Protect 2015

Protect 2015

Logger API – Coexisting in an analytical world

Aaron Kramer, CISSP, CEH

Kevin Romero, CISSP

@SecGeek

#HPProtect

Agenda

- Logger 6.1 and the Logger API
- Security Analytics
- MSSP Integration
- User Behavior Analytics Integration
- ArcSight Interactive Discovery Integration
- Logger 6.1 Dynamic Lookup Tables Integration
- Protect724.hp.com Post
- Q & A

Logger 6.1 and the Logger API

In short, not a lot has changed for the Logger API

- SOAP Supports Login, Search, and Report services
  - PERL ‘reference’ client on Protect724
  - https://protect724.hp.com/message/20137 (read the thread to the bottom!)
- REST Supports Login, Search services
  - Python RESTful client : https://protect724.hp.com/message/64045
  - RESTful Search supports
  - Return of field summarization
  - Status-of-search calls
  - Return of Histogram attributes
  - Drilldown
  - Return of Chart data
  - Stop Search
  - Close Search

Logger API

- Eventually, all of Logger's Web Services will move to simpler RESTful services. The SOAP Web Services will be deprecated in a future release. Therefore, we encourage users to move toward using the RESTful Web services where available
- Web services are not available for trial Loggers. To take advantage of this feature, you need the Enterprise version

Security analytics

- Retrieving events from Logger
- Doing something with the events
- User Behavior Analytics
- ArcSight Interactive Discovery
- Other Visualization, ie Tag Cloud
- Situational Awareness

Managed Security Services Provider (MSSP) integration

- MSSP user interface branding and customized customer portals tailored to provide user specific dashboards and views.
  - Search single and peered Loggers and run reports for download
- Provide greater granularity and control on allowed searches to prevent data leakage or spillover using MSSP-enforced filters on search (field=CustomerA)

```
Python Snippet
#Set the parameters for event retrieval. Use offset as index to begin pulling events in increments of 100.

event_options = {"user_session_id" : session_ID, "search_session_id" : search_ID, "summary_fields" : fset_partial, "dir" :
options.sort, "length" : 100,"offset" : event_offset, "fields" : fset_partial}

events_data = requests.post(events_uri, data=json.dumps(event_values), headers=headers, verify=False)

strread = json.loads(events_data.text)
```

- https://protect724.hp.com/message/64045

User Behavior Analytics integration

- What is User Behavior Analytics (UBA)?
  - A new offering by HP ArcSight to perform behavioral baselines based on peer groups and roles.
  - High privileged account monitoring, Application security intelligence via activity and transaction analytics and fraud analysis.
  - Provides broader network event intelligence using peer anomalies.

- Use UBA CEF connector to prepopulate historical data as opposed to waiting for new events to be forwarded to UBA.
  - Use in a post breach scenario to uncover patient zero.
  - This allows for populating the users with their associated and varying user names or roles.
    - Sample search to export RAW CEF:

      logger_data_export.py -Q "sourceUserName IS NOT NULL OR destinationUserName IS NOT NULL“ -R

    - Events to populate the user table RULE in UBA for associating users.
  - Logger API to provides historical data while UBA in parallel retrieves an event feed to continue learning behavioral trends going forward.

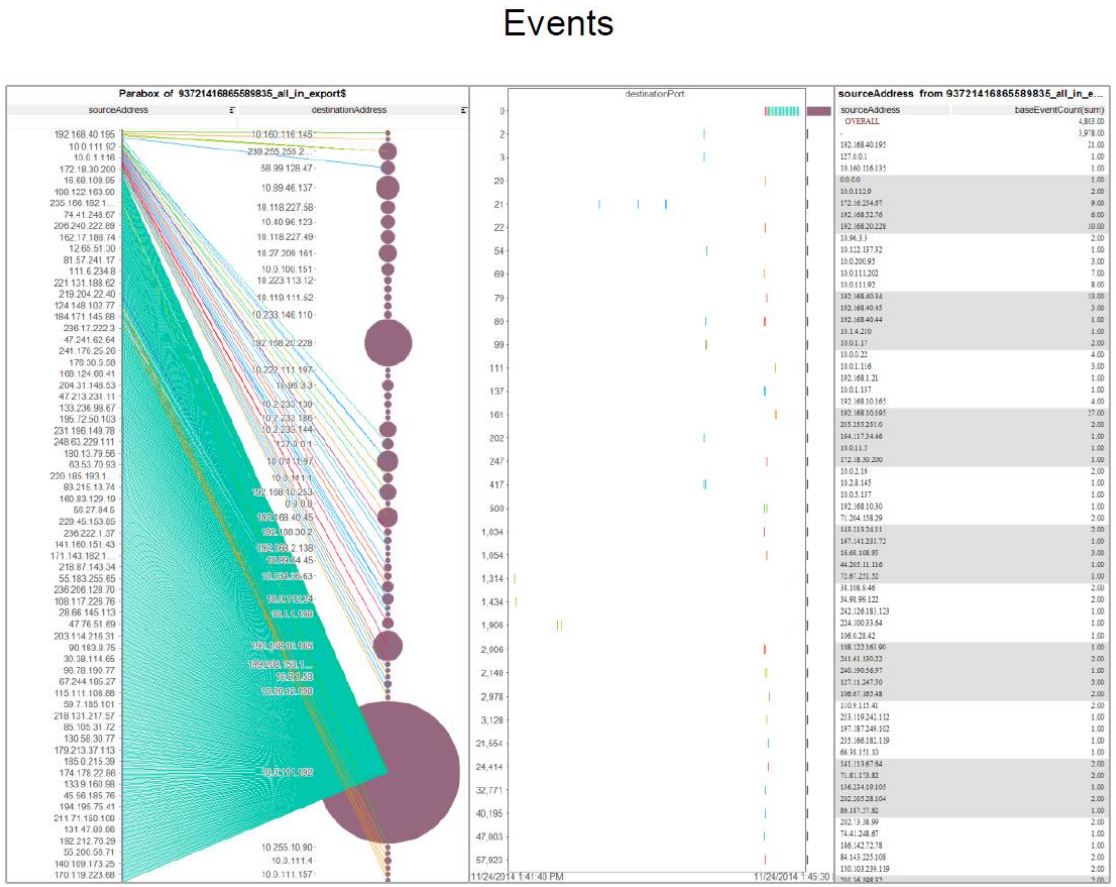
User Behavior Analytics integration

Example Sources and Queries for populating HP UBA

- categoryDeviceGroup = "/Identity Management/AAA" AND categoryBehavior ="/Authentication/Verify" AND sourceUserName IS NOT NULL
- deviceVendor = Damballa OR deviceVendor = FireEye OR deviceVendor = "Trend Micro“
- deviceVendor="McAfee" AND deviceProduct="Web Gateway" AND sourceUserName IS NOT NULL AND NOT sourceUserName="-“
- deviceVendor="Symantec“
- deviceVendor="Unix" AND NOT categoryBehavior ="/Access/Stop“
- categoryDeviceGroup="/VPN“
- ((deviceVendor="Microsoft" AND categoryBehavior="/Authentication/Verify") AND NOT (deviceCustomString5="Kerberos")) AND NOT (sourceUserName IS NULL AND destinationUserName IS NULL) OR NOT (sourceUserName = "-" OR sourceUserName CONTAINS "$" OR destinationUserName CONTAINS "$" OR destinationUserName CONTAINS "$" OR destinationUserName = "SYSTEM")

ArcSight Interactive Discovery integration

- What is ArcSight Interactive Discovery
  - ArcSight Interactive Discovery augments ArcSight Logger and ArcSight Enterprise Security Management's Pattern Discovery, dashboards, reports, and analytical graphics. Interactive Discovery provides enhanced forensic data analysis and reporting capabilities using a comprehensive selection of pre-built interactive statistical graphics.
- Use SOAP API to run scheduled reports
  - Reports are exported and saved in CSV format for existing AID project templates
    - Utilize pre-existing reports specific to Hunt Team analysis.
    - Allows Hunt Teams to perform analysis on current or up to date information automatically.
    - Provides additional access control and limits administrative overhead when managing separate products.



Visualization of Big Data – scatterplot

This example reveals a low and slow scan

Business statement

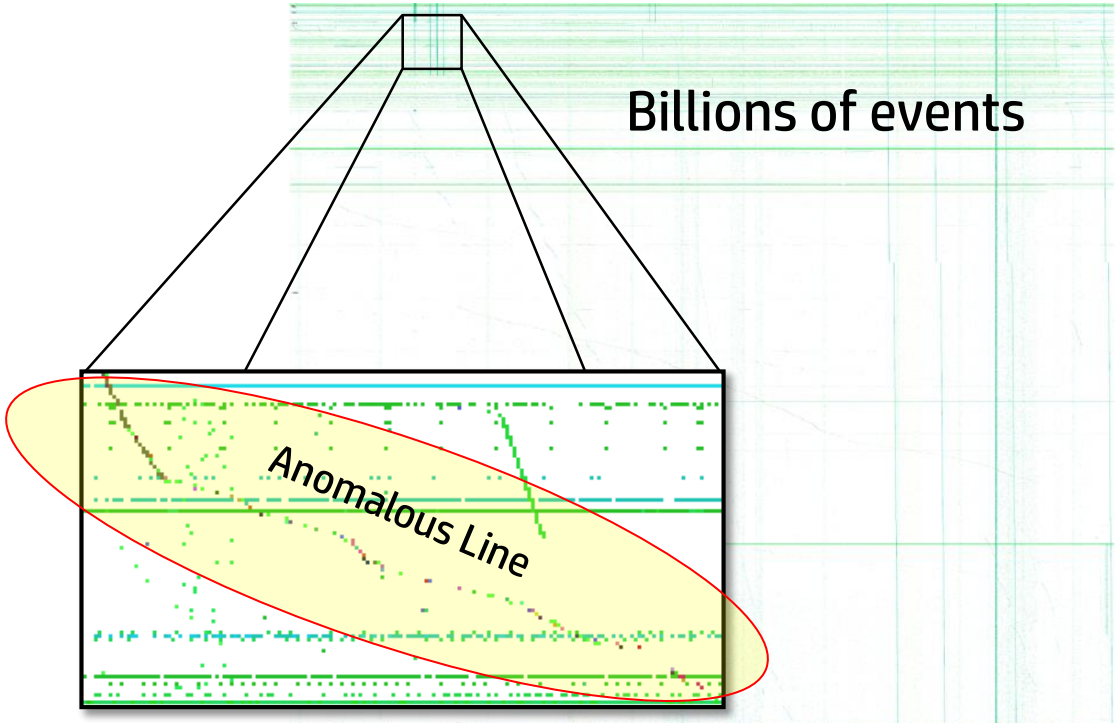
- Find sophisticated port scan activity (distributed, randomized)

Analytics statement

- Plot multiple months of data on one scatterplot

Findings from visualization

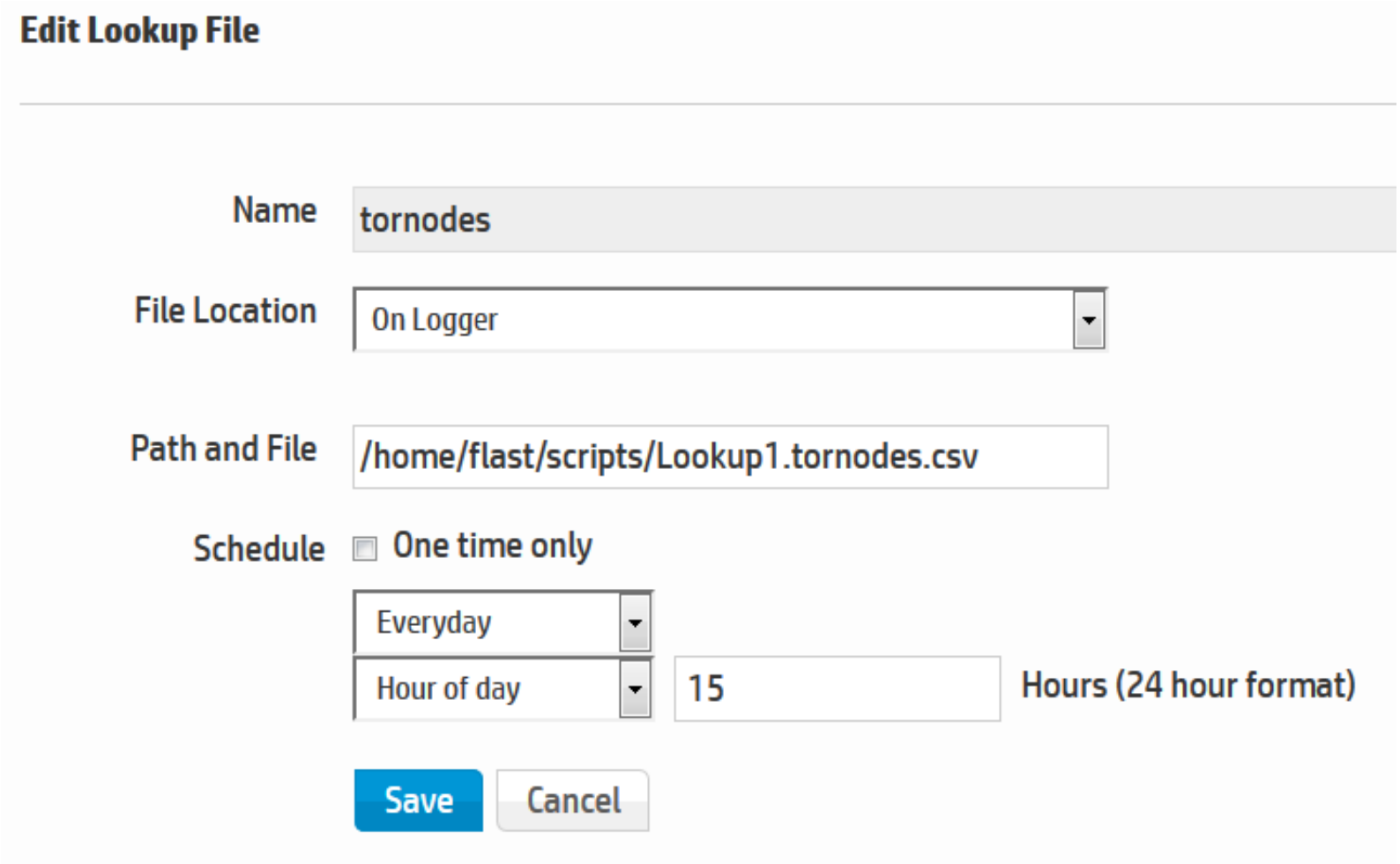
- Single multi-week scan from distributed, internal sources indicates advanced attacker



Logger 6.1 – updating Lookup tables

- What is Logger Lookup
  - Pulling in a CSV file from outside Logger, and using the table in a search
    - Common values, values NOT in common
  - Also called “Static Correlation”
  - Use this table of Tor Exit Node IPAddresses, does any of my Logger traffic show any communications with any Tor Exit Nodes?
- Logger 6.0 Introduced Lookup Tables
- Logger 6.1 Introduced ability to update the Tables underneath Logger
- Tor
  - Python Code to retrieve list of values
  - Write CSV file suitable for Logger loading, in the right place
  - Logger Lookup Table Scheduling
- Operational Awareness

Logger 6.1 – updating Lookup tables



Logger 6.1 – Ideas for dynamic lookup tables

- Tor Exit Nodes – every 30 minutes
- Bogons = routing black holes, daily
- GEO IP Relevance = 6.1 Feature: INSUBNET
- HTTP Status Codes
- Microsoft Event Codes, for all versions of Windows
- Asset Owners = Who owns a server?
- Employee / Organization = Who's server is it?
- Operational = Which Data Center, which rack, which shelf, etc.

Protect724.HP.com Post

- Python REST API Code
  - Demo examples of using REST API from python client
    - https://protect724.hp.com/message/64045
  - TOR dynamic Lookup fetch, reformat, update csv file
    - https://protect724.hp.com/message/64045
- ArcSight Interactive Discovery “Project” File

- Look for future updates
- You are encouraged to contribute!

For more Protect sessions:

TT3916

Amit Khandekar - Build your own real-time security Threat intelligence feeds - **Thursday 4pm**

B3895

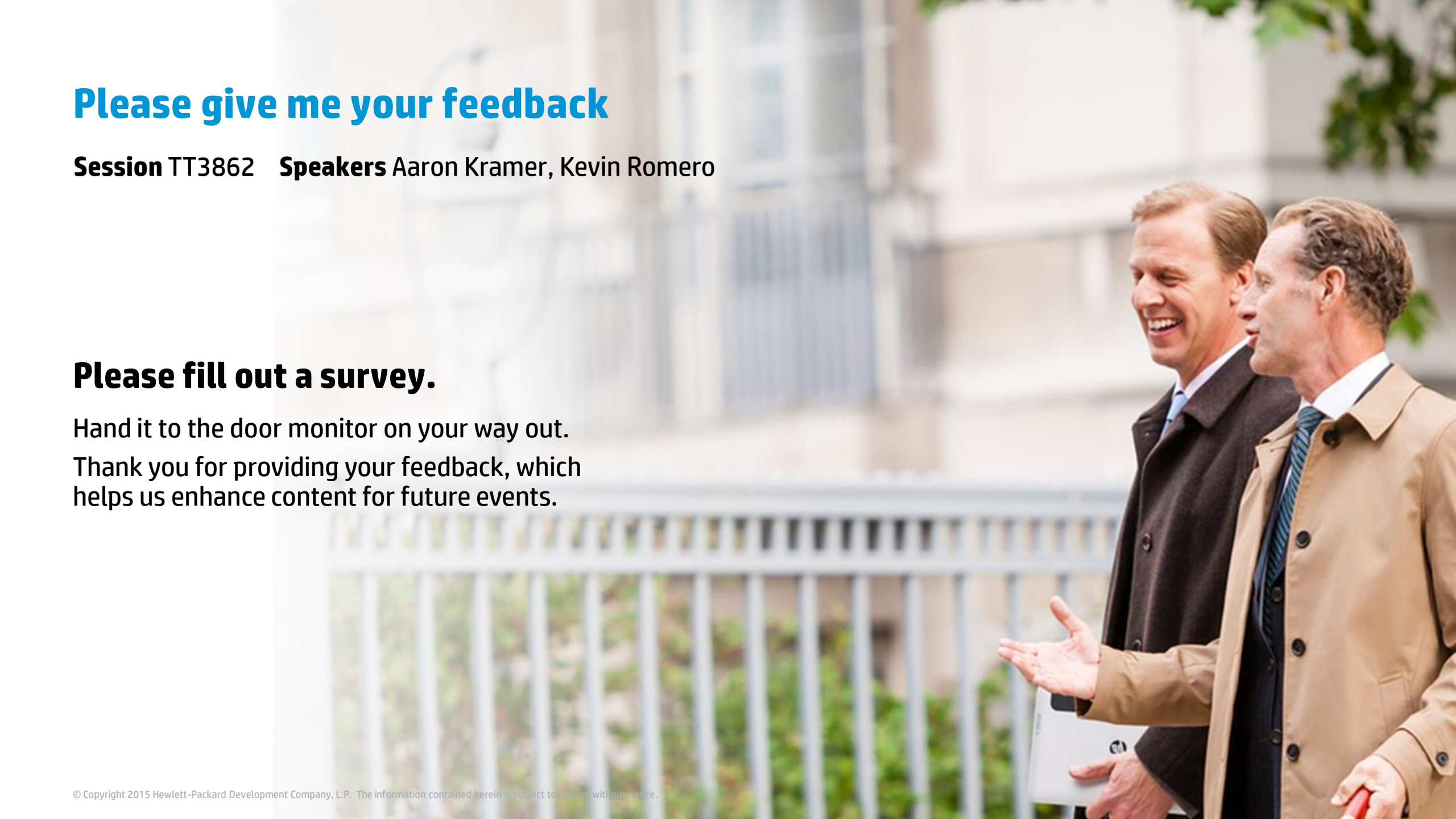
Brian Wolff and Paul Carman - Stunning Visualization for your Security events of HP ArSight SIEM through Interactive Discovery - **Thursday 2pm**

B3926

Tim Wenzlau - Monitoring anomalous activities of the privileged – uncovering UBA use cases in ESM - **Thursday 9:00am**

Please give me your feedback

Session TT3862 **Speakers** Aaron Kramer, Kevin Romero



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