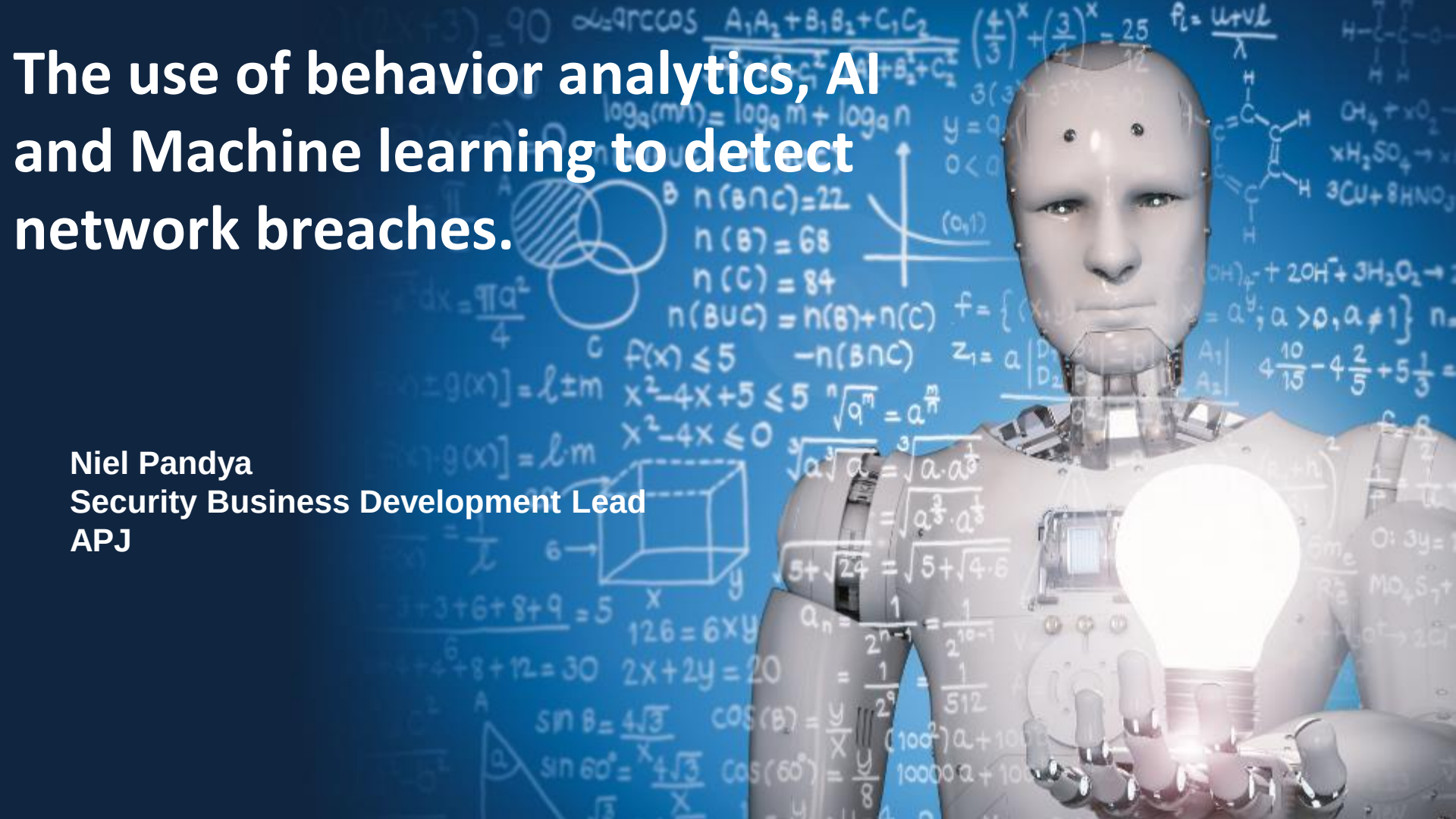
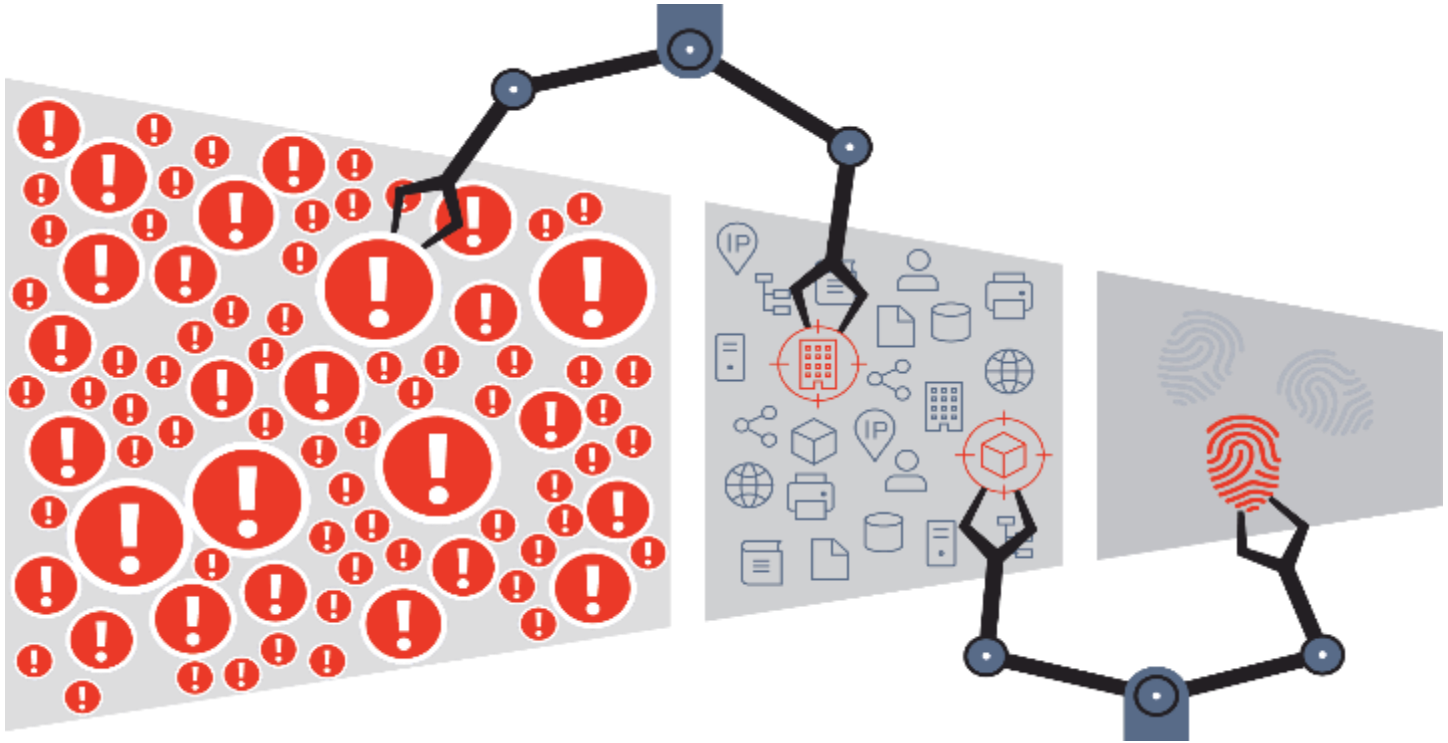
The use of behavior analytics, AI and Machine learning to detect network breaches.



Niel Pandya
Security Business Development Lead
APJ

What Interset Does: Detect Threats within the network based on behavior

Billions of Events → Hundreds of Anomalies → A Handful of Prioritized Threat Leads



Interset

An outside attacker has only a minimal understanding of a compromised account's access levels and the target data's location.
Because of this, an outside attacker attempting to complete reconnaissance and lateral movement stages of an attack will look very different from **normal** users.

Select the right tool for the job

Data Breach

- Data Staging
- Data Exfiltration
- Email Exfiltration
- Print Exfiltration
- USB Exfiltration
- Unusual data access
- Unusual uploads

Advanced Threat

- Compromised Account
- C2 Activity Detection
- Impossible Journeys
- Internal Recon
- Dormant Account
- Unusual Traffic
- Password Manipulation
- Abnormal Processess
- Unusual Applications
- Infected Host
- Malicious Tunneling
- Bot Detection

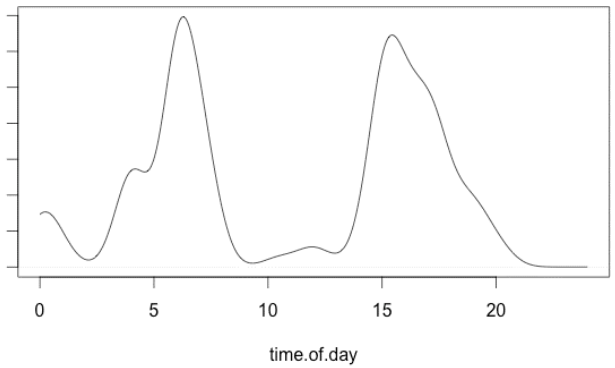
IP Theft

- Mooching
- Snooping
- Interactions with dormant resources/files
- High Risk IP/Data Access
- Lateral Movement

Fraud

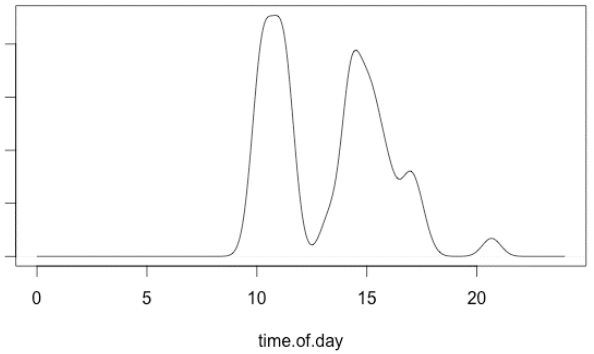
- Transaction Abuse
- Expense Fraud

Working hours (like most behaviors) vary from person to person



Employee 1

- Starts work fairly early in morning
- Early lunch break
- Sometimes works past midnight



Employee 2

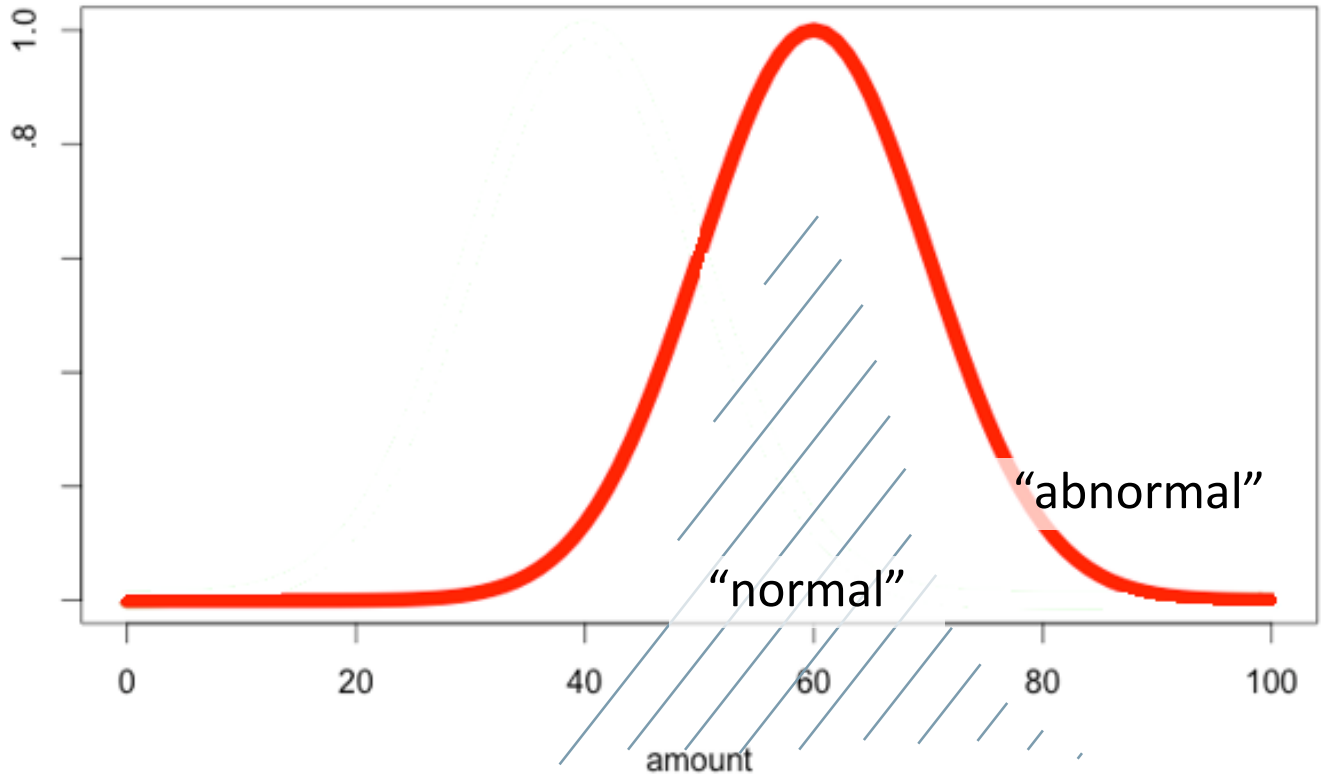
- Fewer hours than Employee 1
- More a traditional “9-to-5” worker
- Occasionally works a bit after 8pm

Detecting threats within the network

if *the mail is from the departing insider*
and *the message was sent in the last 30 days*
and *the recipient is not in the organization's domain*
and *the total bytes summed by day are more than a specified threshold*
then *send an alert to the security operator*

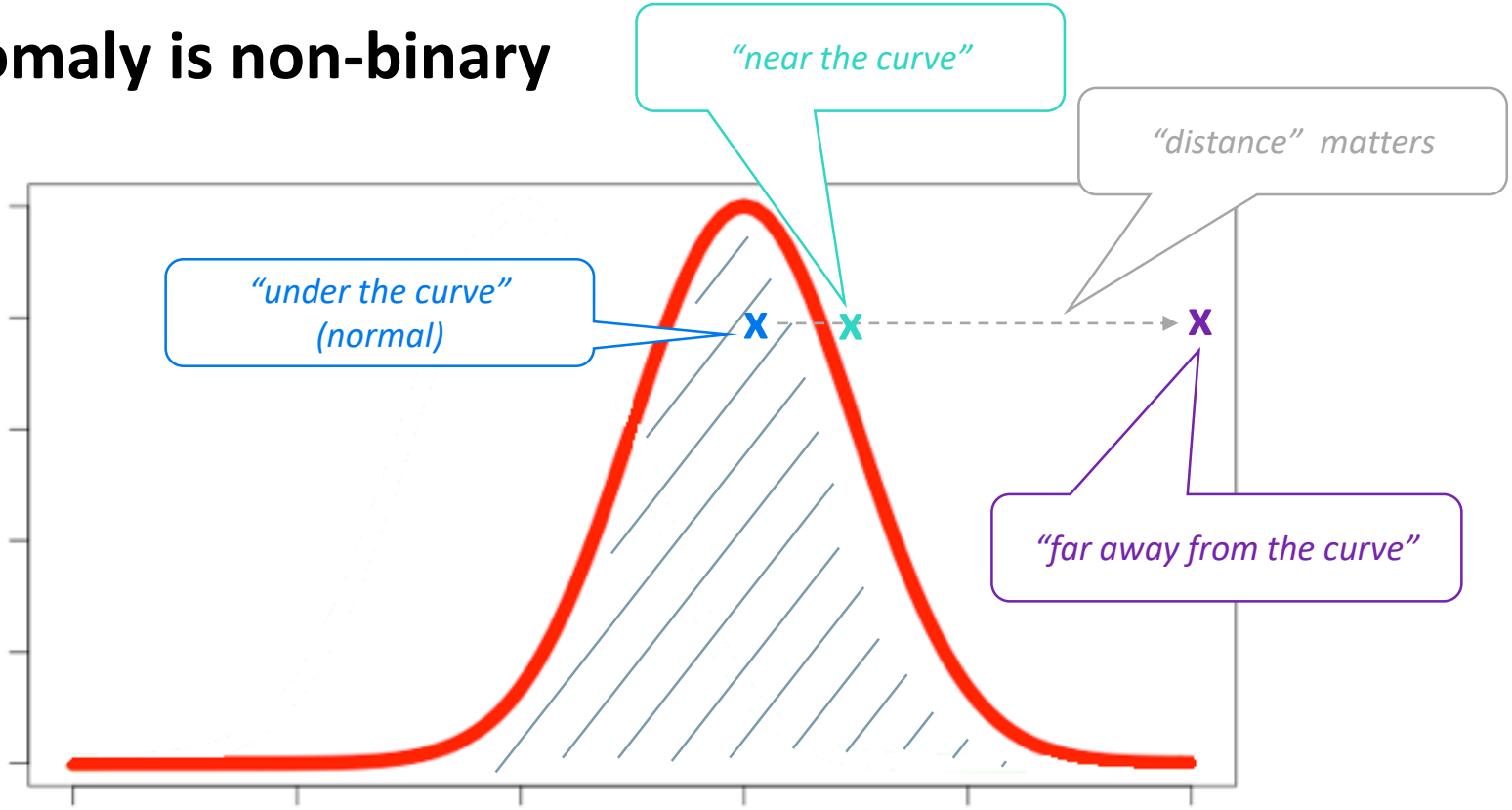
A Pattern for Increased Monitoring for Intellectual Property Theft by Departing Insiders, Andrew Moore, Carnegie Mellon 2011

Ru



When only “under” or “outside” the curve matter, then the paradigm is binary

An anomaly is non-binary

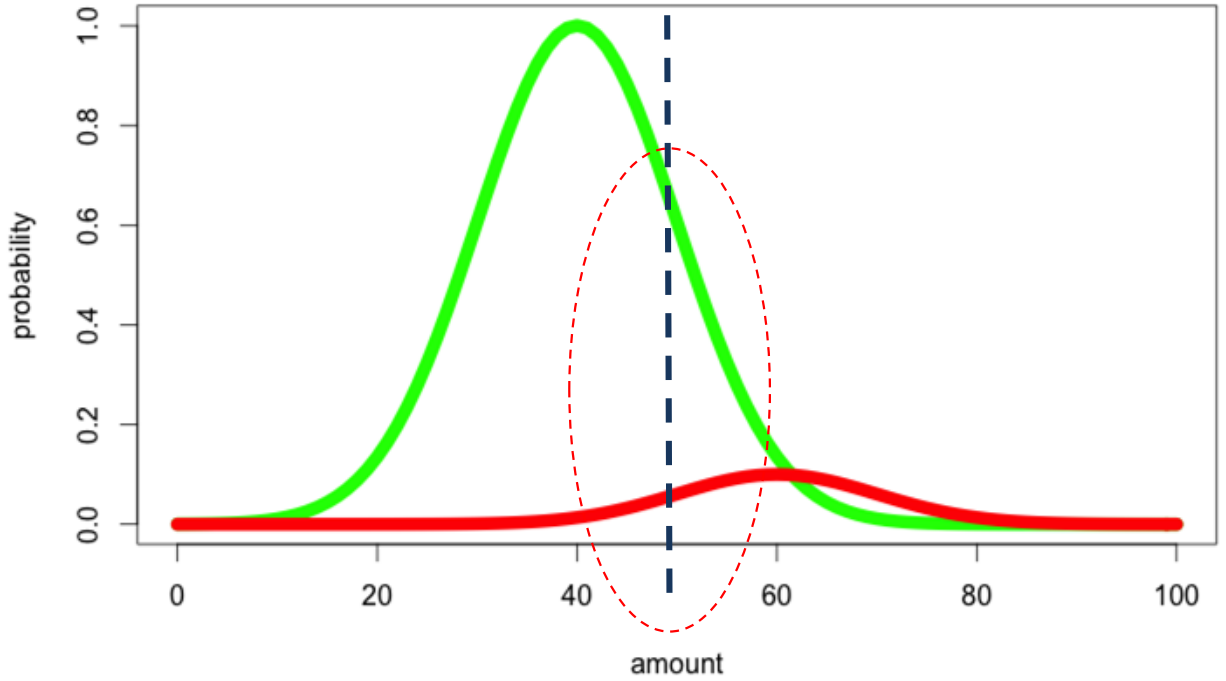


"Distance off" the curve matters – the further away the value is from an expected result, the more it matters: how abnormal is it?

Detecting threats within the network

if *the mail is from the departing insider*
and *the message was sent in the last 30 days*
and *the recipient is not in the organization's domain*
and *the total bytes summed by day are more than a specified threshold*
then *send an alert to the security operator*

A Pattern for Increased Monitoring for Intellectual Property Theft by Departing Insiders, Andrew Moore, Carnegie Mellon 2011



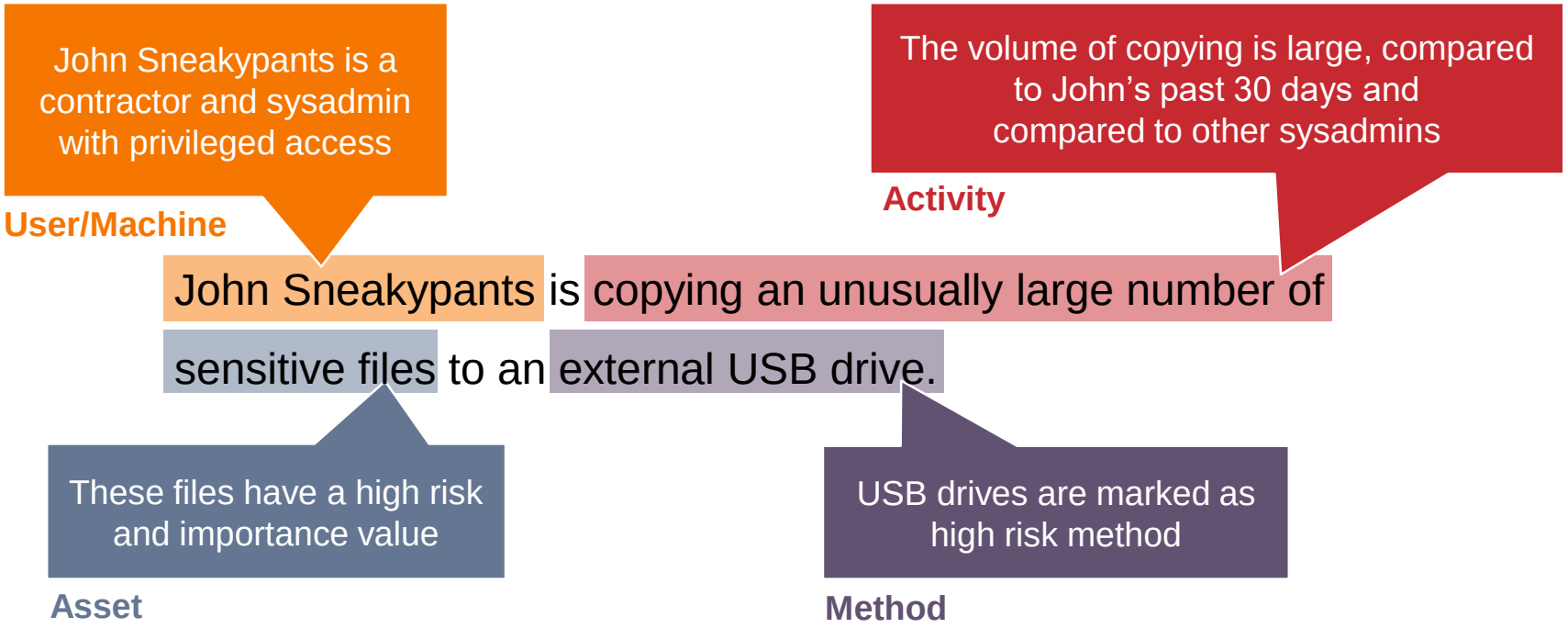
Detecting threats within the network

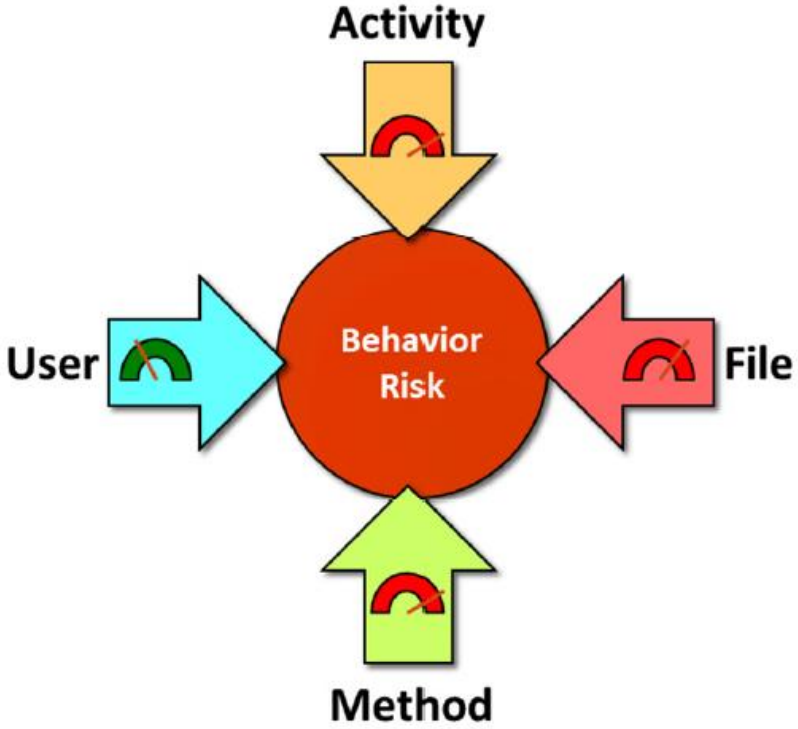
if *a person sends an email*
and *the data contained in the email is an unusual amount compared to the person's historical unique normal baseline*
then *trigger a high probability / high risk anomaly alert*

Billie.Dennis sent 13.9MB of data via email in a day, a larger email size than normal. Billie.Dennis typically sends at most 163kB of data via email in a day.

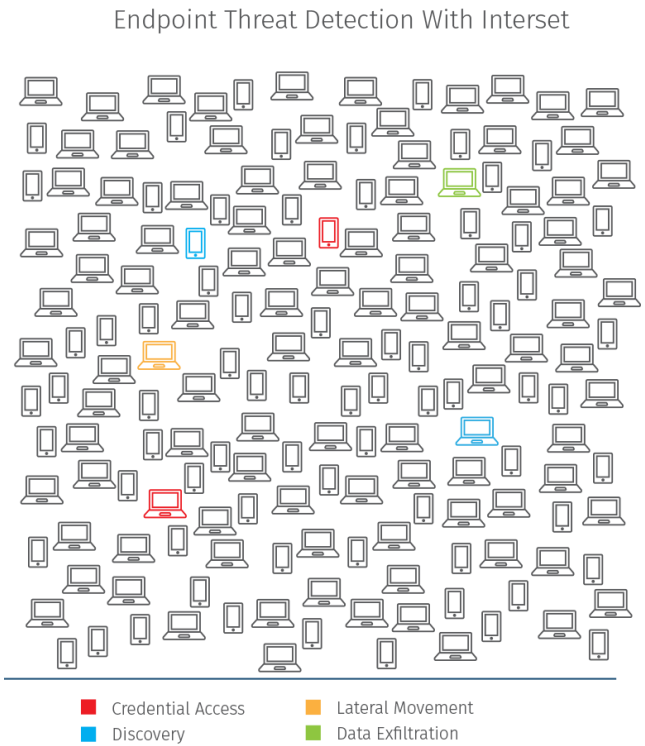
Exfiltration Data Sent Email Billie.Dennis

The Math: Quantifying Unusual Behaviors




Activity
User
Behavior
Risk
File
Method

EDR and Interset



Interset's advanced user and entity behavioral analytics (UEBA) analyzes billions of events and shines a new light on user information—such as abnormal login frequency, date or time of work, unusual machines—in order to expose difficult-to-find threats. Interset's partnership with CrowdStrike combines detailed and accurate data provided by CrowdStrike Falcon, giving security teams the necessary context to detect signs of credential access, discovery, lateral movement, or data exfiltration quickly and effectively.

Differentiators: Dynamic Peering

Peering (The way everyone else does it…)

Product

Stephan Jou
CTO

Shaun Pilkington
Intern

Maria Pospelova
Data Scientist

Engineering

Michael Iles
Level I Developer

Emilie Lavigne
Level III Developer

Josh Mahonin
QA

Sales

Mario Daigle
Regional Director

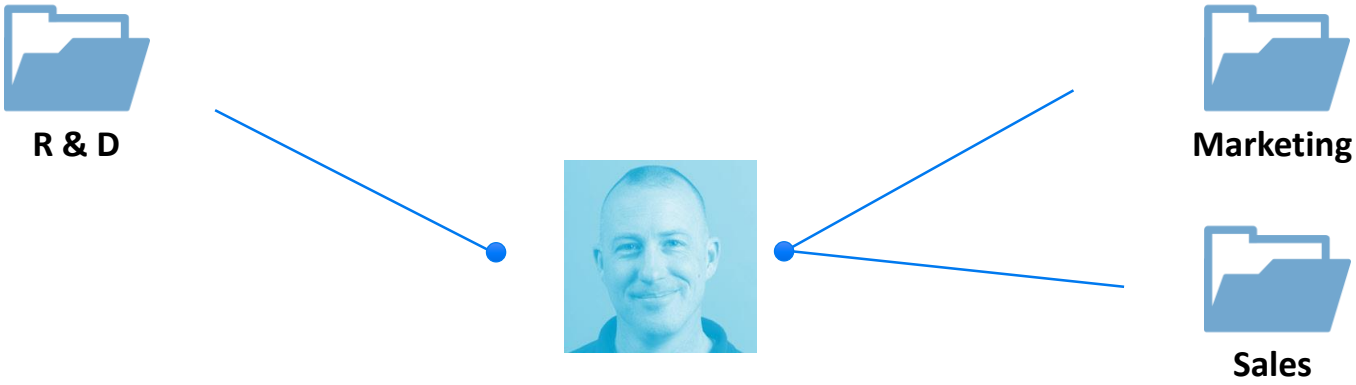
Pabi Ambikainathan
Account Exec

Jay Lillie
Sales Engineering

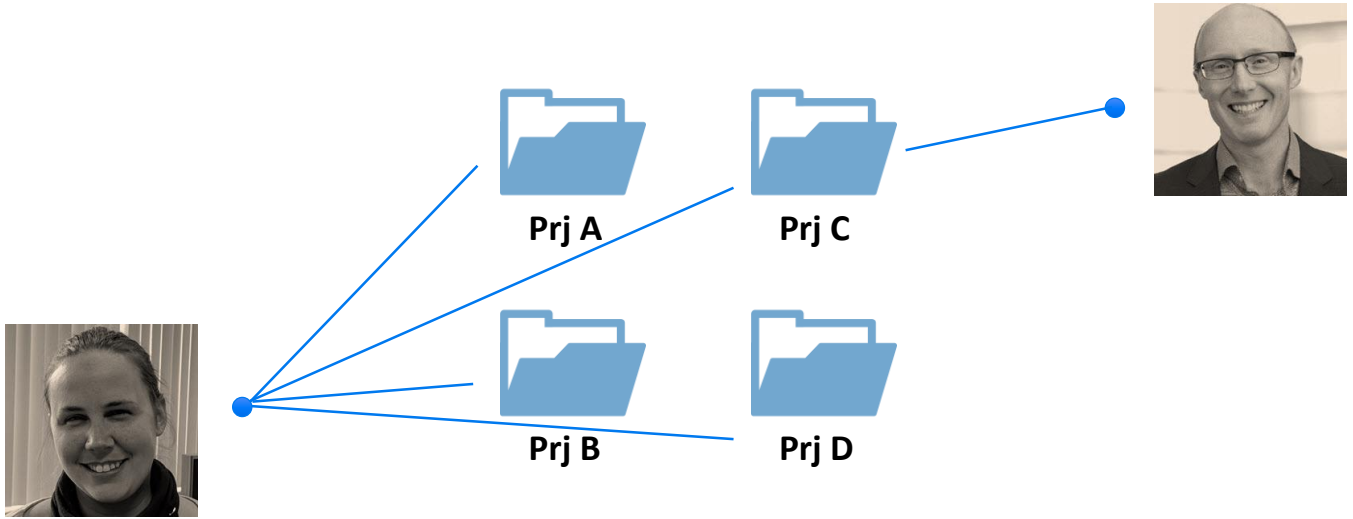
Peering (Locations according to the org chart)

Product	Engineering	Sales
 R & D	 Prj A	 Prj C	 Marketing
 Prj X	 Prj B	 Prj D	 Sales

Peering (One of many exceptions…)



Peering (Even more patterns…)



Peering (The Interset way)

Group A

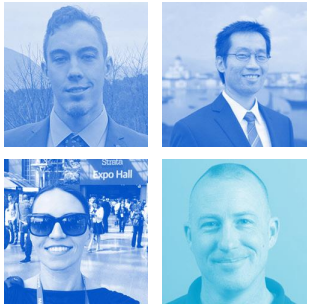
Sales
Contacts

Group C

Prj X

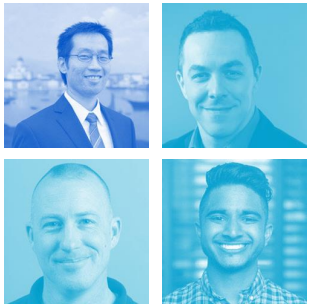
Group B

R & D
Folder



Group D

Marketing
Folder

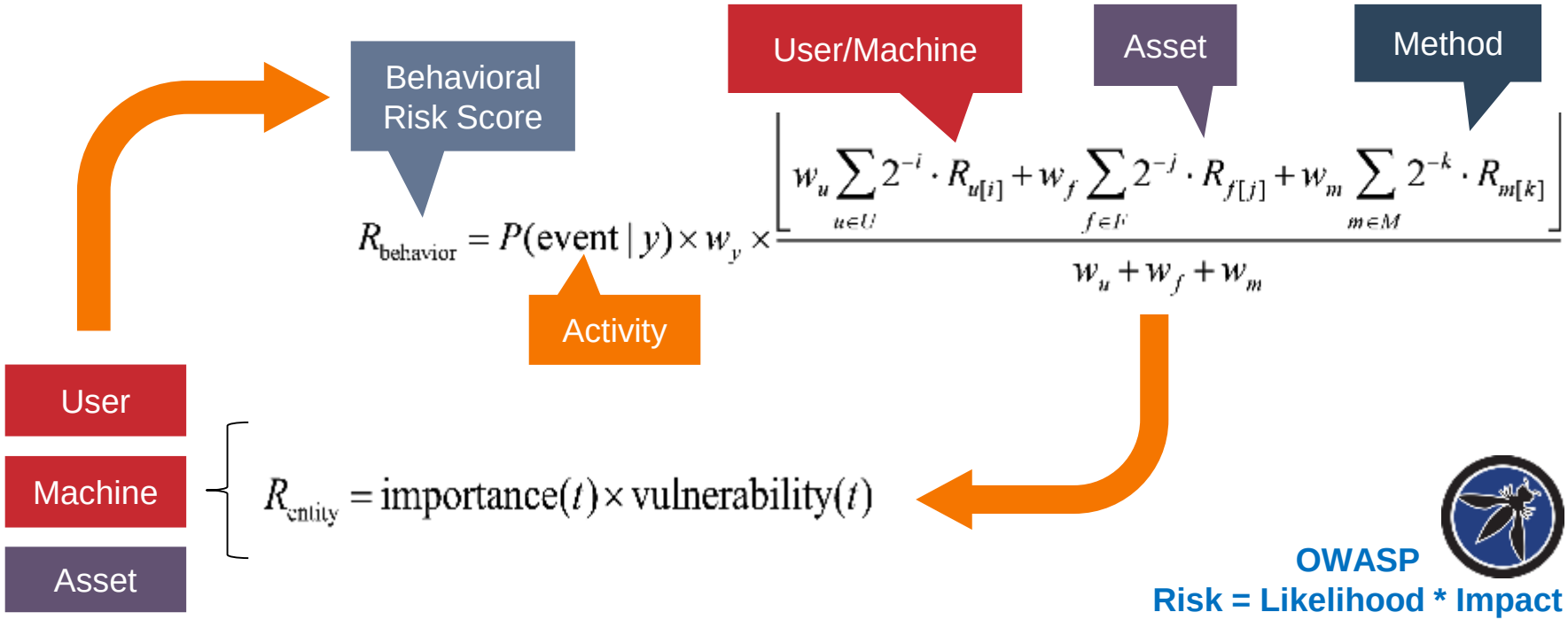


Peering (The Interset way)

Don’t try to manage all of these groups or maintain rules…

…instead, survey they ecosystem and find the patterns to determine what is out of place

The Math: Quantifying Risky Entities

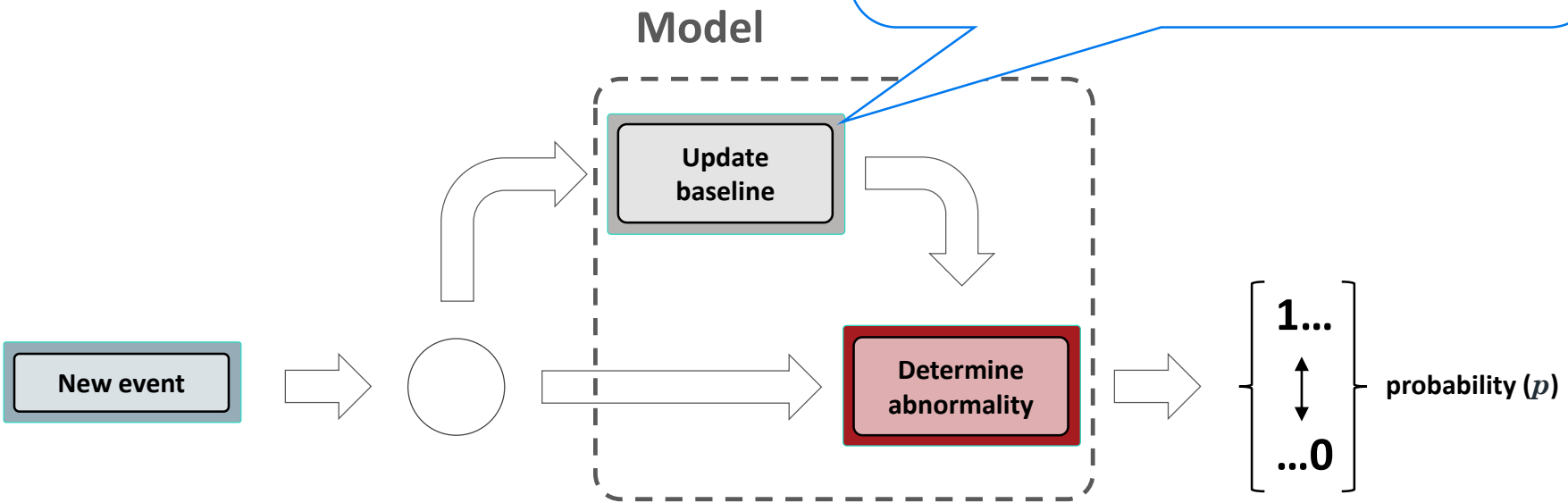


OWASP
Risk = Likelihood * Impact

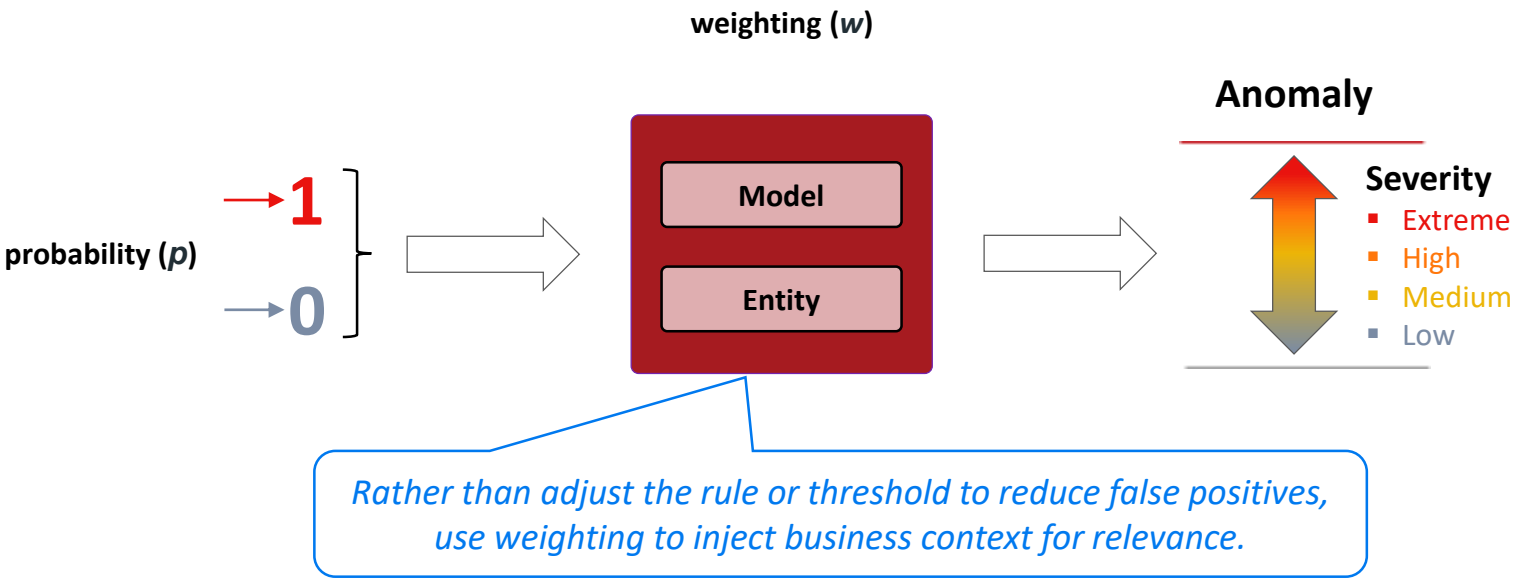
Determine probability…

When we talk about a "dynamic" baseline, this is what we mean. It changes over time:

- *It is based only on what we observe* in situ
- *Every new event is incorporated*
- *It is not based on any "third party" expected behavior*



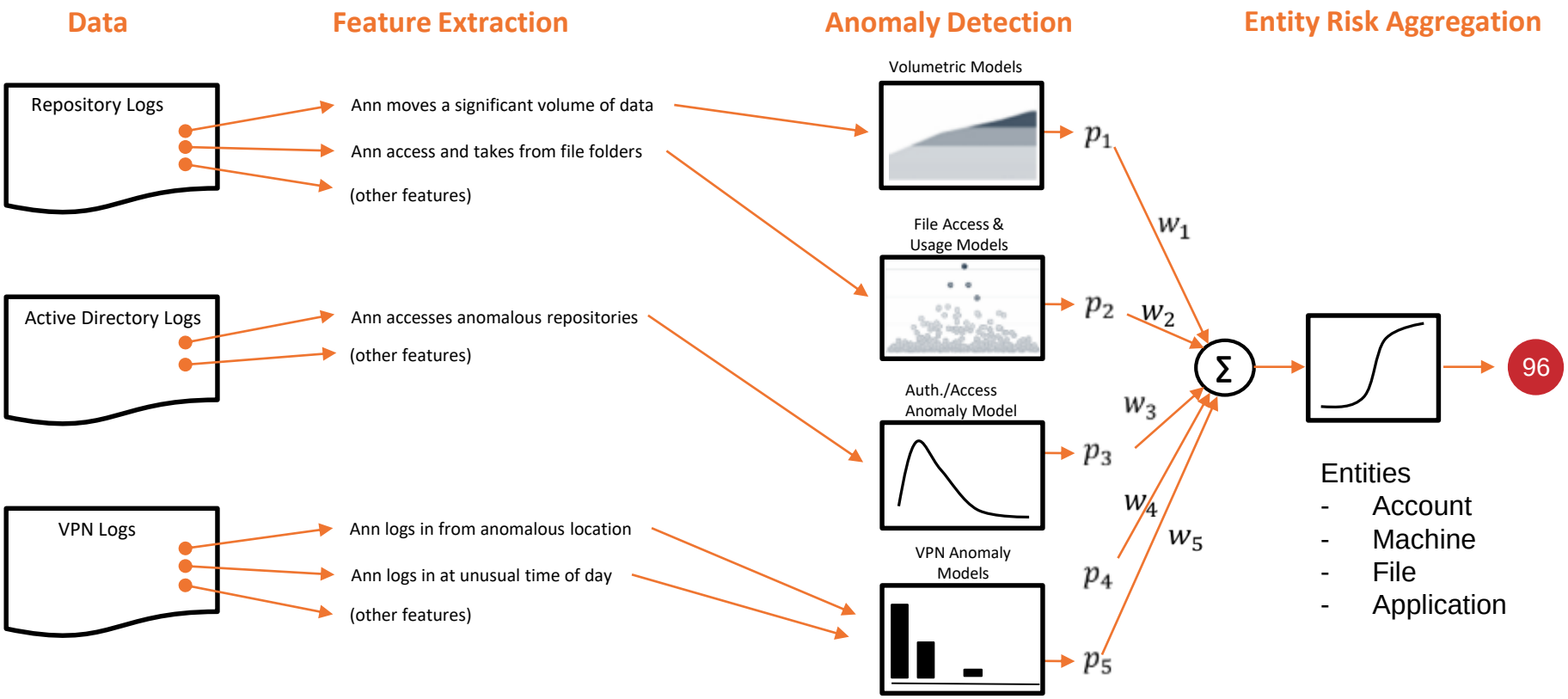
…and combine with weighting to get an alert



The Math: Quantifying Risky Entities

- … *and* moves a significantly high volume of data than normal **96**
- … *and* takes from a folder on a repository an unusual number of times **80**
- … *and* accesses repositories that she and her peers do not usually access **65**
- … VPNs in from China **46**
- Ann Funderburk works at an unusual hour **15**

Analytical Framework: From Log Data to Risky Entities



1. No static weighting

If we were to pretend that events are equivalent to anomalies…

Others

User behavior that has “unusual” characteristics gets assigned a static value

- **5 points:** An event after pre-defined working hours login
- **15 points:** Moving more than 250MB of data but less than 500MB of data from a pre-defined “risky” location

Interset

- **Working hours**
  - Have we seen this user work these hours before?
  - If we have seen these hours before, was it recently or long ago?
  - How much outside of previously observed working hours is the event?
- **Amount of data moved**
  - Is this a location this user has accessed previously?
  - How does the amount of data moved compare to previous volumes for self, peers, and population?
  - Has any user accessed this location recently?

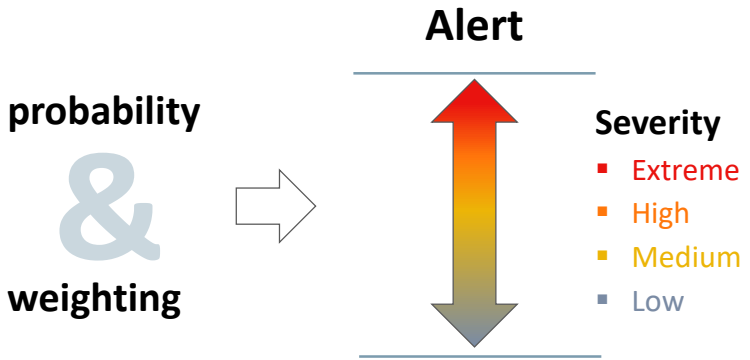
An alert combines probability and weighting

How unusual?

- Compared to self
- Compared to peers
- Compared to entire population

How much does it matter?

- Significance of the behavior
  - Login from another country
  - Accessing new server
- Entity enrichment
  - User w/ bad performance review
  - “Honeypot” file share
  - Mergers & acquisition data
  - Contractors coming to the end of contract
  - Recently traveled overseas



Calculation is context-based

Interset risk scores are not step functions and they build-in the concept of “decay” over time

Just because the alerts in this period of were “high risk,” there was not an automatic push for the entity risk score itself to move into a “high risk” range

Risk score does not immediately return to zero just because of the absence of anomalies; this is the concept of controlled decay.

Note it took a number of actions against an already elevated risk profile to push Jacob to a new peak risk score.

MICRO FOCUS Interset

Detect, Investigate, and Respond Better with Interset and ATT&CK

Interset UEBA covers 75% of the ATT&CK framework—and growing

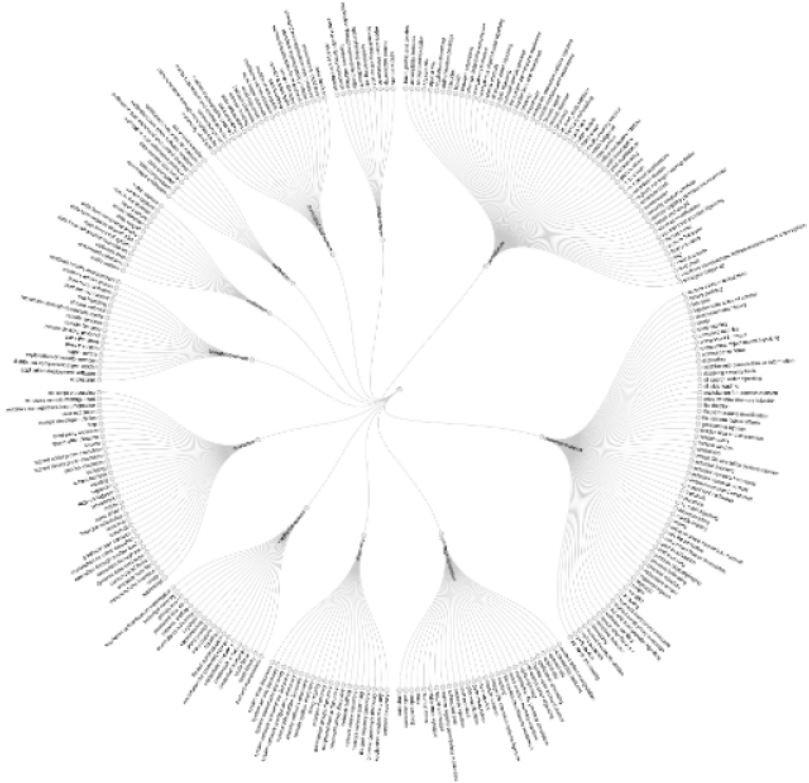
What is MITRE ATT&CK?

MITRE

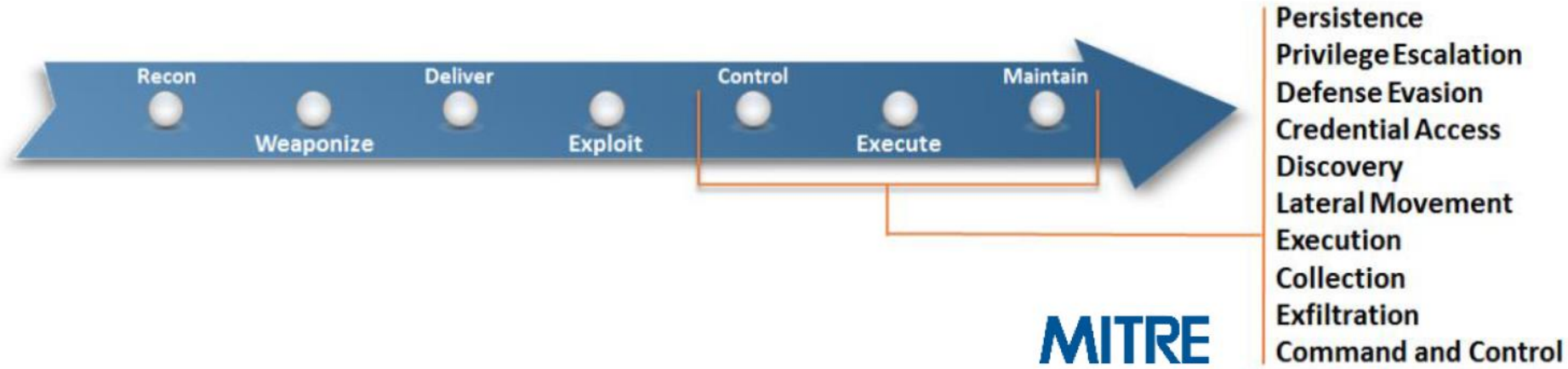
- Not-for-profit organization dedicated to making the world safer
- Operate multiple federally funded R&D centers

ATT&CK

- Adversarial Tactics, Techniques & Common Knowledge
- Started in 2013 to document results from the FMX research project
- Using endpoint telemetry and analytics to detect post-compromise activity on enterprise networks



Scope of ATT&CK



Principals of ATT&CK

Understand Adversary Behavior

- The best driver for defense is understanding the offense
- Need to focus on real-world examples
- Provides a mechanism to measure against

Analytics is foundational

- Traditional solutions cannot keep up
- Typical indicators are too narrow

Common taxonomy

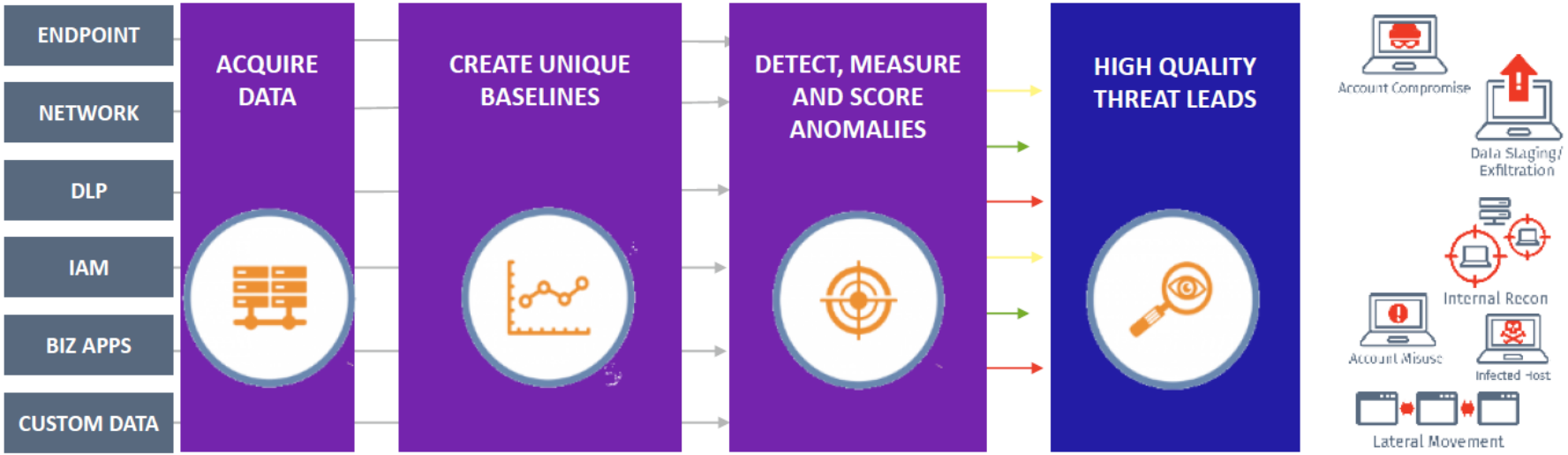
- Establish a common language when comparing across adversary groups
- Existing concepts were too high-level

Tactics & Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	31 items	56 items	28 items	59 items	20 items	19 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture		Multi-hop Proxy
	Launchctl	Component Firmware	File System Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Local Job Scheduling	Component Object Model Hijacking	Hooking	Deobfuscate/Decode Files or Information	Kerberoasting	Remote System Discovery	Shared Webroot	Screen Capture		Multiband Communication
	LSASS Driver	Create Account	Image File Execution Options Injection	Disabling Security Tools	Keychain	Security Software Discovery	SSH Hijacking	Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	System Information Discovery	Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking	New Service	DLL Side-Loading	Network Sniffing	System Network Configuration Discovery	Third-party Software			Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Path Interception	Exploitation for Defense Evasion	Password Filter DLL	System Network Connections Discovery	Windows Admin Shares			Remote File Copy
	Regsvr32	File System Permissions Weakness	Plist Modification	Extra Window Memory Injection	Private Keys	System Owner/User Discovery	Windows Remote Management			Standard Application Layer Protocol
	Rundll32	Hidden Files and Directories	Port Monitors	File Deletion	Replication Through Removable Media	System Service Discovery				Standard Cryptographic Protocol
	Scheduled Task	Hooking	Process Injection	File System Logical Offsets	Securityd Memory					Standard Non-Application Layer Protocol
	Scripting	Hypervisor	Scheduled Task	Gatekeeper Bypass	Two-Factor Authentication Interception					Uncommonly Used Port
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Hidden Files and Directories						Web Service
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	Hidden Users						
	Signed Script Proxy Execution	Launch Agent		Hidden Window						
	Source			HISTCONTROL						
	Space after Filename			Image File Execution Options Injection						

MICRO FOCUS Interset

Behavioral Threat Approach



Key data sources

Gather the raw data and group

Determine what is normal

Find the behavior that matters

Roll up the riskiest entities

Identify Threats

Differentiators: Pre-defined Data Model

Interset Approach

- ETL process convert the raw events into pre-defined abstract data type (Authentication/Data Store/Web Proxy/End Point..)
- Provide abundant pre-defined data model (behavior rule) on supported data types, no need for customization and tuning
- Ingestion is a bit complicate, rest of work is simple
- Not able to add additional data model or support new data type by field SE

Processing a range of sources to find unusual behavior

With over 450+ individual models, a remarkable amount of context is available to find threats that matter

Some representative data sources we process…

Authentication	Data Store	Endpoint	NetFlow	Printer	Web Proxy	Custom
•Who is authenticating from an unusual location? •When is a rarely used account active?	•Who is accessing data they have never touched before? •When is an unusually large amount of data moving to a new location?	•Which machines have unusual processes running? •When is an unusual remote storage device being used?	•When is non-standard traffic using a standard port? •Which machine is receiving traffic from an unusual source?	•Who is printing to unusual locations? •When are unusually large print jobs received?	•What new websites have never been accessed before? •Which websites are receiving unusually large amounts of data?	•Expense reports •Vacation time •Others…

…to automatically detect relevant anomalies

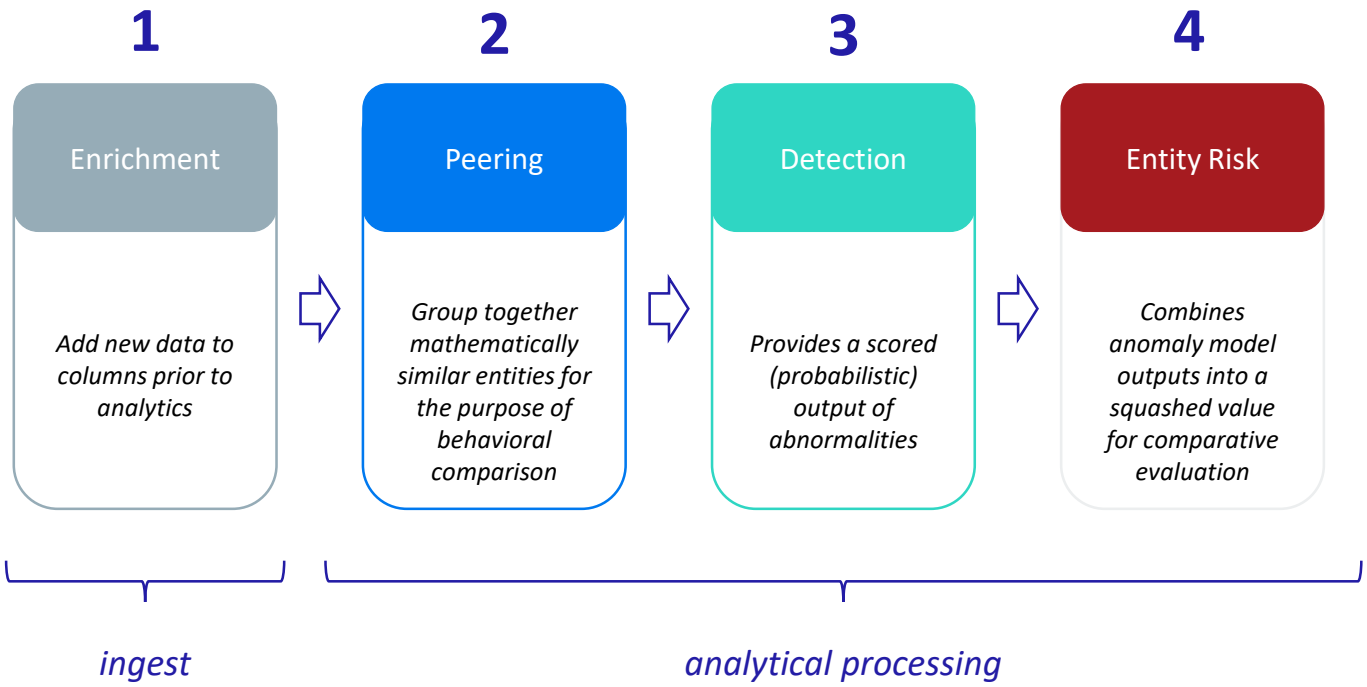
Interset strengths

1. Principled math (may need PoC to prove)
   a. Rigorous data science
   b. Anomaly detection through unsupervised machine learning

2. Enormous scale
   a. “Big Data” native from the start
   b. Horizontally scalable to monitor hundreds of thousands of unique entities and billions of events per day

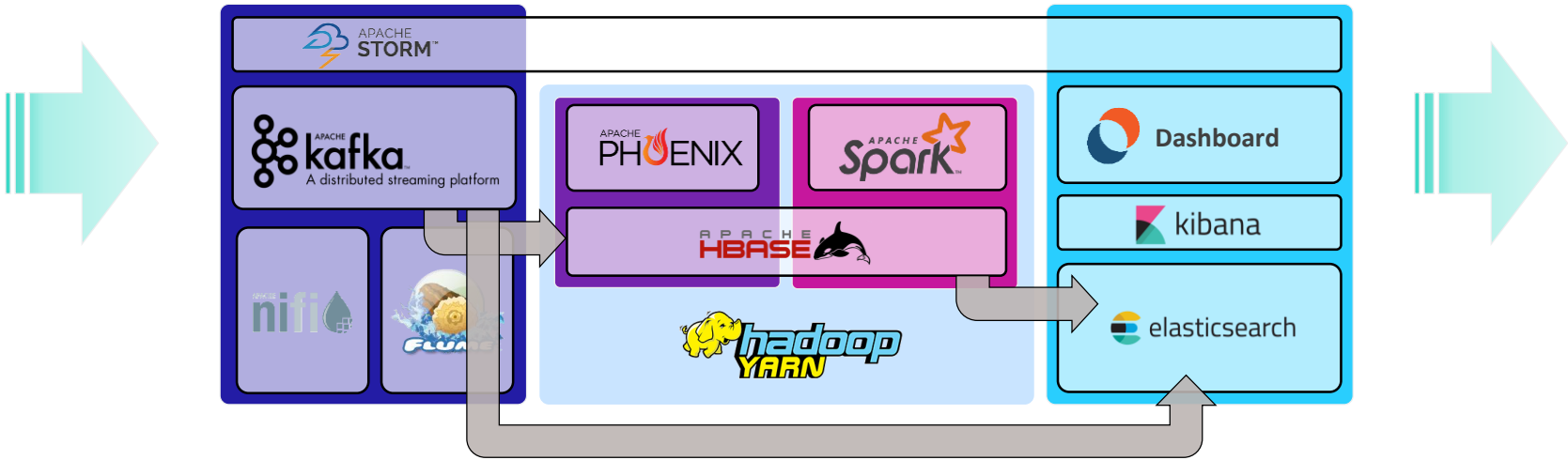
3. Security ecosystem integration
   a. Interset plays one role by design
   b. Designed to work with data and tools the customer already has

Machine learning is used in four primary roles



Big Data Architecture

Moving data: End-to-end




MICRO®
FOCUS