Accelerate your Cloud-Driven Transformation

Antonio Forzieri
EMEA Cyber Security Specialization and Advisory

splunk> turn data into doing™


75%
P R N D
25
MAX
3
mph
25
Stopping for traffic control in 0 ft
Use accelerator or cruise stalk to continu

New companies

Greatwide Truckload
Next update: 8 Days 5 : 22 : 37

CI Selecta SIA
Next update: 8 Days 4 : 54 : 28
LOCK

ALIZON
Next update: 8 Days 4 : 11 : 21
LOCK

Haines Homes LLC
Next update: 8 Days 3 : 38 : 58

MSPharma
Next update: 7 Days 16 : 01 : 32
LOCK

Caltlar Games
Next update: 6 Days 18 : 44 : 21

Active Business & Technology
Next update: 5 Days 16 : 49 : 58
LOCK

Grupo Philips
Next update: 5 Days 16 : 06 : 37
LOCK

Cambridge Weight Plan Ltd
Next update: 5 Days 14 : 13 : 07

Avaddon team collects and analyzes information about our clients and their companies. We specialize in customer privacy data, financial information, databases, credit card information and more.
Now we would like to talk about the cost of non-collaboration and self-service data recovery.
Encrypted files are not the main problem. Companies cannot understand the risk of information leakage, especially private information.
Such leaks of information lead to losses for the company, fines and lawsuits. And don't forget that information can fall into the hands of competitors!
As we know from the reports, the cost of company recovery services can be ten times more than our amount for the ransom.
When hiring third-party negotiators or recovery companies, listen to what they tell you, try to think, are they really interested in solving your problems or are they just thinking about their profit and ambitions?
Avaddon Locker cannot be decrypted without the help of the Avaddon general decryptor!

Greatwide Truckload

Company:	Greatwide Truckload
Address:	2150 Cabot Blvd W, Langhorne, Pennsylvania, 19047, United States
Website:	www.greatwide-tm.com
Phone:	(215) 428-4800 800-283-9709 877-562-0837
Next update:	8 Days 5 : 22 : 37

Greatwide Truckload, the company does not want to cooperate with us, so we give them **240 hours** to communicate and cooperate with us. If this does not happen before the time counter expires, we will leak valuable company documents.

We have a lot of valuable data, such as: classified information, confidential agreements and more, contracts, legal data, driver's documents, customer database as well as their personal data, tax

Full dumps

Steel Art Signs Corp.
Published data: 517.74 MB

Targetcom
Published data: 947.98 MB

Basque Center for Applied Mathematics-BCAM
Published data: 134.2 MB

Mikro Trading
Published data: 2.36 MB

Schneider & Branch
Published data: 23.23 GB

Zhuhai Languan Electronic Technology Co., Ltd
Published data: 158.65 MB

AlohaABA
Published data: 1.4 GB

SISCOMAT
Published data: 463.93 MB

La compagnie du SAV
Published data: 28.24 MB

What does Digital Transformation Mean to YOU?

Img Ref –

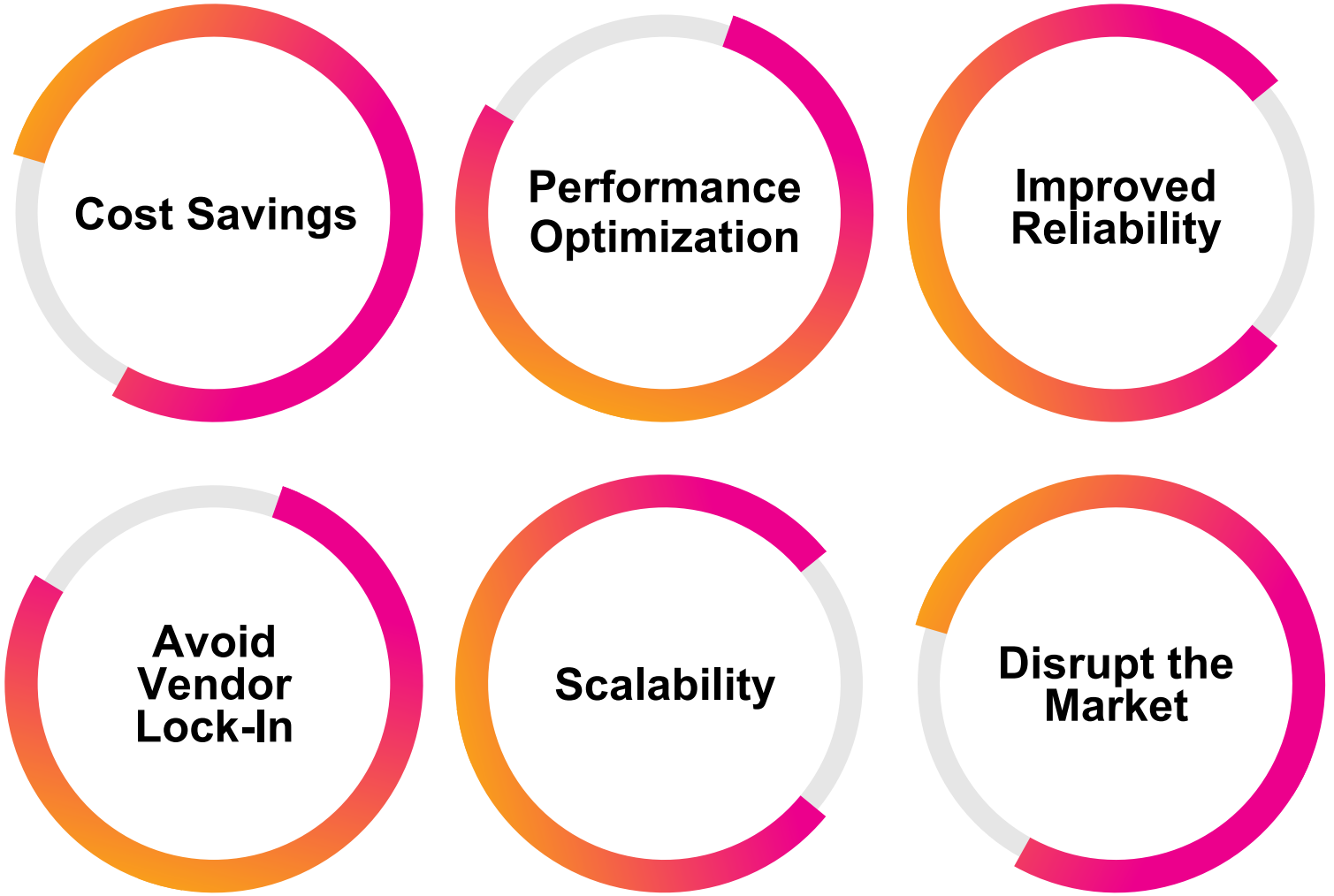
Cloud is here to stay

Enterprise Cloud Adoption Continues to Accelerate - Present & Projected

Cloud Market	Multi-Cloud Strategy	Cloud Services & Security	Cloud Teams	Cloud Spend
623.3B	93%	94%	66%	1.2M
2023	Present	Present	Present	Present 50% of Enterprises

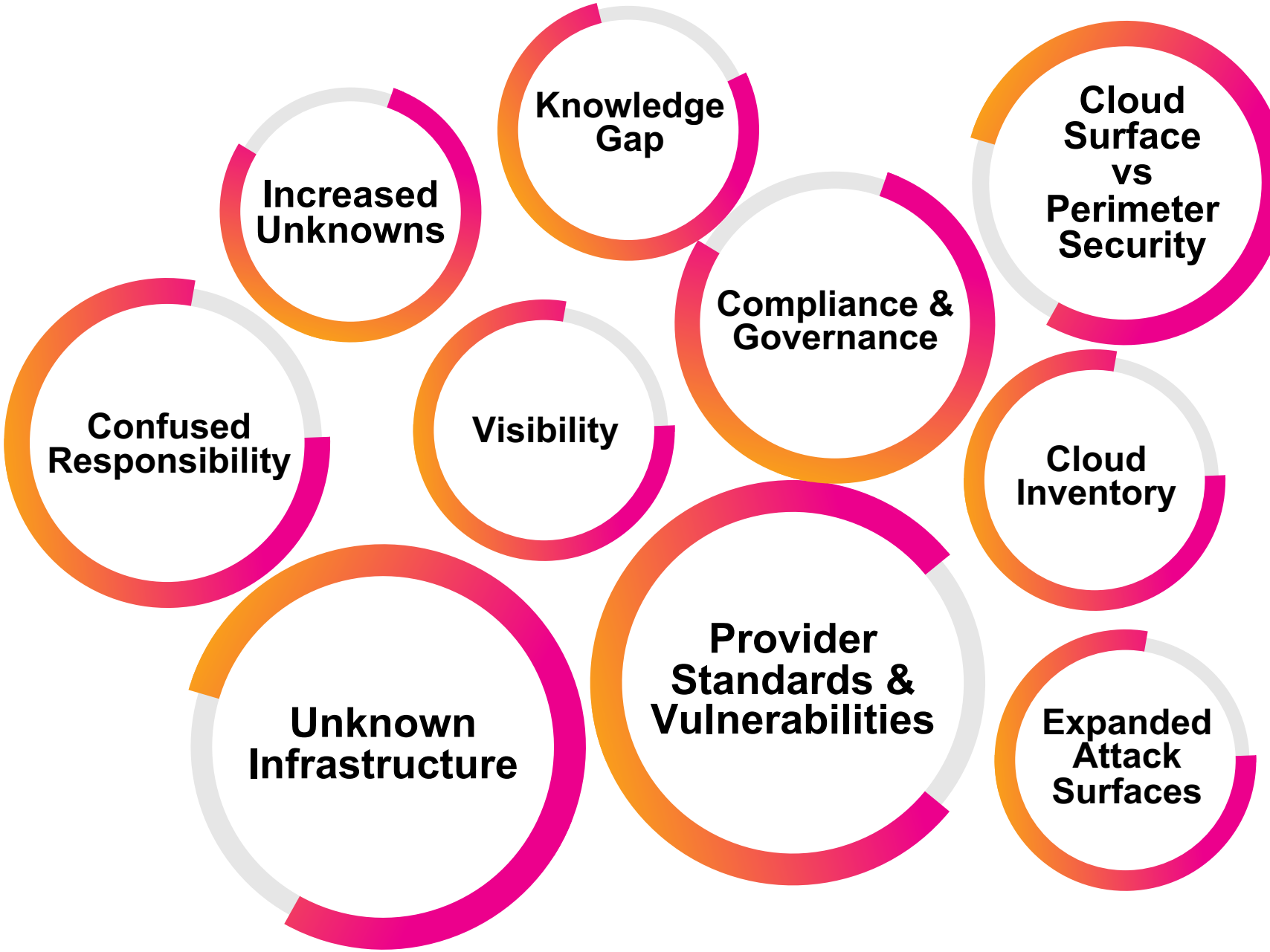
(Source: Forbes, Flexera, Blog)

Benefits of Multi-Cloud Adoption



Source: *Flexera 2020 State of the Cloud Report*

Challenges of Cloud Security & Operations



2021 Global Tech Outlook

The Drive & Priorities

84%

Actively Pursuing Digital Transformation

45%

Security is Top Priority

Top Challenges

27%

Integration Issues are Top barriers.

26%

Security is Top barriers.

The Human Touch

30%

Need to improve Collaboration

27%

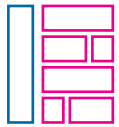
Need to Transform Culture

splunk> turn data into doing™

Reference – RedHat 2021 Global Tech Outlook Report – Interviewed from 1470 Leaders

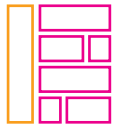
Cloud is a Critical Enabler of Transformation but Increases Complexity

Retain & Optimize
Tightly Coupled Apps, Slow Deployment Cycles



Phase 1

Lift & Shift
Primarily Cloud IaaS



Phase 2

Re-Factor
More Modular, Dependent App Components

Phase 3

Re-Architect
Loosely Coupled Microservices, Serverless Functions

Phase 4

More data centers to monitor and secure

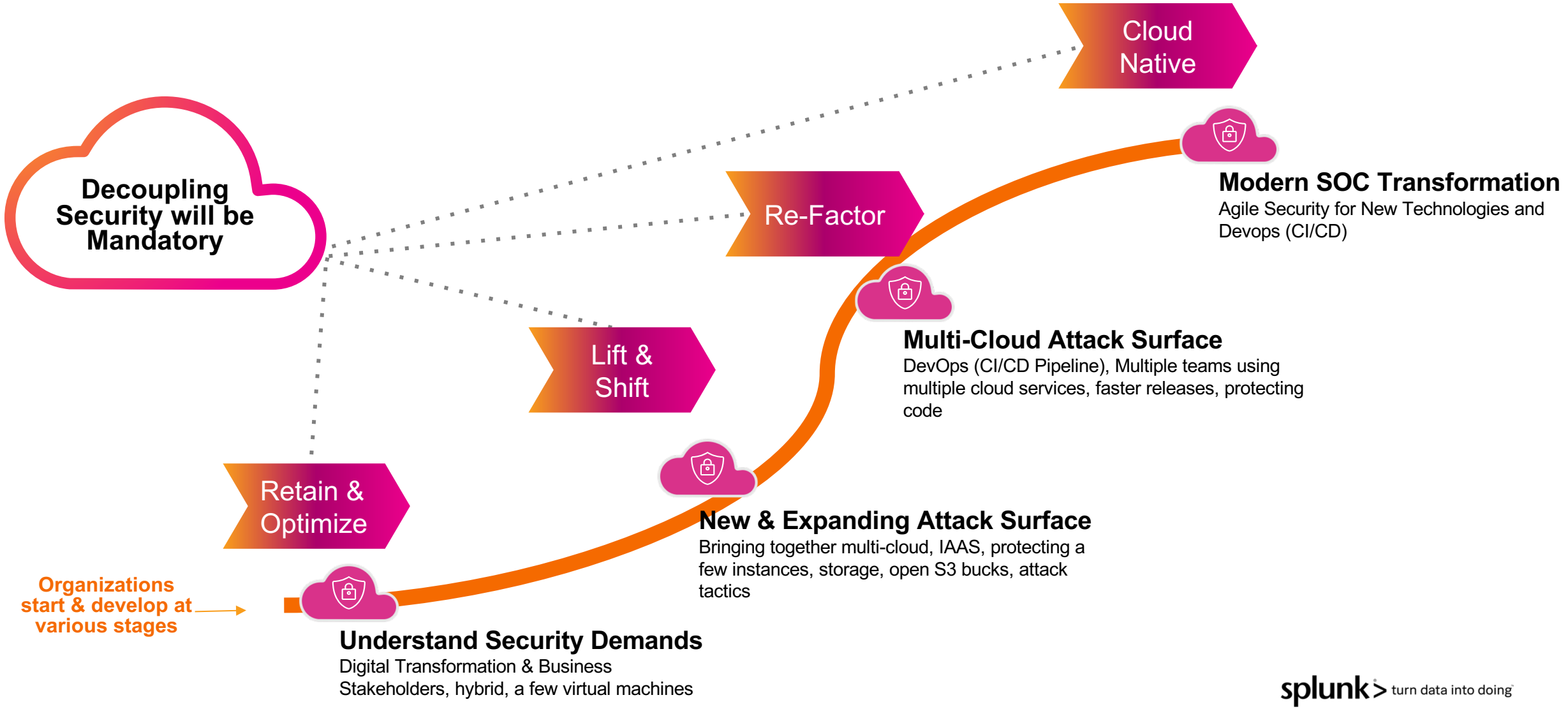
More data across an expanded attack surface

More complexity and unpredictability

More frequent releases and risk

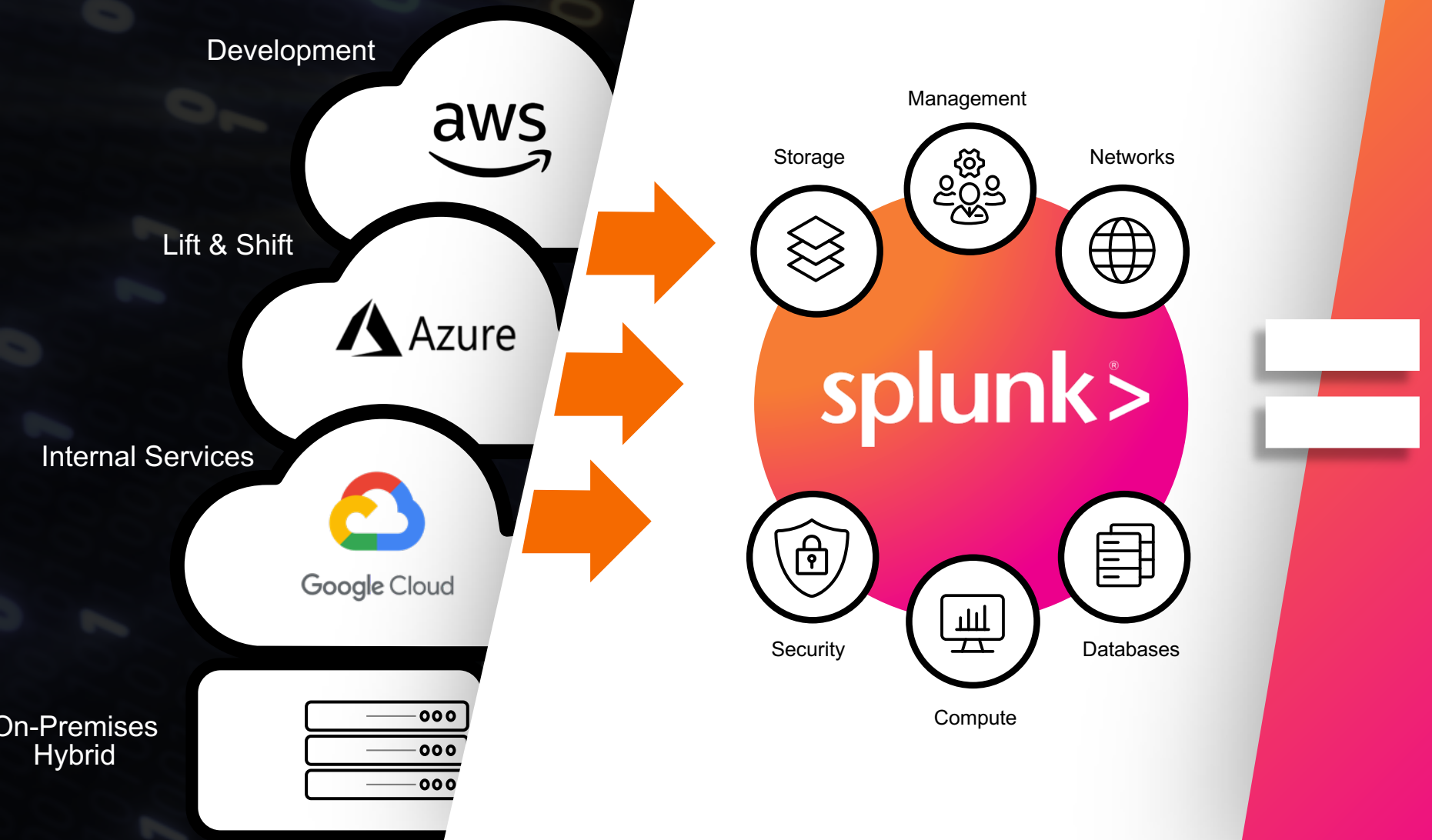
Parallelized Cloud Transformation

Cloud Security shifts at different speeds



Operationalize Security

Value of seeing events across hybrid-cloud environments



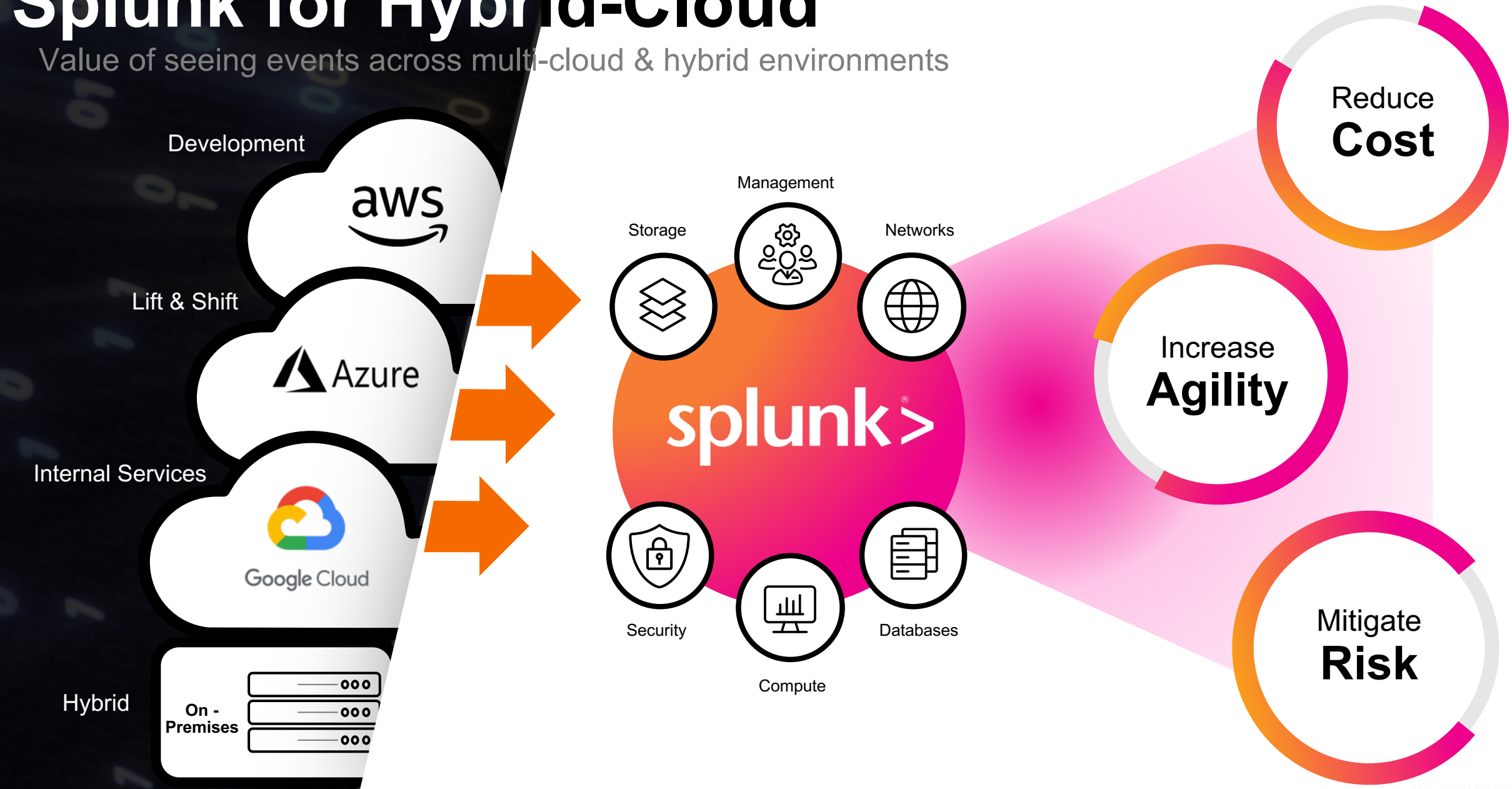
Monitor, investigate and detect vulnerabilities & misconfigurations across cloud environments

Visualize and analyze multi-cloud threat surfaces and vulnerabilities

Establish & enhance tools for cloud auditing across multiple cloud providers

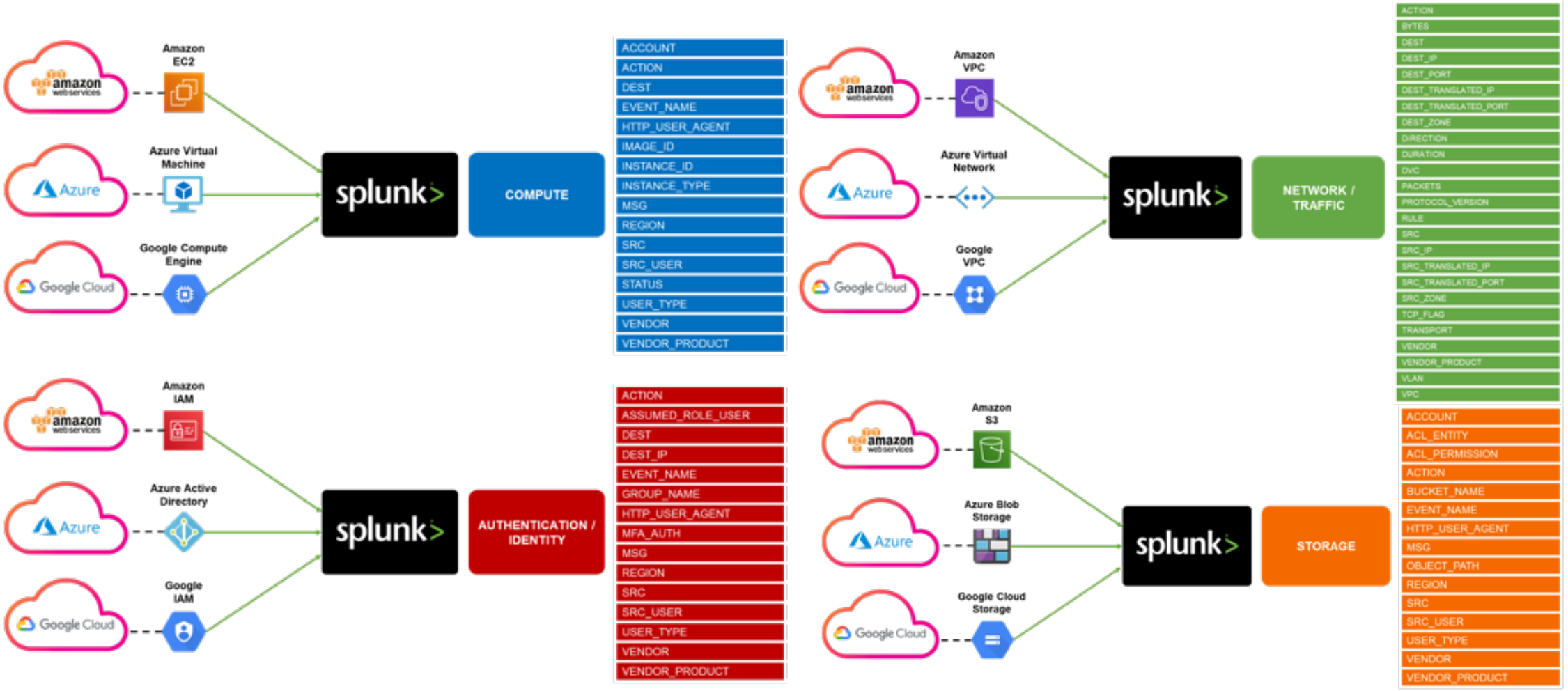
Splunk for Hybrid-Cloud

Value of seeing events across multi-cloud & hybrid environments



DeepDive for Multi-Cloud Security Monitoring

Splunk Expert-Led Session



Build and strengthen a unified cloud security posture

Operationalize data across multi-cloud environments

- Proactively monitor, investigate and detect threats and misconfigurations across cloud environments
- Bring cloud security data together for better visibility and faster response
- Comprehensive security with enhanced auditing, visualization and analytics

What we hear from customers

CONFUSION: I have no clear understanding where I should start.

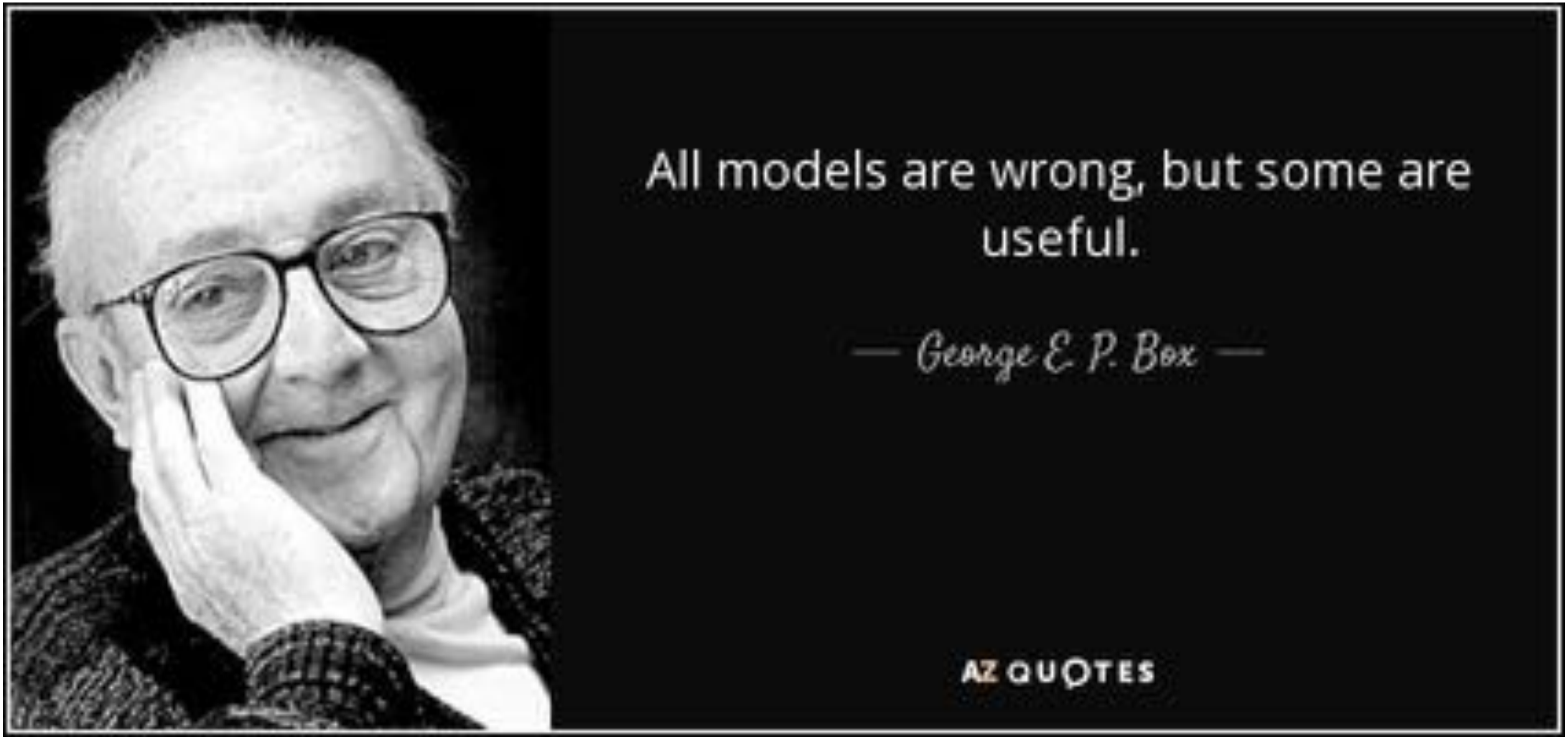
PLANNING: I'm not sure I can build a roadmap to mature my SOC.

SPEED: Deploying a SIEM is very complex and takes a lot of time.

BUDGET: I don't have enough money to monitor my infrastructure.

VALUE: I'm not sure I can easily show value to my boss.

MITRE | ATT&CK™



MITRE ATT&CK: your friendly framework!

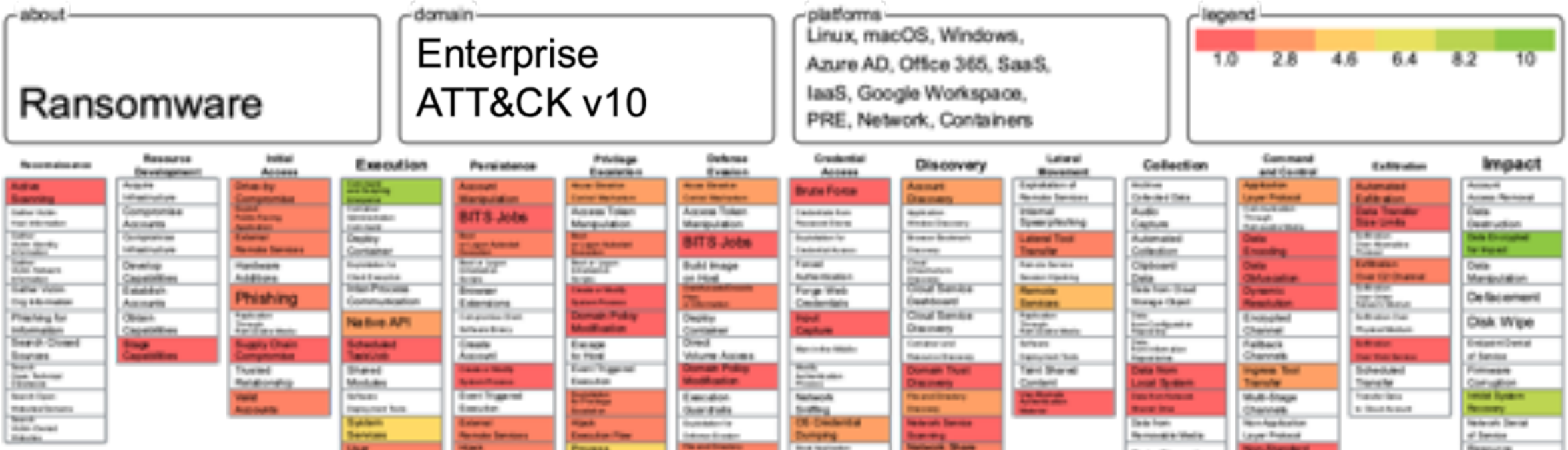
Exfiltration and Encryption are only the last stages

MITRE ATT&CK™

The de-facto gold standard Cyber Security Framework

Where should we start from?

TOP 10 Ransomware groups techniques

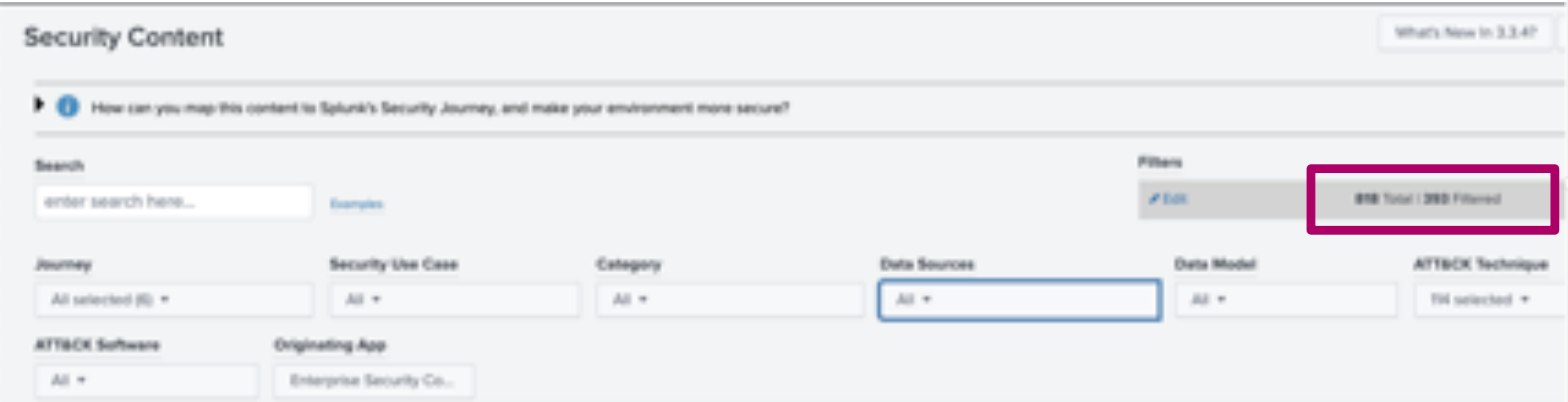


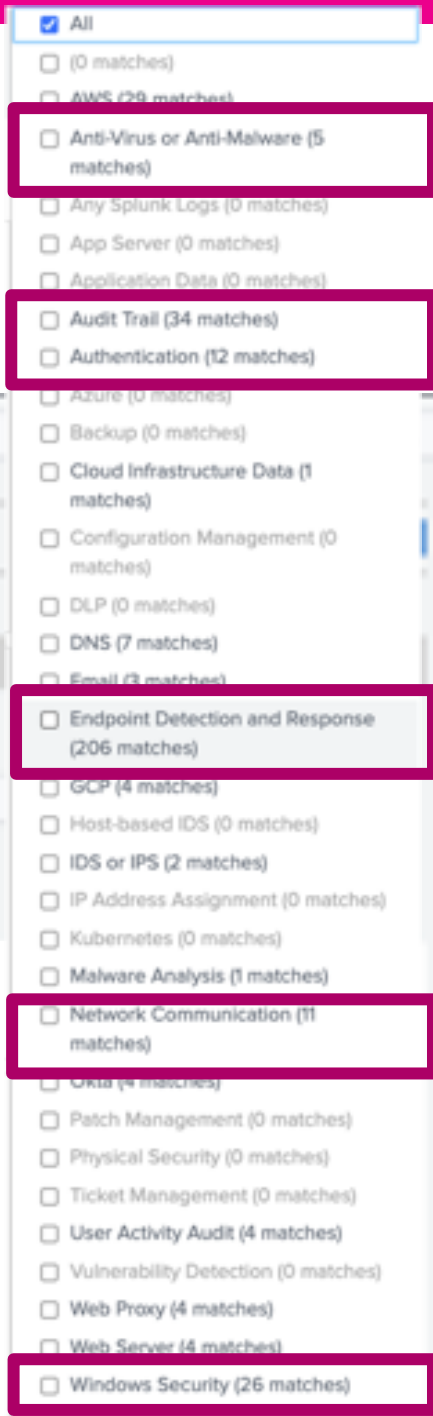
Main Ransomware Groups	
Egregor	Maze
Darkside	Avaddon
Conti	Revil
DopplePaymer	Pysa
Nefilim	Netwalker

splunk> turn data into doing

How can Splunk help me with this?

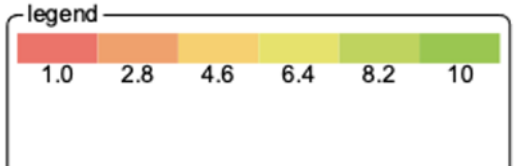
How can Splunk ES help me?



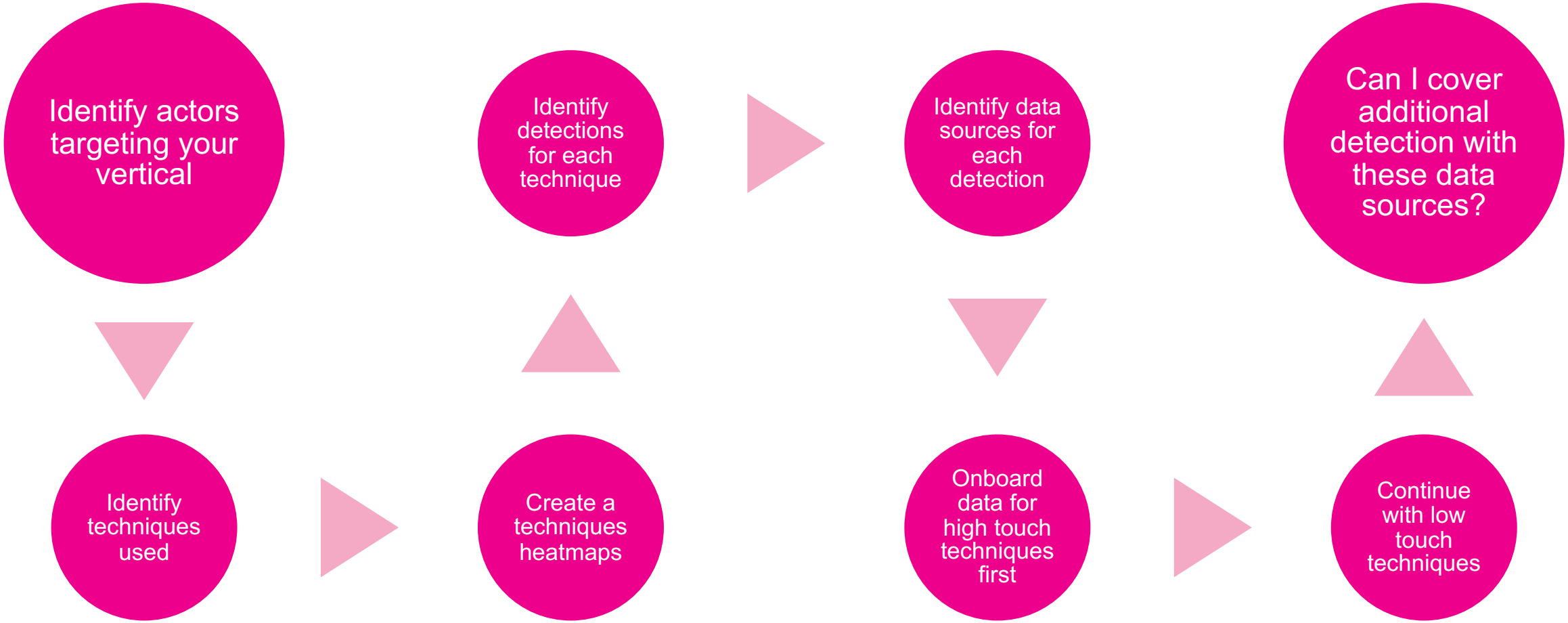


In order to enable these out-of-the-box rules these data sources are required:

- Endpoint Detection and Response (Crowdstrike/Sysmon/Osquery…)
- Windows Workstation and Server logs (Windows Event Security, Audit Trail, User Activity)
- Network devices (Firewalls and IDS)
- DNS
- EMAIL
- Cloud



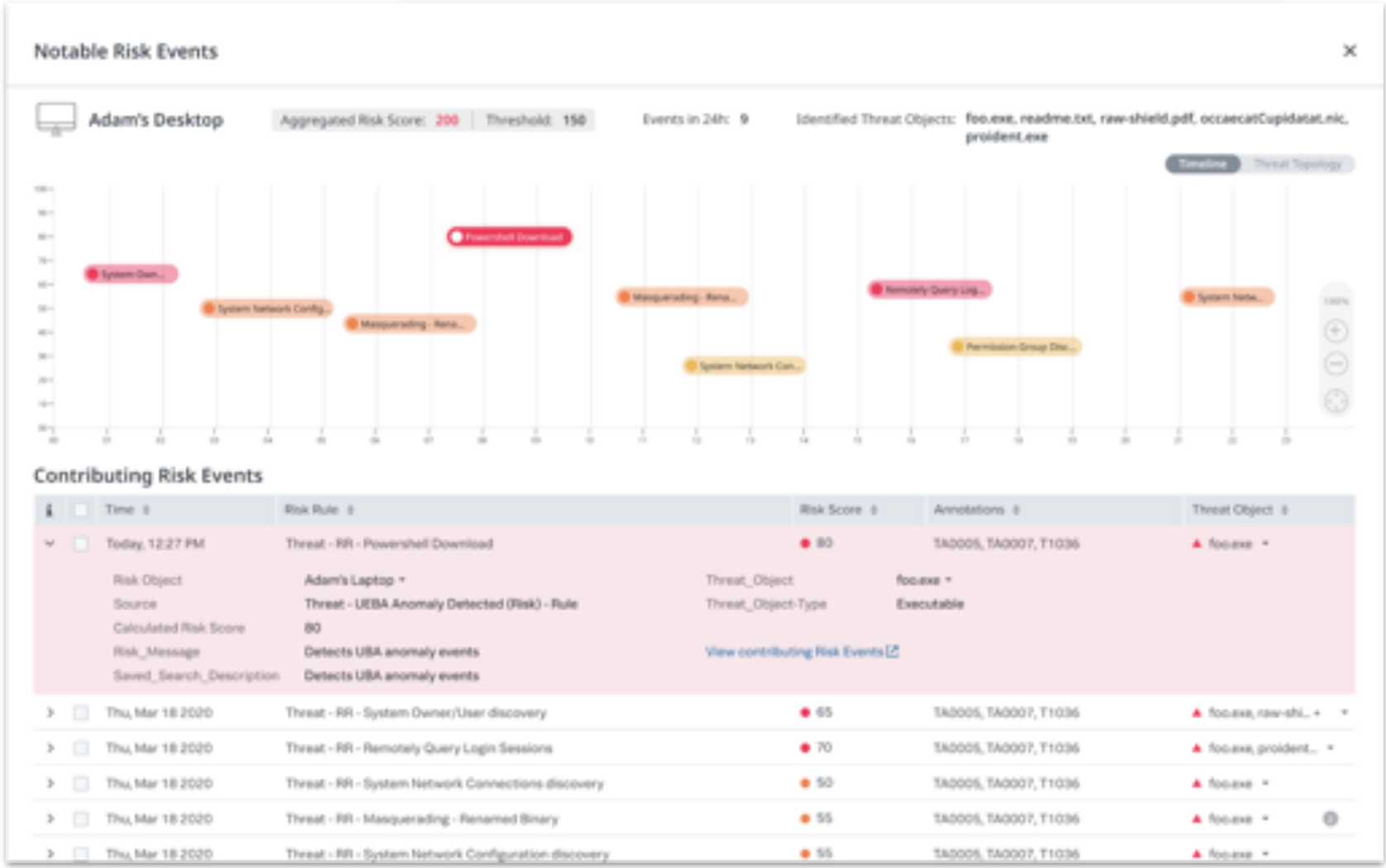
Which process can we embrace ?



Risk-Based Alerting Event Timeline

Splunk Enterprise Security 6.6

- Quickly identify timelines around contributing Risk Events
- Comprehensive view of overall threat activity combined into a single risk-based event.
- Improved visibility between risk objects, risk attributions, threat objects and the timeline of detection
- Reduce MTTD and shorten MTTR SOC metrics



splunk> turn data into doing

Thank you

splunk> turn data into doing