



Enterprise Strategy Group | Getting to the bigger truth.™

Security Analytics in the Cloud Era—Top 5 Industry Trends

Christina Richmond, Principal Analyst

December 10, 2019

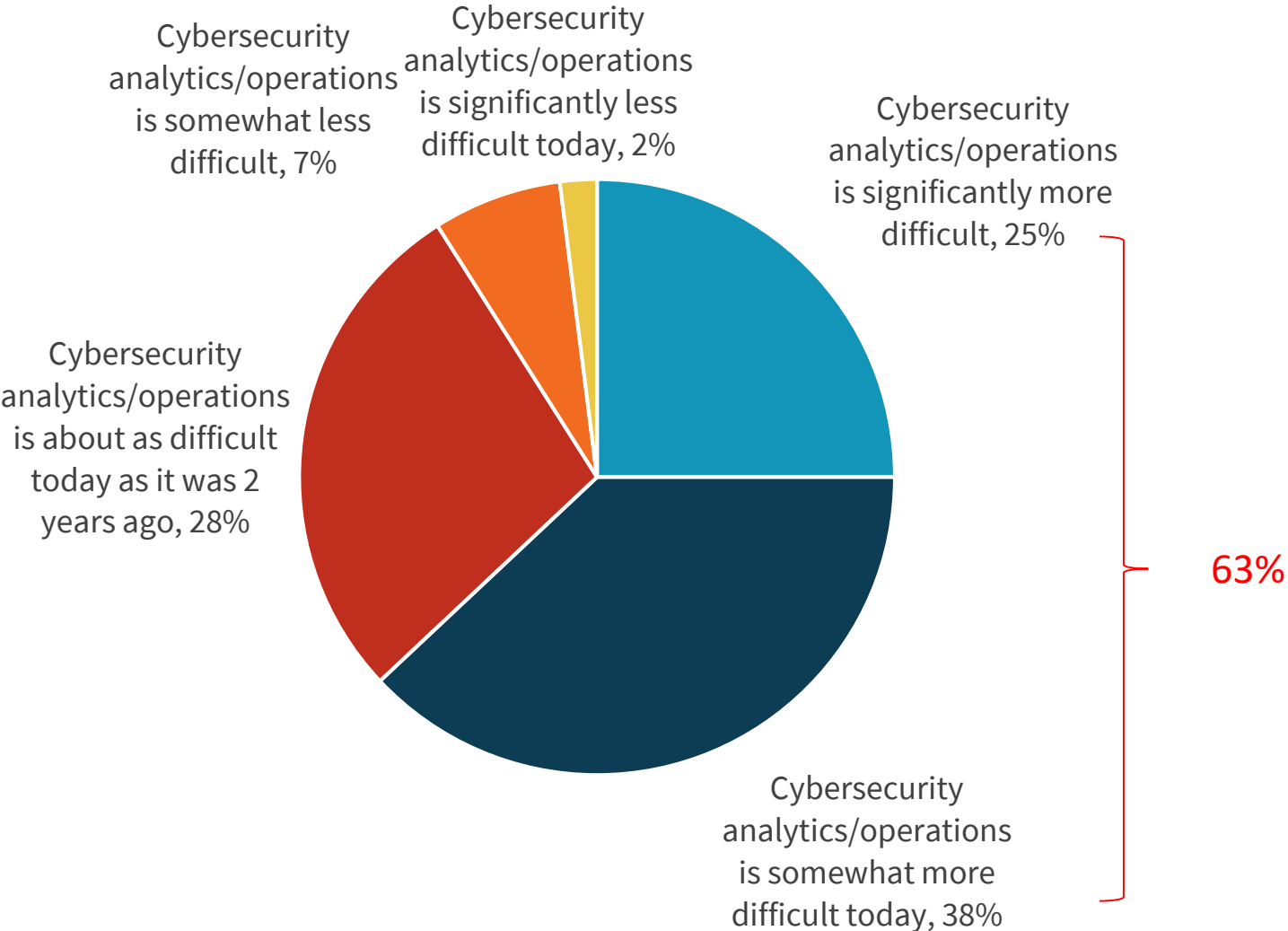
PREPARED BY ESG FOR



Agenda

- Impact of external and internal trends on the SOC
- The security data pipeline
- Limitations of traditional SIEM tools
- Staffing and skills
- The onset of cloud-based security analytics and operations
- Strategic directions

Nearly Two-thirds Believe Security Analytics and Operations Is More Difficult Today



Question text:
Which of the following best describes your opinion about cybersecurity analytics and operations? (Percent of respondents, N=406)

Why? Changing Threat Landscape and Security Operations Model

The threat landscape is evolving and changing rapidly

41%

We collect and process more security data today than we did two years ago

35%

The volume of security alerts has increased over the past 2 years


34%

The attack surface has grown over the past two years

30%

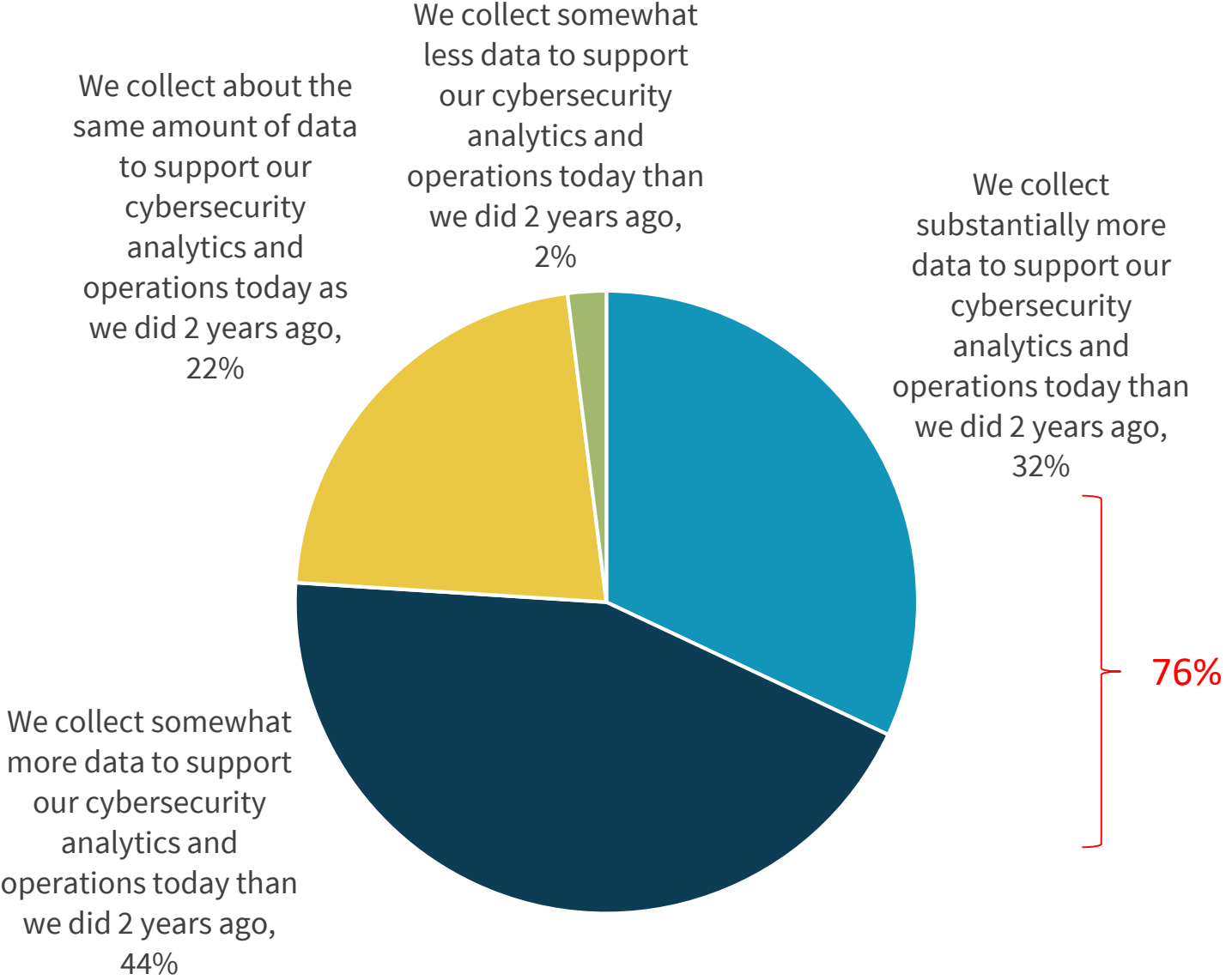
Question text:

You indicated that cybersecurity analytics and operations is more difficult today than it was 2 years ago. What are the primary reasons why you believe this to be true? (Percent of respondents, N=256, three responses accepted)



Trend 1:
The security data pipeline dilemma:
More data, more problems

Trend Toward Larger Volumes of Security Data



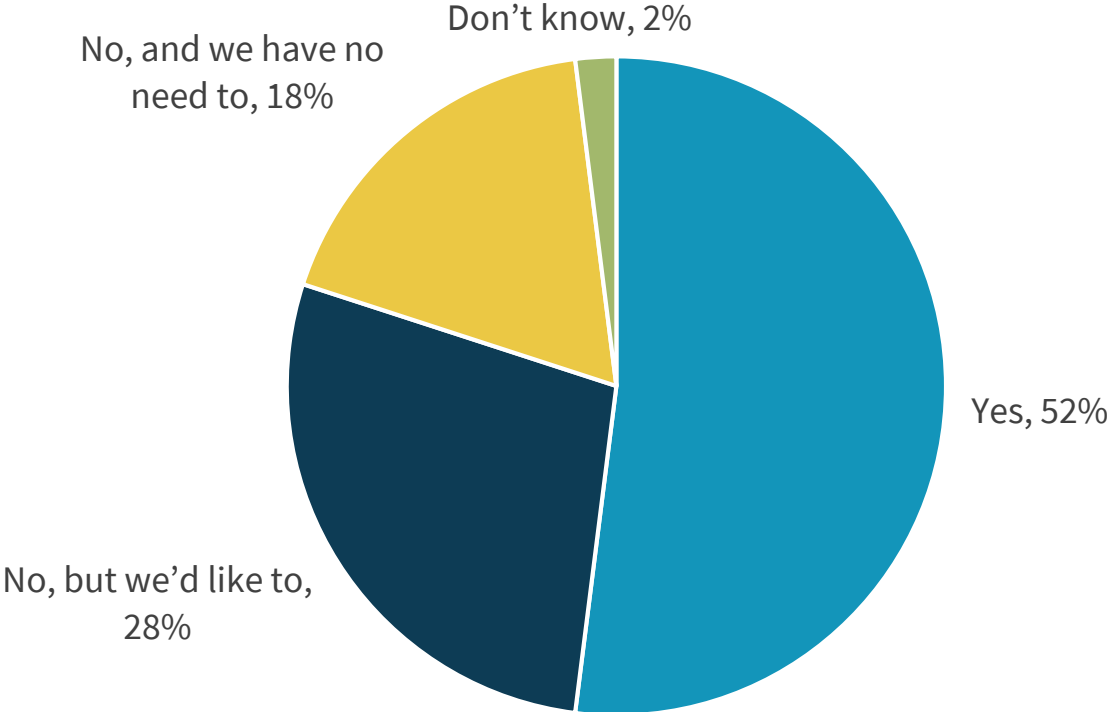
Question text:

Think about the amount of data your organization collects to support all its information security activities (i.e., risk management, regulatory compliance, incident detection/response, security analysis/forensics, etc.). How has the amount of data your organization collects to support its information security activities changed in the last 2 years? (Percent of respondents, N=406)



Increasing Security Data Retention

Change in security data retention periods



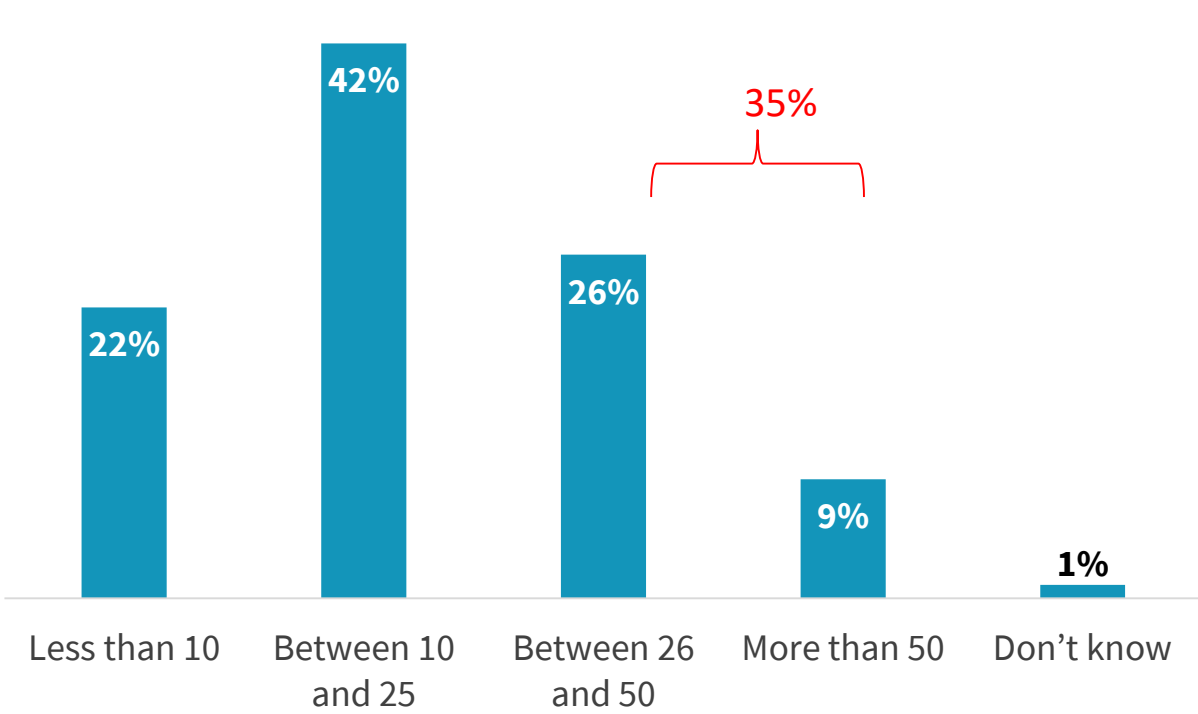
Question text:
Is your organization retaining security data for longer periods of time now than it did in the past? (Percent of respondents, N=406)

A person wearing a dark cap and a dark hoodie is seen from behind, sitting at a desk in a server room. They are looking at a computer monitor displaying various data visualizations, including a line graph and a network diagram. The room is dimly lit with blue light from the screens. In the background, another person is visible, also working at a computer. The overall atmosphere is technical and focused.

Trend 2:
Traditional on-premises SIEM
is an incomplete solution

SIEM, Threat Intelligence, and EDR Most Commonly Used Security Analytics and Operations Tools

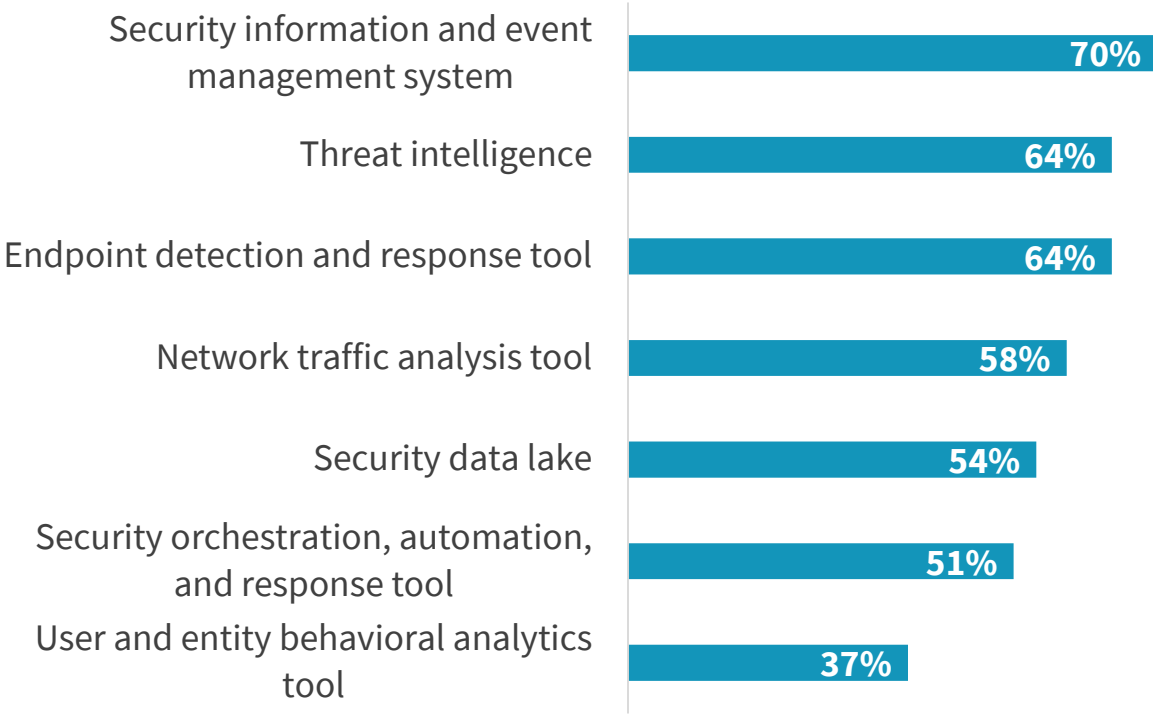
Total security analytics tools in use



Question text:

Approximately how many security technologies (commercial, open source, and homegrown) is your organization using to support its efforts around security analytics and operations? (Percent of respondents, N=406)

Types of security analytics tools used regularly

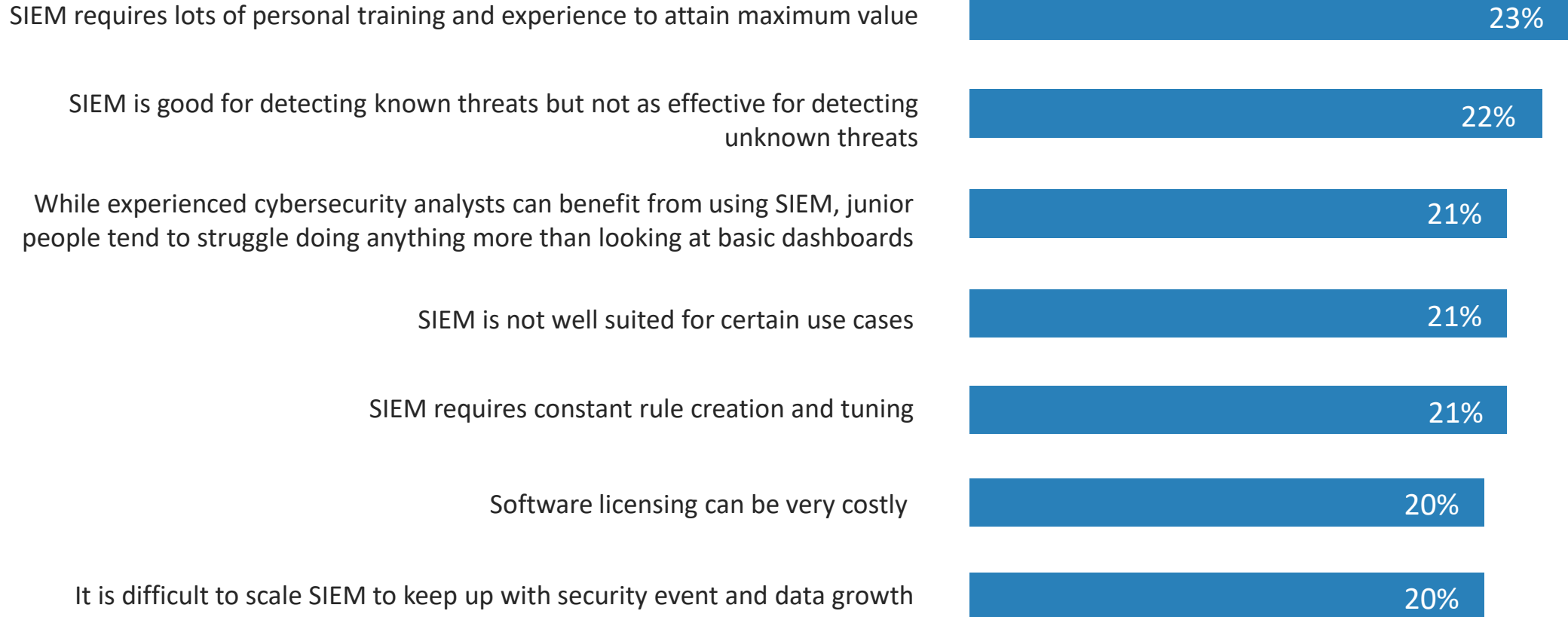


Question text:

Which of the following types of security analytics and operations tools does your organization use on a regular basis (i.e., deployed in production and used daily as part of security operations)? (Percent of respondents, N=406, multiple responses accepted)



SIEM Limitations include Personnel Demands and Overhead



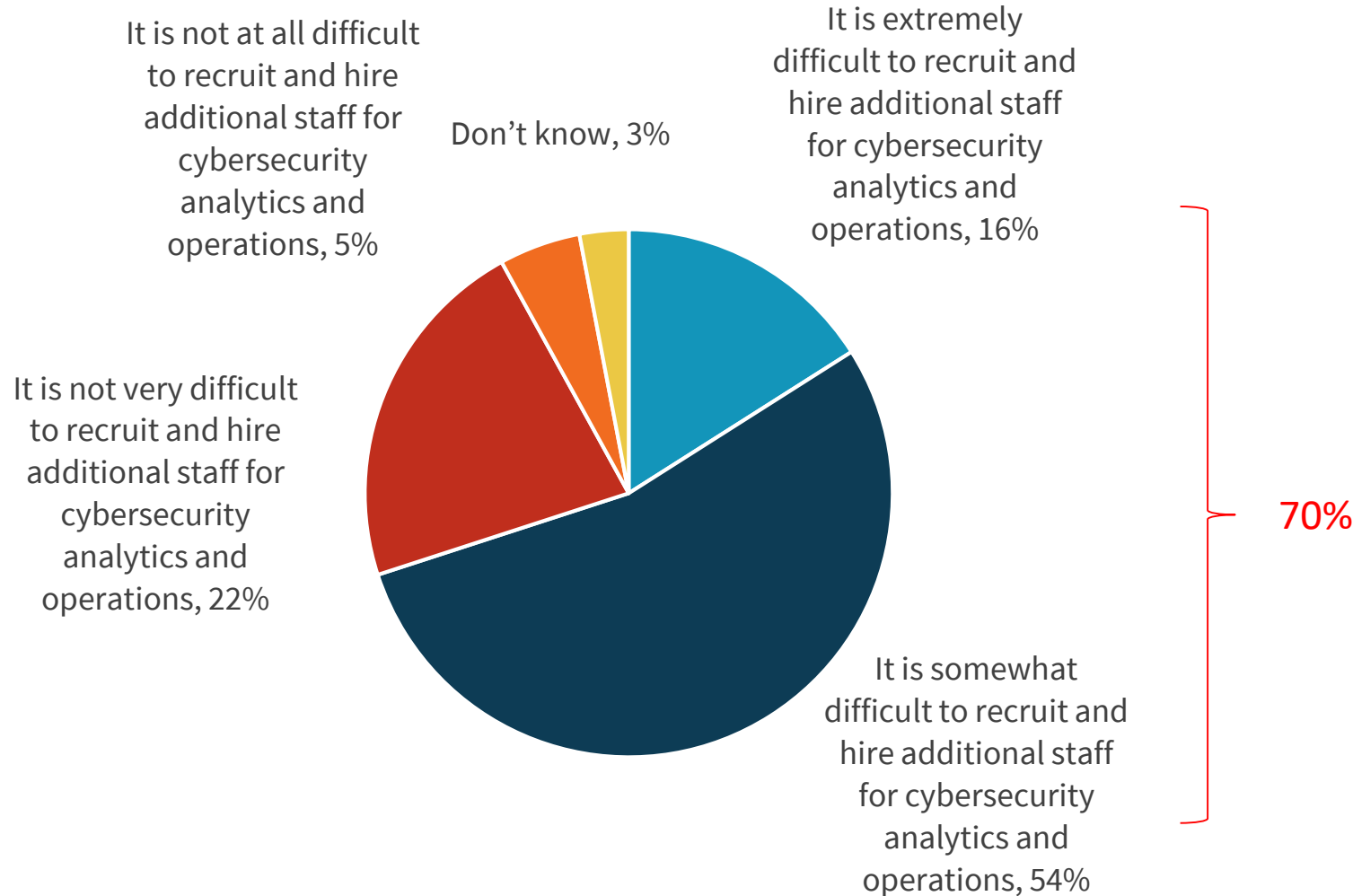
Question text:
What are the most challenging attributes of SIEM for your organization?
(Percent of respondents, N=384, three responses accepted)

A man in a plaid shirt is sitting at a desk in a dimly lit office, looking at several computer monitors. The monitors display various data visualizations, including bar charts, line graphs, and code snippets. The overall atmosphere is professional and focused on data analysis.

Trend 3:
Staffing and skills shortages
create opportunity for
managed services

75% of survey respondents claim that the cybersecurity skills shortage has had an impact on their organization's security operations

Staffing and Skills Issues are Commonplace

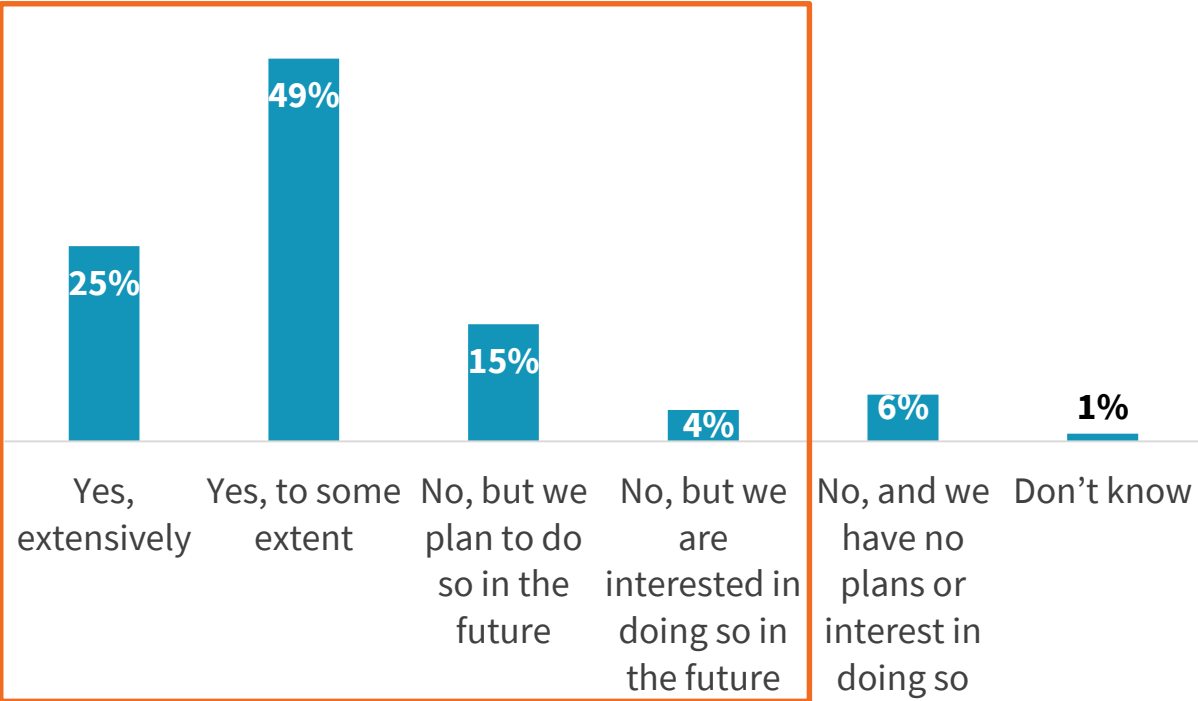


Question text:

When your organization actively recruits and hires cybersecurity staff specifically for analytics and operations, how would you characterize this effort? (Percent of respondents, N=406)

Majority Use Security Analytics Managed Services and Most Will Increase This Usage

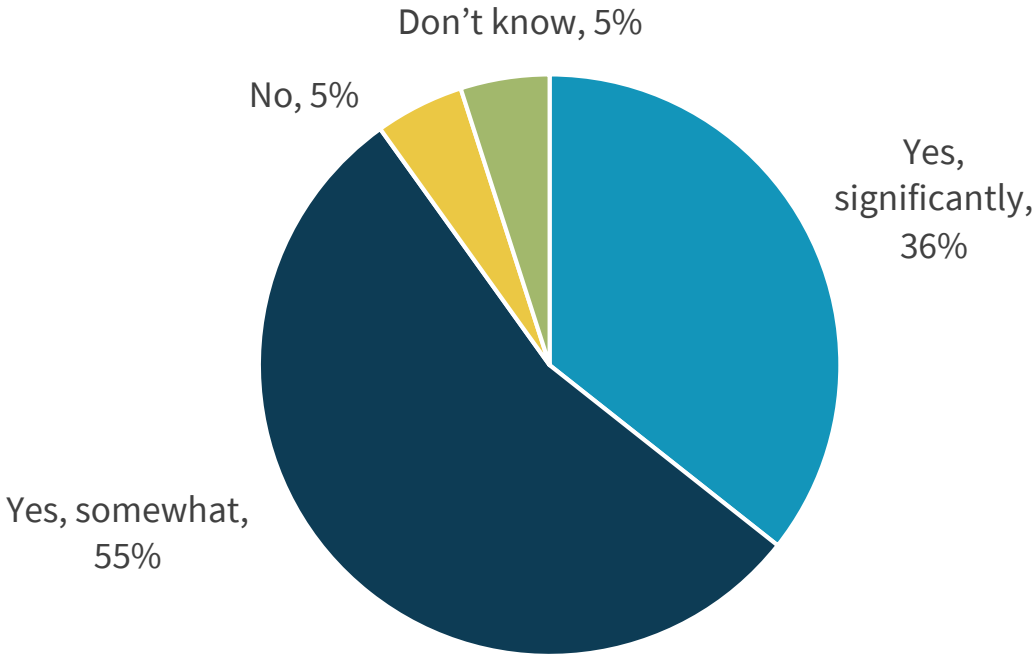
Usage of managed services for security analytics



Question text:

Does your organization use managed security services for any aspect of security analytics and operations? (Percent of respondents, N=406)

Expected change in security analytics managed service usage



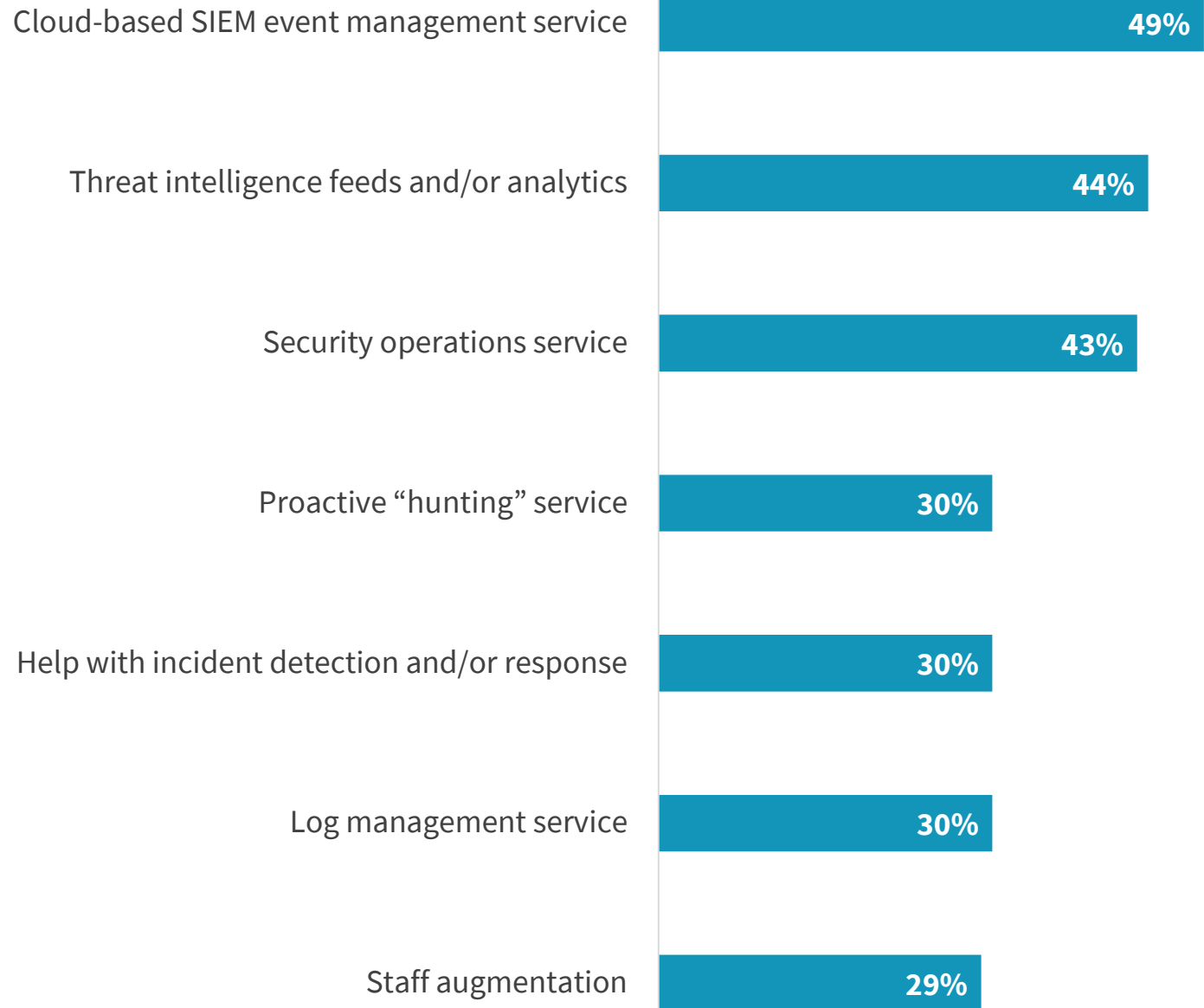
Question text:

Will your organization increase its use of managed security analytics and operations services over the next 12 to 18 months? (Percent of respondents, N=377)

Future Managed Services Plans

Question text:

What type of managed security services does your organization use or plan to use for security analytics and operations? (Percent of respondents, N=377, multiple responses accepted)





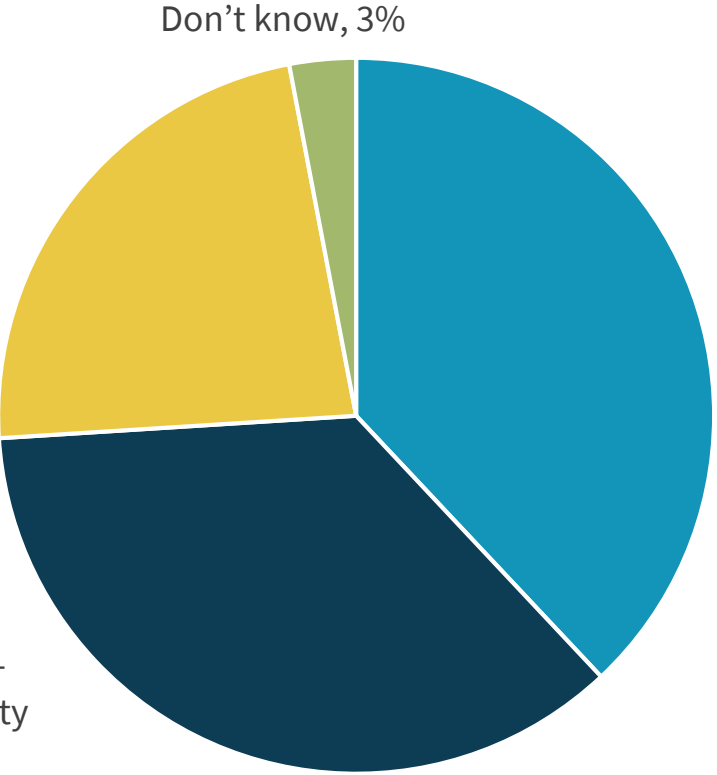
Trend 4:
Cloud serves dual role as source of
and tool for security analytics data

Cloud-based Security Analytics and Operations

- 82% of respondents agree that their organization is moving a large volume of workloads to the public cloud
- 33% say that monitoring, reporting, and analysis of cloud-based workloads is a common SIEM use case
- 38% of organizations are already using public cloud-based security analytics/operations tools today

Alternative Strategies for Cloud-based Security Analytics Technology Skew Toward Movement and Replacement

Supplement an existing security analytics technology with additional capabilities delivered by a cloud-based security analytics provider, 23%

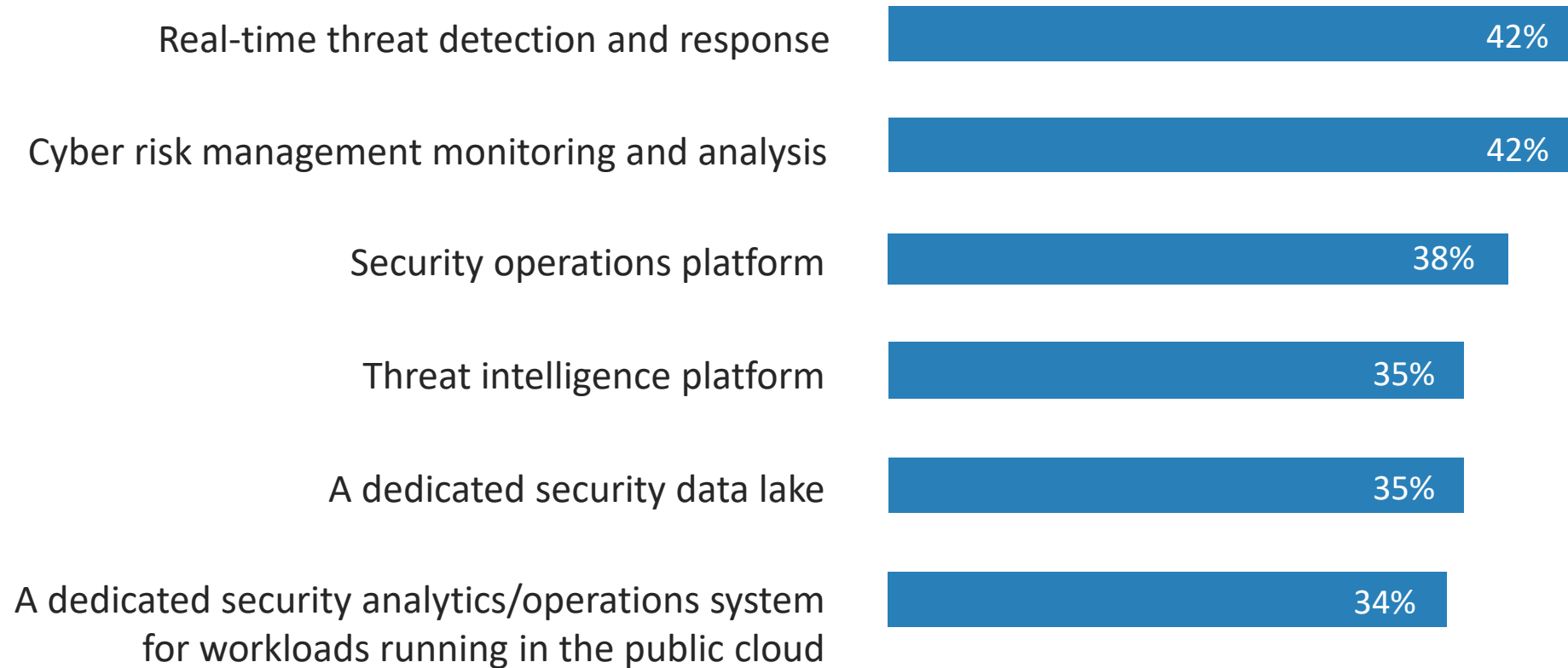


Move some or all its existing security analytics technology infrastructure to the cloud, 38%

Replace its on-premises security analytics technology with a cloud-based alternative, 36%

Question text:
Which of the following best describes your organization's likeliest security analytics and operations strategy with regards to public cloud services?
(Percent of respondents, N=379)

Cloud-based Security Operations Technology Considerations



Question text:

For which of the following use cases is your organization using – or would your organization consider using – cloud-based security analytics? (Percent of respondents, N=379, multiple responses accepted)



Trend 5:
Future security analytics plans will
include automation/orchestration
and machine learning

Security Operations Automation and Orchestration



65%

Question text:

Has your organization deployed – or does it plan to deploy – technologies designed for security analytics and operations automation and orchestration? (Percent of respondents, N=406)

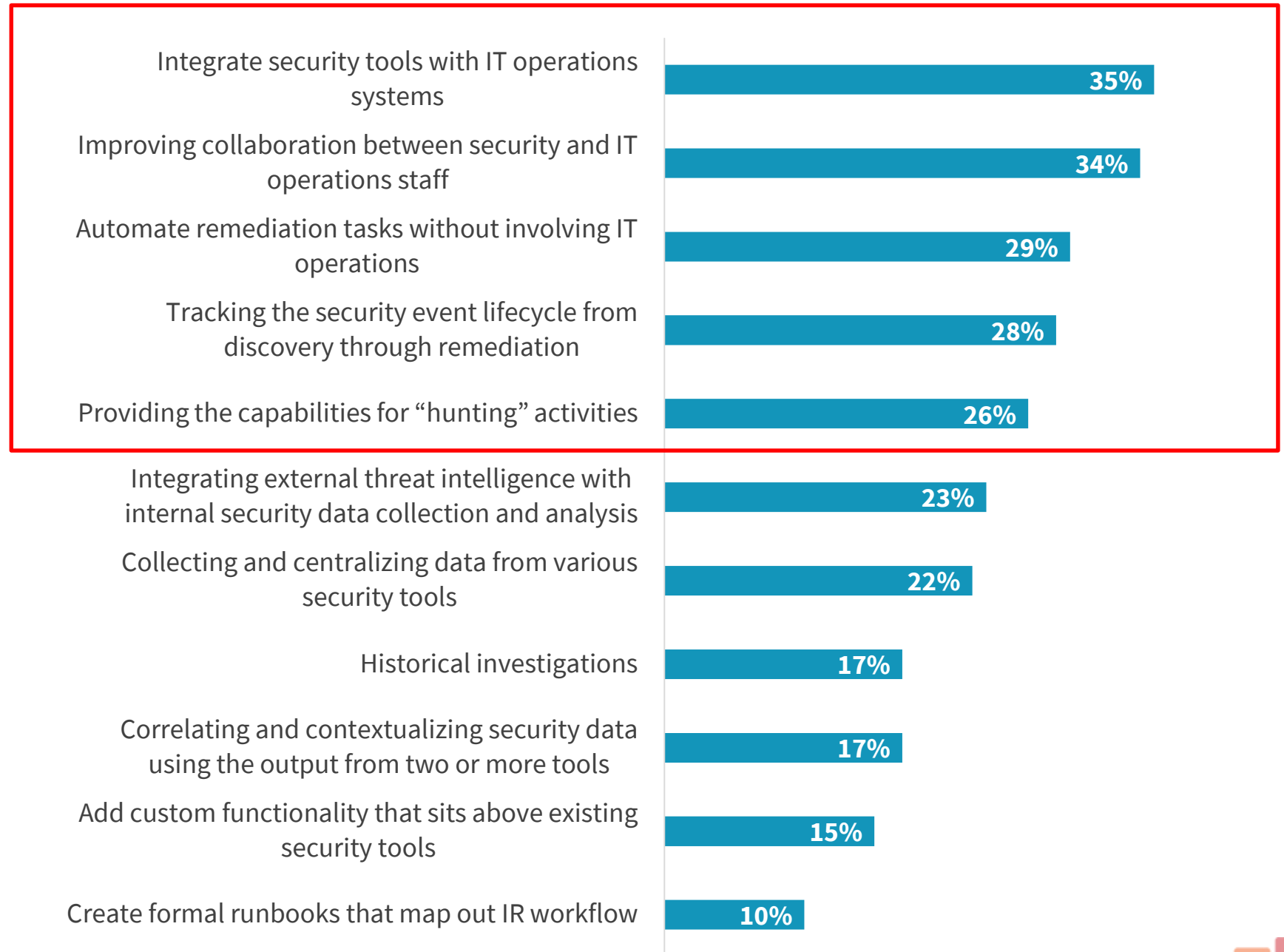


Top Use Cases for Security Operations Automation and Orchestration

Emphasis on bridging security and IT operations

Question text:

What types of tasks are or would be the top priorities for security operations automation/orchestration? (Percent of respondents, N=366, three responses accepted)



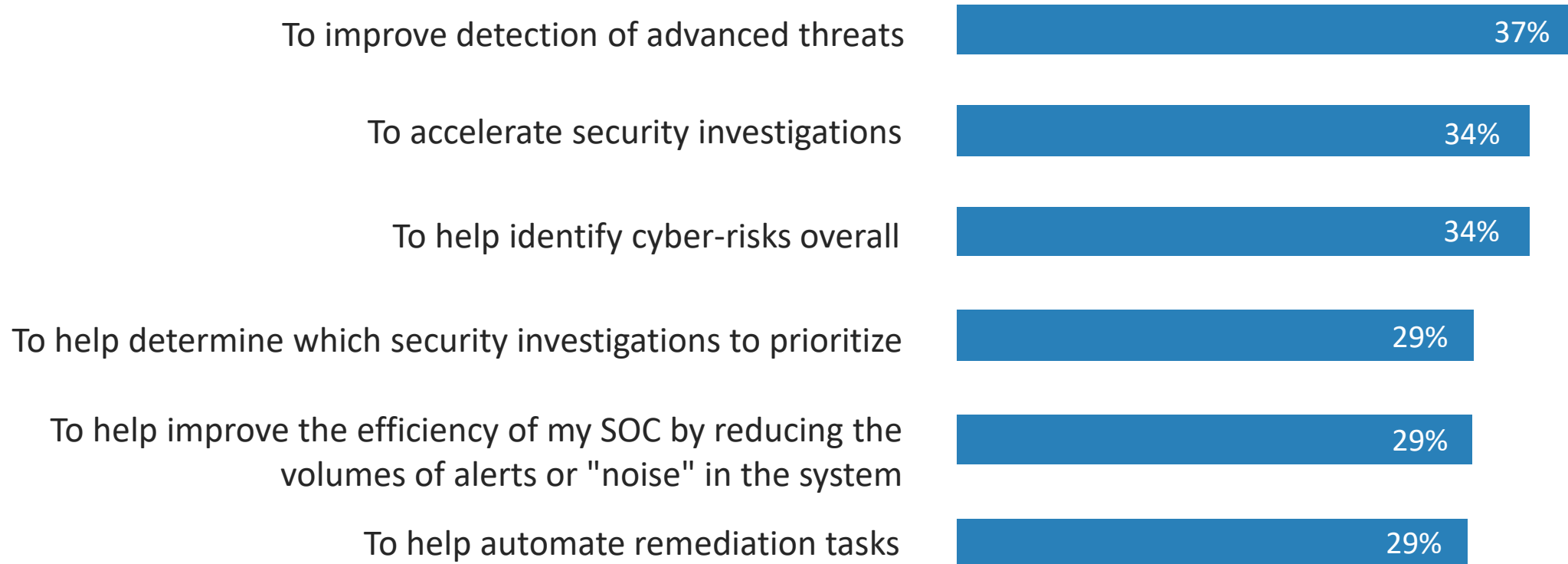
Use of Machine Learning for Security Analytics and Operations



Question text:

Does your organization leverage – or does it plan to leverage – machine learning technologies for security analytics and operations? (Percent of respondents, N=406)

Primary Reasons for Machine Learning Include Acceleration and Accuracy Improvements



Question text:

What are the primary reasons for your organization's usage of or interest in machine learning to support analytics and operations? (Percent of respondents, N=363, multiple responses accepted)

The Bigger Truth

- The current security analytics/operations model is unsustainable
- All indicators point to the cloud
- Managed services should be a part of all solutions
- Next-generation SOC technology must include process automation and advanced analytics



Thank You!

Please contact us for more information

Christina Richmond – Principal Analyst
christina.richmond@esg-global.com



www.esg-global.com



[@ESG_Global](https://twitter.com/ESG_Global)



www.facebook.com/ESGglobal



www.linkedin.com/company/enterprise-strategy-group



www.youtube.com/user/ESGglobal



Chris Calvert

Cofounder & VP of Strategy

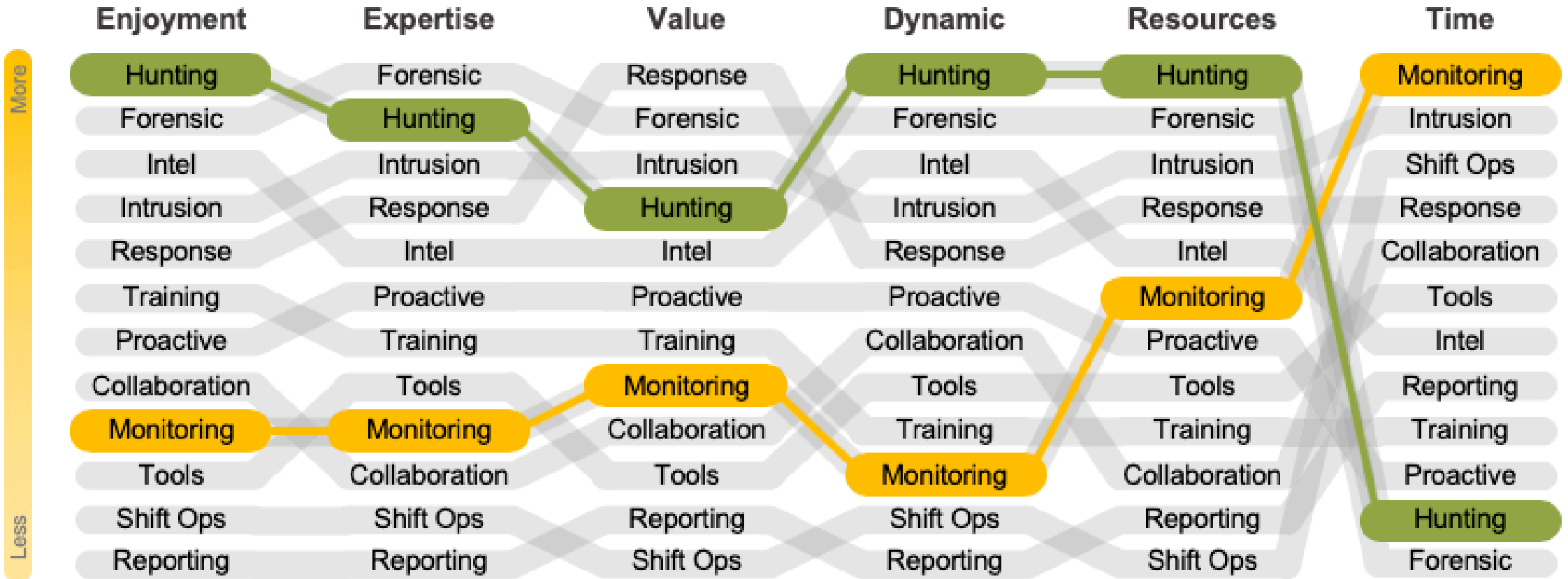
Agenda

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



Voice of the Analyst Survey

Activity Rankings Across Perceptual Dimension



Voice of the Analyst Survey, [Cyentia Institute](#)

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 = $A \rightarrow B$, “Ability to learn or act intelligently” – Andrew Ng



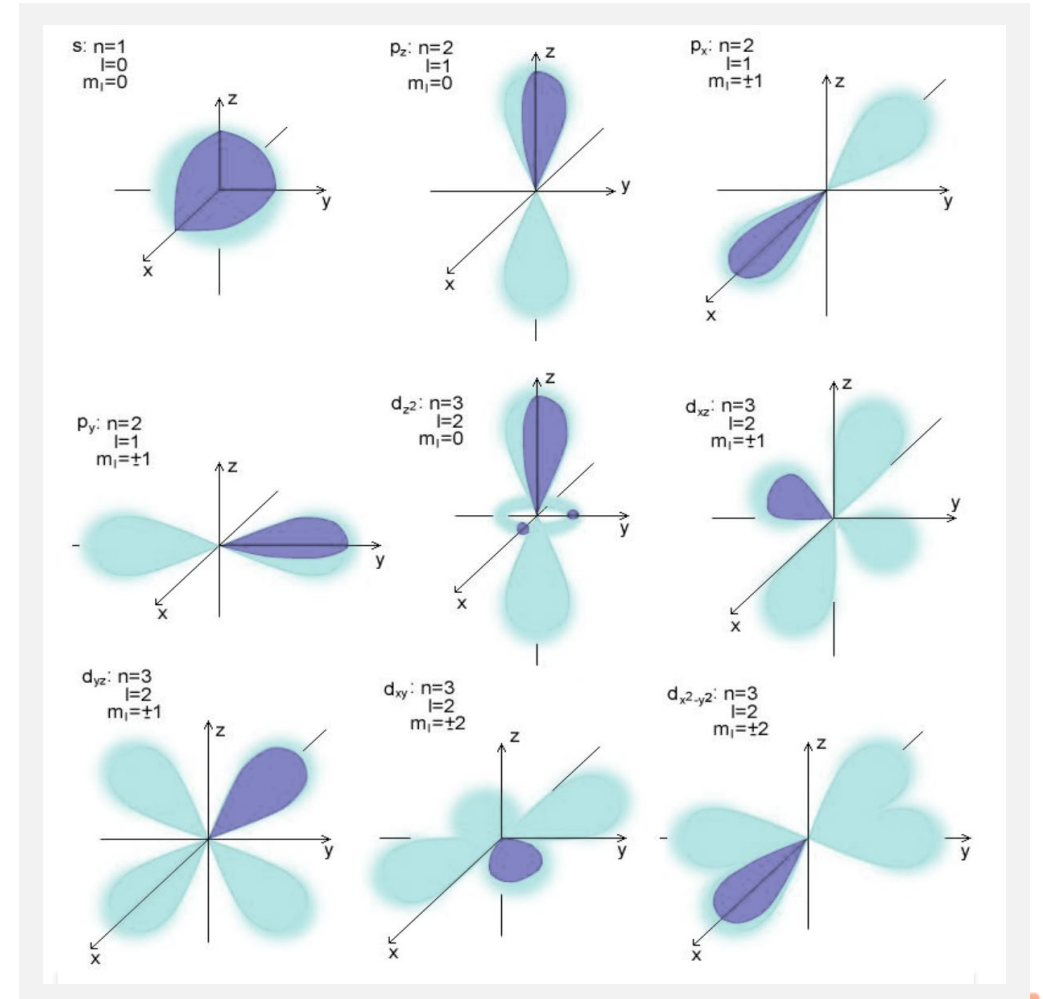
Learning Software

Data is meaningless without judgement

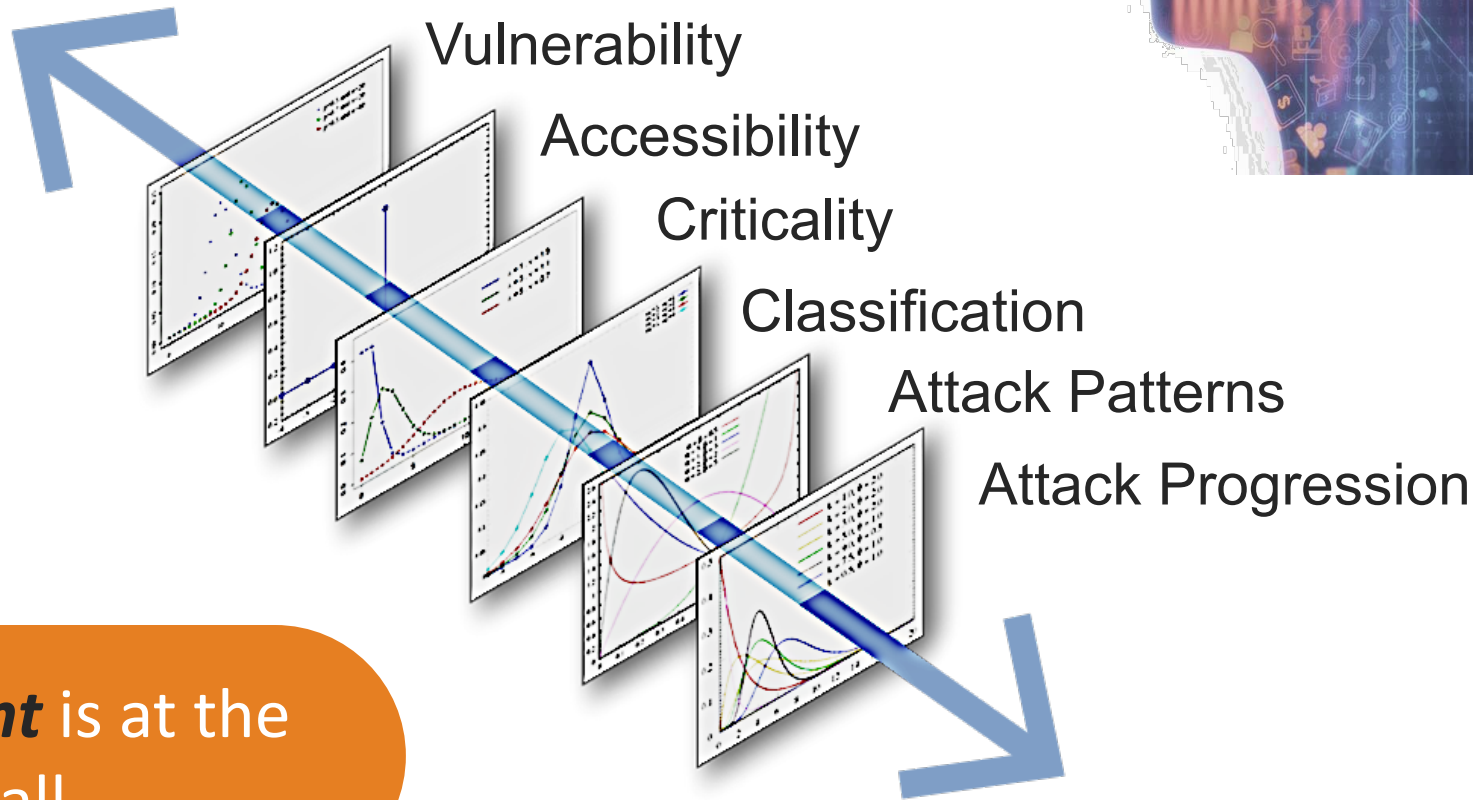
- Lab data is equivalent to “school learning”
- Labeled, enterprise, production data is equivalent to “experience”
- Artificially generated datasets are “lying” to the model
- Judgement = expertise (reasoning and heuristics)

Uncertainty and Prediction

- Probability Theory
- “... is just common sense reduced to calculation”
– Dead French Mathematician
- But it really is more than that...



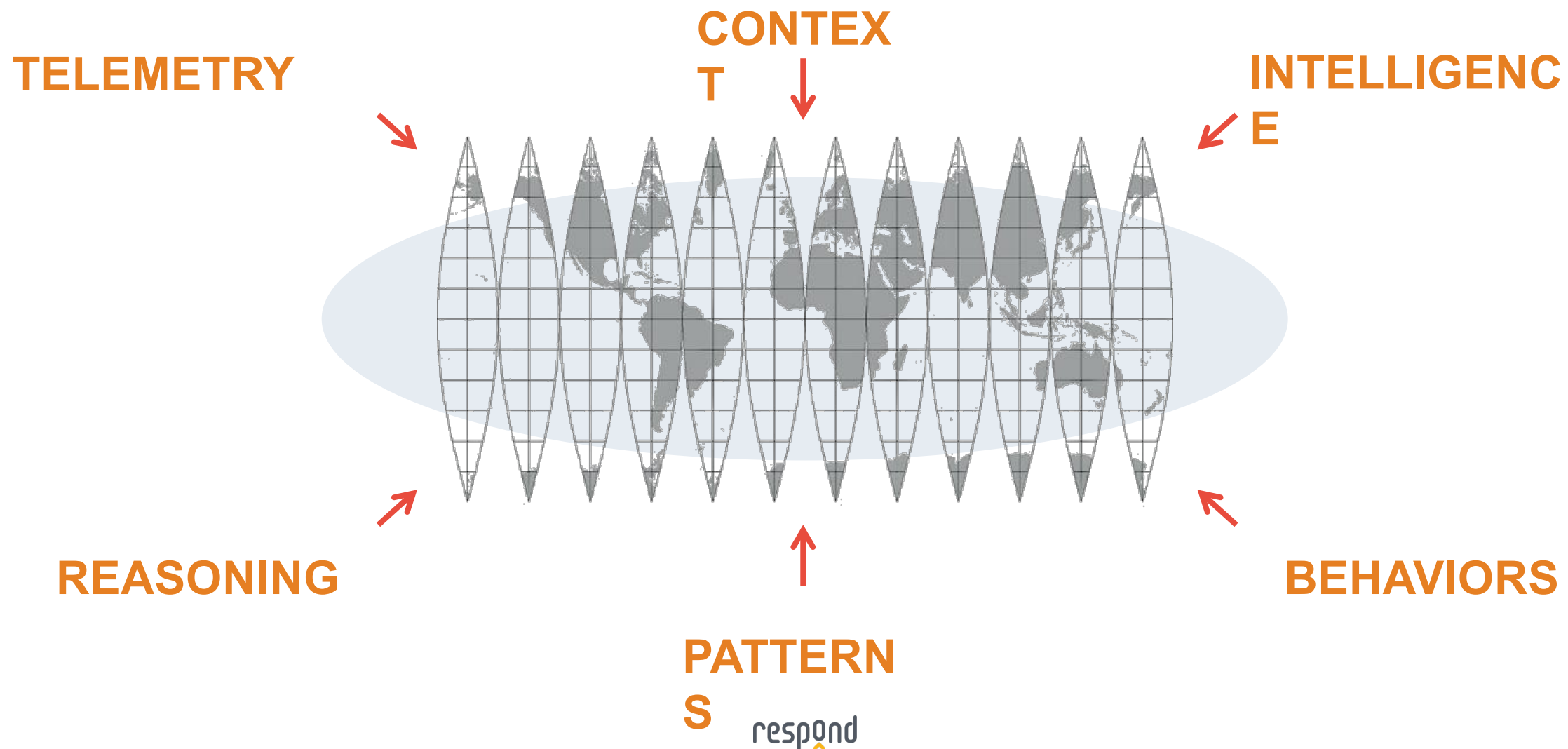
Everything is a Distribution



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



* Possible States of the World





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

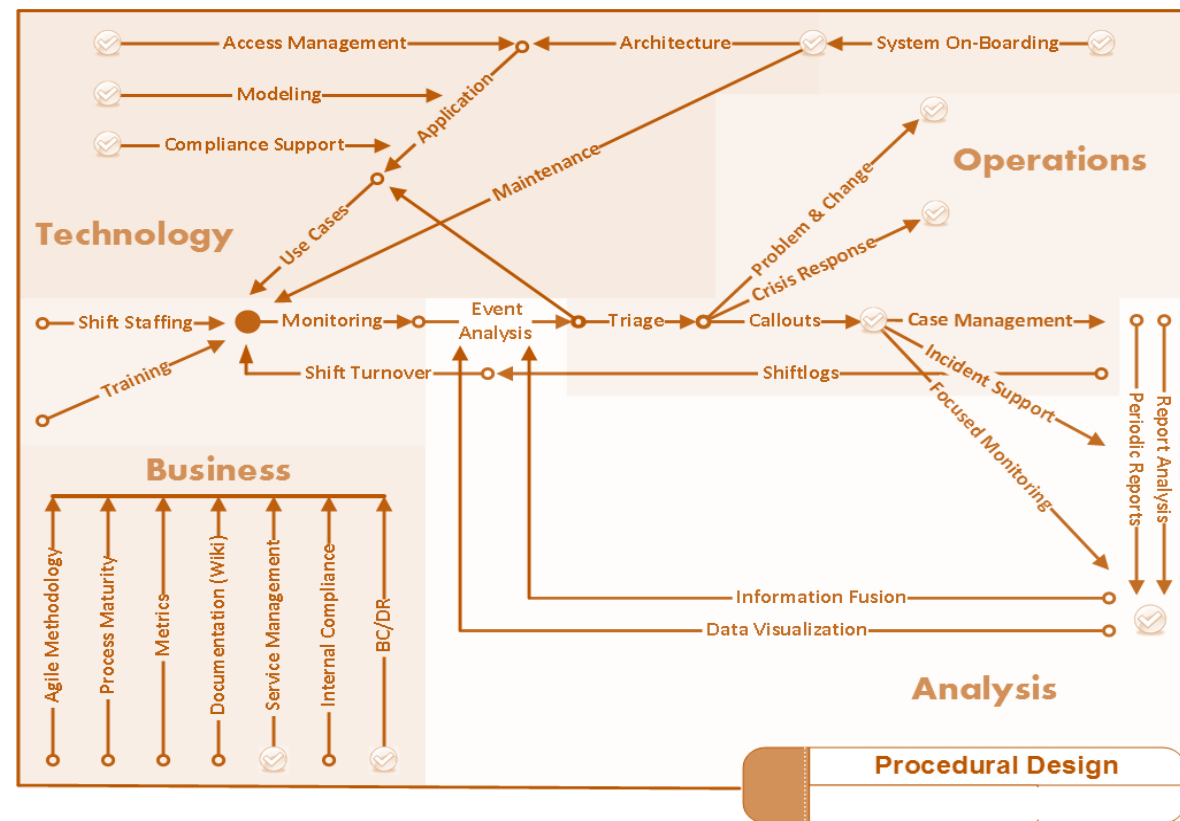
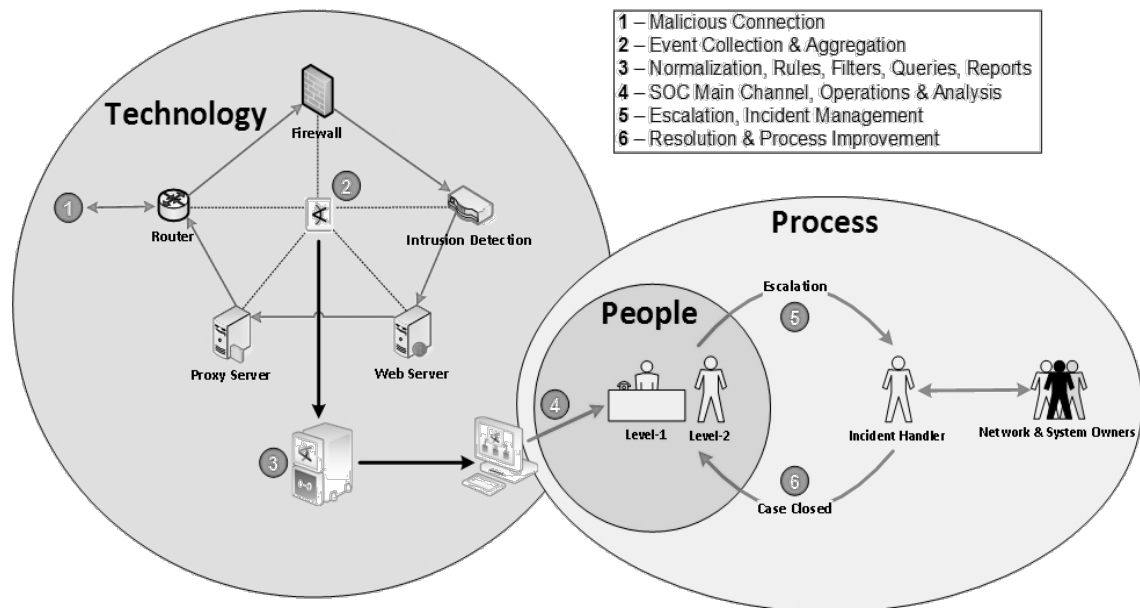
Must change and must change quickly.

Is **AI** the answer?

SECURITY OPERATIONS ON AI

Task & Process Automation

Start with blueprints



SECURITY OPERATIONS ON AI

SIEM Rules are Highly Specific and

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

Network

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 unauthorized	Network Recon	Scanning	Network Sensor			Network Compromised?
IDS alerts from the same source	Network Recon	Scanning	Network Sensor			Network Compromised?
Distributed port scanning	Network Recon	Scanning	Network Sensor			Network Compromised?
Top and bottom 10 aggregated	Network Recon	Scanning	Network Sensor			Operations and Infrastructure
Report on assets currently being	Network Recon	Scanning	Network Sensor			Operations and Infrastructure
Open to closed case ratio and time	Network Recon	Scanning	Network Sensor			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

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



-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

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



Let's put these two back together again.

ALIGNING FOR THE FUTURE

Match the Math to the Problem

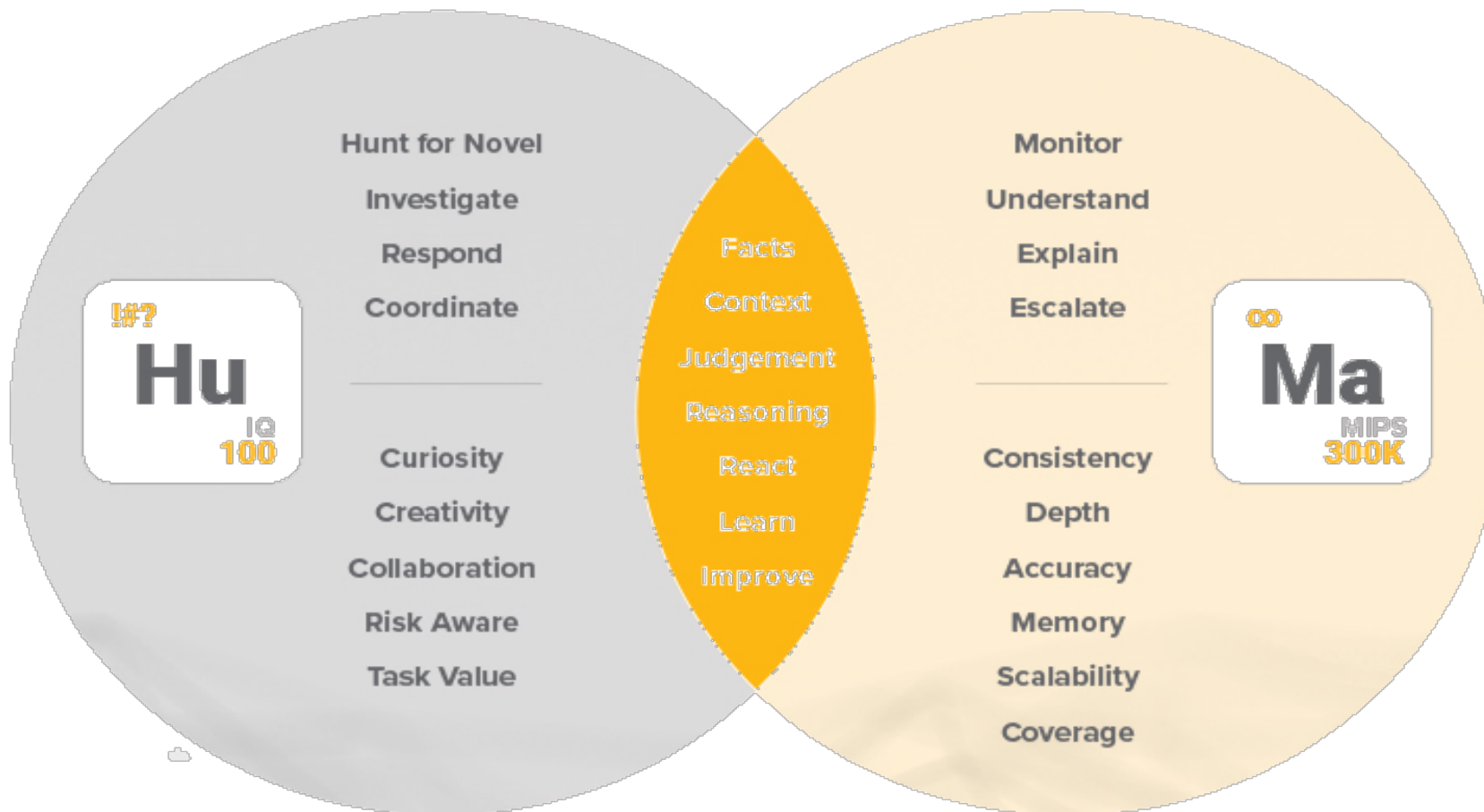
PROBLEM

- 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!**

Human + Machine in Security Operations



Perceptive

Transactional

TEACHING AND LEARNING FROM MACHINES

How this works...

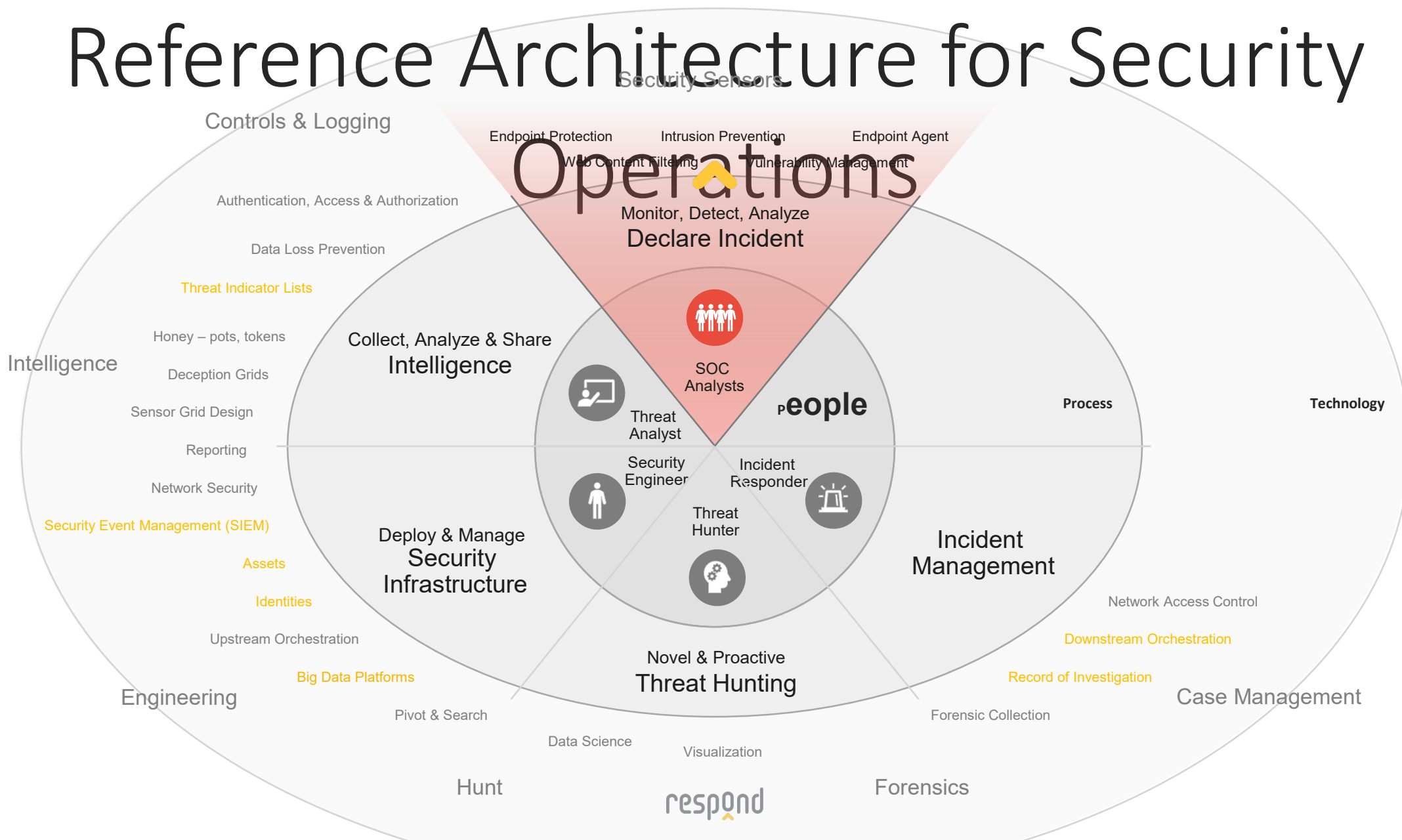
From:

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





“Monitoring for Bad”

← OLD

NEW →

“Managing Bad”



Thank You

www.respond-software.com/blog

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