The Power of AI to Disrupt Security Operations

Chris Calvert

Cofounder & VP of Strategy

respond

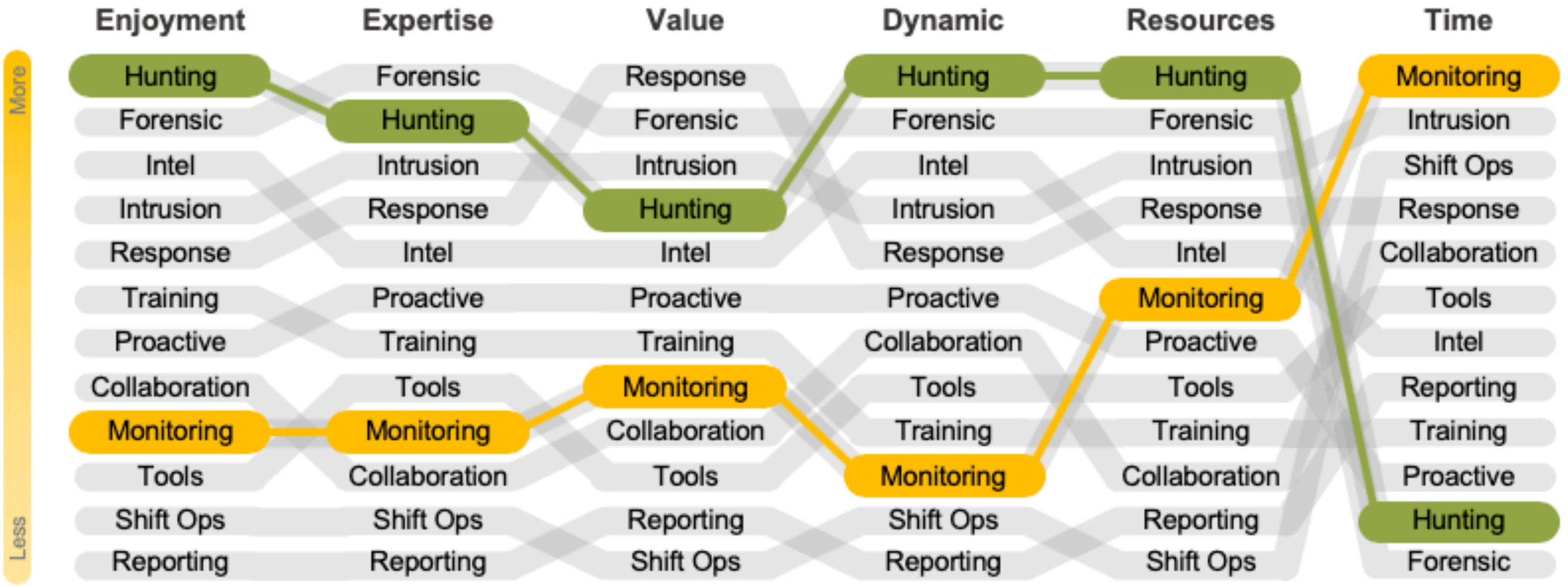
Agenda

- Problem slide... ☺
- Artificial Intelligence Ugh!
- Security Operations
- Aligning for the Future

We aren’t learning by osmosis...

Voice of the Analyst Survey

Activity Rankings Across Perceptual Dimension



Voice of the Analyst Survey, Cyentia Institute

Artificial Intelligence

What does that even mean?

Artificial Intelligence

Machines that mimic cognitive functions such as learning, problem solving and decision-making.

- A new brand on what used to be called **MATH**
- Deep Learning = Neural Networks (1943) + image processing GPUs
- nAI means Narrow AI
- nAI = A → B, “Ability to learn or act intelligently” – Andrew Ng

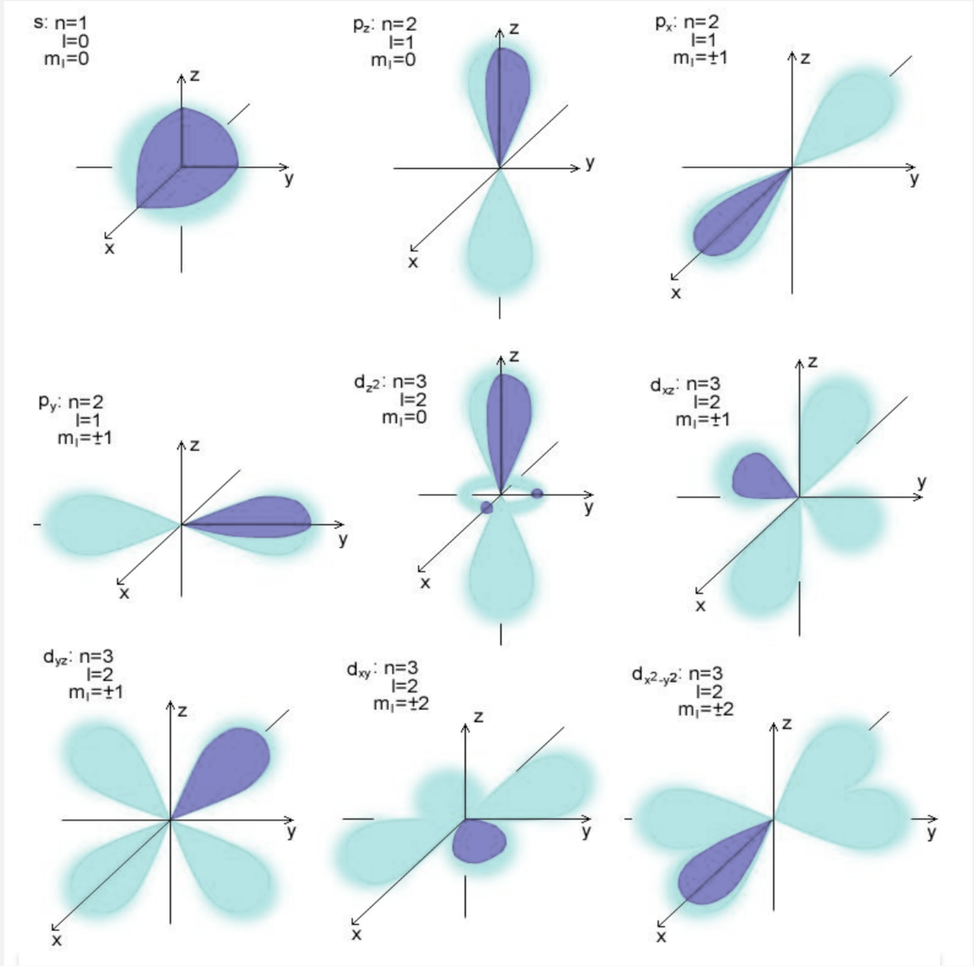
Learning Software

Data is meaningless without judgement

- Lab data is equivalent to “school learning”
- Labeled, enterprise, production data is equivalent to “experience”
- Artificially generated datasets are “lying” to the model
- Judgement = expertise (reasoning and heuristics)

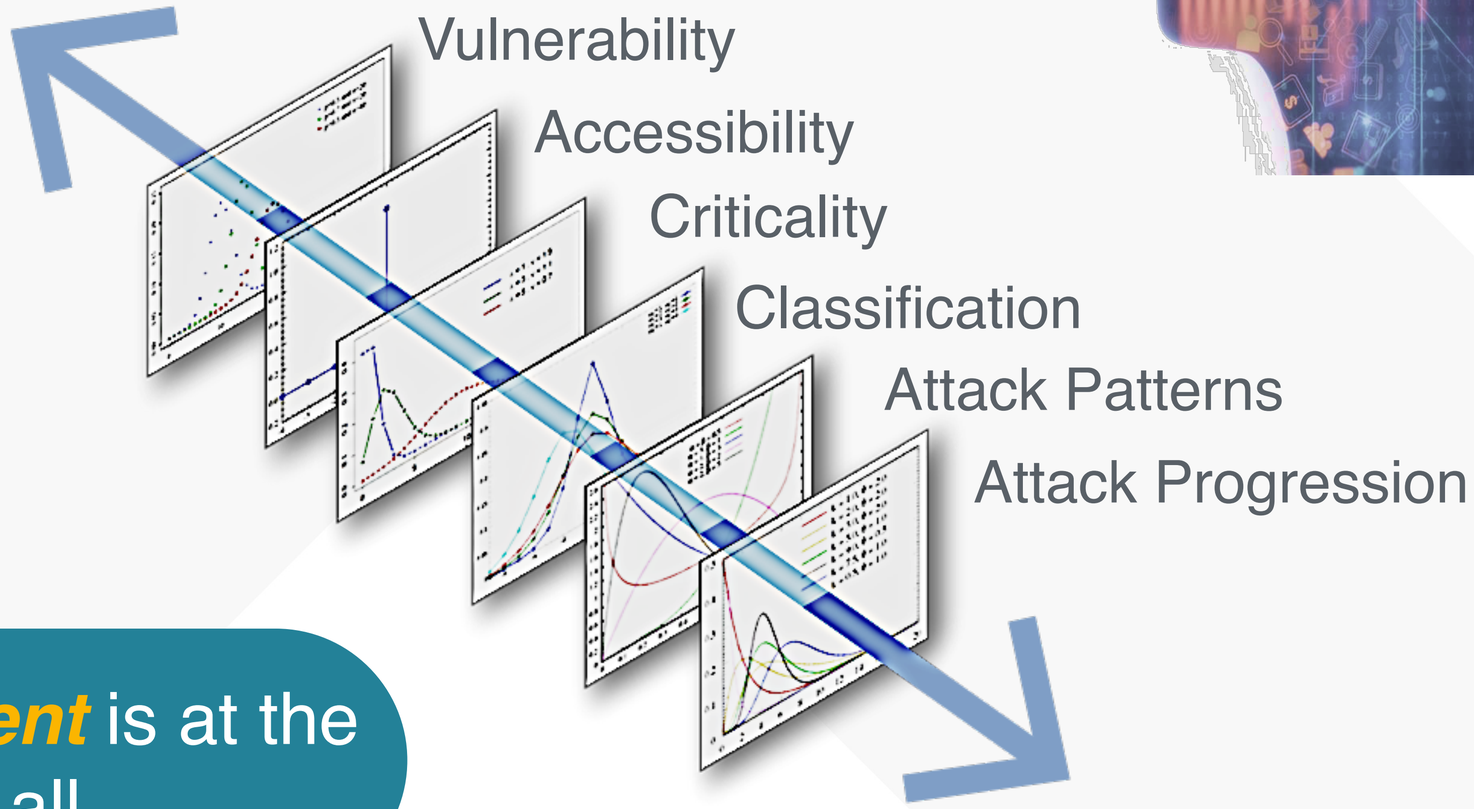
Uncertainty and Prediction

- Probability Theory
- "… *is just common sense reduced to calculation*"
  - – **Dead French Mathematician**
- But it really is more than that…



respond

Everything is a Distribution



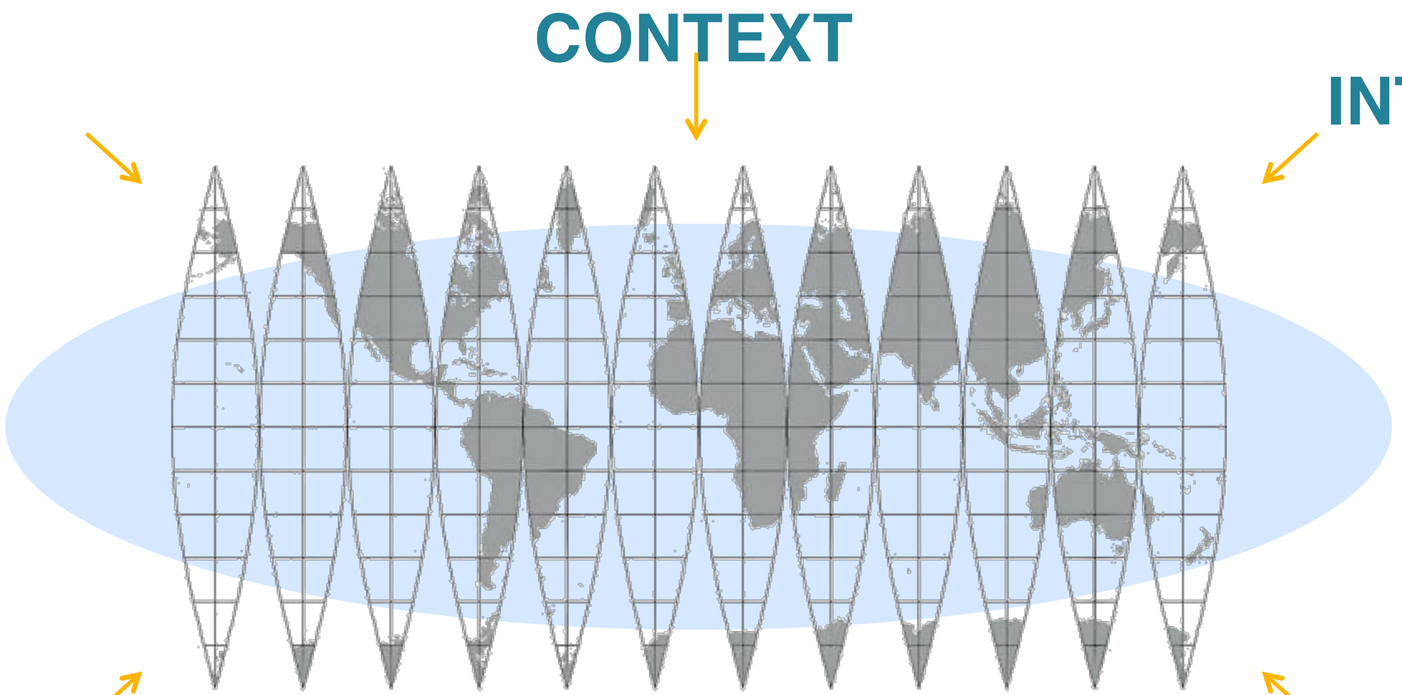
The ***most likely incident*** is at the center of them all.

* Possible States of the World

CONTEXT

TELEMETRY

INTELLIGENCE



REASONING

BEHAVIORS

PATTERNS

Security Operations

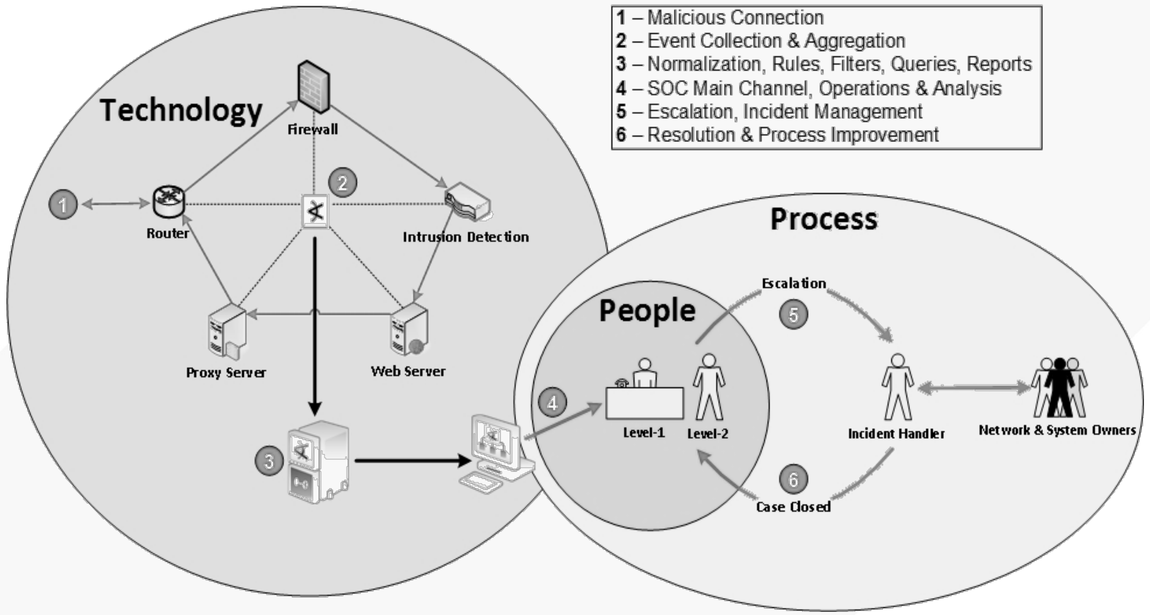
Is deep in process and procedures
designed to **minimize human error!**

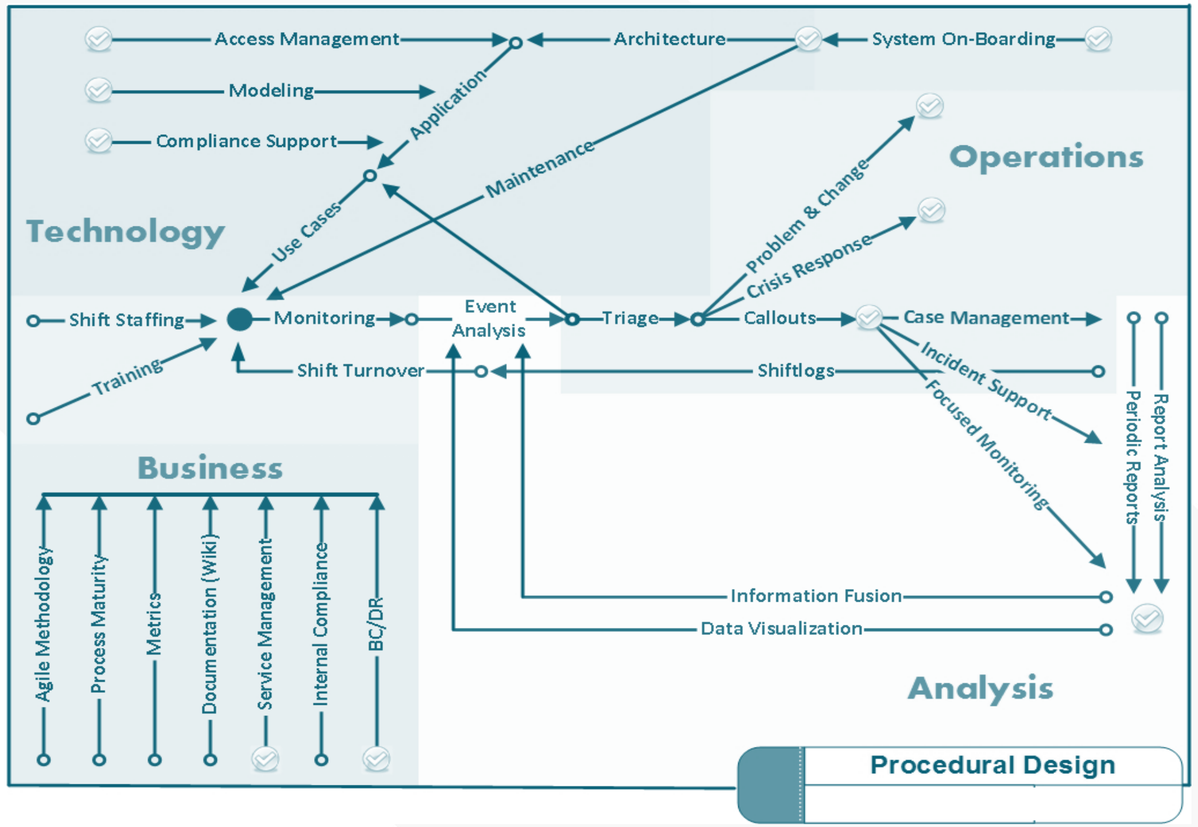
Must change and must change quickly.

Is **AI** the answer?

Task & Process Automation

Start with blueprints





respond

SIEM Rules are Highly Specific and Narrow

This analysis is derived from a complete list of SIEM rules boiled down into their most atomic form. Example below:

SIEM Rule	Category	Sub-category	Data Source	MSS	Customer 1	Decision Supported
Antivirus signatures out of date	Malware	Policy Violation	Endpoint			System Infected?
Multiple viruses detection on single system	Malware	Infection	Endpoint	MSS	Mature SOC	System Infected?
Mobile malware detected on executive BYOD device	Malware	Espionage	Mobile			System Infected?
Executable or large file downloads from uncategorized site	Malware	Exploit	Web Filter			System Infected?
Abnormal user agent	Malware	Infection	Web Filter			System Infected?
User clicked suspicious link	Malware	Phishing	Web Filter		Mature SOC	System Infected?
Distributed account scanning	Network Recon	Stealth	Authentication		Mature SOC	Network Compromised?
Port scan of critical internal system	Network Recon	Scanning	Network Sensor	MSS	Mature SOC	Network Compromised?
Internal scanning by unauthori						Network Compromised?
IDS alerts from the same sou						etwork Compromised?
Distributed port scanning						twork Compromised?
Top and bottom 10 aggrega						erations and Infrastructure
Report on assets currently be						perations and Infrastructure
Open to closed case ratio and ti						Operations and Infrastructure
Excessive account lockouts in a short timeframe	Penetration Attempts	Scanning	Authentication		Mature SOC	Account Compromised?
Multiple firewall denies followed by an accept from the same source	Penetration Attempts	Exploit	Firewall	MSS	Mature SOC	Network Compromised?
IPS event not blocked	Penetration Attempts	Exploit	Network Sensor	MSS	Mature SOC	Network Compromised?
Alert on all IDS/IPS high and medium events	Penetration Attempts	Exploit	Network Sensor	MSS	Mature SOC	Network Compromised?
Multiple IDS events to same host	Penetration Attempts	Scanning	Network Sensor	MSS	Mature SOC	Network Compromised?
IDS event matches known IoC	Penetration Attempts	Threat Intelligence	Network Sensor	MSS	Mature SOC	Network Compromised?
RDP connection where source is not an internal address	Penetration Attempts	Remote Access	Authentication	MSS	Mature SOC	System Compromised?
IDS event related to critical systems	Penetration Attempts	Exploit	Context	MSS	Mature SOC	System Compromised?
Unusual system restarts on critical servers (production) without approved change ticket	Penetration Attempts	Exploit	Endpoint			System Compromised?
New system process created outside of baseline on critical server	Penetration Attempts	Suspicious Process	Endpoint			System Compromised?

MSSP Typical Rules = 25% of Total
Mature Security Operations Center = **45% of Total**

TOO MANY FACTORS TO CONSIDER

Rules and Queries

Telnet protocol used

IRC port accessed

Security logs cleared by user

5 failed logins

Default account accessed

Malware not cleaned

Brute force attempted

SQL injection attempt

LONG TAIL DECISION ANALYSIS

-VS-

Robotic Decision Automation

Network Intrusion
- Network
- Attack signatures
- Perimeter & internal

Endpoint Protection
- Host-based agent
- Malware signatures
- User environment

URL Filtering / Proxy
- Internet browsing
- Suspicious connects
- Network chokepoint

Endpoint Detection
- Operating system
- All system activity
- Servers & users

Signatures

Analytics

Patterns

History

Context

Assets

Behaviors

Intelligence

$$f(\theta,\lambda)=\sum_{\mathbf{x}}\left(\prod_{\lambda_x:x\sim\mathbf{x}}\lambda_x\prod_{\mathbf{f}_i\sim\mathbf{x}}\theta_{\mathbf{f}_i}\right)$$

respond

Aligning for the Future

Let’s put these two back together again.

Match the Math to the Problem

PROBLEM

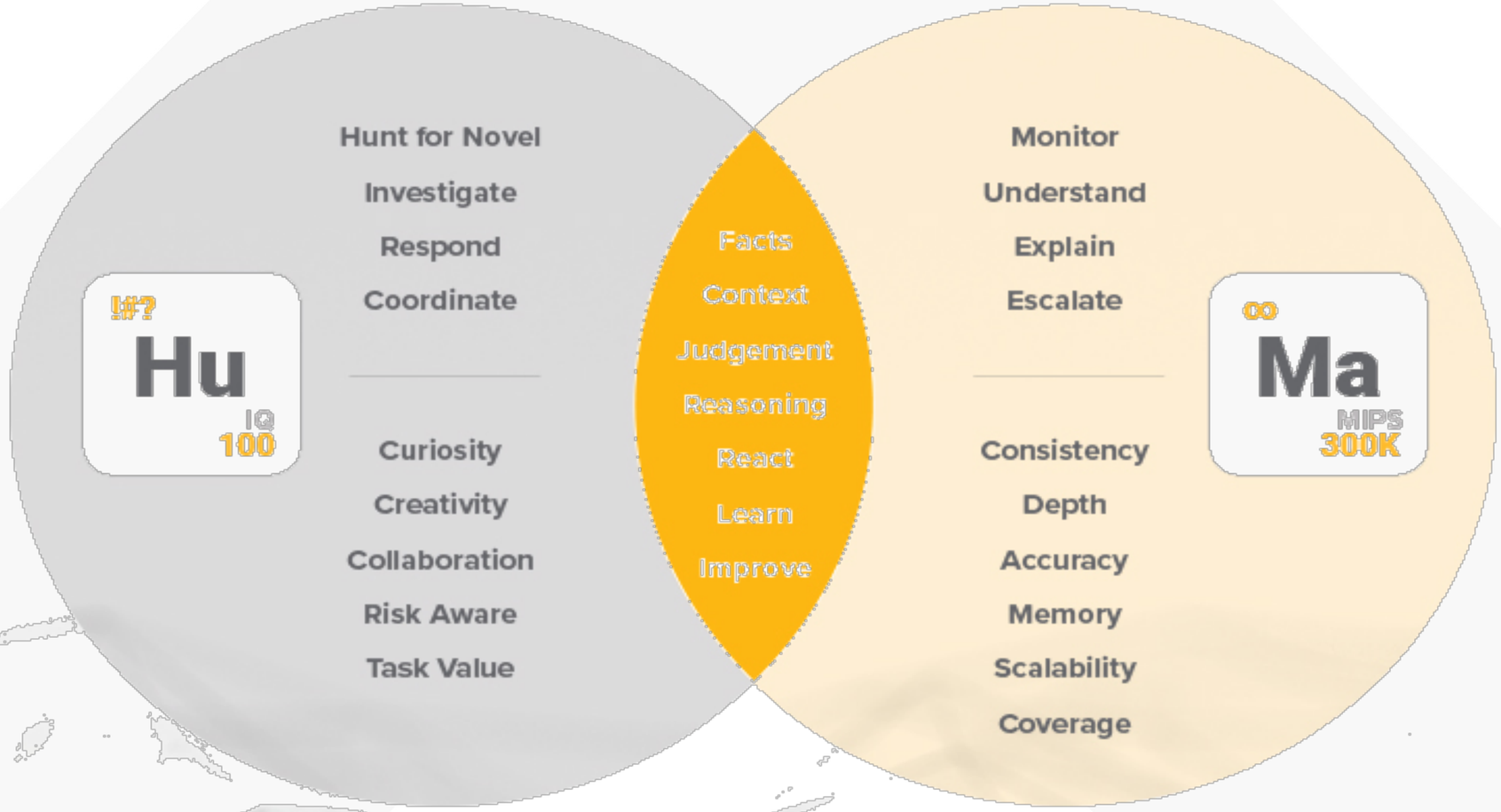
- NIDS false positive reduction
- Malware classification
- Behavioral baselines
- Recognition (signature, image)
- Anomalies, how malicious?
- Understand relationships
- **Complicated problem...**

MATHEMATICS

- K-Means clustering
- Bayesian filters
- Statistics
- Deep learning
- Anomaly detection
- Conditional probability
- **Hybrid solution!**

Aligning for the Future

Human + Machine in Security Operations



Perceptive

Transactional

respond

How this works...

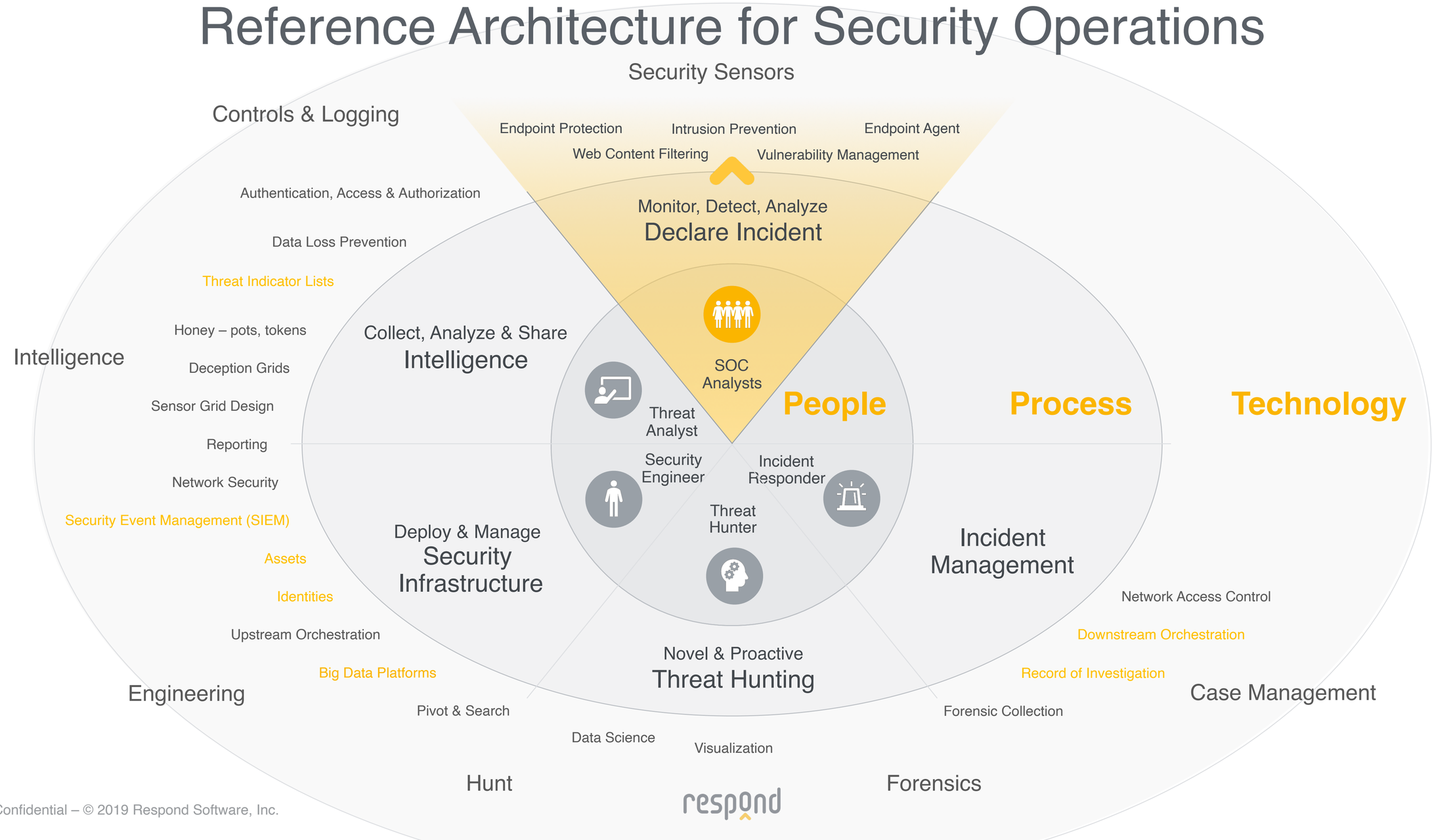
From:

1. Subject matter expertise and experience
2. Careful definition of a fact
3. Problem solving, reasoning process
4. Initial judgements and labelled data
5. Cross-customer learning
6. Deeper questioning of the model
7. Improved inputs (data, arch., config.)

Turned into:

1. Relevant facts (evidence, features)
2. Single feature of a model (meaning)
3. Probabilistic models
4. Informed decision of a “rookie” model
5. Highly experienced decision (vs. human)
6. New useful information, optimal mix
7. Continuous improvement

Reference Architecture for Security Operations

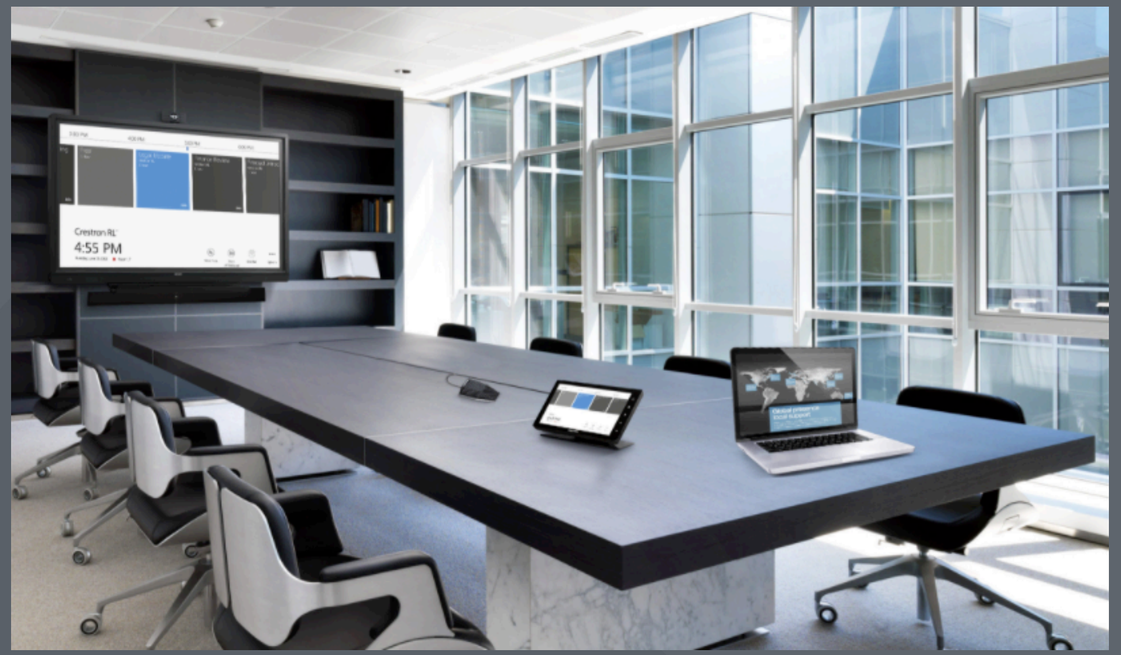


“Monitoring for Bad”

← OLD

NEW →

“Managing Bad”



respond

Thank You

FOLLOW

www.respond-software.com/blog

https://www.linkedin.com/company/respond-software-inc./