44%

Have trouble managing their SIEM

eIQnetworks 2013 SIEM Survey
#1 challenge

Identification of key events

SANS 2012 Log Management and Event Management Survey
34%

Have trouble writing rules!

Information Week Report
“You don’t provide me with best practices.”

- Customer EMEA Region
“I haven’t caught anything in a year.”

- Customer Americas Region
“Companies struggle with SIEM, we know why.

Let’s tell them why then help them fix it”

- HP ArcSight Employee
Succeed with SIEM – ArcSight Activate Framework

Standard content development framework focused on helping you get the most from your HP ArcSight implementation

Train and retain resources

- Standardized framework enables consistent and repeatable processes that reduces training time for new employees
- Sharable content facilitates technology use and knowledge transfer

Maintain SIEM content

- Install packages drive fast deployment and efficient use of resources
- Common, reusable methodology to create content and rules

Keep up with security challenges

- Guidance, advice, standard use cases, and content packages optimize catching the bad guy
- Documented common framework enables knowledge sharing of threats, trends and monitoring capabilities
 Activate
A mature SIEM solution

Spend more time integrating
people, process and technology

Spend less time building
basic content
Arcsight Activate Framework

The ArcSight Activate Framework is a modular content development method designed to quickly deploy actionable use cases.

End to end solution
ArcSight Activate will provide customers with the appropriate information to generate the raw data for consumption.

Modular integration
The framework is designed to provide a maturity path for our customers.
The path focuses on developing certain skills and establishing the appropriate security controls for incident detection.

Detect complex attacks
Detecting complex attacks gets easier as more modules are layered on top of a solid foundation and coverage is expanded across the enterprise.
ArcSight Activate packages

Threat tracking
Indicators and warnings
Situational awareness
Base content

Indicators and warnings
Product based packages organized by solution. Provides the foundational elements for data enrichment on the outer layers.

Situational awareness
Integrates contextual information from:
• Network & asset models
• Indicators & warnings packages

Threat tracking
Continue to build on contextual information
• Business impact
• Threat impact
• Next expect event
Maturity roadmap

Customers are faced with internal challenges while integrating SIEM

**Log management**
- Log management policy
- System auditing configuration
- Time synchronization
- Infrastructure capability

**IT practices**
- Infrastructure knowledge
- IT management procedures
- System configuration baselines
- Network segmentation

**Security controls**
- Security technologies
- Network infrastructure coverage
- System configuration
- Staff capabilities

Provide guidance  
Simplify content  
Divide and conquer
Initial installation and configuration

End device
- Configure device
  - Install
    - Configure
      - Customize

SmartConnector
- Install
  - Configure
    - Install activate solutions
      - Install product Packages
        - Run test plan

Activate content
- Install base
  - Integrate alerting
    - Integrate reporting

Workflow
- User use content
Where do we start?

Focus on strengths
Our typical customers are network geeks. Starting by protecting the perimeter device makes the integration process easy.

Focus on ownership
Starting with use cases where the SIEM owners control the end device bypasses bureaucracy.

Prescriptive integration
Activate modular approach to use case integration focuses on building the required skills while developing the a mature collection environment.
High level package structure and installation

**Step 1:**
**Base Package:**
Provides all common components

**Step 2:**
**Solution Package:**
Provides common elements used to resolve specified use cases

**Step 3:**
**Product packages:**
Each solution has a set of resources to meet use case requirements
No configuration!

For Base and Solution Packages
Product packages

1. Open the Filter

/All Filters/ArcSight Activate/Use Cases/Perimeter and Network Monitoring/Tracking and Identification/All Firewall Accept Traffic

and add

/All Filters/ArcSight Activate/Core/Product Filters/Check Point Firewalls/Network Traffic Management/Check Point Firewall Accepts Events.

If there are multiple firewalls in the environment, add them within an OR statement.

2. Open the Filter

/All Filters/ArcSight Activate/Use Cases/Perimeter and Network Monitoring/Tracking and Identification/All Firewall Accept Traffic

and add

/All Filters/ArcSight Activate/Core/Product Filters/Check Point Firewalls/Network Traffic Management/Check Point Firewall Denies Events.
Operating systems

1. Configure your devices
2. Configure your connectors
3. Install the content
4. Integrate into workflow

Level 1
Indicators & warnings

Level 2
Situational awareness

Data enrichment

Perimeter
and network monitoring
Operating system monitoring
Attack lifecycle coverage

I control the domain controllers!
Finally... I got something for a network model

Iterative Wins
Get basic zones into the SIEM. It really doesn't have to be perfect.

Accuracy is Key
If you know the data is wrong, keep it general.
You are better off getting a high level network model than an incorrect one.

Model Tagging
Each Situational Awareness package will have some basic categorization requirements.
The idea is to get some basic alerting in place. More intelligent use cases can be completed after a little focused information gathering.
Maturity model revisited

Increase Enterprise Coverage OR Expand on the Attack lifecycle and data enrichment

Level 3
Threat analysis

Level 2
Situational awareness

Level 1
Indicators & warnings

Data enrichment

Perimeter and network monitoring
Operating system monitoring
Security application monitoring

Attack lifecycle coverage
You have a functional system.
No development required.

Perfect for new customers
Okay, that’s cool
but how does this all work?
Indicators and warnings

The forensic trail left behind on the target

Use case
Methodology
Targets

Indicators and warnings

Gain access
Exploit
Service
Client

IDS Signatures
Malware detected
Application Errors
System Errors
Process execution
Service Execution

© Copyright 2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.
Analyzed use cases 10

Found 100 indicators and warnings
Indicators and warnings

**User authentication**
- Successful user login
- Brute force attack in progress

**User management**
- Account lockouts
- User added to administrative group

**Product suspicious events**
- Denial of service event detected
- Multiple SQL injection attempts

**System changes**
- Changes to critical registry files
- Kernel modules unloaded

**System errors**
- Data execution prevention alert
- Service crashed unexpectedly

**Product patterns**
- Baseline system processes
- Baseline network flows

Countermeasures
Indicators and warnings

Why do we care?

Identification
Get the right events with the right fields driving workflow and establishing appropriate patterns for upper level correlation.

Tracking
Store any relevant indicators within lists. This data will be used for reporting and correlation at the upper level.

Provide the foundational elements for data enrichment
Attack life cycle for threat detection

Recon
- Firewall, IDS, services

Weaponization
- IOC, external Intel

Delivery
- IDS, Inline-AV, next-gen firewalls, WAF

Exploit & Install
- System AV, OS audit logs and FIM

Cmd & Ctrl
- Proxies, firewalls, IDS

Objectives
- SIEM, IAM, OS audit logs, firewall, IDS

Disrupt the adversary

Look for bad guys
Multi sensor data fusion

Definition:
The process of integrating data to represent an object in a consistent, accurate and useful manner.

Enrichment and refinement
Data is processed and becomes more valuable at higher levels.

Tested theory
In use in various fields, defense, health care, transportation

ArcSight ESM’s features play right into this model
ArcSight content in data fusion

**Level 0: Data refinement**
Devices and SmartConnectors
Configuration

**Level 1: Object refinement**
ArcSight ESM simple correlation and tracking

**Level 2: Situational refinement**
ArcSight ESM with Integrations

**Level 3: Threat refinement**
Alerting based on System State, and attack progression

- **End Device**
  - Configure and tune

- **SmartConnector**
  - Calibrate and tuning

- **Base Events**

- **Channels**
  - Real-Time Workflow

- **Reports**
  - Reporting Framework

- **Lists**

- **Rules**
  - Tracking and Categorization

- **Filters**
  - Indicators and Warnings

- **Integration**
  - Modeling & External Data

- **Correlation Events**
How Data Enrichment Works

Level 0: Data refinement
- Devices and SmartConnectors
- Configuration

Level 1: Object refinement
- ArcSight ESM simple correlation and tracking

L2: Situational refinement
- ArcSight ESM with Integrations

L3: Threat refinement
- Alerting based on System State, and attack progression

End Device
- Configure and tune

SmartConnector
- Calibrate and tuning

Base Events

Channels
- Real-Time Workflow

Reports
- Reporting Framework

Rules
- Tracking and Categorization

Filters
- Indicators and Warnings

Lists

Correlation Events

Integration
- Modeling & External Data

Filters
- Situational Context

Reports
- Reporting Framework

Rules
- Threat Impact Increased Priority

Filters
- Threat Analysis

Lists
**Example:**

**Profiling user system activity**

**Basic baseline example**

1. User Login Temporary Trend or Lightweight rule Populates AL
2. Alert when user/system combo is not in list
Let’s zero in on two attributes tracked in lists

**Attack progression**
Track progression in a series of lists.

**System state**
Track state in a series of lists.

---

**Endless possibilities**

- Logon from compromised system
- New service on exploited system
- User activity w/o login on exploited system
- Attack progression on targeted system
- Large transfers to hostile hosts
ArcSight activate accelerator

Phase 1: Preparation
- SIEK assessment
- Short-term roadmap
  - Activate workshop

Phase 2: Initial capability
- Activate content
- Content migration
- Threat and context
- SIEK roadmap

Phase 3: Maturity
- Enhancements

© Copyright 2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.
Altering our design methodology

Expectations

Change current methodology

Common approach to building use cases is to go grab all the logs you can gather and see what you can do them.
This simply doesn’t work and is quite costly over the long term.

Business relevant use case

Needed to switch to a more business relevant approach that covered a range of indicators for better detection capabilities.
Capturing and storing the relevant information that support a complete solution would move us away from fragmented capabilities.

Outcome

New approach to use case Design
Improving our information infrastructure

Expectations

Reduce irrelevant log collection
Processing and storing all data in the SIEM is costly with little ROI. We needed to reduce the number of irrelevant events making room for more relevant events.

Monitoring infrastructure
We were looking for more efficient ways to monitored the SIEM infrastructure and event collection from key security devices.

Outcome

Return on investment
Build better and complete content solutions

Expectations

Optimize correlation capabilities
Holy grail of cross-device correlation

Attack life cycle
Mapping all the indicators to the attack life cycle opens up a range of possibilities

Outcome

Content deliverables
For product types
Mapped to the Attack life cycle
Clean incident and development workflow

**Expectations**

**Content development life cycle**
- Take advantage of specialized skill sets
- Maturity roadmap strategy
- Repeatable discrete objectives
- Reusable content through methodology

**Catch more bad guys**
- Build easy to understand content
- Complete use case solutions

**Outcome**

Easy to understand content

Team Cohesion

Content Portability
Our challenges

Paradigm shift

Moving away from data source focus to Collecting events that serve our business needs
Our challenges

Understanding system behavior is not easy
No matter the tool
Our challenges

Time and resources

Time constraints
- Initial resourcing
- Time commitments

Skill sets
- Device analysis
- Cross-pollination
- Get out of your comfort zones

External teams
- Collaboration
- Introducing change
Please give me your feedback

**Session** 3267    **Speaker** Petropoulos

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