

# 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

$\frac{1}{3}$  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

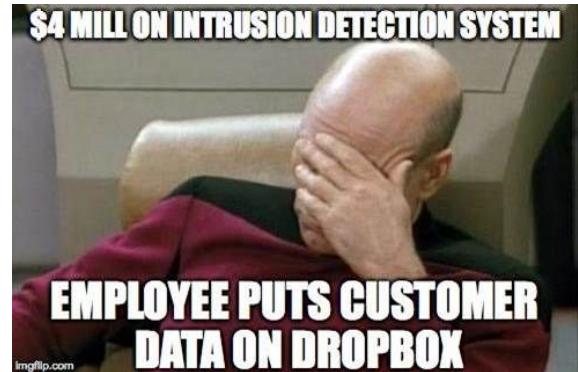
- Vendors
- Contractors
- Partners



# 2 Types of Insider Threats

## Malicious

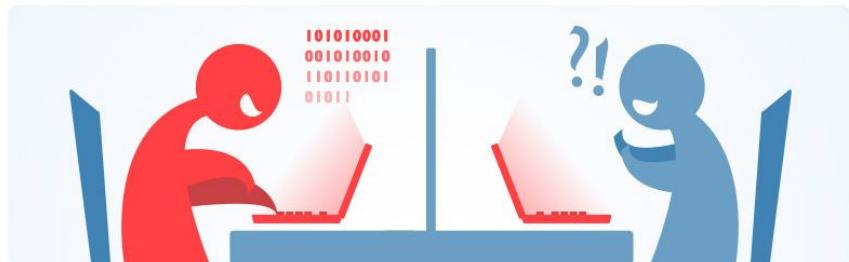
- Sabotage
- Intellectual Property theft
- Espionage
- Fraud



## Unintentional

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

Insider threat classification by CA Technologies



Malicious insiders

Intentionally use their access to sensitive data to harm the company

Inadvertent insiders

Cause damage to the company unintentionally

# **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

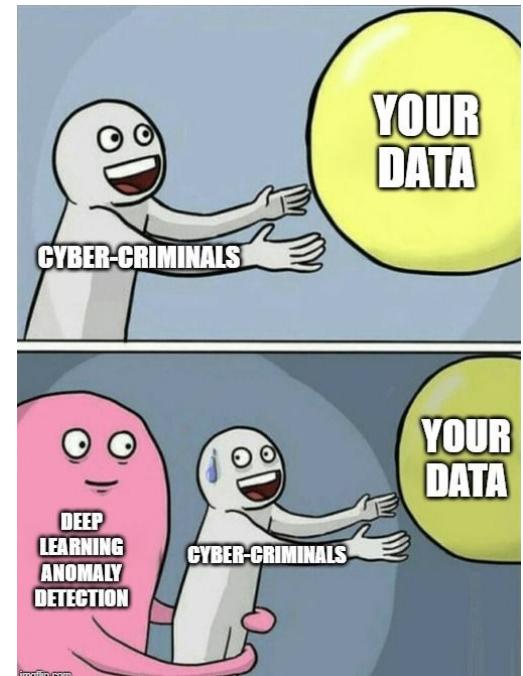
## Why is this helpful for Insider Threats?

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 LAST REFRESHED : TUE, 15 JAN 2019 @ 23:04:01

3.7K TOTAL EVENTS 1 THREATS TODAY 4 VIOLATIONS TODAY 2 VIOLATORS TODAY

EVENTS Enter text to search... INCIDENTS IN MY QUEUE ASSIGNED TO GROUPS

Admin

### TOP VIOLATORS

⌚ Last 24 hours ▾ 2 TOTAL VIOLATORS

Type text to filter...

<span>NEW VIOLATIONS</span> X	<span>IN PROGRESS</span> X
-------------------------------	----------------------------

 Xb@sh IronGroup Department: SAP Administrator JAN 15 RISK SCORE 71.5

 ROOT Datasource Name: Xbash-OQuery JAN 15 RISK SCORE 68.4

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	<span>Potential Cloud-Hadoop-Yarn Infrastructure Attack</span> No of Stages: 4, Risk Scoring Scheme:STATIC, Weight:65.0	 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	 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	 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	 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	 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

VIOLATIONS				Action Status	3 Pending	0 In-Progress	1 Completed
<input type="button" value="Filter threats"/>	<input type="button" value="Refresh"/>	<input type="button" value="Clear"/>					
 26 APR 2017 WEDNESDAY	7:43:36 PM	<span style="background-color: #f08080; border: 1px solid black; padding: 2px;">49.174K</span>	Access to Java Files by Non-Engineering Dept [G-DRV] 	Account <a href="#">BPEARSON@SECURONIX.COM</a> performed <a href="#">move</a> from ipaddress	Action Taken	Reviewed - Confirmed Violation	
	7:43:36 PM	<span style="background-color: #f08080; border: 1px solid black; padding: 2px;">49.174K</span>	Access to License Files by Sales Department [G-DRV] 	Account <a href="#">BPEARSON@SECURONIX.COM</a> performed <a href="#">move</a> from ipaddress	Comment	null	
	7:43:36 PM	<span style="background-color: #f08080; border: 1px solid black; padding: 2px;">237.898K</span>	Drive Permission Set to Self [G-DRV] 	Account <a href="#">BPEARSON@SECURONIX.COM</a> performed <a href="#">change_user_access</a> from ipaddress	Time	Tue, 9 May 2017 16:13:32	
	7:43:36 PM	<span style="background-color: #f08080; border: 1px solid black; padding: 2px;">49.174K</span>	Drive Permissions to External Domain [G-DRV] 	Account <a href="#">BPEARSON@SECURONIX.COM</a> performed <a href="#">move</a> from ipaddress			

## 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

**DEFINE POLICY**

**Policy Name\***

Unusual Volume of Data Emailed to External Domain

Provide unique name which will describe what type of violation it detects. Special characters are not allowed.

**Description**

This policy determines an abnormally high volume of emails sent to external domains compared to their normal baseline behavior

**Select Violation Entity\***

Activity Account

Select the entity that the risk should apply to?

"Users" - Returns list of users violating policy. Orphan accounts(or uncorrelated accounts) will be ignored.

"ActivityAccount" - Returns list of activity accounts (both correlated and uncorrelated) violating the policy.

"Resources" - Returns list of resources violating the policy.

**Do you want to run the policy on a**

Datasource    Functionality

Email/Email Security

# Policy Violations

Policy: Unusual volume of data emailed to external domain

## DEFINE RISK AND THREAT

### Category\*

Create New Policy Category



DATA EXFILTRATION

Category is displayed on dashboard as a widget and risk will be aggregated for policies

### Threat Indicator\*

Create New Threat Indicator

Edit Killchain Stage and Response Actions

Data egress via email

Violations detected are indicative of threat

# Policy Violations

Policy: Unusual volume of data emailed to external domain

WHAT DO YOU WANT TO DETECT ?

**Spike in Volume/Amount : Detects spike in amount of event attribute in particular time window.**

RARE BEHAVIOR   SPIKE IN NUMBER OF OCCURRENCES   **SPIKE IN VOLUME/AMOUNT**

TRAFFIC ANALYZER   PHISHING   BATCHED ANALYTICS   CUSTOM ANALYTICS



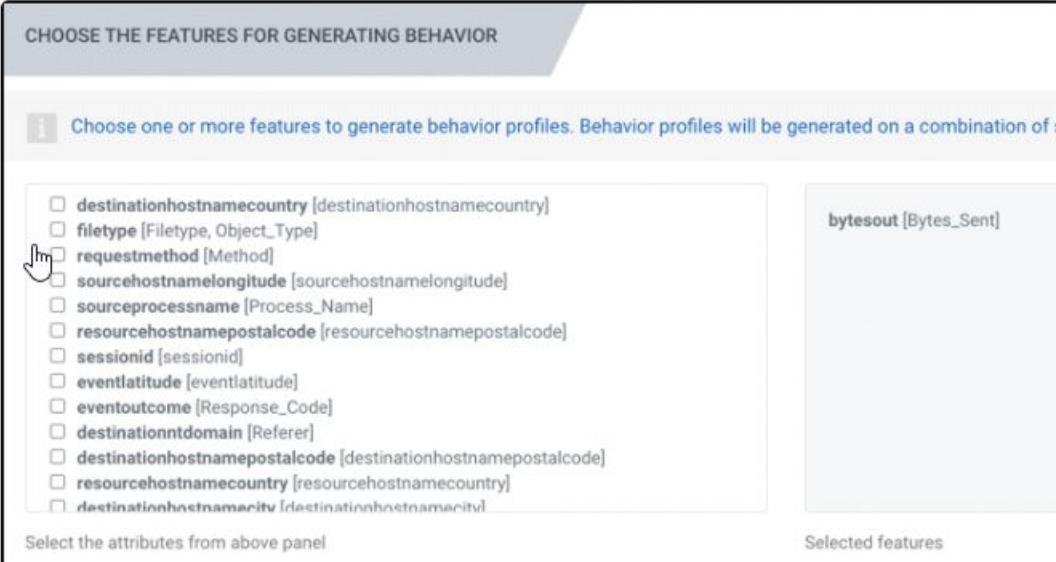
CHOOSE THE FEATURES FOR GENERATING BEHAVIOR

Choose one or more features to generate behavior profiles. Behavior profiles will be generated on a combination of selected features.

destinationhostnamecountry [destinationhostnamecountry]  
 filetype [Filetype, Object\_Type]  
 requestmethod [Method]  
 sourcehostnamelongitude [sourcehostnamelongitude]  
 sourceprocessname [Process\_Name]  
 resourcehostnamepostalcode [resourcehostnamepostalcode]  
 sessionid [sessionid]  
 eventlatitude [eventlatitude]  
 eventoutcome [Response\_Code]  
 destinationntdomain [Referer]  
 destinationhostnamepostalcode [destinationhostnamepostalcode]  
 resourcehostnamecountry [resourcehostnamecountry]  
 destinationhostnamecity [destinationhostnamecity]

**bytesout [Bytes\_Sent]**

Select the attributes from above panel      Selected features



# Policy Violations

Policy: Unusual volume of data emailed to external domain

**BEHAVIOR INFORMATION**

**Behavior Name**

Unusual Volume of Data Emailed to External Domain

Provide unique name for this behavior

**Choose Time Window**

Hourly    Daily    Weekly    Monthly    Day of Week

Behavior will be generated according to time window selected

WHAT SHOULD GET FLAGGED AS VIOLATIONS ?

Number of occurrences of selected features is unusually higher than behavior baseline for :

Self    Other Accounts    Peer Groups

Choose the Analytical Technique to run

Abnormally higher Amount than User's Daily Behavior

Flag as Violations when Rarity crosses Sigma Threshold Value

Slight Deviation   High Deviation   0.85

**CRITERIA TO FILTER EVENTS**

i Conditions contains either set of rules or set of subgroups. Set of Groups and Rules w

+ Email Receiver Domain IS NOT EQUAL TO Email Sender Domain RE

# Policy Violations

Policy: Unusual volume of data emailed to external domain

## RISK SCORING TECHNIQUE

Do you want to save violations and calculate risk scores for this policy?

YES

If Yes, violations will be searchable in Spotter and risk scores will be calculated for

### Risk Scoring Technique

Static Risk Score

Aggregated Risk Score

### Criticality

LOW



Set criticality for this policy. It affects risk score calculation. By default criticality sc

Do you want to escalate this policy as a Threat?

NO

If Yes, this policy will be escalated as a Threat instead of a Violation and will appear

# Policy Violation

SUMMARY VIOLATION EVENTS

[Edit Filters](#)

((policyid = 80 or policyid = 70 or policyid = 75 or policyid = 76)) AND employeeid = "103764723750774423342"

20,336 events fetched out of matched 20,336 events

ALL TIMES SHOWN ARE IN CST6CDT

1 day per column Linear

Fri 21 Apr 23 Tue 25 Thu 27 Sat 29 May Wed 03 Fri 05 May 07 Tue 09

Show Fields Export First < 1 2 3 > Last

MON, 1 MAY 2017 @ 06:59:57 PM resourcegroupname: Ironport policymame: Excessive number of emails to personal email address-42

accountname = DUSTER.JIM , deviceaction = CLEAN , message = Send mail , ipaddress = 224.99.147.239 , resourcegroupname = Ironport , resourcename = Ironport , emailrecipient = jim.dust22@gmail.com , emailrecipientdomain = gmail.com , emailsender = jduster@securonix.com , emailsenderdomain = securonix.com , emailsubject = Imp , filename = MOU-def2015.docx , filesize = 73013

category = ACCOUNT MISUSE,DATA EXFILTRATION , policymame = Excessive number of emails to personal email address-42 , riskthreatname = Excessive # of Emails Sent to Personal Email Address , violator = Activityaccount

department = Sales , division = /Sales/Sales-West , employeeid = 103764723750774423342 , firstname = Jim , hiredate = 12/12/2016 17:38:15 , lanid = Duster.Jim , lastname = Duster , location = home=Austin, TX , status = 1 , statusdescription = false , workemail = jduster@securonix.com

usercriticality = Low , workfax = Duster.Jim , enabledate = 04/28/2017 14:38:33 , updatedate = 04/29/2017 18:44:25 , useriskscore = 0.01 , usertimezoneoffset = CST

MON, 1 MAY 2017 @ 06:59:49 PM resourcegroupname: Ironport policymame: Excessive number of emails to personal email address-42

accountname = DUSTER.JIM , deviceaction = CLEAN , message = Send mail , ipaddress = 224.99.147.239 , resourcegroupname = Ironport , resourcename = Ironport , emailrecipient = jim.dust22@gmail.com , emailrecipientdomain = gmail.com , emailsender = jduster@securonix.com , emailsenderdomain = securonix.com , emailsubject = Imp , filename = MarketingPlan2016.pptx , filesize = 88983

category = ACCOUNT MISUSE,DATA EXFILTRATION , policymame = Excessive number of emails to personal email address-42 , riskthreatname = Excessive # of Emails Sent to Personal Email Address , violator = Activityaccount

# **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](https://twitter.com/ualbanyCDO)



Instagram: [ualbany\\_cdo](https://www.instagram.com/ualbany_cdo)



Website: [uacyber.org](https://uacyber.org)



Myinvolvement: **Cyber Defense Org**

We have a discord!

