Insider Threat Detection
Security, Risk and Governance

Identity & Access Management

Endpoint Management

Security Operations

Information Archiving

Analytics & Machine Learning

Content Manager
What is ArcSight Intelligence?
(FKA “Interset”)

- 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

- 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)

Analysis
Looking for the “knowns”

Anomaly detection
Detecting abnormal behaviors (Inside(r) Threat)

Behaviors
Unsupervised Machine Learning
450+ models

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

- Data exfiltration (IP, Data)
- Trespassing on the network (Sabotage, Espionage, APT)
What we do: Detect Inside(r) Threats

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

Threshold

Legitimate activity will dwarf malicious activity, leading to alert fatigue
Unsupervised ML Approach

**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
John Sneakypants is a contractor and sysadmin with privileged access. These files have a high risk and importance value. USB drives are marked as high risk method.

The volume of copying is large, compared to John's past 30 days and compared to other sysadmins. John Sneakypants is copying an unusually large number of sensitive files to an external USB drive.
The Math: Quantifying Risky Entities

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

- **User/Machine**

- **Asset**

- **Method**

- **Activity**

- **User**

- **Machine**

- **Asset**

- **OWASP Risk = Likelihood * Impact**

\[ R_{entity} = \text{importance}(t) \times \text{vulnerability}(t) \]
The Math: Quantifying Risky Entities

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