Hewlett Packard
Enterprise

Protect 2016

Please give me your feedback

Session ID: B10024 **Speaker:** Christopher L Kaija

—Use the mobile app to complete a session survey

1. Access “My schedule”
2. Click on the session detail page
3. Scroll down to “Rate & review”
   - If the session is not on your schedule, just find it via the app’s “Session Schedule” menu, click on this session, and scroll down to “Rate & Review”
   - If you don’t have it, download the event app today. Go to your phone’s app store and search for “HPE Protect 2016”

—To access the session survey online, go to the Agenda Builder in the event session catalog and click on your session

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

Hacking the Hallways
SIEM and PSIM, Revisited

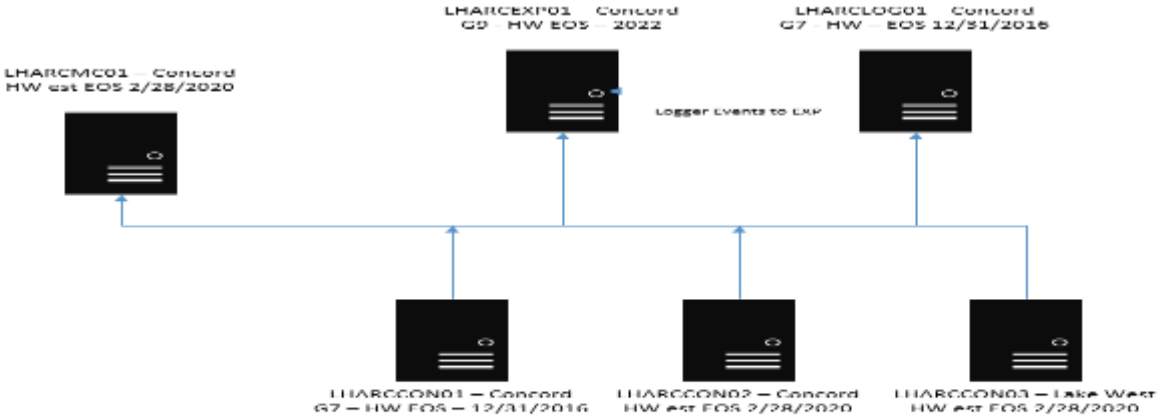
Session B10024 Christopher L Kaija, CISSP

Lake Health

- Lake County Ohio's primary Hospital provider, 30 miles east of Cleveland.
- Lake Health has been operating as the primary health care provider in this area since 1902.
- We are a non-profit with strategic partnerships with both the Cleveland Clinic and University Hospitals Seidman Cancer Center.

Lake Health – ArcSight Infrastructure

“Information wants to be free…. it also wants to be expensive” Steven Brand to Steve Wozniak, The Whole Earth Review



Lake Health Arc Sight Infrastructure Overview

LHARCLXP01 – DL380 G9 – Model – LL7600 – Arc Sight Lxpress 6.9
LHARCLOG01 – DL380 G7 – Model - L7400s – Arc Sight Logger 6.0 Patch 2 – 8 TB – 100K EPS Incoming
LHARCMC01 – DL380 G8 – Model – C6515S – Arc MGMT Center 2.0 Patch 2 – 15 Nodes – 1 Container – 4 Connectors
LHARCCON01 – DL380 G7 – Model – C6408M – Arc MGMT Center 2.0 Patch 2 – 8 Containers – 32 Connector |
LHARCCON02 – DL380 G8 – Model – C6504 – Arc MGMT Center 2.0 Patch 2 – 2 Nodes – 4 Containers – 16 Connectors (L or R)
LHARCCON03 – DL380 G8 – Model – C6504 – Arc MGMT Center 2.0 Patch 2 – 2 Nodes – 4 Containers – 16 Connectors (L or R)

Who is this person?

- ArcSight Express 3.0, 4.0, Express 6.9.1c
- ArcSight Logger 5.1 to 6.1
- ConApp / ArcMc migration to MC 2.2
- Smart Connectors v5 to v7
- IT industry since 2000, previous USN. Cisco, Juniper, Riverbed, F5 networks, Blue Coat, Aruba Wireless, Checkpoint etc.

Tip of the Hat to the Experts

- Colby DeRodeff – Co-Founder and CSO of Anomali, Inc. author of “The Convergence of Physical and Logical Security.”
- Brian Contos – Securonix, Head of Worldwide Security Strategy and contributor to CSO online
- They created and gave the original “Hacking the Hallways” presentations and podcast in 2006.

Crime Prevention Through Environmental Design

- CPTED principles include Natural Surveillance, Natural Access Control, Territorial Reinforcement, Maintenance and Management.
- Most organizations handle the first three in a top notch fashion. Security Plans reviewed, planned, mapped, reviewed again, and finally approved and installed see the following examples.

Natural Access Control

Natural Surveillance

Aokigahara Forest, Japan

Hitachi Seaside Park, Japan

Territorial Reinforcement

Demographics: Environmental Studies

- Sources of new untapped data analytics for use in multiple areas SIEM and PSIM integrations.
- Govt. Census Data, Neighborhood breakdowns (address, zip code, county, city.)
- Vendor based and free solutions abound: ESRI, Movoto, Cross Check, City-Data all have a free limited and paid version of the demographics they offer.

Integrations, are they truly possible?

- Yes, most vendors have either API’s or allow for database level queries to gain customer requested information.
- You have to know what you want to find before pulling it all into a PSIM or SIEM. If you’re using a Big Data solution, there is more give and take, as the previous two may be size constrained.

Office Space = RISK

- IT Security should require constant review and mitigation of overall Organizational Exposure to unwanted or preventable risk.
- Office Space – the immediate location or area under which an entity provides goods or services at a fixed or pre-determined location.
- Mitigating controls would include constant review of policy, procedures, and the logical and physical security components to ensure nominal working order.

Process Improvement?

Lake Health

Case Study – The restraining order that could have worked.

- Restraining Order issued for a person with a known vehicle license plate.
- Video Surveillance software capable of scanning license plates and sending alerts based on recognition factors.
- Due to system implementation restraining order was allowed to be violated due to inaction.

Lake Health

Case Study – contd.

- Process review – need for a Service Catalog, documentation, employee and Guard training, along with implementation and testing of the new capability.
- Legal liability limited due to nature of the incident and parties involved.

Case Study 2 – Violent Crime on the Commuter Train

- 2006 Homeland Security News Wire, writes a scathing article against the installation or use of dummy cameras as a means of deterrence.
- 2016 In response to a previous fatal shooting on a commuter train, BART admits not all cameras actually function, and states all trains will receive working cameras.
- Legal Liability – Off the charts, as the legal precedence when seeing cameras at use in the area a prudent person expects a nominal amount of safety and security.

Case Study 2 – Security is the new Free WiFi

- Ask yourself – At your facilities, are all cameras live?
- When you see signs that say “Protected by X” do you feel safer?
- If you see a blue call box, do you expect it to work and someone to answer?
- If so, society as a whole now has an expectation of Security – no longer should it be a ‘nice to have’ or an option.

Case Study 3 – Fire in the Hole!

- Life Saving – the quintessential must do of all Physical Security implementations is Life Saving, protecting the assets is a by-product.
- Mag Locks, Card Readers, Alarm Panels, Elevators, all automatically react if an emergency is detected and this pre-programed response is activated automatically.

Case Study 3 – contd.

- In some organizations not all doors Fail Open in a fire, however the first responders have away around that – the Knox Box.
- Knox Box – a small fire proof lock or combination box on the outside of a building that contains badges for use in an emergency that have been granted access to all doors and areas within the premises.
- Knox Box, key and/or combination are typically head by the local first responders who typically do not work for the organization.

Lake Health

Case Study 3 – contd.

- Organizations should after every incident pull all Physical Security access reports to review and track the locations of all Knox badge uses as appropriate.
- If the incident was on the fifth floor, why was a badge used on the fourth, or in the R&D section at an adjacent building?

Case Study 3 – contd.

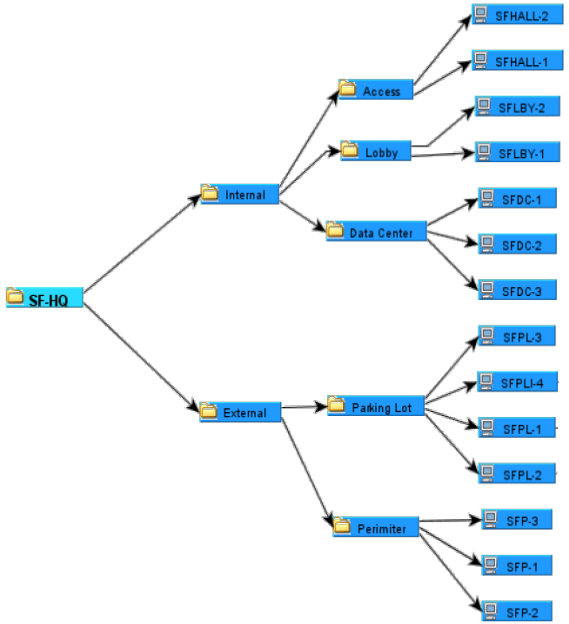
- Integrating your Physical Security infrastructure into your SIEM just makes sense.
- SIEM's typically already see where you logged in, what devices you use, what websites you browse, and what behavioral activity is deemed normal for your job role, individually or as a group.
- Now expand to include every where you went inside the buildings, remotely across the world in real-time.

ArcSight – Physical Security Modeling

- This can be achieved in ArcSight Express 3.0c, 4.0c, 40c Patch 1, and ESM 6.9.0c and 6.9.1c. It is time consuming but highly doable even with limited staff.
- Requirements – A high level of understanding or the Physical security infrastructure set up and dependencies.

ArcSight – Mapping Cameras to Asset Zones

- Two Ways to bring in your Security Cameras – Vulnerability scan with auto asset creation or manually.
- Locations – SF-HQ can be geo-located, if the network is unique with an ArcSight collection point also you can dynamically manage all assets and prioritize alerting in a more manageable fashion.
- To remain consistent to the Physical alarm structure keep your Asset Zone names similar where possible.



ArcSight – Alarm Panels to Asset Zones

- Most vendors the alarm panel itself is network aware, if it loses network connectivity the panel contains a copy of card access and alarm configurations.

ArcSight – Alarm Panels to Asset Zones

- These typically can be taken into ArcSight the same way as the IP Cameras using either vulnerability scans and auto asset creation or manually. (Manual maybe best a lot of these are considered fragile systems.)
- The same process can be used for all HVAC panels, generator panels, etc.

ArcSight – Door/Card Readers to Alerting

- This is the hardest part of this exercise – most Card Readers are near field devices with no ability to truly be network aware, so currently lake Health uses alternate interfaces off of the Alarm Panels to track door input fields and tie those back to logical names.
- ArcSight – Alerting limitation – you can not alert on an Asset if an IP is not associated with it, so all Door alerts appear as Panel Alarms with additional information attached.

ArcSight – Requirements to integrate Badges

- Our Vendor – LENEL
- Preferred – 5 MS SQL system views that can be queried against remotely on a scheduled basis and output to csv. (All badges, All Swipes, All Users, All User Activity, All Camera/ Panel Alarms.)
- ArcSight Flex Connector – to read the above output.

ArcSight – Current implementation

- Automated Queries on the Lenel DB directly, ArcSight picks up files remotely processes and deletes old files.
- SQL are on the next slide these are cleaned up and using default Lenel names for DB tables.
- Process Improvements – SystemViews would remove application versioning issues with SQL table, and FlexConnector testing is time consuming.

ArcSight –List for Badge to Unique User

- This is used to refresh Active Lists with net new badges, users, or changes. This works in hand with IAM solutions to verify multiple data points.

```
select b.ID, b.EMPID, b.DEACTIVATE, e.LASTNAME, e.FIRSTNAME from BADGE b, (
    select ID, LASTNAME, FIRSTNAME from EMP) as e
where b.ID=e.ID
```

ArcSight – SQL Queries for Badge Swipes

- This query ties all Badge Swipes to the User's Badge

```
Select p.EMPID , p.EVENT_TIME_UTC, p.DEVID,s.ID , t.EVDESCR , f.NAME, g.READERDESC, e.LASTNAME, e.FIRSTNAME
From EVENTS p
INNER JOIN BADGE s  ON s.empid = p.EMPID
INNER JOIN EVENT t ON t.EVENTID = p.EVENTID
INNER JOIN ACCESSPANE f ON f.PANELID = p.DEVID
INNER JOIN READER g ON g.PANELID = p.DEVID
INNER JOIN EMP e ON s.ID = e.ID
WHERE p.EVENT_TIME_UTC > DATEADD(day, -1, GETDATE())
```

ArcSight – Lenel give it all -

- This query is a good one if you see weird fields or unparsed events in your Flex Connector.

```
SELECT *
 FROM BADGE s FULL OUTER JOIN EMP e
  ON (s.ID = e.ID)
 FULL OUTER JOIN EVENTS p
  ON (s.EMPID = p.EMPID) ;
```

ArcSight – Requirements to integrate Cameras

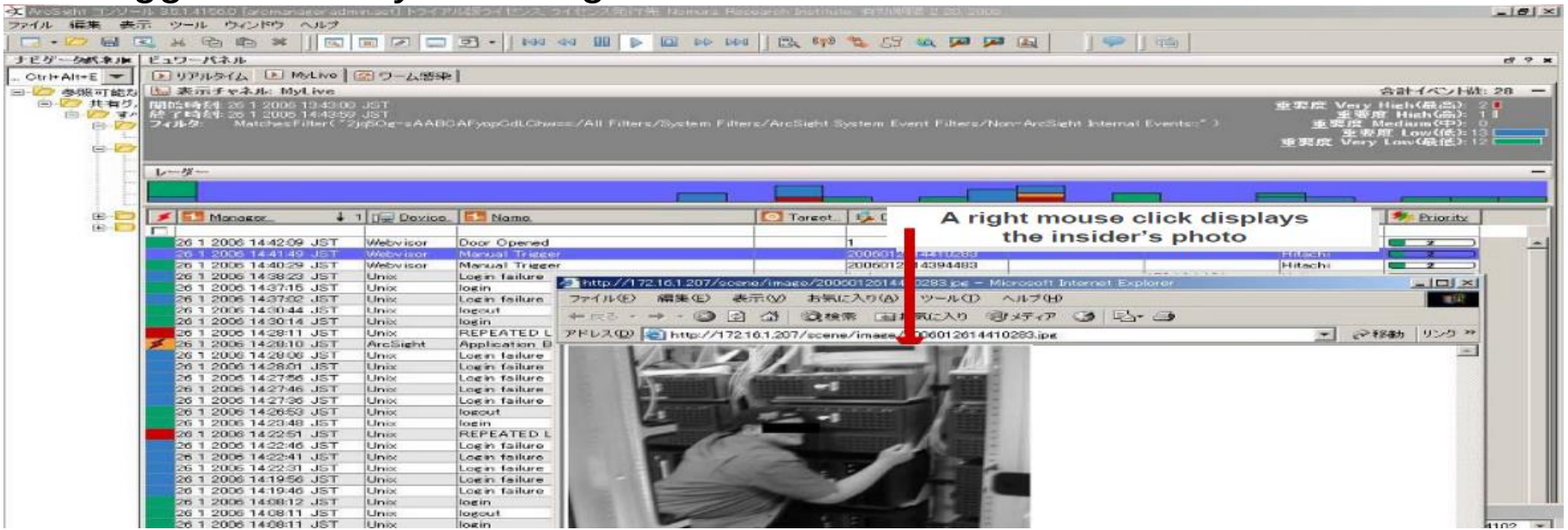
- Our Vendor – Axis, Hitachi, older Lenel
- Preferred – All scripted API calls from the main management server – stills saved locally to SD card, and recorded video – archived to DC for review.
- ArcSight – Alerts raised to a channel or dashboard, using integration commands that trigger scripts to fire if necessary.

ArcSight – Current implementation

- ArcSight Console – integrated command launch camera IP, Log on, Snap Still.
- API's for Axis Cameras and Python script that works on some Hitachi's next slides.
- Process Improvements – Get better at scripting, replace old cameras, review camera placements, cut OPEX.

ArcSight – Still Camera API (sample)

- This is from the original Hacking the Hallways the console UI and triggers virtually unchanged.



ArcSight – IP Camera Vendors API scripts

- Axis - http://www.axis.com/us/en/support/technical-notes/live-snapshots
- Hitachi – depends on camera – Crucial imaging or standard – Hitachi support was able to provide the script used – I will check with them if we can distribute the support URL or pdf.

Lake Health

ArcSight – Activate Framework – I do, Do you?

- This is not available under ArcSight Express 3.0 or 4.0.
- Activate was previously used within ESM.
- Activate does work with new Express 6.9.0c and 6.91c.
- Functionally it improves the performance and speed of the Manager, across all operations.

ArcSight Activate Framework – 100 ft view

- Helps reduce Rule sprawl by condensing functional areas of interest into Packages.
- As an example take the Express Package for Cisco Monitoring – its perfectly fine package works for all things Cisco.
- However I also need rules, filters, content for Citrix NetScalers, Array Networks, F5, WatchGuard Firewall, Juniper router and firewall, various remote VPN solutions.
- Activate does this all in a Network Monitoring Package, it's possible not all the products will be there, but there are more than just Cisco.

ArcSight – Activate – resources

- HPe ArcSight Activate wiki –

https://hpe-sec.com/foswiki/bin/view/ArcSightActivate/WebHome

- HPe ArcSight – Protect 724

https://www.protect724.hpe.com/welcome

- HPe ArcSight Marketplace –

https://saas.hpe.com/marketplace/arcsight

Lake Health

Questions?

For more information

Supporting Sessions

- Seeking Insider Threats: B10054 – FRI – 11:30 – Annapolis 1
- HPe Security ArcSight as the security nerve center: B9909 – FRI – 9:00 – Magnolia 1
- Tuning and deploying with HPe Security ArcSight Marketplace and Activate Framework – 600 HPe Showcase

Also at the Conference

- HPe Security ArcSight Activate Threat Intelligence packages: B10039 – WED – 3:45 – Baltimore 5
- HPe Security ArcSight ESM – ESM now and the way forward: B10334 – Thu – 4:15 Baltimore 2

Additional sites of interest

- http://saas.hpe.com/marketplace/arcsight
- https://www.protect724.hpe.com/welcome
- https://www.hpe.com/us/en/services/consulting.html
- https://www.hpe.com/us/en/services.html
- http://www8.hp.com/us/en/software-solutions/enterprise-security.html

B10024 Your feedback is important to us. Please take a few minutes to complete the session survey

Please give me your feedback

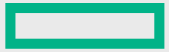
Session ID: B10024 **Speaker:** Christopher L Kaija

—Use the mobile app to complete a session survey

1. Access “My schedule”
2. Click on the session detail page
3. Scroll down to “Rate & review”
   - If the session is not on your schedule, just find it via the app’s “Session Schedule” menu, click on this session, and scroll down to “Rate & Review”
   - If you don’t have it, download the event app today. Go to your phone’s app store and search for “HPE Protect 2016”

—To access the session survey online, go to the Agenda Builder in the event session catalog and click on your session

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



Hewlett Packard
Enterprise

Thank you