RSA Conference 2018
San Francisco | April 16 – 20 | Moscone Center

NOW MATTERS

SESSION ID: IDY-F03

# DETECTION OF AUTHENTICATION EVENTS INVOLVING STOLEN ENTERPRISE CREDENTIALS

**Mijung Kim**

Research Engineer
Micro Focus

**Pratyusa K. Manadhata**

Principal Researcher
Micro Focus

# Motivation

# Problem statement



Scalable, reliable, and timely detection of *malicious authentication events*

# Challenges



- Base rate fallacy

- Similarity of good and bad events

Wikimedia.org

# A machine learning based solution



Data → Features → Models → Validation

Infrastructure

# An authentication event

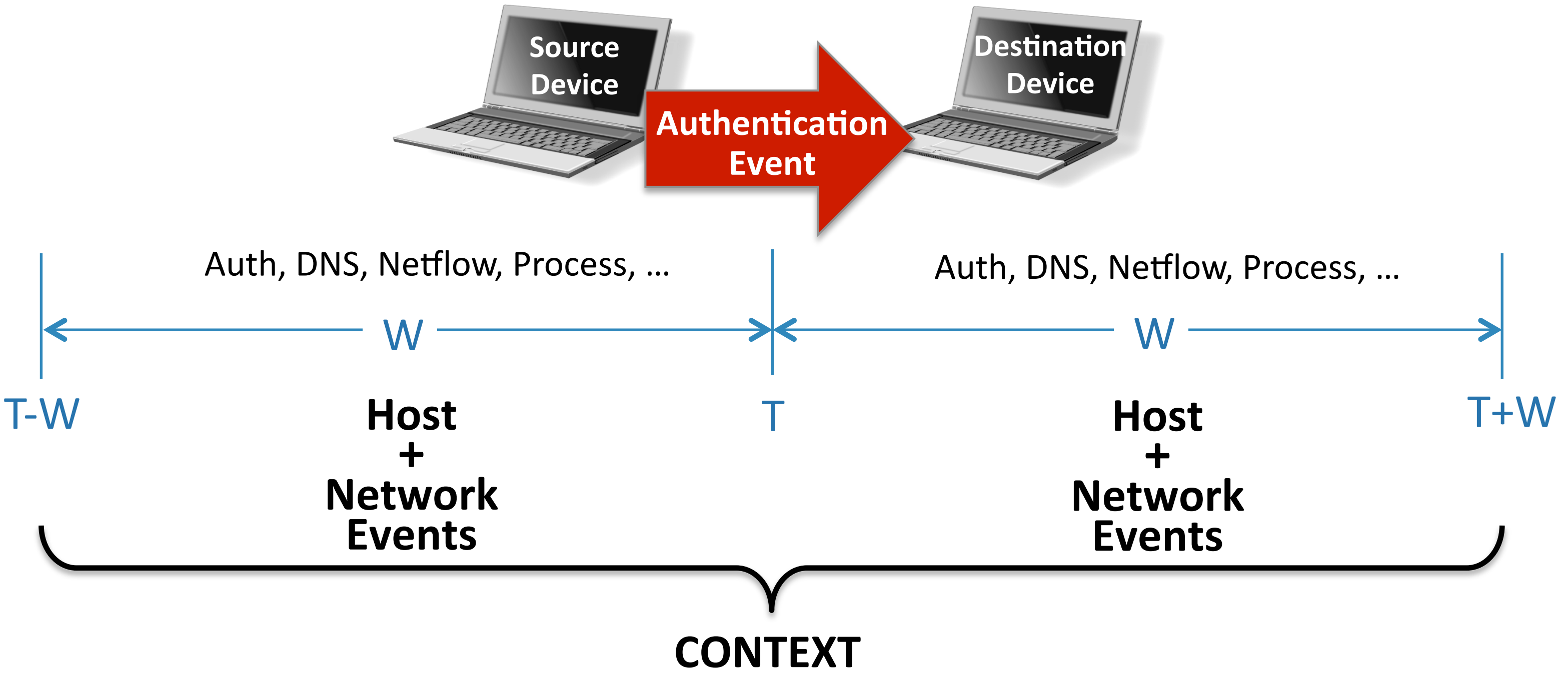


- Time of authentication
- Source device and source user
- Destination device and destination user
- Authentication type, orientation, logon type, outcome

*Hard to differentiate malicious from benign*

# The context of an event





# Modified problem statement



Scalable, reliable, and timely *classification* of an *authentication event's context*

# EXPERIMENTAL RESULTS

# Los Alamos National Labs data



- Collected from Los Alamos National Labs' network over 58 days

| | |
|---|---|
| Users | 12.4K |
| Devices | 17.7K |
| Events (Authentication, DNS, Netflow, Process) | 1.65B |
| Authentication events | 1.05B |

https://csr.lanl.gov/data/cyber1/

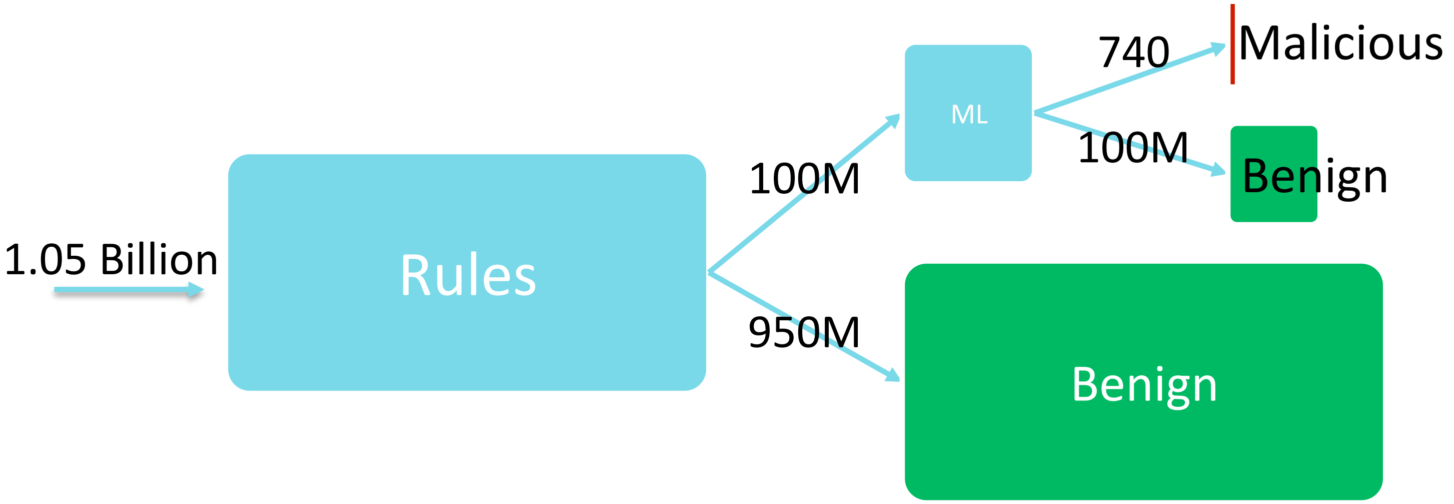
# Malicious authentication events



749 events performed by a red team using stolen credentials

How to distinguish 749 malicious events from 1.05B events?

# Data reduction for scalability



# Examples



- Filter out local events
- Focus on network authentication
- Focus on successful authentication
- ..

*Rule matching shouldn't have false negatives, but false positives*

# Feature extraction



- Given an authentication event at time T, extract features from
  - Events on the source device in the time period (T-W)
  - Network events between the source and the destination
  - Events on the destination device in the time period (T + W)
- Feature identification via domain expertise

# Example features



- Authentication logs
  - Failures/successes at the source and the destination
- Netflow logs
  - Connections per protocol, Number of bytes/packets on standard/non-standard ports, ..
- DNS logs
  - Frequency of DNS events at the source and the destination, ..

# Model selection

- Model selection data
  - Randomly chosen 10K legitimate events and 3.5K compromised events
  - 5 fold replication of compromised events to handle class imbalance

- Training and test split: 75%:25% and 10 fold cross validation

# Performance of different models

| Model | True Positive Rate | False Positive Rate |
|---|---|---|
| Random Forest | 0.988 | 0.030 |
| Logistic Regression | 0.977 | 0.056 |
| Naïve Bayes | 0.929 | 0.154 |
| Multilayer Perceptron | 0.973 | 0.076 |
| SMO | 0.951 | 0.135 |

Reporting 75:25 split results (10 fold CV results are similar)

# An ‘end to end’ experiment



- Model generation
  - 8K benign and 2.5K malicious (5 fold replication)
- Parameter selection
  - 80M benign and 124 malicious
- Error estimation on Test data
  - 20M benign and 124 malicious

# Precision-recall plots



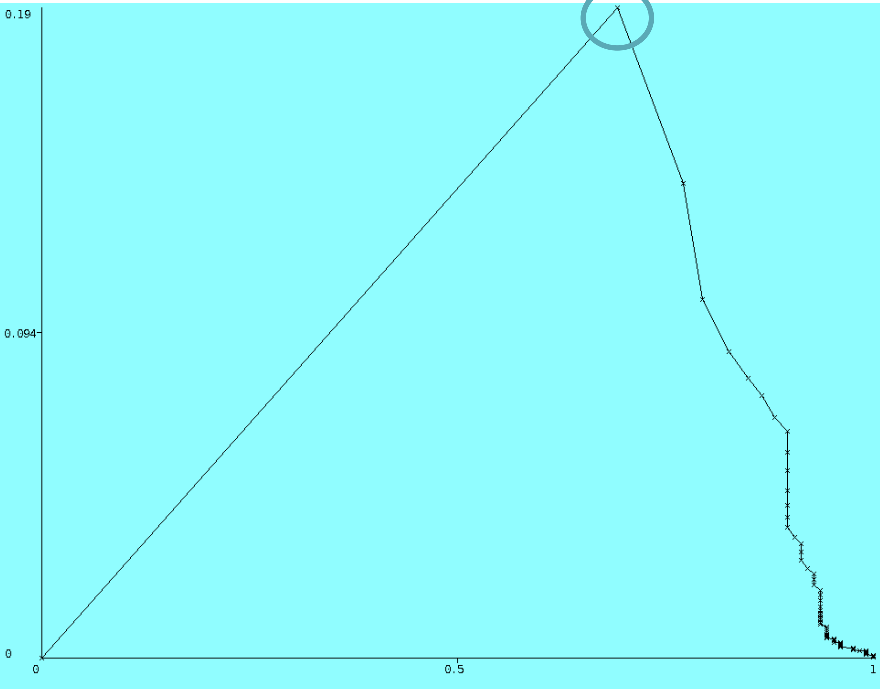
- Better than ROC plots for imbalanced data sets
  - Even a very low FPR produces many FPs

- Precision
  - Fraction of true positives in events detected as malicious
  - TP /(TP + FP)

- Recall:
  - Fraction of malicious events detected
  - TP / (TP + FN)

# Threshold selection

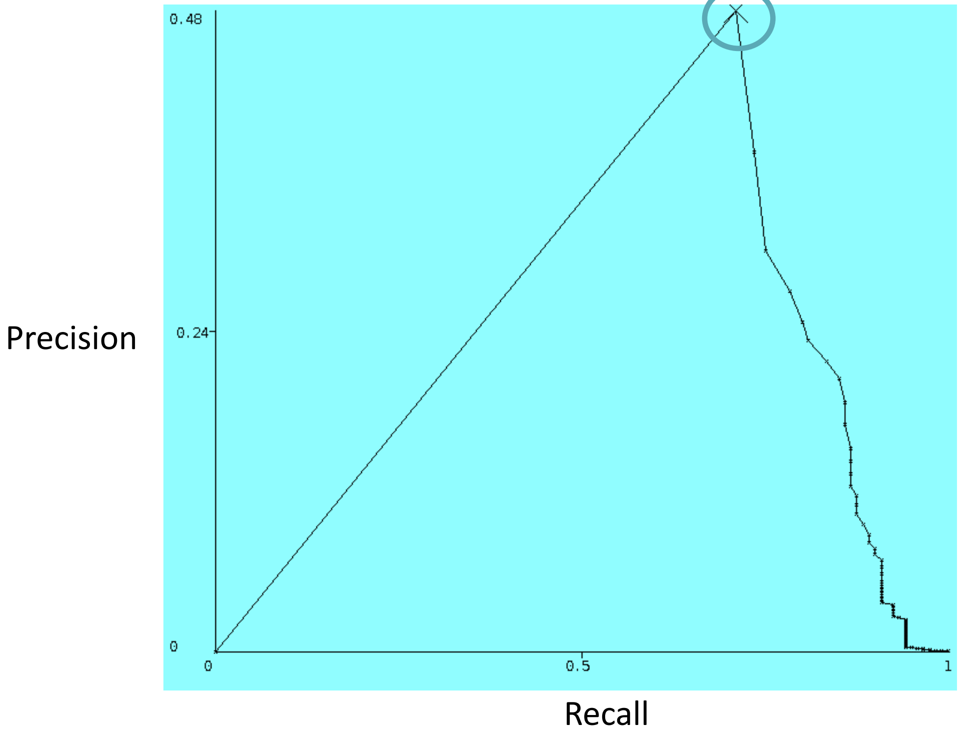
Precision




Recall

Threshold = 0.99
Precision = 0.19
Recall = 0.75

# Test data results




Threshold = 0.99
Precision = 0.48
Recall = 0.75

In order to identify 3/4th of the malicious events, the model will generate 52% false positives.

That is, *1 out of every 2 detections will be a false positive.*

# A note about false positives



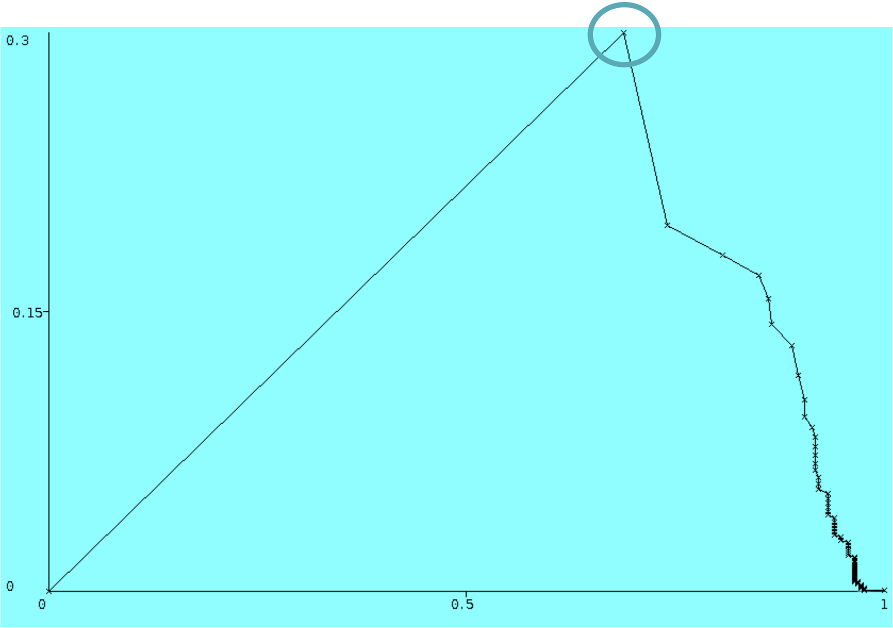
- 1 false positive for each true positive may seem high
- But the number of true positives are very low
  - so the absolute number of false positives will be low.

- Test data: 120 true positives over 60 days.

# Features from only authentication events



Precision




Recall

Threshold = 0.99
Precision = 0.3
Recall = 0.70

*2 out of every 3 detections will be false positives.*

# MODEL GENERATION INFRASTRUCTURE

# Model generation and prediction challenges



- Scalable feature computation and model learning
- Real time detection of compromised authentication events
- Performance issues
  - Feature extraction takes too long

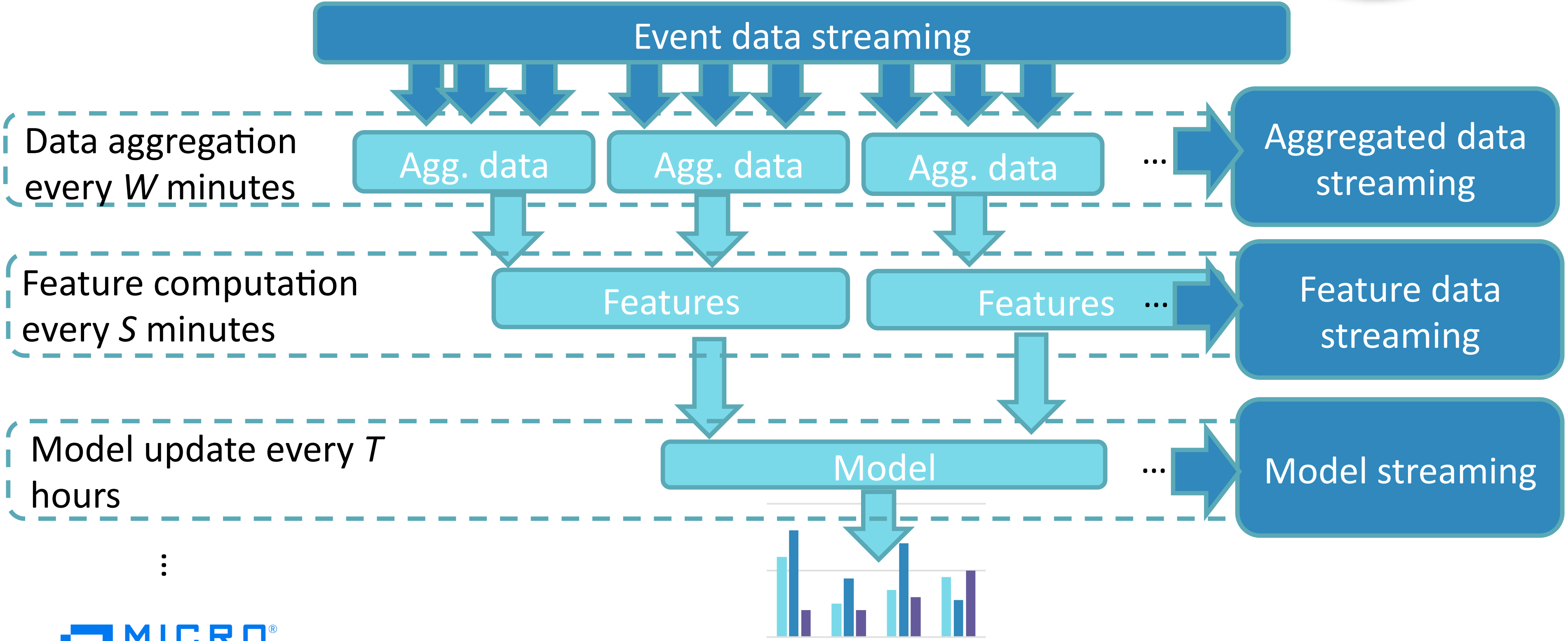
# Scale and performance assumptions



- Data volume in a large enterprise
  - 5 billion events/day  (with 0.5 KB/event, 2.5 TB/day, without compression)
  - Higher number of events when including high volume sources such as Netflow

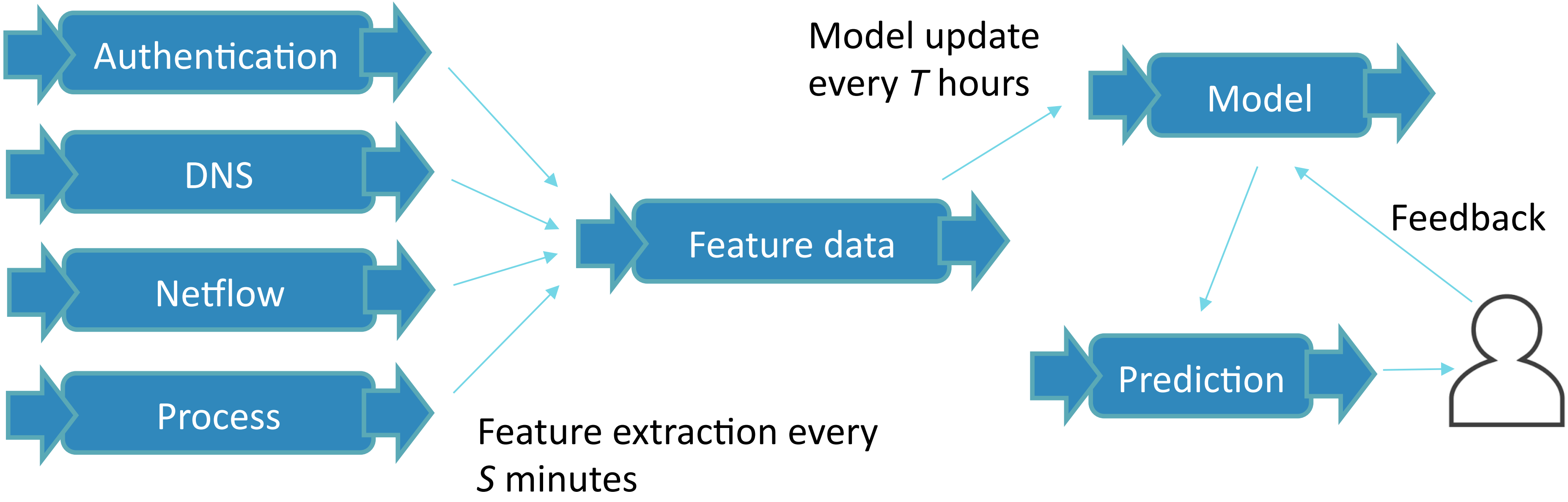
- Streaming data in nature
- Analytics is continuous, not just on data at rest

# Event streaming framework



# Streaming malicious authentication detection

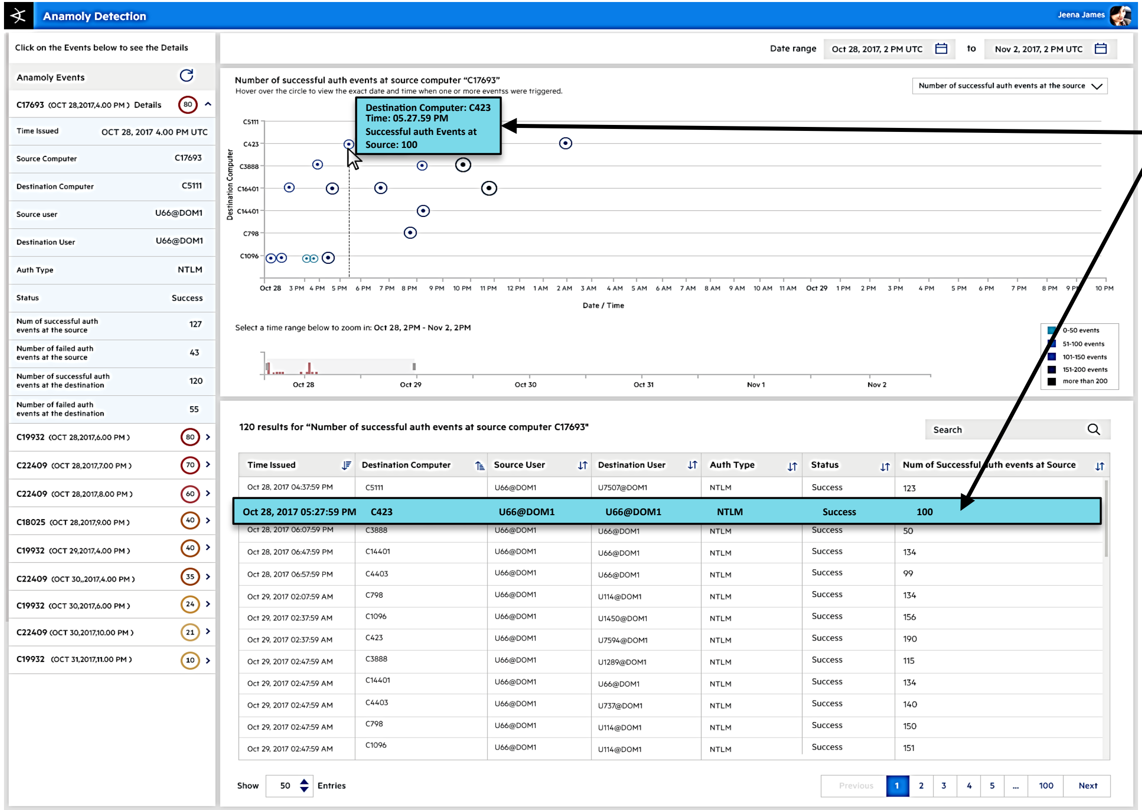




# User Interface



Ranked list of malicious events

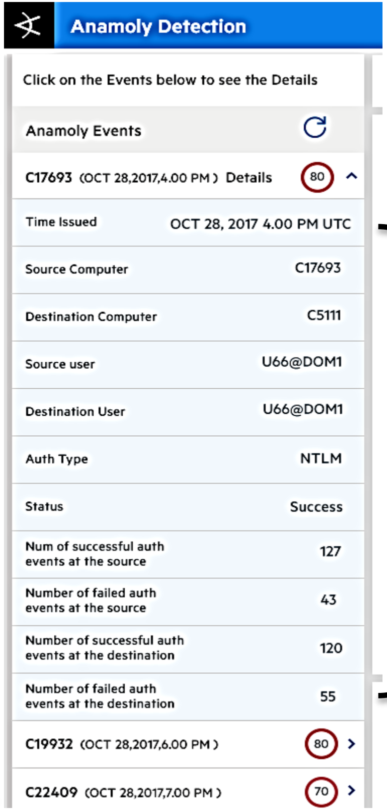



Feature values for an authentication event

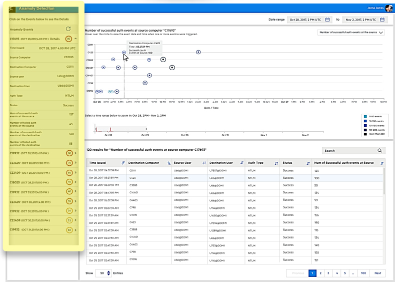
# User Interface



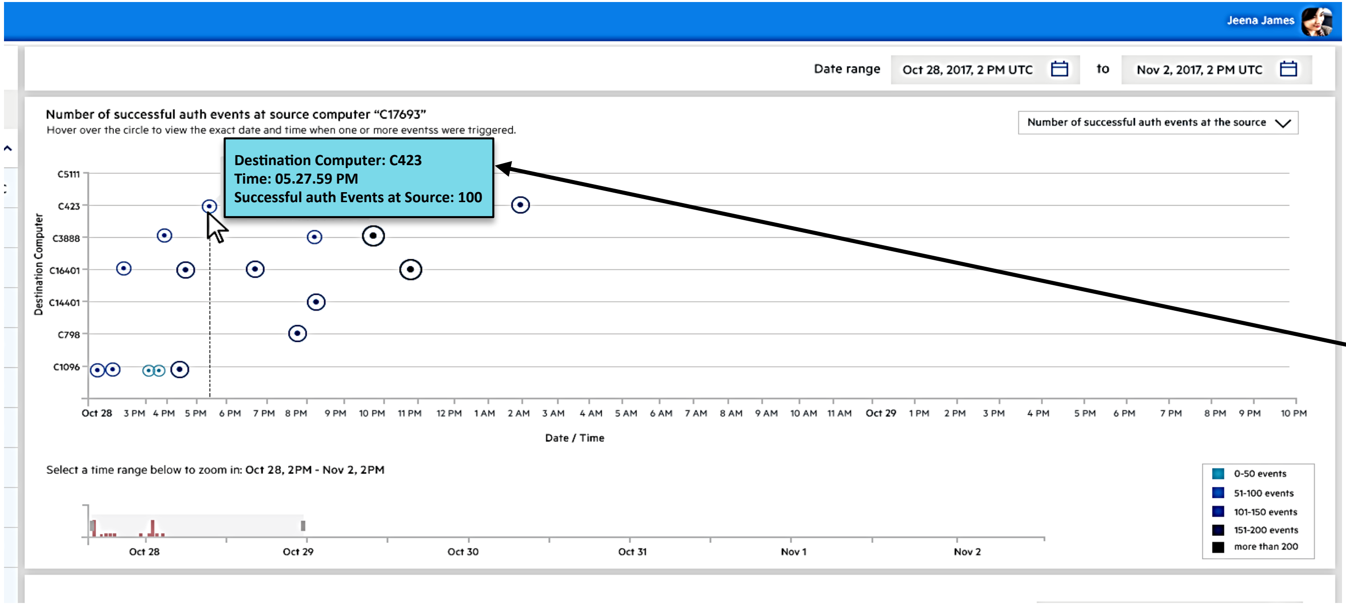
Ranked list of malicious events

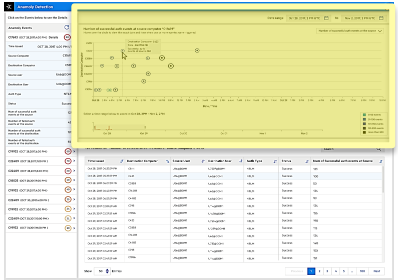



Details of malicious event



# User Interface

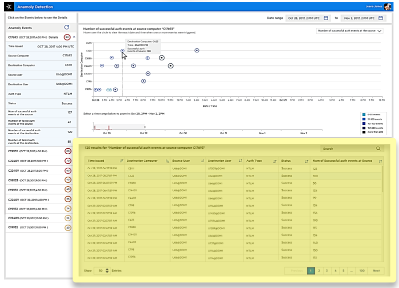


Feature values for an authentication event

# User Interface





120 results for "Number of successful auth events at source computer C17693"

Search

| Time Issued | Destination Computer | Source User | Destination User | Auth Type | Status | Num of Successful auth events at Source |
|---|---|---|---|---|---|---|
| Oct 28, 2017 04:37:59 PM | C5111 | U66@DOM1 | U7507@DOM1 | NTLM | Success | 123 |
| **Oct 28, 2017 05:27:59 PM** | **C423** | **U66@DOM1** | **U66@DOM1** | **NTLM** | **Success** | **100** |
| Oct 28, 2017 06:07:59 PM | C3888 | U66@DOM1 | U66@DOM1 | NTLM | Success | 50 |
| Oct 28, 2017 06:47:59 PM | C14401 | U66@DOM1 | U66@DOM1 | NTLM | Success | 134 |
| Oct 28, 2017 06:57:59 PM | C4403 | U66@DOM1 | U66@DOM1 | NTLM | Success | 99 |
| Oct 29, 2017 02:07:59 AM | C798 | U66@DOM1 | U114@DOM1 | NTLM | Success | 134 |
| Oct 29, 2017 02:37:59 AM | C1096 | U66@DOM1 | U1450@DOM1 | NTLM | Success | 156 |
| Oct 29, 2017 02:37:59 AM | C423 | U66@DOM1 | U7594@DOM1 | NTLM | Success | 190 |
| Oct 29, 2017 02:47:59 AM | C3888 | U66@DOM1 | U1289@DOM1 | NTLM | Success | 115 |
| Oct 29, 2017 02:47:59 AM | C14401 | U66@DOM1 | U66@DOM1 | NTLM | Success | 134 |
| Oct 29, 2017 02:47:59 AM | C4403 | U66@DOM1 | U737@DOM1 | NTLM | Success | 140 |
| Oct 29, 2017 02:47:59 AM | C798 | U66@DOM1 | U114@DOM1 | NTLM | Success | 150 |
| Oct 29, 2017 02:47:59 AM | C1096 | U66@DOM1 | U114@DOM1 | NTLM | Success | 151 |

Show 50 Entries

Previous 1 2 3 4 5 ... 100 Next

Feature values for an authentication event

# Applying today's lesson in your enterprise

- Start collecting event logs in your enterprise
  - Authentication logs
  - DNS logs, Netflow logs, …
- Learn a classifier
  - Collect a labeled data set
  - Extract features
  - Learn a classifier and validate the classifier
- Apply the classifier to future authentication events
  - Flag the identified events for further examination

# Related work



- Data set
  - https://csr.lanl.gov/data/cyber1/
  - A. D. Kent, "Cybersecurity Data Sources for Dynamic Network Research," in Dynamic Networks in Cybersecurity, 2015.
- Data Breaches, Phishing, or Malware? Understanding the Risks of Stolen Credentials, Thomas et al., ACM Conference on Computer and Communications Security (CCS), Nov 2017, Dallas, TX.
- Detecting Credential Compromise in Enterprise Networks, Mobin Javed, PhD Thesis, UC Berkeley, 2016.

# THANK YOU!

manadhata@alumni.cmu.edu

m.kim@microfocus.com