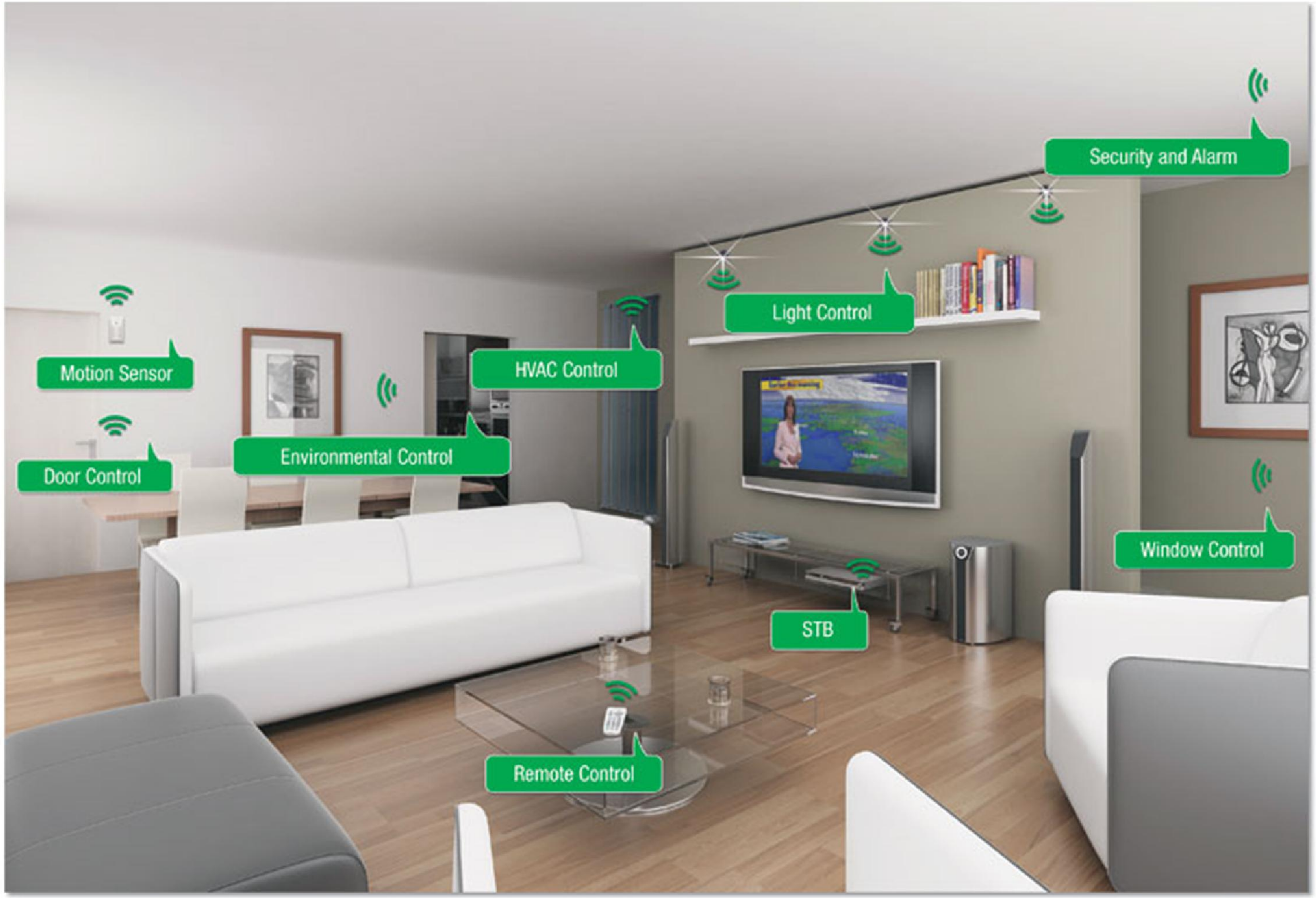
Hiệp hội An toàn thông tin Việt Nam

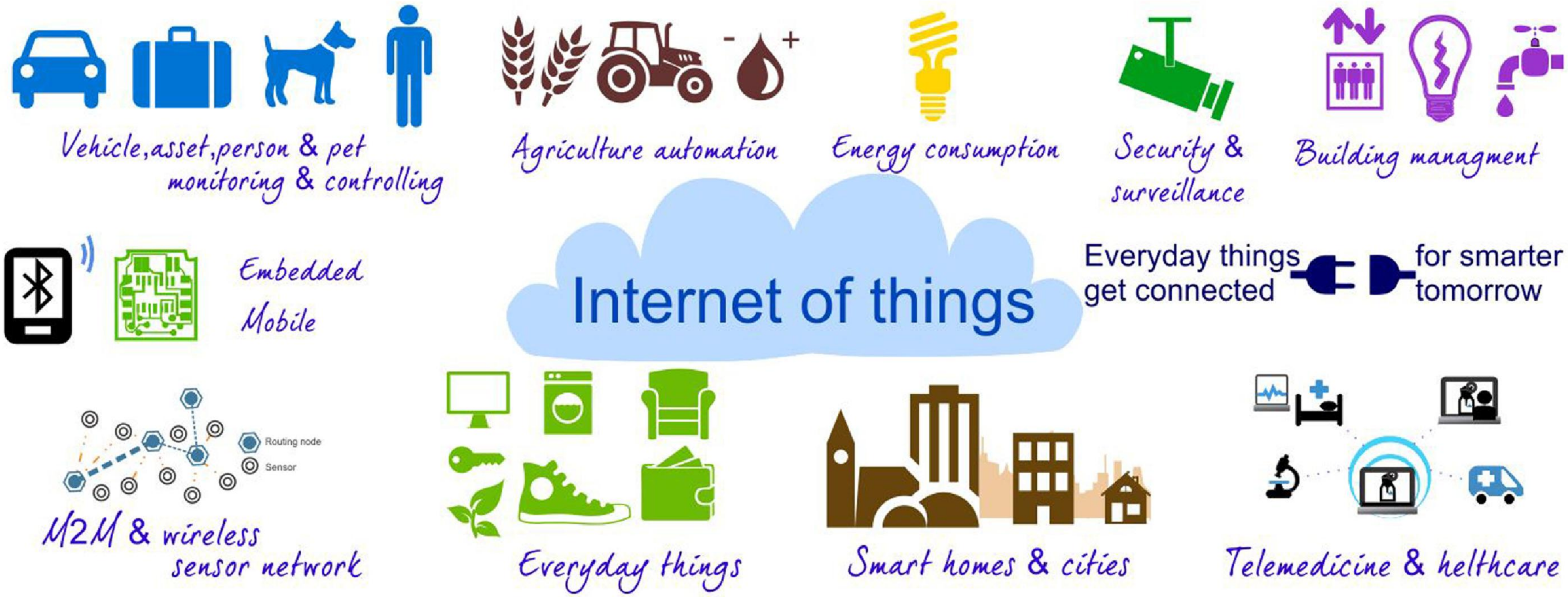
GIÁM SÁT VẬN HÀNH VÀ BẢO MẬT CHO IOT & 4G

Nguyen Thanh Dat
Deputy CEO, Vietnam Cyberspace Security Technology (VNCS)

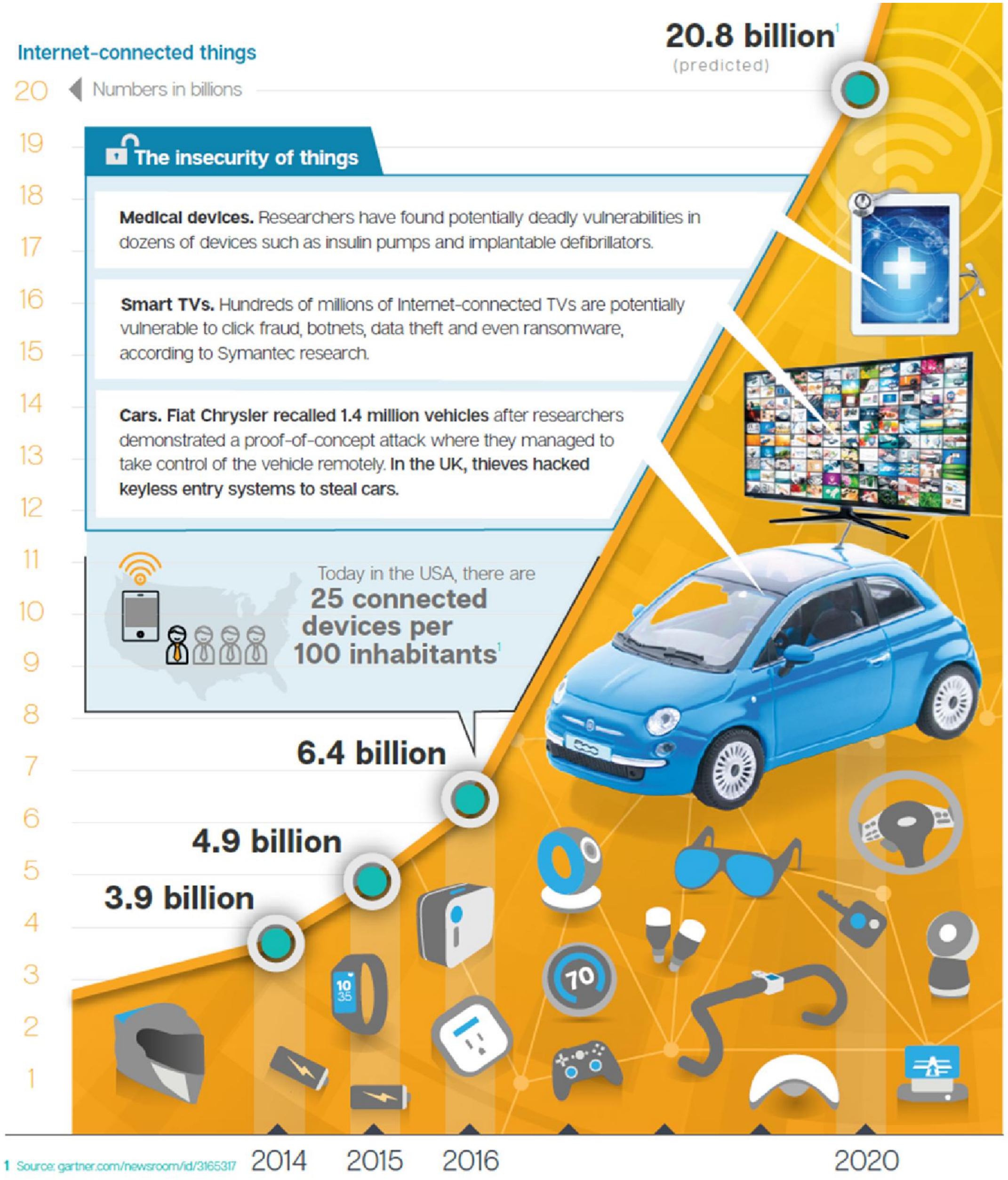
Internet of Thing



Internet of Thing



Internet of Thing



The insecurity of things

Medical devices. Researchers have found potentially deadly vulnerabilities in dozens of devices such as insulin pumps and implantable defibrillators.

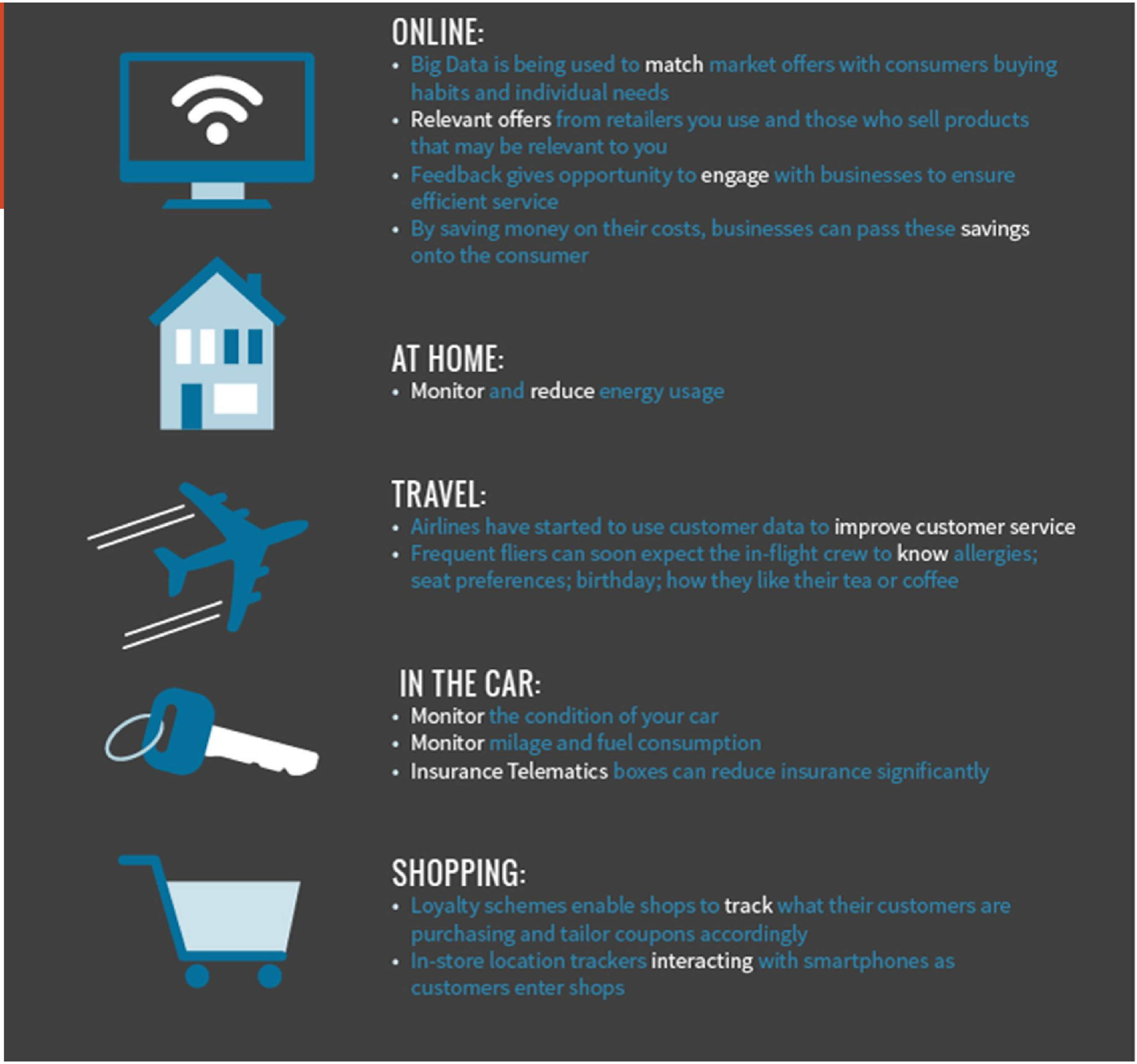
Smart TVs. Hundreds of millions of Internet-connected TVs are potentially vulnerable to click fraud, botnets, data theft and even ransomware, according to Symantec research.

Cars. Fiat Chrysler recalled 1.4 million vehicles after researchers demonstrated a proof-of-concept attack where they managed to take control of the vehicle remotely. **In the UK, thieves hacked keyless entry systems to steal cars.**

Today in the USA, there are **25 connected devices per 100 inhabitants**[1]

[1] Source: gartner.com/newsroom/id/3165317

Benefits



ONLINE:

- Big Data is being used to match market offers with consumers buying habits and individual needs
- Relevant offers from retailers you use and those who sell products that may be relevant to you
- Feedback gives opportunity to engage with businesses to ensure efficient service
- By saving money on their costs, businesses can pass these savings onto the consumer

AT HOME:

- Monitor and reduce energy usage

TRAVEL:

- Airlines have started to use customer data to improve customer service
- Frequent fliers can soon expect the in-flight crew to know allergies; seat preferences; birthday; how they like their tea or coffee

IN THE CAR:

- Monitor the condition of your car
- Monitor milage and fuel consumption
- Insurance Telematics boxes can reduce insurance significantly

SHOPPING:

- Loyalty schemes enable shops to track what their customers are purchasing and tailor coupons accordingly
- In-store location trackers interacting with smartphones as customers enter shops

Source : Vouchercloud

Security ?

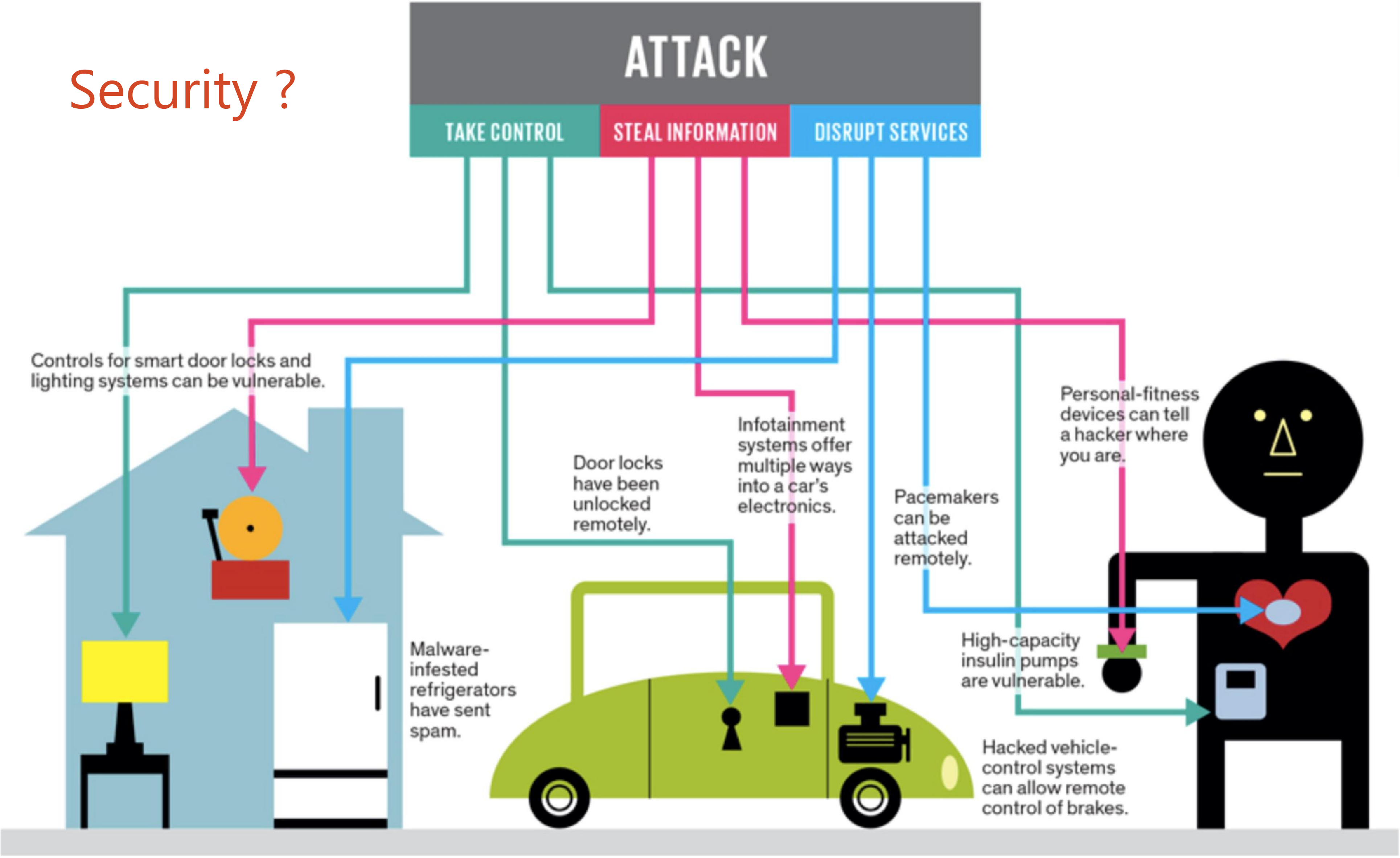

ATTACK
TAKE CONTROL
STEAL INFORMATION
DISRUPT SERVICES
Controls for smart door locks and lighting systems can be vulnerable.
Door locks have been unlocked remotely.
Infotainment systems offer multiple ways into a car's electronics.
Pacemakers can be attacked remotely.
Personal-fitness devices can tell a hacker where you are.
Malware-infested refrigerators have sent spam.
High-capacity insulin pumps are vulnerable.
Hacked vehicle-control systems can allow remote control of brakes.

Illustration: J. D. King

Tôi muốn hack tất cả mọi thứ có chip
trong bán kính 2 dặm

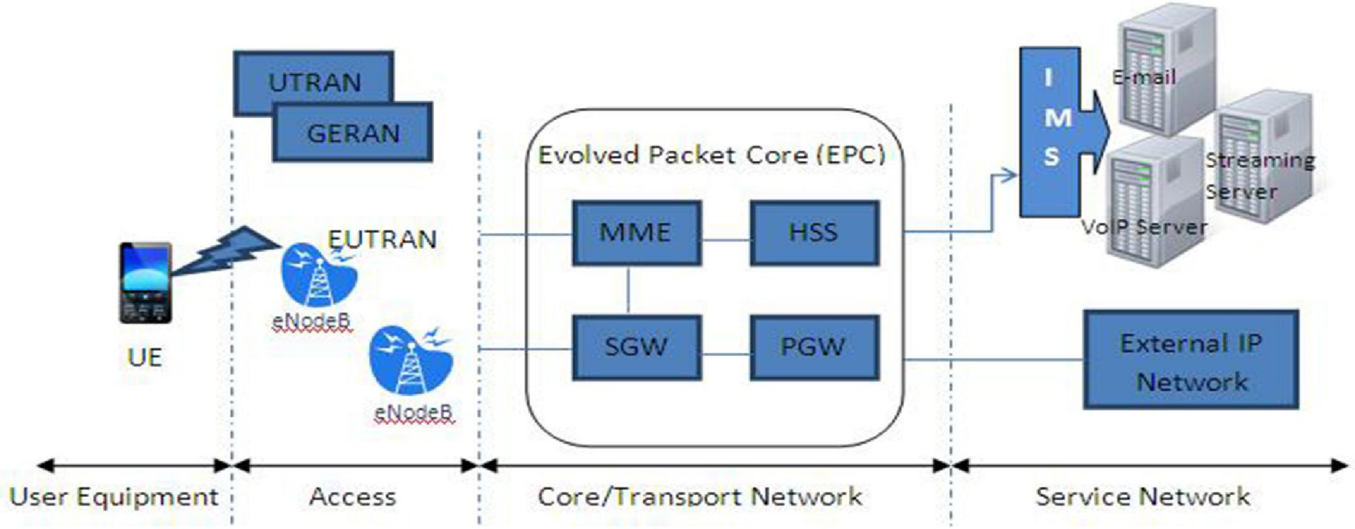
Smart Home giving away the keys to your kingdom?

Medical Devices Are Vulnerable to Life-Threatening Hacks

Chrysler recalls 1.4 million cars at risk of being remotely hijacked

Smart TV got infected with ransomware

4G LTE
Security risks



UE

- ❖ Physical attacks
- ❖ Lack of security standards & controls on UEs
- ❖ Risk of data loss, privacy
- ❖ Application layer: virus, malware, phishing

Access

- ❖ Physical attacks
- ❖ Eavesdropping, Redirection, MitM attacks, DoS
- ❖ Rogue eNodeBs
- ❖ Privacy

Core

- ❖ Unauthorised access
- ❖ DoS and DDoS attacks
- ❖ Overbilling attacks (IP address hijacking, IP spoofing)

Service

- ❖ Unauthorised access
- ❖ Service abuse attacks, Theft of service
- ❖ Network snoop, session hijacking

Source: www.csiac.org

Liệu các công nghệ hiện tại có giải quyết được những thách thức mới ?

Thách thức

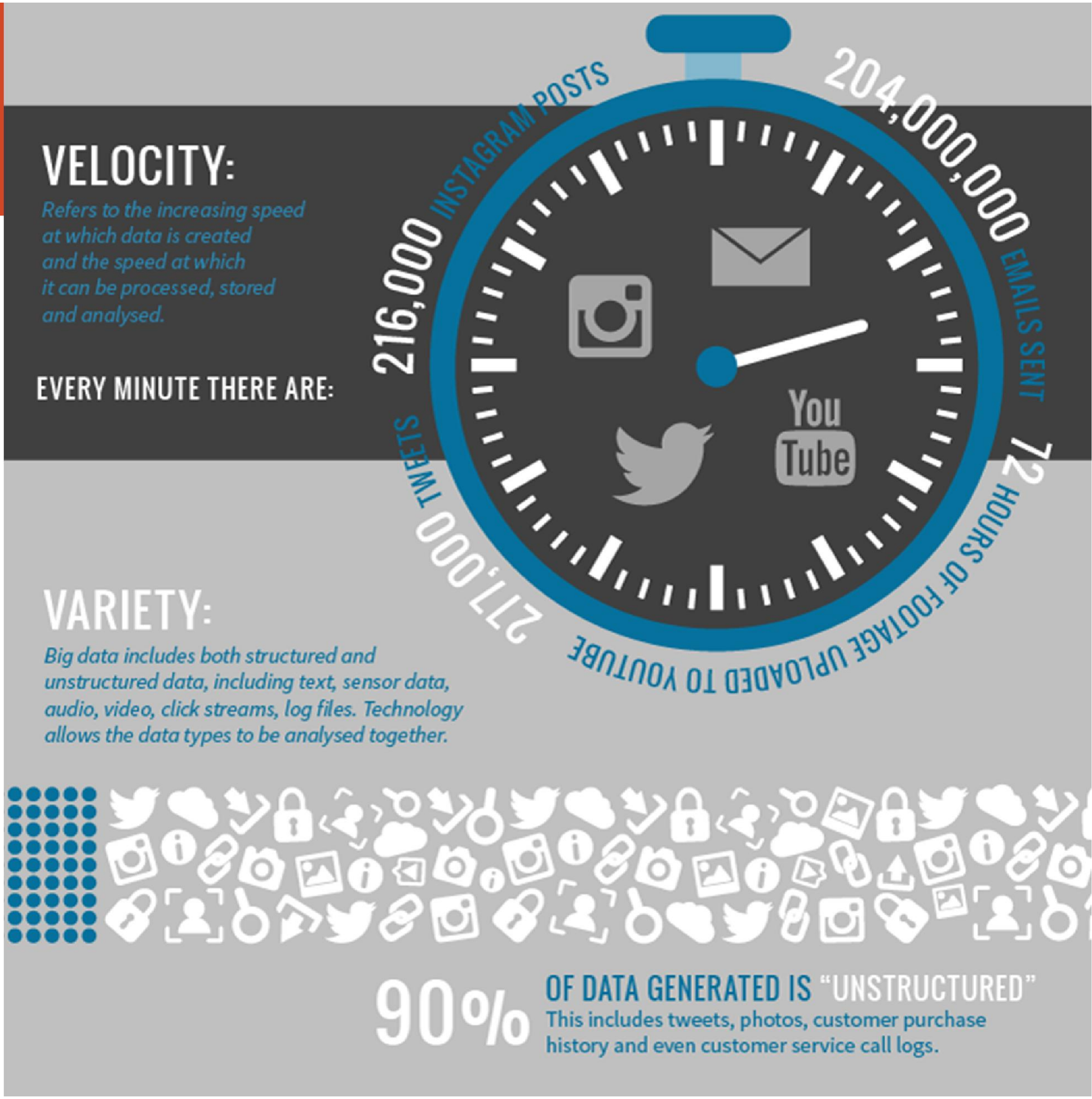
Scalability

Reporting & Visualization

Big data storage

Information Context

Breadth of functions



VELOCITY:

Refers to the increasing speed at which data is created and the speed at which it can be processed, stored and analysed.

EVERY MINUTE THERE ARE:

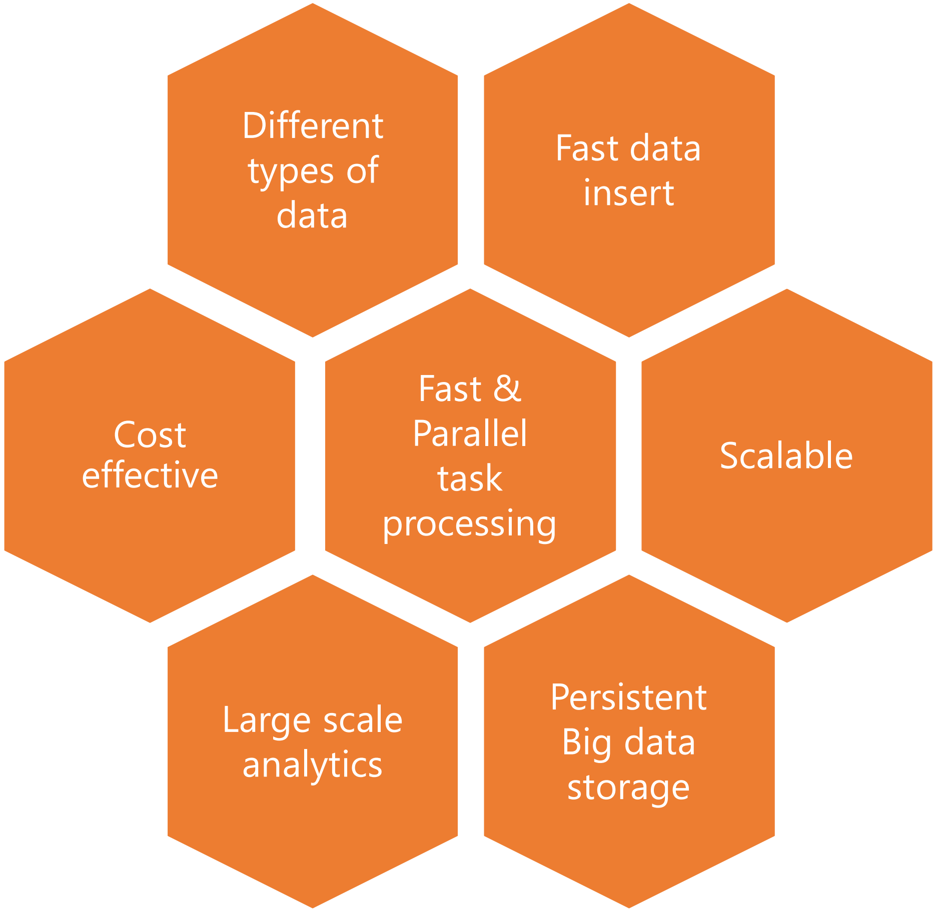
VARIETY:

Big data includes both structured and unstructured data, including text, sensor data, audio, video, click streams, log files. Technology allows the data types to be analysed together.

90% OF DATA GENERATED IS "UNSTRUCTURED"

This includes tweets, photos, customer purchase history and even customer service call logs.

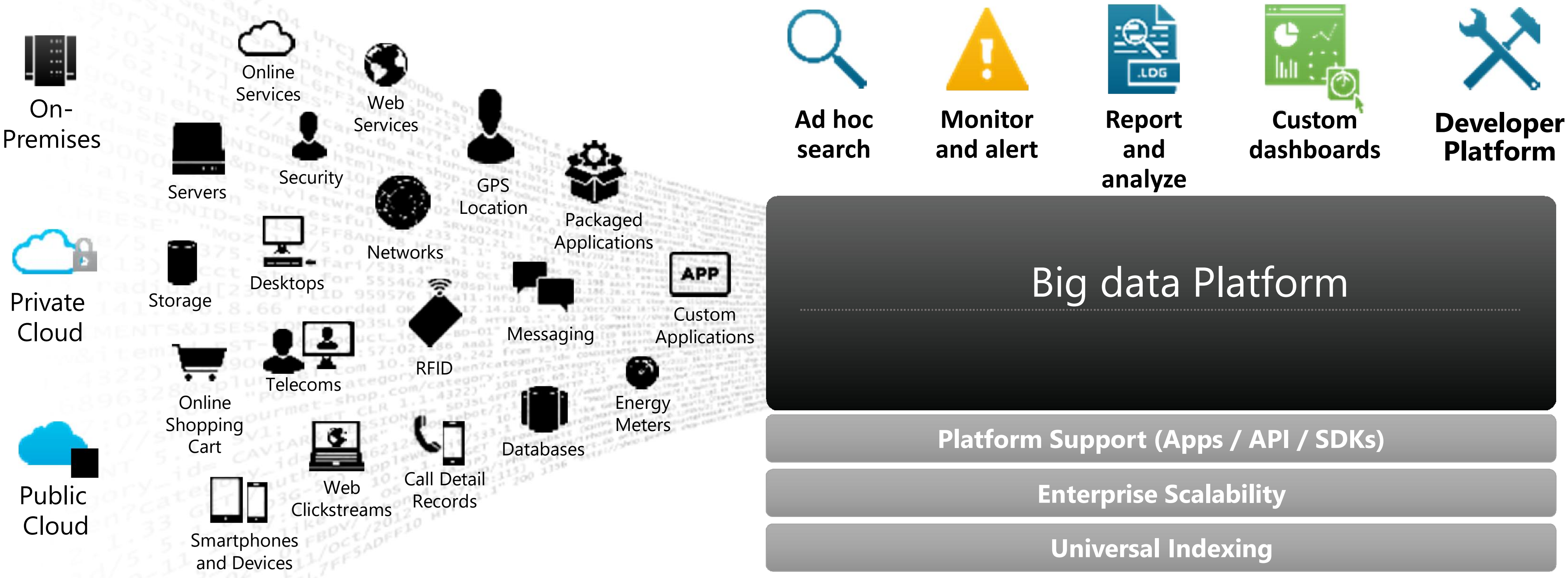
Lợi ích trong việc ứng dụng Big Data



Nền tảng Big Data cho vận hành và bảo mật

Data: Any Location, Type, Volume

Answer Any Question



On-Premises

Private Cloud

Public Cloud

Online Services

Web Services

Servers

Security

GPS Location

Packaged Applications

Networks

Storage

Desktops

Messaging

Custom Applications

RFID

Telecoms

Online Shopping Cart

Energy Meters

Databases

Web Clickstreams

Call Detail Records

Smartphones and Devices

Ad hoc search

Monitor and alert

Report and analyze

Custom dashboards

Developer Platform

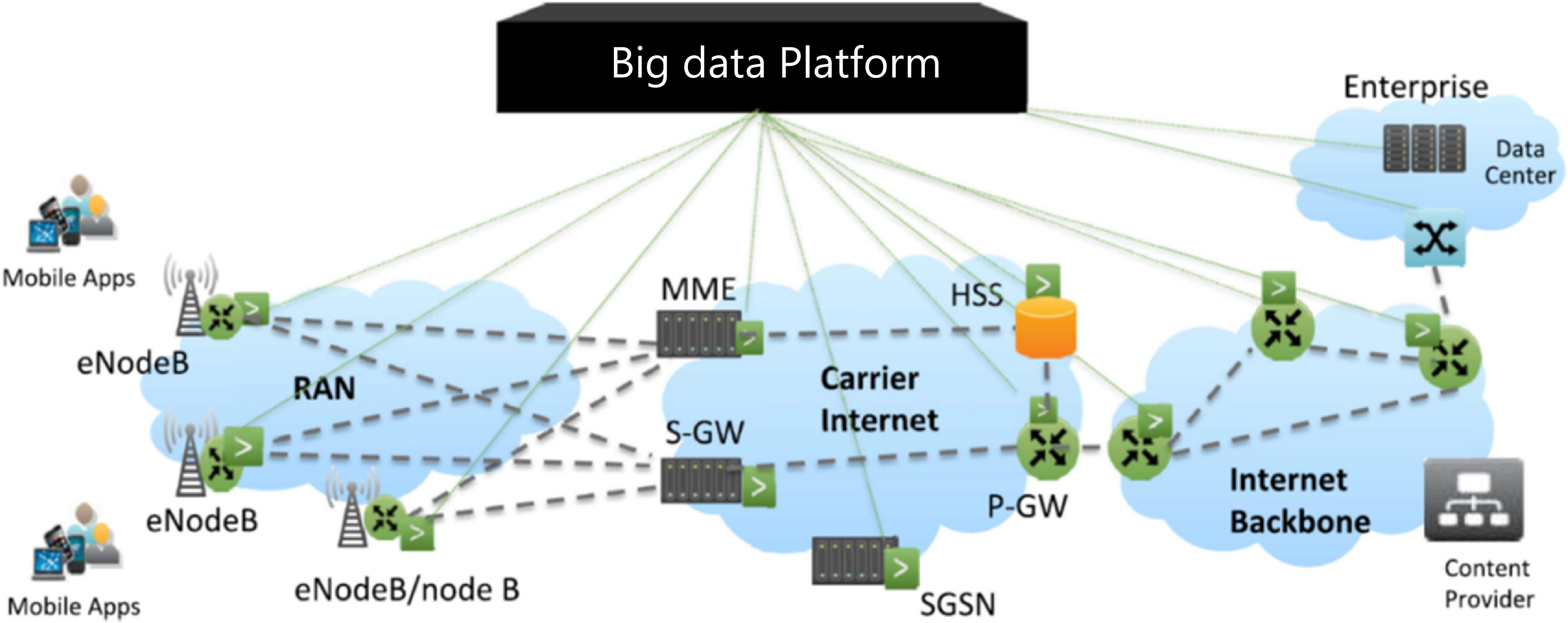
Big data Platform

Platform Support (Apps / API / SDKs)

Enterprise Scalability

Universal Indexing

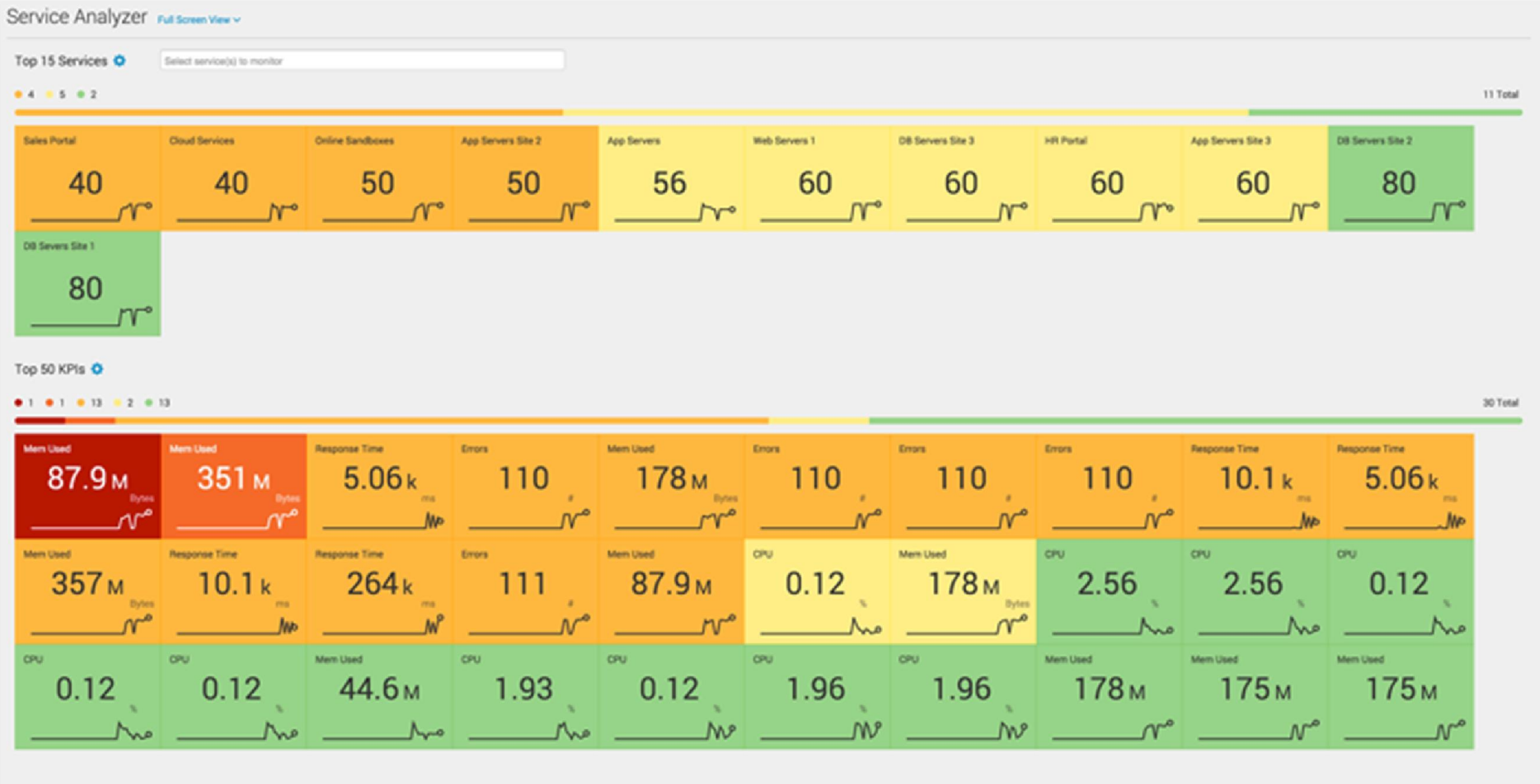
For Telco



Big data Platform
Enterprise
Data Center
Mobile Apps
eNodeB
RAN
MME
HSS
Carrier Internet
S-GW
eNodeB
Mobile Apps
eNodeB/node B
SGSN
P-GW
Internet Backbone
Content Provider

Operational Intelligence

High-level view of services and composite health scores



Service Analyzer

Top 15 Services

● 4 ● 5 ● 2 — 11 Total

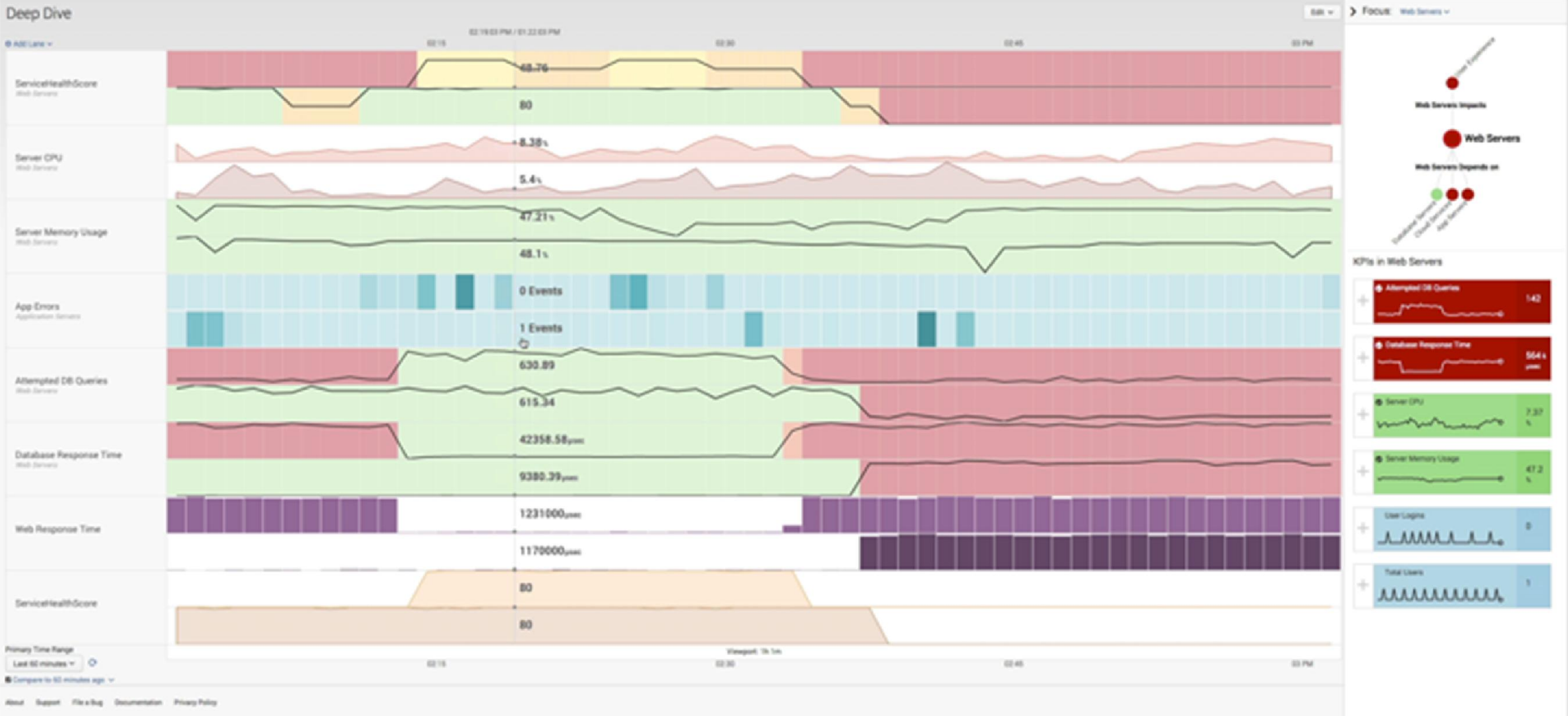
Sales Portal 40	Cloud Services 40	Online Sandboxes 50	App Servers Site 2 50	App Servers 56	Web Servers 1 60	DB Servers Site 3 60	HR Portal 60	App Servers Site 3 60	DB Servers Site 2 80
DB Severs Site 1 80									

Top 50 KPIs

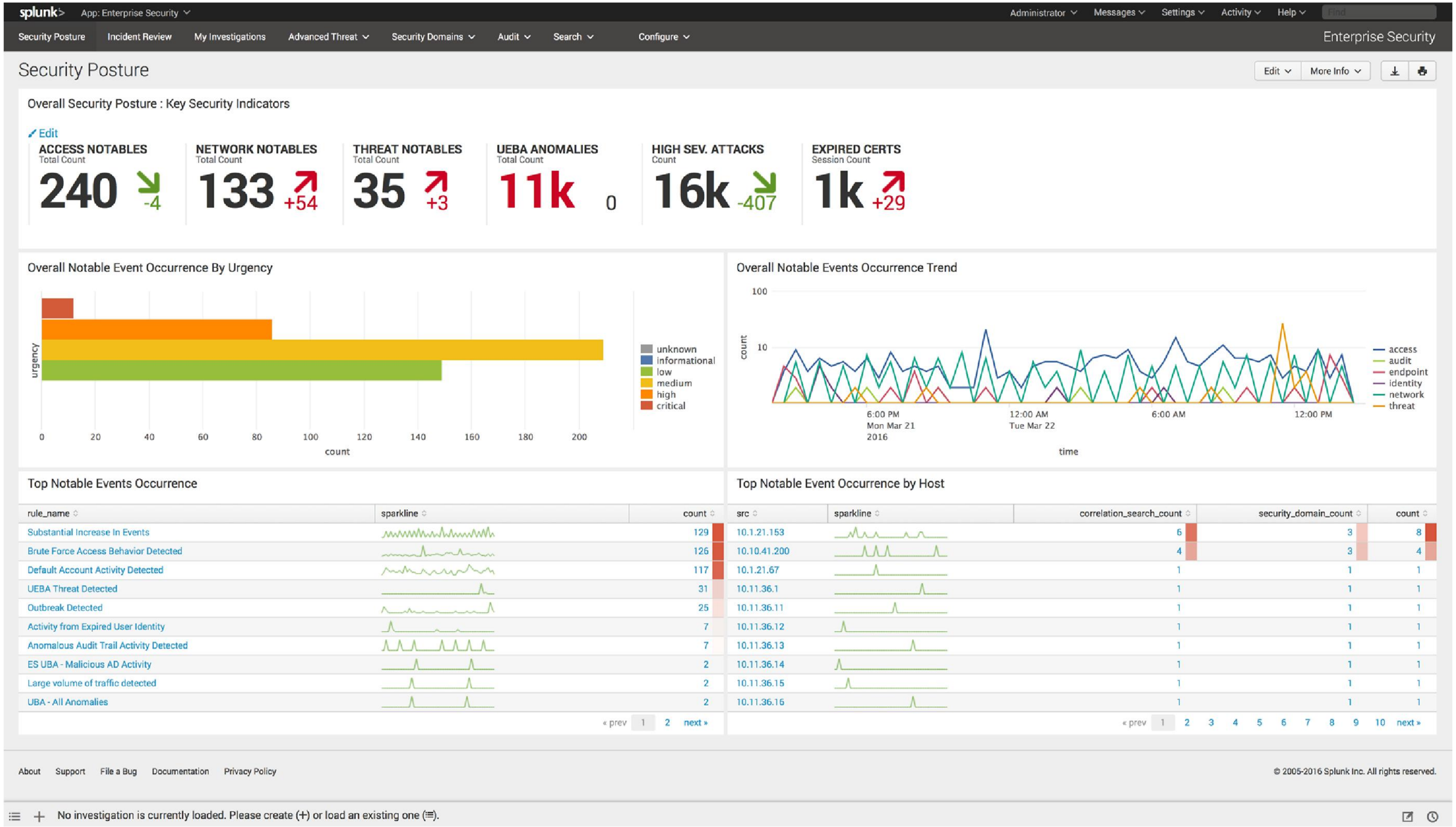
● 1 ● 1 ● 13 ● 2 ● 13 — 30 Total

Mem Used 87.9 M Bytes	Mem Used 351 M Bytes	Response Time 5.06 k ms	Errors 110 #	Mem Used 178 M Bytes	Errors 110 #	Errors 110 #	Errors 110 #	Response Time 10.1 k ms	Response Time 5.06 k ms
Mem Used 357 M Bytes	Response Time 10.1 k ms	Response Time 264 k ms	Errors 111 #	Mem Used 87.9 M	CPU 0.12 %	Mem Used 178 M Bytes	CPU 2.56 %	CPU 2.56 %	CPU 0.12 %
CPU 0.12 %	CPU 0.12 %	Mem Used 44.6 M	CPU 1.93 %	CPU 0.12 %	CPU 1.96 %	CPU 1.96 %	Mem Used 178 M	Mem Used 175 M	Mem Used 175 M

Deep Dives


Deep Dive
Edit
Add Lane
02:19:03 PM / 01:22:03 PM
02:15
02:30
02:45
03 PM
ServiceHealthScore
Web Servers
48.76
80
Server CPU
Web Servers
8.38%
5.4%
Server Memory Usage
Web Servers
47.21%
48.1%
App Errors
Application Servers
0 Events
1 Events
Attempted DB Queries
Web Servers
630.89
615.34
Database Response Time
Web Servers
42358.58μsec
9380.39μsec
Web Response Time
1231000μsec
1170000μsec
ServiceHealthScore
80
80
Primary Time Range
Last 60 minutes
Compare to 60 minutes ago
Viewport: 1h 1m
About
Support
File a Bug
Documentation
Privacy Policy
Focus: Web Servers
User Experience
Web Servers Impacts
Web Servers
Web Servers Depends on
Database Servers
Cloud Services
App Servers
KPIs in Web Servers
Attempted DB Queries
142
Database Response Time
564 k μsec
Server CPU
7.37 %
Server Memory Usage
47.2 %
User Logins
0
Total Users
1

Security Posture



Security Posture

Overall Security Posture : Key Security Indicators

ACCESS NOTABLES Total Count	NETWORK NOTABLES Total Count	THREAT NOTABLES Total Count	UEBA ANOMALIES Total Count	HIGH SEV. ATTACKS Count	EXPIRED CERTS Session Count
240 ↘ -4	133 ↗ +54	35 ↗ +3	11k 0	16k ↘ -407	1k ↗ +29

Overall Notable Event Occurrence By Urgency

Overall Notable Events Occurrence Trend

Top Notable Events Occurrence

rule_name	sparkline	count
Substantial Increase In Events		129
Brute Force Access Behavior Detected		126
Default Account Activity Detected		117
UEBA Threat Detected		31
Outbreak Detected		25
Activity from Expired User Identity		7
Anomalous Audit Trail Activity Detected		7
ES UBA - Malicious AD Activity		2
Large volume of traffic detected		2
UBA - All Anomalies		2

« prev 1 2 next »

Top Notable Event Occurrence by Host

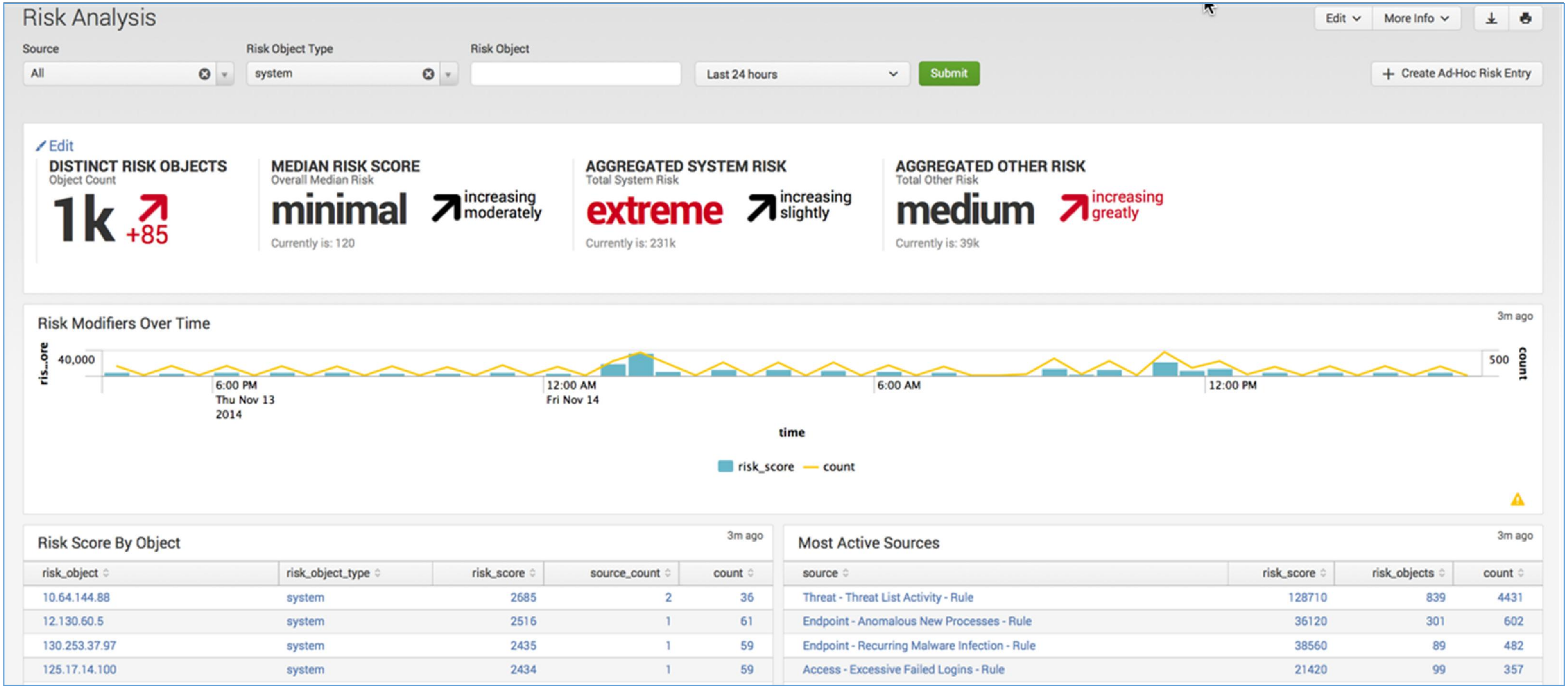
src	sparkline	correlation_search_count	security_domain_count	count
10.1.21.153		6	3	8
10.10.41.200		4	3	4
10.1.21.67		1	1	1
10.11.36.1		1	1	1
10.11.36.11		1	1	1
10.11.36.12		1	1	1
10.11.36.13		1	1	1
10.11.36.14		1	1	1
10.11.36.15		1	1	1
10.11.36.16		1	1	1

« prev 1 2 3 4 5 6 7 8 9 10 next »

About Support File a Bug Documentation Privacy Policy

No investigation is currently loaded. Please create (+) or load an existing one (≡).

Risk-Based Analytics



Risk Analysis

Source: All

Risk Object Type: system

Risk Object:

Last 24 hours

DISTINCT RISK OBJECTS
Object Count
1k +85

MEDIAN RISK SCORE
Overall Median Risk
minimal increasing moderately
Currently is: 120

AGGREGATED SYSTEM RISK
Total System Risk
extreme increasing slightly
Currently is: 231k

AGGREGATED OTHER RISK
Total Other Risk
medium increasing greatly
Currently is: 39k

Risk Modifiers Over Time

Risk Score By Object

3m ago

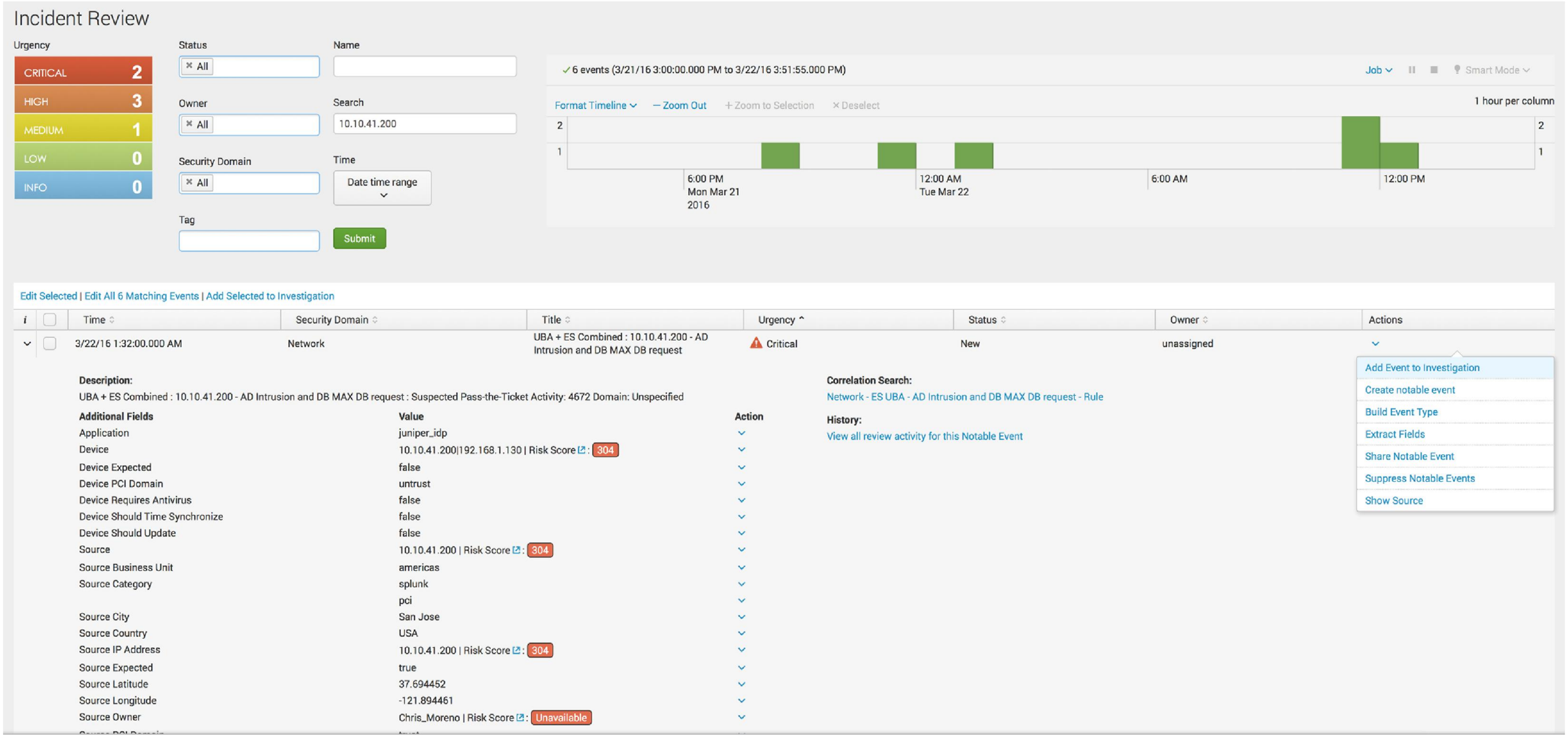
risk_object	risk_object_type	risk_score	source_count	count
10.64.144.88	system	2685	2	36
12.130.60.5	system	2516	1	61
130.253.37.97	system	2435	1	59
125.17.14.100	system	2434	1	59

Most Active Sources

3m ago

source	risk_score	risk_objects	count
Threat - Threat List Activity - Rule	128710	839	4431
Endpoint - Anomalous New Processes - Rule	36120	301	602
Endpoint - Recurring Malware Infection - Rule	38560	89	482
Access - Excessive Failed Logins - Rule	21420	99	357

Fast Incident Review and Investigation



Incident Review

Urgency

CRITICAL	2
HIGH	3
MEDIUM	1
LOW	0
INFO	0

Status: × All

Name:

Owner: × All

Search: 10.10.41.200

Security Domain: × All

Time: Date time range

Tag:

✓ 6 events (3/21/16 3:00:00.000 PM to 3/22/16 3:51:55.000 PM)

Edit Selected | Edit All 6 Matching Events | Add Selected to Investigation

i	□	Time	Security Domain	Title	Urgency	Status	Owner	Actions
⌄	□	3/22/16 1:32:00.000 AM	Network	UBA + ES Combined : 10.10.41.200 - AD Intrusion and DB MAX DB request	⚠ Critical	New	unassigned	⌄

Description:

UBA + ES Combined : 10.10.41.200 - AD Intrusion and DB MAX DB request : Suspected Pass-the-Ticket Activity: 4672 Domain: Unspecified

Additional Fields	Value	Action
Application	juniper_idp	⌄
Device	10.10.41.200|192.168.1.130 | Risk Score : 304	⌄
Device Expected	false	⌄
Device PCI Domain	untrust	⌄
Device Requires Antivirus	false	⌄
Device Should Time Synchronize	false	⌄
Device Should Update	false	⌄
Source	10.10.41.200 | Risk Score : 304	⌄
Source Business Unit	americas	⌄
Source Category	splunk	⌄
	pci	⌄
Source City	San Jose	⌄
Source Country	USA	⌄
Source IP Address	10.10.41.200 | Risk Score : 304	⌄
Source Expected	true	⌄
Source Latitude	37.694452	⌄
Source Longitude	-121.894461	⌄
Source Owner	Chris_Moreno | Risk Score : Unavailable	⌄

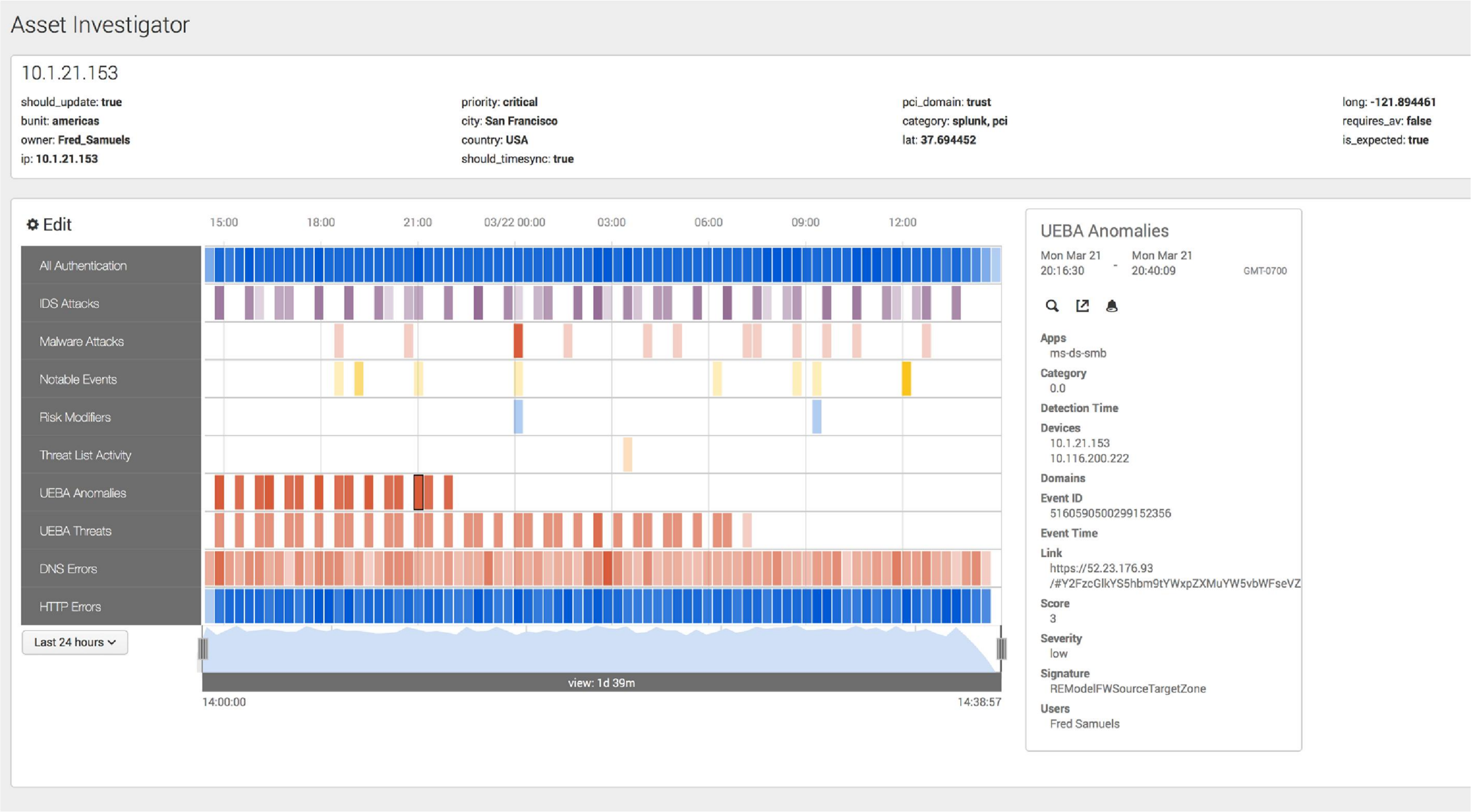
Correlation Search:

Network - ES UBA - AD Intrusion and DB MAX DB request - Rule

History:

View all review activity for this Notable Event

Visual Investigations for All Assets and Users



Asset Investigator

10.1.21.153

should_update: **true**
bunit: **americas**
owner: **Fred_Samuels**
ip: **10.1.21.153**

priority: **critical**
city: **San Francisco**
country: **USA**
should_timesync: **true**

pci_domain: **trust**
category: **splunk, pci**
lat: **37.694452**

long: **-121.894461**
requires_av: **false**
is_expected: **true**

UEBA Anomalies

Mon Mar 21 20:16:30 - Mon Mar 21 20:40:09 GMT-0700

Apps
ms-ds-smb

Category
0.0

Detection Time

Devices
10.1.21.153
10.116.200.222

Domains

Event ID
5160590500299152356

Event Time

Link
https://52.23.176.93
/#Y2FzcGlkYS5hbm9tYWxpZXMuYW5vbWFseVZ

Score
3

Severity
low

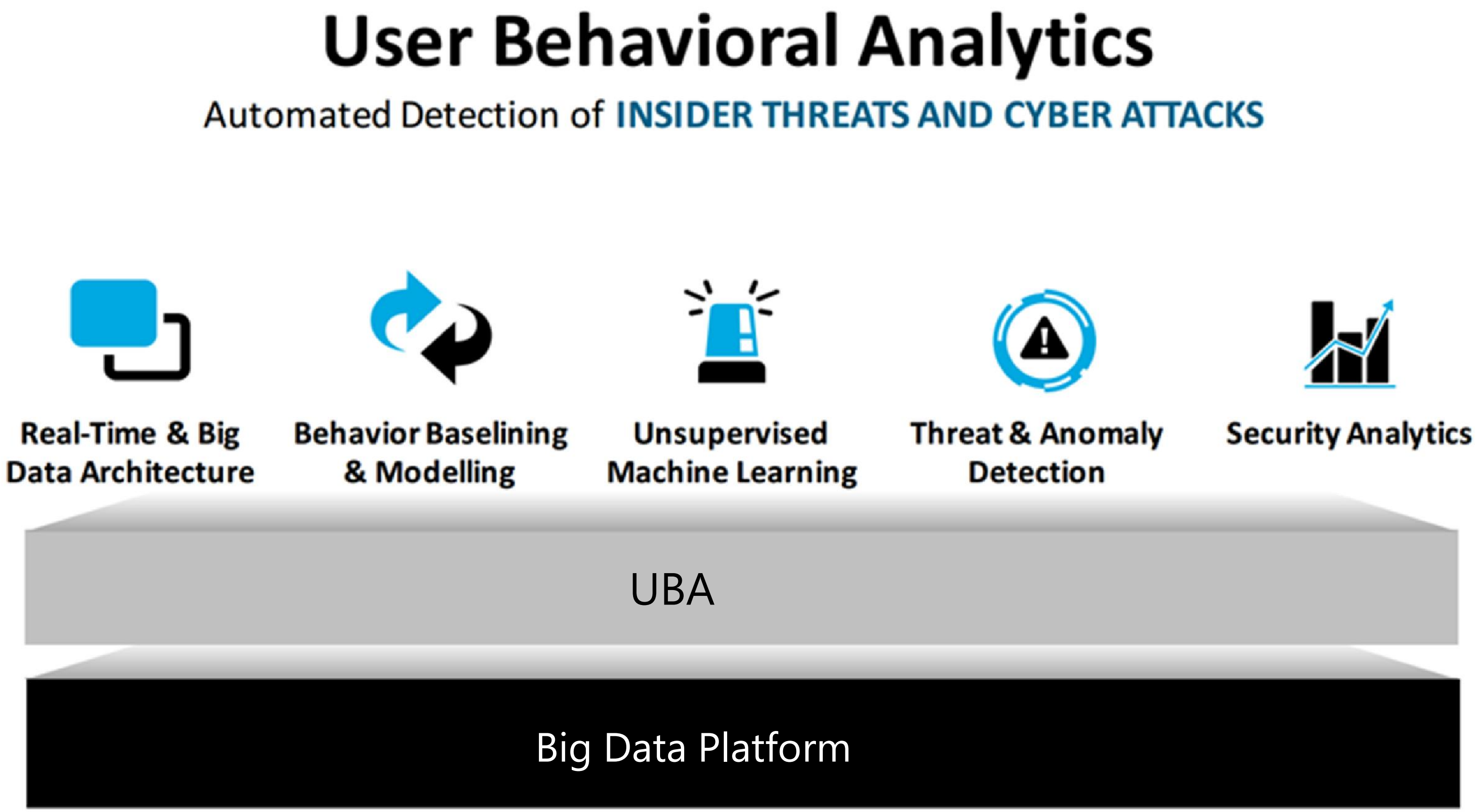
Signature
REModelFWSourceTargetZone

Users
Fred Samuels

DETECT **MALICIOUS INSIDER THREATS**

DETECT **ADVANCED CYBERATTACKS**

User Behavior Analytics - APT & Insider Threat



User Behavioral Analytics

Automated Detection of **INSIDER THREATS AND CYBER ATTACKS**

Real-Time & Big Data Architecture

Behavior Baselining & Modelling

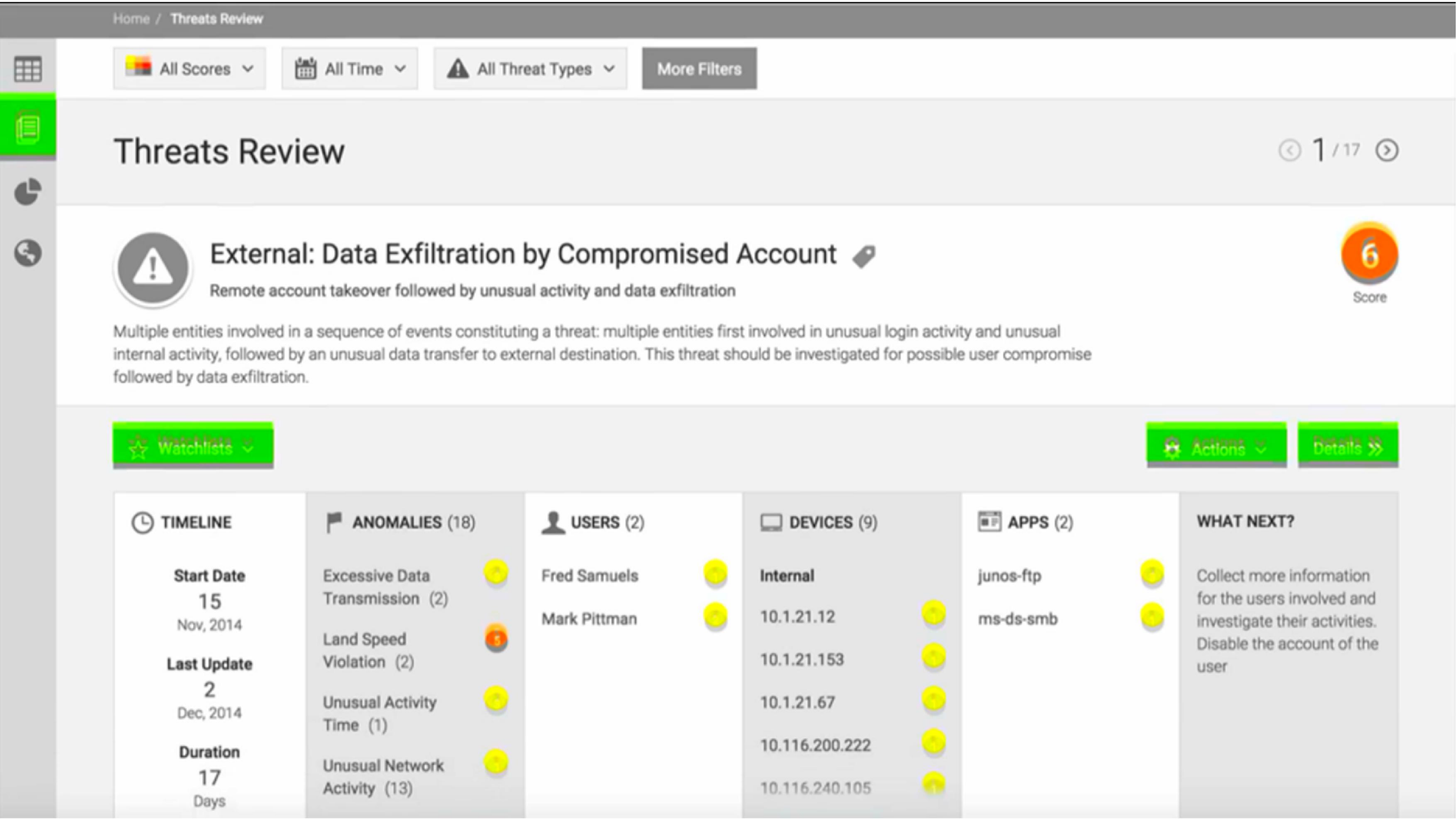
Unsupervised Machine Learning

Threat & Anomaly Detection

Security Analytics

UBA

Big Data Platform



Threats Review

1 / 17

External: Data Exfiltration by Compromised Account

Remote account takeover followed by unusual activity and data exfiltration

6
Score

Multiple entities involved in a sequence of events constituting a threat: multiple entities first involved in unusual login activity and unusual internal activity, followed by an unusual data transfer to external destination. This threat should be investigated for possible user compromise followed by data exfiltration.

TIMELINE

Start Date
15
Nov, 2014

Last Update
2
Dec, 2014

Duration
17
Days

ANOMALIES (18)

- Excessive Data Transmission (2)
- Land Speed Violation (2)
- Unusual Activity Time (1)
- Unusual Network Activity (13)

USERS (2)

- Fred Samuels
- Mark Pittman

DEVICES (9)

Internal

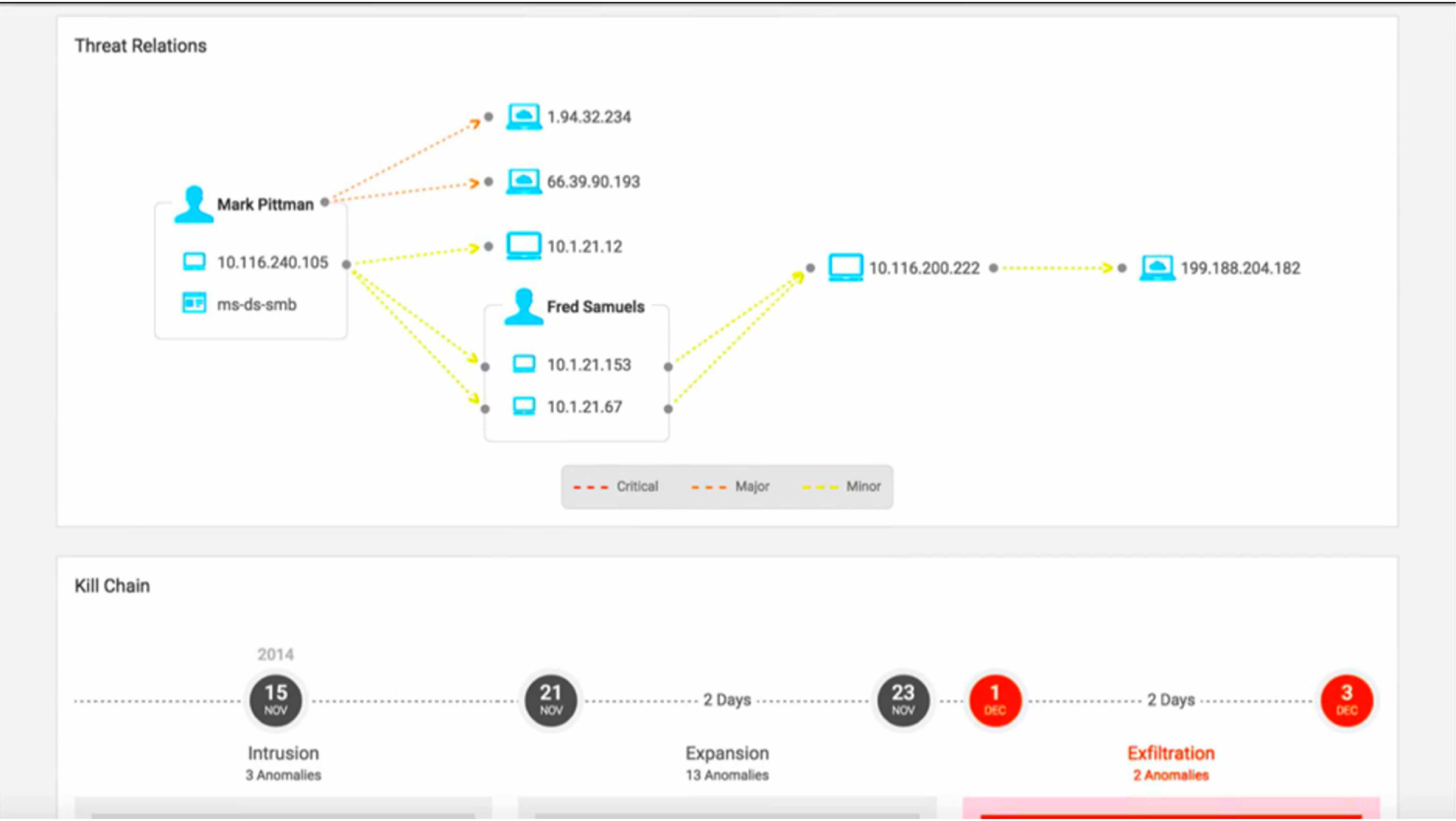
- 10.1.21.12
- 10.1.21.153
- 10.1.21.67
- 10.116.200.222
- 10.116.240.105

APPS (2)

- junos-ftp
- ms-ds-smb

WHAT NEXT?

Collect more information for the users involved and investigate their activities. Disable the account of the user



Threat Relations

Mark Pittman

10.116.240.105

ms-ds-smb

1.94.32.234

66.39.90.193

10.1.21.12

Fred Samuels

10.1.21.153

10.1.21.67

10.116.200.222

199.188.204.182

- - - Critical - - - Major - - - Minor

Kill Chain

2014

15 NOV

21 NOV

2 Days

23 NOV

1 DEC

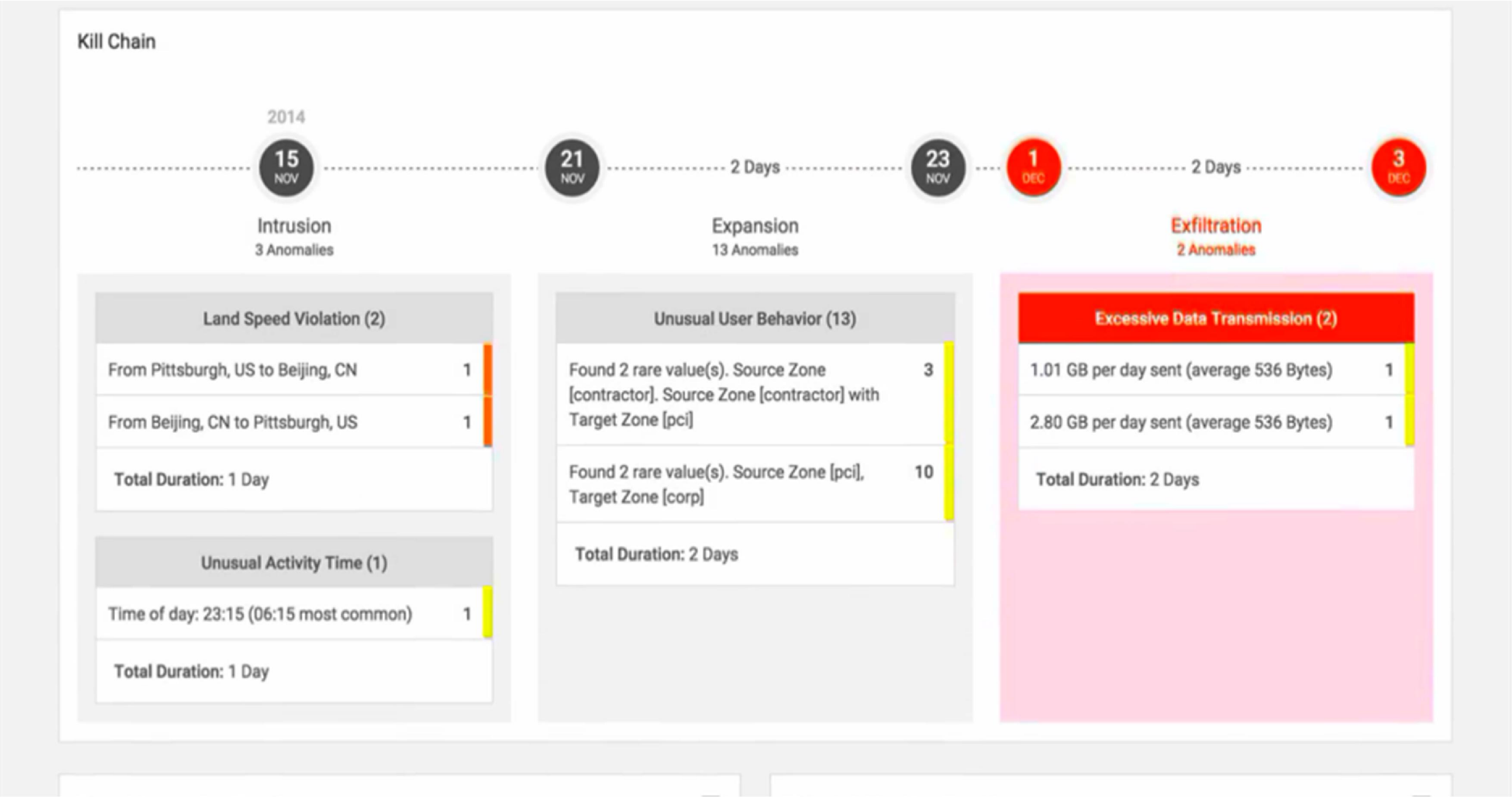
2 Days

3 DEC

Intrusion
3 Anomalies

Expansion
13 Anomalies

Exfiltration
2 Anomalies



Kill Chain

Intrusion
3 Anomalies

Land Speed Violation (2)	
From Pittsburgh, US to Beijing, CN	1
From Beijing, CN to Pittsburgh, US	1
Total Duration: 1 Day	

Unusual Activity Time (1)	
Time of day: 23:15 (06:15 most common)	1
Total Duration: 1 Day	

Expansion
13 Anomalies

Unusual User Behavior (13)	
Found 2 rare value(s). Source Zone [contractor]. Source Zone [contractor] with Target Zone [pci]	3
Found 2 rare value(s). Source Zone [pci], Target Zone [corp]	10
Total Duration: 2 Days	

Exfiltration
2 Anomalies

Excessive Data Transmission (2)	
1.01 GB per day sent (average 536 Bytes)	1
2.80 GB per day sent (average 536 Bytes)	1
Total Duration: 2 Days	

Leading Telcos Drive Results with Big Data Platform

at&t	**Troubleshoot and monitor** Apple iPhone network services across four load balanced data centers.
vodafone	Vodafone has **reduced support escalations by 90%** and time to **resolve services issues by 67%.**
Telstra	Troubleshoot service delivery problems with video content delivered to mobile devices as part 3G offerings.
T · ·Mobile·	**Meet PCI requirements** by tracking and monitoring access to network resources / cardholder data
SaskTel	**Mitigated fraud** by using combination Firewall IDP logs and cross referencing to subscriber IP Addresses.
telenor	Proactively manage operations and **respond before an outage occurs or service erodes**
metroPCS	**Increased margins** by gaining insight into Call Detail Records (CDRs) and partner tariff databases.

VNISA

VIETNAM INFORMATION SECURITY ASSOCIATION

Thank you

Nguyen Thanh Dat

Datnt@vncs.vn / 0924298686

Viet Nam Cyberspace Security Technology

https://vncs.vn