Advanced content management with HP ArcSight ESM 6.5

Paul Brettle – Presales Manager, Americas Pacific Region
Forward-looking statements

This is a rolling (up to three year) Roadmap and is subject to change without notice.

This document contains forward looking statements regarding future operations, product development, product capabilities and availability dates. This information is subject to substantial uncertainties and is subject to change at any time without prior notification. Statements contained in this document concerning these matters only reflect Hewlett Packard's predictions and / or expectations as of the date of this document and actual results and future plans of Hewlett-Packard may differ significantly as a result of, among other things, changes in product strategy resulting from technological, internal corporate, market and other changes. This is not a commitment to deliver any material, code or functionality and should not be relied upon in making purchasing decisions.
This is a rolling (up to three year) Roadmap and is subject to change without notice.

This Roadmap contains HP Confidential Information.

If you have a valid Confidential Disclosure Agreement with HP, disclosure of the Roadmap is subject to that CDA. If not, it is subject to the following terms: for a period of 3 years after the date of disclosure, you may use the Roadmap solely for the purpose of evaluating purchase decisions from HP and use a reasonable standard of care to prevent disclosures. You will not disclose the contents of the Roadmap to any third party unless it becomes publically known, rightfully received by you from a third party without duty of confidentiality, or disclosed with HP’s prior written approval.
“Managing content across multiple ESMs is a nightmare!”

SoC Manager – EMEA Banking ESM customer
Agenda

• Terminology
• Current content management
• What the problems are and why
• Building content to make your life easy
• Use cases
• How to build the framework
• Distribution and management mechanisms
• Future content management
• Summary
Analysts will leverage the ArcSight Console or a web browser to access the Global or Regional ESM Instances.

Correlated and the base events will be forwarded from each Regional ESM instance to the Global ESM Instance for Global Correlation.

Events from all SmartConnectors will be forwarded to the Regional ESM Instances.
Terminology

- Resource – filter, rule, dashboard, data monitor...
- ARB – ArcSight Resource Bundle
- Package / Content – logically connected content
- Archive – an exported bundle of XML data
- Manager – the processing engine of ESM
- Single pane of glass / SOC view
Current content management

• Suffer serious management issues around content
• What, where and when?
  • What content is actually used
  • Standard content – base content that is included
  • Custom content – what has been created for you?
  • Use case content – more recent content provided by use case wizard
  • Where is the content needed?
    • Which systems need it? Which have valid log sources
  • When was it updated and who did the changes?
• Package management
• Version management
What are the problems and why?

- Problems are obvious and not-so obvious

  - Standard content
    - If it's changed, how will you understand what is involved?
  
  - Custom content
    - Does it leverage existing standard content?
    - What is the impact of a small change?

  - Building fresh content
    - 100% custom per installation and difficult to replicate

- Dependencies!
Example of dependency

- Managing dependencies can be complex
- Issues around understanding the impact and issues are

• How to fix issues
• How to extend the Use Case
• What is to be included in the content
• Testing the content and backward compatibility

Standard content is riddled with dependencies
Recommended to carefully use standard content
Building content to make your life easy

- **Use Case approach**
- **Design and build content based on logical grouping**
  - Smaller, simpler and contained
  - Reduce dependencies
- **Group on purpose, log source, threat / risk**
  - Be consistent and make sure grouped together
- **Consider options, and how it will be used**
  - What is needed and if we can address the three “W” questions
- **Customising default content**
  - Use it, but be careful, dependencies can strike!
  - Can copy what is needed!
What is a use case?

- Compliance – FISMA, PCI, SOX, etc...
- Network Security – Firewalls, IDS, Routers & Switches
- Malware
- Systems – Application and Operating System
- User Monitoring – Identity, Privileged User, Shared Accounts
- SOC Metrics – Management Metrics, Analyst Team, Infrastructure Performance
- Fraud – Banking, ATMs
- Others?
Defining a use case

1. Problem Statement
2. Define the objective
3. Identify Data source
4. Define thresholds
5. Identify deliverables
6. Evaluate and refine

And refine
Example use case – audit log cleared

How do I know when the audit log is cleared on my systems?

Problem Statement

I need to be notified when audit logs are cleared for my critical assets

Define the objective

What are my thresholds?
(Always, Frequency based, something else?)

Identify Data source

Operating System
IDS/IPS (Host)
Firewalls

Evaluate And refine

How do I want to be made aware?
• Notification to CIRT
• Dashboard tracking
• compliance
• Report to Auditors of
• Audit Log Cleared

Identify deliverables

Define thresholds

© Copyright 2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.
Building a use case

- **Capture the data / requirements consistently**
- **Utilise a standard process**
  - What works for you is great
  - Consider Use Case forms
    - [https://protect724.arcsight.com/1523](https://protect724.arcsight.com/1523) (Cindy Jones)
- **Targeted, simple, manageable**
- **Steer clear of monolithic packages**

1. **Problem Description/Overview – What are you trying to detect?**

2. **Current Solution – How is the problem being addressed today?**

3. **Priority/Risk – What is the cost of not solving this problem?**
Simple tactics to make your life easy

- **KISS principle still stands**
- **Normal mechanisms stand, but control is the key**
  - Keep named user control around role based access
  - Limit options for access rights – operators DON’T need write
  - Group by general use / log source type / purpose – your choice
  - Use the numbering structures / schemes
  - Remember the use case process and captured data
    - Build out on deliverables
    - Build out on threat / risk
ArcSight use cases

- Under used previously – been present since ESM 4.5
- Much more content and documentation around for ESM 6.0c and Express 4.0
- Look at focused content built around specific data sets
  - Usually focused around several active lists – imported or used as standard
  - Linked resources for filters, active channels etc – common naming, structure etc
- Wizard tool to drive content configuration
Configuring a use case
Create your own Use Cases

- Make change to console.properties file for ArcSight Console
- Some documentation - unsupported

SystemRoot=C:\Windows
fips.enabled=false
server.hostname=redhat64
server.port=8443
server.proxy.enabled=false
console.ui.browser=C:\Program Files\Internet Explorer\IEXPLORE.EXE
console.multiUserInstall=false
ui.showUseCaseNavigator=true
echo ui.showUseCaseEditorPanels=true>> config\console.properties
Managing the content

- **Security – role based access model**
  - Use the user access model to address this
  - Carefully define the read / write to components
  - Ensure set in place for rules / lists

- **User access**
  - Who can change and process involved
  - Knowledgebase to track requirements and updates – Wiki?
  - Enforce consistent roles across tiers
Distribution and management mechanisms

- **Distribution can be done several ways:**
  - Sneakernet – manual with USB sticks? Still valid!
  - Automated – using mechanism to push content as needed

- **Proof of concept based around previous discussions**
  - Use case approach – linked resources around common content
  - Make use of archives – push and automate content as needed

- **Consider test / pre-prod / prod environments**
  - How does the mechanism work for transition between
  - What is to be included
  - Manual management likely needed
Mechanisms to automate

- **Trigger package mechanism**
  - Active List based – make a change, trigger an action
  - Needs to be an audit based system – active lists are fully audited

- **Push packages to remote node**
  - Archive out the content – standard location in resource tree
  - Push to XML file
  - Feed into relevant nodes

- **Archives are excellent for this**
  - Import and export while operational – minimal impact
  - Supports updating and access controls
Automate in operation

Add to List

Audit event generated

Rule fire – rule action

Run script on OS

Export XML package

Push to node(s)

Push to node(s)

Push to node(s)
Walk through of proof of concept
In operation – the commands!

Export Archive:
/opt/arcsight/manager/bin/arcsight archive -o -u admin -p password -m express40 -f /home/arcsight/backup/packages.xml -uri "/All Active Channels/Packages" -uri "/All Dashboards/Packages" -uri "/All Data Monitors/Packages" -uri "/All Filters/Packages" -uri "/All Rules/Packages"

Import Archive:
/opt/arcsight/manager/bin/arcsight archive -i -u admin -p password -m appliance -f /home/arcsight/backup/packages.xml
Future developments

• **Better logging**
  - Simple logging in place, obviously needs more Version controls
  - Current system supports anything and relies on careful management

• **Should use incremental mechanism**
  - Session lists for change and when?

• **Trigger through external system**
  - Integrate with external Wiki application with details of shared content development
  - Trigger from authorisation of change

• **Variables & ESM node names**
  - Made provision for Active List of ESM names, could integrate via variables
Content management

ESM 6.5 content management functionality

- **Reads installed packages**
- **Define peers for content**
- **Define the subscribers**
  - Which ESM systems will receive package
- **Define a schedule (if needed)**
- **Manually push content to ESM**
- **Previous history**
  - Success and failures
  - Manual and scheduled

### Content Management

**Packages**

- **Packages**
  - **Package**
  - **URI**
  - **Last Push**
  - **Push Status**
  - **Follow Schedule**

- **Push History**
  - **Date**
  - **Push Status**

© Copyright 2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.
Content management in action

<table>
<thead>
<tr>
<th>Package</th>
<th>Push History: Threat Detector 2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>IdentityView 2.5</td>
<td>Date: 08/28/2013 12:48:47 PM, Push Status: 1 Successful</td>
</tr>
<tr>
<td>RepSM - Demo Lists</td>
<td>Date: 08/28/2013 12:42:24 PM, Push Status: 1 Failed</td>
</tr>
<tr>
<td>Reputation Security Mo...</td>
<td>/All Packages/ArcSight Solutions/Rep...</td>
</tr>
<tr>
<td>Threat Detector 2.0</td>
<td>/All Packages/ArcSight Solutions/Thre...</td>
</tr>
</tbody>
</table>
What works and what doesn't work!

- **ESM 6.5 Content Management feature**
  - Known to suffer some issues
  - Can be unreliable with larger packages
  - Relies on ESM 6.5 at all points (doesn’t work for Express or other versions of ESM)

- **Not ideal for backup option**
  - Replication does packages and not all content
  - Will push active rules also
What works and what doesn't work!

- "SQL Table drop"
  - works well with Oracle
  - DOES work with CORR Engine based systems
  - Good for a backup process

- **Archive mechanism – as discussed here**
  - Works well for smaller packages / content
  - Has proven to have some issues
  - Use backup process to ensure consistency

- **Extended archive mechanism – several options available**
  - Implemented by HP Professional Services – discuss with them
  - Implemented by HP CDC – discuss with them
Future content management

• Several options for the future
  • Bug fixes for ESM 6.5
  • Possible extending of functionality to other platforms

• “Roll-your-own” with full flexibility

• Differential option for package
  • In operation with several installations – contact for more detail

• Needs careful consideration and management
  • How to fit into the people and process
  • Understand limitations and how to deal with updates
Summary

• Use case, use case and use case
• Smaller focused packages – not larger monolithic
• Consider dependencies, but make sure access control in place
• “Roll-your-own” or new functionality, your choice

• Critical to understand requirements – not force unnecessary content
• Deliver value and capability – nor overhead and complexity
• Fast to react and respond – not tied up in versions and testing
Please give me your feedback

Session TB3001  Speaker Paul Brettle

Please fill out a survey.

Hand it to the door monitor on your way out.

Thank you for providing your feedback, which helps us enhance content for future events.
Thank you