Behind the Analytics
...and the FUD

Matt Hathaway, Director, IDR Solutions

RAPID7

Gain the clarity, command, and confidence to embrace innovation and drive your business forward. Rapid7 transforms your data and uncertainty into answers.

We can help you with...

Vulnerability Management

SIEM

Application Security

IT Operations

User Behavior Analytics

Penetration Testing

Managed Services

Security Advisory Services

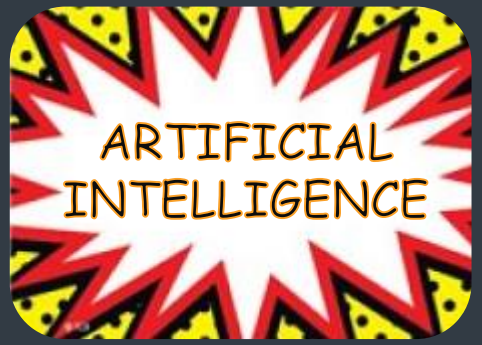
RAPID7

Behind the Analytics
...and the FUD

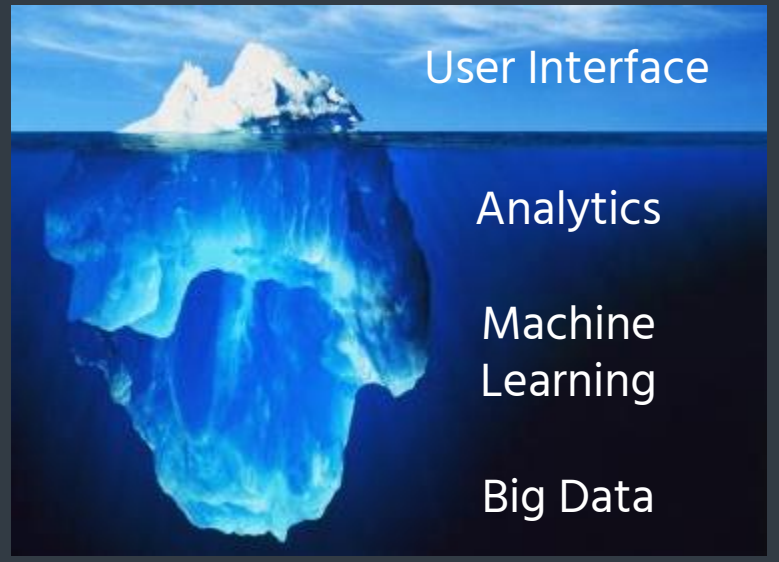
Matt Hathaway, Director, IDR Solutions

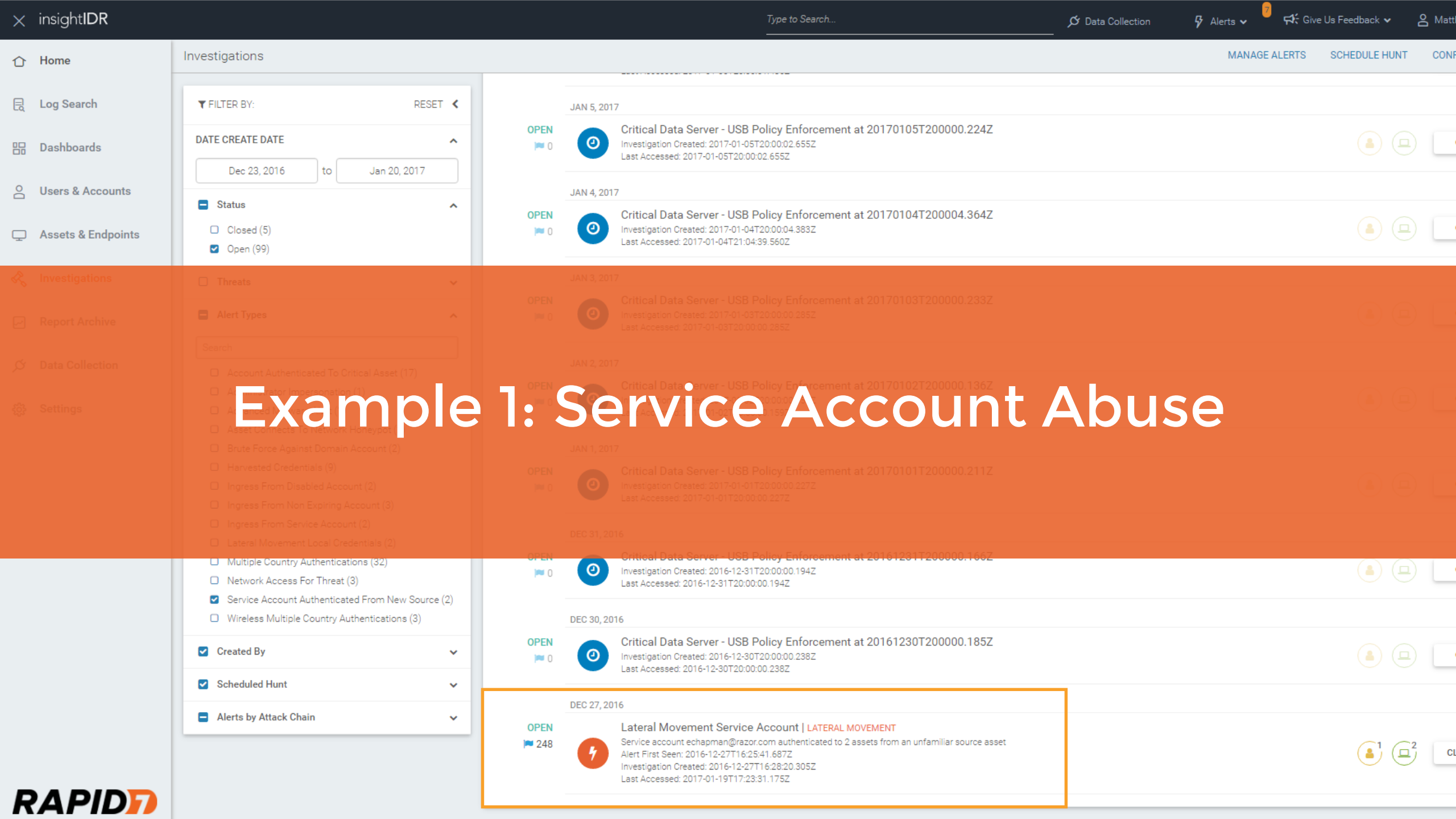
RAPID7

Answering the “So what?”

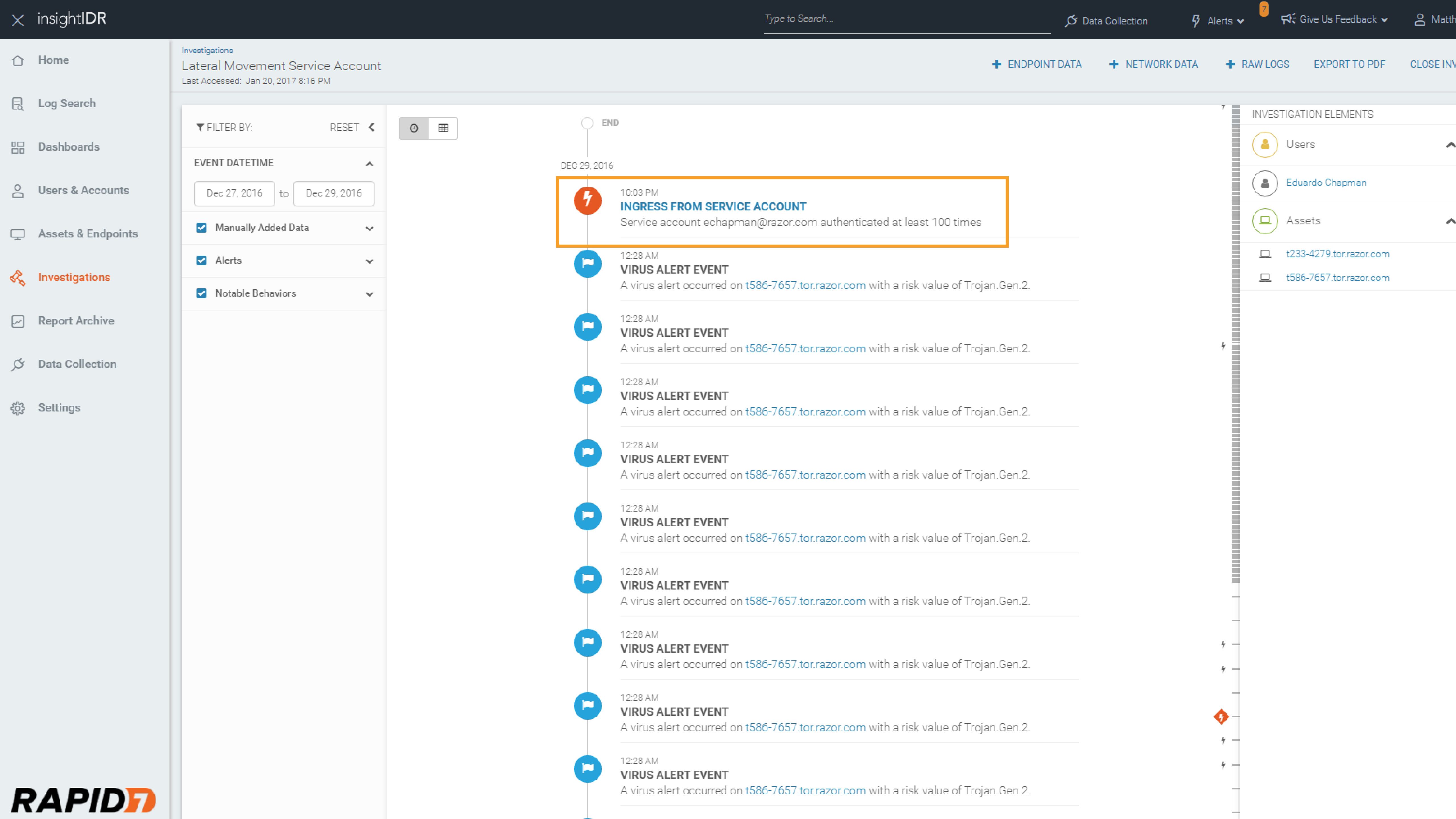


- You’re hearing them.
- How are they **really** being used?





Example 1: Service Account Abuse


insightIDR
Type to Search...
Data Collection
Alerts
7
Give Us Feedback
Matth
Home
Log Search
Dashboards
Users & Accounts
Assets & Endpoints
Investigations
Report Archive
Data Collection
Settings
RAPID7
Investigations
Lateral Movement Service Account
Last Accessed: Jan 20, 2017 8:16 PM
ENDPOINT DATA
NETWORK DATA
RAW LOGS
EXPORT TO PDF
CLOSE INV
FILTER BY:
RESET
EVENT DATETIME
Dec 27, 2016
to
Dec 29, 2016
Manually Added Data
Alerts
Notable Behaviors
END
DEC 29, 2016
10:03 PM
INGRESS FROM SERVICE ACCOUNT
Service account echapman@razor.com authenticated at least 100 times
12:28 AM
VIRUS ALERT EVENT
A virus alert occurred on t586-7657.tor.razor.com with a risk value of Trojan.Gen.2.
12:28 AM
VIRUS ALERT EVENT
A virus alert occurred on t586-7657.tor.razor.com with a risk value of Trojan.Gen.2.
12:28 AM
VIRUS ALERT EVENT
A virus alert occurred on t586-7657.tor.razor.com with a risk value of Trojan.Gen.2.
12:28 AM
VIRUS ALERT EVENT
A virus alert occurred on t586-7657.tor.razor.com with a risk value of Trojan.Gen.2.
12:28 AM
VIRUS ALERT EVENT
A virus alert occurred on t586-7657.tor.razor.com with a risk value of Trojan.Gen.2.
12:28 AM
VIRUS ALERT EVENT
A virus alert occurred on t586-7657.tor.razor.com with a risk value of Trojan.Gen.2.
12:28 AM
VIRUS ALERT EVENT
A virus alert occurred on t586-7657.tor.razor.com with a risk value of Trojan.Gen.2.
12:28 AM
VIRUS ALERT EVENT
A virus alert occurred on t586-7657.tor.razor.com with a risk value of Trojan.Gen.2.
12:28 AM
VIRUS ALERT EVENT
A virus alert occurred on t586-7657.tor.razor.com with a risk value of Trojan.Gen.2.
INVESTIGATION ELEMENTS
Users
Eduardo Chapman
Assets
t233-4279.tor.razor.com
t586-7657.tor.razor.com

What went into this one alert?

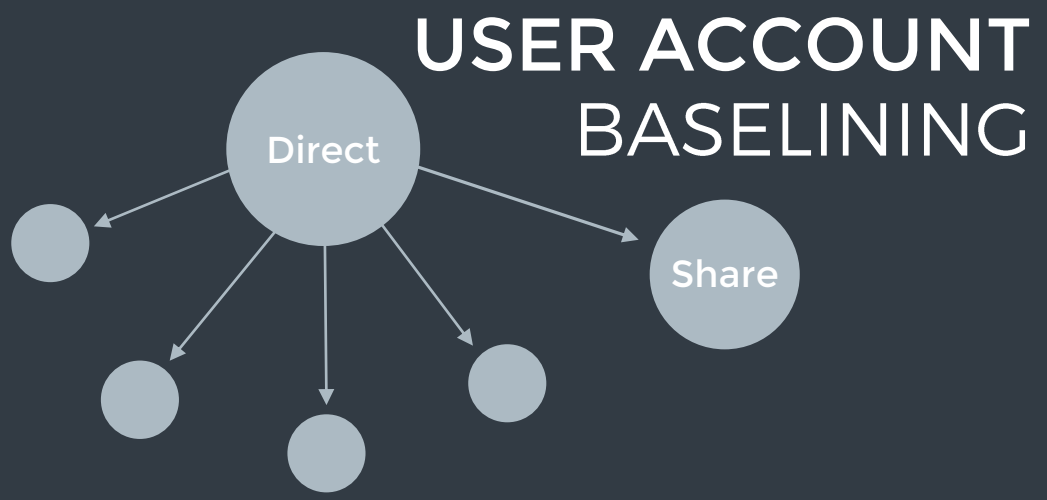
3 major components

Every account's characteristics are monitoring for classification

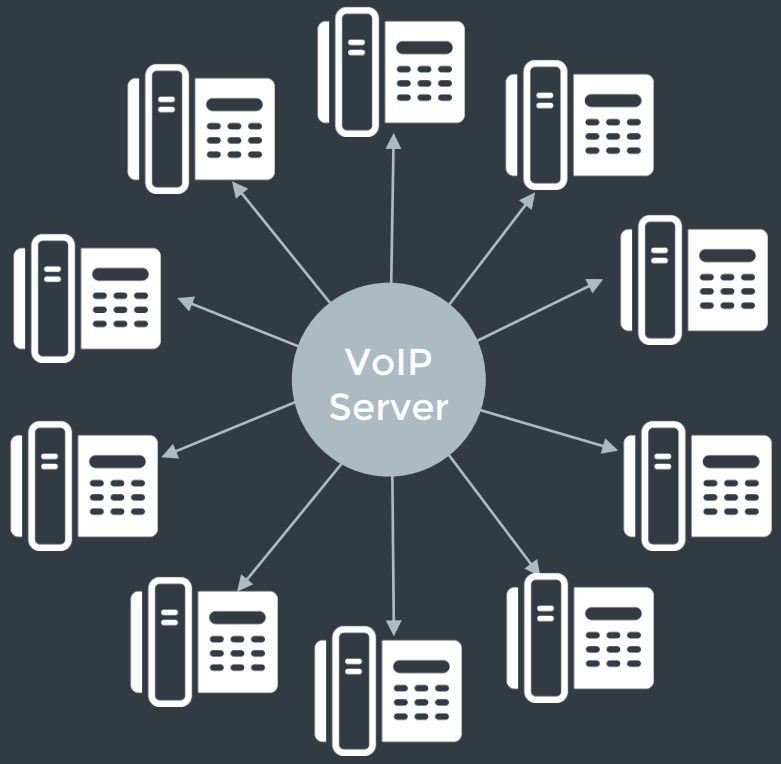
Each account's activity is baselined according to its corresponding classification

Every remote authentication is mapped between assets and compared to the baseline

Baselining Different Account Types



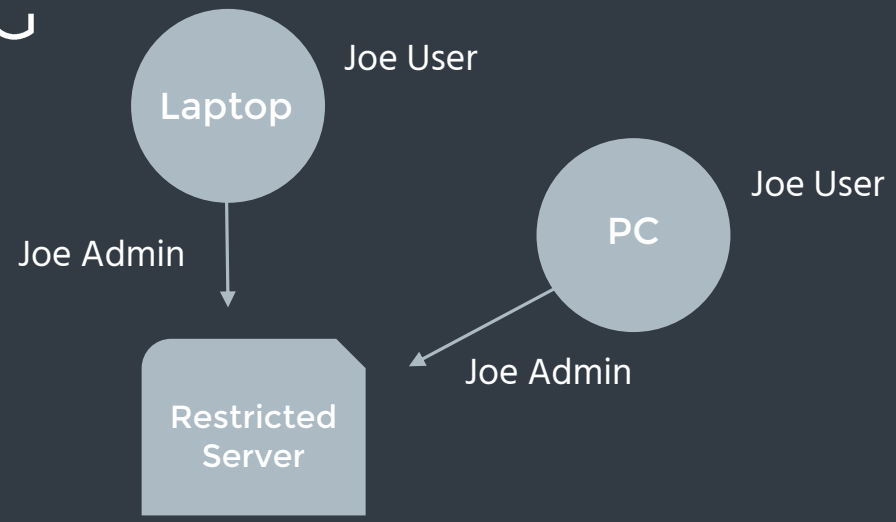
Baselining Different Account Types



SERVICE ACCOUNT
BASELINING

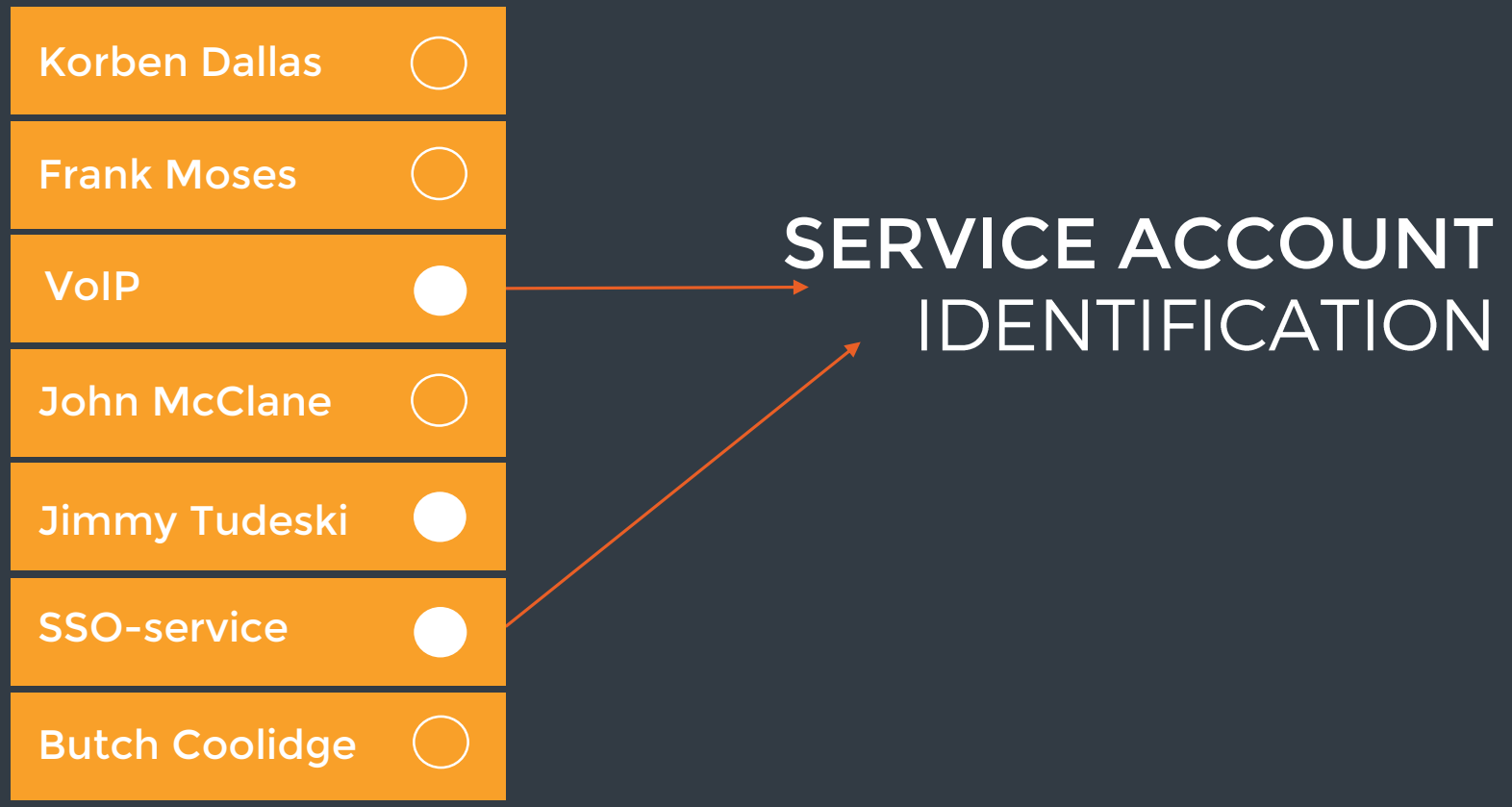
Baselining Different Account Types

DOMAIN ADMIN ACCOUNT
BASELINING

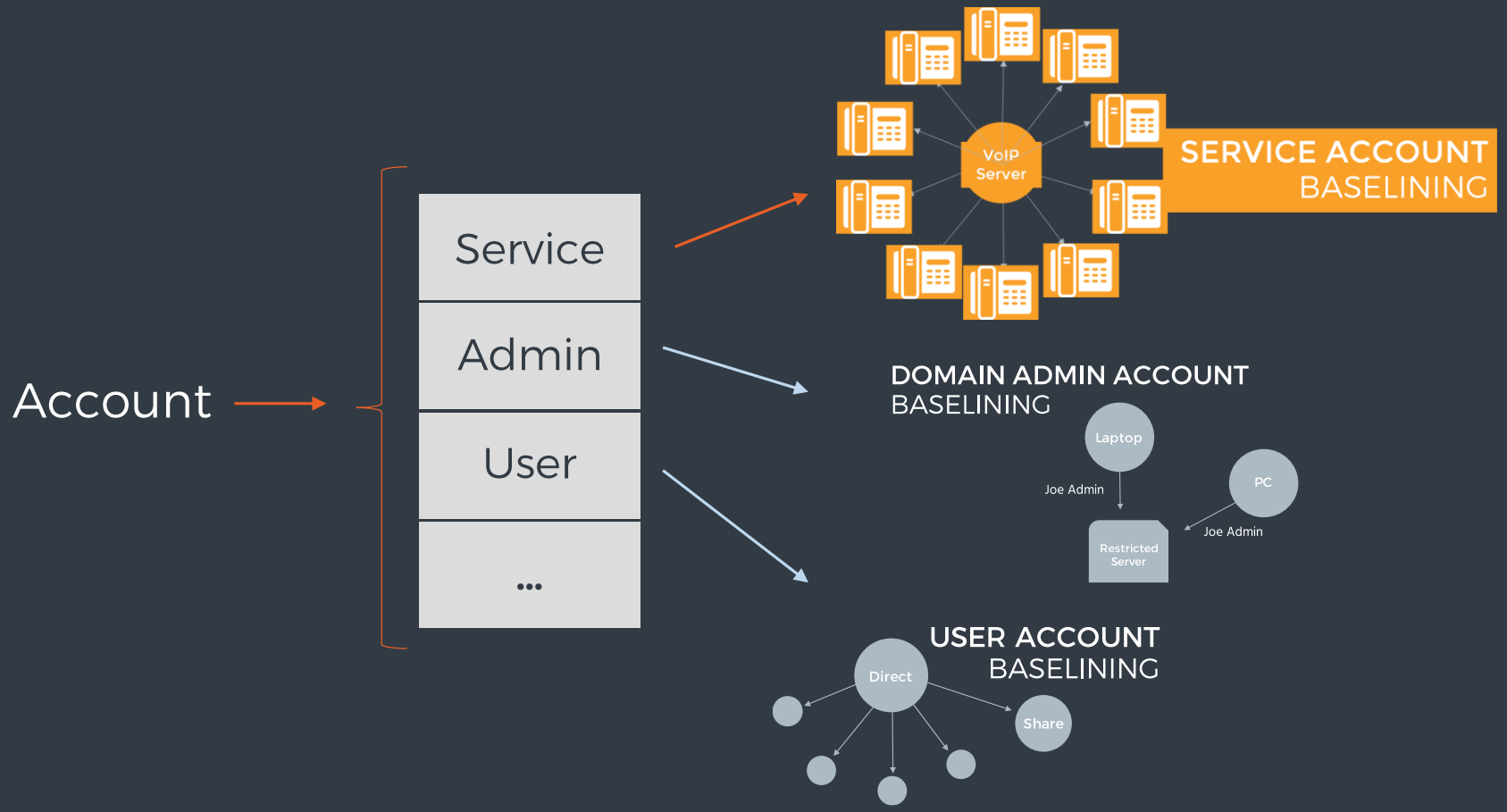


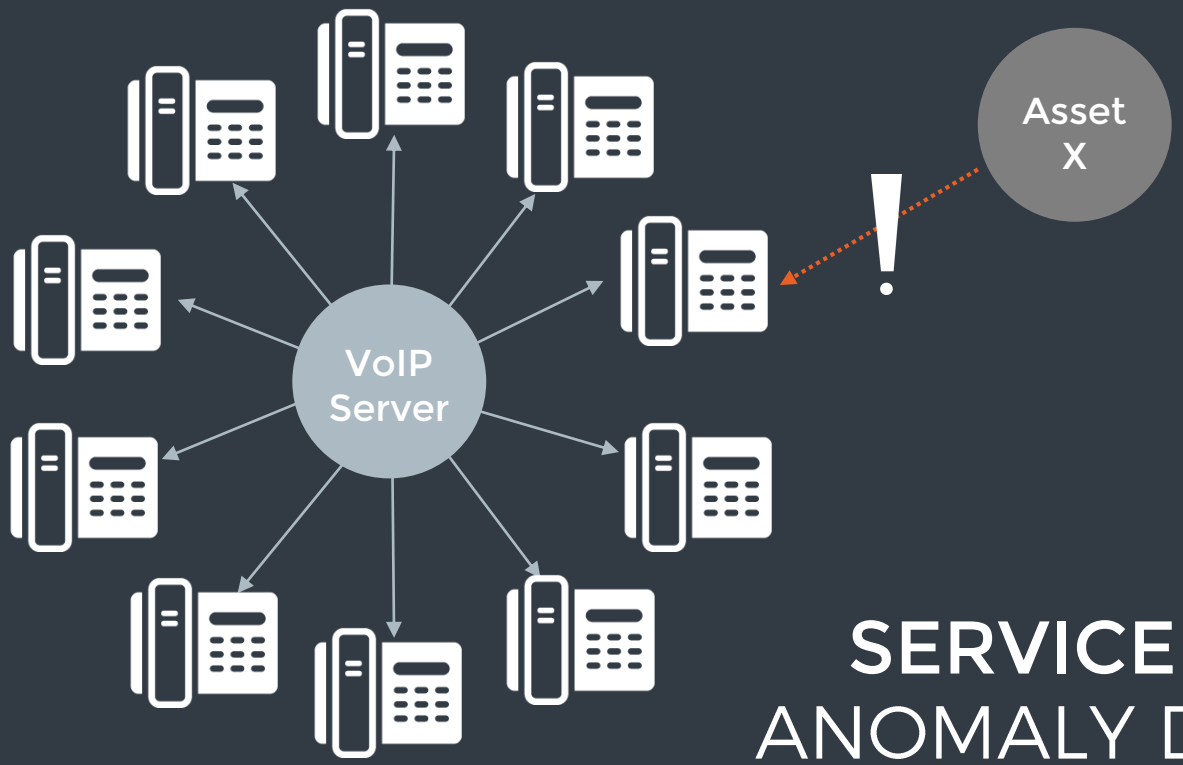
RAPID7

Account Characteristics



Account Classification



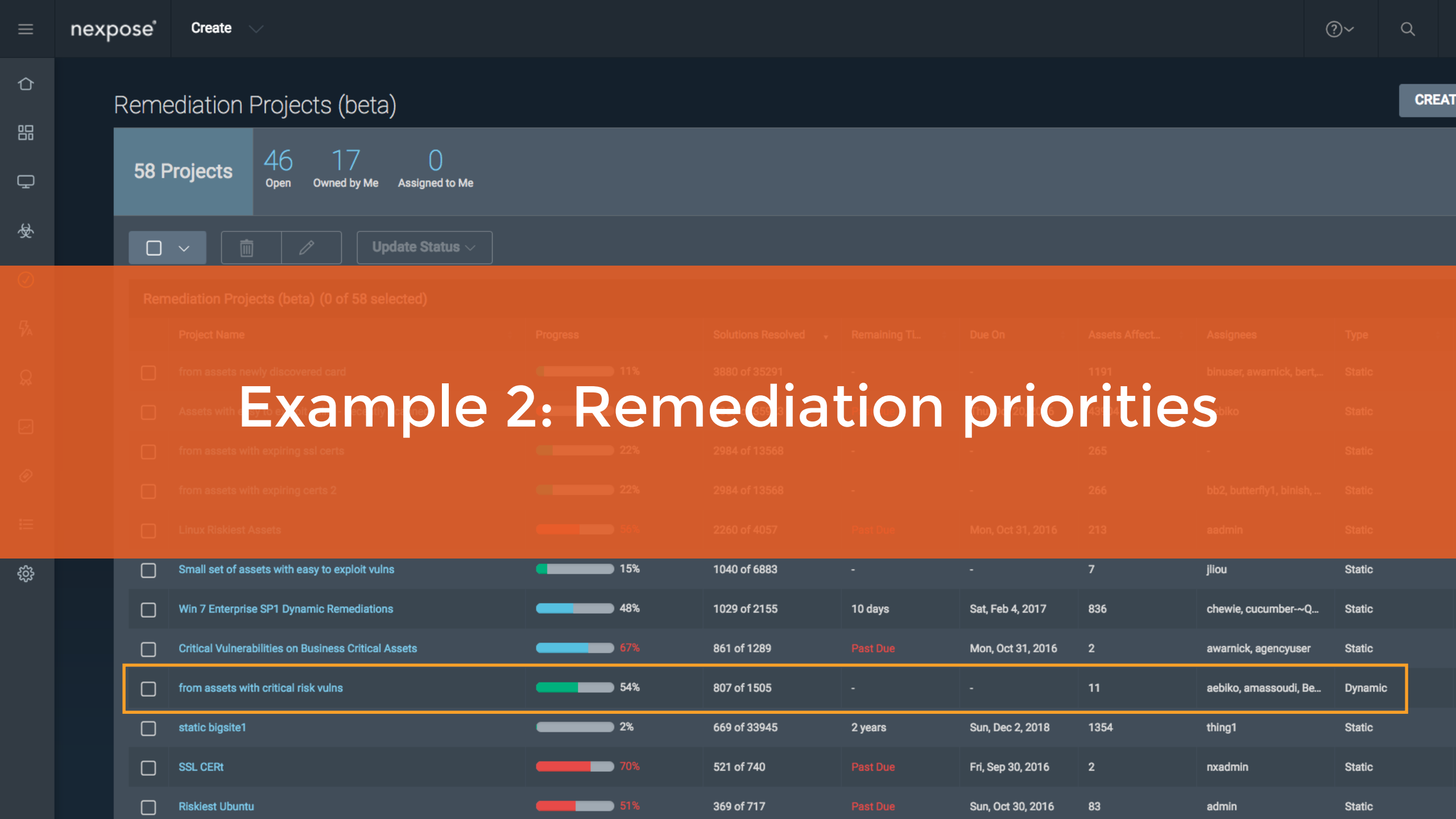


SERVICE ACCOUNT
ANOMALY DETECTION

RAPID7

With all of these together, alert

InsightIDR
ALERT



Example 2: Remediation priorities

from assets with critical risk vulns

PROJECT OVERVIEW (BETA)

PROJECT NAME	from assets with critical risk vulns
DESCRIPTION	-
CREATED ON	Tue, Sep 27, 2016
ASSETS AFFECTED	11
TOTAL REMEDIATIONS	1505
PROGRESS	54%
REMAINING TIME	-
DUE ON	-
ASSIGNEES	Akihito Ebiko, Arian Massoudi, Bear, bin2
OWNER	jliou@rapid7.com
TYPE	Dynamic
CARD ASSET FILTER	(asset.vulnerability.severity = 'CRITICAL') && (asset.vulnerability.title CONTAINS 'cve-2016-6662' || asset.vulnerability.title CONTAINS 'cve-2016-6663')
ASSET FILTER	asset.vulnerability.title CONTAINS 'cve-2016-6662' || asset.vulnerability.title CONTAINS 'cve-2016-6663'
VULNERABILITY FILTER	-

1508 Solutions

1075 Unknown Solutions

0 Pending Verification

Update Status

Remediation Solutions (0 of 1508 selected)

Solutions	Assets Affect...	Vulnerabil...	Risk Redu...	Status
Upgrade to the latest version of Oracle MySQL	11	310	389,877	Open
Upgrade to the latest version of Google Chrome	1	802	370,897	Open
Upgrade to the latest version of Mozilla Firefox	1	738	361,751	Open
Upgrade to the latest version of Oracle Java	1	432	212,805	Open
Upgrade to the latest version of PHP	2	151	125,039	Open
Configure SMB signing for Windows	11	2	17,744	Open
MS16-001: Cumulative Security Update for Internet Explorer 8 for Windows 7 (KB3124275)	3	29	16,256	Open
MS16-001: Cumulative Security Update for Internet Explorer 8 for Windows Server 2008 R2 x64 Edition (KB31242...	1	28	15,732	Open
MS14-039: Security Update for Windows Server 2008 R2 x64 Edition (KB2973201)	1	21	13,034	Open
MS16-106: Security Update for Windows 7 (KB3185911)	3	24	12,387	Open
MS15-085: Security Update for Windows Server 2008 R2 x64 Edition (KB3071756)	1	20	9,993	Open
MS16-044: Security Update for Windows 7 (KB3146706)	3	19	8,837	Open
Disable insecure TLS/SSL protocol support	11	4	7,909	Open
MS16-144: December, 2016 Security Only Quality Update for Windows 7 (KB3205394)	3	20	7,797	Open
MS15-080: Security Update for Windows 7 (KB3078601)	3	12	6,581	Open

What went into this list of priorities?

3 major components

Every project is a series of remediation solutions with a live total Risk Reduction

Each solution has a live total Risk Reduction achieved if completed

The Risk Reduction is the combined total of each vulnerability's Real Risk score

RAPID7

Remediation Projects

1.	**Traders environment**	**35,291**
2.	Linux riskiest assets	13,567
3.	Static bigsite	12,654
4.	Corporate sales remediations	7,985
5.	Riskiest ubuntu	4,325
6.	Assets with medium vulns	1,509
7.	Assets with expiring certs	665

Priority #1

Traders environment **Total: 35,291**

1.	Upgrade to latest version of Oracle	10,434
2.	Configure SMB signing for Windows	5,437
3.	Upgrade to latest version of Firefox	4,903
4.	MS16-001: Security update	2,101
5.	MS16-106: Security update for Windows 7	323
6.	MS15-085: Security update for Internet Exp	224

VULNERABILITY RISK SCORE

CVSS
AGE
EXPLOIT EASE
EXPLOITS KNOWN

\+ Superseding vulnerability patched

\+ Solution implemented

\+ Asset criticality changed

RAPID7

EXAMPLE

Remediation Projects

1.	**Traders environment**	**35,291**
2.	Linux riskiest assets	13,567
3.	Static bigsite	12,654
4.	Corporate sales remediations	7,985
5.	Riskiest ubuntu	4,325
6.	Assets with medium vulns	1,509
7.	Assets with expiring certs	665

Priority #1

Corporate sales remediations **Total: 35,291**

1.	Upgrade to latest version of Google Chrome	12,686
2.	Configure SMB signing for Windows	15,437
3.	Upgrade to latest version of PHP	8,943
4.	Upgrade to latest version of Oracle Java	2,101
5.	MS16-106: Security update for Windows 7	732
6.	MS15-09: Security update for Windows Server	523

VULNERABILITY RISK SCORE

- CVSS
- AGE
- EXPLOIT EASE
- EXPLOITS KNOWN

\+ Superseding vulnerability patched

\+ Solution implemented

\+ Change in asset criticality

RAPID7

In Summary

- Analytics ≠ Superpowers
- They are effective when targeted
- 90% of work is beneath the surface

RAPID7

Thank You!

RAPID7