HP NonStop Customer Technical Talk

HP NonStop Server Security and HP ArcSight SIEM

04/12/2012

HP NonStop – Karen Copeland
HP Enterprise Security – Morgan DeRodeff
XYPRO – Barry Forbes

NonStop Enterprise Division
Agenda

- Topic Introduction
- HP’s ArcSight SIEM Solution
- Integration with NonStop using Merged Audit
- Q & A
Introduction

This presentation describes HP’s recent integration with HP ArcSight SIEM for security monitoring of HP Integrity NonStop servers.

This integration is available to customers as of February 2012.
Cyber crime is increasing...

2011 was the worst year for security breaches
Today’s Cybercrime Is Different

## Attacks
- Smart Humans
- High Value Targets

## Defenses
- Signatures Ineffective
- No Choke Point

## Vulnerabilities
- Key Systems Unwatched
- Key Users Unmonitored

Business faces more risk than ever.

Traditional defenses won’t work.

A different approach is required.
Verizon Breach Report

An advance look at Verizon’s 2012 Breach Report expected out this summer.

This graph shows that hacking increased in 2011 while malware declined slightly.

System monitoring challenges today

Review of the sheer volume of event and security data generated on most enterprise systems is a daunting task without sophisticated tools.

The small event that gets missed might be the one that allows a breach to occur.
Integration with HP ArcSight SIEM

- Security analytics for HP Non-Stop Servers
- Reduce cost handling security incidents
- Streamline regulatory compliance

Now available from HP
HP Enterprise Security
Security Intelligence Platform
HP ArcSight SIEM
HP Enterprise Security

Market leading products and services

- Security Information and Event Management
- Log Management
- Application Security
- Network Security
- Data Protection
- Threat Research
- Security Services
HP has the only security intelligence platform that gives clients the insight to proactively manage their specific enterprise threats and risks.
Customers Nearing 10,000
HP Security Intelligence Platform

- **Establish** complete visibility across all applications and systems

- **Analyze vulnerabilities** in applications and operations to understand risk

- **Respond adaptively** to build defenses against the exploitation of vulnerabilities

- **Measure security effectiveness and risk** across people, process, and technology to improve over time
Role of a SIEM
(Security Information and Event Management)

Security Events
millions of events/day

Security Incidents
prioritized alerts or incidents/day

Response Actions
automated remediation and forensics analysis

Who brought the web-site down?
Who leaked financial data?
Who made fraudulent banking transactions?

Determine source and scope of attack
Block source IP-address at Firewall or IPS
Create trouble-ticket for security incident for further investigation

Monitored Devices
HP ArcSight SIEM
HP or 3rd Party Controls
HP ArcSight SIEM Platform

A comprehensive platform for monitoring modern threats and risks

- **Capture** any data from any system
- **Manage** and store every event
- **Analyze** events in real time
- **Identify** unusual behavior
- **Respond** quickly to prevent loss
NonStop Server events processed by HP ArcSight

HP ArcSight SIEM

Correlation  Forensics  Reporting

NonStop Events passed by Merged Audit (CEF* Certified)

- LOGON-SUCCESS
- LOGON-FAILURE
- LOGOFFS
- SECURITY-CONFIG
- SOFTWARE-NORM-MSGS
- USERID-MAINT
- PRIV-ACTION-HLR
- PRIVILEGED-ACTION
- OBJ-ACCESS-PASS
- OBJ-ACCESS-FAIL

- AUDIT-LOG-INIT
- AUDIT-FAILURE
- NETWORK-CONNECT
- XYGATEHE-CONNECT
- XYGATEAC-SUCCESS
- XYGATEAC-FAILURE
- XYGATE-CATCHALL-SUCCESS
- XYGATE-CATCHALL-FAILURES
- HLR-FAILURE
- BASE24-CATCHALL
- SYSLOG-UNCATEGORIZED-EMS

* CEF = ArcSight Common Event Format
HP ArcSight Dashboard: NonStop Events
HP ArcSight: Provides Situational Awareness

Traditional Security Monitoring

- IP Address
- Data
- Asset Data
- Scan Data
- Location

HP’s Hybrid Security Monitoring

- Attributes
- User Actions
- User
- Data
- App
- Roles
- Changes
- Txns
- Access Rights
HP ArcSight: User and Departmental Risk Monitoring
HP ArcSight: User and Departmental Risk Monitoring
Why HP Enterprise Security Products

- Industry-leading, automated security solutions and visibility
  - HP ArcSight SIEM, Fortify, TippingPoint all MQ Leaders/Best in Class
  - Security intelligence delivered in context
  - Trusted, proactive and automated action
  - Cloud-ready

- World’s best research for security intelligence and risk management
  - Best in class application security and network security research
  - Discovers more vulnerabilities than the rest of the market combined

- Integrated with leading IT operations solutions
  - Universal Log Management tied to Systems Event Management
  - Enhanced asset and threat modeling
  - A key component of the HP IT Performance Suite
HP NonStop Servers
and XYGATE Merged Audit
HP NonStop and XYGATE Merged Audit

• Recently HP began shipping XYGATE Merged Audit to customers as part of a bundle of security products to enhance the Integrity NonStop Operating System, Mission Critical Edition.
• All systems shipped after Sept 2010 automatically include the OS Security product bundle.
• HP and XYPRO jointly support Merged Audit for customers.
• The security bundle can be ordered by customers who purchased their system prior to Sept 2010.
• Merged Audit has been enhanced in J06.13 and H06.24 to deliver NonStop events to the HP ArcSight SIEM Solution.
XYGATE Merged Audit (XMA)

Features

- Part of the XYGATE Suite of products, XMA is a well-established product available for the NonStop market for 10 years.
- A single repository on the NonStop for audit data from multiple sources.
- Reports on NonStop server security activities using predefined or customized reports.
- Helps you prepare for PCI audits or for periodic security reviews.
- Collects data for a single NonStop server or multi-server view.
- Filters allow you to extract selected data
- Supports customizable security alerts
- Collects ACI Base24 events (optional)
- Collects HP Home Location Registry (HLR) events (optional)
- Feeds data to enterprise audit tools & systems
- Formats and feeds data to HP ArcSight SIEM
- Certified as of XMA release T0928AAD (XYGATE Merged Audit 1.83).

PCI/DSS 10.5.3 calls out collection of “audit data in a centralized log server or media that is difficult to alter.”
NonStop servers are now certified through the use of XYGATE Merged Audit to integrate NonStop events into HP ArcSight SIEM.

- The XYGATE Merged Audit team worked closely with the HP ArcSight team to complete the HP ArcSight CEF certification process which ensures that NonStop events are properly integrated into ArcSight SIEM.
- Filters were designed to format security-related audit events on the NonStop server to meet the CEF standard.
- NonStop data now appears in the correct schema fields within the ArcSight platform so it can be correlated with events from other sources and feed dashboards and reports.
- A free log adapter is needed on for the ArcSight SIEM to make this work. This can be downloaded from the ArcSight Protect site.
XYGATE Merged Audit Architecture

Optional plug-in products are available to collect events from ACI BASE24 logs or HP’s HLR Application.

Filter events and configure alerts to send events to the XMA database and off the server.

New! Integration with HP’s industry leading solution → HP ArcSight SIEM
Merged Audit and HP ArcSight SIEM

The NonStop Server needs the latest version of XYGATE Merged Audit as of J06.13/H06.24 to send events to HP ArcSight SIEM.

If you’ve already invested in Merged Audit or the OS Security bundle, there is no cost for this feature.

An special XMA Connector is needed on the HP ArcSight server to translate NonStop events correctly. Free download available for HP ArcSight customers.

Reports can now include NonStop events in addition to events from the rest of the customer’s enterprise.
NonStop Customers

Who would be interested in the ArcSight integration?

Customers looking for an enterprise level SIEM solution to integrate event data from all the servers in their enterprise.

NonStop customers who previously considered the Compliance Log Warehouse (CLW) and are looking for a replacement solution.

Customers who want to easily and inexpensively integrate monitoring of NonStop events into their already existing HP ArcSight SIEM environment.
Customers who are interested in finding out more about ArcSight can go to:


Customers who already have ArcSight installed in their data center can get the log adapter for Merged Audit from this website (you’ll need to register):

https://protect724.arcsight.com/docs/DOC-2654

Select T9028AAD in HP NonStop Scout to get the latest version of Merged Audit.

For general information about this solution go to:

http://www.hp.com/go/nonstop/security/compliance
THANK YOU