



**Hewlett Packard
Enterprise**

ArcSight Advanced Security Analytics

**Petr Hněvkovský, CISSP, CISA, CISM
Senior Solution Architect, EMEA**

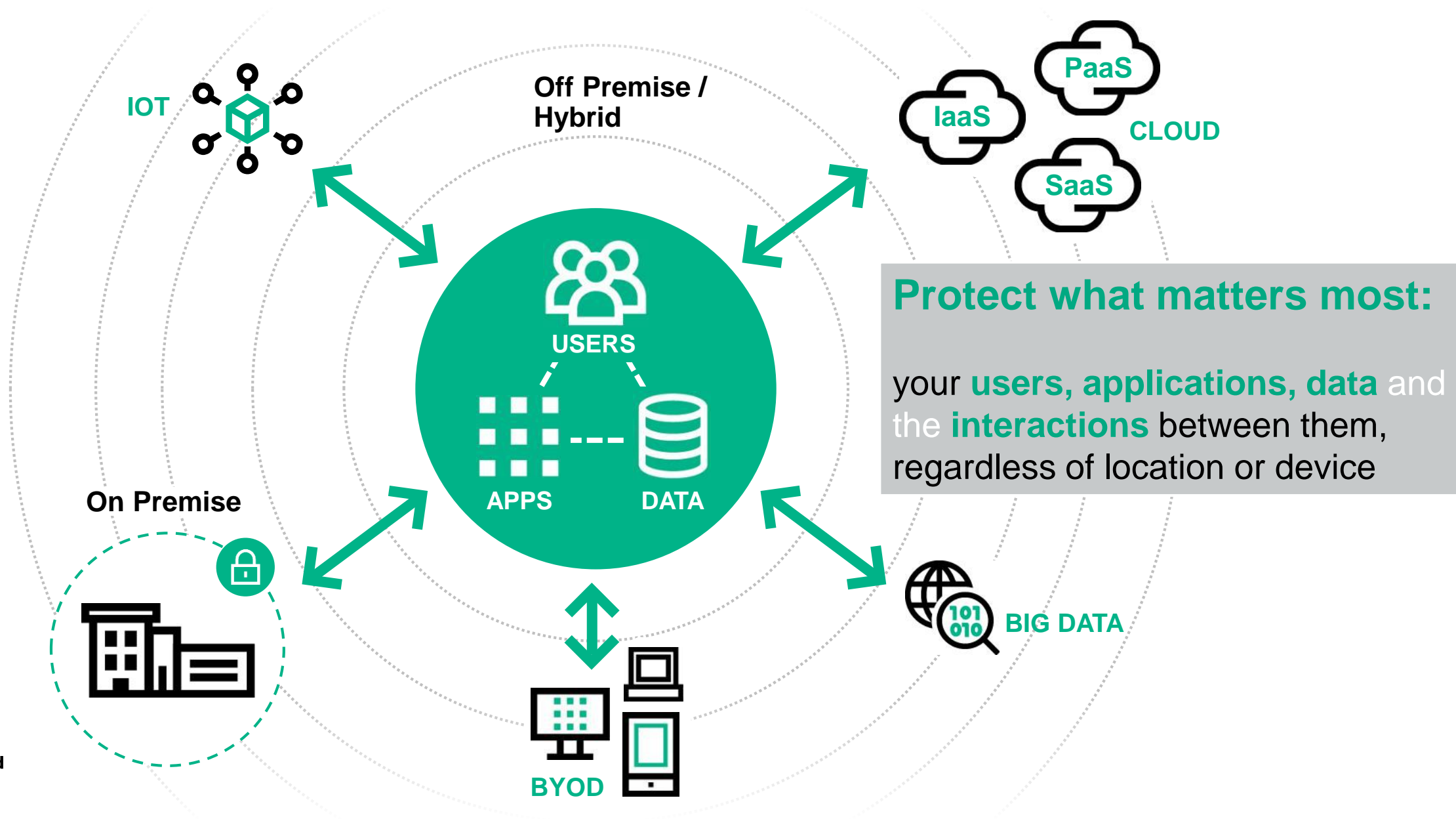
June 2016



Agenda

- Introduction
- SAP UI Analytics
- User Behaviour Analytics
- DNS Malware Analytics
- Q&A

Today's digital Enterprise needs a new style of protection





SAP UI Logging

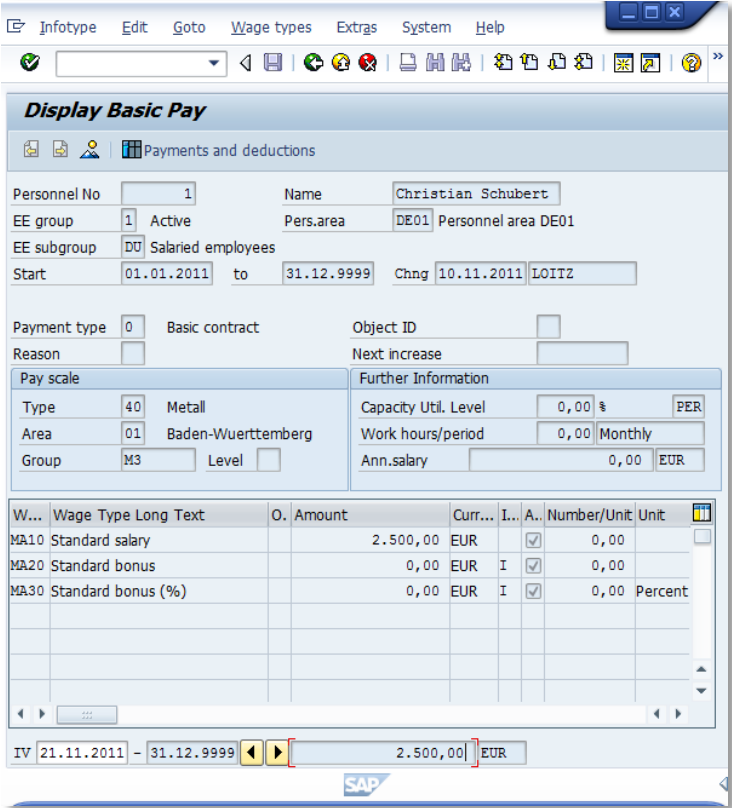
Existing SAP audit features

- SAP System logs (SM21)
 - All system errors
 - Alerts
 - Unsuccessful authentication attempts
 - Process messages in system log
- HR Log data (RPUAUD00)
 - Unauthorized access attempts
 - Who, what, when has modified infotype data
- Security Audit Log (SM 18-19-20)
 - Unsuccessful authentication attempts
 - Successful / failed RFC-requests
 - RFC-request calling modules functions
 - User accounts changes
 - Successful / failed transaction initiations
 - Changes to audit level
- Logging Changes to Table Data (SE13)
 - Table changes log

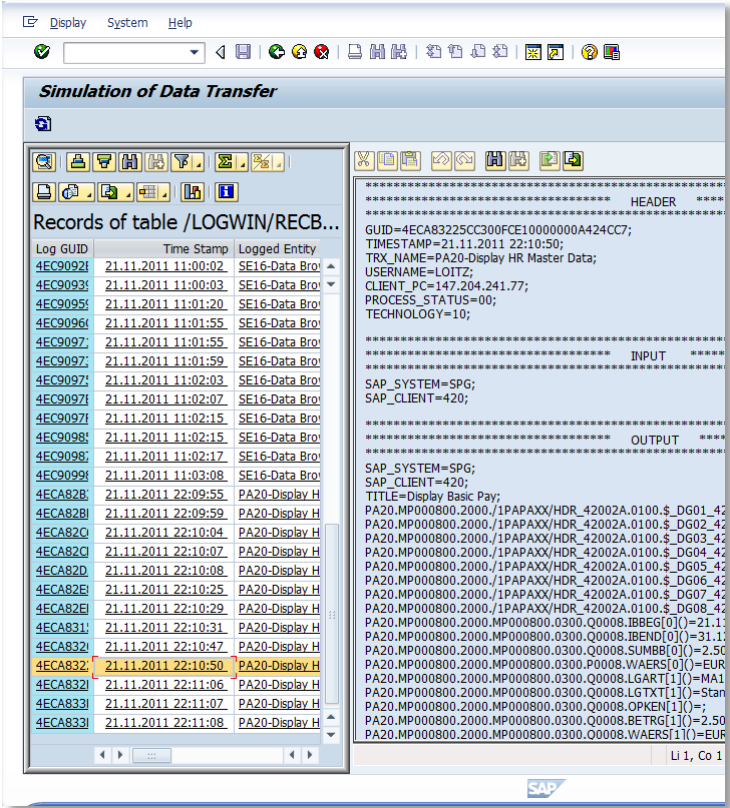
Good for system errors and the fact of a change..

but will **not** provide insights on data views or data changes inside SAP transaction!

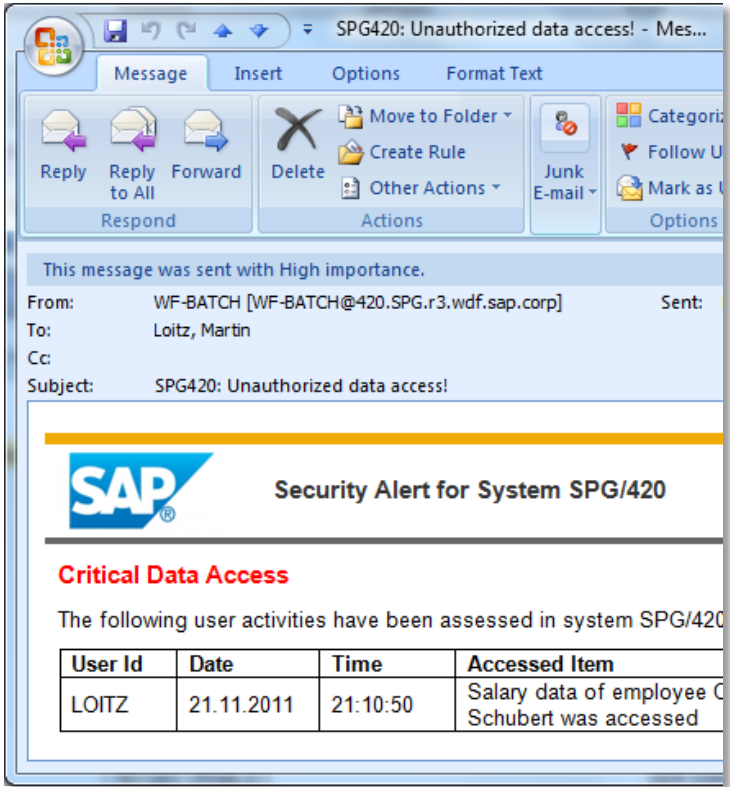
UI Logging workflow



Просмотр пользователем



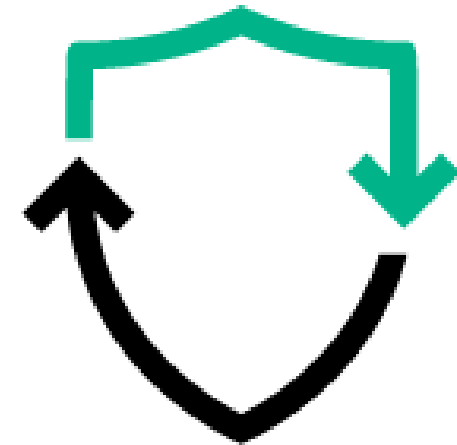
Запись в лог



Уведомления

Use cases

- SAP HR. PII
 - Transaction PA20, infotype 0002
- SAP HR. Payroll
 - Transaction PA20, infotype 290 subtype 21
- SAP HR. Payments report
 - Transaction RPLPAY00
- SAP CRM
 - Clients
 - Contracts



PII usecase: user activity

Display Personal Data

Find by

- Person
 - Collective search help
 - Search Term
 - Free search

Personnel No

EE group Active Pers.area Personnel area DE01

EE subgroup Salaried employees

Start To Chng LOITZ

Name

Title Last name Title

First name Initials

Name prefix Other title

Formatting Spec.format

Birth data

NameAtBirth

Name Prefix Other title

Birthdate Birthplace

Language Ctry o.birth

Nationality Other nat.

Marital status/religion

Mar.Status Since Religion

No. child.

PII usecase: audit trail

BASIC (4)					
ie	Client IP in Log	Host Name	Proc. Sts	Platform	Sub Tech
D	147.204.248.246	MOWN60259514A		10	
D	147.204.248.246	MOWN60259514A		10	
D	147.204.248.246	MOWN60259514A		10	
D	147.204.248.246	MOWN60259514A		10	

Records of Table /LOGWIN/REC_INF (7)					
Transaction code	Client-Side TCode	Current Function Code	Entry Type	PBO Fla	
PA20	PA20		20	X	
PA20	PA20		20	X	

Attribute/Value pairs (29)			
Index	Parent Index	Name	Name Value
0	0	P0002-BEG...	22.07.1980
0	0	P0002-END...	31.12.9999
0	0	P0002-AED...	13.11.2013
0	0	P0002-UN...	LOITZ
0	0	RP50M-SPR...	
0	0	Q0002-AN...	Mr
0	0	P0002-NAC...	Schubert
0	0	P0002-TIT...	Christian
0	0	P0002-VO...	
0	0	P0002-INITS	
0	0	P0002-VO...	
0	0	P0002-NA...	
0	0	P0001-ENA...	Christian Sc...
0	0	P0002-KNZ...	00
0	0	P0002-NA...	
0	0	P0002-VO...	
0	0	P0002-NA...	
0	0	Q0002-GB...	22.07.1980
0	0	Q0002-GB...	
0	0	P0002-GB...	
0	0	P0002-SPR...	EN
0	0	P0002-GBL...	

Running reports: user activity

Payments and Deductions									
M									
Key date: 17.06.2014									
PerNo	Name	Activity		PT	PA	PS	Group	PL	
Infotyp		Subtyp					Ob	Start Date	End Date
Reas.									
W. type		Amount	Curr	D	Number	Unit		%difference	
00000001	Christian Schubert					40 01 M3			
0008	Basic Pay	0			Basic contract			17.06.2014-17.06.2014	
MA10	Standard salary	1.600,00	EUR		0,00			0,00	
MA20	Standard bonus	153,39	EUR		0,00			0,00	
MA30	Standard bonus (%)	0,00	EUR		0,00			0,00	
****	Total	1.753,39	EUR		0,00			0,00	

Running reports: audit trail

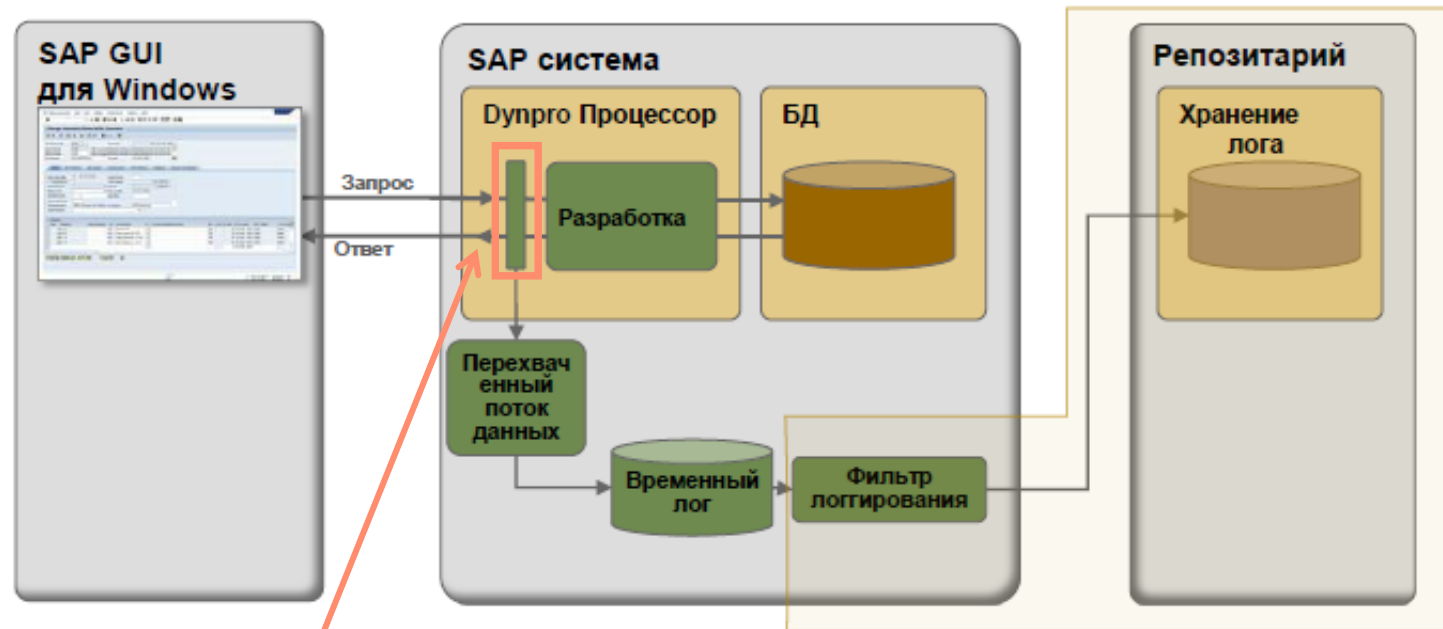
e	Client IP in Log	Host Name	Proc. S...	Platform	Sut
>	10.67.192.123	dewdfm0328		10	
>	10.67.192.123	dewdfm0328		10	
>	10.67.192.123	dewdfm0328		10	
>	10.67.192.123	dewdfm0328		10	
>	10.67.192.123	dewdfm0328		10	
>	10.67.192.123	dewdfm0328		10	
>	10.67.192.123	dewdfm0328		10	
>	10.67.192.123	dewdfm0328		10	
>	10.67.192.123	dewdfm0328		10	
>	10.67.192.123	dewdfm0328		10	
>	10.67.192.123	dewdfm0328		10	

Transaction code	Client-Side TCode	Current Function Code	Entry Type	PBO Flag	Screen Title	Ctrl Ty...	Element name
SE38	SE38		30	X	Payments ...		

Attribute/Value pairs (17)

Index	Parent Index	Name	Name Value
1	0	REPORT_LI...	Key date: 02.07.2014
2	0	REPORT_LI...	
3	0	REPORT_LI...	
4	0	REPORT_LI...	PerNo Name Activity PT PA PS Group PL
5	0	REPORT_LI...	Infotyp Subtyp Ob Start Date End Date
6	0	REPORT_LI...	Reas.
7	0	REPORT_LI...	W. type Amount Curr D Number Unit %difference
8	0	REPORT_LI...	
9	0	REPORT_LI...	00000001 Christian Schubert 40 01 M3
10	0	REPORT_LI...	
11	0	REPORT_LI...	0008 Basic Pay 0 Basic contract 02.07.2014-02.07.20
12	0	REPORT_LI...	
13	0	REPORT_LI...	MA10 Standard salary 1.600,00 EUR 0,00 0,00
14	0	REPORT_LI...	MA20 Standard bonus 153,39 EUR 0,00 0,00
15	0	REPORT_LI...	MA30 Standard bonus (%) 0,00 EUR 0,00 0,00
16	0	REPORT_LI...	***** Total 1.753,39 EUR 0,00 0,00
17	0	REPORT_LI...	

SAP GUI-client logging



SAP UI Logging

Server oriented architecture

UI Logging – is NetWeaver add-on, which is able to see inside data exchange between SAP server and SAP GUI-client

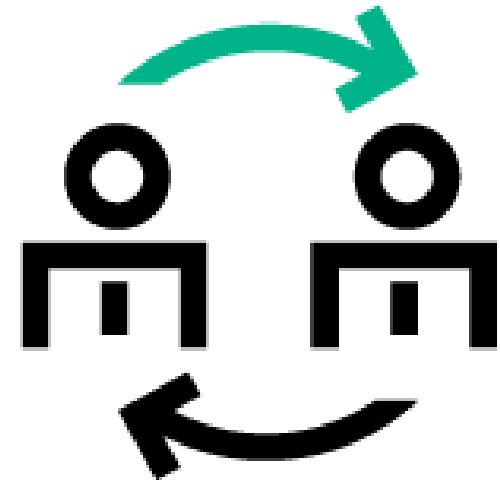
Plus for segregation of roles we put logs into secure archive



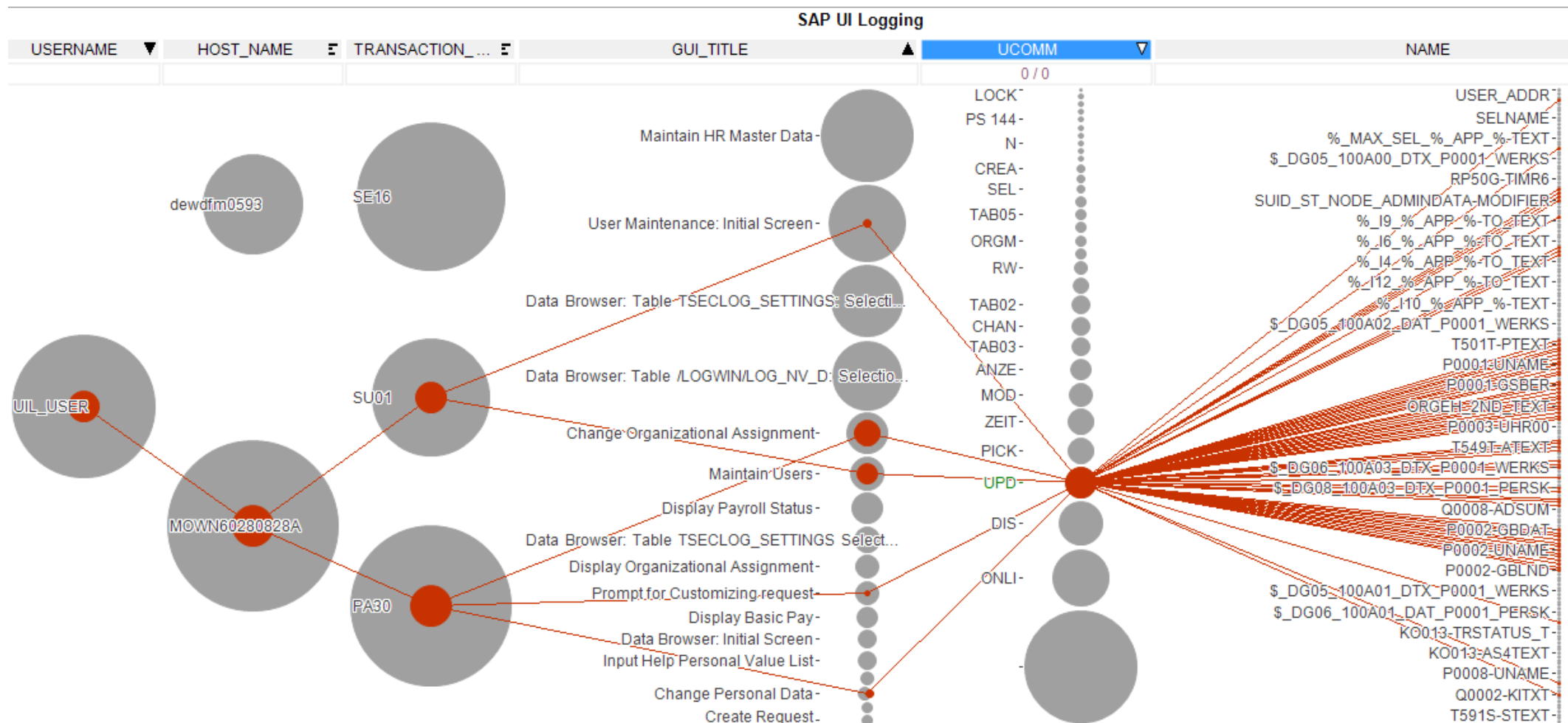
ArcSight Analytics

User activity monitoring with ArcSight

- Needle in a haystack
 - who has been changing this infotype in last 3 months?
 - what infotypes this person has changed in last 2 weeks?
- Correlation
 - customer billing info changed and reverted back during a week
 - customer discount changed more than by 10%
 - during a set window of time user has approved too much bills (#/\$\$) than usual



HPE ArcSight: user UPDate activity visualization



Log analysis by HPE ArcSight

The screenshot displays the HPE ArcSight Command Center interface. The top navigation bar includes links for Dashboards, Events, Reports, Cases, Applications, and Administration. Below this, a search bar is highlighted with a red box, containing the query: `(Change Personal Data OR Change Organizational Assignment) AND ER1`. The search results are displayed in a table with columns: **endTime**, **name**, **sourceAddress**, **destinationAddress**, and **priority**. The table shows six events, all with a priority of 2. The first two events are expanded, showing their raw log data. The raw data for the first event includes fields such as **eventId**, **end**, **mrt**, **art**, **cnt**, **type**, **priority**, **src**, **sourceZone**, **msg**, **Organizational Assignment**, **cs5**, **cs6**, **fname**, **fileId**, **fileHash**, **oldfileName**, **oldfilePath**, **oldfileHash**, **originator**, **duser**, **duid**, **dproc**, **sourceServiceName**, **sprv**, **flexString1**, **flexString1Label**, **TRX_NAME**, **aid**, **3xq**, **ScE8BBDfetPqUIP6Xw**, **at**, **flexmulti_db**, **av**, **7.0.6.7189.0**, **atz**, **Europe/Moscow**, **agentAssetId**, **4Qc8AZU8BABCJs9GBvnlQWQ**, **deviceExternalId**, **ER1**, **deviceFacility**, **17**, **dtz**, **Europe/Moscow**, **lblString1Label**, **NAME**, **lblString2Label**, **VALUE**, **lblString4Label**, **GUI_TITLE**, **lblString5Label**, **oat**, **flexmulti_db**, **oav**, **7.0.6.7189.0**, **oatz**, **Europe/Moscow**, **oahost**, **AFONIN1**, **oagt**, **192.168.1.38**, **oagentZone**, **100000056**, **oagentAssetId**, **4Qc8AZU8BABCJs9GBvnlQWQ**, **fdeviceExternalId**, **ER1**, **fd**, **fdtz**, **Europe/Moscow**.

	endTime	name	sourceAddress	destinationAddress	priority
1	2015/08/27 12:40:52 PDT	SAP UI	10.27.192.203		2
2	2015/08/27 12:40:51 PDT	SAP UI	10.27.192.203		2
3	2015/08/27 12:40:51 PDT	SAP UI	10.27.192.203		2
4	2015/08/27 12:40:51 PDT	SAP UI	10.27.192.203		2
5	2015/08/27 12:40:51 PDT	SAP UI	10.27.192.203		2
6	2015/08/27 12:40:50 PDT	SAP UI	10.27.192.203		2

HPE ArcSight: user

Активный канал: Исследовать[!xGhcE8BACbZPVUh6wBhg==]

Время начала: 27 авг 2015 21:28:00 MSK
Время окончания: 27 авг 2015 22:28:00 MSK
Фильтр: (ИД агента = "replay" And Пользовательские привилегии цели NOT Is "NULL")
Встроенный фильтр: Фильтр отсутствует
Проверенные правила: Нет правила

Всего событий: 753
Очень высокий: 0
Высокий: 0
Средний: 0
Низкий: 0
Очень низкий: 753

Радар

Время окончания	Адрес злоумышленника	Имя хоста злоумышленника	Имя пользователя	Пользовательская строка 4 устройства	Строка Flex 1	Пользовательская строка	Пользовательская строка	Пользовательская строка	Внешний ИД
27 авг 2015 22:27:52 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	\$_DG01_100A03_DA...	1000003	/IPAPAXX/HDR_10003A	ER 1
27 авг 2015 22:27:44 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	T528T-PLSTX	Штат Долж1	MP000100	ER 1
27 авг 2015 22:27:45 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	PLANS_2ND_TEXT	Technolog 1 grade	MP000100	ER 1
27 авг 2015 22:27:46 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	P0001-STELL	00000000	MP000100	ER 1
27 авг 2015 22:27:48 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	P0001-ORGEH	50000010	MP000100	ER 1
27 авг 2015 22:27:39 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	T503T-PTEXT	Top Manager	MP000100	ER 1
27 авг 2015 22:27:40 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	PPRHR-PROZT	100,00	MP000100	ER 1
27 авг 2015 22:27:42 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	P0001-SBMOD	ZRU1	MP000100	ER 1
27 авг 2015 22:27:43 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	P0001-PLANS	50000075	MP000100	ER 1
27 авг 2015 22:27:34 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	T501T-PTEXT	Active	MP000100	ER 1
27 авг 2015 22:27:36 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	P0001-ABKRS	01	MP000100	ER 1
27 авг 2015 22:27:37 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	T549T-ATEXT	Monthly	MP000100	ER 1
27 авг 2015 22:27:38 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	P0001-PERSK	UH	MP000100	ER 1
27 авг 2015 22:27:30 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	T001P-BTEXT	texttru11	MP000100	ER 1
27 авг 2015 22:27:31 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	P0001-GSBER	0001	MP000100	ER 1
27 авг 2015 22:27:32 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	HRCA_BAREA-BUS_A...	Business area 0001	MP000100	ER 1
27 авг 2015 22:27:33 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	P0001-PERSG	1	MP000100	ER 1
27 авг 2015 22:27:24 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	P0001-BUKRS	ZRU1	MP000100	ER 1
27 авг 2015 22:27:25 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	HRCA_COMPANY-CO...	ОАО "Демо-компания"	MP000100	ER 1
27 авг 2015 22:27:26 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	P0001-WERKS	ZRU1	MP000100	ER 1
27 авг 2015 22:27:27 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	T500P-NAME1	Регион ZRU1	MP000100	ER 1
27 авг 2015 22:27:28 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	P0001-BTRTL	ZR11	MP000100	ER 1
27 авг 2015 22:27:19 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	\$_DG08_100A03_DT...	Top Manager	/IPAPAXX/HDR_10003A	ER 1
27 авг 2015 22:27:20 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	P0001-BEGDA	01.01.2015	MP000100	ER 1
27 авг 2015 22:27:21 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	P0001-AEDTM	04.08.2015	MP000100	ER 1
27 авг 2015 22:27:22 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	P0001-UNAME	UIL_USER	MP000100	ER 1
27 авг 2015 22:27:13 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	\$_DG03_100A03_DA...	1	/IPAPAXX/HDR_10003A	ER 1
27 авг 2015 22:27:14 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	\$_DG04_100A03_DT...	Active	/IPAPAXX/HDR_10003A	ER 1
27 авг 2015 22:27:15 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	\$_DG05_100A03_DA...	ZRU1	/IPAPAXX/HDR_10003A	ER 1
27 авг 2015 22:27:16 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	\$_DG06_100A03_DT...	Регион ZRU1	/IPAPAXX/HDR_10003A	ER 1
27 авг 2015 22:27:18 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	\$_DG07_100A03_DA...	UH	/IPAPAXX/HDR_10003A	ER 1
27 авг 2015 22:27:07 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	T527X-ORGTX	Finance	MP000100	ER 1
27 авг 2015 22:27:08 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	ORGEH_2ND_TEXT	Finance	MP000100	ER 1
27 авг 2015 22:27:09 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	P0001-VDSK1	ZRU1	MP000100	ER 1
27 авг 2015 22:27:10 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	\$_DG01_100A03_DA...	1000003	/IPAPAXX/HDR_10003A	ER 1
27 авг 2015 22:27:12 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	\$_DG02_100A03_DA...	Ковалев Алексей	/IPAPAXX/HDR_10003A	ER 1
27 авг 2015 22:27:01 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	P0001-PLANS	50000075	MP000100	ER 1
27 авг 2015 22:27:00 MSK	10.27.192.203	MOWN60280828A	UIL_USER	Display Organizational Assignment	PA30-Maintain HR Master Data	T528T-PLSTX	Штат Долж1	MP000100	ER 1

Атрибуты

Фильтр

Поля сортировки

Изменить

Сводка

Event условия

event1

ИД агента = /All Connectors/Site Conne

Имя хоста устройства NOT Like %sap

OR

Сообщение NOT StartsWith проверк

Причина NOT Is NULL

Пользовательские привилегии и

NOT

URI зоны агента NOT Is NULL

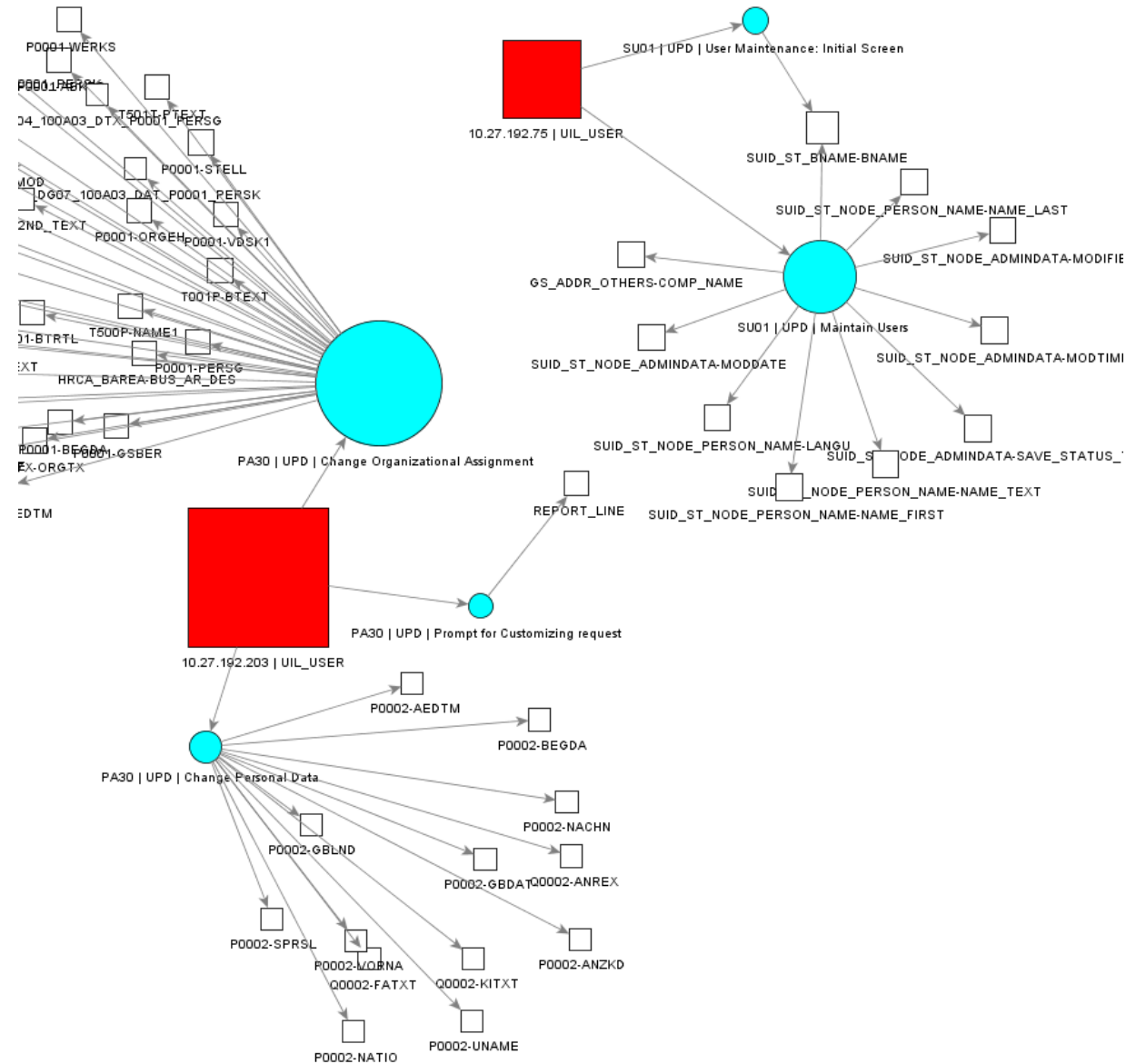
Common Conditior

+/- Глобальная переменная

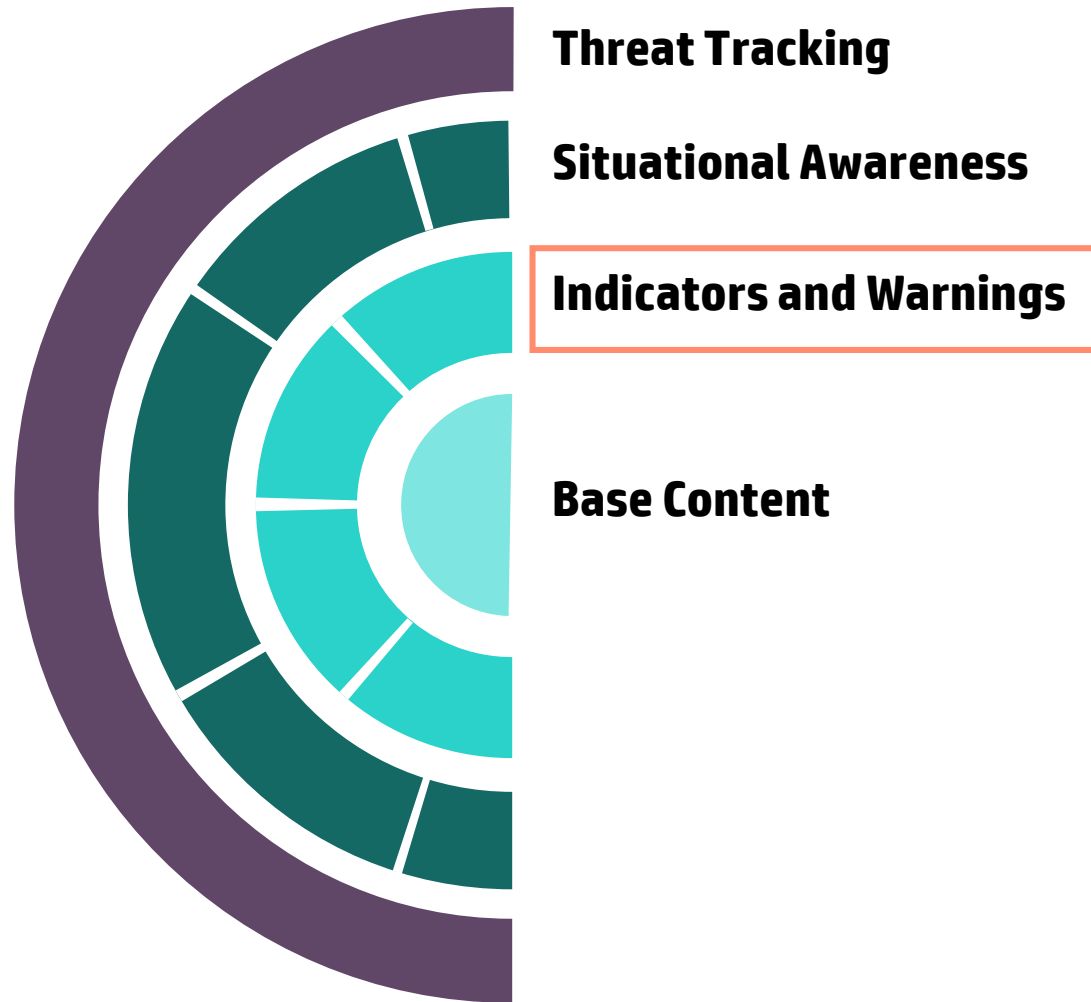
Он.

Условие

User activity visualization HPE ArcSight



ArcSight Activate Framework



Indicators & 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

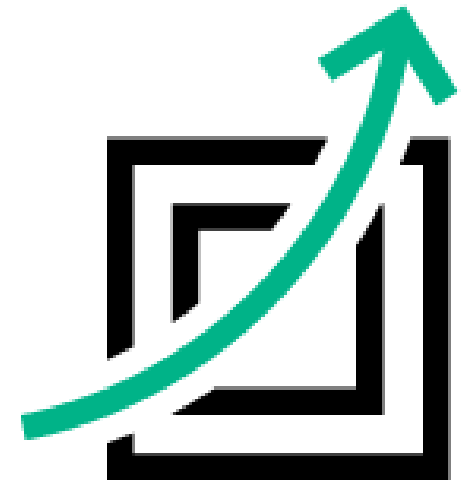
Threat Tracking

Continue to build on contextual information

- Business impact
- Threat Impact
- Next expect event

Analytics use cases on steroids

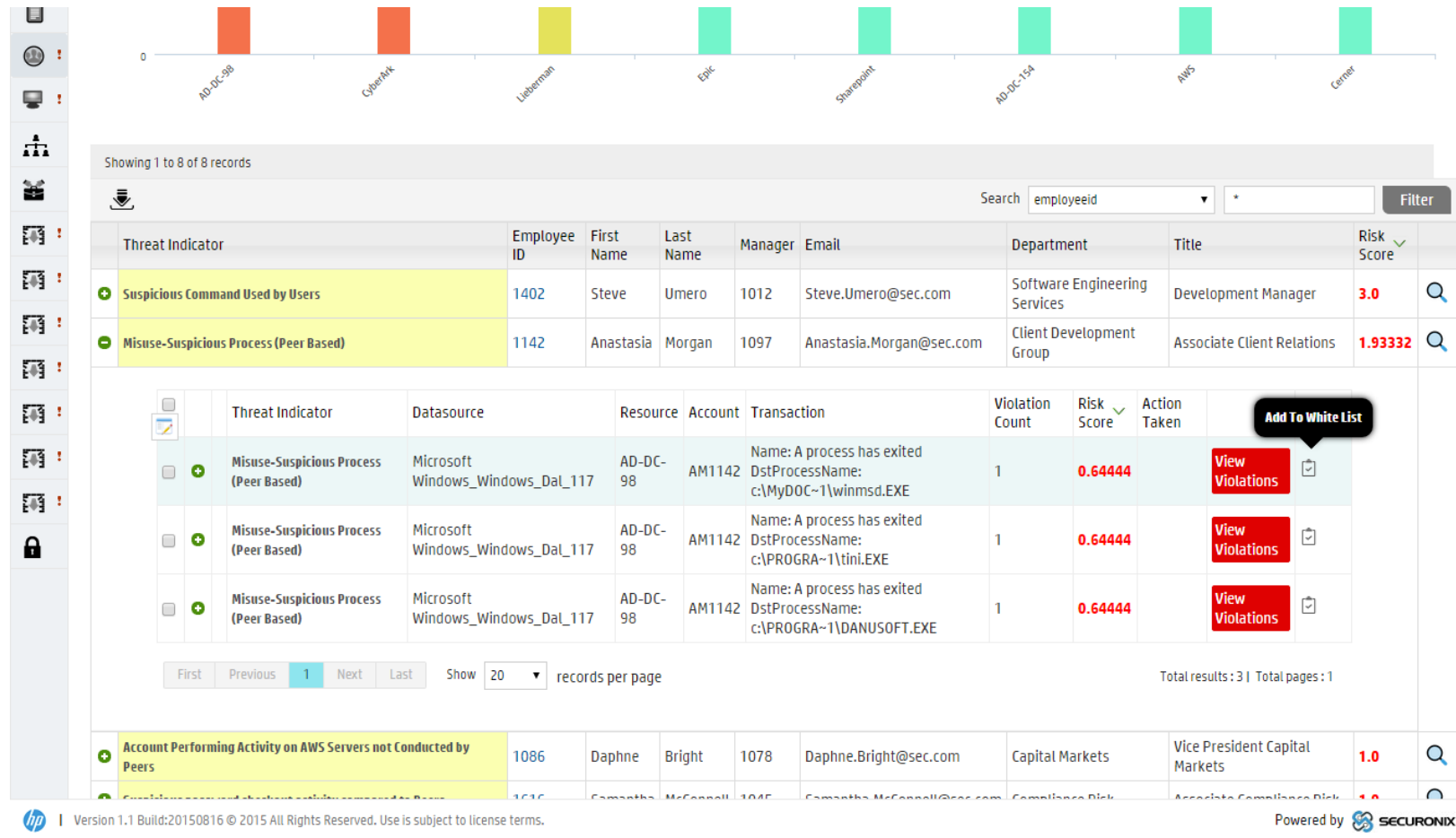
- PII data access
- Salary bonus and compensation fraud
- HR (or other internal or compliance) controls automation
- Customer data access – VIP, medical etc.
- Procurement fraud
- etc.





User Behaviour Analytics

UBA – User centric analytics



Easily view any user details

User Peer Groups

User Risk Scoreboard

Investigation Workbench

Identity Attributes show many details, including Visual Representation

Visual Drill Down

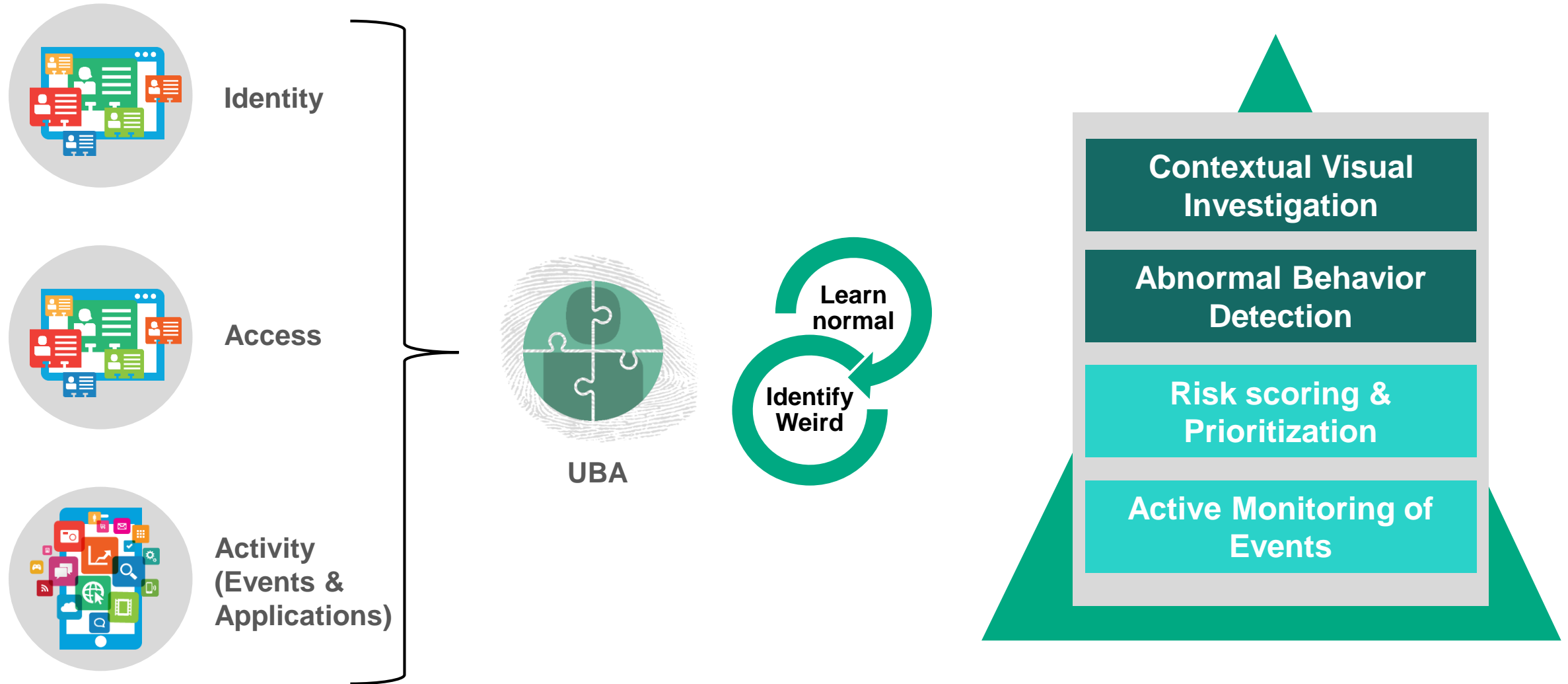
Resources Access History

Policy Violations

Policy Violations Drill Down

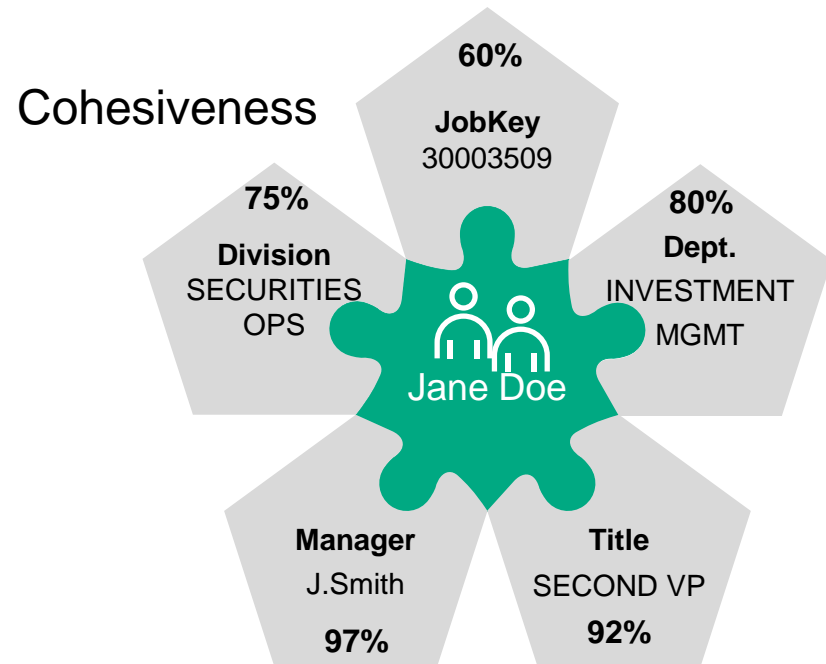
Policy Violations White listing

HPE User Behavior Analytics flow



UBA - detecting “not normal” by comparing to peers

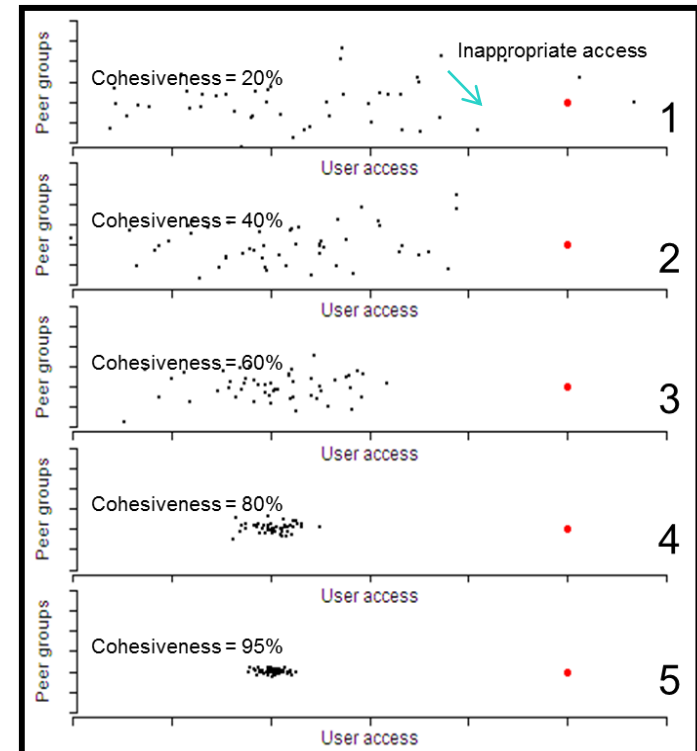
Outlier classification



- Statistical calculation of Peer cohesiveness
- Risk associated with outliers increases with peer cohesiveness

Peer group analysis

- Logically group users based on roles and responsibilities
- Detect anomalous behavior of a user compared to peers



Low risk

High risk



DNS Malware Analytics

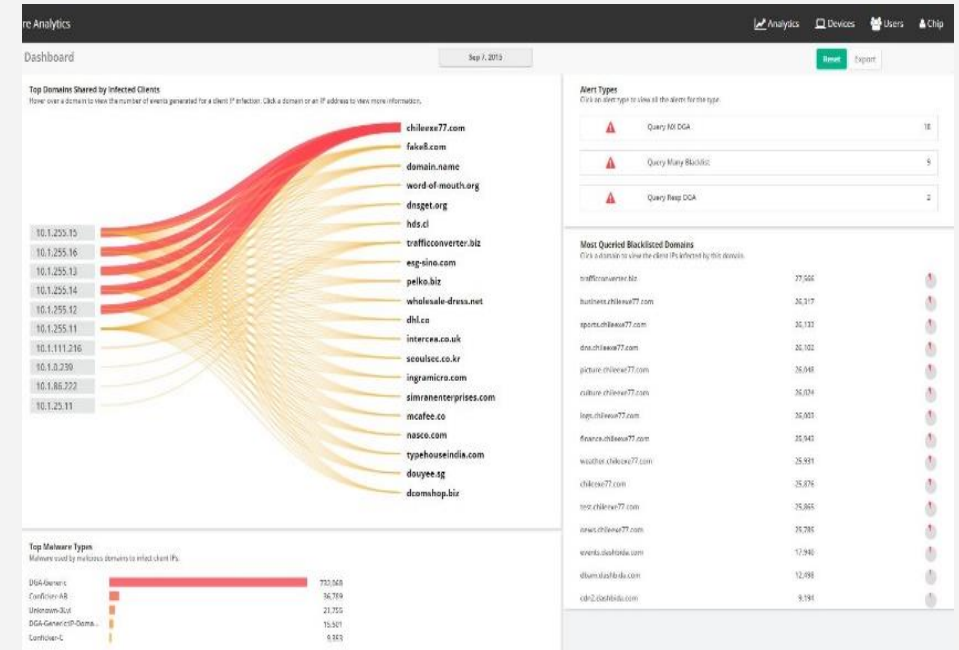
ArcSight DNS Malware Analytics - (DMA 2.6)

DNS Malware Analytics

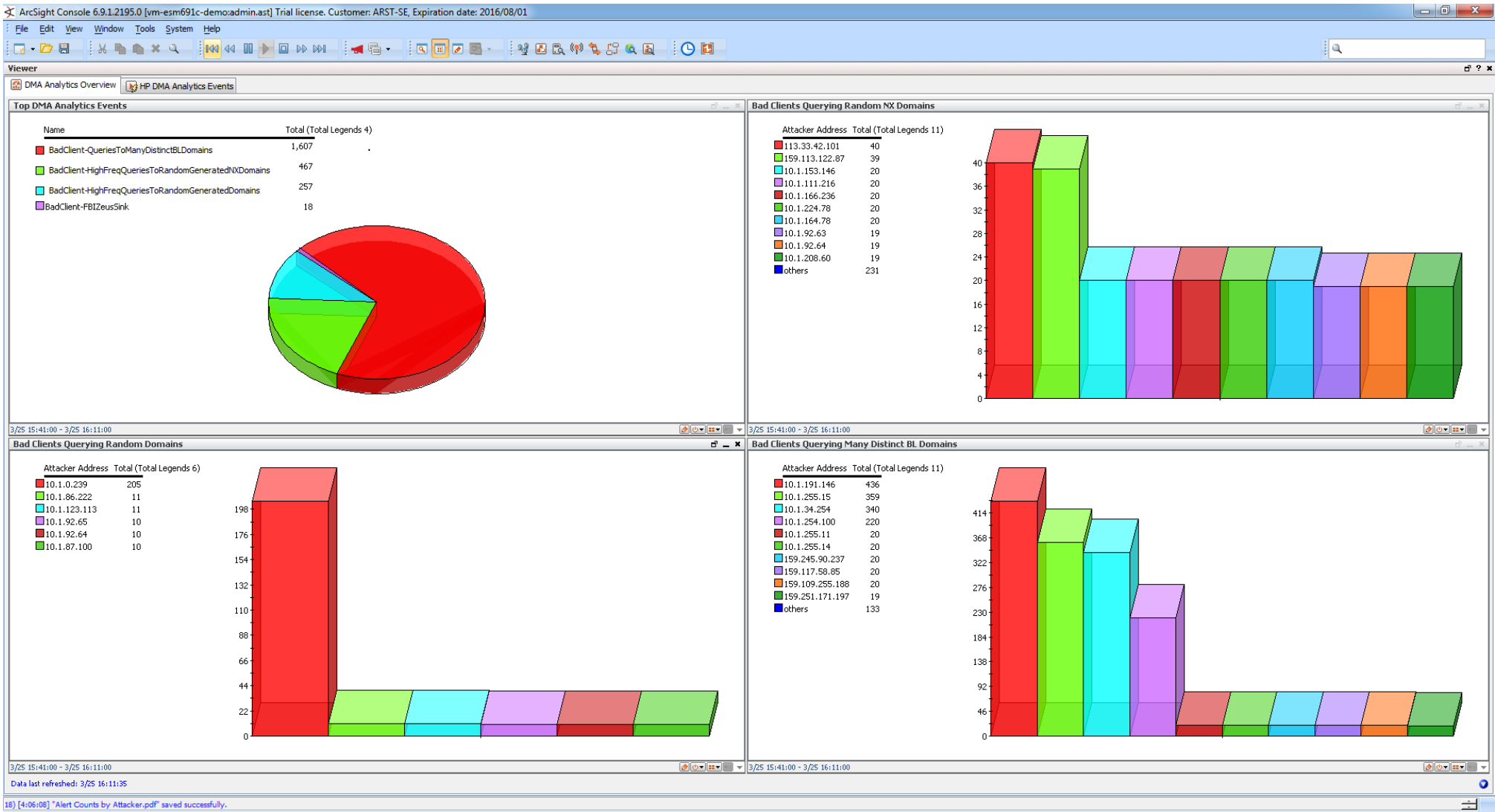
- 20 minutes to start detecting malware
- Near zero false positives
- Real-time analysis detect breaches before damage
- 18B DNS packets/day inspected at HPE center
- 10^9 reduction in data boosts ROI

The
Power of
SIEM and
Analytics

- Automated breach detection that frees analysts up by eliminating investigation and starting remediation
- Detect threats while passing key info to SIEM systems so analysts can take action much faster



ArcSight ESM – DMA Alerts

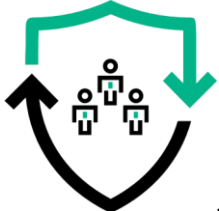


ArcSight Advanced Analytics from business perspective



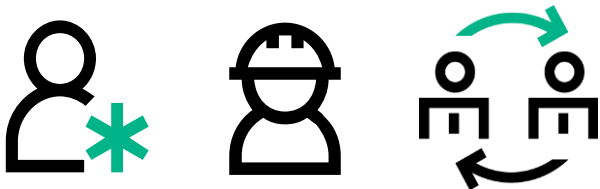
Business

Risk Management | Security | Compliance



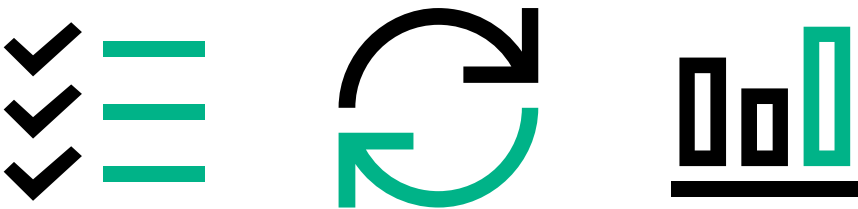
People

Analysts | Hunters | Users| External



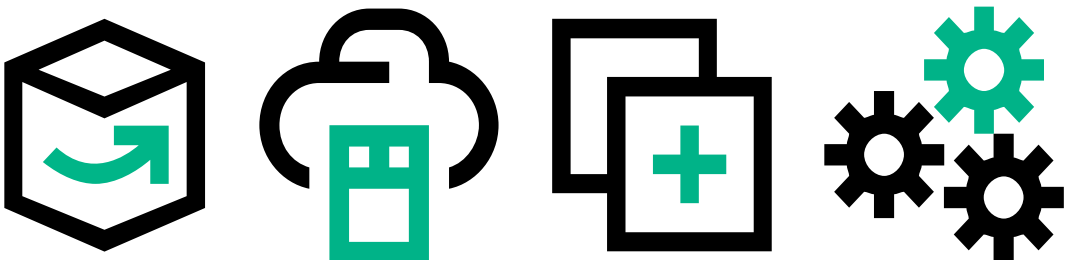
Process

Consistent | Reviewed | Measurable



Technology

Adaptive | Efficient| Resilient | Scalable





Hewlett Packard
Enterprise

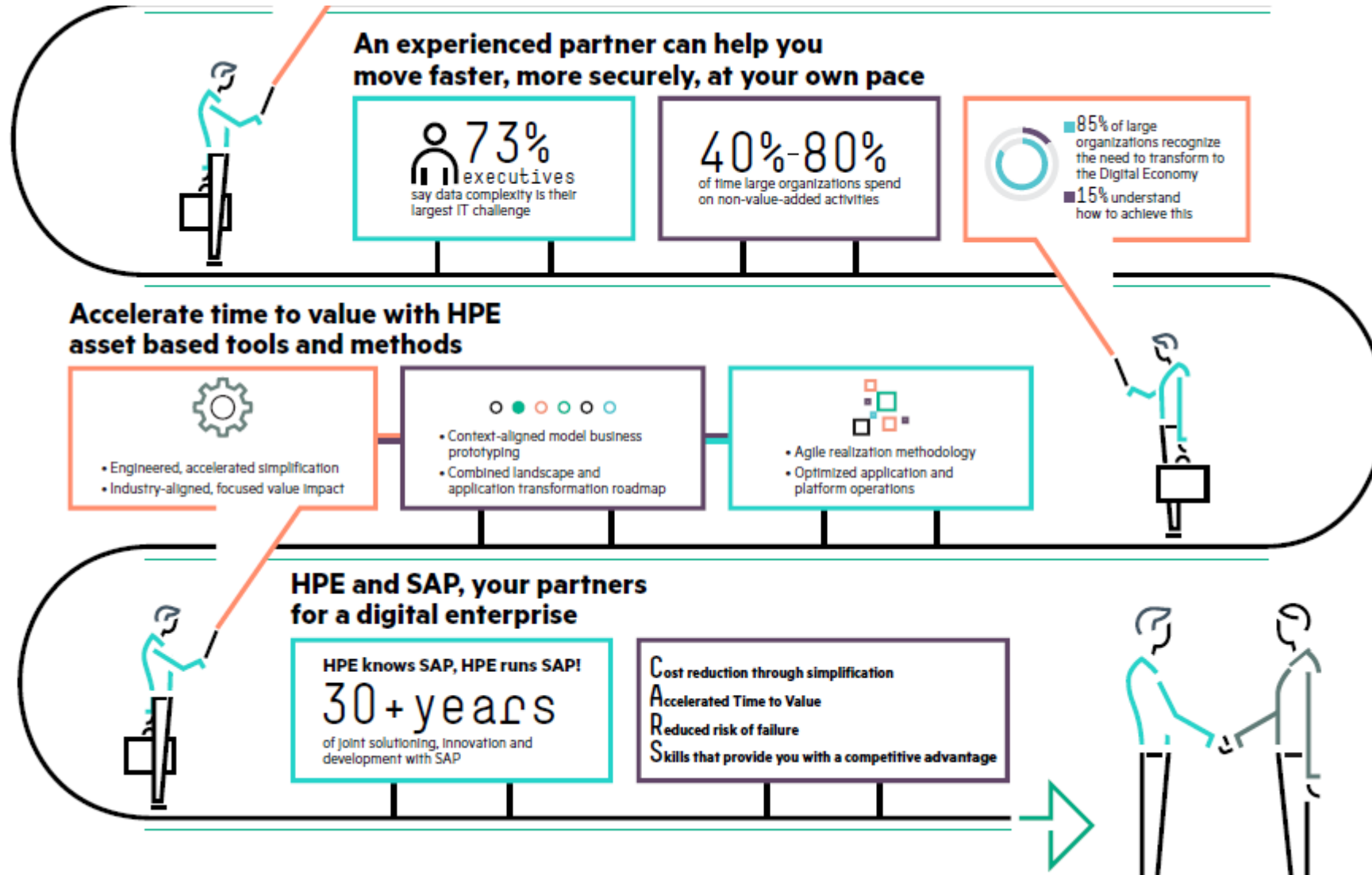
Спасибо

Petr.Hnevkovsky@hpe.com



Backup slides

SAP & HPE partnership



PII usecase: user activity

Display Documents and Certificates (RU)

Find by

- Person
 - Collective search help
 - Search Term
 - Free search

Personnel No Name

EE group Active Pers.area Personnel area DE01

EE subgroup Salaried employees

Start - Chngd LEBEDEVD

Passport of RF Citizen

Series Iss. Date

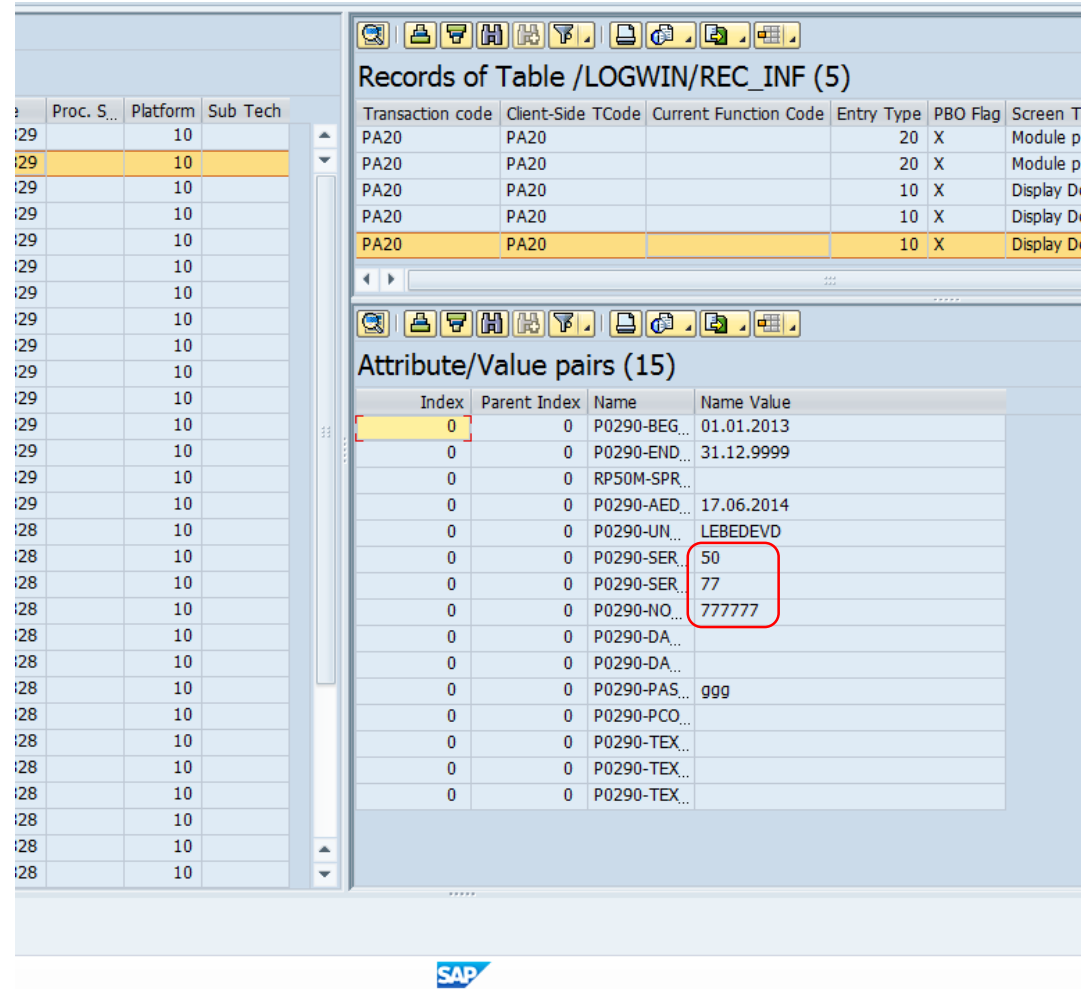
Expiry Date

Issued by

Subunit

Additional info

PII usecase: audit trail



The screenshot shows the SAP audit trail for table /LOGWIN/REC_INF. The left pane displays a list of records with columns Proc. S., Platform, and Sub Tech. The right pane shows the details of the selected record (PA20) with columns Transaction code, Client-Side TCode, Current Function Code, Entry Type, PBO Flag, and Screen Title. Below this, the 'Attribute/Value pairs (15)' table is shown, listing various attributes and their values. The values 50, 77, and 777777 are highlighted with red boxes.

Transaction code	Client-Side TCode	Current Function Code	Entry Type	PBO Flag	Screen Title
PA20	PA20		20	X	Module pr
PA20	PA20		20	X	Module pr
PA20	PA20		10	X	Display Dc
PA20	PA20		10	X	Display Dc
PA20	PA20		10	X	Display Dc

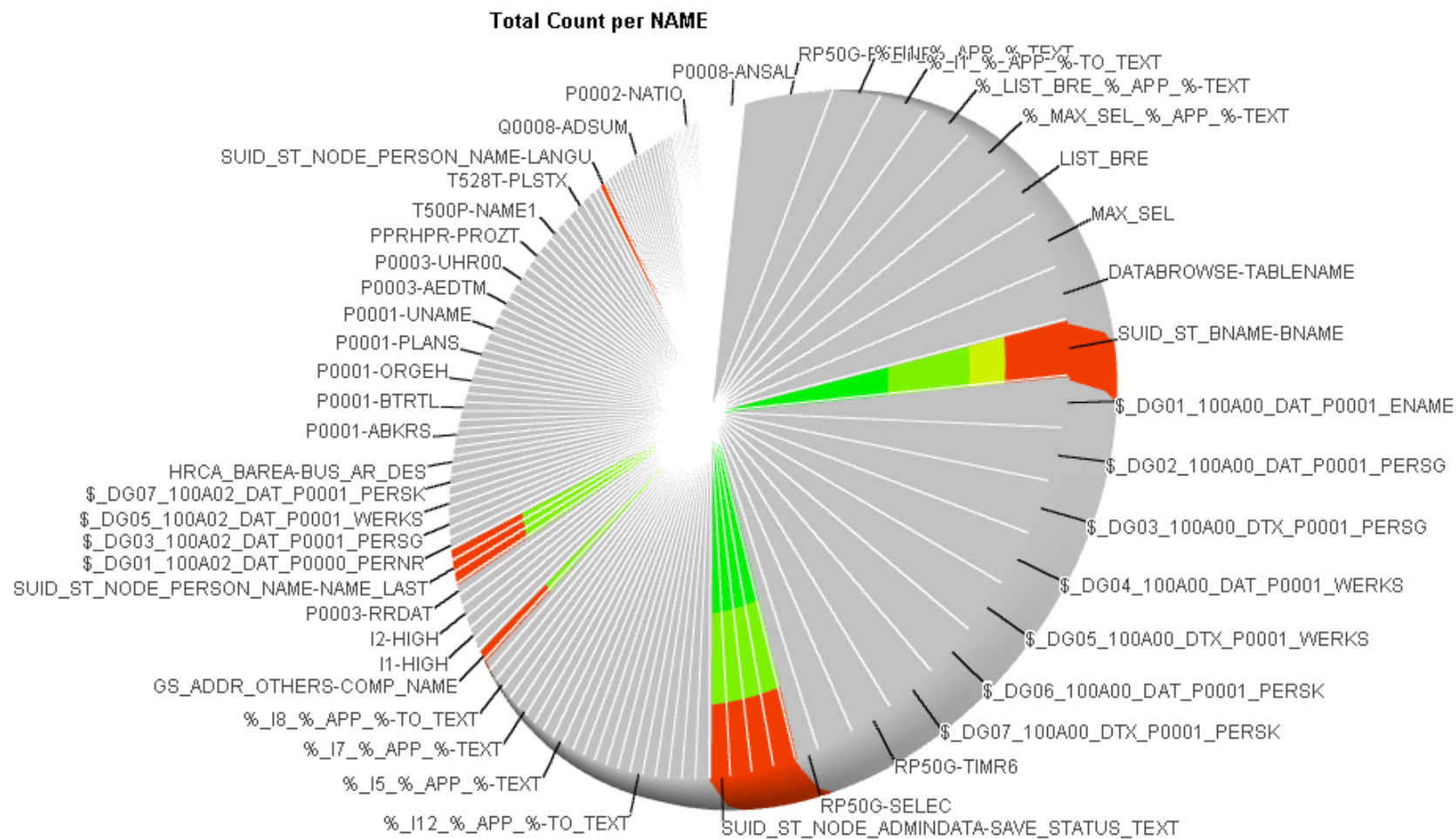
Index	Parent Index	Name	Name Value
0	0	P0290-BEG...	01.01.2013
0	0	P0290-END...	31.12.9999
0	0	RP50M-SPR...	
0	0	P0290-AED...	17.06.2014
0	0	P0290-UN...	LEBEDEV
0	0	P0290-SER...	50
0	0	P0290-SER...	77
0	0	P0290-NO...	777777
0	0	P0290-DA...	
0	0	P0290-DA...	
0	0	P0290-PAS...	ggg
0	0	P0290-PCO...	
0	0	P0290-TEX...	
0	0	P0290-TEX...	
0	0	P0290-TEX...	

Technical details

- Joint offer SAP+HPE
 - Solution could be customized to fully address specific user cases
 - Fully supported by SAP / HPE
 - SAP GUI for Windows available SAP NetWeaver 7.00, 7.01, 7.02, 7.31. 7.40 will be available soon
- Could be extended to:
 - Logging of CRM Web Client UI
 - Logging of Business Warehouse Access (Bex Analyzer, Bex Web, BW-IP, BICS, MDX)
 - Logging of Web Dynpro ABAP
 - Logging of RFC/BAPI & Web Service (на подходе)
- Other UI could be supported on a request basis



User activity visualization HPE ArcSight



Succeed with SIEM – ArcSight Activate Framework

Get the most from your HPE ArcSight implementation



Train & 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

Indicators and Warnings



User Authentication

Successful User Login
Brute Force Attack in Progress



User Management

Account Lockouts
User Added to Administrative Group



Product Specific 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



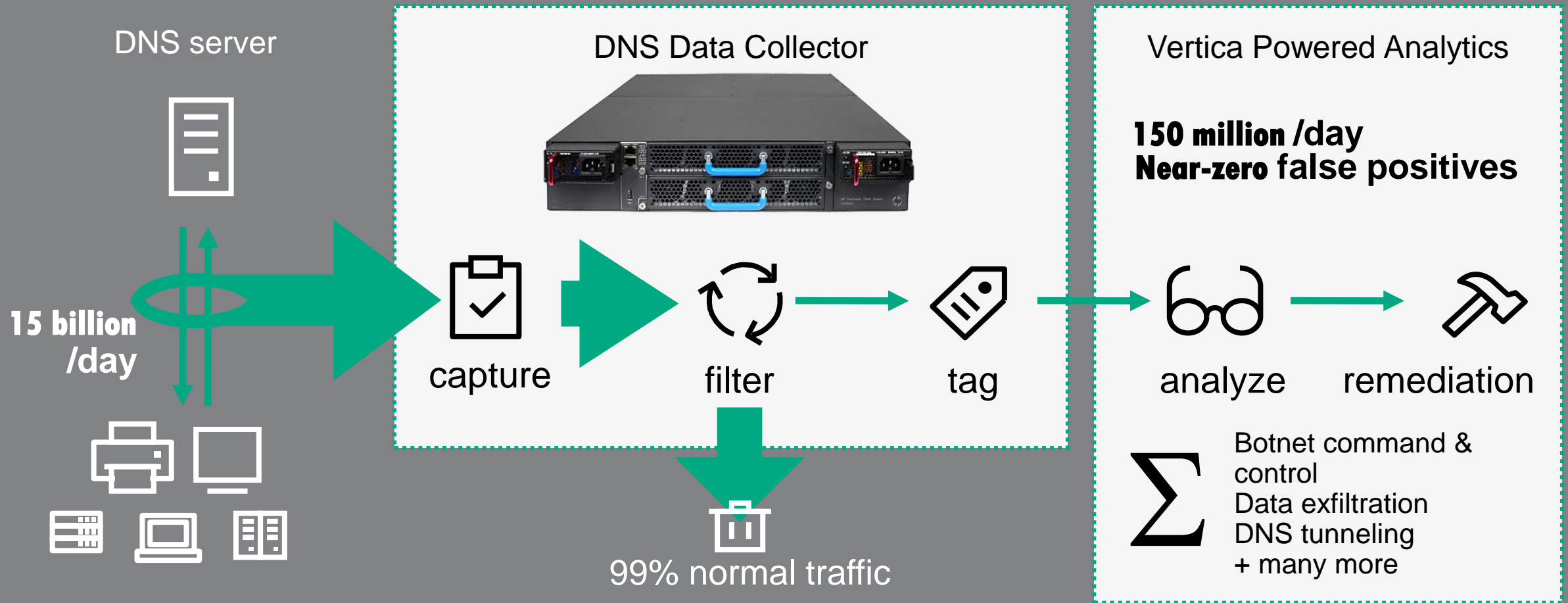
Product Patterns

Baseline System Processes
Baseline Network Flows

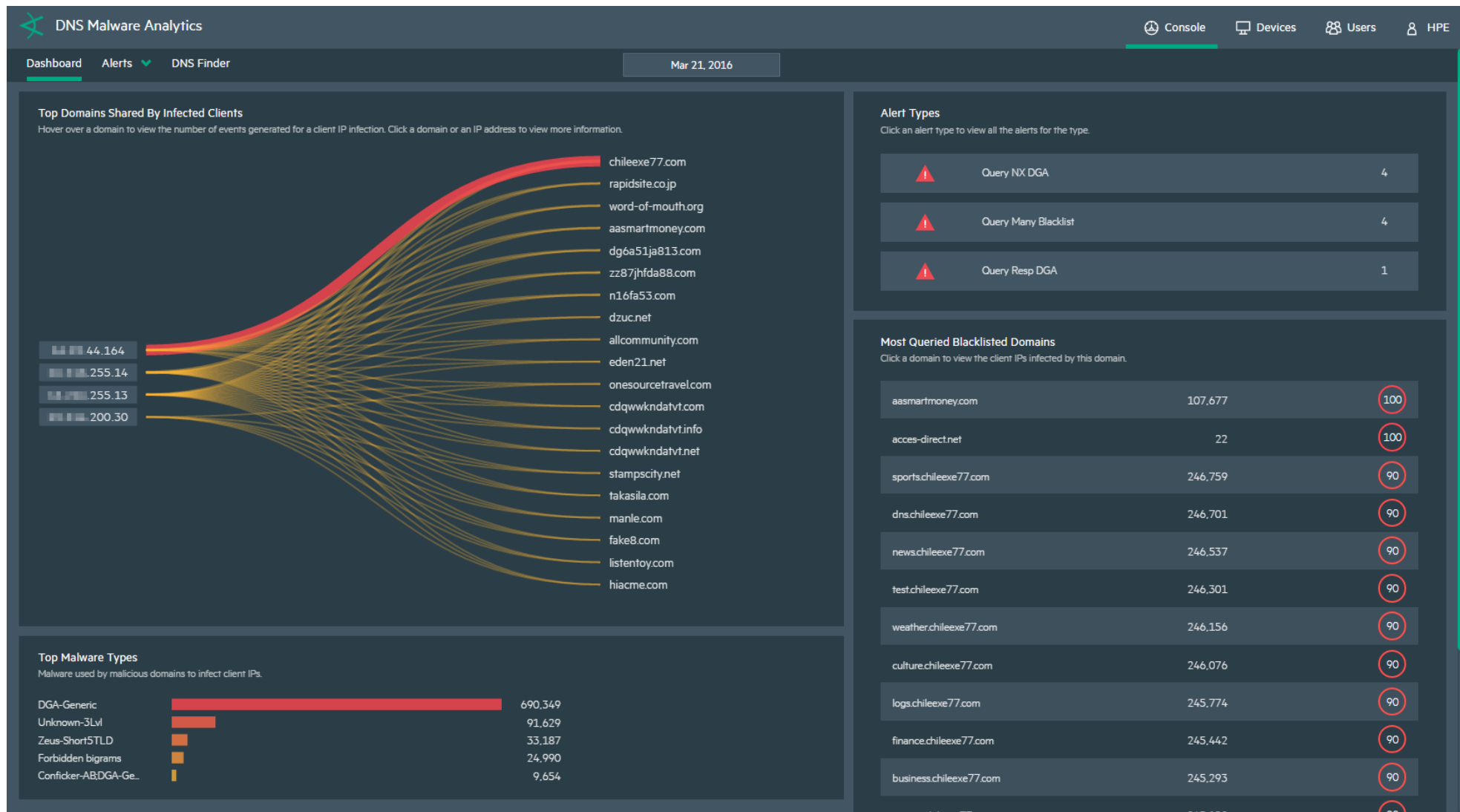
Countermeasures



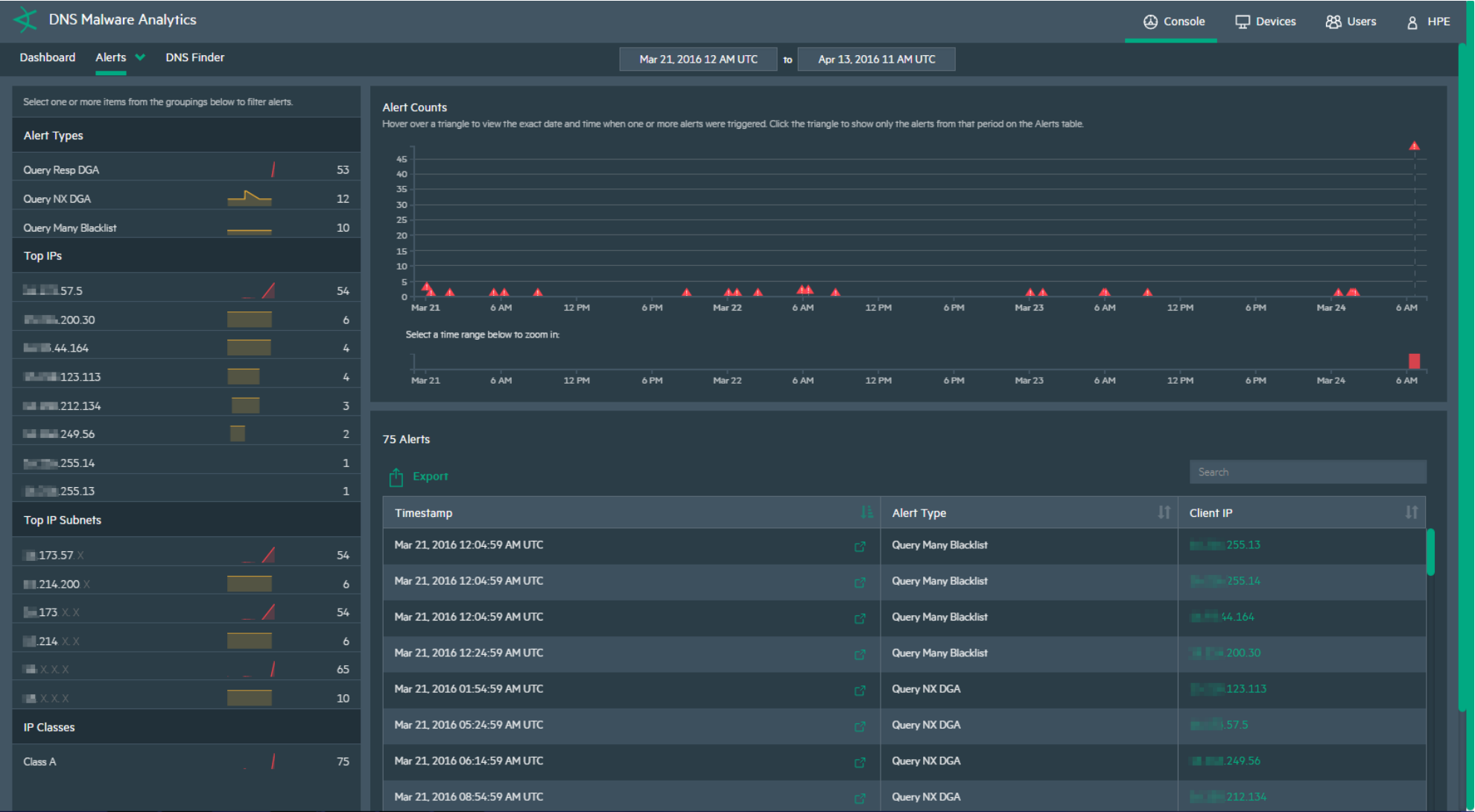
Vertica-powered DMA pushes the boundaries of advanced analytics



DMA - Dashboard



DMA – Alerts View



DNS Malware Analytics

ConsoleDevicesUsersHPE

DashboardAlertsDNS Finder

Alerts > Alert Details for "Mar 24, 2016 01:53:59 AM UTC"

Select one or more items from the groupings below to filter events.

Suspicious Client

Client IP200.30

Type of AlertQuery Resp DGA

Time IssuedMar 24, 2016 01:53:59 AM UTC

Domain Type

Graylist1,571

Blacklist44

Categories of DNS Events

A1,118

NXDOMAIN497

Malware Breakdown

DGA-Generic11481148.0 per hour

Forbidden bigrams8585.0 per hour

Unknown-3Lvl6868.0 per hour

Conficker-AB6868.0 per hour

Zeus-Long6TLD5252.0 per hour

RepSM4444.0 per hour

Conficker-ABDGA-GenericZeus-Short5TLD3232.0 per hour

Virut3030.0 per hour

Events Surrounding the Alert

Click a sparkline to filter the Events table to only include the events from that period.

1,615 Events Triggering the Alert

Search

Timestamp	Domain Requested	Resolution	Category	Malware
Mar 24, 2016 12:26:06 AM UTC	traffic.em.io	54.183.1.218	A	DGA-Generic
Mar 24, 2016 12:26:19 AM UTC	hk3740.xoxv.net	59.188.138.240	A	DGA-Generic
Mar 24, 2016 12:26:34 AM UTC	reveal.dsid.me	54.77.14.98	A	DGA-Generic
Mar 24, 2016 12:26:34 AM UTC	reveal.dsid.me	52.30.172.196	A	DGA-Generic
Mar 24, 2016 12:26:34 AM UTC	reveal.dsid.me	52.18.255.162	A	DGA-Generic
Mar 24, 2016 12:26:45 AM UTC	user.yswm.net	219.146.68.116	A	DGA-Generic
Mar 24, 2016 12:26:45 AM UTC	user.yswm.net	219.146.68.115	A	DGA-Generic
Mar 24, 2016 12:26:45 AM UTC	user.yswm.net	118.180.9.137	A	DGA-Generic
Mar 24, 2016 12:26:45 AM UTC	user.yswm.net	118.180.9.136	A	DGA-Generic