Teamcenter Security Monitoring through SAS Analytics

Siemens - SAS joint user behavioral analytics project

Scott Allen Mongeau
Cybersecurity Data Scientist – Principal Business Solutions Manager
SAS Institute

Overview

- Requirements
- Solution overview
- Development process
- Analytics methods
- Example anomalies
- Conclusion

Requirements

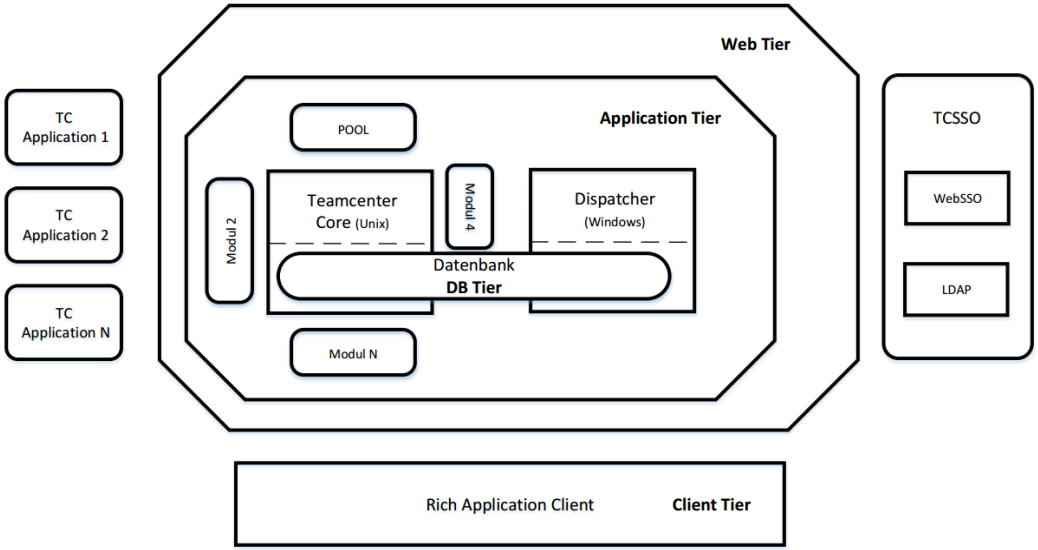

Auntie Anne's
WAY OUT WEST
NEWSSTAND

Teamcenter Security Requirements

- **Teamcenter PLM** = managing product lifecycles, contains sesitive intellectual property
- Multi-tiered web services, browser based application with array of add-on modules

High-level requirements - PoC

- Key use case = protecting intellectual property / preventing improper use and exfiltration
- Non-invasive, automated, asyncronous
- Minimize administrative overhead
- Strict user privacy (anonymization)
- Identify highly unusual anomolous user behaviors
- Minimize false alerts through embedded contextual understanding of typical / atypical behavior

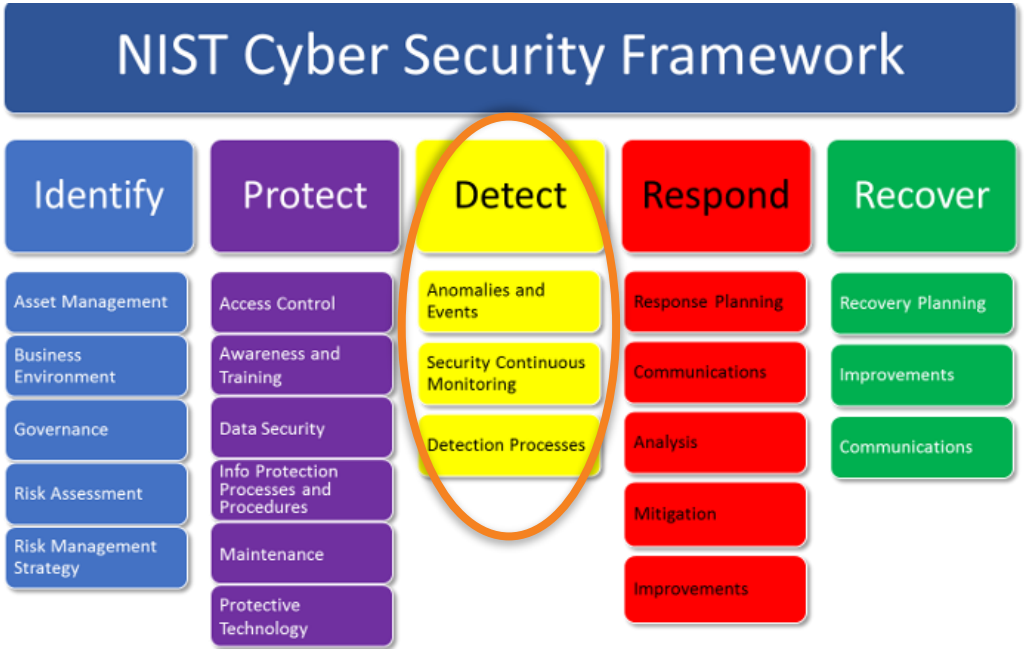


Teamcenter Security Requirements

- **Teamcenter PLM** = managing product lifecycles, contains sesitive intellectual property
- Multi-tiered web services, browser based application with array of add-on modules

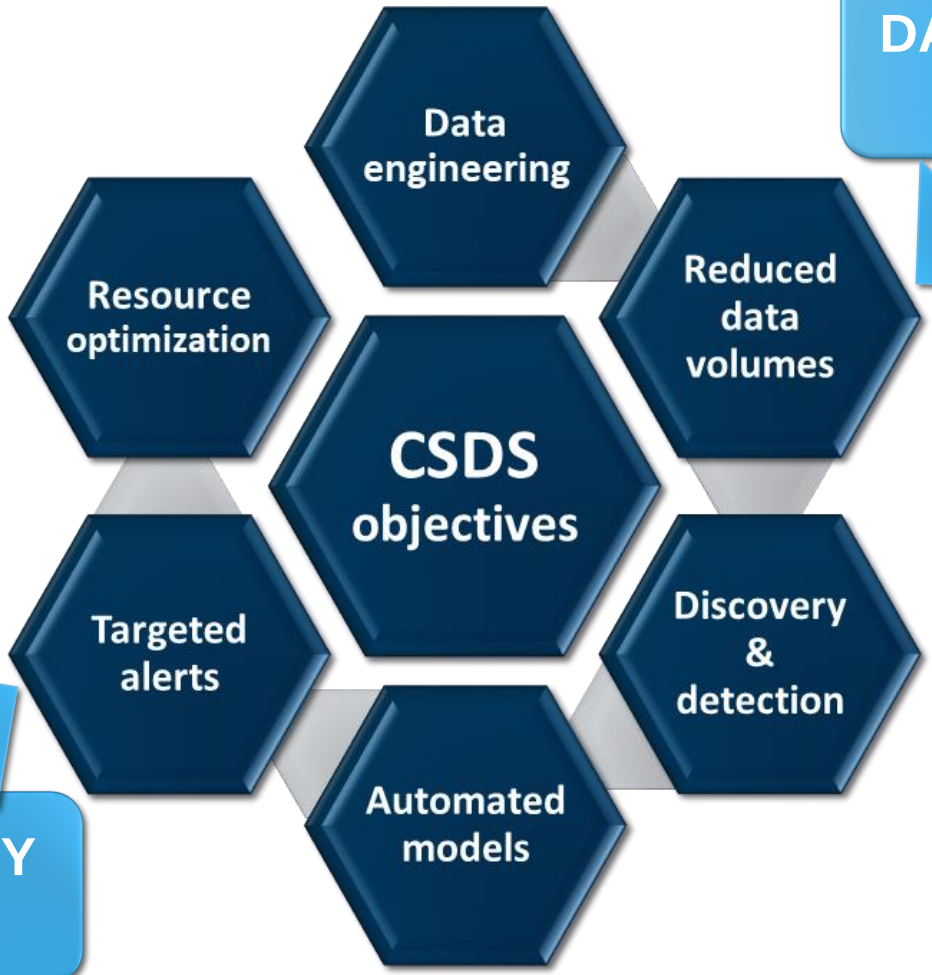
High-level requirements - PoC

- Non-invasive, automated, asyncronous
- Minimize administrative overhead
- Strict user privacy (anonymization)
- Key use case = protecting intellectual property / preventing improper use and exfiltration
- Identify highly unusual anomolous user behaviors
- Minimize false alerts through embedded contextual understanding of typical / atypical behavior



CSDS

Cyber Security Data Science



DATA SCIENCE METHODS

CYBERSECURITY GOALS

sas

Solution Overview

TeamCenter Log Analytics

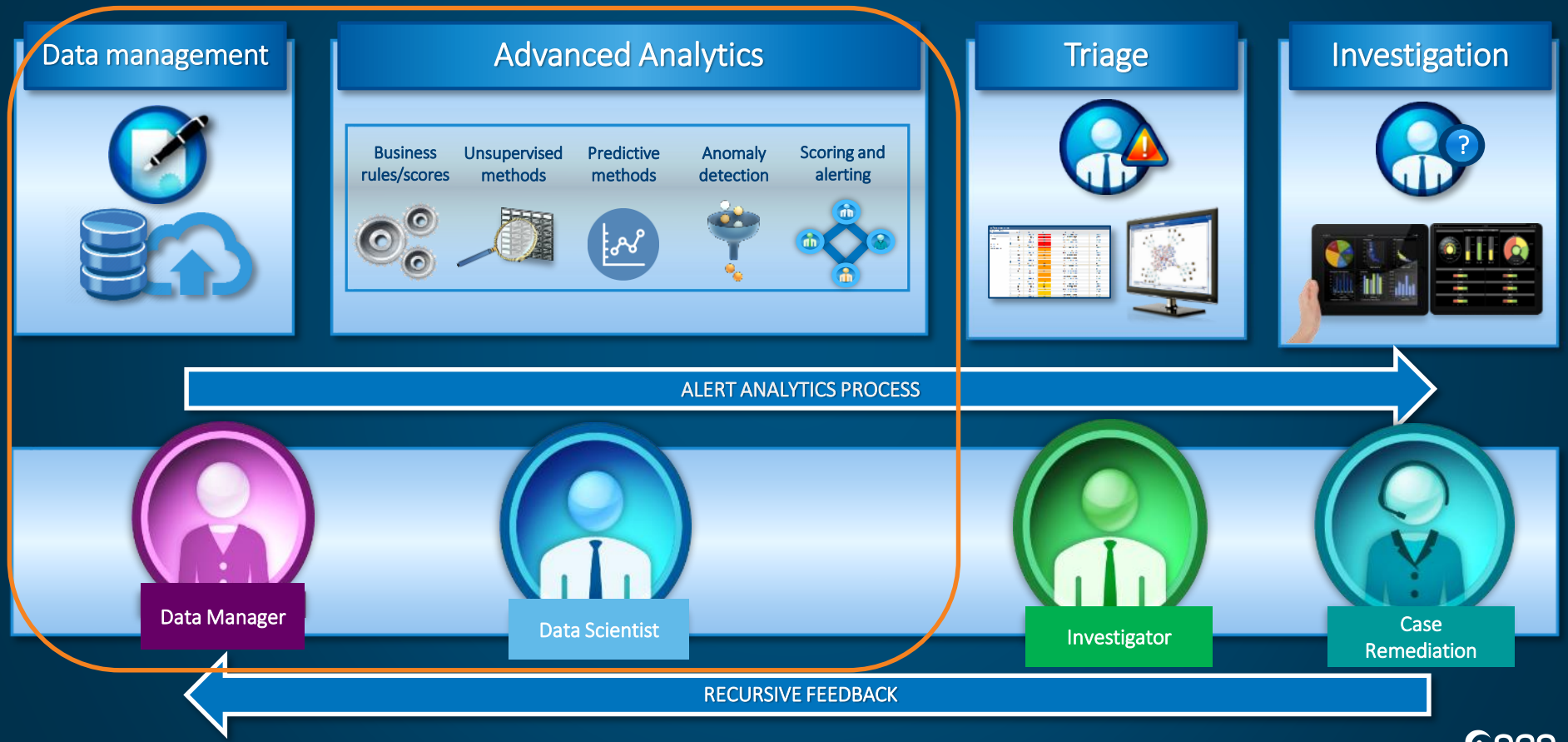
Ingest raw log data in **batch**

Refine data and apply **advanced analytics**

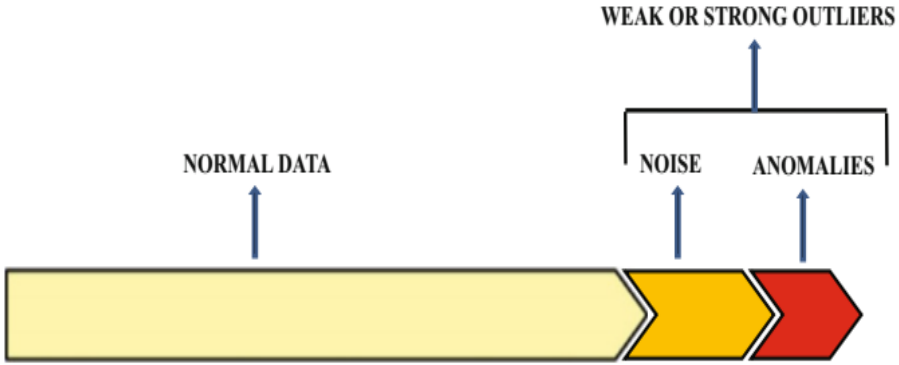
Deliver **focused anomaly alerts**

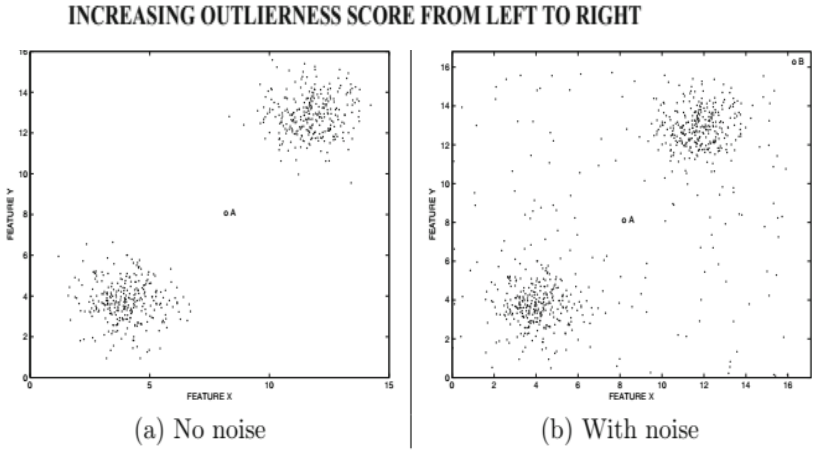
Internal follow-up

High-Level Functional Process

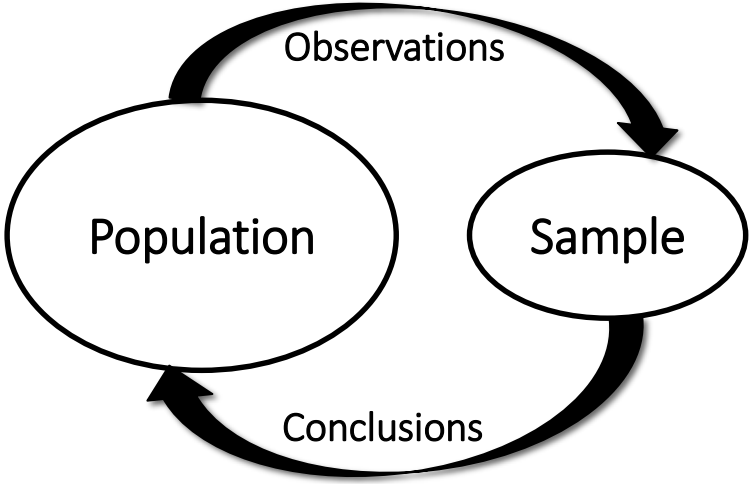


Anomaly Detection: Simply Complex



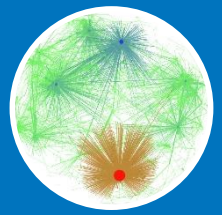


Inferential Statistics



SOURCE Aggarwal, Charu C. (2017). "Outlier Analysis: Second Edition". Springer International Publishing AG.

Assessing Key Features to Produce Focused Anomalies



Network context

Session summaries

Functional calls

Exception indicators

Composite for User Baselines

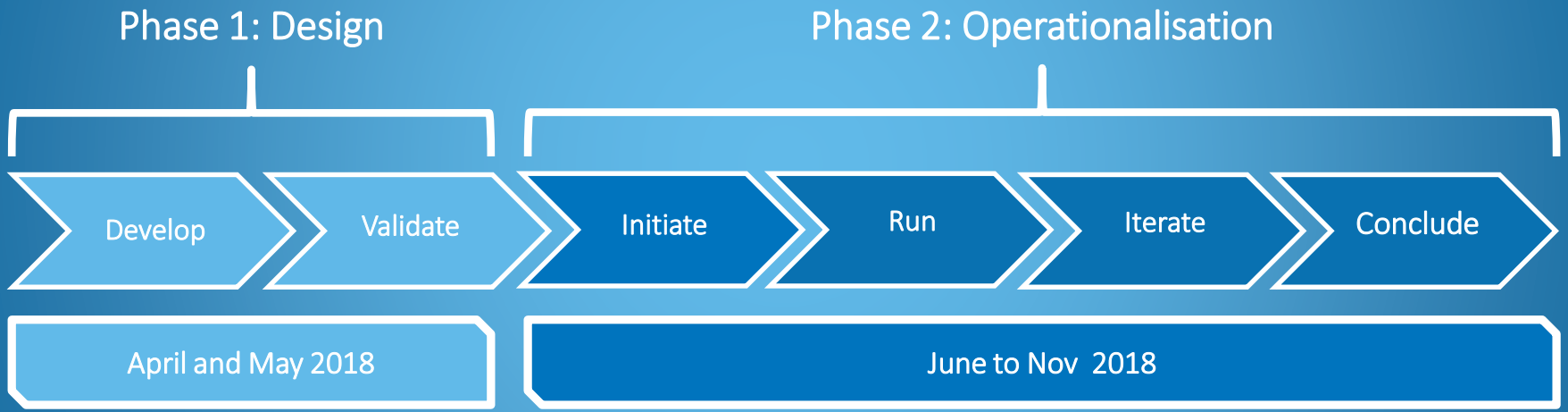
1. FLAG - many high measures

2. CHANGE - changes in behavior

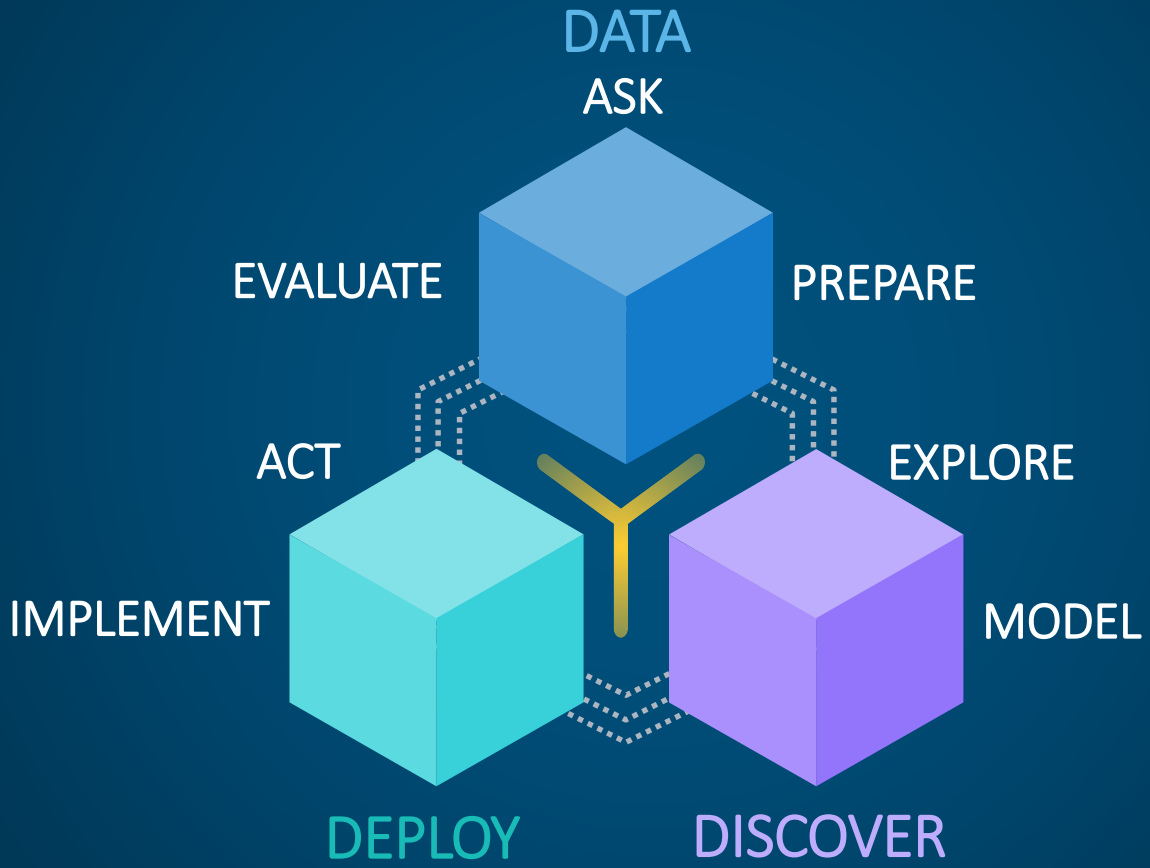
3. UNUSUAL - outliers

Development Process

Cybersecurity Analytics for TeamCenter PLM

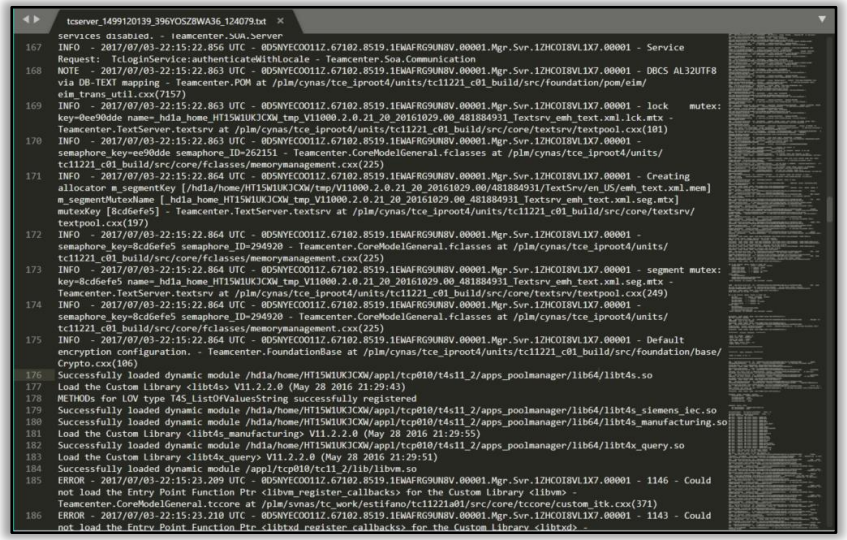


SAS Analytics Process



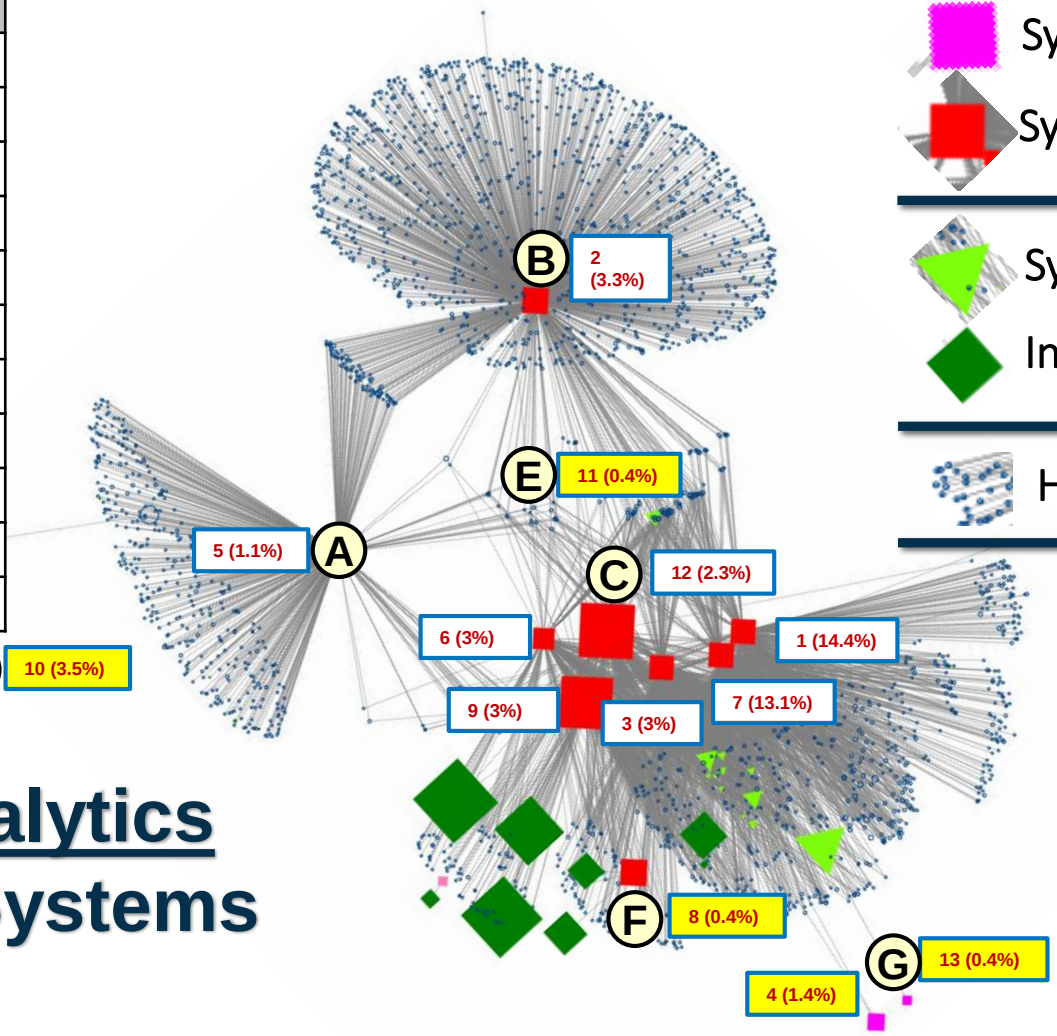
Inferential Exploration

- Exploratory analytics
- Initial sample = 2 weeks TC syslog sessions
- Initial challenges
  - Unstructured
  - Little documentation
  - Little known concerning structure/context (codes, functional relevance)
  - Verbose (many codes, commands, etc.)
- Initial investment in data selection and feature engineering



USER TYPE	# SESSIONS
System-User	10331
System-User	9497
Interface-User	7559
System-User	6936
System-User	3287
System-User	2769
System-User	1998
Interface-User	1382
Interface-User	1156
*User **	*934*
Interface-User	793

** User XXXXXXXX*



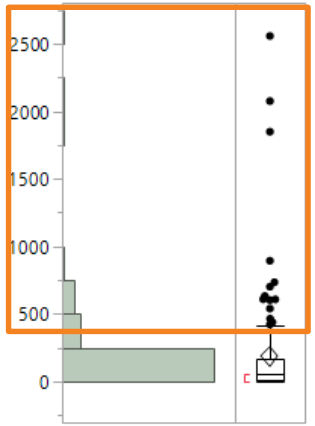
Graph Analytics
Multiuser Systems

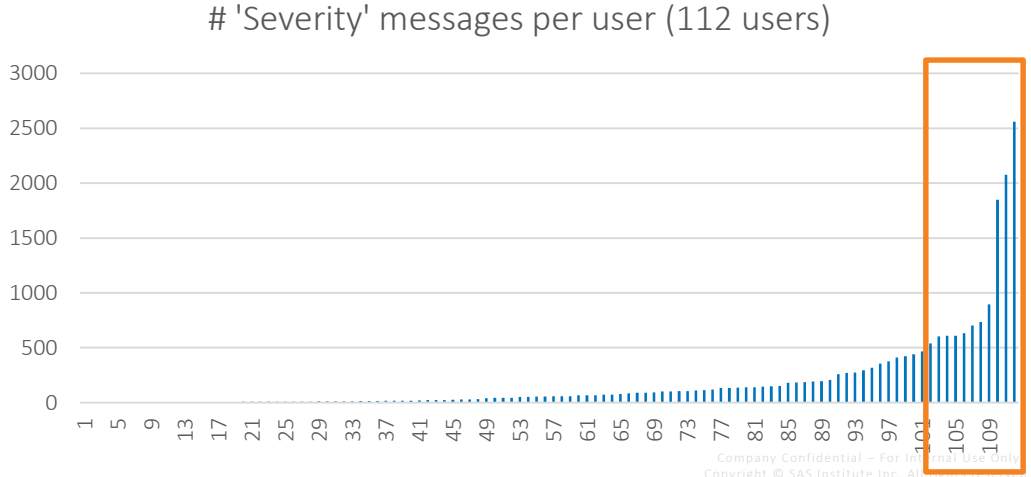
sas

States Indicative of Exceptions

Example: 'SEVERITY'

- Determine how many users and sessions with term
- Aggregate total for each user and make record
  - Expand details for frequent terms (e.g. mean, st dev, total)
- Profile and determine outliers
- Record flag for outliers
- *Validate with systems experts to determine significance*





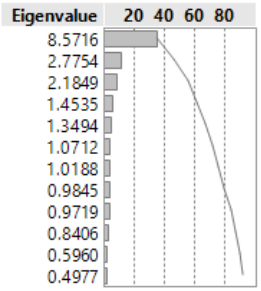
Quantiles

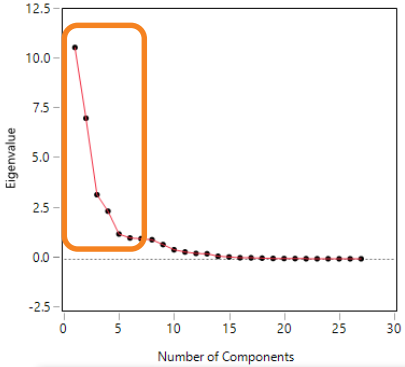
100.0%	maximum	2559
99.5%		2559
97.5%		1889.725
90.0%		517.5
75.0%	quartile	172.75
50.0%	median	55.5
25.0%	quartile	9.75
10.0%		3.3
2.5%		1.825
0.5%		1
0.0%	minimum	1

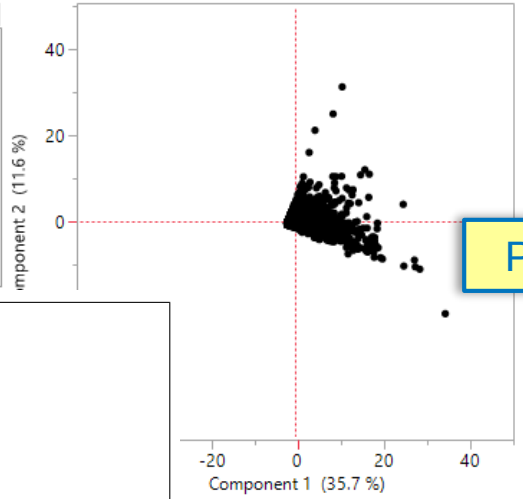
Summary Statistics

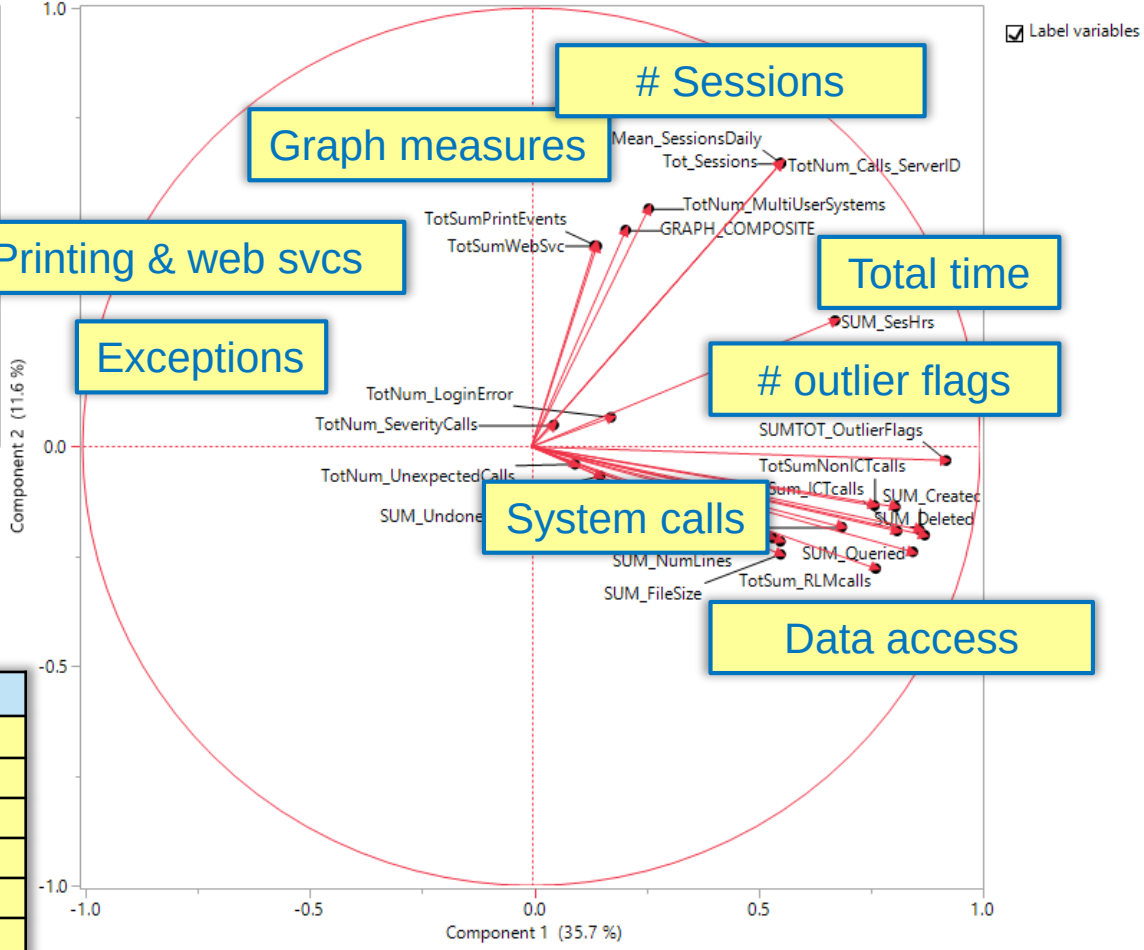
Mean	184.01786
Std Dev	380.96684
Std Err Mean	35.997982
Upper 95% Mean	255.35026
Lower 95% Mean	112.68545
N	112

Principal Component Analysis (PCA)









# Var	Suggested Variable Components
9	Key events (created, deleted, queried)
10	# sessions, server ID calls, # outlier flags
6	File sizes and # lines
6	Non-ICT calls, unexpected calls
3	Data access calls
3	Multi-user systems / graph measures

Log File Measures Extracted

Session summaries

Session events

Exception indicators

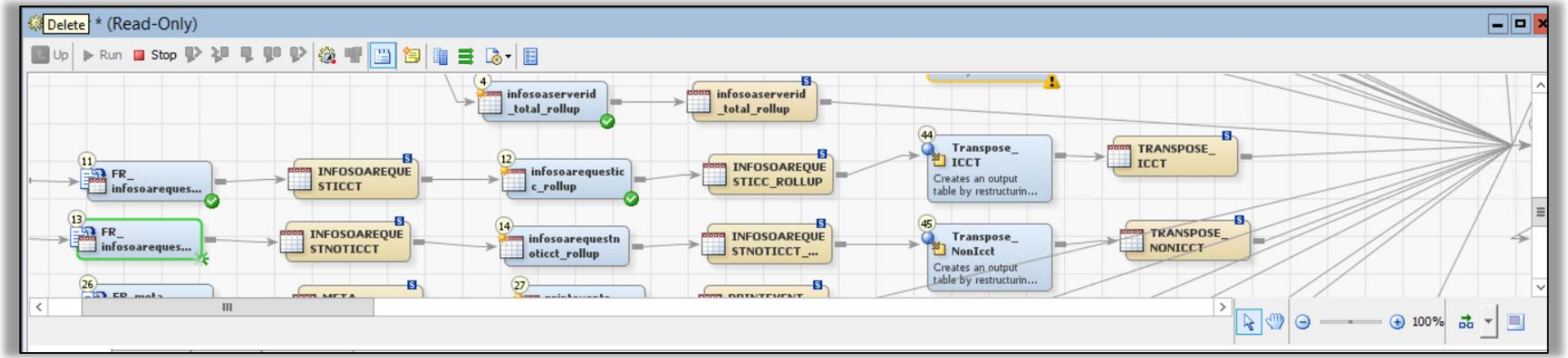
Functional calls

Network context

1 week & 6 week roll-ups
- Total sum ∑
- Standard deviation σ
- 110 total measures

Resulting ETL Process

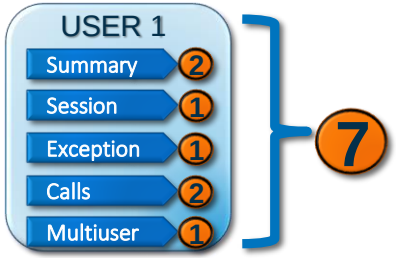
- SAS extract-transform-load (ETL) to process data and orchestrate analytics
- Specialized data handing: *i.e. time zone adjustment, segmentation of specialized users & subcommand handling*
- Regularized and reliable – *flat data goes in and focused anomalies are produced*

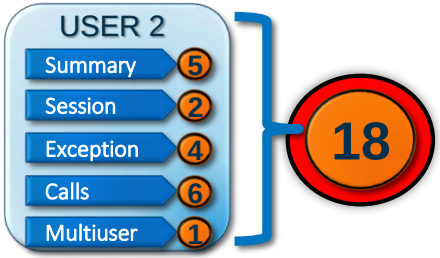


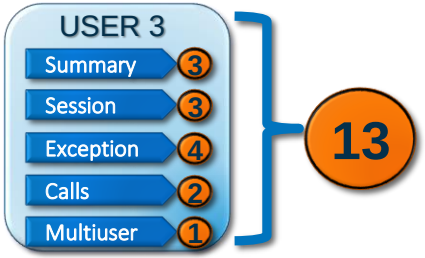
Analytics Methods

Cybersecurity Anomaly Detection

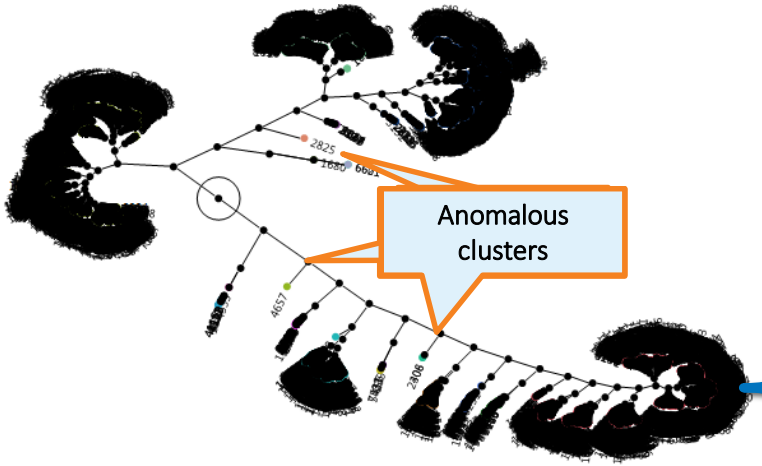
Multiple Methods to Surface Anomalies



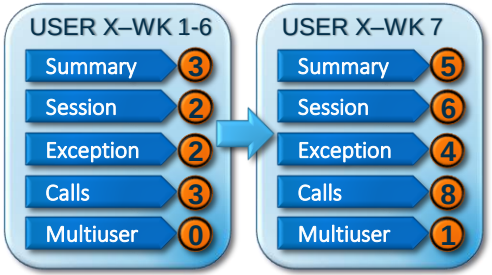


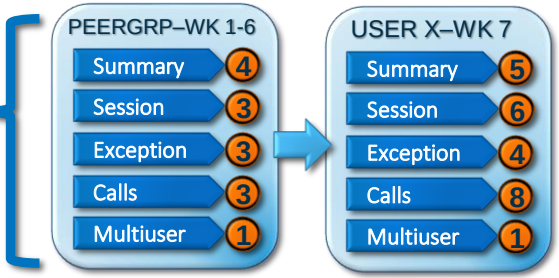


1. UNIVARIATE 'FLAGS'



2. UNSUPERVISED MACHINE LEARNING

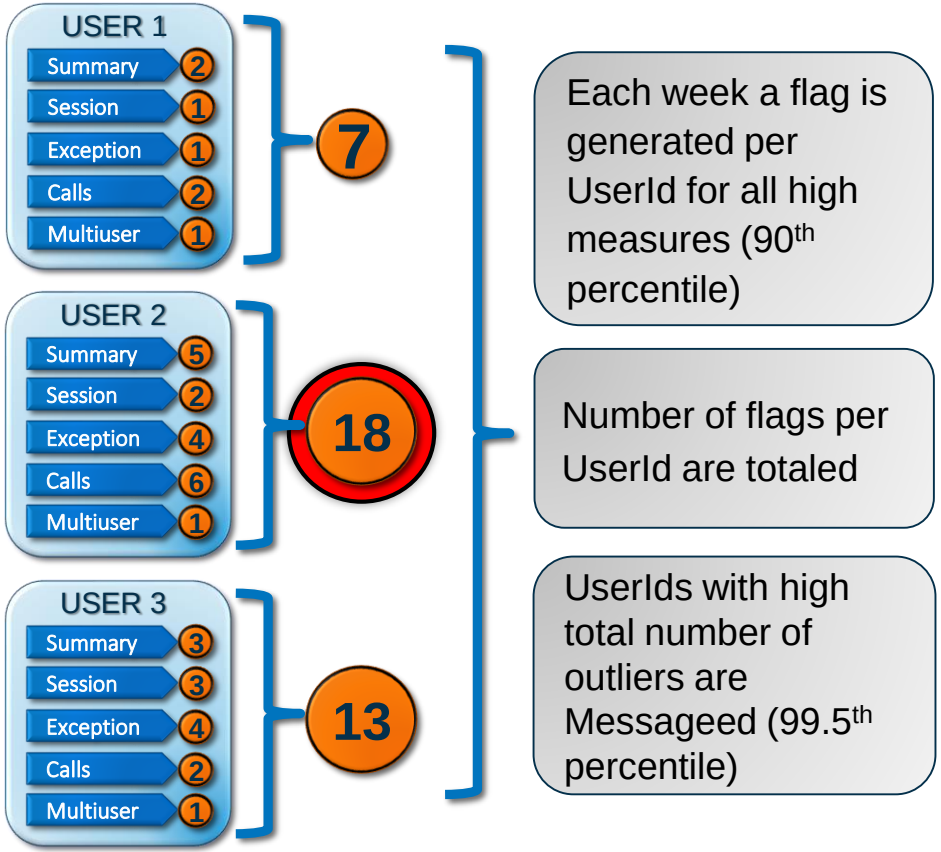




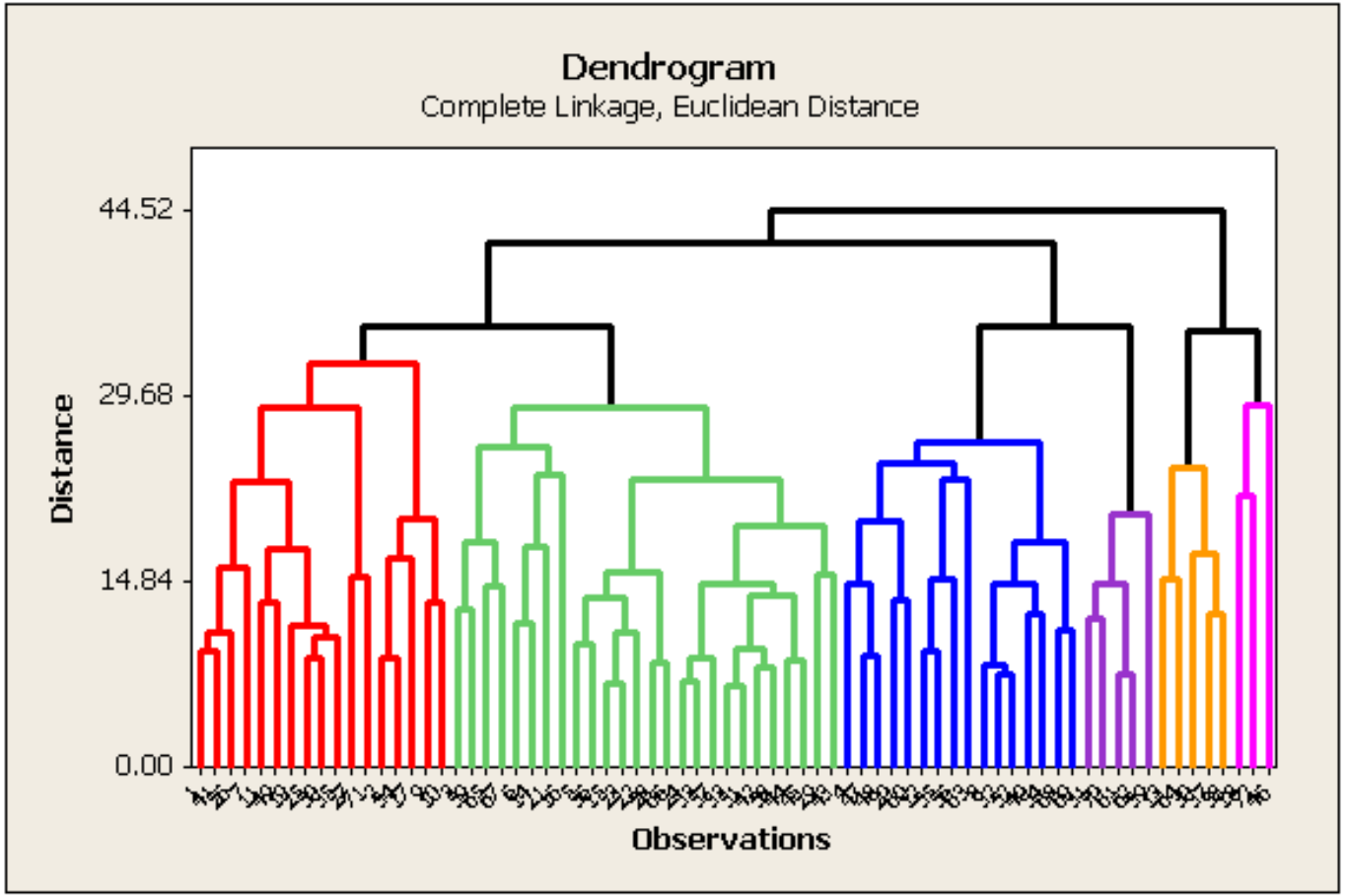
3. DEVIATION FROM OWN PATTERNS (OWN & PEER GROUP)

1. ‘FLAG’ Messages

Univariate Flag Outliers (**MSG1**) - Many Individual Outliers in 1 Week



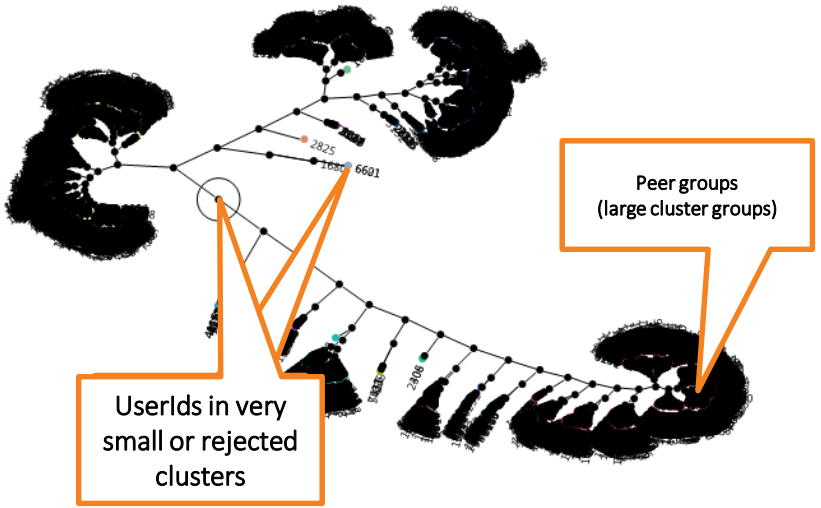
Unsupervised Machine Learning: Cluster Analysis



2. ‘UNUSUAL’ Messages

Multivariate Cluster Anomalies (**MSG 2, 3, 5 & 6**) - Small or Rejected (1 & 6 wks)

Each week all UserIds are run through cluster analysis –
both on ***1 week*** and ***6 weeks*** of aggregated data



“UNUSUAL”
Anomalies surface from cluster analysis

“NORMAL”
Large clusters indicate users behaving in similar ways

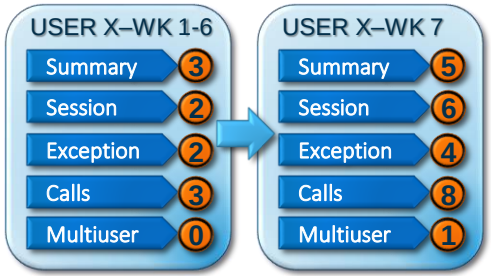
3. ‘CHANGE’ Messages

Latest week against six previous weeks **(MSG 4 & 7)**

Based on 7 consecutive weeks of data, the latest week (wk 7) for each user is compared against:
1) Own average activities in previous 6 weeks
2) Peer group of similar users in previous 6 weeks

This produces:
- Users who far exceed own 6 week averages
- Users who far exceed peer group 6 week avg

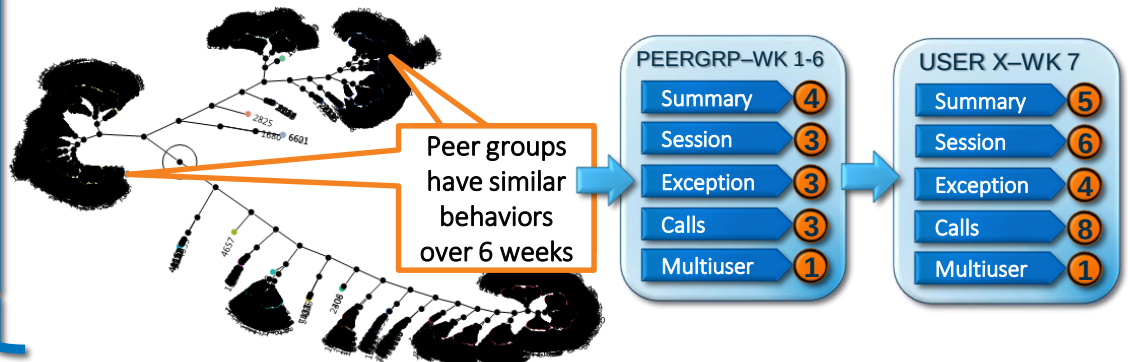
1. OWN DELTA



MSG 4

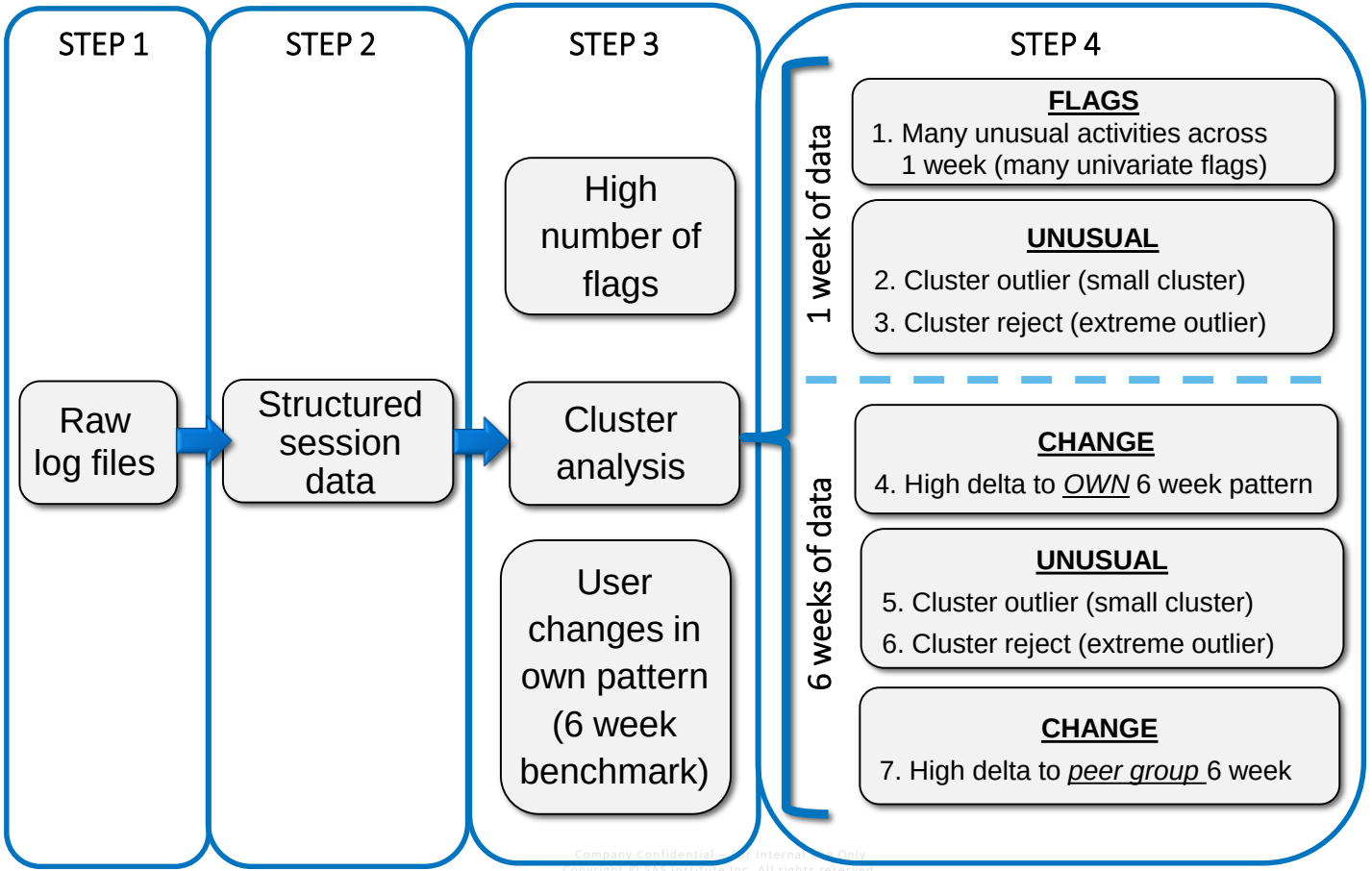
MSG 7

2. PEER GROUP DELTA



Summary Overview

Anomaly Detection Methods

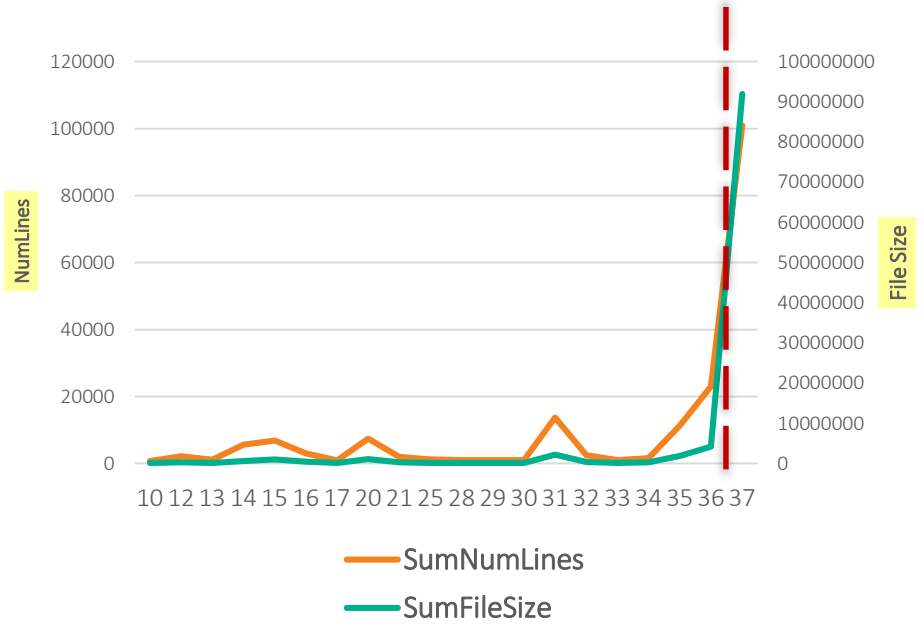


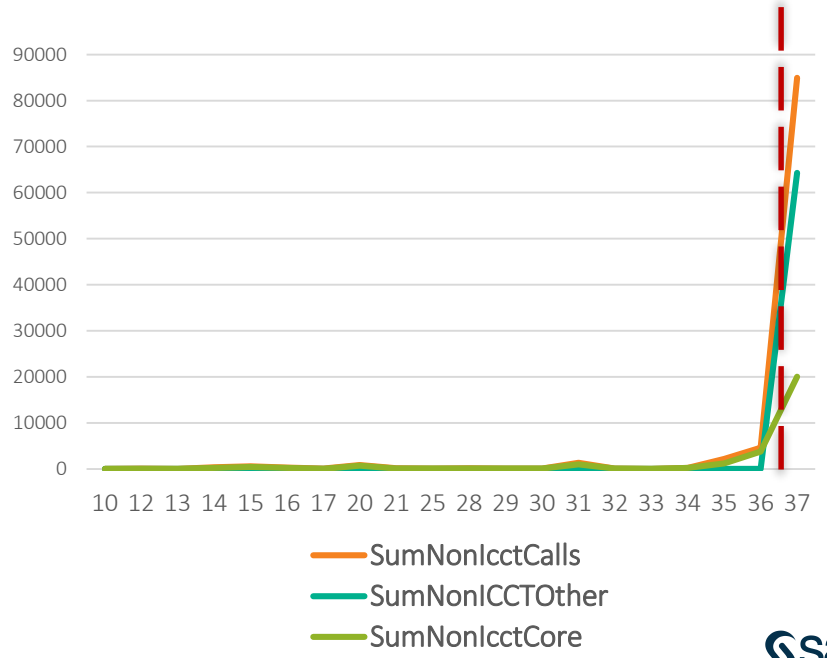

HUMAN
ORGAN
FOR TRANSPLANT

Example Anomalies

Example Anomaly: Red Teaming

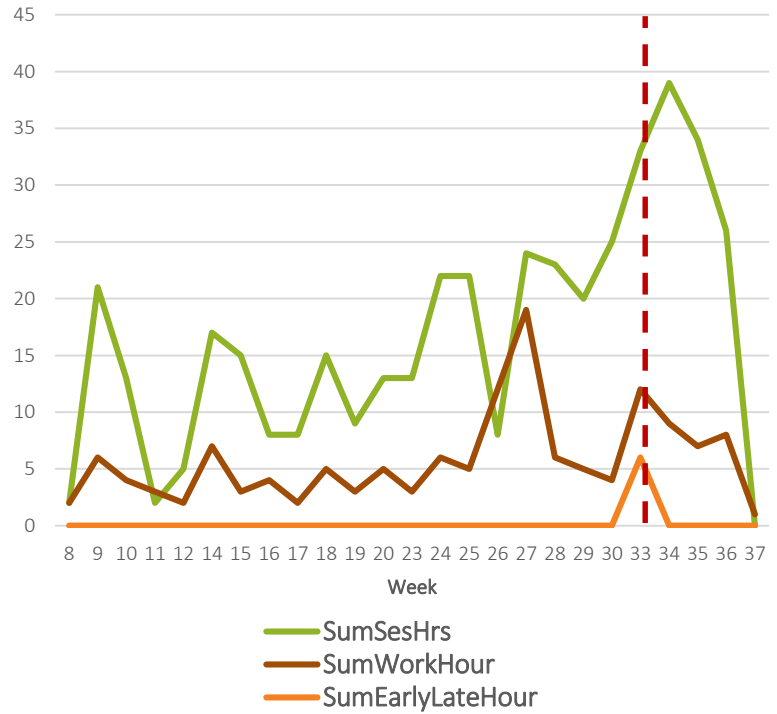
- Alert messages **UNUSUAL (3)** and **CHANGE (4&7)**
- Some of variables showing particular spike:
  Very high session activities, large number of system calls





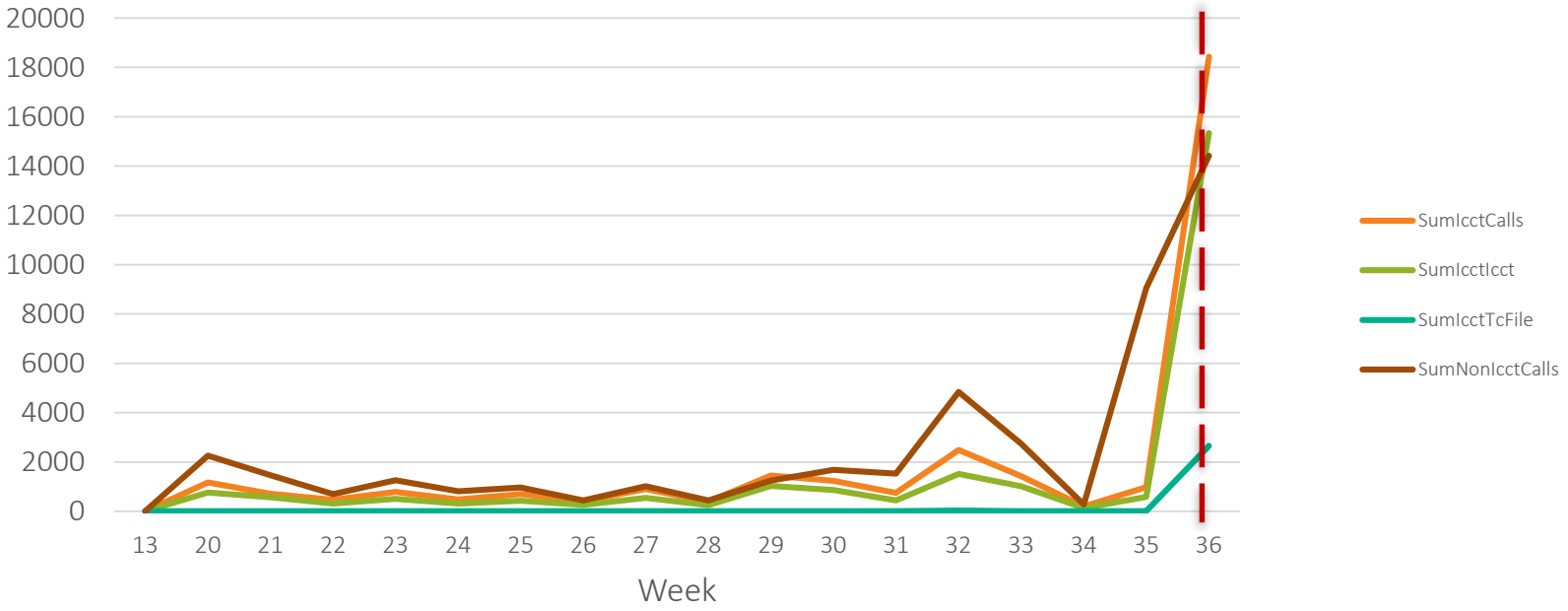
Example Anomaly: Team Leader in Performance Incident

Alerted – **CHANGE** (MSGs 4 & 7)



Example Anomaly: Unusual Behaviour

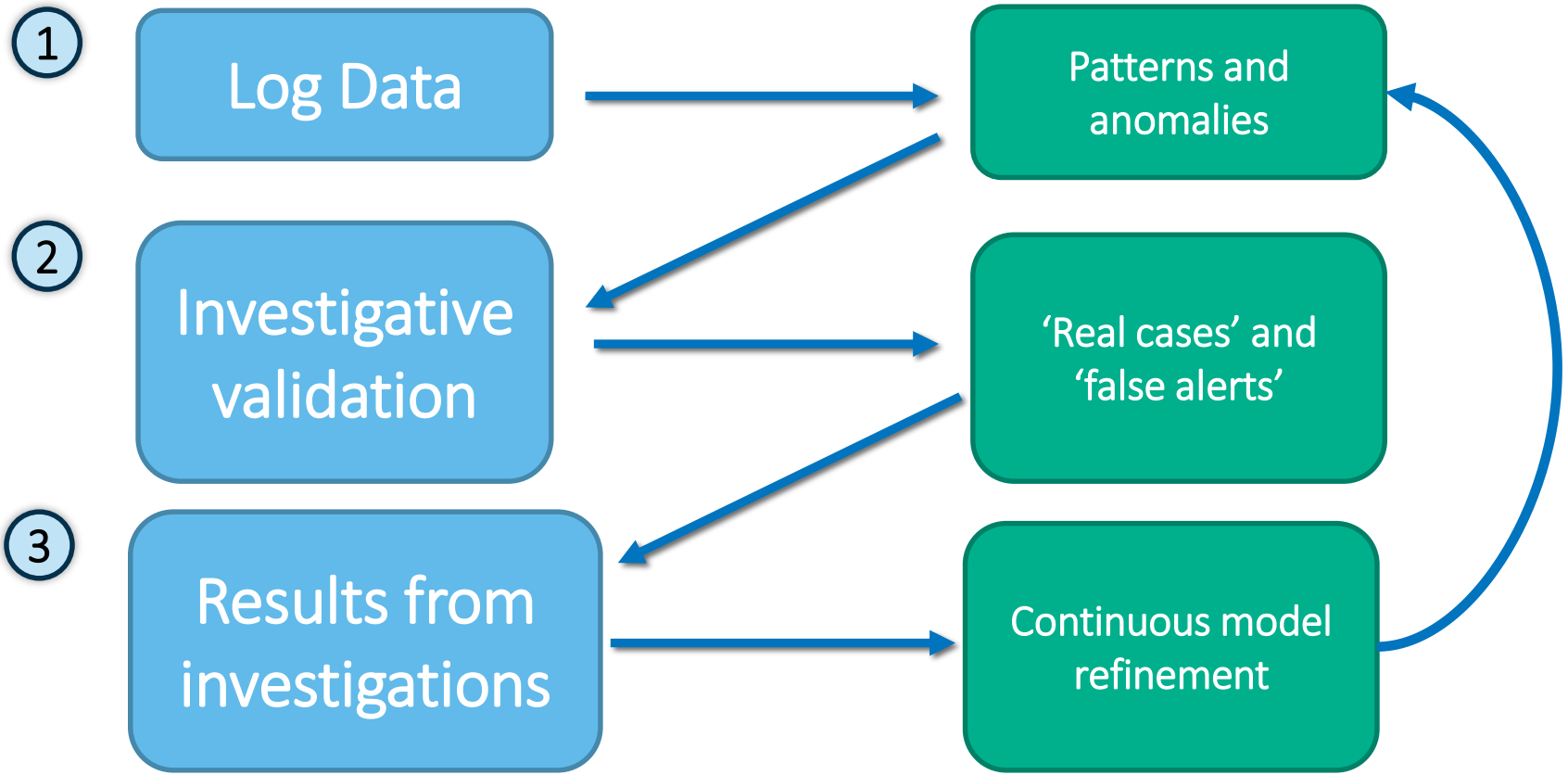
- System calls spike during week 36
- Received alert **UNUSUAL** (MSG 2) on week 36



Conclusion


Auntie Anne's
WAY OUT WEST
NEWSSTAND

Continuous Detection Improvement Process



Scott Mongeau
Certified Analytics Professional (CAP)
MA MA GD MBA PhD (ABD)

+31 68 370 3097

scott.mongeau@sas.com

Scott Mongeau

SARK7

QUESTIONS?

APPENDIX

References

- Aggarwal, C. (2013). “Outlier Analysis.” Springer. http://www.springer.com/la/book/9781461463955
- Kirchhoff, C., Upton, D., and Winnefeld, Jr., Admiral J. A. (2015 October 7). “Defending Your Networks: Lessons from the Pentagon.” Harvard Business Review. Available at https://www.sas.com/en_us/whitepapers/hbr-defending-your-networks-108030.html
- Longitude Research. (2014). “Cyberrisk in banking.” Available at https://www.sas.com/content/dam/SAS/bp_de/doc/studie/ff-st-longitude-research-cyberrisk-in-banking-2316865.pdf
- Ponemon Institute. (2017). “When Seconds Count: How Security Analytics Improves Cybersecurity Defenses.” Available at https://www.sas.com/en_us/whitepapers/ponemon-how-security-analytics-improves-cybersecurity-defenses-108679.html
- SANS Institute. (2015). “2015 Analytics and Intelligence Survey.” Available at https://www.sas.com/en_us/whitepapers/sans-analytics-intelligence-survey-108031.html
- SANS Institute. (2016). “Using Analytics to Predict Future Attacks and Breaches.” Available at https://www.sas.com/en_us/whitepapers/sans-using-analytics-to-predict-future-attacks-breaches-108130.html
- SAS Institute. (2016). “Managing the Analytical Life Cycle for Decisions at Scale.” Available at https://www.sas.com/content/dam/SAS/en_us/doc/whitepaper1/manage-analytical-life-cycle-continuous-innovation-106179.pdf
- SAS Institute. (2017). “SAS Cybersecurity: Counter cyberattacks with your information advantage.” Available at https://www.sas.com/en_us/software/fraud-security-intelligence/cybersecurity-solutions.html
- SAS Institute. (2019). “Data Management for Artificial Intelligence.” Available at www.sas.com/en_us/whitepapers/data-management-artificial-intelligence-109860.html
- Security Brief Magazine. (2016). “Analyze This! Who’s Implementing Security Analytics Now?” Available at https://www.sas.com/en_th/whitepapers/analyze-this-108217.html
- UBM. (2016). “Dark Reading: Close the Detection Deficit with Security Analytics.” Available at https://www.sas.com/en_us/whitepapers/close-detection-deficit-with-security-analytics-108280.html