



splunk>

Creating Privacy Auditing and Controlled Substance Diversions Platforms for Healthcare

Jennings Aske | SVP, CISO, NewYork–Presbyterian

John Frushour | Deputy CISO, NewYork–Presbyterian

Shirley Golen | Global Healthcare Industry Marketing, Splunk

Gleb Esman | Senior Product Manager, Fraud Analytics and Research, Splunk



Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2018 Splunk Inc. All rights reserved.

Today's Session Agenda

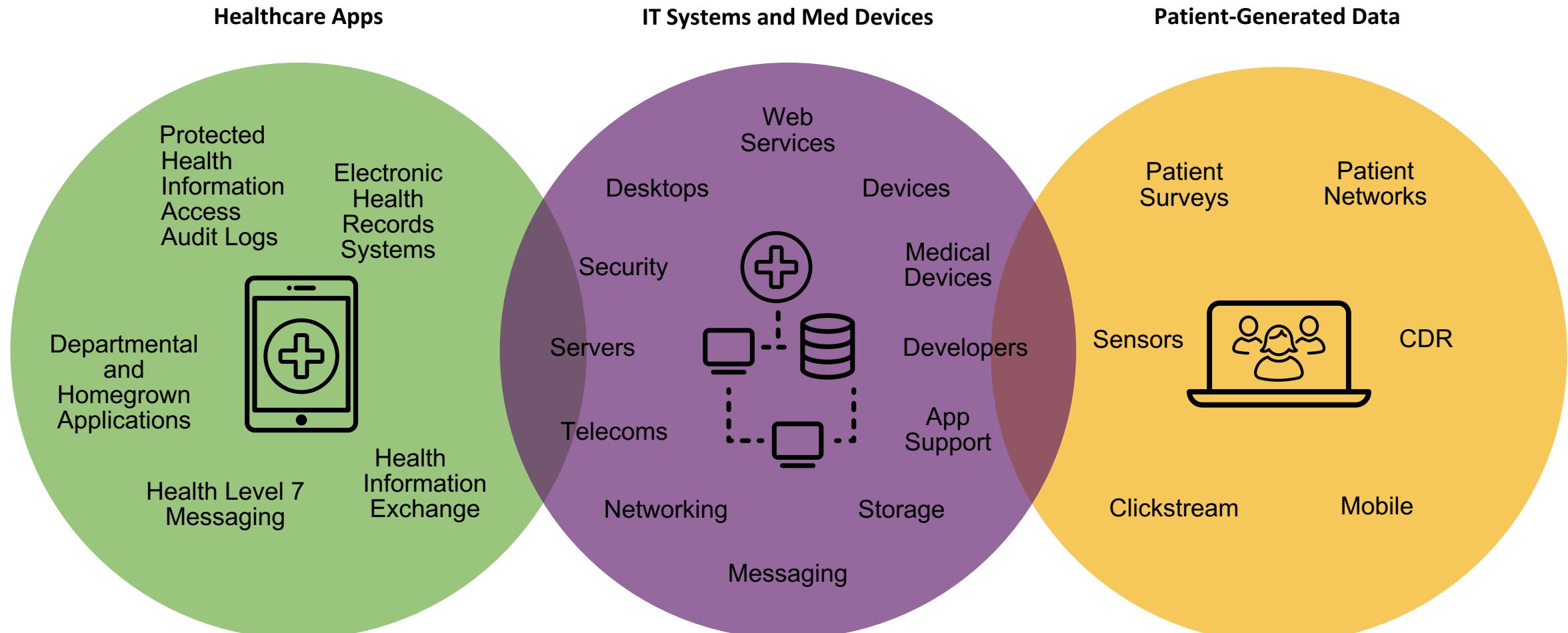
- ▶ Shirley Golen
 - Splunk and Healthcare
 - ▶ Gleb Esman
 - Project Background
 - ▶ Jennings Aske and John Frushour
 - Information Security and IT Operations
 - Patient Privacy
 - Pharmacy/Opioid Diversion
 - ▶ Q&A

► Q&A

Splunk and Healthcare

One Platform, Multiple Use Cases in Healthcare

Healthcare Data is Time-Oriented and Diverse...



One Platform, Multiple Use Cases in Healthcare

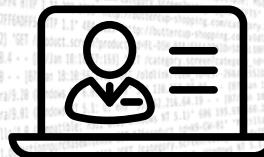
Healthcare Sources



Core IT



Patient-Facing Data



Providing Better Patient Outcomes

Lowering Costs

Cybersecurity Protection

Protecting Privacy of Patient Health Information

Controlled Substance Diversion

Detecting Fraud

Privacy Platform Collaboration

Background



Challenges with Existing Off-the-shelf Privacy Systems

► Scalability and Performance

- Legacy designs involves complex, poorly documented, mixed architectures

► Rigid and Inflexible

- Hardcoded to specific data formats
 - Hardcoded to specific interfaces, limited APIs

► Lack of control

- Hard to modify and customize without vendor
 - Requires vendor-driven, expensive and prolonged consulting engagements
 - Often “black box” with unwillingness by vendor to cooperate with others

► Crippling, add-on costs

- Vendor-enforced fees to maintain system is working order and upgrade

General Requirements for Privacy Platform

- ▶ Scalability
- ▶ Extensible, customizable solution
- ▶ Support for many privacy use cases
- ▶ Support for large number of diversified, poorly documented, poorly structured, possibly mis formatted data sources coming in large quantities in possibly erratic manner from large number of different healthcare applications, systems and possibly unstable data sources and activity logs.
- ▶ Have system capable of normalizing, analyzing and detecting thousands of anomalies, instances of violations and suspicious activity events over critical patient and healthcare data.

Splunk Healthcare Privacy Platform

Full Data Visibility

- **Data Flow** (consistency, stability)
 - **EHR Records** (normalized and raw views)
 - **Activity** (EHR access stats across all entities)
 - **Anomalies** (ML and detection)



Incident Management

- **Alerts** (Categories, Tags, Status, Comments)
 - **Filtering**
 - **Workflow**



Business Use Cases

- Privacy Monitoring
(EHR access)
 - Medications Access
(Pharmacy, Access, Diversion, Opioids abuse)
 - Security
(Logins, IDs, System access)



Investigations

- Dashboards
 - Visualizations
 - Drilldowns
 - Reports



Creating Privacy Auditing and Controlled Substance Diversion Platforms for Healthcare



NYP and Splunk

Information Security and IT Operations

Patient Privacy

Pharmacy/Opioid Diversion

NYP and Splunk

Information Security and IT Operations

St. Anthony's Hospital Fire



St. Anthony's Hospital Fire



Health care 'disproportionately affected' by data security incidents

Written by **Colin Marrs** on 2 June 2017 in **News**

Information Commissioner's Office shows sharp increase in data breach incidents in central government and courts sectors.



ICO releases four years' worth of data on security breaches - Photo credit: Tobias Felber/DPA/Press Association Images

Healthcare's Attack Surface

- ▶ Healthcare is 1/6 the US's GDP
- ▶ 900K physicians, 2.8 million nurses and administrative staff
- ▶ 230K physician practices
- ▶ 5700 hospitals
- ▶ What else?
 - skilled nursing facilities, pharmacies, ambulatory surgery centers...
- ▶ And more to come:
 - 165K mobile healthcare apps, telehealth, “smart” consumer devices...

BUSINESS

Cyberattack Forces West Virginia Hospital to Scrap Computers

Petya attack forces Princeton Community Hospital to use paper records as it scraps, rebuilds computer network



A cyberattack on Princeton Community Hospital's computer network in West Virginia made officials decide to replace it. Staff are using paper forms until a new system is installed. PHOTO: MATT MCCLAIN/THE WASHINGTON POST/GETTY IMAGES

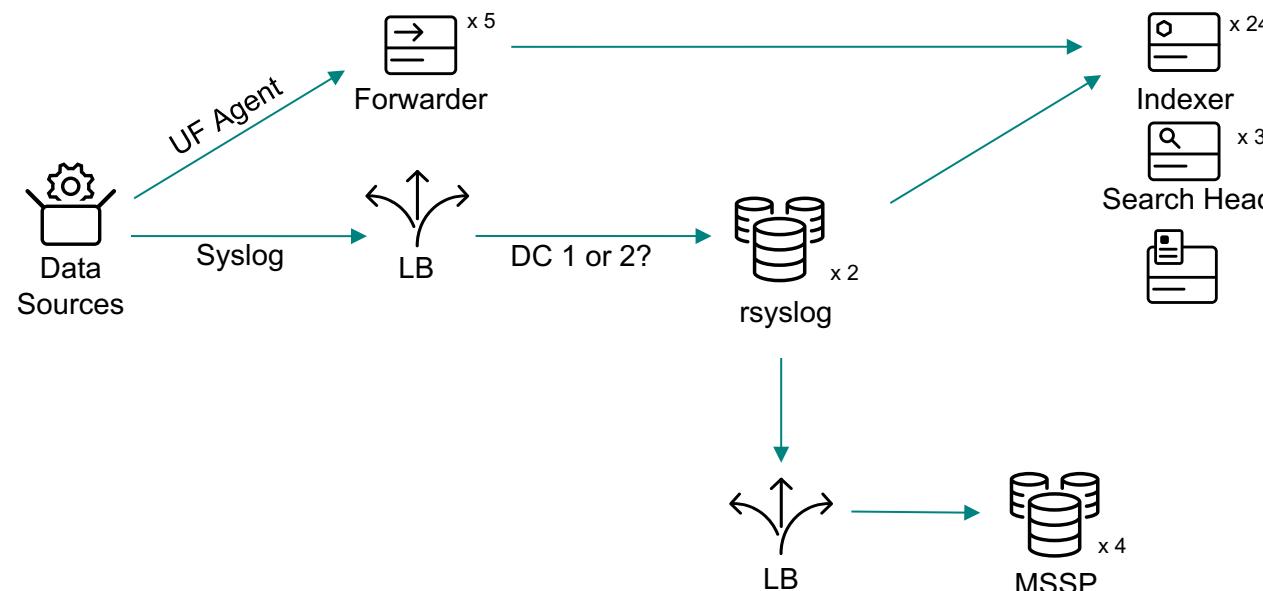
Source: WSJ.com

The Visibility Problem

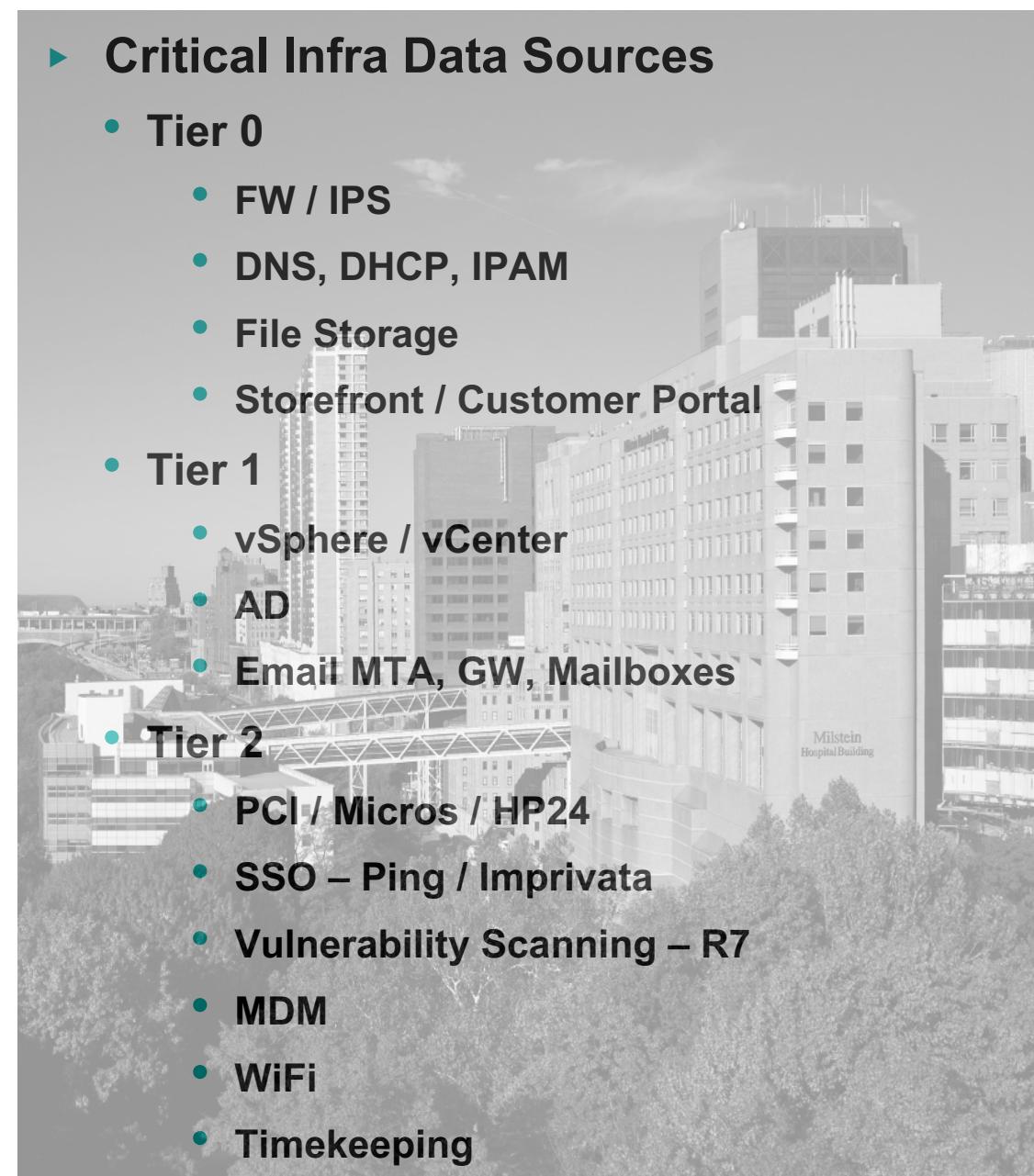


NYP-Splunk Architecture

- ▶ Active-Active, multi DC
 - Load balanced ingress for MSSP cloning
 - Spatial Locality



- ▶ Critical Infra Data Sources
 - Tier 0
 - FW / IPS
 - DNS, DHCP, IPAM
 - File Storage
 - Storefront / Customer Portal
 - Tier 1
 - vSphere / vCenter
 - AD
 - Email MTA, GW, Mailboxes
 - Tier 2
 - PCI / Micros / HP24
 - SSO – Ping / Imprivata
 - Vulnerability Scanning – R7
 - MDM
 - WiFi
 - Timekeeping



NYP and Splunk

Patient Privacy

Your health records are supposed to be private. They aren't.

The federal law that protects health information is violated often and easily, and it's hardly ever enforced.

Charles Ornstein • December 30, 2015



NY Consortium – Privacy Project

- ▶ NY Consortium
 - Columbia University Irving Medical Center
 - Weill Cornell Medicine
 - NewYork-Presbyterian
- ▶ Project Goal – Implement a scalable, extensible solution for Privacy Officer operations in the areas of:
 - Auditing,
 - Monitoring; and
 - Investigations.
- ▶ Increase efficiency of current privacy workflows:
 - Reduce false positive alerts, and facilitate workflows; and
 - Provide a solution that a non-technical privacy analyst could leverage for investigations.

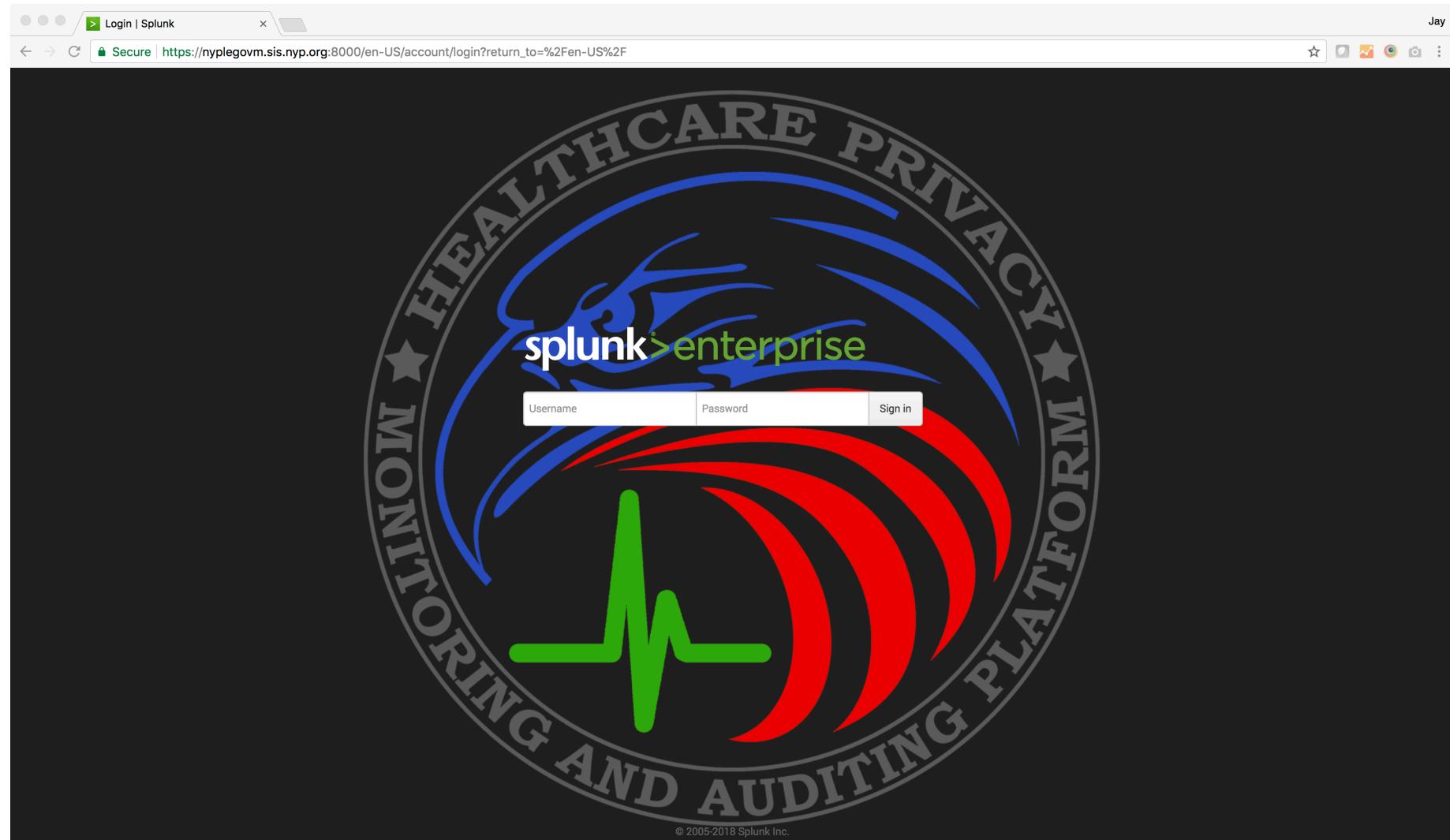
Privacy Use Cases

1. Higher than user normal
2. Excessive Hours with Activity
3. Access outside of work hours
4. Excessive Demographics Access
5. Access to VIP
6. All accesses by user over a specified time
7. Accesses by all users to a given MRN
8. Break the Glass
9. Employee Access to Employee Patient Records
10. Deceased Patient Access
11. Deceased Patient Demographic Access
12. Failed login attempts alert
13. Employee Patient Access
14. Compare Usage among Peers
15. Failed login attempts report
16. Mismatched user login
17. Access from off campus
18. Access from off campus outside of work hours
19. Access to consecutive MRNs
20. Access by inactive user
21. User over time statistics

Evaluation Process

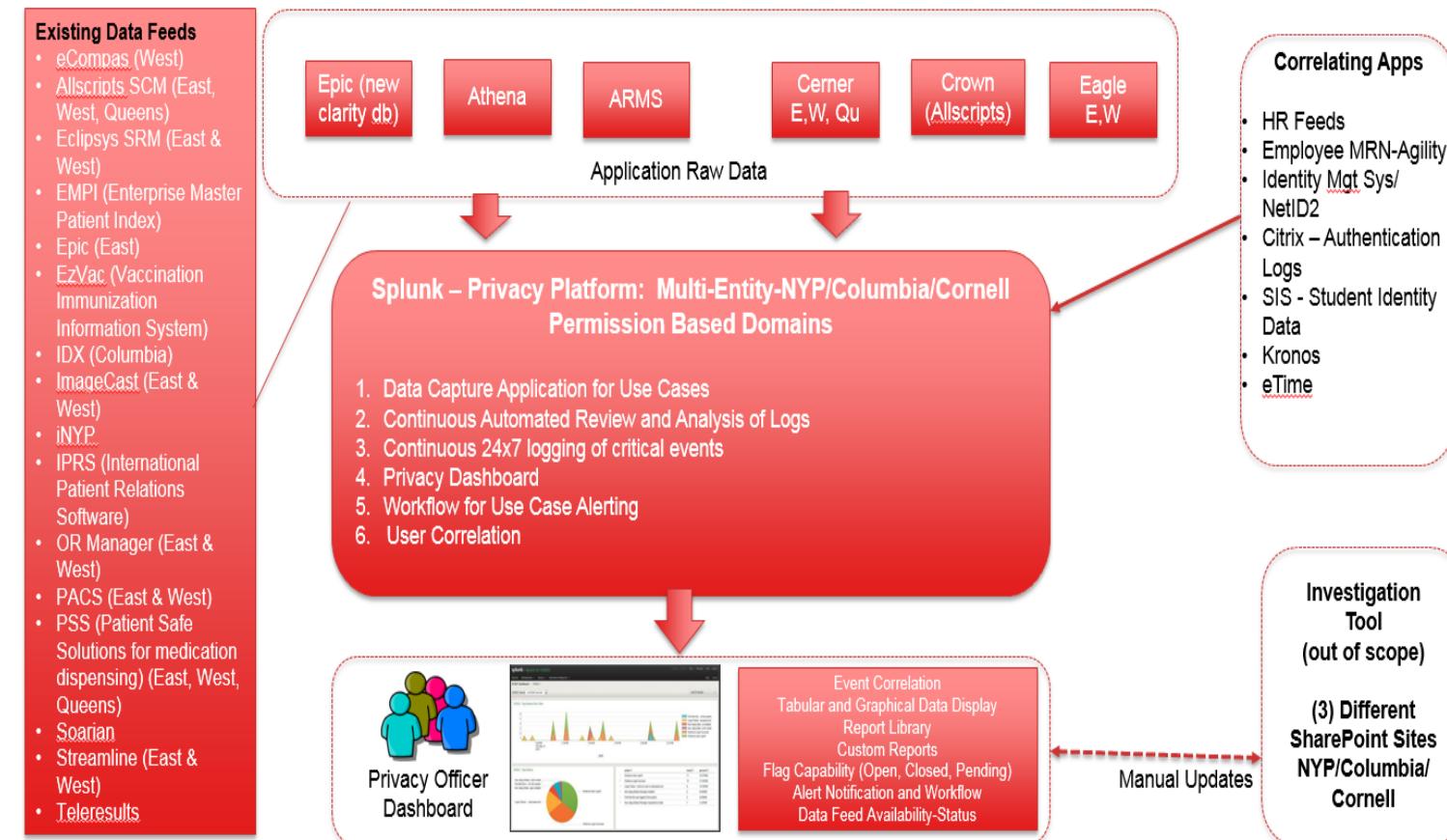
- ▶ Commercial off the Shelf (COTS) vs. Build
 - COTS products reviewed:
 - Fairwarning, Protenus, Cognetyx, Maize Analytics
 - Concerns about scalability, poor data enrichment, missing use cases
 - Splunk:
 - Scalable machine data aggregation
 - Currently used by Weill Cornell and NYP InfoSec teams for security analytics
 - Correlation, artificial intelligence and machine learning capabilities superior to COTS products
- ▶ The NYP Consortium chose to build with Splunk

Healthcare Privacy Monitoring and Auditing Platform



Healthcare Privacy Monitoring and Auditing Platform

Privacy Platform Functional Map



Healthcare Privacy Monitoring and Auditing Platform

Reports & Investigations

Search Identity Management System records
Search and list all available personnel records

All accesses by specific user
Investigate all accesses by a specific user over time

Compare usage among peers
Compare usage among peers of the same department and title

Access of specific MRN
Find all users who accessed specific MRN

Department Activity Analysis
Analyze combined activity within specific department or all departments combined

User Activity Analysis
Analyze Activity of a specific user or provider

MRN/Patient ID Access Analysis
Analyze access to specific MRN/Patient ID

The screenshot displays a web-based application interface for healthcare privacy monitoring. On the left, a sidebar menu includes 'About', 'Data Flow Monitor', 'Reports & Investigations' (which is currently selected), and 'Suspicious & Abnormal Activity'. The main content area is titled 'Reports & Investigations' and contains several sections with corresponding dashboards and numerical data points:

- Search Identity Management System records:** Shows a grid of personnel records with a count of 370.
- All accesses by specific user:** Shows a timeline of activity with counts 1.6 and 1.20.
- Compare usage among peers:** Shows a bar chart with a count of 1.14.
- Access of specific MRN:** Shows a bar chart with a count of 64.
- Department Activity Analysis:** Shows a bar chart for Pediatrics with a total count of 170,336.
- User Activity Analysis:** Shows a bar chart with a count of 1.7.
- MRN/Patient ID Access Analysis:** Shows a bar chart with a count of 1.7.

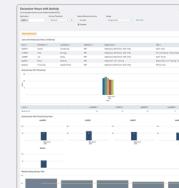
Healthcare Privacy Monitoring and Auditing Platform

Suspicious & Abnormal Activity

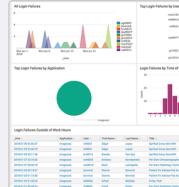
Higher than user normal
Higher than normal MRN access
1.1



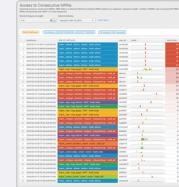
Excessive hours with activity
Hours exceed normal course of daily activity
1.2



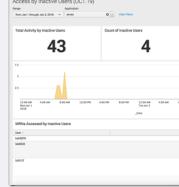
Failed login attempts
Find and analyze all failed login attempts within specific timeframe
1.12



Access to consecutive MRN's
Access to consecutive MRN's
1.17



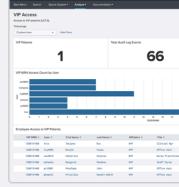
Access by inactive users
Detect accesses by users who are marked as inactive within central user database
1.19



Employee MRN Access
Employee access to employee patient records
1.9



VIP Access
Access to VIP patients
1.5



The screenshot displays a web-based interface for monitoring healthcare privacy. The top navigation bar shows the URL nyplegovm.sis.nyp.org:8000/en-US/app/hc-privacy-monitor/start_menu. The left sidebar menu includes links for About, Data Flow Monitor, Reports & Investigations, Suspicious & Abnormal Activity (which is currently selected), and Suspicious & Abnormal Activity. The main content area is titled "Suspicious & Abnormal Activity" and lists seven categories of monitoring: "Higher than user normal", "Excessive hours with activity", "Failed login attempts", "Access to consecutive MRN's", "Access by inactive users", "Employee MRN Access", and "VIP Access". Each category has a corresponding dashboard thumbnail and a numbered callout box (e.g., 1.1, 1.2, 1.5, 1.9, 1.12, 1.17, 1.19) indicating its specific function or identifier.

MRN Access

MRN Access (UC1.7) | Splunk

Secure | https://nylegovm.sis.nyp.org:8000/en-US/app/hc-privacy-monitor/mrn_access?patient_id=3154399&form.timerange.earliest=1514782800&form.timerange.latest=1517461200&form.sourcetype=allscript... Jay

splunk> App: Healthcare Privacy Monitor

Start Menu Search Splunk System ▾ Analyze ▾ Documentation ▾ Jay Benfield ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

MRN Access (UC1.7)

Range Application Action Top MRNs MRN Search

during Jan 2018 Any Any 3154399 3154399 Hide Filters

Edit Export ...

MRN Activity

95
logged interactions with 3154399

MRN Activity by Time of Day

Time (Hour)	Actions
8	2
11	3
12	5
14	4
15	28
16	7
18	3
19	14
20	11
21	18

MRN Most Active User

rii9005
is the most active user on 3154399

MRN Actions by User

Action	Int105	bec9054	brg7003	brs9117	rii9005	stm9065
create	0	0	0	0	12	4
update	0	0	0	0	10	1
view	0	0	0	0	15	1

MRN Activity Over Time

Date/Time	Create	Update	View
Mon Jan 1 2018	3	18	0
Mon Jan 8 2018	1	0	0
Mon Jan 15 2018	0	0	3
Mon Jan 22 2018	5	0	5
Mon Jan 29 2018	0	2	3

MRN Activity Detail

_time	User	Application	MRN	Raw Event Action
2018-01-31 11:39:50	Int105	imagecast	3154399	Edited
2018-01-29 12:57:39	rii9005	ecompas	3154399	Viewed
2018-01-29 12:57:38	rii9005	ecompas	3154399	Viewed
2018-01-29 12:43:14	rii9005	ecompas	3154399	Viewed
2018-01-29 12:43:13	rii9005	ecompas	3154399	Viewed
2018-01-29 12:43:11	rii9005	ecompas	3154399	Viewed

MRN Activity Detail Outside of Work Hours

_time	User	Application	MRN	Raw Event Action
2018-01-26 21:15:04	rii9005	ecompas	3154399	Viewed
2018-01-26 21:15:04	rii9005	ecompas	3154399	Edited
2018-01-26 21:11:05	rii9005	ecompas	3154399	Added
2018-01-26 21:09:59	rii9005	ecompas	3154399	Viewed
2018-01-26 21:09:59	rii9005	ecompas	3154399	Edited

User Access

User Access (UC1.6, UC1.20)

Range: during Jan 2018 | Application: Any | Action: Any | Top Users: rii9005 | Search for User: rii9005 | Hide Filters

rii9005 User Information

First Name	Last Name	Affiliation	Department	Title
Riselly	Imbert	NYP	CHP-HIV Medical Case Mgt Grant	Health Educator

Total User Activity: **370** logged interactions by rii9005

User Activity by Time of Day

Time (Hour)	Actions (count)
9	16
11	16
12	32
13	32
14	48
15	48
18	16
19	16
20	16
21	32

Most Frequently Accessed MRN: **3409439** is the most frequently accessed MRN by rii9005

Actions by MRN

Action	MRN	Count
create	3154399	84
create	3409439	63
create	3773663	42
create	4151251	21
update	5882247	105
view	6624435	126
view	7652200	147
view	7787750	168
view	3154399	189
view	3409439	210

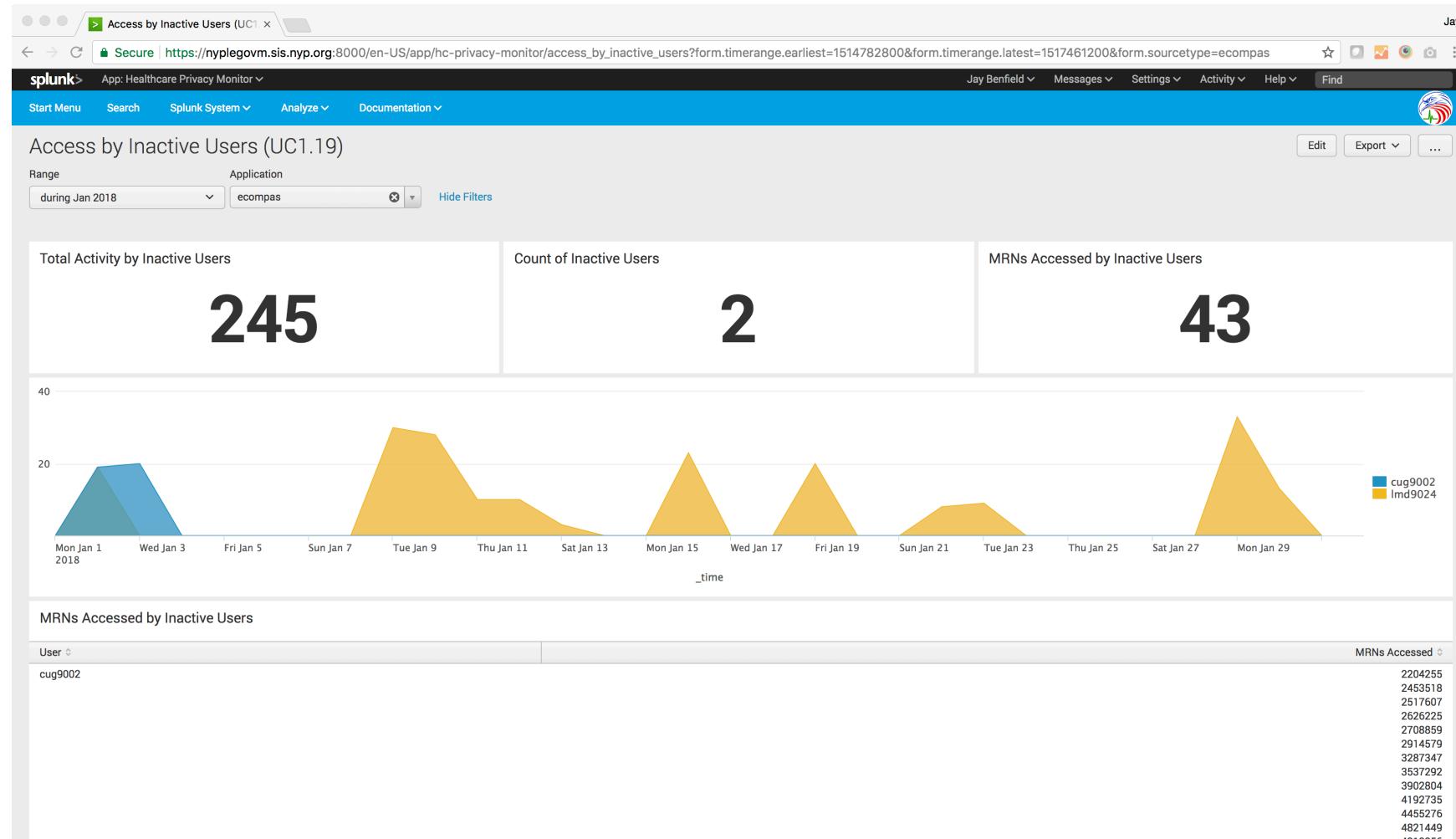
Actions by Application

Action	Application	Count
create	ecompas	~100
update	ecompas	~80
view	ecompas	~120

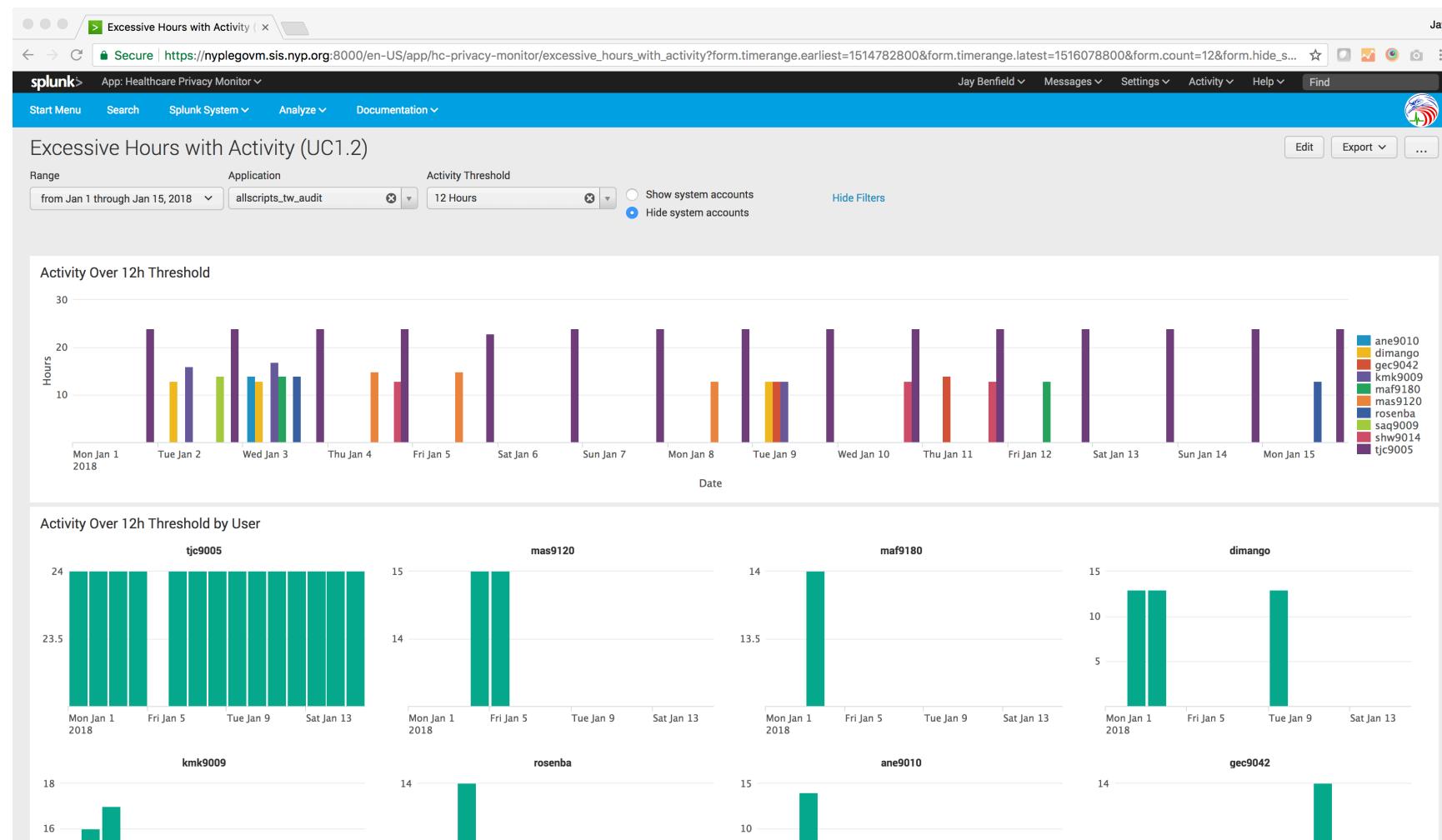
Actions Over Time

Application Activity Over Time

Access by Inactive Users



Excessive Hours with Activity



Failed Login Attempts

Splunk App: Healthcare Privacy Monitor

Range: during Jan 2018 | Application: imagecast | Login Failure Threshold: 3

Failed Login Attempts (UC1.12)

Login Failures by Application Over Threshold

Application	User	First Name	Last Name	Title	Affiliation	Department	Login Failure Count
imagecast	mar9167	Marivel	Assad	Sr Account Administrator	Cornell	Rad-Chairman	4
imagecast	matosdi	Diana	Matos-Soto	Patient Fin Advisor-Pat Access	NYP	Patient Access Services	4
imagecast	dad9077	Darly	Delva	X-Ray Tech	NYP	Diagnostic Xray	3
imagecast	jam2014	Janet	Melendez	Medical Records Assistant	Cornell		3
imagecast	rad2011	Raquel	Dowling	Medical Records Clerk	Cornell	Radiology	3
imagecast	gin7002	Gissille	Nimphius	Secretary	ServCorp	CD / NYP Imaging	3
imagecast	lic9034	Lisa	Gandolfo	Assistant Attending	PHPA	Radiology	3

All Login Failures

Top Login Failures by User

Top Login Failures by Application

Login Failures by Time of Day

NYP and Splunk

Pharmacy/Opioid Diversion

The American Epidemic

Bleak New Estimates in Drug Epidemic: A Record 72,000 Overdose Deaths in 2017

Fentanyl is a big culprit, but there are also encouraging signs from states that have prioritized public health campaigns and addiction treatment.

Aug. 15, 2018

Drug overdoses killed about 72,000 Americans last year, a record number that reflects a rise of around 10 percent, according to new preliminary [estimates](#) from the Centers for Disease Control. The death toll is higher than the peak yearly death totals from [H.I.V.](#), car crashes or gun deaths.

Using Splunk to Identify Diversion

- ▶ Splunk will ingest logs from several source systems to identify potential diversion. Correlation and machine learning will allow Splunk to learn and predict anomalous behavior indicating potential diversion.
- ▶ Current NYP sources:
 - Allscripts electronic health record
 - EMPI
 - Electronic Prescription of Controlled Substances (EPCS)
 - Kronos timekeeping
 - Omnicell pharmacy dispensing system
 - Workday

Using Splunk to Identify Diversion

- ▶ Splunk will ingest logs from several source systems to identify potential diversion. Correlation and machine learning will allow Splunk to learn and predict anomalous behavior indicating potential diversion.
- ▶ Current NYP sources:
 - Allscripts electronic health record
 - EMPI
 - Electronic Prescription of Controlled Substances (EPCS)
 - Kronos timekeeping
 - Omnicell pharmacy dispensing system
 - Workday

Pharmacy Diversion Use Cases

1. Medications removed by any user not working that day.
2. Users who remove medications from pharmacy cabinet without documentation of administration in EMR.
3. User return of medication in pharmacy cabinet within one hour – doing this more than others.
4. Doctors who prescribe controlled substances for patients they have never seen (outpatient).
5. User who removes medication from pharmacy cabinet for a patient who is discharged who does this more than peers.
6. User who removes opioid medications from pharmacy cabinet for a patient with no pain score - doing this more than others.
7. User prescribes for patient in “wrong” clinical unit

Pharmacy Diversion Use Cases

7. Monitor quantity of dispensed medication for controlled substances - users exceeding peers.
8. Pharmacy cabinet frequency of access - comparison against self, against peers.
9. Prescriptions for coworkers.
10. Patient seen in one facility and prescription filled in another, with geography scatter map.
11. Opioid clinical guidelines (e.g., initial, detox - exceeding, comparison against peers).
12. User pattern anomalies using machine learning.
13. Diversion of expensive, non-controlled substances



Building a \$60 Billion Data Model to Stop US Healthcare Fraud (Part 1)



At Splunk, we look at big problems as data challenges; solutions are always data-driven. The patterns of [fraud](#) are always hidden within the data—no matter how sophisticated fraudsters are in how they abuse the system and stay under the radar. Solutions to all problems big and small start with gathering data and seeing the big picture through the data analytics lens.

With modern US Healthcare programs' complexity and sophistication, fraud losses in healthcare cost US taxpayers a staggering number approaching one



Using Splunk to Identify Diversion

► Privacy Monitoring and Auditing

- Build-out of production environment, initial deployment schedule
- “Epic use cases”

► Pharmacy Diversion

- Finalize initial use cases and requirements documentation;
- Development environment build-out, and project planning.

Q&A

Thank You

Don't forget to rate this session
in the .conf18 mobile app

