false positives or locate and preserve otherwise temporary artifacts. Examples of these events include email attachments containing intellectual property, unapproved applications and URLs of inappropriate websites.

Automated Response

As alerts from perimeter and network security solutions are created, EnCase Cybersecurity can be configured to automatically take snapshots of all hosts involved in the event. This ensures a real-time glimpse into the state of the computer at the time of the alert, revealing known, unknown and hidden processes, as well as running DLLs and network socket information – automatically delivering the critical data you need to prioritize alerts and address the highest areas of risk before damage occurs.

About Guidance Software (NASDAQ: GUID)

Guidance Software is recognized worldwide as the industry leader in digital investigative solutions. Its EnCase® Enterprise platform is used by numerous government agencies, more than 65 percent of the Fortune 100, and more than 40 percent of the Fortune 500, to conduct digital investigations of servers, laptops, desktops and mobile devices. Built on the EnCase Enterprise platform are market-leading electronic discovery and cyber security solutions, EnCase eDiscovery, EnCase Cybersecurity, and EnCase Analytics, which empower organizations to respond to litigation discovery requests, perform sensitive data discovery for compliance purposes, conduct speedy and thorough security incident response, and reveal previously hidden advanced persistent threats or malicious insider activity. For more information about Guidance Software, visit www.encase.com.