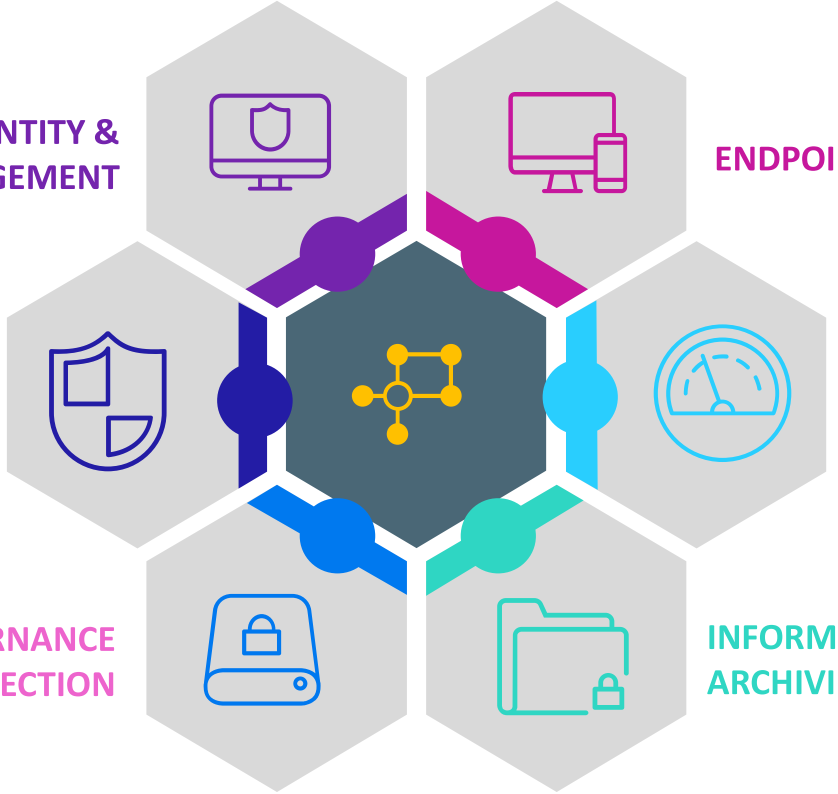
MICRO FOCUS

Interset

Insider Threat Detection

Security, Risk and Governance

MICRO FOCUS



NetIQ

IDENTITY & ACCESS MANAGEMENT

ENDPOINT MANAGEMENT

ZENworks

FORTIFY

APPLICATION SECURITY

SECURITY OPERATIONS

ArcSight

Voltage security

DATA GOVERNANCE & PROTECTION

INFORMATION ARCHIVING

Content Manager

Structured Data Manager
ControlPoint

ANALYTICS & MACHINE LEARNING

ArcSight Intelligence

What is ArcSight Intelligence?

(FKA “Interset”)

INTERSET → ArcSight Intelligence

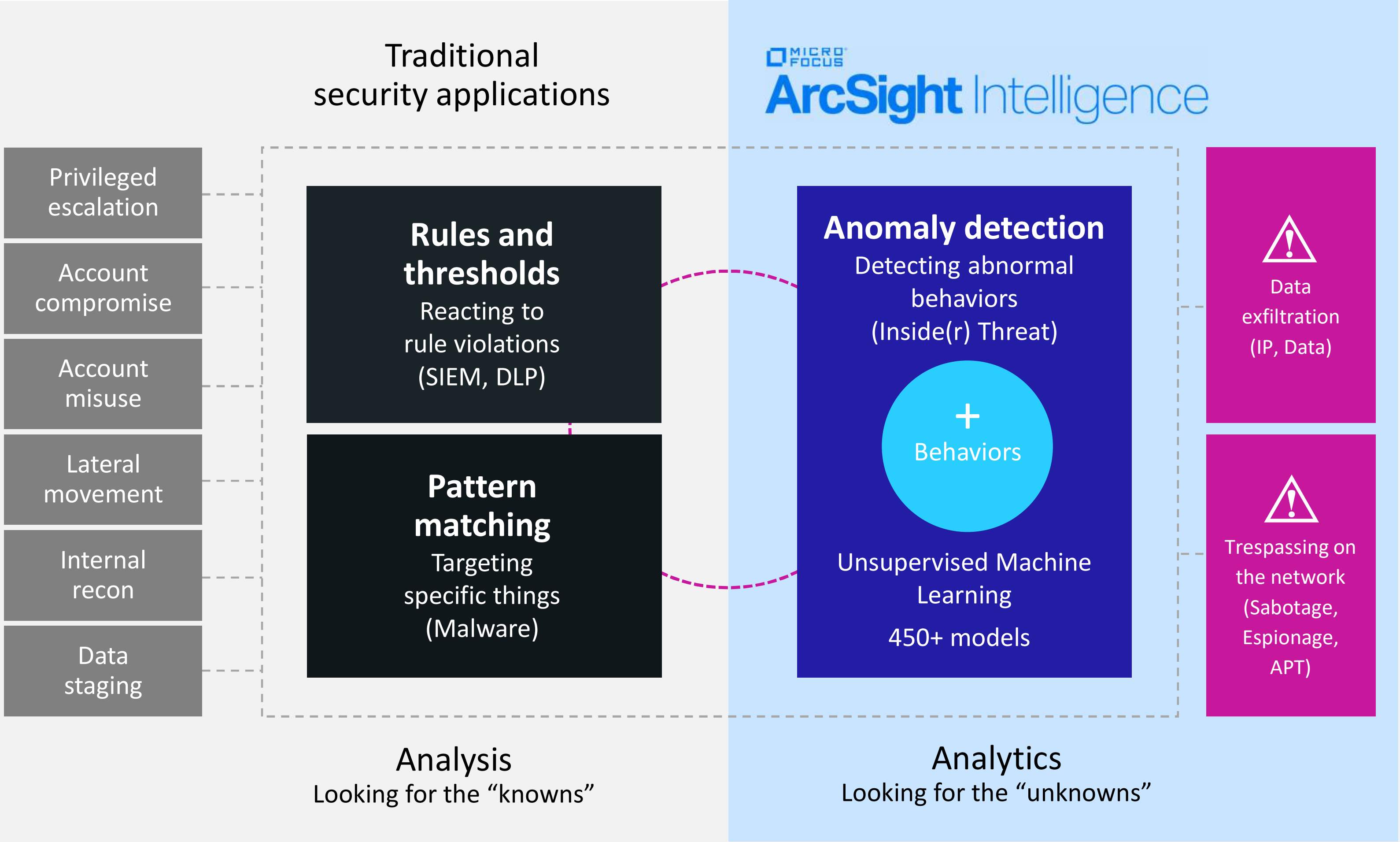
- **100%** Unsupervised Machine Learning
- **Hundreds** of threat detection algorithms & always growing
- **MITRE** ATT&CK Mapping
- **13** data types analyzed*

  *Falcon populates 4 model libraries (Access, Endpoint, Network & Repository)
- **100+** person years of development, hardening, and refinement

- **7+** years of security analytics in the market
- Part of the **In-Q-Tel** portfolio
- Acquired by **Micro Focus** February 2019

*** Traditional on-prem or SaaS deployment**

Interset UEBA Augments Traditional Analytics

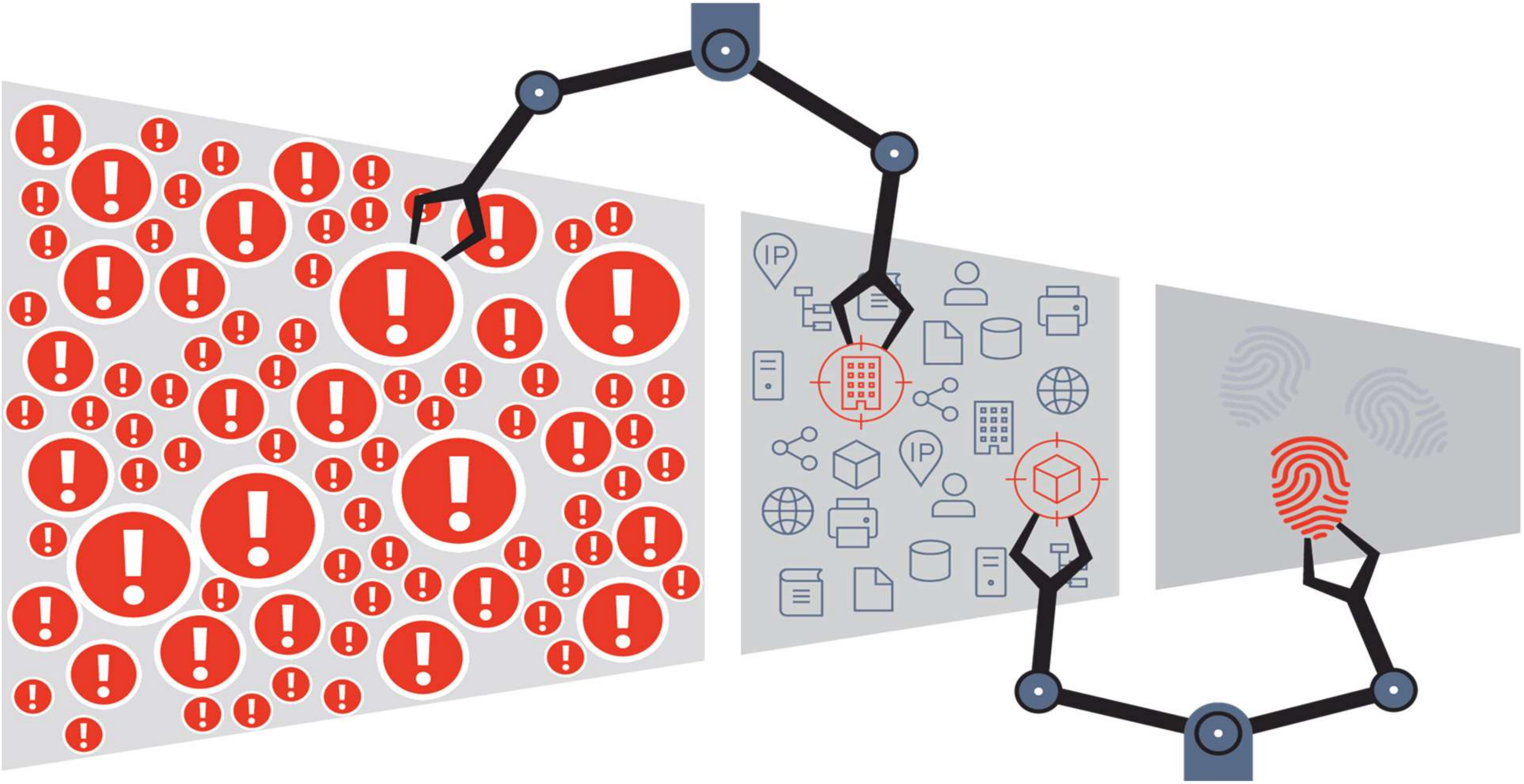


Traditional security applications
MICRO FOCUS
ArcSight Intelligence
Privileged escalation
Account compromise
Account misuse
Lateral movement
Internal recon
Data staging
Rules and thresholds
Reacting to rule violations (SIEM, DLP)
Pattern matching
Targeting specific things (Malware)
Anomaly detection
Detecting abnormal behaviors (Inside(r) Threat)
+ Behaviors
Unsupervised Machine Learning
450+ models
Data exfiltration (IP, Data)
Trespassing on the network (Sabotage, Espionage, APT)
Analysis
Looking for the "knowns"
Analytics
Looking for the "unknowns"

- Purpose-built for Insider Threat detection - Trusted users w/ no policy violations
- Creates individual unique normals, detects abnormal, assigns risk score 0-100
- Recent Insider Threat Hunting Wins (Source code exfil, RDP, shadow DB brute force, blind spots, reduced dwell time)
- CISO Fans

What we do: Detect Inside(r) Threats

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



Human Approach Rules / thresholds

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*

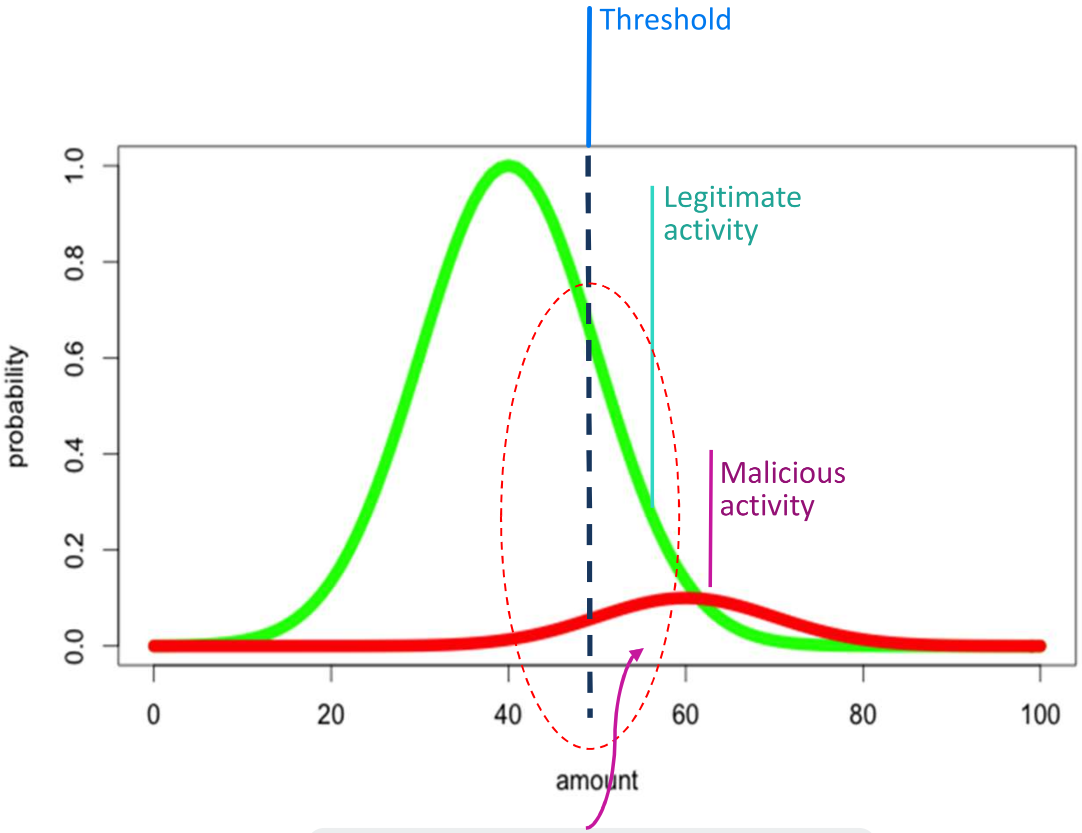
and *the total bytes summed by day are more than a specified threshold*

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

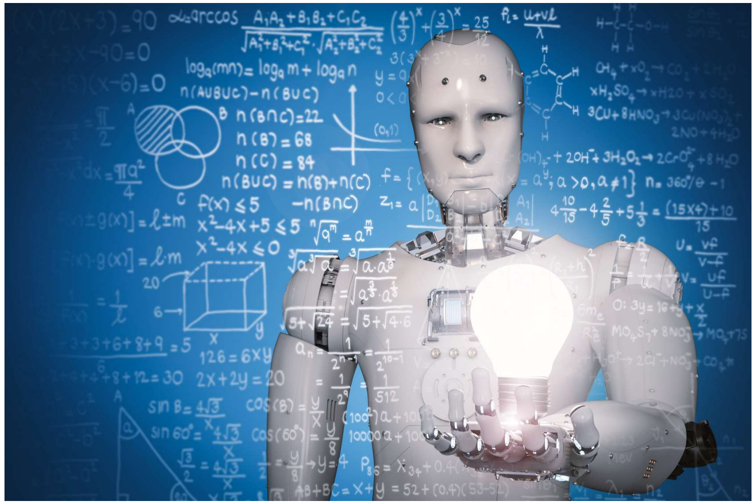
How We Do It

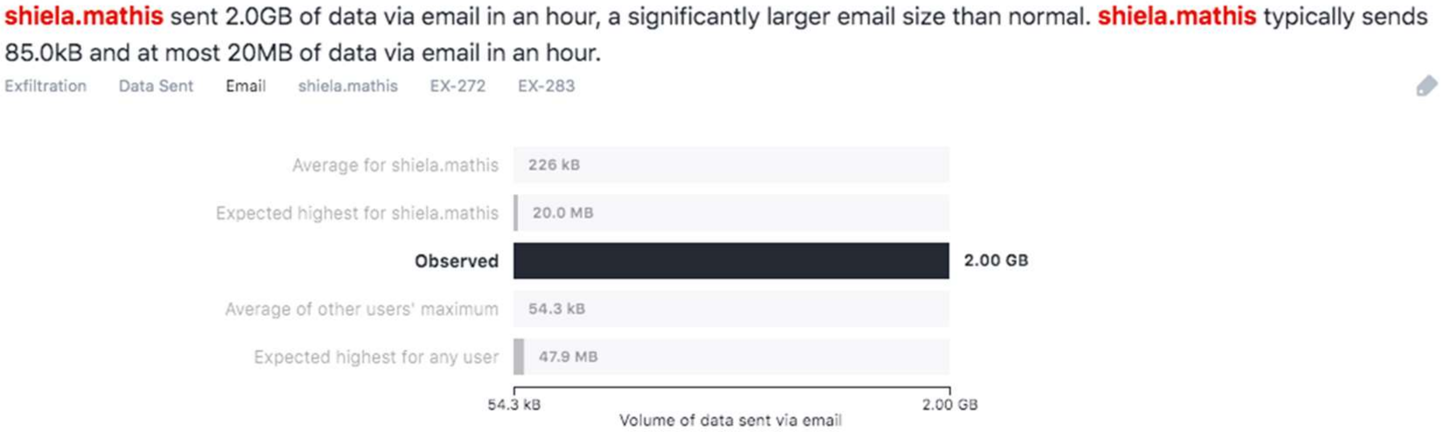
- Mine security data with advanced mathematical algorithms and unsupervised ML to reveal threats.
- Define normal entity behaviors called “Unique Normal” with unsupervised ML.
- Use mathematic models to compare “Unique Normal” with itself and peers to identify behavioral anomalies which could indicate threats.



Legitimate activity will dwarf malicious activity, leading to alert fatigue

Unsupervised ML Approach





shiela.mathis sent 2.0GB of data via email in an hour, a significantly larger email size than normal. shiela.mathis typically sends 85.0kB and at most 20MB of data via email in an hour.

Exfiltration   Data Sent   Email   shiela.mathis   EX-272   EX-283

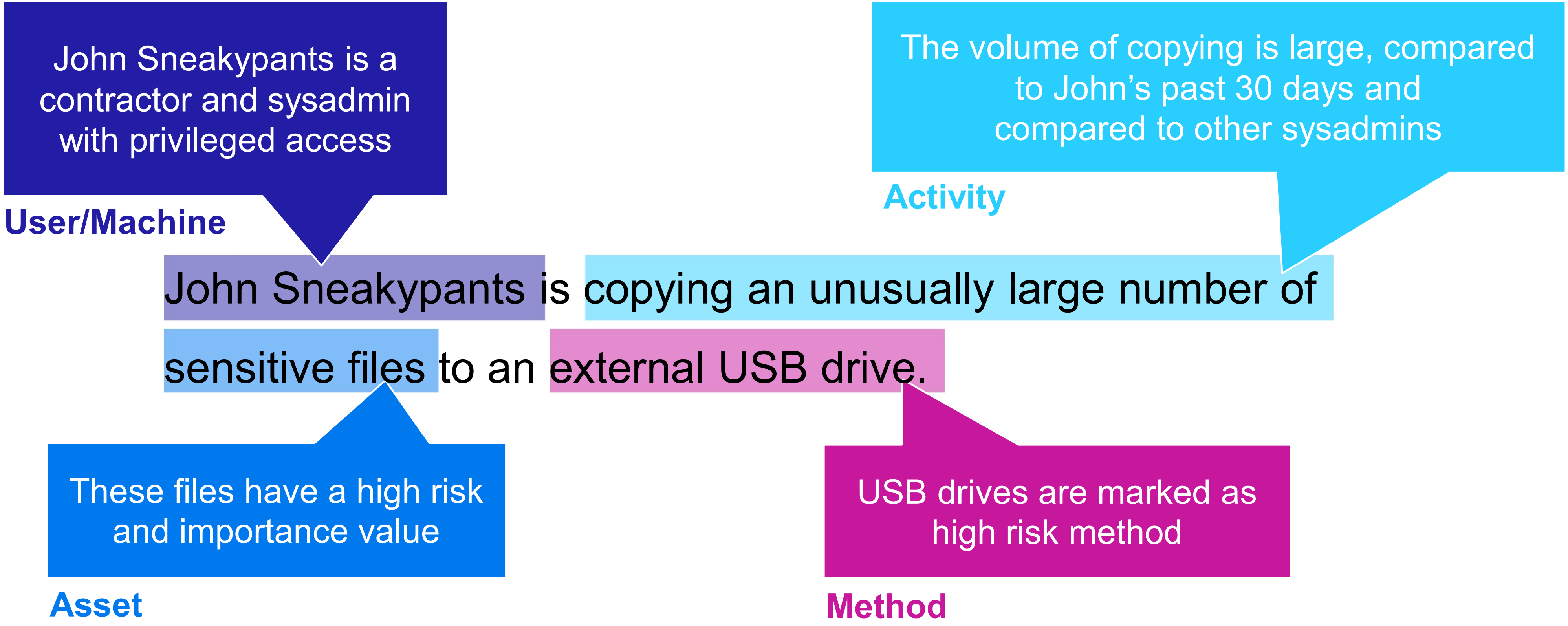
Average for shiela.mathis
226 kB
Expected highest for shiela.mathis
20.0 MB
Observed
2.00 GB
Average of other users' maximum
54.3 kB
Expected highest for any user
47.9 MB
54.3 kB
2.00 GB
Volume of data sent via email

***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*

The Math: Quantifying Unusual Behaviors



John Sneakypants is a contractor and sysadmin with privileged access

User/Machine

The volume of copying is large, compared to John’s past 30 days and compared to other sysadmins

Activity

John Sneakypants is copying an unusually large number of sensitive files to an external USB drive.

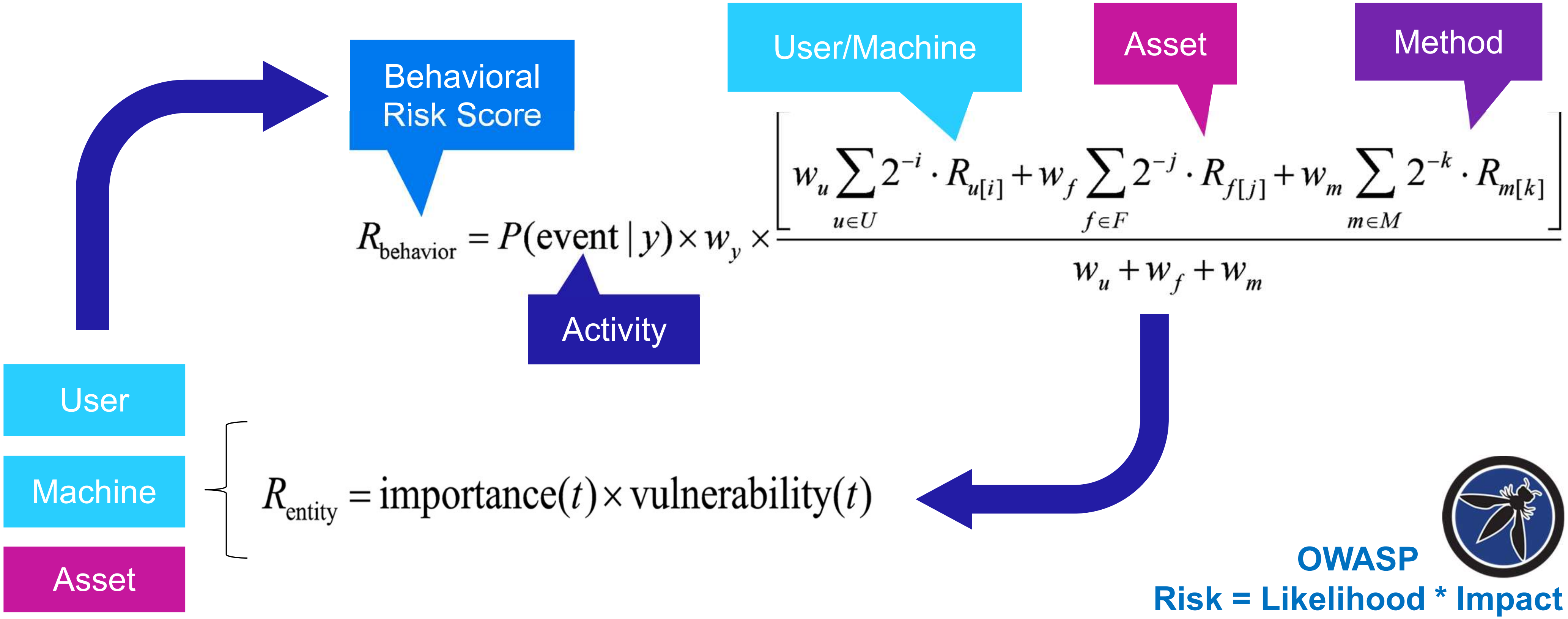
These files have a high risk and importance value

Asset

USB drives are marked as high risk method

Method

The Math: Quantifying Risky Entities



Behavioral Risk Score

User/Machine

Asset

Method

$$R_{\text{behavior}} = P(\text{event} \mid y) \times w_y \times \frac{\left[w_u \sum_{u \in U} 2^{-i} \cdot R_{u[i]} + w_f \sum_{f \in F} 2^{-j} \cdot R_{f[j]} + w_m \sum_{m \in M} 2^{-k} \cdot R_{m[k]} \right]}{w_u + w_f + w_m}$$

Activity

User

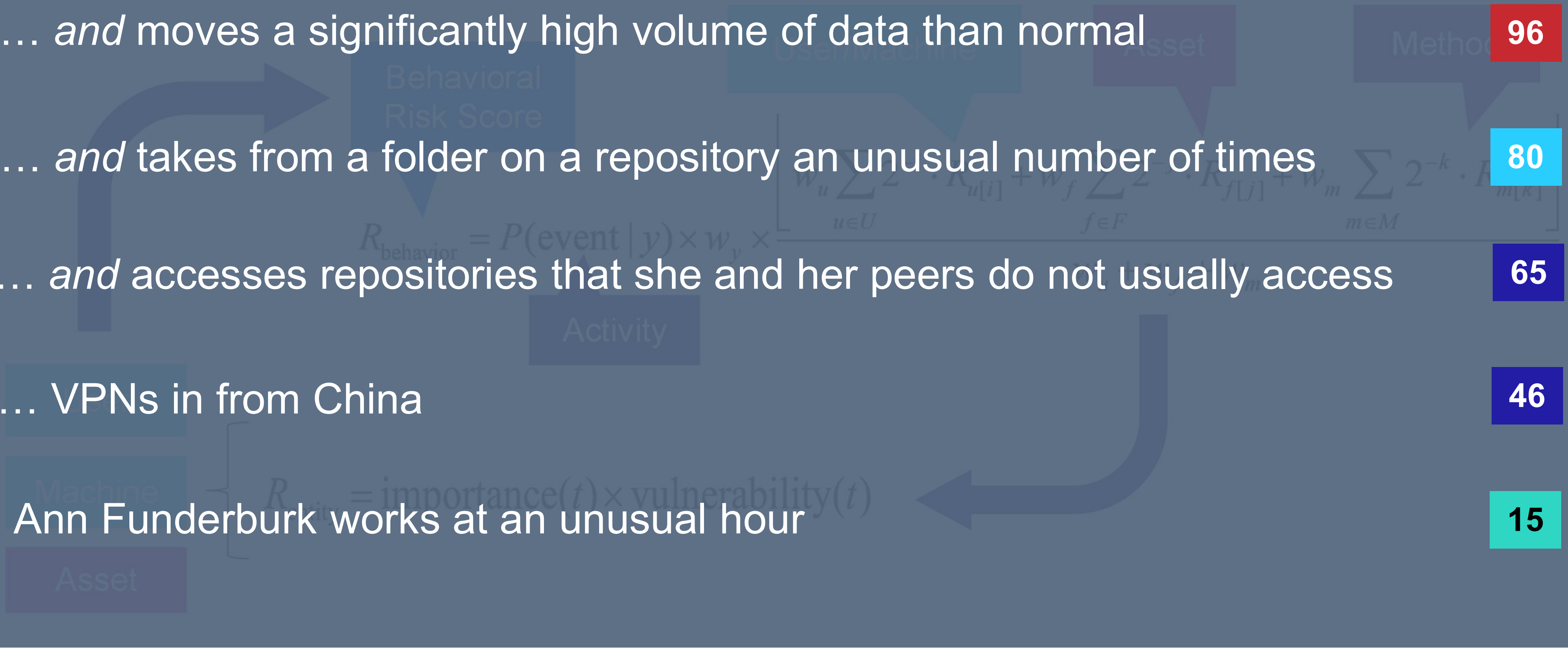
Machine

Asset

$$R_{\text{entity}} = \text{importance}(t) \times \text{vulnerability}(t)$$

OWASP
Risk = Likelihood * Impact

The Math: Quantifying Risky Entities


Behavioral Risk Score
User/Machine
Asset
Method
$R_{\text{behavior}} = P(\text{event} \mid y) \times w_y \times$
$w_u \sum_{u \in U} 2^{-k} \cdot R_{u[i]} + w_f \sum_{f \in F} 2^{-k} \cdot R_{f[j]} + w_m \sum_{m \in M} 2^{-k} \cdot R_{m[k]}$
Activity
Machine
Asset
$= \text{importance}(t) \times \text{vulnerability}(t)$

• … *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