Security Analytics in Big Data

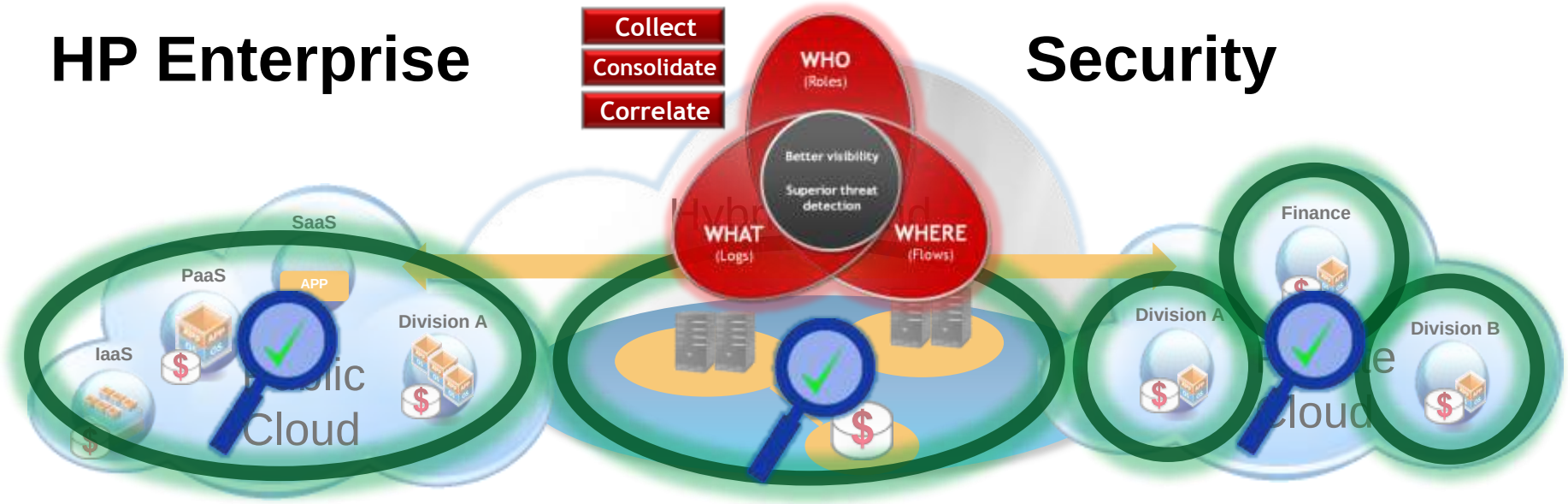
Alexandre F Moraes, CISSP

Solutions Architect Manager Latin America

HP Enterprise Security

afmoraes@hp.com

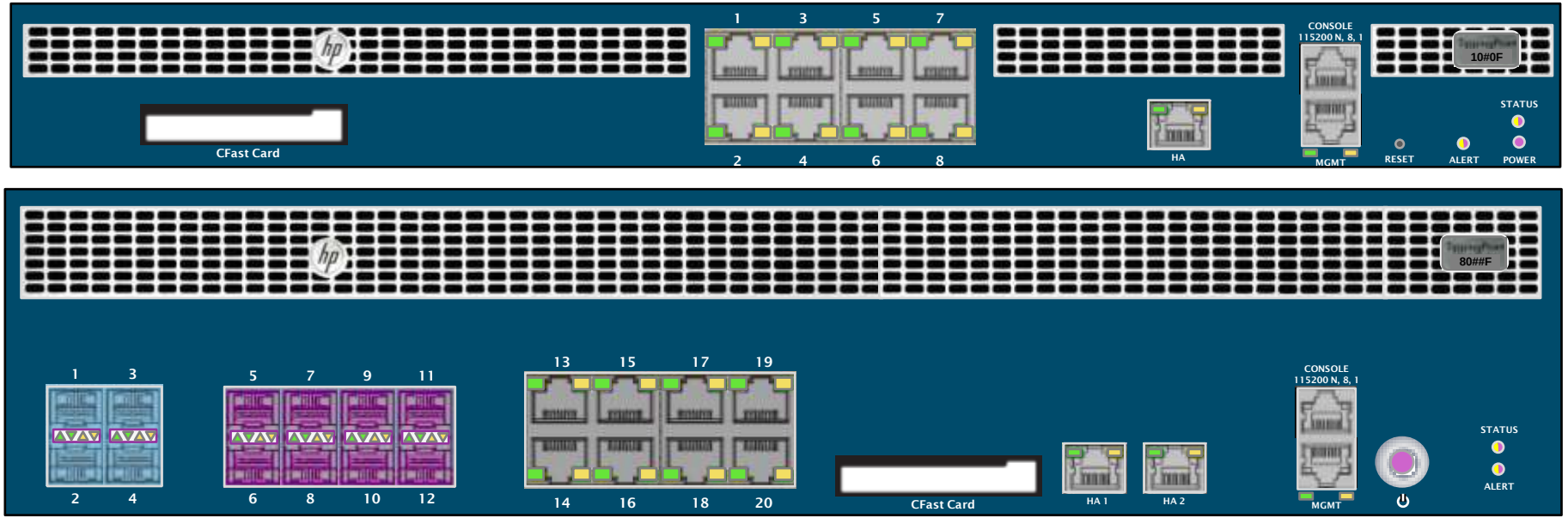
HP Enterprise Security



FORTIFY | TippingPoint | ArcSight

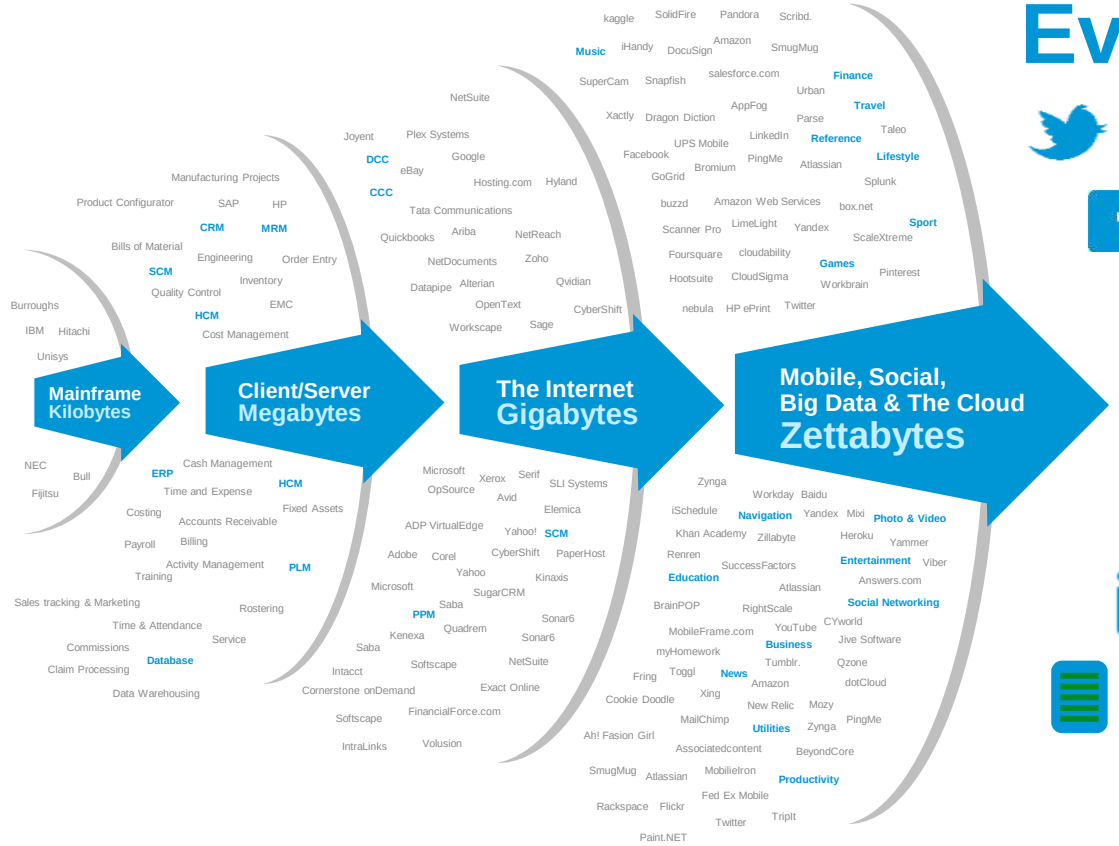
- **Vulnerability Awareness**
  - Vulnerability Scanning
  - Source Code Analysis
  - Software Security Assurance
- **Proactive Defense**
  - Flexible Security-Zone Segmentation
  - Well-Known- and Zero-Day-Exploit Protection
  - Adaptive Network Defense
- **Visibility**
  - Security-Information and Event Management System
  - Event Correlation
  - Context-Visibility

New ! NGFW



S1050F – 500Mbps / 250Mbps (FW+AppID / FW+IPS)	S8005F – 5Gbps / 2.5Gbps (FW+AppID / FW+IPS)
S3010F – 1Gbps / 500Mbps (FW+AppID / FW+IPS)	S8010F – 10Gbps / 5Gbps (FW+AppID / FW+IPS)
S3020F – 2Gbps / 1Gbps (FW+AppID / FW+IPS)	S8020F – 20Gbps / 10 Gbps (FW+AppID / FW+IPS)

Accelerating innovation & time to value



Every 60 seconds

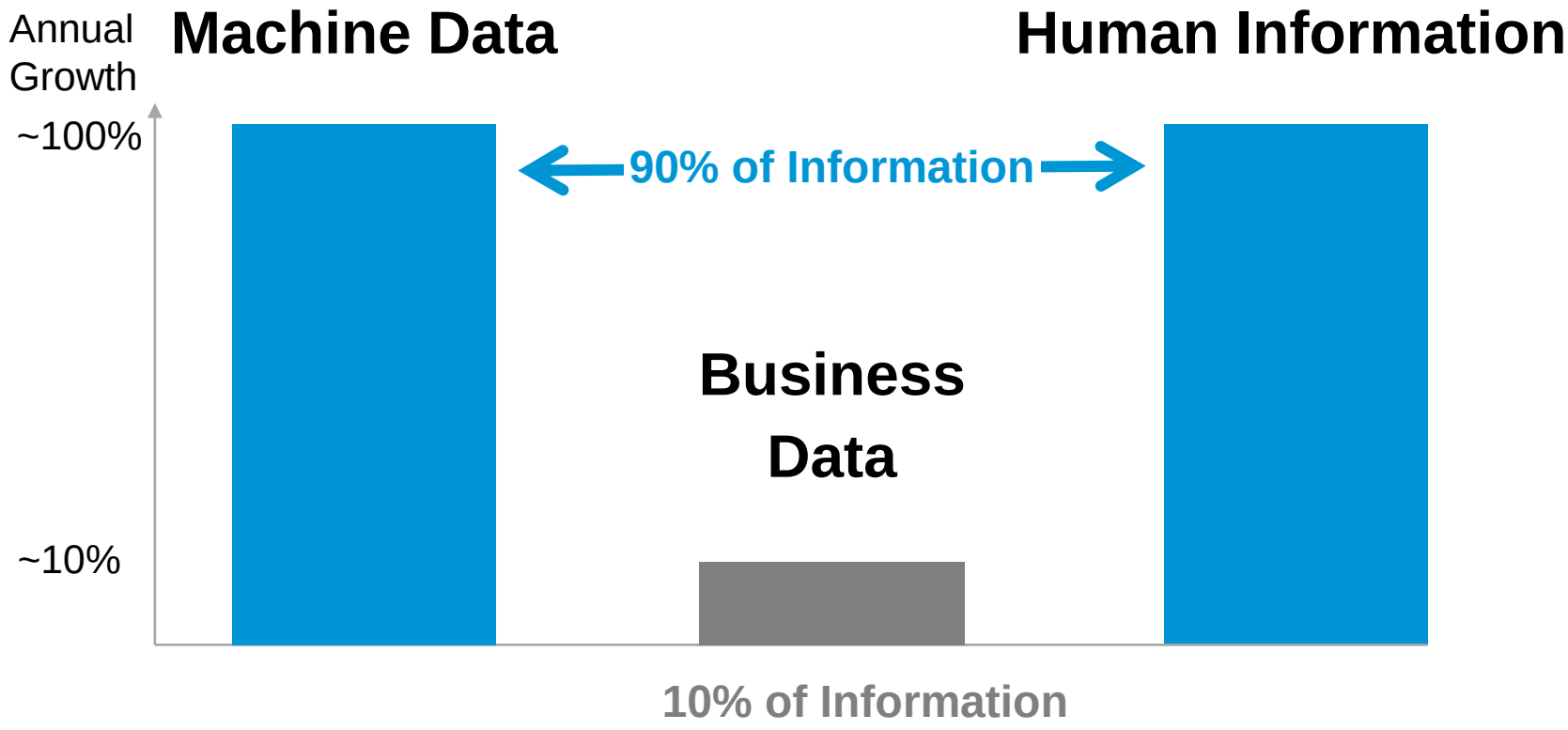
- **98,000+** tweets
- **695,000** status updates
- **11million** instant messages
- **698,445** Google searches
- **168 million+** emails sent
- **1,820TB** of data created
- **217** new mobile web users

Yottabytes

Big Data

- **Walmart : 1 Million of Transactions per Hour: 2.56 Terabytes / day**
- **Facebook: 50 Billions of pictures in the database**
- **50 % of the data is non structured: video, images, audio...**

Big Data landscape



Business challenge Opportunities lost

Competitive advantage in the digital universe in 2012

Massive amounts of useful data are getting lost

% of data that would be potentially useful IF tagged and analyzed

23%

3%

% actually being tagged for Big Data Value (will grow to 33% by 2020)

0.5%

% of the Digital Universe that actually is being tagged and analyzed

[1]Source: IDC The Digital Universe in 2020, December 2012

Technology challenge Legacy techniques have fallen short.

Stale technologies

Talent shortage

IT frustration

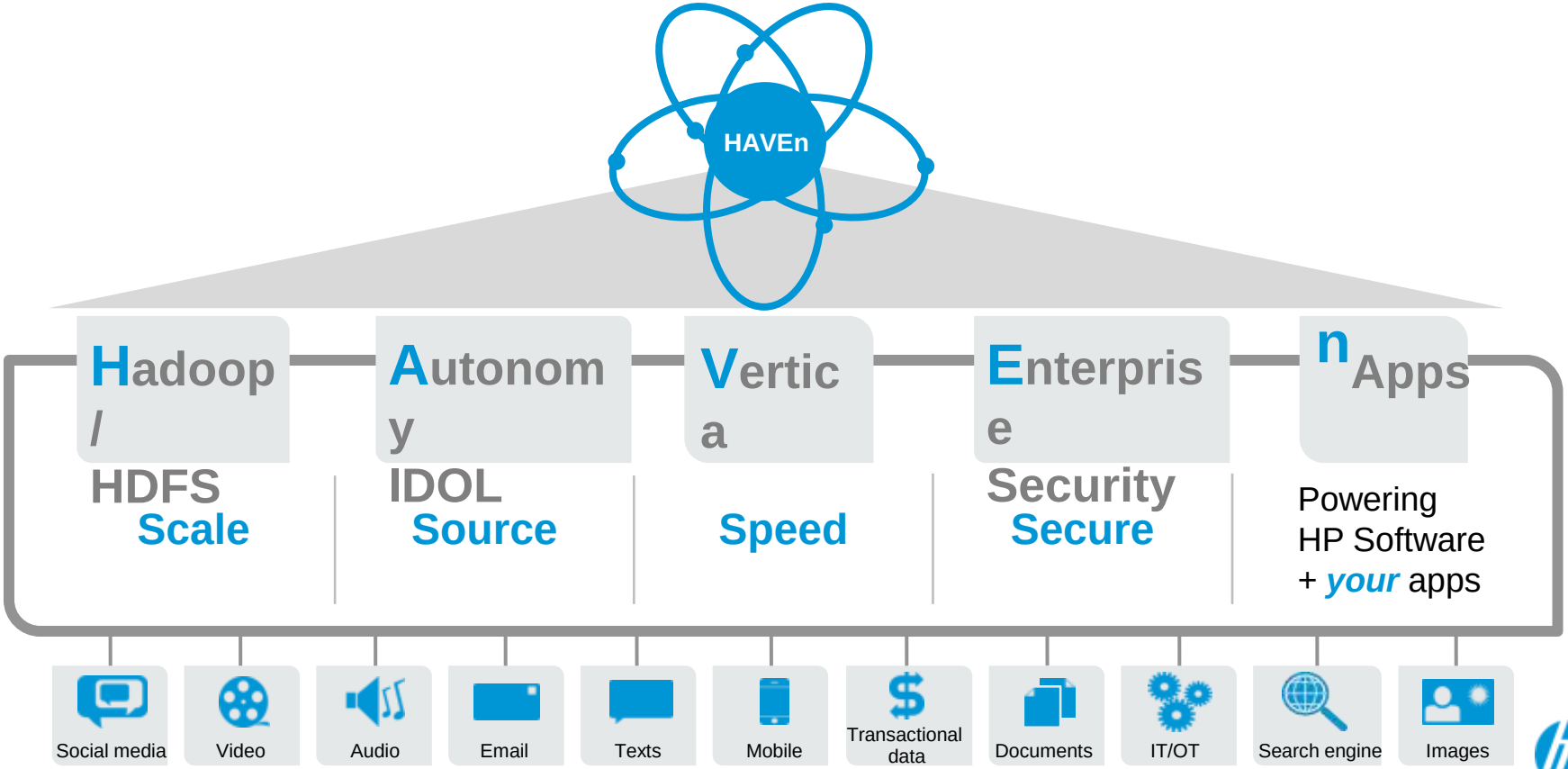
Lack of insight

86%

of corporations **cannot** deliver the right information, at the right **time** to support enterprise outcomes all of the time[3]

[3]Source: Coleman Parkes Survey Nov 2012

HAVEn – the #1 Big Data platform



hp.com/haven

Proactive Protection - Security Analytics

Turning events & logs into actionable intelligence

- Powered by HP HAVEn

Harness the power of ArcSight SIEM and Vertica Analytics

- Reduce false positives
- Minimize impact of security breach
- Transform security from defense to proactive protection

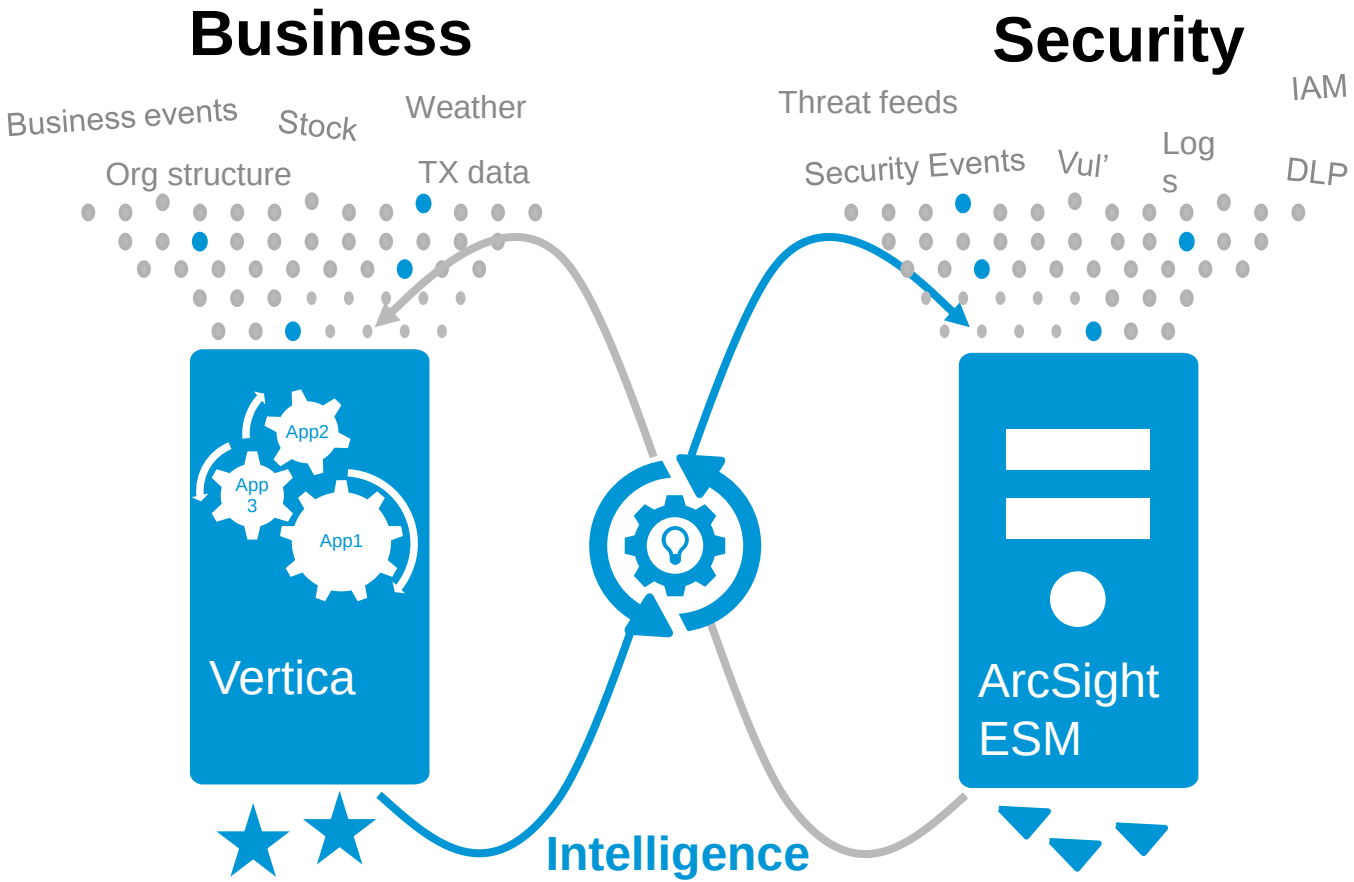
Hadoop

Autonomy

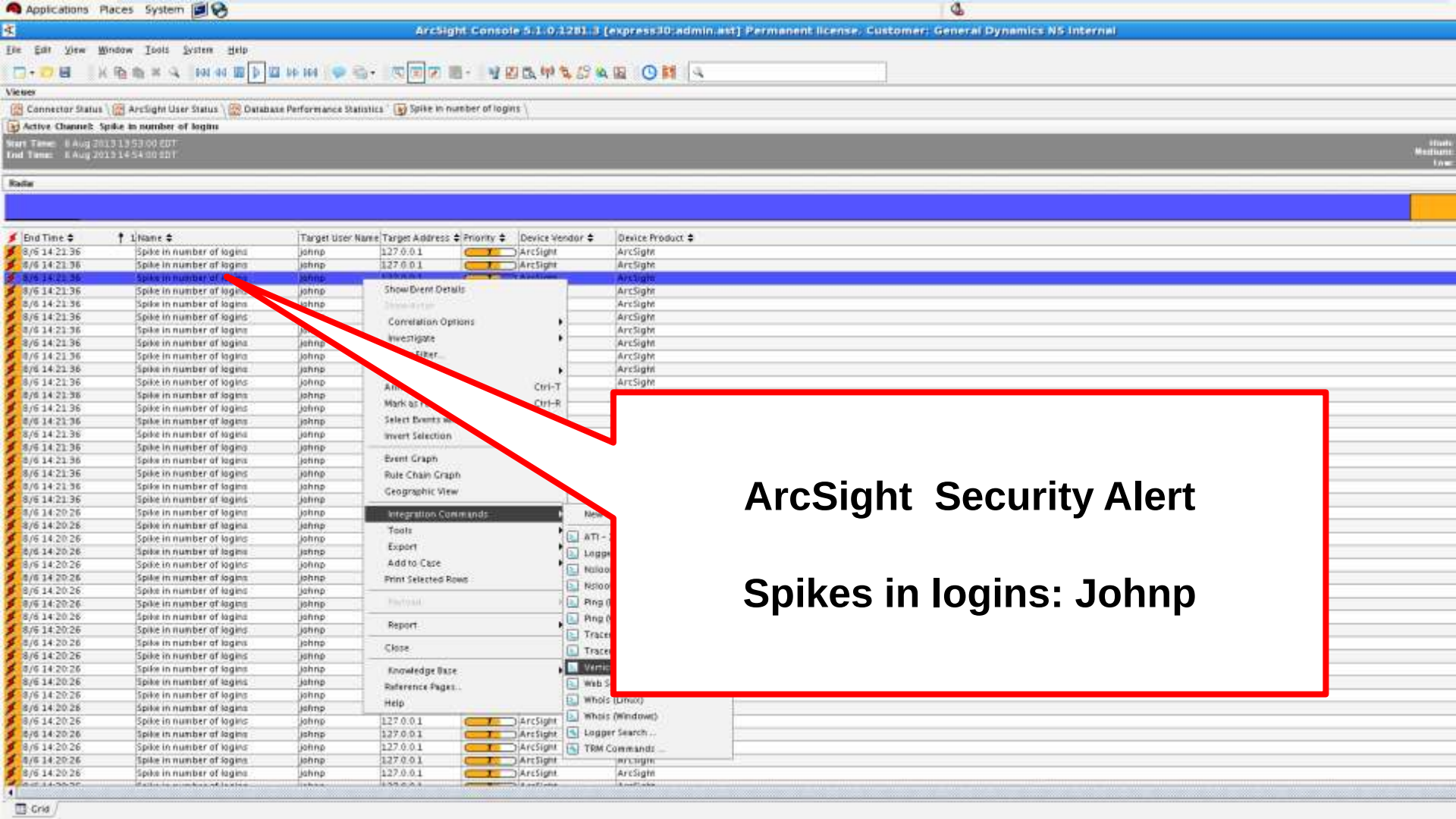
Vertica

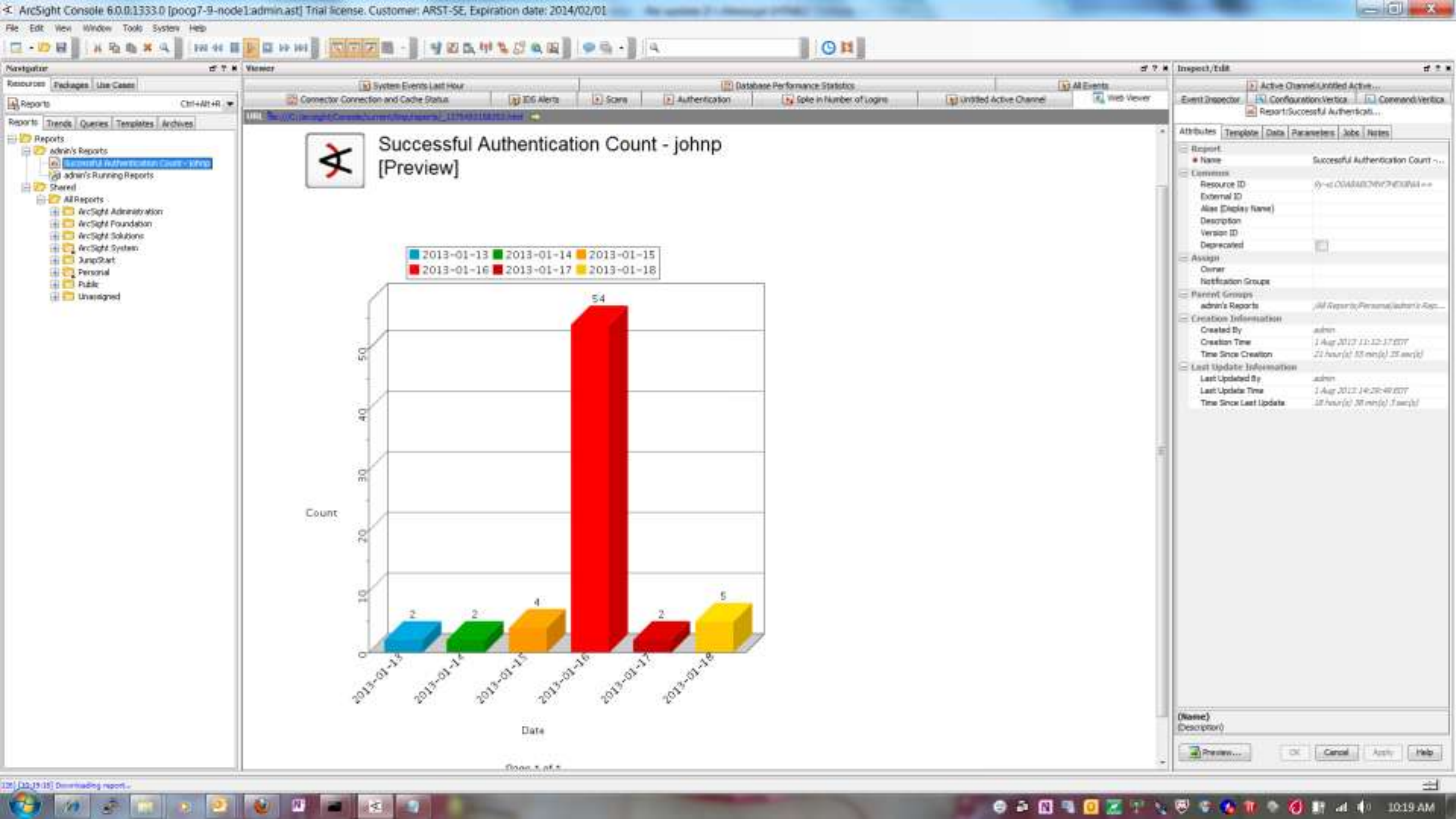
Enterprise Security

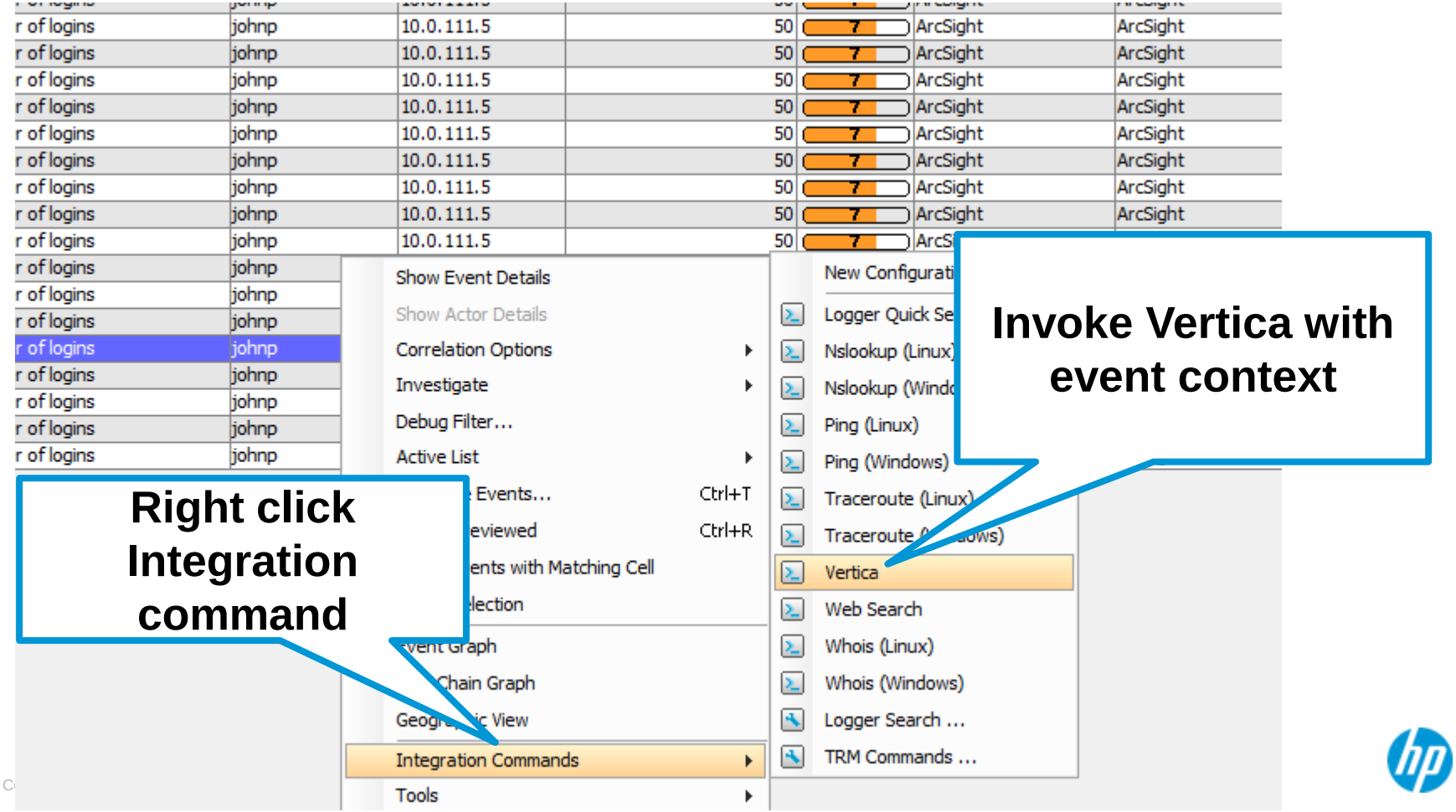
n-Apps

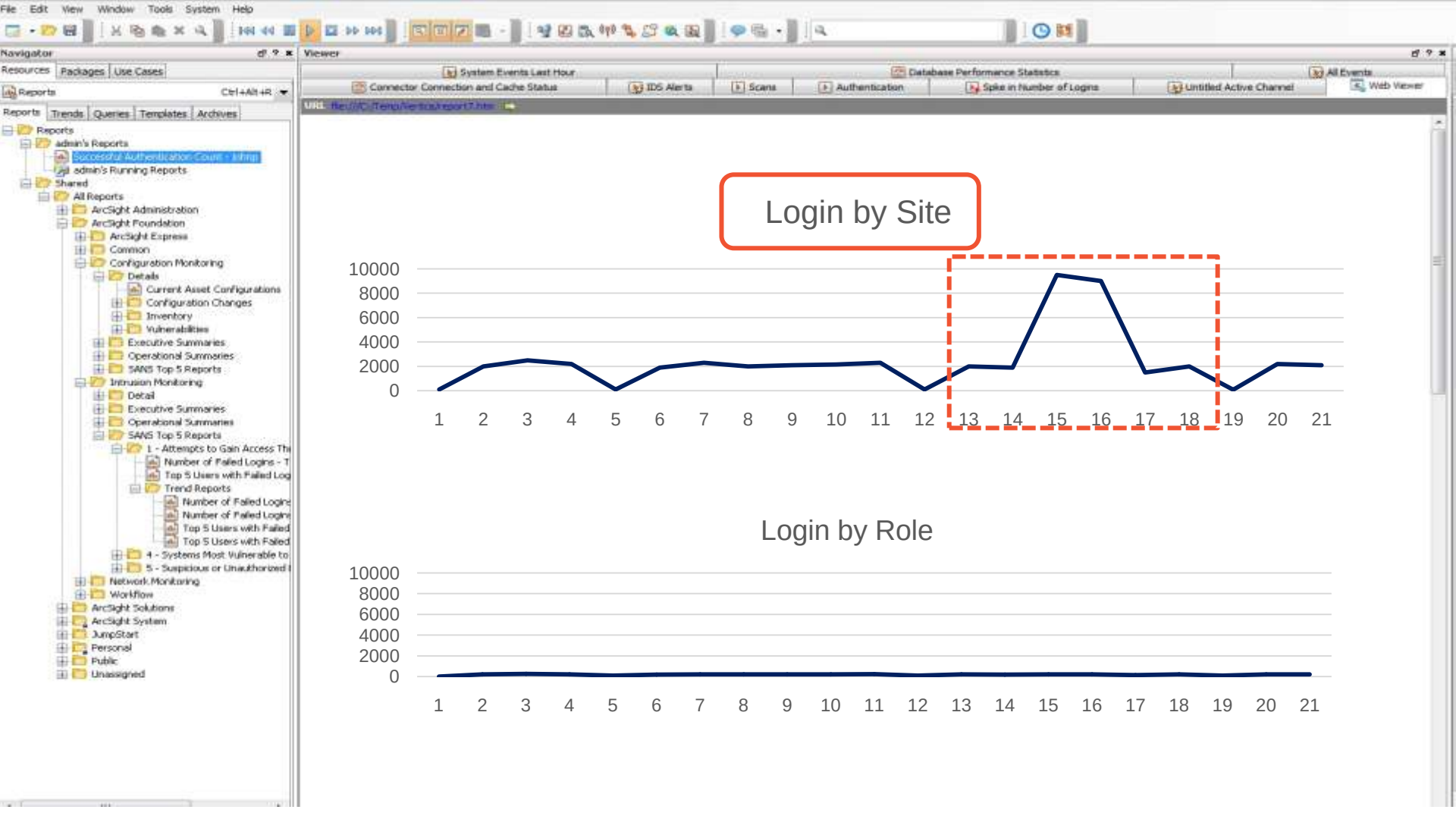


Events + context + analytics


ArcSight Console 5.1.0.1281.3 [express30:admin.ast] Permanent license, Customer: General Dynamics NS Internal
Spike in number of logins
End Time
Name
Target User Name
Target Address
Priority
Device Vendor
Device Product
johnp
127.0.0.1
ArcSight
Show Event Details
Correlation Options
Investigate
Integration Commands
Tools
Export
Add to Case
Print Selected Rows
Report
Close
Knowledge Base
Reference Pages...
Help
Event Graph
Rule Chain Graph
Geographic View
Invert Selection
Whois (Linux)
Whois (Windows)
Logger Search...
TRM Commands...
ArcSight Security Alert
Spikes in logins: Johnp


ArcSight Console 6.0.0.1333.0 [pocg7-9-node1:admin.ast] Trial license. Customer: ARST-SE, Expiration date: 2014/02/01
File Edit View Window Tools System Help
Navigator
Resources Packages Use Cases
Reports Ctrl+Alt+R
Reports Trends Queries Templates Archives
Reports
admin's Reports
Successful Authentication Count - johnp
admin's Running Reports
Shared
All Reports
ArcSight Administration
ArcSight Foundation
ArcSight Solutions
ArcSight System
JumpStart
Personal
Public
Unassigned
Viewer
System Events Last Hour
Database Performance Statistics
All Events
Connector Connection and Cache Status
IDS Alerts
Scans
Authentication
Spike in Number of Logins
Untitled Active Channel
Web Viewer
Successful Authentication Count - johnp
[Preview]
2013-01-13
2013-01-14
2013-01-15
2013-01-16
2013-01-17
2013-01-18
Count
Date
54
2
2
4
2
5
0
10
20
30
40
50
Inspect/Edit
Active Channel:Untitled Active...
Event Inspector
Configuration:Vertica
Command:Vertica
Report:Successful Authenticati...
Attributes Template Data Parameters Jobs Notes
Report
Name
Successful Authentication Count -...
Common
Resource ID
External ID
Alias (Display Name)
Description
Version ID
Deprecated
Assign
Owner
Notification Groups
Parent Groups
admin's Reports
Creation Information
Created By
admin
Creation Time
Time Since Creation
Last Update Information
Last Updated By
admin
Last Update Time
Time Since Last Update
(Name)
(Description)
Preview...
OK
Cancel
Apply
Help
Downloading report...
10:19 AM


r of logins johnp 10.0.111.5 50 7 ArcSight ArcSight
Show Event Details
Show Actor Details
Correlation Options
Investigate
Debug Filter...
Active List
Events... Ctrl+T
eviewed Ctrl+R
ents with Matching Cell
lection
Integration Commands
Tools
New Configurati
Logger Quick Se
Nslookup (Linux)
Nslookup (Windo
Ping (Linux)
Ping (Windows)
Traceroute (Linux)
Traceroute (
ows)
Vertica
Web Search
Whois (Linux)
Whois (Windows)
Logger Search ...
TRM Commands ...
Right click Integration command
Invoke Vertica with event context


File Edit View Window Tools System Help
Navigator
Resources Packages Use Cases
Reports Ctrl+Alt+R
Reports Trends Queries Templates Archives
Reports
admin's Reports
Successful Authentication Count - Isilingo
admin's Running Reports
Shared
All Reports
ArcSight Administration
ArcSight Foundation
ArcSight Express
Common
Configuration Monitoring
Details
Current Asset Configurations
Configuration Changes
Inventory
Vulnerabilities
Executive Summaries
Operational Summaries
SANS Top 5 Reports
Intrusion Monitoring
Detail
Executive Summaries
Operational Summaries
SANS Top 5 Reports
1 - Attempts to Gain Access Thi
Number of Failed Logins - T
Top 5 Users with Failed Log
Trend Reports
Number of Failed Logins
Number of Failed Logins
Top 5 Users with Failed
Top 5 Users with Failed
4 - Systems Most Vulnerable to
5 - Suspicious or Unauthorized
Network Monitoring
Workflow
ArcSight Solutions
ArcSight System
JumpStart
Personal
Public
Unassigned
Viewer
System Events Last Hour
Database Performance Statistics
All Events
Connector Connection and Cache Status
IDS Alerts
Scans
Authentication
Spike in Number of Logins
Untitled Active Channel
Web Viewer
URL file:///C:/Temp/Vertica/report7.html
Login by Site
10000
8000
6000
4000
2000
0
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21
Login by Role
10000
8000
6000
4000
2000
0
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21

Proactive Protection - Security Analytics

Detecting Information Leakage

- Powered by HP HAVEn

Harness the power of ArcSight SIEM and Autonomy IDOL

- Distill meaning and make decisions based on it, not just match keywords or tags
- “judge” events based on their context

Hadoop

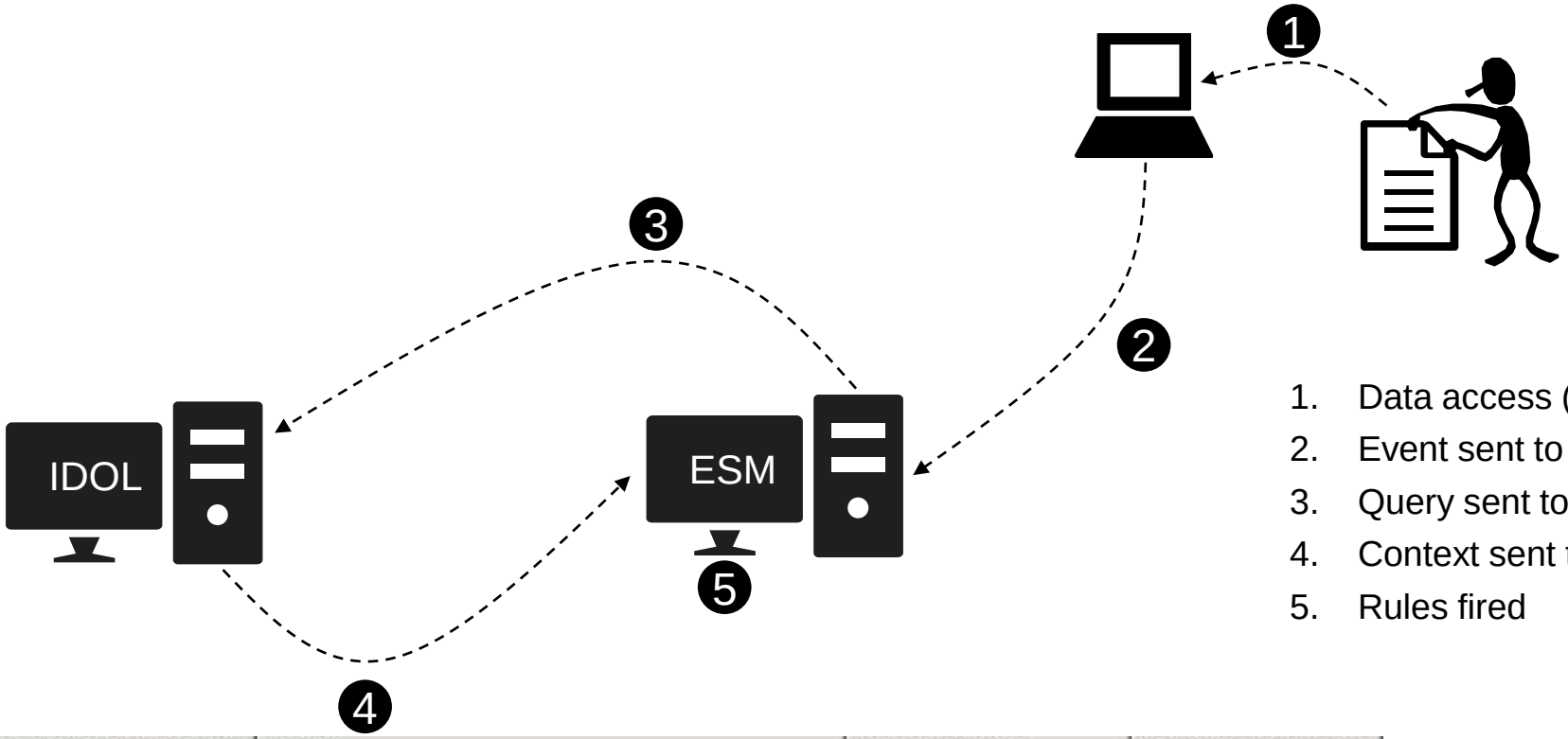
Autonomy

Vertica

Enterprise Security

n-Apps

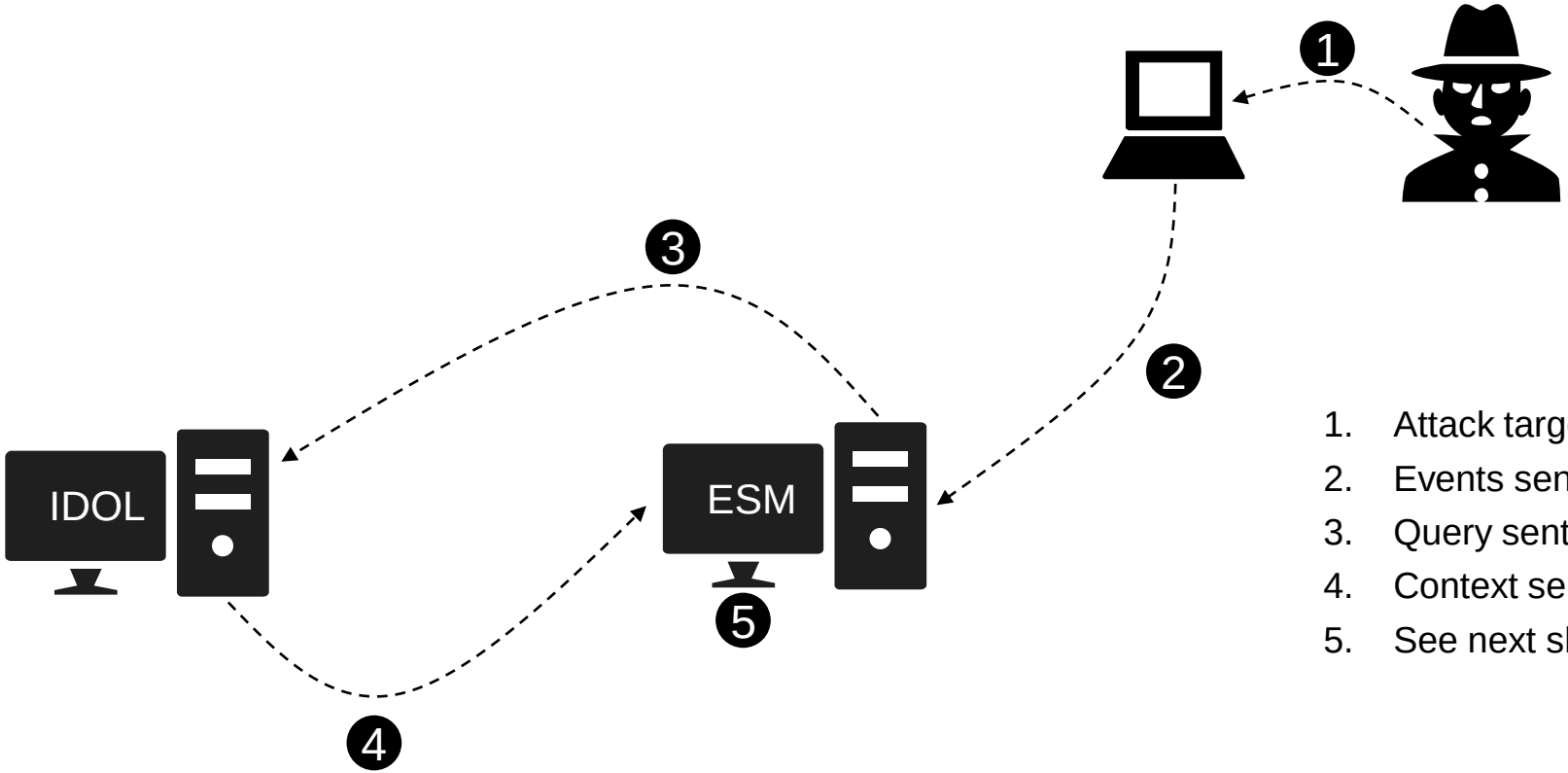
Sample Usecase: Detecting Information Leakage



1. Data access (file, email)
2. Event sent to ESM
3. Query sent to IDOL
4. Context sent to ESM
5. Rules fired

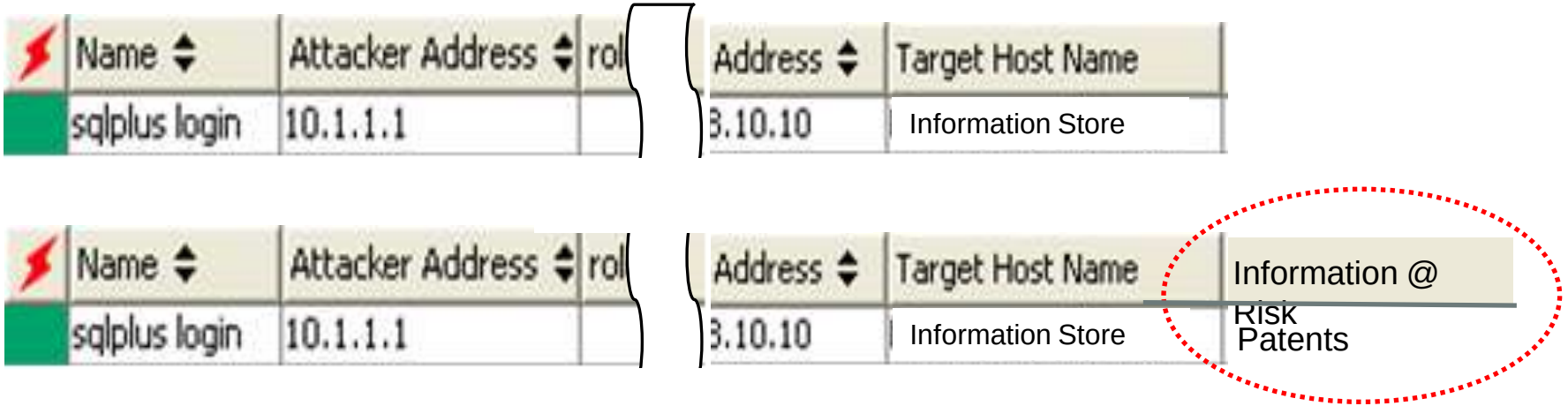
Manager Receipt Time	Name	Source User Name	Destination User Name
2 Sep 2012 15:29:30 PDT	IDOL - Potential loss of Mergers data - Proximity: 57.02	Jameson Jones	peter.chambliss@gma...
2 Sep 2012 15:29:30 PDT	IDOL - Potential loss of Research data - Proximity: 51.15	Jameson Jones	peter.chambliss@gma...
2 Sep 2012 15:29:30 PDT	IDOL - Potential loss of HR data - Proximity: 60.08	Jameson Jones	peter.chambliss@gma...

Sample Usecase: Information at Risk



1. Attack target
2. Events sent to ESM
3. Query sent to IDOL
4. Context sent to ESM
5. See next slide

Sample Usecase: Data under Attack (cont’)

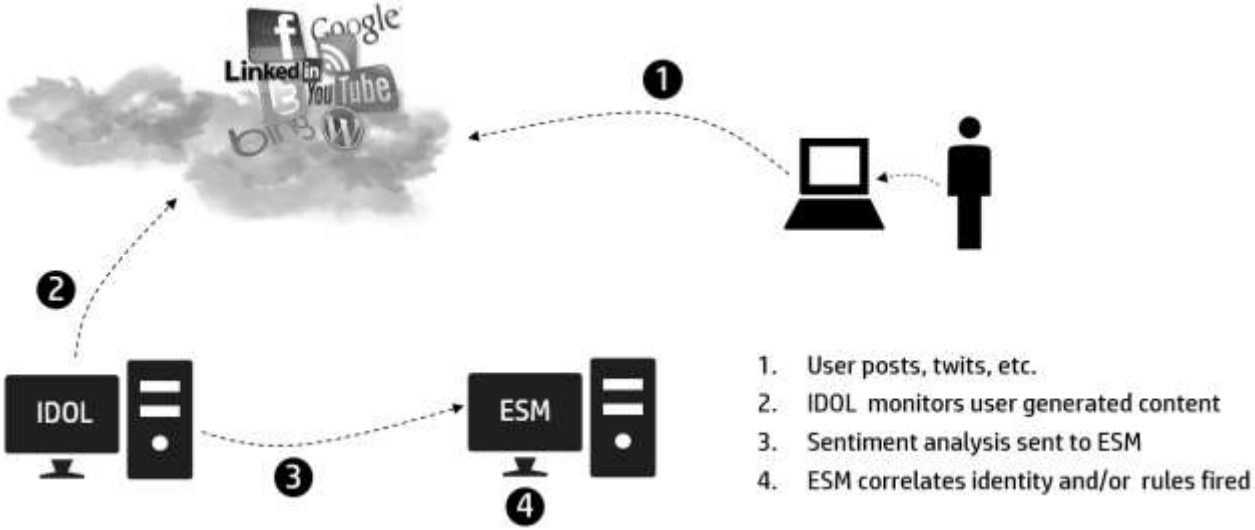


Sample Usecase: Threat Monitoring through Sentiment Analysis

- Intelligence has a long history of providing pivotal information to decision-makers

- Monitoring the spiraling amount of user generated content on the internet (social media) and analyze it for sentiment

Sample Usecase: Threat Monitoring through Sentiment Analysis



End Time	Device Product	Name	Sentiment	Social Media Website
14 Feb 2013 07:47:41 PST	ArcSight	Social Media - Hacktivist (DDOS) Threat	Negative	http://twitter.com/hakdplnt/statuses/301054906566066177
14 Feb 2013 07:47:41 PST	ArcSight	Social Media - Insider Threat	Negative	http://www.glassdoor.com/Reviews/Employee-Review-
14 Feb 2013 07:47:41 PST	ArcSight	Social Media - Hacktivist Threat	Negative	http://twitter.com/hakdplnt/statuses/301085122676002816
14 Feb 2013 07:47:41 PST	ArcSight	Social Media - Hacktivist Threat	Negative	http://twitter.com/hakdplnt/statuses/301061389127122945
14 Feb 2013 07:47:41 PST	ArcSight	Social Media - Hacktivist Threat	Negative	http://twitter.com/hakdplnt/statuses/301054906566066177
14 Feb 2013 07:47:41 PST	ArcSight	Social Media - Hacktivist Threat	Negative	http://twitter.com/YourAnonNews/statuses/299182747463872512
14 Feb 2013 07:47:41 PST	ArcSight	Social Media - Hacktivist Threat	Negative	http://twitter.com/YourAnonNews/statuses/299159456149815296

hp.com/haven