Cyber Defense Organization

Fall 2020 - Insider Threat

Shadowing

https://forms.gle/Pdjhm2GR8ce4cp8M7

What is an Insider Threat?

- Insider - Current / Former employee, contractor or partner who has / had authorized access to the organization's network, systems or data
- Insider Threat - insider intentionally or unintentionally misuses access to negatively affect the confidentiality, integrity, or availability of the organization's critical information or systems
- People - biggest asset but also your biggest risk

25% of all security incidents involve insiders

⅓ of organizations have faced an insider threat incident

Who are these Insiders?

Employees

- Privileged Users (IT team members)
- Knowledge Workers (Analysts or Developers)
- Resigned or Terminated Employees
- Employees involved in a merger/acquisition

Third Parties

- Vendors
- Contractors
- Partners

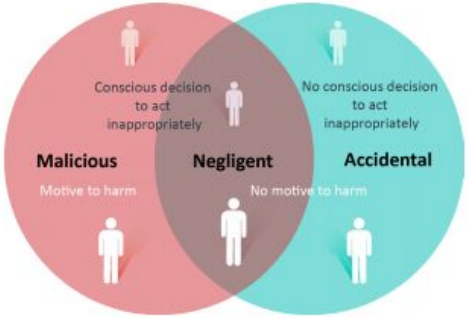
2 Types of Insider Threats

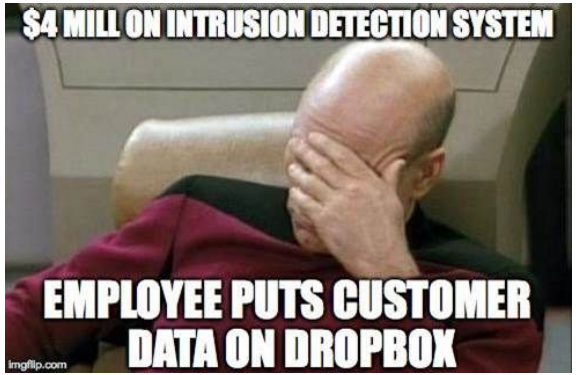
Malicious

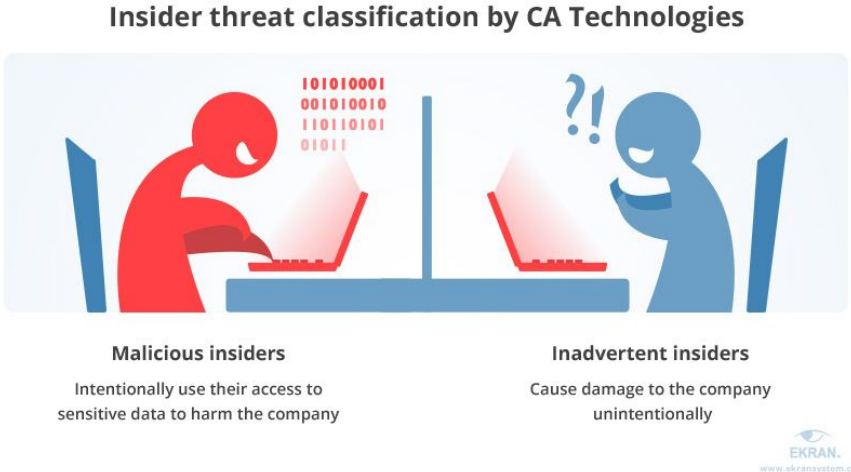
- Sabotage
- Intellectual Property theft
- Espionage
- Fraud

Unintentional

- Human Error
- Bad Judgment
- Phishing
- Malware
- Stolen Credentials







Insider Threat Solutions

1. Detect Insider Threats - uncover alarming user activity by identifying anomalous behavior
2. Investigate Incidents - investigate user activity in minutes
3. Prevent Incidents - reduce risk with real - time user notifications and blocking
4. Protect User Privacy - anonymize user data to protect employee and contractor privacy and meet regulations
5. Satisfy Compliance - meet compliance requirements regarding insider threats
6. Integrate Tools - integrate insider threat detection with SIEMs and other security tools for insight

Security Information and Event Management (SIEM)

Collects and aggregates log data generated throughout an organization's technology infrastructure and analyzes and reports on it

Difficulties with early SIEMs

- Data sets are inflexible so SIEMs couldn't process data from some sources
- Difficult to maintain and operate
- Produces a high number of false positives
- Struggles to keep up with evolving threats

Next Gen SIEMs - offer more variety and volume of data while having a variety of methods to analyze

Next Gen SIEMs

1. Collect Data

Collect data across the organization from various devices such as firewalls, servers, workstations

- Next Gen SIEMs - include integration with cloud infrastructure, enterprise applications, etc

2. Enrich Data

Add context to the event - identity, permissions, geolocation

3. Store Data

Stored within a database

- Next Gen SIEM - big data infrastructure & unlimited scalability

Next Gen SIEMs

4. Apply Correlation and Analytics

Draw conclusions from the data and find anomalies

Next Gen SIEMs - advanced analytic techniques

- Machine Learning
- User and Entity Behavior Analytics (UEBA)
- Threat Chain Models

5. Investigate and Mitigate Threats

Security Orchestration, Automation, and Response (SOAR)

- Assist analysts in investigations by providing a workbench to respond to security events

6. Provide Data Insights and Reporting

Search within database quickly and visualize data with dashboards

Securonix

- Next Generation SIEM - includes log management, behavior analytics-based threat detection and automated incident response within one platform

SECURONIX

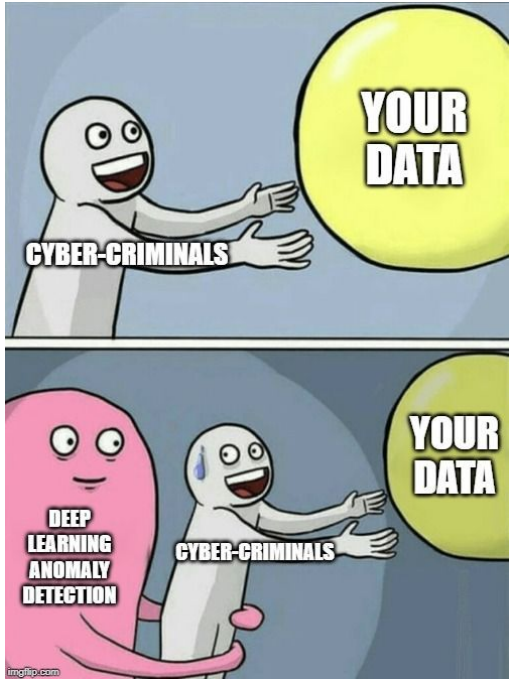
Why is this helpful for Insider Threats?

Attackers don't need to penetrate the network, they are already inside of it

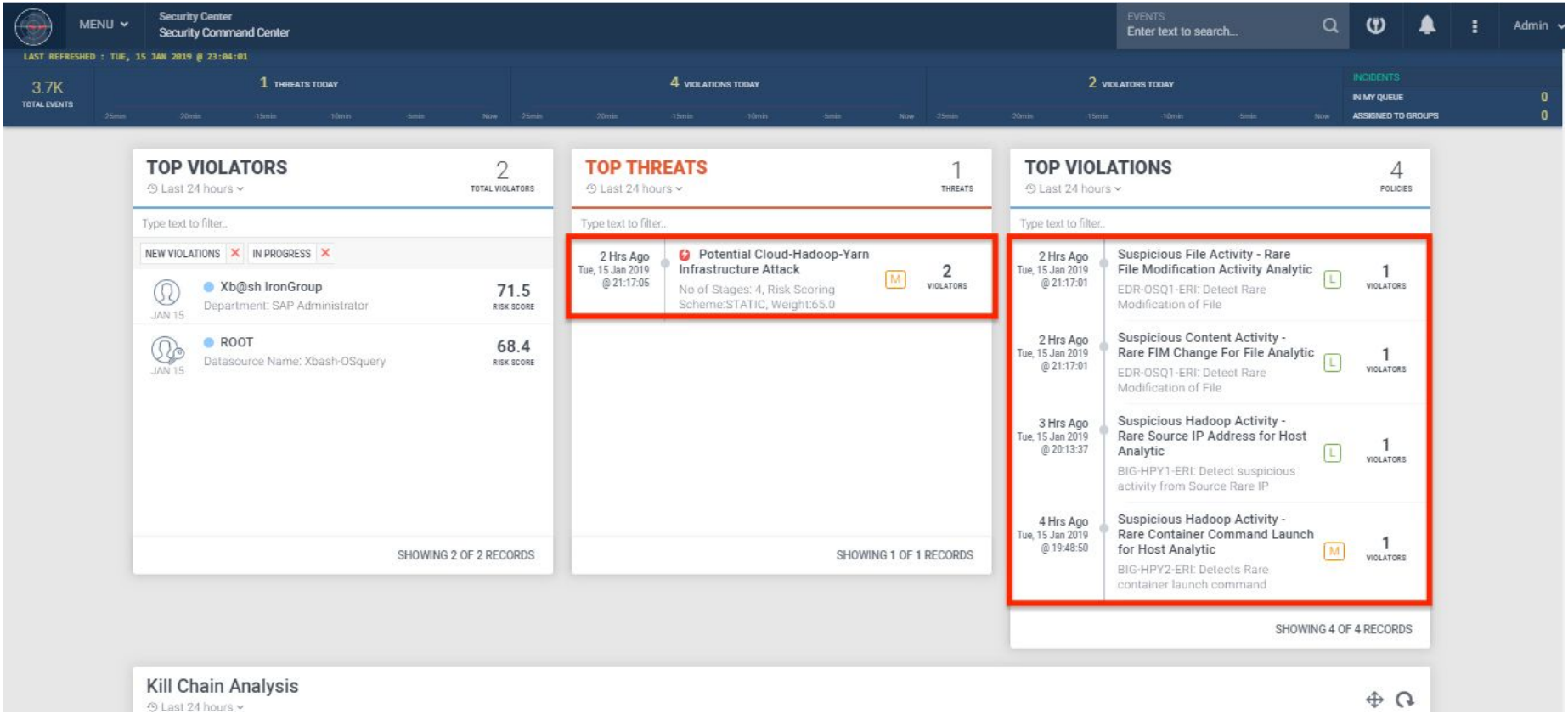
Behavior-based analytics techniques

- Establishes behavioral profiles for each user, peer group, department, etc
- Detects variations in normal patterns against these groups

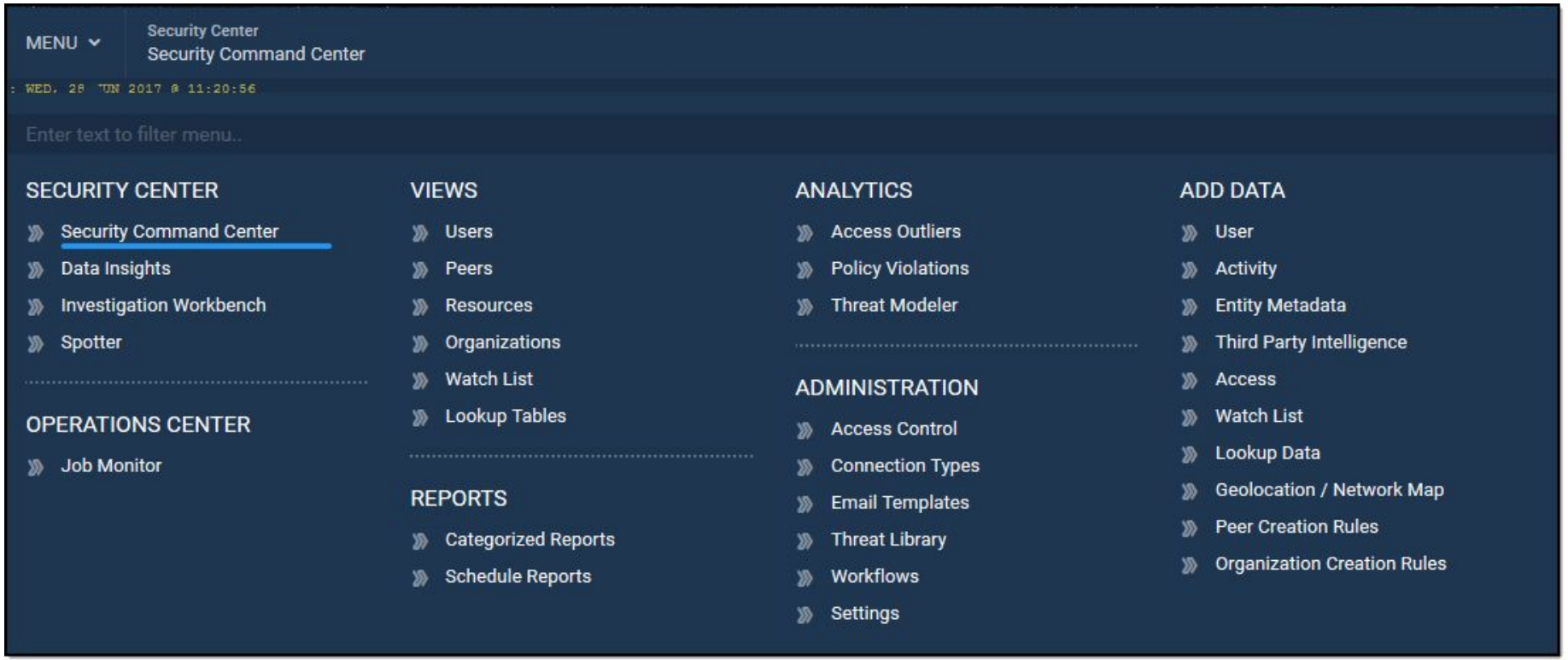
Super helpful way to accomplish this is through Policy Violations!



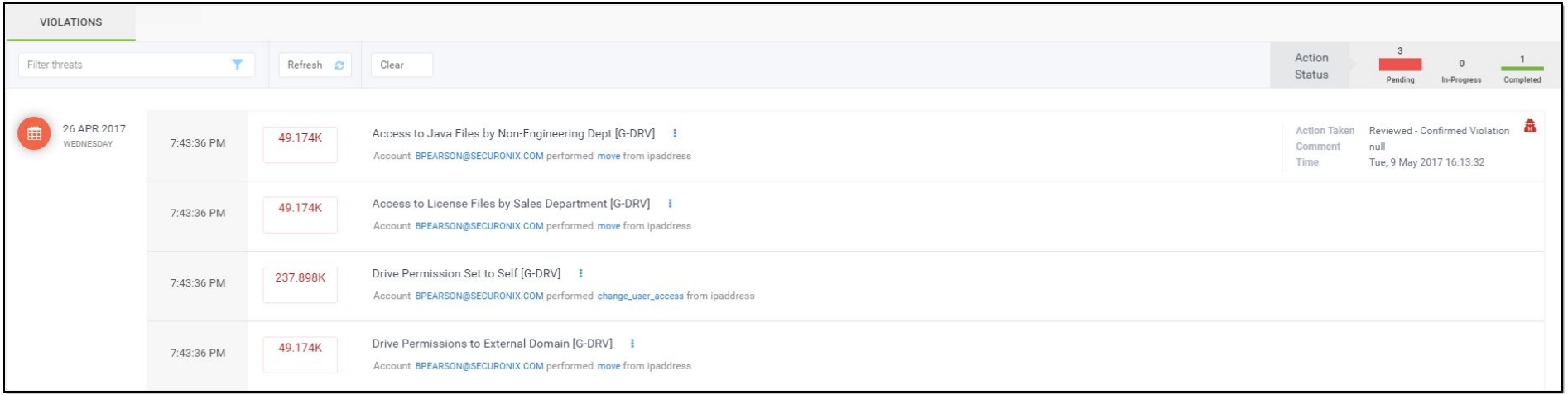
Securonix


MENU
Security Center
Security Command Center
EVENTS
Enter text to search...
Admin
LAST REFRESHED : TUE, 15 JAN 2019 @ 23:04:01
3.7K
TOTAL EVENTS
1 THREATS TODAY
4 VIOLATIONS TODAY
2 VIOLATORS TODAY
INCIDENTS
IN MY QUEUE 0
ASSIGNED TO GROUPS 0
TOP VIOLATORS
Last 24 hours
2
TOTAL VIOLATORS
Type text to filter..
NEW VIOLATIONS
IN PROGRESS
JAN 15
Xb@sh IronGroup
Department: SAP Administrator
71.5
RISK SCORE
JAN 15
ROOT
Datasource Name: Xbash-OSquery
68.4
RISK SCORE
SHOWING 2 OF 2 RECORDS
TOP THREATS
Last 24 hours
1
THREATS
Type text to filter..
2 Hrs Ago
Tue, 15 Jan 2019
@ 21:17:05
Potential Cloud-Hadoop-Yarn Infrastructure Attack
No of Stages: 4, Risk Scoring Scheme:STATIC, Weight:65.0
M
2
VIOLATORS
SHOWING 1 OF 1 RECORDS
TOP VIOLATIONS
Last 24 hours
4
POLICIES
Type text to filter..
2 Hrs Ago
Tue, 15 Jan 2019
@ 21:17:01
Suspicious File Activity - Rare File Modification Activity Analytic
EDR-OSQ1-ERI: Detect Rare Modification of File
L
1
VIOLATORS
2 Hrs Ago
Tue, 15 Jan 2019
@ 21:17:01
Suspicious Content Activity - Rare FIM Change For File Analytic
EDR-OSQ1-ERI: Detect Rare Modification of File
L
1
VIOLATORS
3 Hrs Ago
Tue, 15 Jan 2019
@ 20:13:37
Suspicious Hadoop Activity - Rare Source IP Address for Host Analytic
BIG-HPY1-ERI: Detect suspicious activity from Source Rare IP
L
1
VIOLATORS
4 Hrs Ago
Tue, 15 Jan 2019
@ 19:48:50
Suspicious Hadoop Activity - Rare Container Command Launch for Host Analytic
BIG-HPY2-ERI: Detects Rare container launch command
M
1
VIOLATORS
SHOWING 4 OF 4 RECORDS
Kill Chain Analysis
Last 24 hours

Securonix


MENU
Security Center
Security Command Center
: WED, 28 JUN 2017 @ 11:20:56
Enter text to filter menu..
SECURITY CENTER
Security Command Center
Data Insights
Investigation Workbench
Spotter
OPERATIONS CENTER
Job Monitor
VIEWS
Users
Peers
Resources
Organizations
Watch List
Lookup Tables
REPORTS
Categorized Reports
Schedule Reports
ANALYTICS
Access Outliers
Policy Violations
Threat Modeler
ADMINISTRATION
Access Control
Connection Types
Email Templates
Threat Library
Workflows
Settings
ADD DATA
User
Activity
Entity Metadata
Third Party Intelligence
Access
Watch List
Lookup Data
Geolocation / Network Map
Peer Creation Rules
Organization Creation Rules

Policy Violations

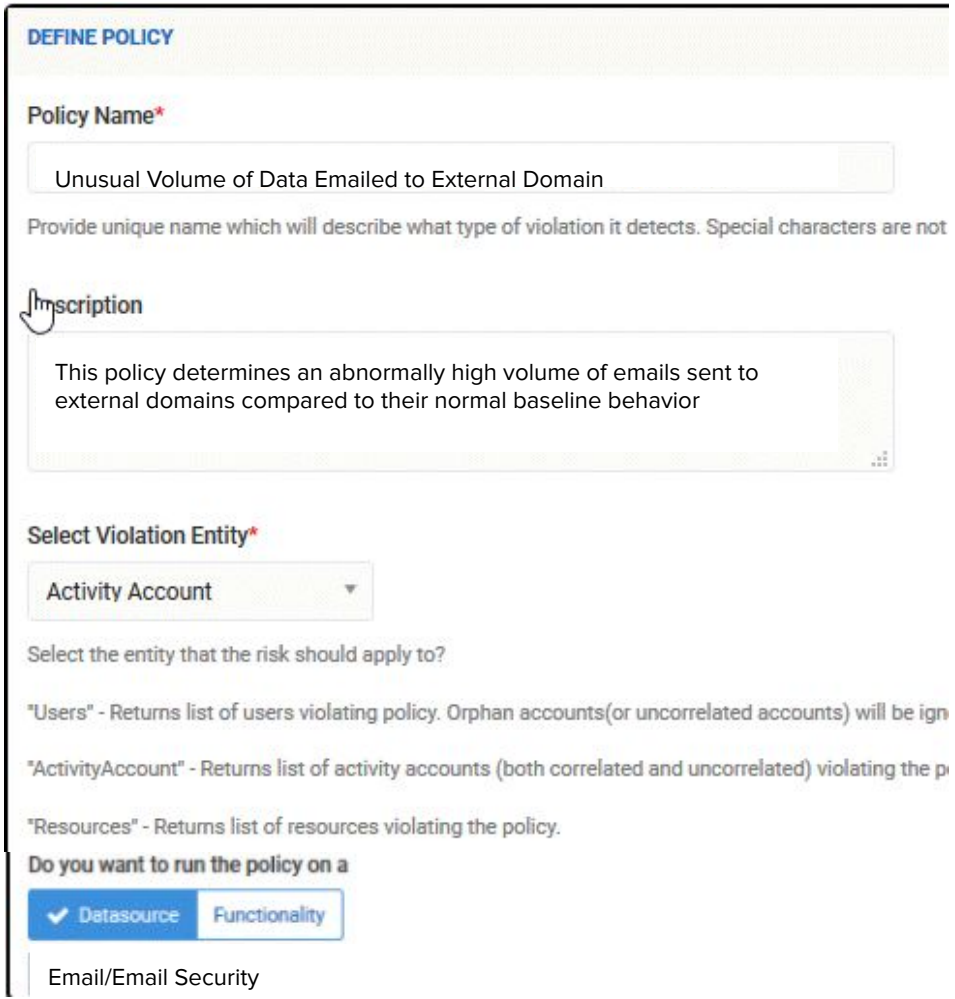


Examples of Policies:

1. Uploading confidential information to a remote site
2. BCC email to a personal email address that contains critical information
3. Employees with upcoming terminations within 30 days
4. Successful login from unusual geographic area

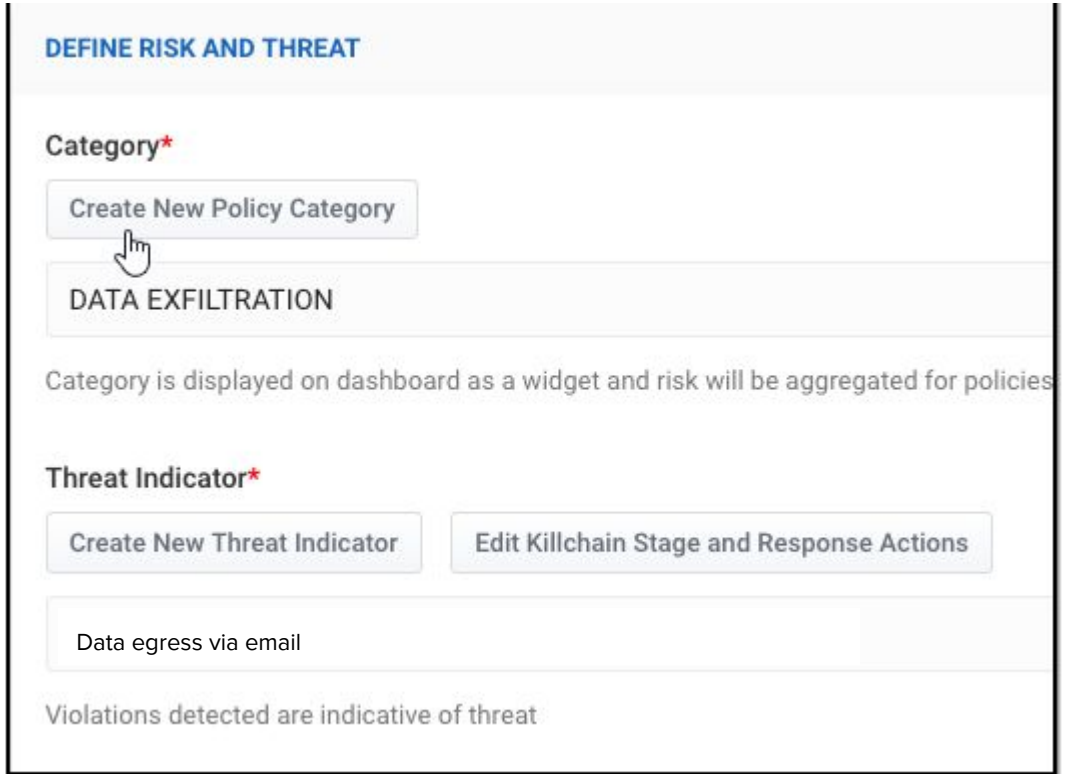
Policy Violations

Policy: Unusual volume of data emailed to external domain



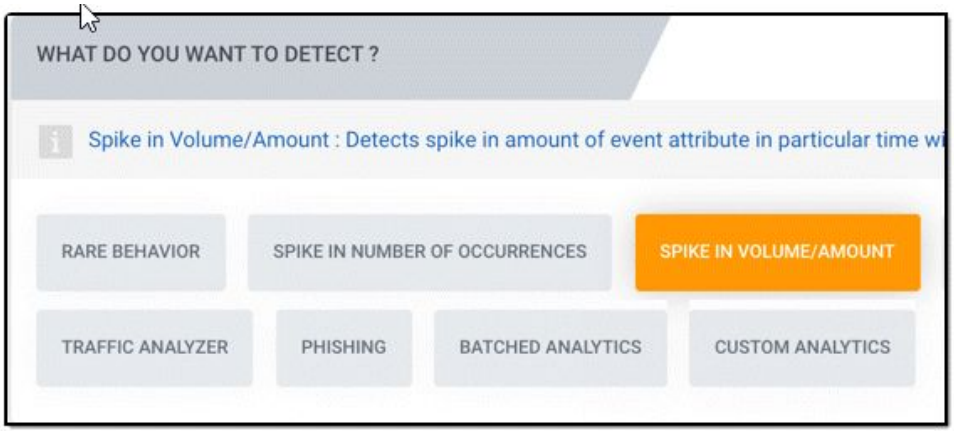
Policy Violations

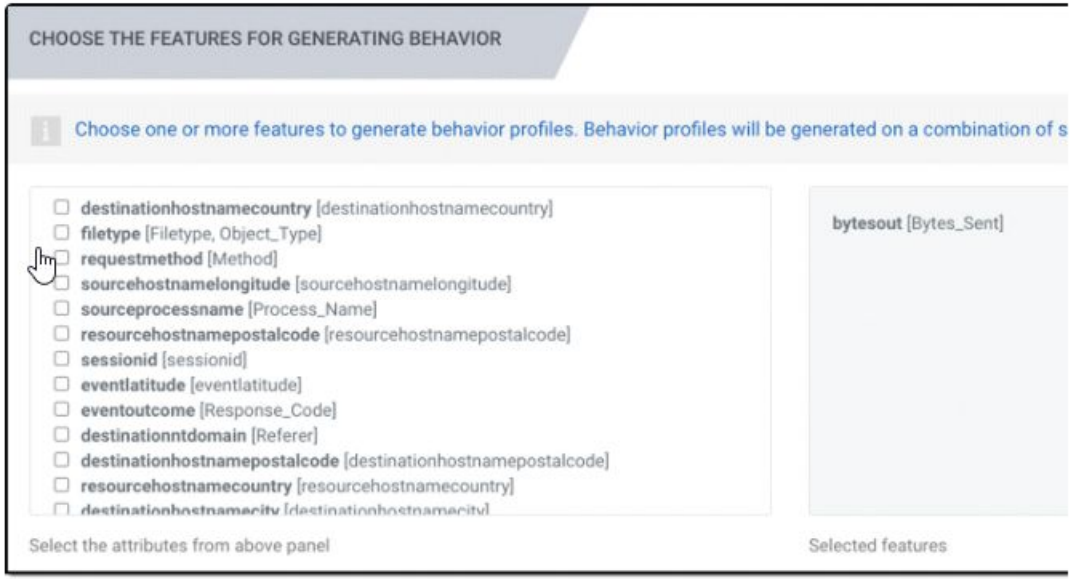
Policy: Unusual volume of data emailed to external domain



Policy Violations

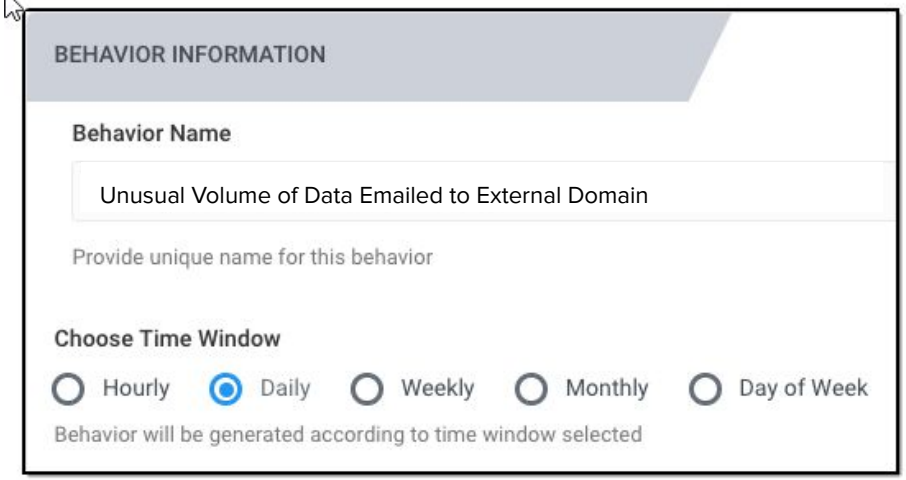
Policy: Unusual volume of data emailed to external domain

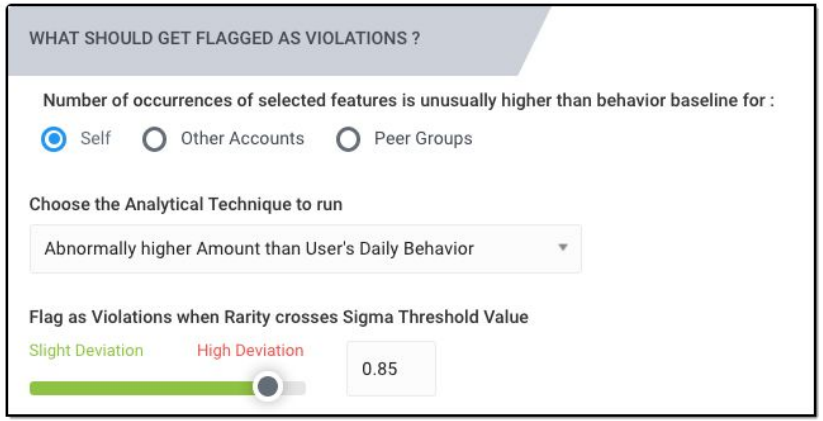


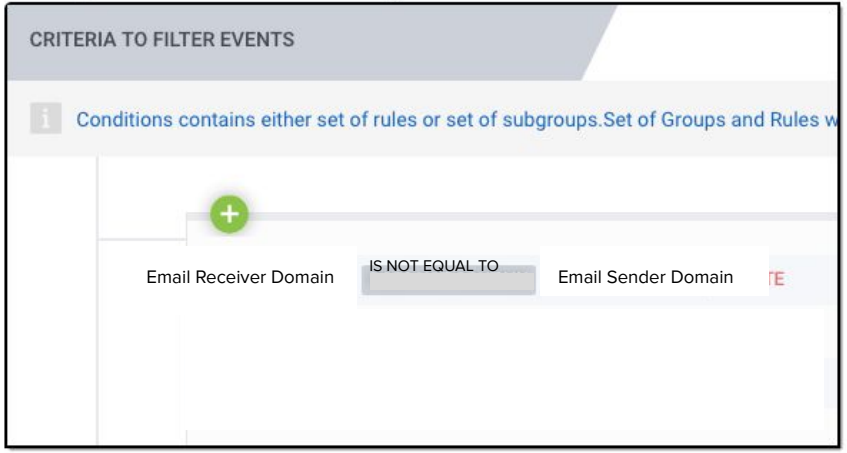


Policy Violations

Policy: Unusual volume of data emailed to external domain

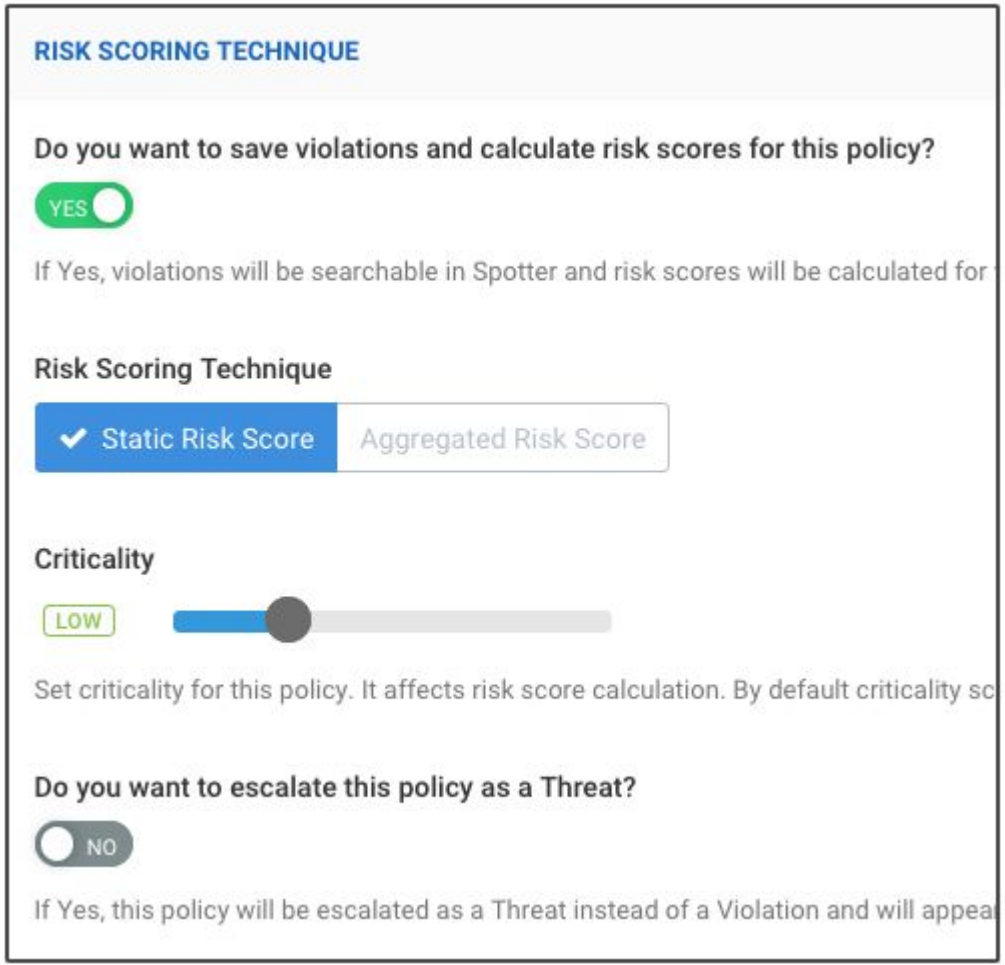




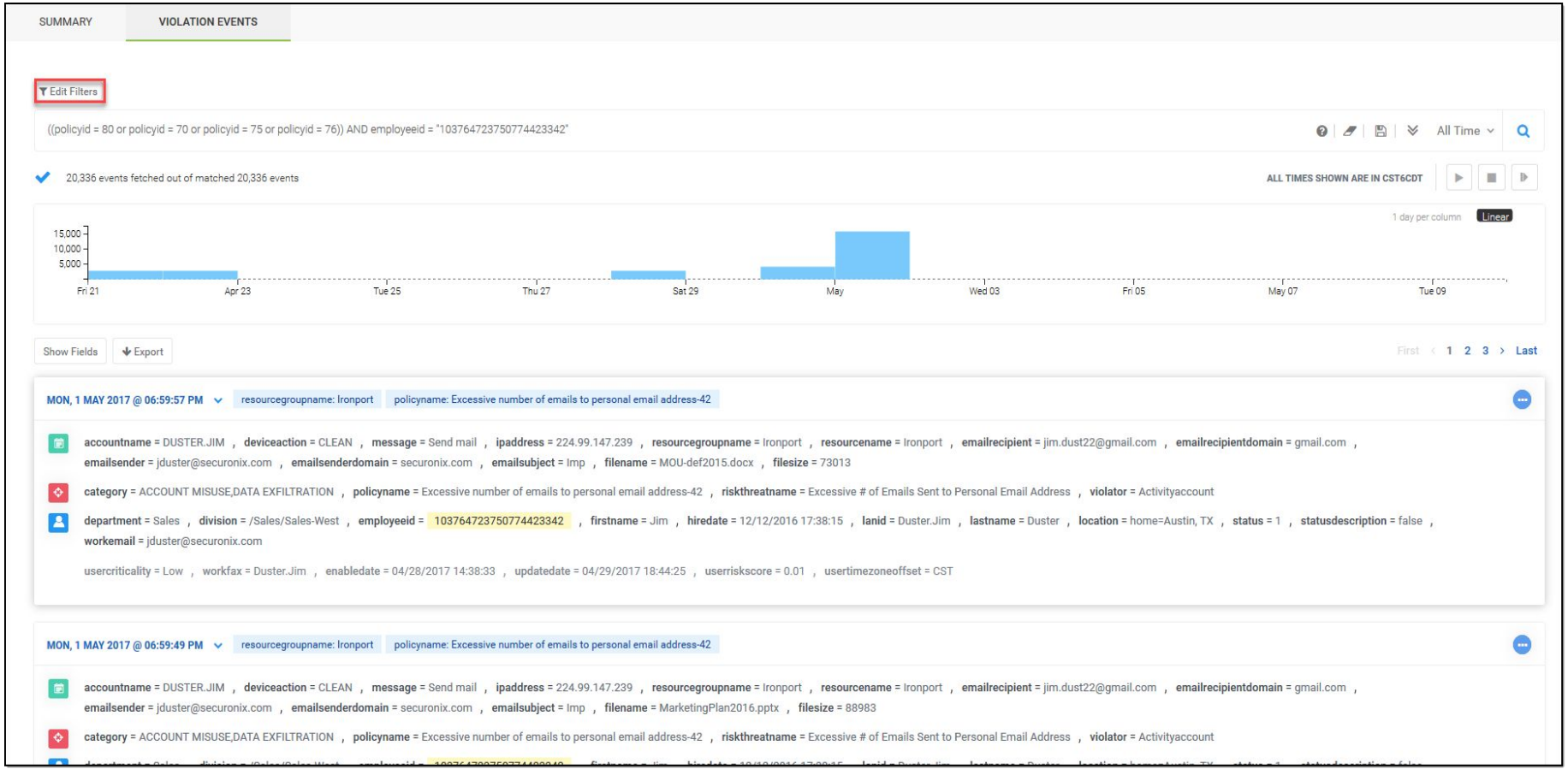


Policy Violations

Policy: Unusual volume of data emailed to external domain



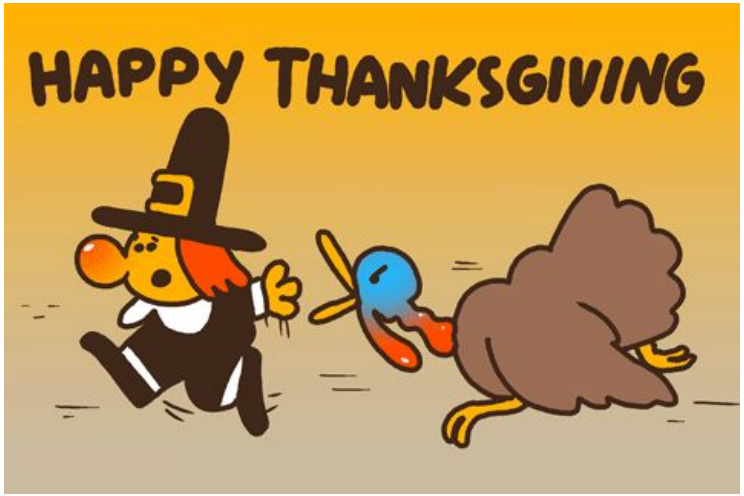
Policy Violation



Free SIEM training!

https://education.splunk.com/course/splunk-7x-fundamentals-part-1-elearning

No Events Next week



Add us on Social Media!

Twitter: **@ualbanyCDO**

Instagram: **ualbany_cdo**

Website: **uacyber.org**

Myinvolvement: **Cyber Defense Org**

We have a discord!