
# Creating Privacy Auditing and Controlled Substance Diversion Platforms for Healthcare

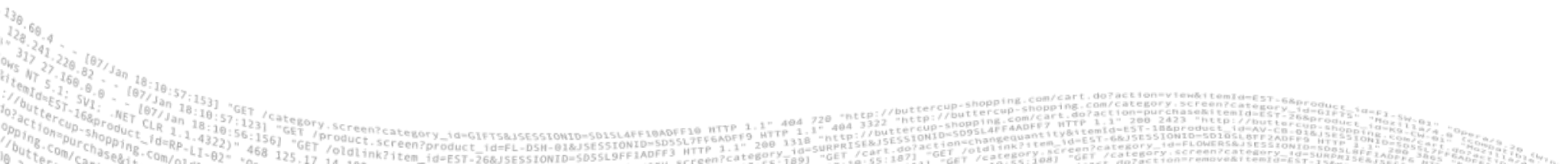
Jennings Aske | SVP, CISO, NewYork–Presbyterian
John Frushour | Deputy CISO, NewYork–Presbyterian
Shirley Golen | Global Healthcare Industry Marketing, Splunk
Gleb Esman | Senior Product Manager, Fraud Analytics and Research, Splunk

# 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.





# Today's Session Agenda

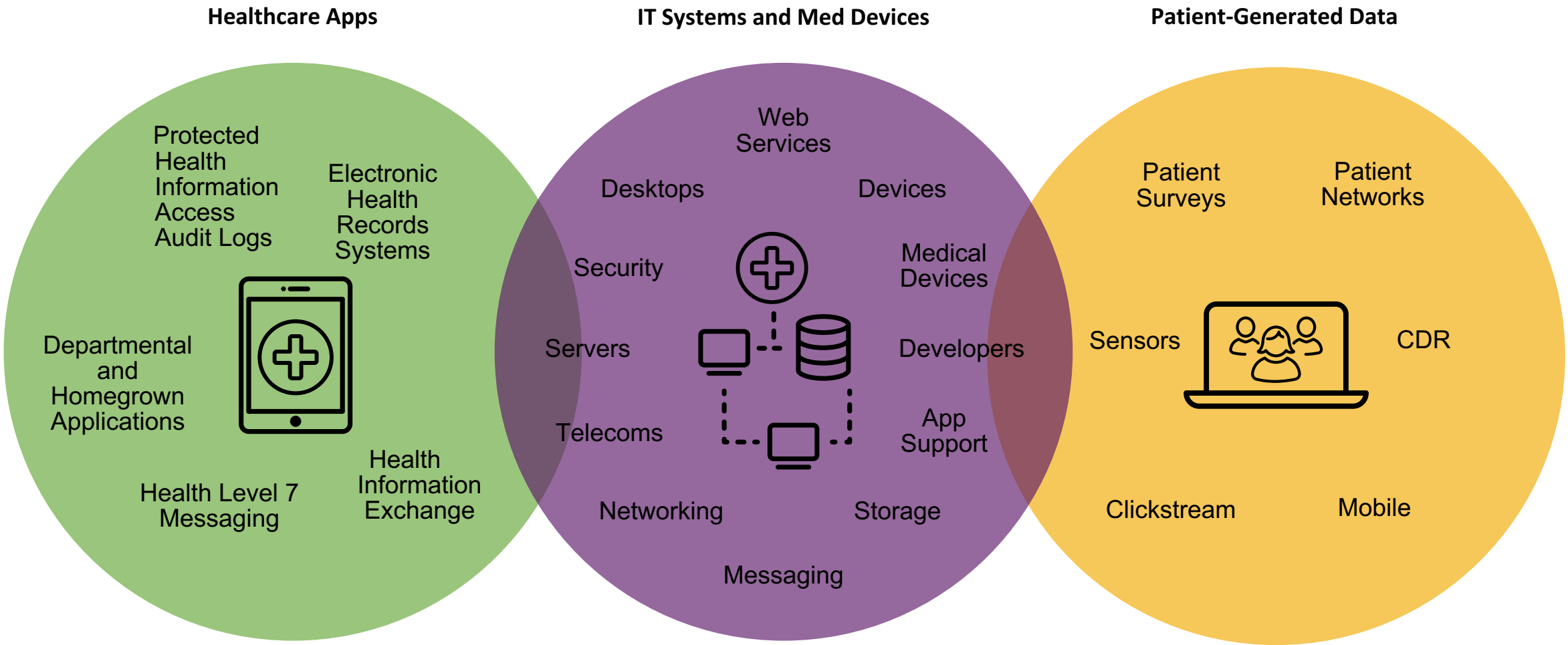
- Shirley Golen
  - Splunk and Healthcare
- Gleb Esman
  - Project Background
- Jennings Aske and John Frushour
  - Information Security and IT Operations
  - Patient Privacy
  - Pharmacy/Opioid Diversion
- Q&A

# Splunk and Healthcare

## One Platform, Multiple Use Cases in Healthcare

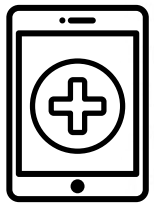
splunk> .conf18

# Healthcare Data is Time-Oriented and Diverse…

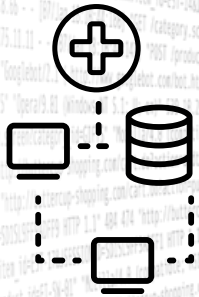


# One Platform, Multiple Use Cases in Healthcare

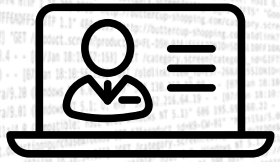
**Healthcare Sources**



**Core IT**



**Patient-Facing Data**



splunk>

- Providing Better Patient Outcomes
- Lowering Costs
- Cybersecurity Protection
- Protecting Privacy of Patient Health Information
- Controlled Substance Diversion
- Detecting Fraud

# Privacy Platform Collaboration

## Background

splunk> .conf18

# 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)

## Business Use Cases

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


## Incident Management

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

## Investigations

- Dashboards
- Visualizations
- Drilldowns
- Reports

splunk> .conf18

# Creating Privacy Auditing and Controlled Substance Diversion Platforms for Healthcare

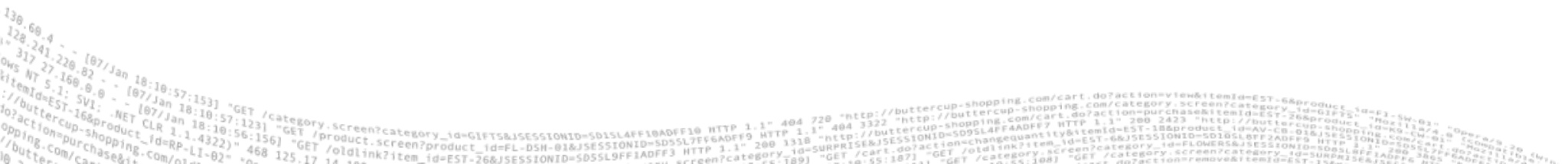
splunk> .conf18

# NYP and Splunk

**Information Security**
**and**
**IT Operations**

**Patient Privacy**

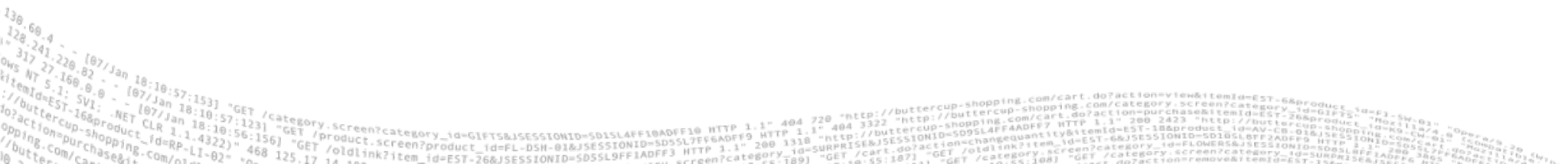
**Pharmacy/Opioid Diversion**



splunk> .conf18

# NYP and Splunk

**Information Security**
**and**
**IT Operations**



splunk> .conf18

# St. Anthony's Hospital Fire

# St. Anthony's Hospital Fire

# Health care 'disproportionately affected' by data security incidents

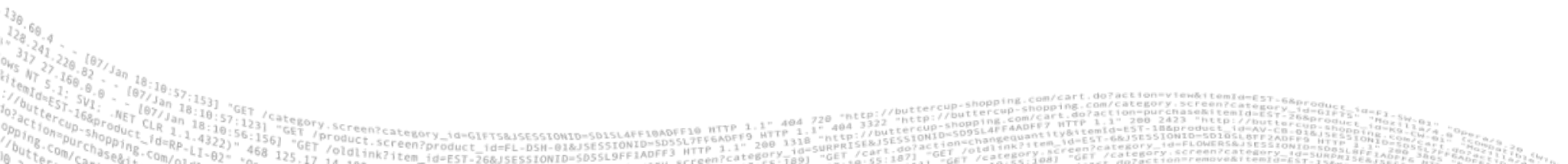
Written by **Colin Marrs** on 2 June 2017 in **News**

**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

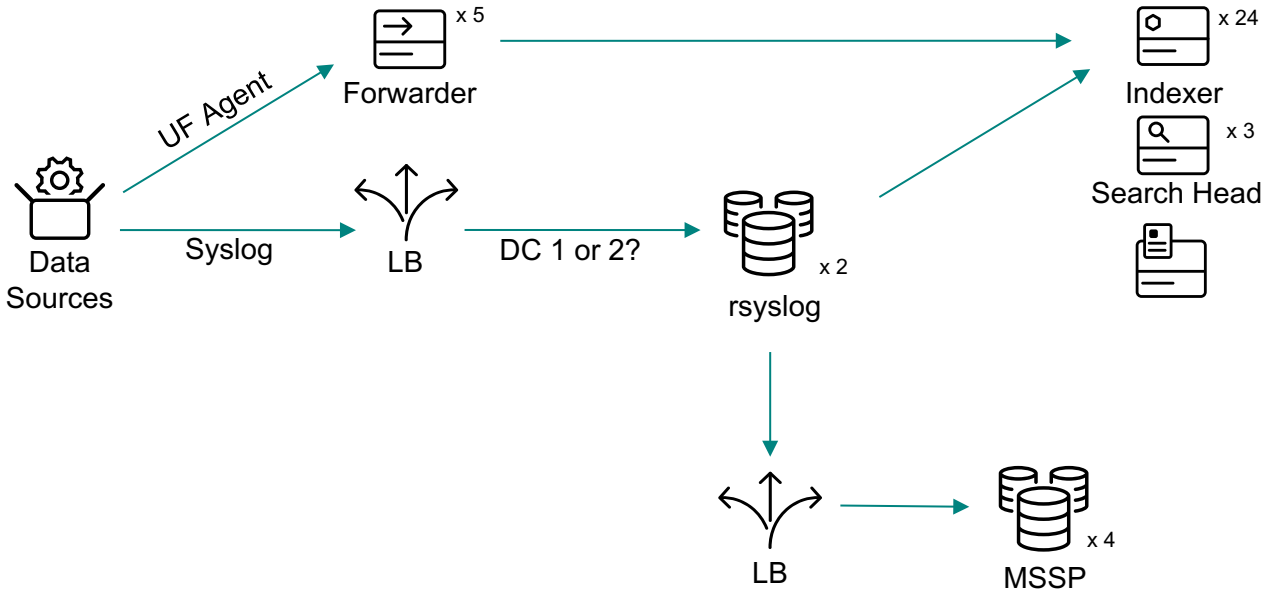
# The Visibility Problem






# NYP-Splunk Architecture

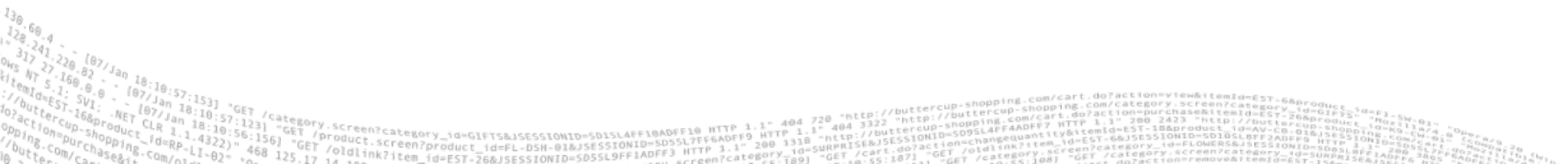
- Active-Active, multi DC
  - Load balanced ingress for MSSP cloning
  - Spatial Locality




- 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**



splunk> .conf18

# 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.

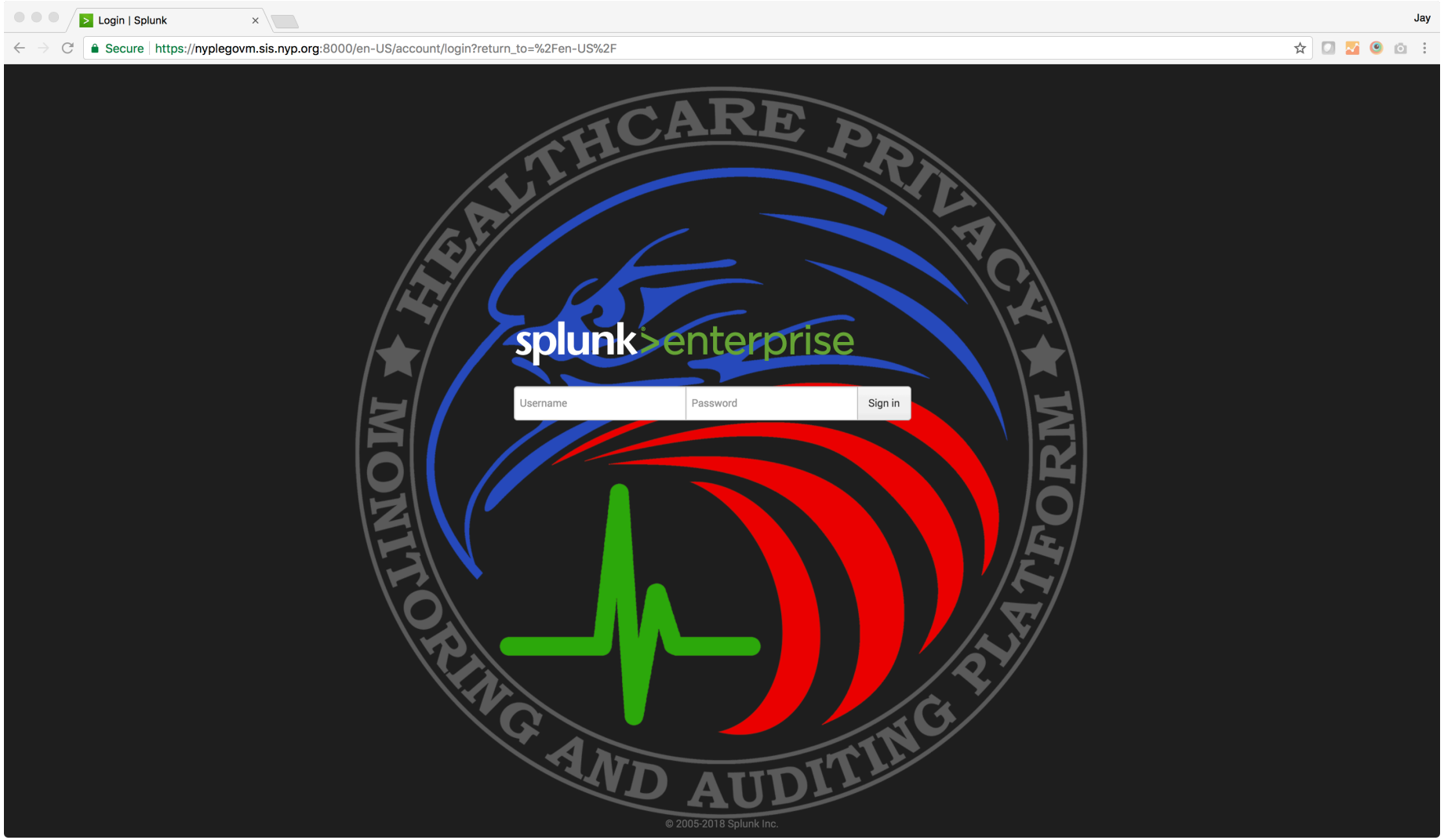
# Privacy Use Cases

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

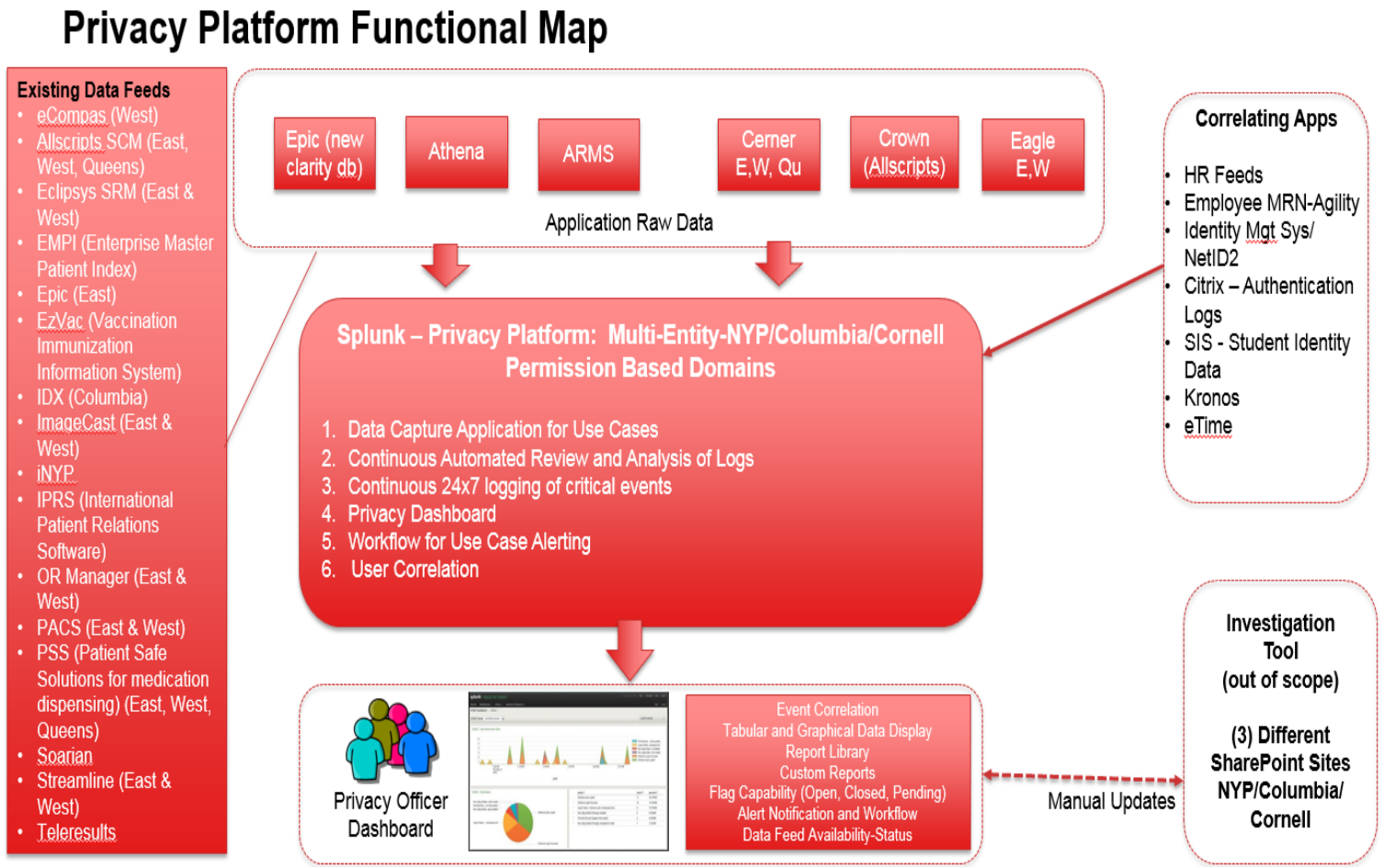
# Evaluation Process

- 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

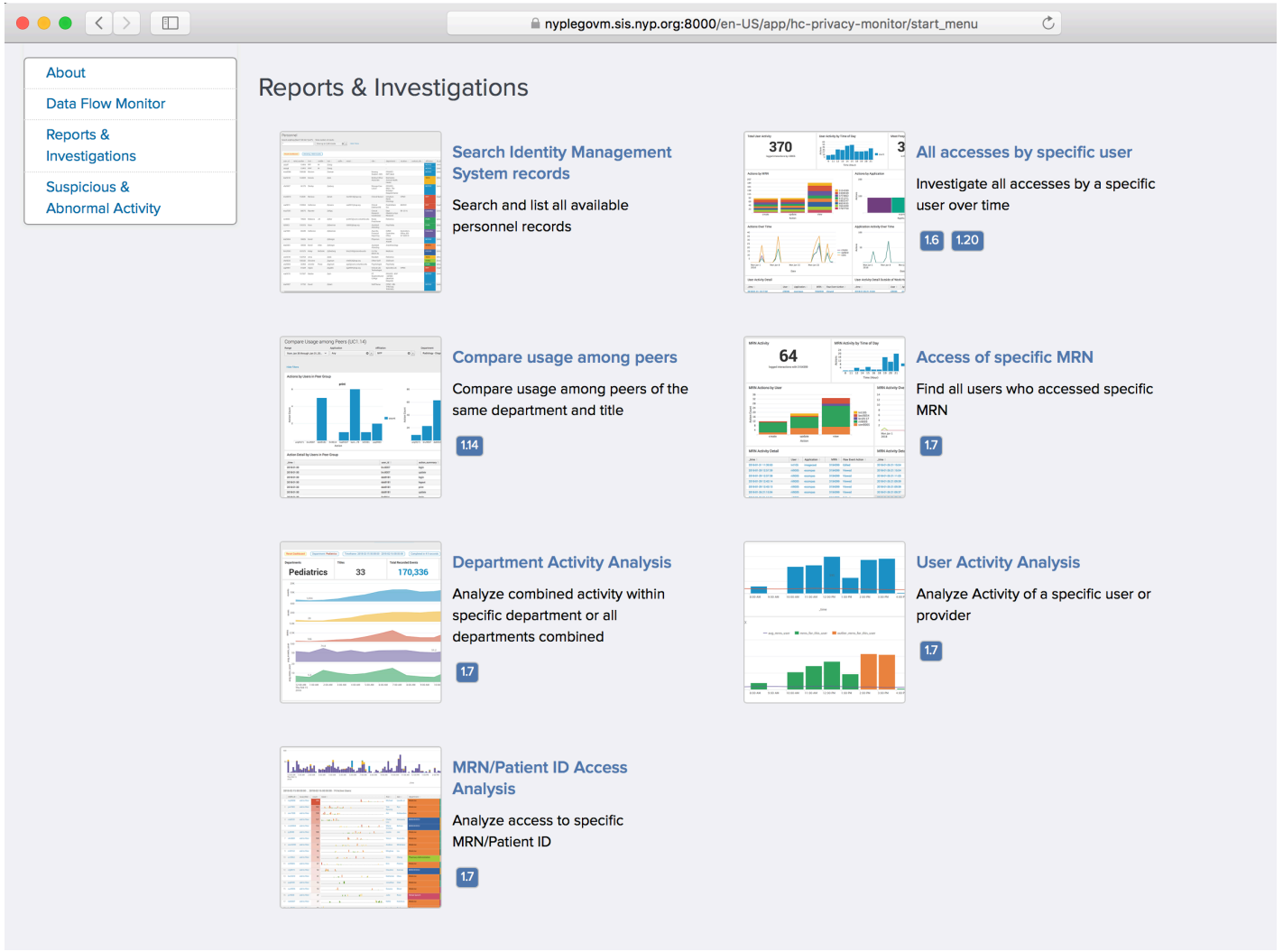


# Healthcare Privacy Monitoring and Auditing Platform



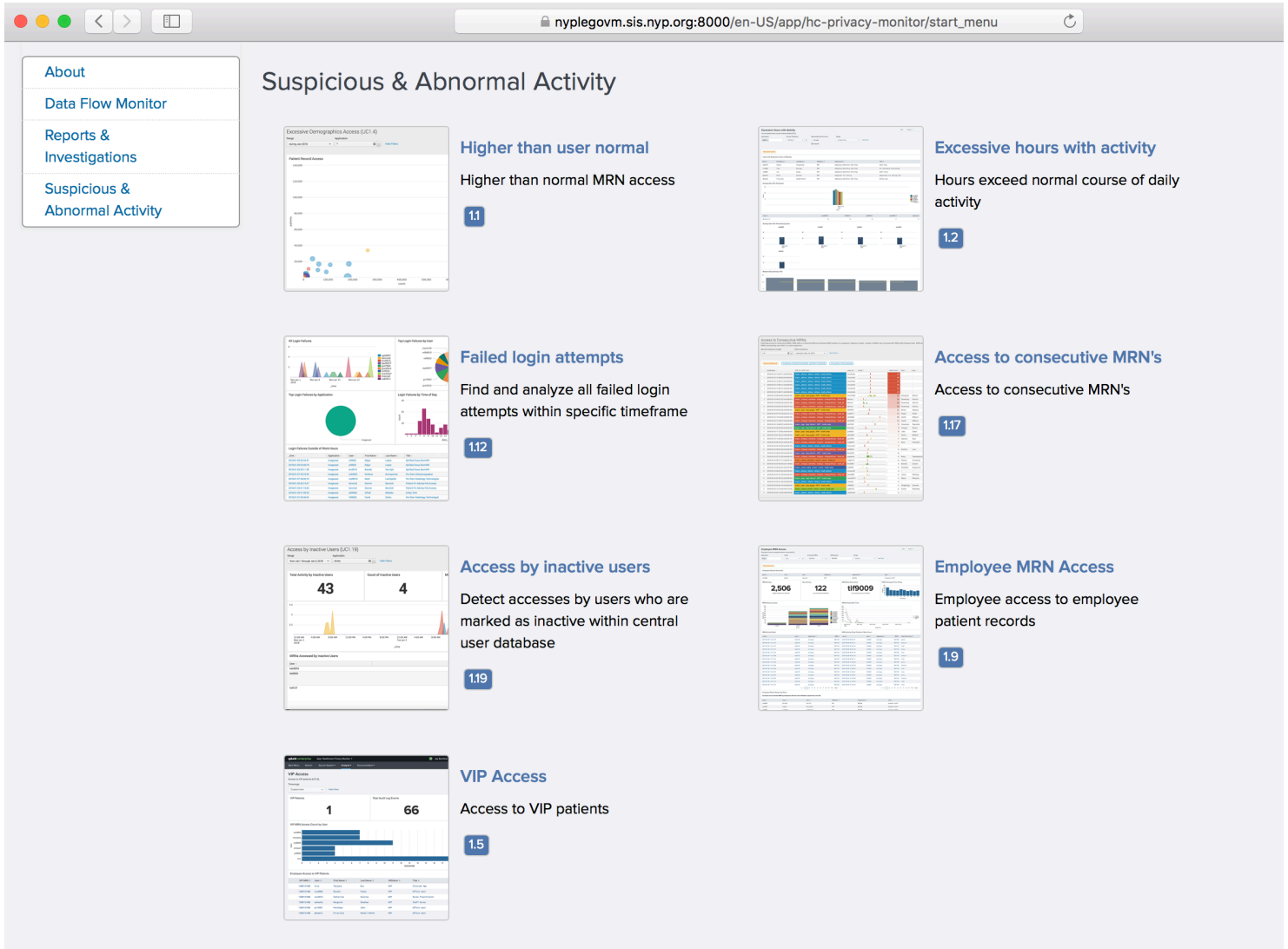

splunk> .conf18

# Healthcare Privacy Monitoring and Auditing Platform



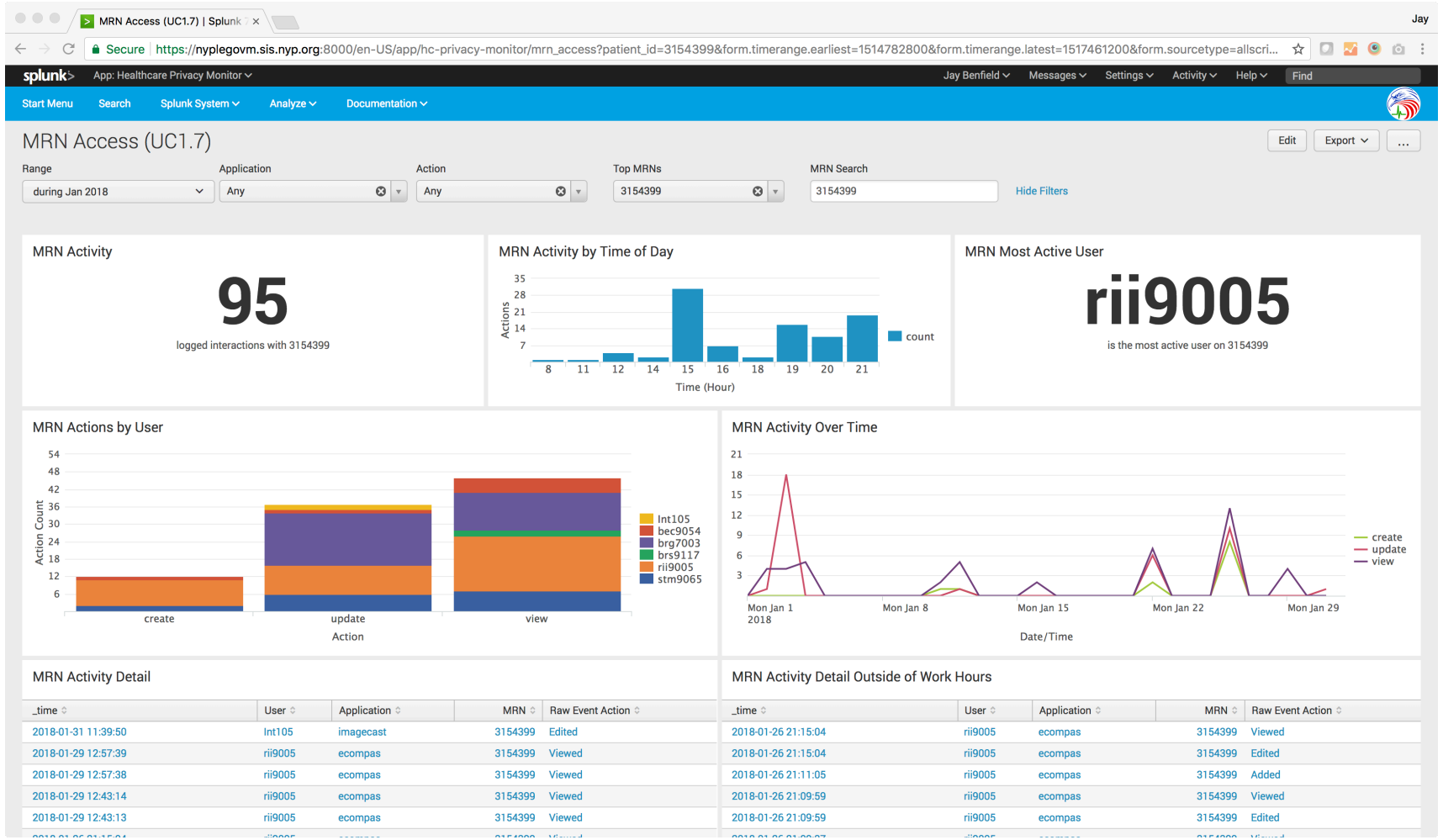

splunk> .conf18

# Healthcare Privacy Monitoring and Auditing Platform



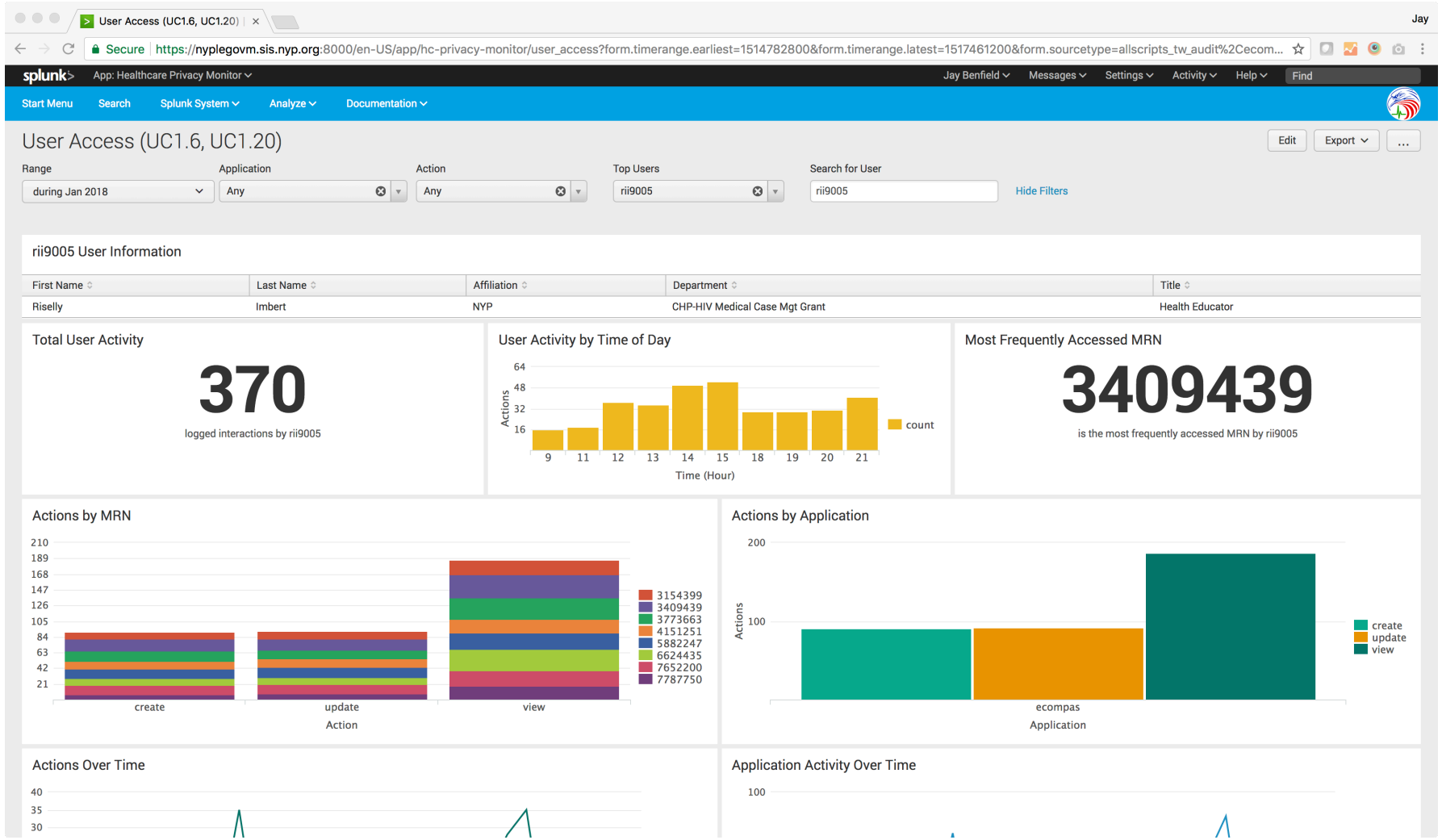

splunk> .conf18

# MRN Access

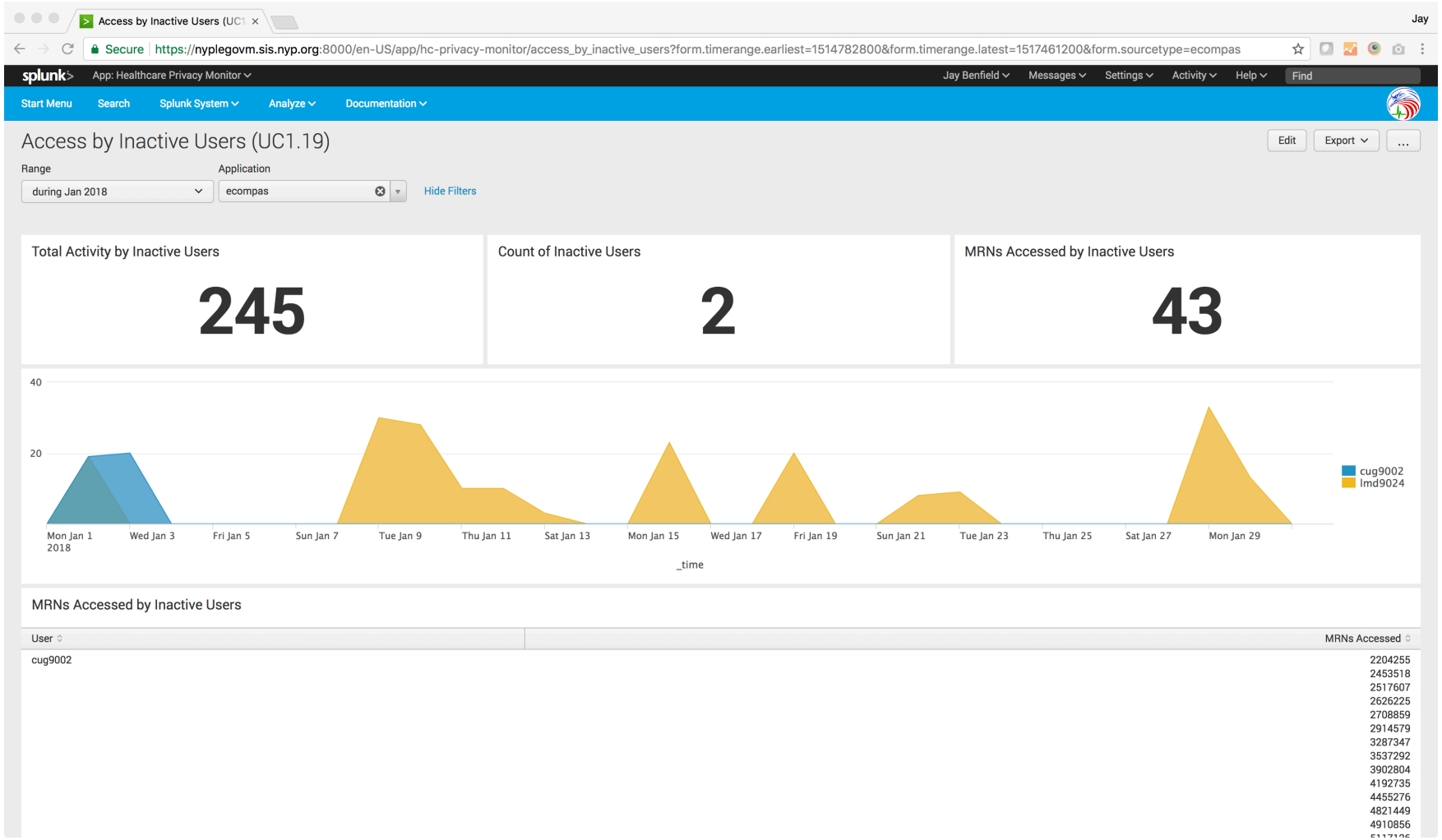



splunk> .conf18

# User Access

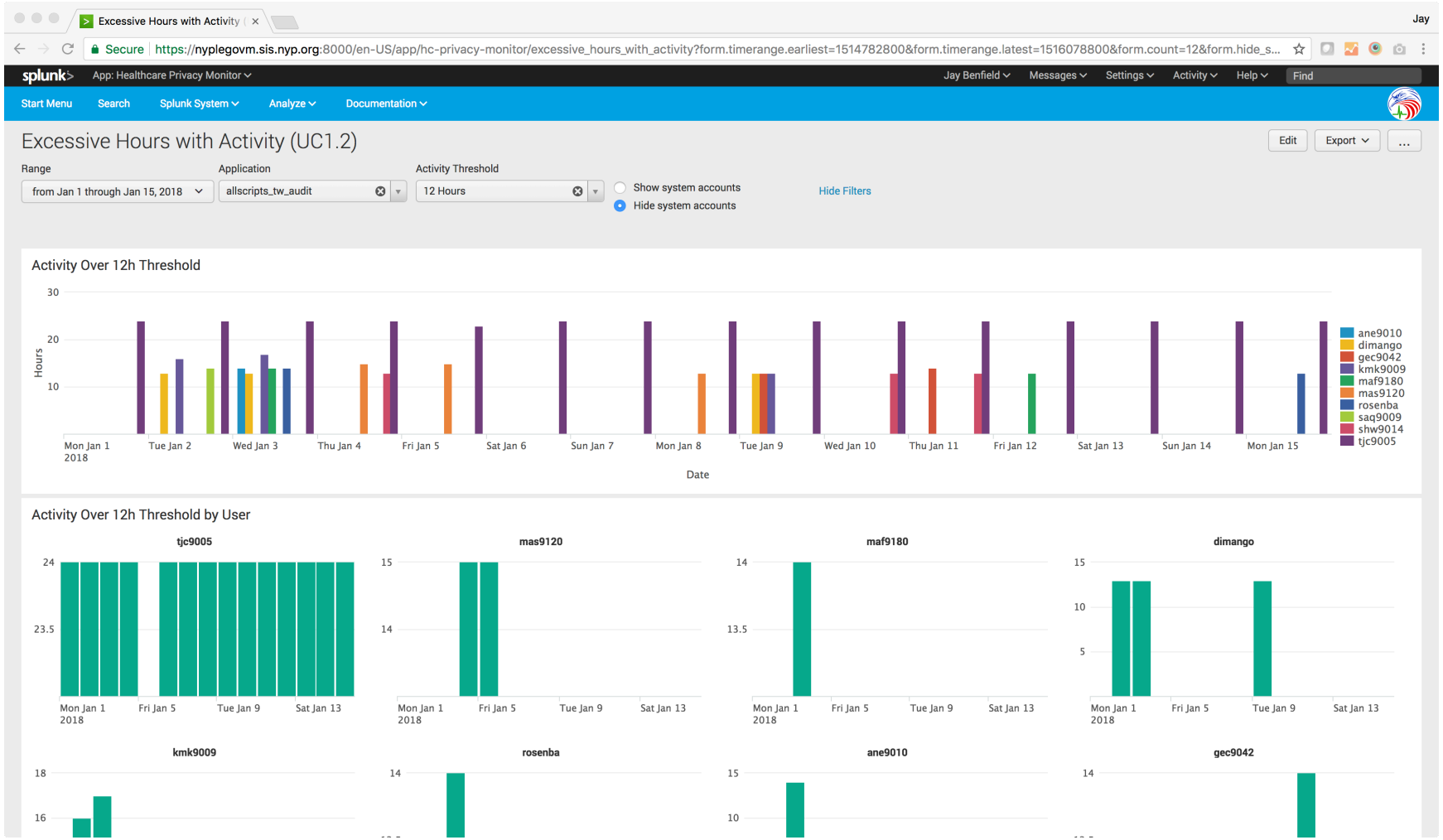


# Access by Inactive Users



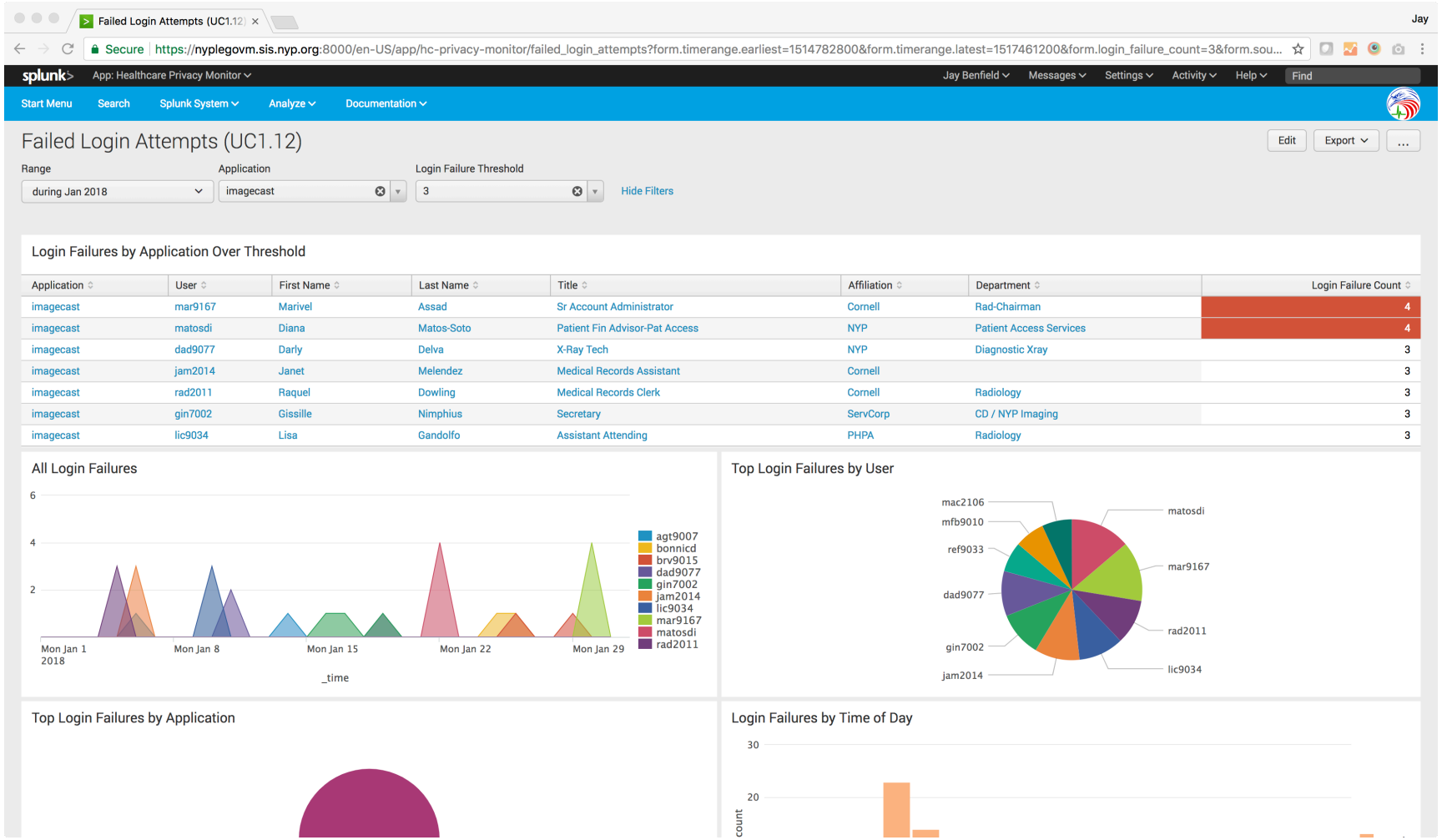

splunk> .conf18

# Excessive Hours with Activity




splunk> .conf18

# Failed Login Attempts




splunk> .conf18

# NYP and Splunk

**Pharmacy/Opioid Diversion**

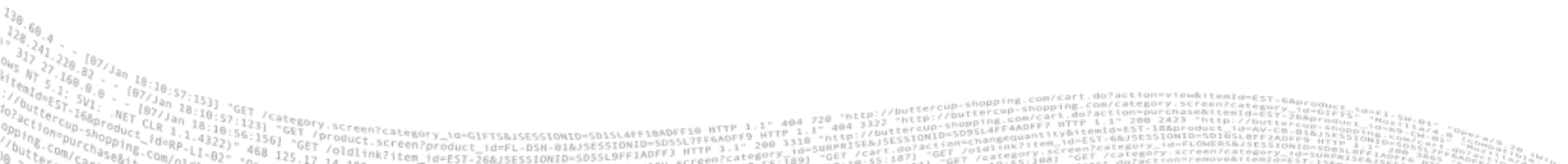
# The American Epidemic

## 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

.CONF & SPLUNKLIVE!

# 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

splunk> .conf18

# Thank You

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