



Protect 2014

Washington, D.C. September 8-11

HP ArcSight SIEM and data privacy best practices

Jeff Northrop, CTO

International Association of Privacy
Professionals

jeff@jnorthrop.me

Frank Lange, Dipl.-Winf., CISSP, CEH

ArcSight Security Architect

frank.lange@hp.com

Privacy is a data security issue

Jeff Northrop, CTO

International Association of Privacy Professionals

jeff@jnorthrop.me



Consumers Care About Privacy



Privacy: Top Issue Around the World

The Web We Want Project (<https://webwewant.mozilla.org>)

What kind of Web do you want?

I want a Web that:



When you select any of the sharing links, we add your location to the map to show the worldwide impact of our community.

Privacy: Top Issue Around the World

The Web We Want Project (<https://webwewant.mozilla.org>)



Privacy: A Competitive Differentiator

Microsoft's Scroogled (<http://scroogled.com>)

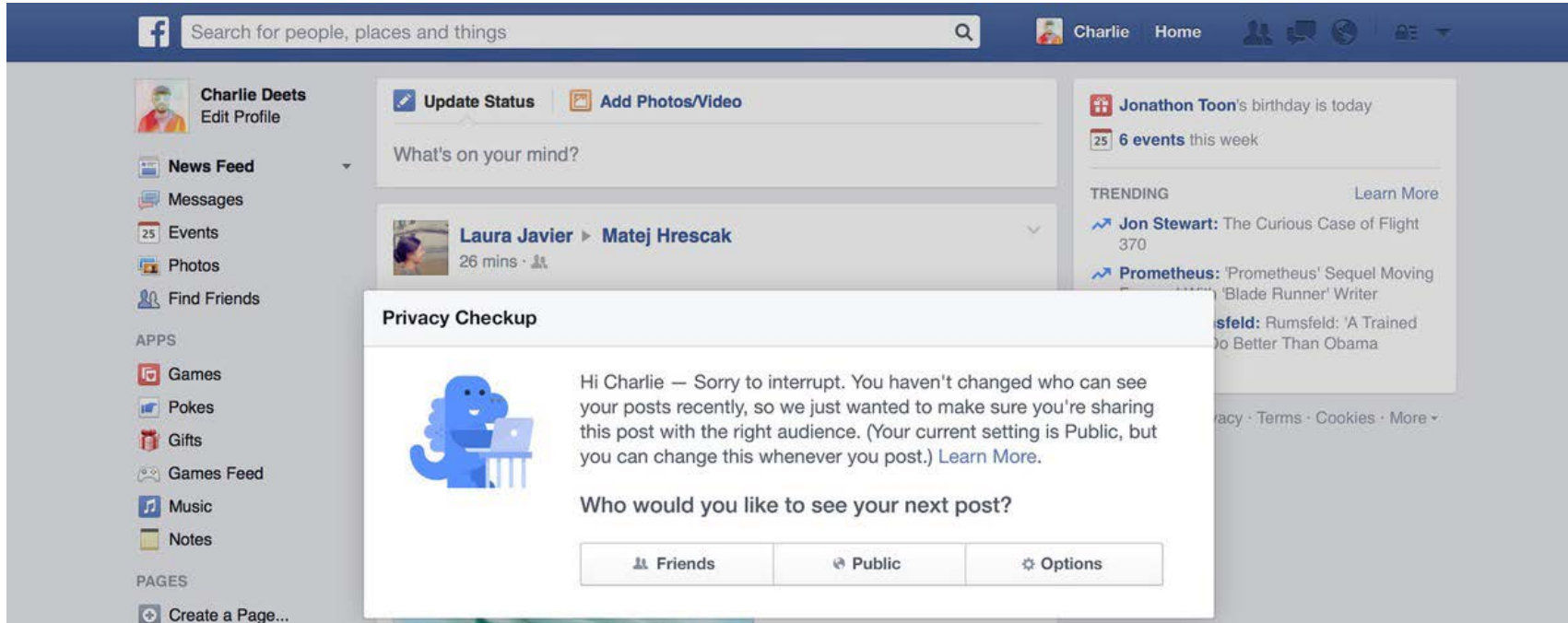
The screenshot shows the Scroogled website interface. At the top, there is a dark navigation bar with a home icon, the text "Ways you get Scroogled!", and links for "Scroogled News", "Store", and "Blog". Below the navigation bar is the "SCROOGLED!" logo in multi-colored letters, followed by "Privacy" and an information icon. To the right, there is a form to "Receive the latest Scroogled news via email:" with a text input field for "Your e-mail address" and a "Submit >" button. Below the form is a link for "Privacy Statement".

Below the navigation bar is a grey bar with social media icons for Facebook and Twitter, and the hashtag "#scroogled".

The main content area features a news article snippet titled "Google Accused of Wiretapping in Gmail Scans — The New York Times". The article text reads: "NYT: Google also argued that non-Gmail users had no expectation of privacy when corresponding with Gmail users." Below the text is a red document icon and a link: "PDF: Read Google's defense >". Below the link is the text: "Watch the video to see how you get Scroogled." To the right of the text is a video player with a large white warning triangle overlay and a "Watch video" button.

Privacy: A Value Proposition

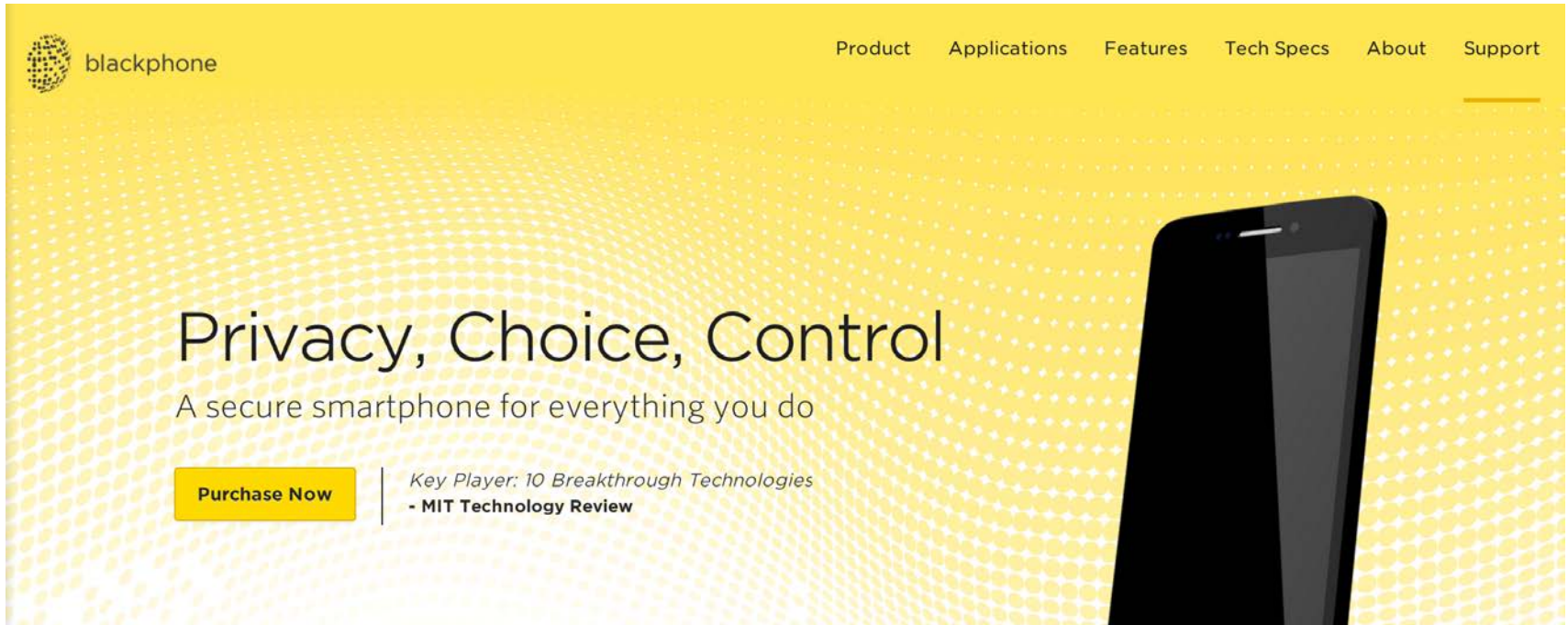
Facebook's anonymous login, privacy dinosaur, enhanced controls, etc.



The image shows a screenshot of a Facebook profile page for Charlie Deets. The page includes a search bar at the top, a navigation menu on the left with options like News Feed, Messages, Events, Photos, Find Friends, and various apps (Games, Pokes, Gifts, Games Feed, Music, Notes), and a main content area with an 'Update Status' prompt and a post by Laura Javier. A 'Privacy Checkup' dialog box is overlaid on the page, featuring a blue dinosaur mascot and the following text: 'Hi Charlie — Sorry to interrupt. You haven't changed who can see your posts recently, so we just wanted to make sure you're sharing this post with the right audience. (Your current setting is Public, but you can change this whenever you post.) Learn More.' Below the text, there are three buttons: 'Friends', 'Public', and 'Options'.

Privacy: The Main Value Proposition

Silent Circle Blackphone (<https://www.blackphone.ch>)



blackphone

Product Applications Features Tech Specs About Support

Privacy, Choice, Control

A secure smartphone for everything you do

[Purchase Now](#)

Key Player: 10 Breakthrough Technologies
- MIT Technology Review

Consumers Care About Privacy



Notice and Consent Does Not Work

Report to the President: Big Data and Privacy (<http://www.whitehouse.gov>)

"Notice and consent is the practice of requiring individuals to give positive consent to the personal data collection practices of each individual app, program, or web service. Only in some fantasy world do users actually read these notices and understand their implications before clicking to indicate their consent."

- President's Council of Advisors on Science and Technology

Regulators Respond

FTC Chairwoman vows to sue companies that collect large amounts of data and misuse it



Regulators Respond

Statistics to consider

- Of the top 10 privacy lawsuits in history, 2013 registered 4 of them. *Source: [Jay Cline](#)*
- Among the 130 “significant” Safe Harbor enforcement actions since 1999, 60% were after 2011. *Source: [Jay Cline](#)*
- Among the 50 data security cases since 2000, half came after 2010. The FTC had begun to deliberately strengthen its foray into holding businesses accountable for specific data security inadequacies through its unfairness power. *Source: [IAPP](#)*
- Prior to 2011 the FTC brought ~3 legal actions/year for violations of consumers’ privacy rights, or those that misled consumers by failing to maintain security for sensitive information. Between 2011 and 2013 there were ~5 such cases/year. *Source: FTC*

FTC's Authority Is Tested in Court

Wyndham case provides a benchmark moment

- **FTC has settled with dozens of companies over accusations of being “unfair,” Wyndham was the first not to settle out of court.**
- **Wyndham suffered a breach of more than 500k records including credit card information. The FTC complaint charged, “the security practices were unfair and violated the FTC Act” due to “Wyndham’s inadequate security procedures.”**
- **In motion to dismiss Wyndham set first court testing case of “FTC authority to go after ‘unfairness’”**
- **FTC prevailed in a district court ruling.**
- **Game changer**

Regulators Respond Globally

Greater enforcement in Europe, and 100 other countries



The Future Is Now: Enterprise Is Accountable

Privacy risk mitigation requires more than compliance with applicable laws a regulations



You Need to Know your Data

Data security needs to play key role in mitigating privacy risk



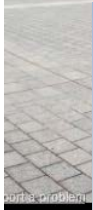
Data privacy in the SIEM world

Frank Lange, Dipl.-Winf., CISSP, CEH
ArcSight Security Architect
frank.lange@hp.com

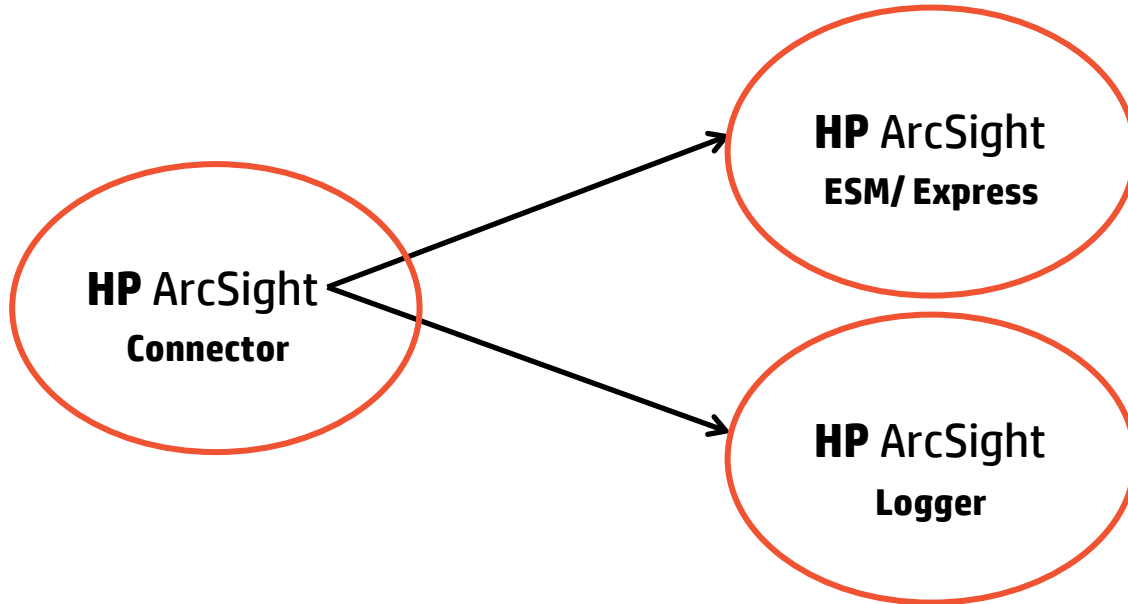


A StreetView example

[Comments](#) [Upload photos](#)



Elements we will talk about



Connector



Connector obfuscation - configuration

Destination specific setting in <agentID.xml>

- One or many fields
- Uses hash algorithm
 - MD5
 - SHA256 (FIPS)
- One way operation
- High performance

. \current\user\agent\3nOjT4xEBABCBuS8G8BXhnw==.xml

| Connector | Networks | Default | Alternate#1 | Notes |
|------------------------------|------------------|---------|-------------|-------|
| Content | | | | |
| Filters | | | | |
| [-] Filter Aggregation | | | | |
| Time Interval | DISABLED | | | |
| Event Threshold | DISABLED | | | |
| Fields to Sum | | | | |
| [-] Processing | | | | |
| Preserve Raw Event | No | | | |
| Turbo Mode | Complete | | | |
| Enable Aggregation (in secs) | Disabled | | | |
| Limit Event Processing Rate | -1 | | | |
| Fields to Obfuscate | Source User Name | | | |
| | Target User Name | | | |

Connector obfuscation – ESM console view

| End Time | Name | Attacker User Name | Target User Name | Attacker Address | Target Address |
|--------------------------|-----------------------|--------------------|------------------|------------------|----------------|
| 21 Aug 2013 00:11:04 PDT | DB access attempt | mwhite | sys | | 10.0.112.213 |
| 21 Aug 2013 00:11:02 PDT | User Account Deleted | Santos | gwashington | | 10.0.112.215 |
| 21 Aug 2013 00:11:02 PDT | User Account Deleted | santos | gwashington | | 10.0.112.215 |
| 21 Aug 2013 00:11:02 PDT | User Account Deletion | Santos | gwashington | | 10.0.112.215 |
| 21 Aug 2013 00:11:02 PDT | User Account Deletion | Santos | gwashington | | 10.0.112.215 |
| 21 Aug 2013 00:11:02 PDT | User Account Deletion | santos | gwashington | | 10.0.112.215 |
| 21 Aug 2013 00:11:02 PDT | User Account Deletion | santos | gwashington | | 10.0.112.215 |

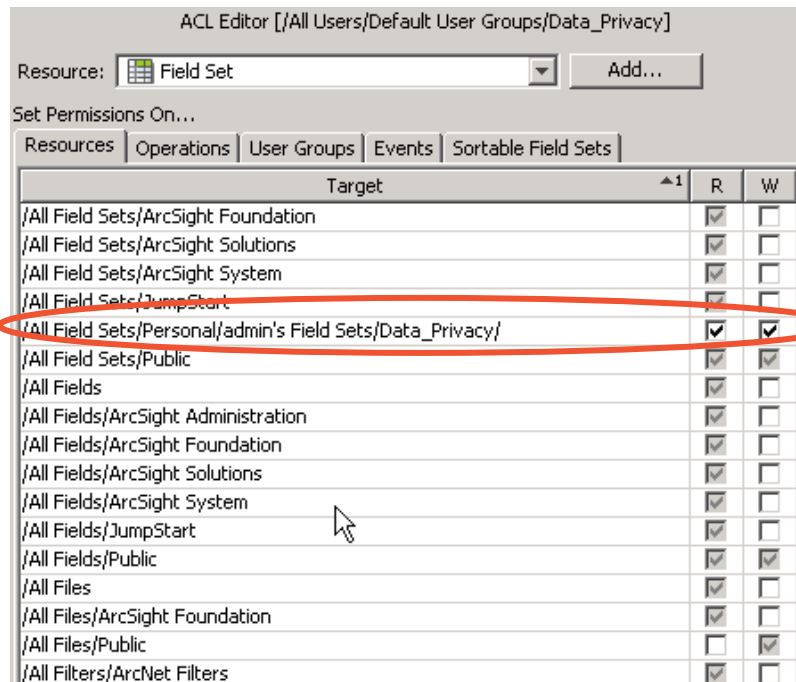
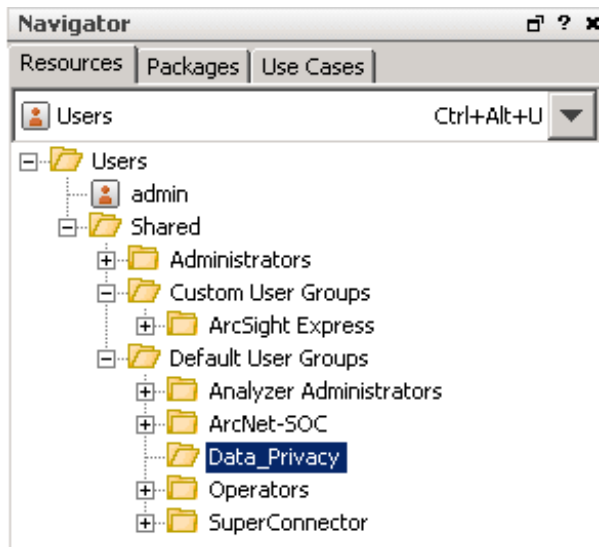


| End Time | Name | Attacker User Name | Target User Name | Attacker Address | Target Address |
|--------------------------|---|-----------------------|-------------------|------------------|----------------|
| 20 Aug 2013 06:56:29 PDT | User Account Deletion | 6f816c94fe41d47a5d... | 7367fdb594821... | | 10.0.112.211 |
| 20 Aug 2013 06:56:29 PDT | User Account Deletion | 6f816c94fe41d47a5d... | 7367fdb594821... | | 10.0.112.211 |
| 20 Aug 2013 06:56:29 PDT | Logon Failure | 200CEB26807D6BF99... | DE2F15D014D40... | 10.0.113.27 | 172.16.1.10 |
| 20 Aug 2013 06:56:29 PDT | Failed Authentication - Windows Work... | 200ceb26807d6bf99f... | de2f15d014d40b... | 10.0.113.27 | 172.16.1.10 |
| 20 Aug 2013 06:56:28 PDT | TCP_MISS | 336D5EBC5436534E6... | | 10.10.30.200 | 192.168.4.205 |
| 20 Aug 2013 06:56:28 PDT | User Account Deleted | F3E3016C9F958241A... | 7792144DADB7... | | 10.0.112.207 |
| 20 Aug 2013 06:56:28 PDT | TCP_MISS | 336D5EBC5436534E6... | | 10.10.30.200 | 192.168.4.205 |

ESM/Express



ESM/Express – role-based access



Access Control Lists (ACL) based on user groups with inheritance



ESM/Express – I. FieldSets

FieldSet

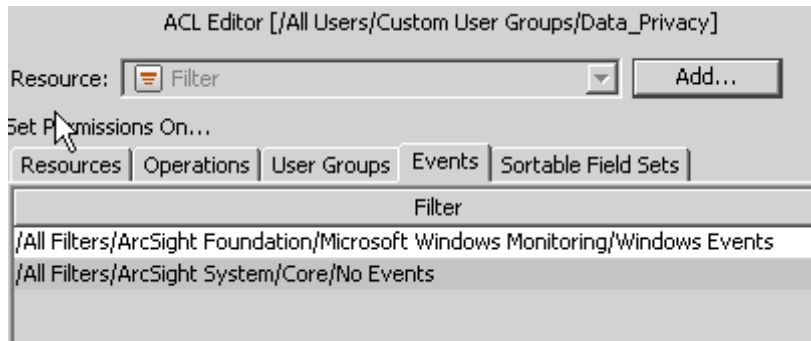
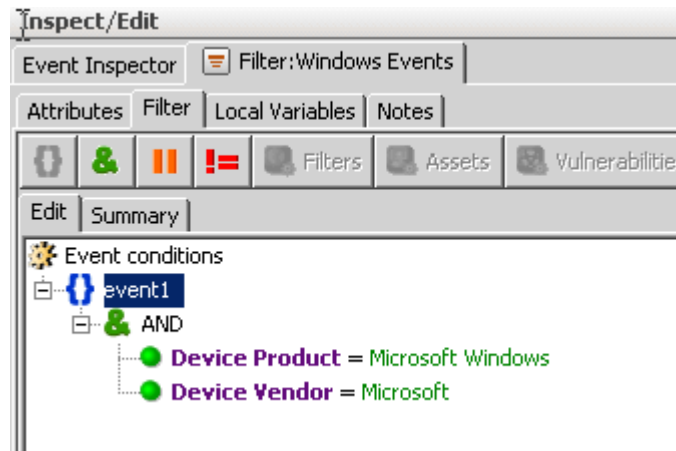
- A number of fields in specific order
- ActiveChannel allows default FieldSet
- Adhoc customizable (Add/Remove Column)

The screenshot displays the ESM/Express interface. At the top left is a 'Radar' chart. Below it is a table with columns for 'End Time', 'Attacker Address', and 'Target'. A context menu is open over the table, showing options like 'Text and Icon', 'Text Only', 'Icon Only', 'Sort Column', 'Remove Sort', 'Columns', and 'Size Column to Fit'. The 'Columns' option is selected, and a sub-menu is open showing 'Add/Remove Column' and 'Replace This Column'. On the right side, a 'Field Set:Field Set Based On A...' window is open, showing a list of fields under 'Selected Fields'. The fields listed are: Manager Receipt Time, Name, Attacker Address, and Target Address. Below this window, a list of available fields is shown, including: Transport Protocol, Type, Vulnerability, Vulnerability External ID, Vulnerability ID, Vulnerability Name, Vulnerability Resource, Vulnerability URI, Category, Threat, Agent, Attacker Geo Latitude, Attacker Geo Location Info, Attacker Geo Longitude, Attacker Geo Postal Code, Attacker Geo Region Code, **Attacker Host Name**, Attacker Mac Address, Attacker Nt Domain, Attacker Port, Attacker Process ID, and Attacker Process Name.

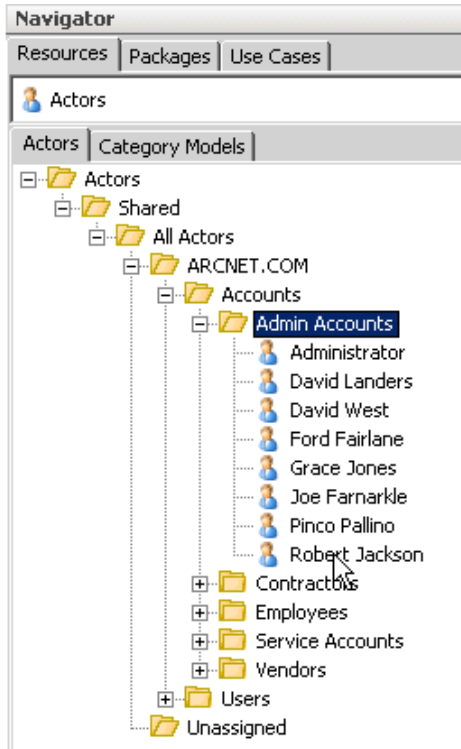
ESM/Express – II. Event Filter

Restricts access to a subset of events

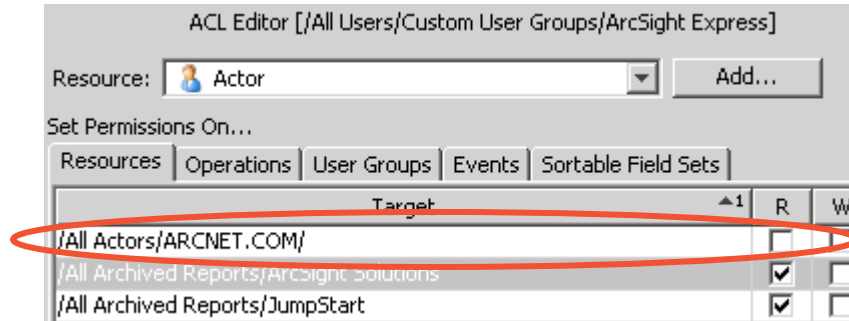
- Based on standard Filters
- Enforced on User Group level
- Transparent to the user



ESM/Express – III. Actors



- IdentityView
- Granular restriction via ACL
- Restriction on all Actors / a Domain / Types
- Allows Mixed Mode



ESM/Express – III. Actors

| End Time | Name | ActorByAccountID.Full N | ActorByAccountID.Depa | Attacker User Name | Target User Name |
|--------------------------|---------------------------|-------------------------|-----------------------|--------------------|------------------|
| 21 Aug 2013 05:24:59 PDT | GRANT ROLE | Robert Jackson | Facilities | RJACKSON | RJACKSON_DBA |
| 21 Aug 2013 05:24:59 PDT | CREATE USER | Robert Jackson | Facilities | RJACKSON | RJACKSON_DBA |
| 21 Aug 2013 05:24:59 PDT | LOGON | Robert Jackson | Facilities | RJACKSON | RJACKSON_DBA |
| 21 Aug 2013 05:24:59 PDT | Successful Logon | Robert Jackson | Facilities | | RJACKSON |
| 21 Aug 2013 05:24:58 PDT | Authentication successful | Robert Jackson | Facilities | | RJACKSON |
| 21 Aug 2013 05:24:58 PDT | Physical Access Granted | Robert Jackson | Facilities | | rjackson |
| 21 Aug 2013 05:24:57 PDT | Audit Log Cleared | Josh Coleman | Finance | | JOSHC |
| 21 Aug 2013 05:24:56 PDT | Job Printed | Josh Coleman | Finance | | JOSHC |
| 21 Aug 2013 05:24:55 PDT | Successful Logon | Josh Coleman | Finance | | JOSHC |



| End Time | Name | ActorByAccountID | ActorByAccountID | Attacker User Name | Target User Name |
|--------------------------|---|------------------|------------------|--------------------|------------------|
| 21 Aug 2013 05:24:59 PDT | GRANT ROLE | | | RJACKSON | RJACKSON_DBA |
| 21 Aug 2013 05:24:59 PDT | CREATE USER | | | RJACKSON | RJACKSON_DBA |
| 21 Aug 2013 05:24:59 PDT | LOGON | | | RJACKSON | RJACKSON_DBA |
| 21 Aug 2013 05:24:59 PDT | Role Violation | | | RJACKSON | RJACKSON_DBA |
| 21 Aug 2013 05:24:59 PDT | After Hours Database Access by At Ri... | | | RJACKSON | RJACKSON_DBA |

Not an all-or-nothing option, allows view of actor data based on membership level

Logger



Logger – Search Group Filter

Restricts access to a subset of events only

- Restriction based on user group membership
- transparent to the Logger user
- RegEx filters
- Applies on peer Loggers
- Performance on RegEx speed

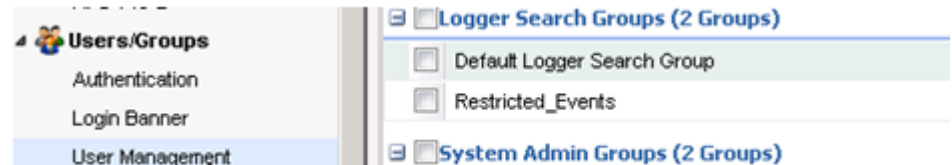
Filters | Search Group Filters

Edit Search Group Filter

You may assign a search filter to a search group that will be appended to all search results.

To create a new search group filter, you must first go to the [Filters](#) page and add a search group.

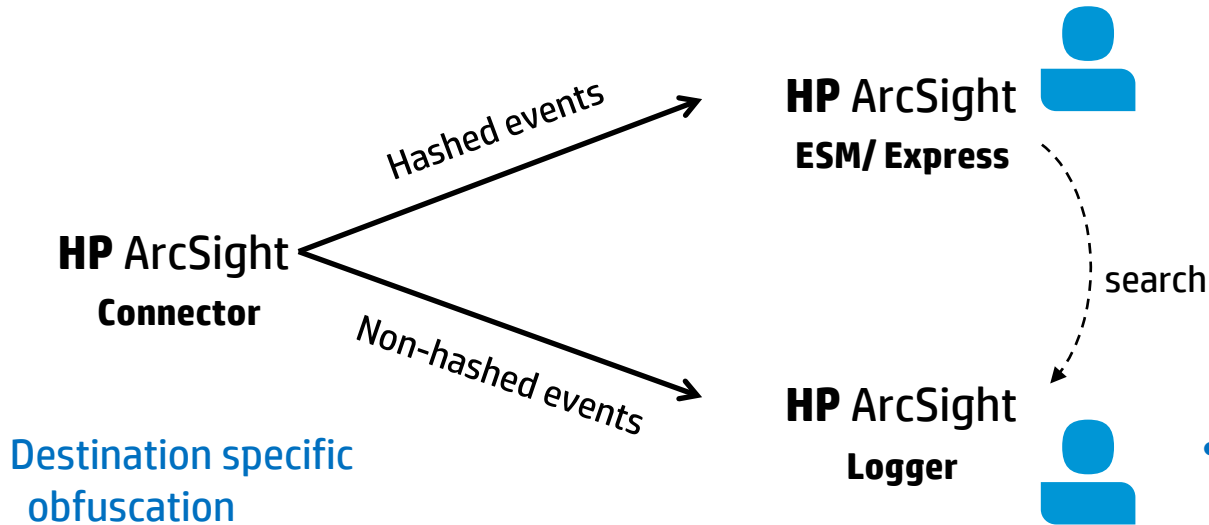
Filter:



All together



A powerful mix – example scenario



- Only obfuscated events to ESM
- Special User with Logger Integration Command can search for unobfuscated data on remote Logger within ESM console

- Only special user is allowed to access unobfuscated data on Logger

Summary

Multi-layer approach

Impact on SIEM design

Correlation and data privacy at the same time

Like a StreetView for SIEM



Tonight's party

@ Newseum

Time

7:00 – 10: 00 pm

Shuttles run between hotel's Porte Cochere (Terrace Level, by registration) and Newseum from **6:30 - 10:00 pm**

Questions?

Please visit the Info Desk by registration

Enjoy food, drinks, company, and a private concert by **Counting Crows**



Please give me your feedback

Session TB2990 **Speaker** Jeff Northrop and Frank Lange

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





Make it matter.