AUTOMATE INCIDENT RESPONSE WITH HP ARCSIGHT ESM AND ENCASE ENDPOINT SECURITY

KEY BENEFITS

- Prioritize response with real-time data from potentially affected endpoints
- Validate which potentially affected endpoints are running unapproved, malicious or hidden processes
- Identify all open ports, associated processes and other temporary data at time of alert
- Associate DLLs with the relevant load process, reveal injected DLLs
- Determine if affected endpoints are storing sensitive data

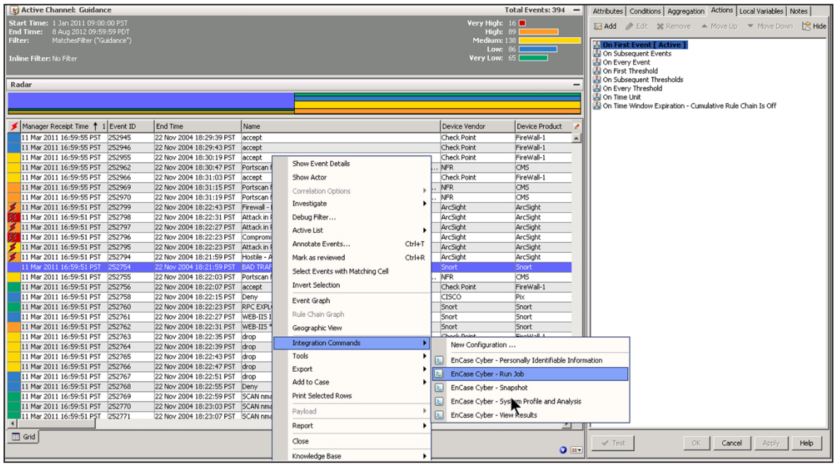
With the proliferation of perimeter and network seurity solutions, your HP ArcSight SIEM platform is receiving countless events per day which translates into an ever growing number of alerts. The sheer volume of alerts makes it difficult to prioritize, track and diagnose every high-priority alert or staff policy violation. Your ability to prioritize and lower your response time is vital as often artifacts on a computer only exist for a small period of time. Therefore, the capture of relevant data is critical before the trail runs cold. Without the integration of alerting and response technologies by the time you determine which alerts are meaningful, it could be too late.

How quickly can you respond to an incident?

How rapidly can you reduce false positives?

Do you have the information you need to effectively prioritize correlated events?

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



Active Channel: Guidance — Total Events: 394

Start Time: 1 Jan 2011 09:00:00 PST
End Time: 8 Aug 2012 09:59:59 PDT
Filter: MatchesFilter ("Guidance")

Inline Filter: No Filter

Very High: 16
High: 89
Medium: 138
Low: 86
Very Low: 65

Radar

Manager Receipt Time	Event ID	End Time	Name	Device Vendor	Device Product
11 Mar 2011 16:59:55 PST	252945	22 Nov 2004 18:29:39 PST	accept	Check Point	FireWall-1
11 Mar 2011 16:59:55 PST	252946	22 Nov 2004 18:29:43 PST	accept	Check Point	FireWall-1
11 Mar 2011 16:59:55 PST	252955	22 Nov 2004 18:30:19 PST	accept	Check Point	FireWall-1
11 Mar 2011 16:59:55 PST	252962	22 Nov 2004 18:30:47 PST	Portscan f	NFR	CMS
11 Mar 2011 16:59:55 PST	252966	22 Nov 2004 18:31:03 PST	accept	Check Point	FireWall-1
11 Mar 2011 16:59:55 PST	252969	22 Nov 2004 18:31:15 PST	Portscan f	NFR	CMS
11 Mar 2011 16:59:55 PST	252970	22 Nov 2004 18:31:19 PST	Portscan f	NFR	CMS
11 Mar 2011 16:59:51 PST	252799	22 Nov 2004 18:22:43 PST	Firewall -	ArcSight	ArcSight
11 Mar 2011 16:59:51 PST	252798	22 Nov 2004 18:22:31 PST	Attack in	ArcSight	ArcSight
11 Mar 2011 16:59:51 PST	252797	22 Nov 2004 18:22:27 PST	Attack in	ArcSight	ArcSight
11 Mar 2011 16:59:51 PST	252796	22 Nov 2004 18:22:23 PST	Compromi	ArcSight	ArcSight
11 Mar 2011 16:59:51 PST	252795	22 Nov 2004 18:22:23 PST	Attack in	ArcSight	ArcSight
11 Mar 2011 16:59:51 PST	252794	22 Nov 2004 18:21:59 PST	Hostile - A	ArcSight	ArcSight
11 Mar 2011 16:59:51 PST	252754	22 Nov 2004 18:21:59 PST	BAD TRAF	Snort	Snort
11 Mar 2011 16:59:51 PST	252755	22 Nov 2004 18:22:03 PST	Portscan f	NFR	CMS
11 Mar 2011 16:59:51 PST	252756	22 Nov 2004 18:22:07 PST	accept	Check Point	FireWall-1
11 Mar 2011 16:59:51 PST	252758	22 Nov 2004 18:22:15 PST	Deny	CISCO	Pix
11 Mar 2011 16:59:51 PST	252760	22 Nov 2004 18:22:23 PST	RPC EXPL	Snort	Snort
11 Mar 2011 16:59:51 PST	252761	22 Nov 2004 18:22:27 PST	WEB-IIS I	Snort	Snort
11 Mar 2011 16:59:51 PST	252762	22 Nov 2004 18:22:31 PST	WEB-IIS *	Snort	Snort
11 Mar 2011 16:59:51 PST	252763	22 Nov 2004 18:22:35 PST	drop	Check Point	FireWall-1
11 Mar 2011 16:59:51 PST	252764	22 Nov 2004 18:22:39 PST	drop		
11 Mar 2011 16:59:51 PST	252765	22 Nov 2004 18:22:43 PST	drop		
11 Mar 2011 16:59:51 PST	252766	22 Nov 2004 18:22:47 PST	drop		
11 Mar 2011 16:59:51 PST	252767	22 Nov 2004 18:22:51 PST	drop		
11 Mar 2011 16:59:51 PST	252768	22 Nov 2004 18:22:55 PST	Deny		
11 Mar 2011 16:59:51 PST	252769	22 Nov 2004 18:22:59 PST	SCAN nma		
11 Mar 2011 16:59:51 PST	252770	22 Nov 2004 18:23:03 PST	SCAN nma		
11 Mar 2011 16:59:51 PST	252771	22 Nov 2004 18:23:07 PST	SCAN nma		

EnCase Endpoint Security integrates with your HP ArcSight SIEM to deliver real-time response, diagnosis and remediation

SIEM Integration

EnCase Endpoint Security automates the incident response process by allowing you to augment rules in HP 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 Endpoint Security can be configured to capture relevant system information at the time the user logs in and correlate that back in the HP ArcSight user console, ensuring an accurate view of what was occurring at the time the unauthorized user was logged in.

hp ArcSight Action Certified 2014

"EnCase is the best out there for incident response and compromise assessments. Before we deployed EnCase, it took two 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."

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

Dynamic Forensic Analysis

Many perimeter solutions integrated with HP 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. EnCase Endpoint Security triages these alerts and automatically kick starts 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 Incident Response

As alerts from perimeter and network security solutions are created, EnCase Endpoint Security 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

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.