



# SEC 1391

## Building a Security Monitoring Strategy 2.0

Paul D'Avilar | Paul Pelletier  
Security Consultants – Professional Services

# Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.

“People ask us all the time, ‘What keeps you up at night?’ And we say, ‘Spicy Mexican food, tweets that affects our stock portfolios, and low cyber (**attacks**) preparedness.’”

Paul and Paul

.conf19

splunk>



**Paul D'Avilar**

Staff Security Consultant | Splunk



**Paul Pelletier**

Sr. Security Consultant | Splunk

# A Little About Us

We're both Splunkers for starters ☺

## ▶ Paul Pelletier

- 18 year infosec veteran with lots of Alphabet soup behind my name
- Used to own my own MSSP
- Worked everywhere from a hometown bank to an underground utility locating company to some of the largest consulting companies in the world
- Securing ICS and Critical infrastructure is one of my passions
- Favorite Quote: I hope for nothing. I fear nothing. I am free. – Nikos Kazantakis

## ▶ Paul D'Avilar

- 15 year infosec veteran with a primary focus on PubSec
- Risk-centric and solution oriented – learning to work starter, not harder
- Reformed Google fanboy
- Deloitte Alum
- World traveler, tinker, home automation, IoT
- Favorite Quote: The best way to predict the future is to create it – Nephew's HS Graduation Wristband (credited: Abraham Lincoln and Peter Drucker)

# Agenda

If all goes well, we will cover

- ▶ Why is Continuous Security Monitoring (CSM) important
  - I think we talked about this last year, but in case you missed it, here's a quick recap
- ▶ What have we learned
- ▶ Patterns and Principles for an effective CSM program
  - Core components
  - Core Data sources and why
  - Essential use cases
    - Machine Learning and Artificial Intelligence vs. heuristic or static based
    - Measuring your maturity
    - How to progress up the maturity curve and stop your adversaries sooner
- ▶ Key Takeaways

# Quick Recap

---

The Wayback Machine

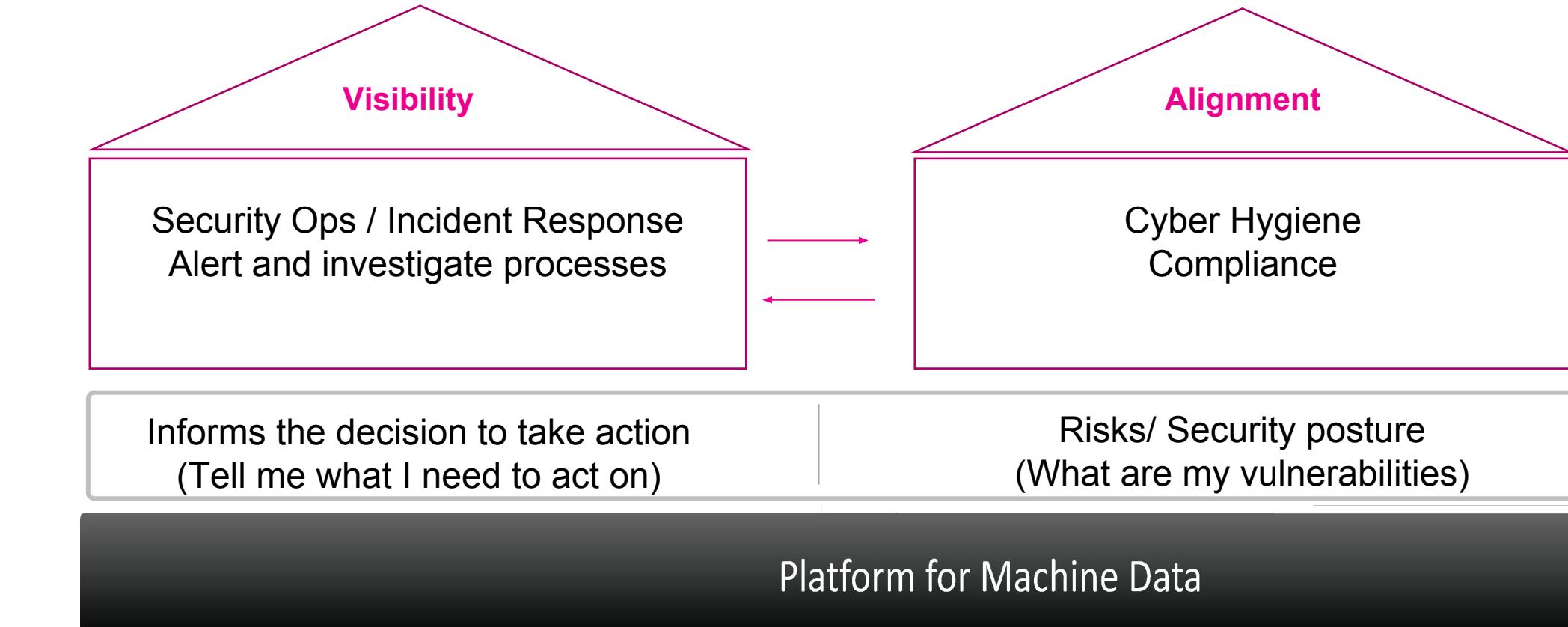


# What's The Point Of Security Monitoring (Again)

Supports the creation and sustainability of value



Identify & protect assets (crown jewels)



A platform based approach is needed to achieve the objectives for security monitoring

# How To Make It Tangible (With A Framework)

Layout a roadmap for operationalizing capabilities to achieve objectives based on existing constraints



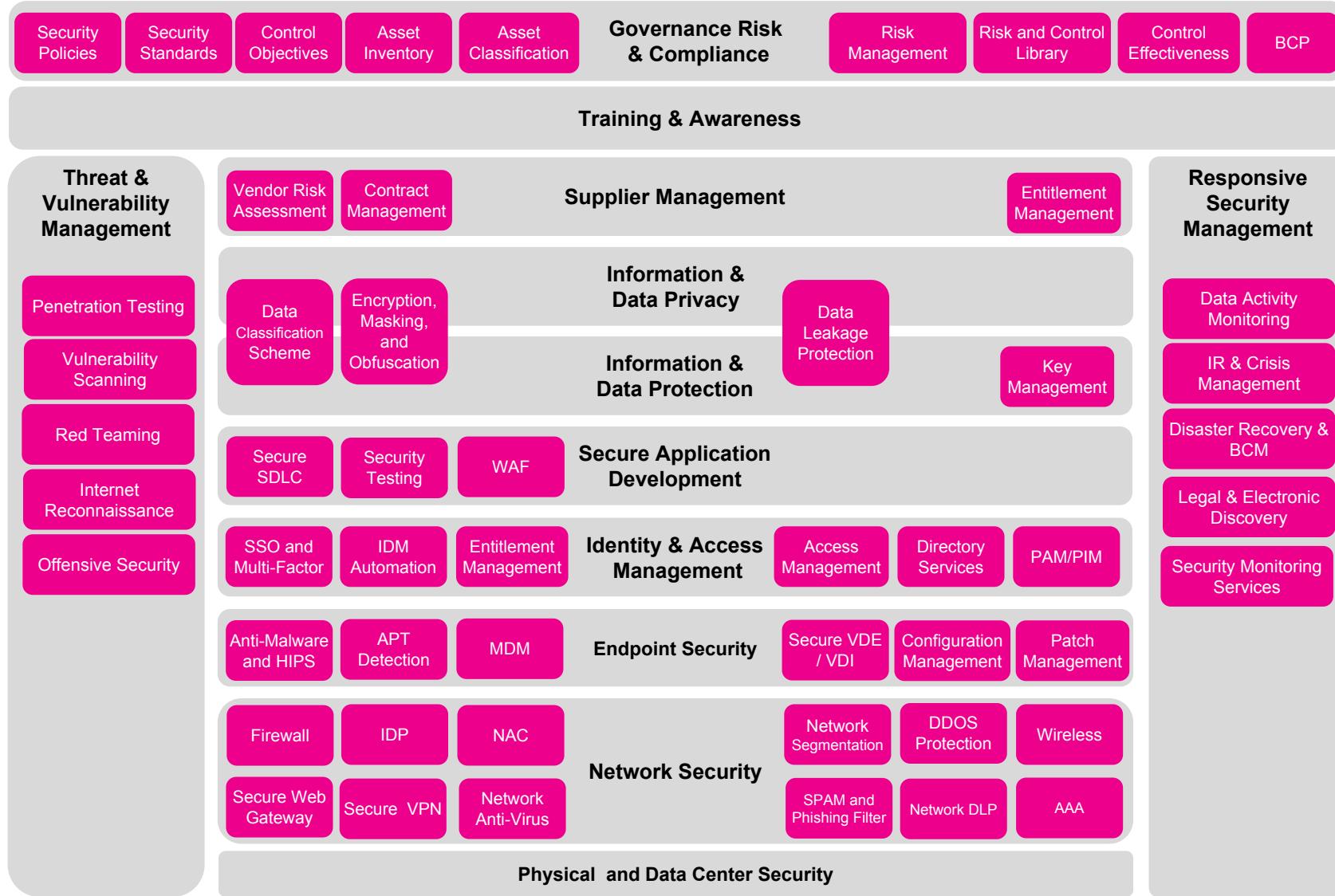
- What matters most
- What is achievable in a defined timeframe
- What support is needed

- Operational Requirements
- Resiliency
- Laws and Regulations
- Budget

- Technologies
- Processes/  
Procedures
- People and skillsets

# Considering Data Sources And Silos

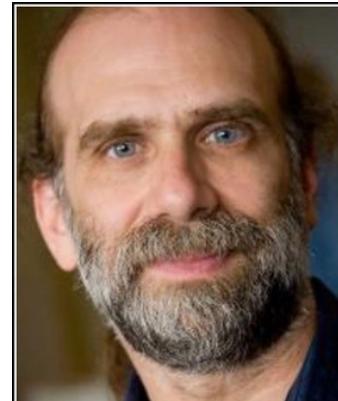
So much noise, focus is essential



# So You've Decided To Implement A CSM

What's the next steps?

- ▶ Hopefully you've picked a framework around which you can drive consistency and measure your growth/maturity
  - Like NIST SP 800-137
  - Risk Management Framework
- ▶ Know Thyself
  - Cyber Security Bible v 1:1
  - Know your people, know your critical assets and crown jewels, data categorization is key!!!
  - What are your drivers? Business needs  Compliance  Regulatory
  - Turn data into actions
- ▶ Drive successful business outcomes
- ▶ Have a tested Incident Response plan in place (make this recurring...)



If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

— Bruce Schneier —

# Wait!, Wait! Midcourse Adjustments

---

Lessons learned after a year of engaging with customers and practitioners on the topic



# Pitfalls And False Starts

Observations from the field on the adoption of key tenets from our presentation and our responses



Paralysis in getting started – stagnation

## Executive Sponsorship

Involvement of key stakeholders that will champion the cause

## Data Onboarding Strategy

Guides users through the getting data into the platform and making it useful process:  
CIM | Validation | Use Cases

## Alerting and Detection Strategy

Event management and incident response framework



Light on substance, strategy and adoption

## Scalability

Plan for the security monitoring infrastructure to support the demands, being agile/ nimble, shorten time-to-value

## Adoption of Technology Trends

Alignment and adoption to technology trends to enable the collection, use, and incorporation of new approach such as containerization, micro-services, hyper-convergence, etc.



Lack of proper resourcing – empowerment of users

## User Enablement

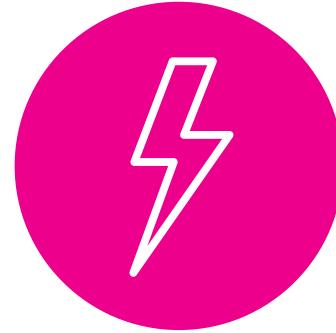
Enable users through formal and informal training, they will provide your biggest return on invested \$\$\$

## Interconnected Security Stack

Integrate your team, processes, and tools together including automation and orchestration where it make sense to decrease the time to make a decision and act

## Analysts Focused

Empower a collaborative SOC...



Under utilization of OOTB capabilities

## Smart Store

Scale up/down memory and data storage independently to save money and maintain search performance.

## Workload Management

Prioritize allocation of compute and memory resources.

## AI & ML-powered Analytics

Augment human skills ...

# Our 2Cents And More

A collection of our recommendations for moving security monitoring forward and up the maturity curve

Function	Recommended Actions	OOTB
Data Onboarding	<ul style="list-style-type: none"> <li>• Make the progress visible (business leaders, ISSOs   Risk Officers) – build apps</li> <li>• Build Quick start guide (TLDR version)</li> <li>• Develop approve architectures/models based on alignment to vetted principles and patterns</li> </ul>	<ul style="list-style-type: none"> <li>Guided Data Onboarding (14+)   Center of Excellence   Security Essentials</li> <li>Center of Excellence</li> <li>Splunk Validated Architectures good examples</li> </ul>
Alert and Detection Strategy	<ul style="list-style-type: none"> <li>• Develop a strategy/plan for deciding importance, increasing fidelity, etc...</li> </ul>	<ul style="list-style-type: none"> <li>Splunk ES Frameworks (e.g. Risk, Threat)   SecKit   Security Essentials   ESCU</li> </ul>
Incident Management Workflow	<ul style="list-style-type: none"> <li>Understand your incident management workflow, it is never too early to build workbooks/runbooks (technology agnostic)</li> </ul>	<ul style="list-style-type: none"> <li>Mission Control   Splunk Phantom</li> </ul>
Technology Strategy for Security	<ul style="list-style-type: none"> <li>Align security infrastructure with organizational strategies and ownership, leverage hybrid models (no snowflakes)</li> </ul>	<ul style="list-style-type: none"> <li>Splunk Cloud   Data Stream Processor   SmartStore</li> </ul>
Productive management	<ul style="list-style-type: none"> <li>Stay on top of your deployment and growth, productively engagement with your customers, build admin app</li> </ul>	<ul style="list-style-type: none"> <li>Monitoring Console</li> </ul>

# So What Is Security Monitoring Again?

---

So lets do something already, strive to gain visibility as well as resiliency





# Pick A Security Monitoring Framework

Lots of different approaches

## ▶ Cyber

- NIST Cyber Security Framework (CSF)
  - One of the most widely adopted methodologies around (it's not just for the US Government, it's good for everyone)
- Australian Cyber Security HHS
- CIS Top 20 Critical Controls
- ISO 27001/2
- ISA62443

## ▶ Compliance

- PCI-DSS
- HIPAA
- GLBA
- SOX





# Define Your Data Collection Strategy

Define your approach for collecting event data across the enterprise

## UF everywhere possible

- ▶ Splunk your all endpoints!!!  
(YES – those laptops and mobile devices)
- ▶ Windows baseline
  - System and Security
- ▶ \*nix baseline
  - /var/log
  - /var/log/audit.log
- ▶ Insightful
  - PowerShell/CLI
  - Sysmon

## Log aggregation when needed

- ▶ Syslog
- ▶ Streaming/ Realtime data sources – Kafka
- ▶ ...

## Third Parties

- ▶ Partners and collaborators
- ▶ Technology providers/ vendors providing services
- ▶ ....

## Containers

- ▶ Docker
- ▶ Kubernetes
- ▶ ....

## Cloud Environments

- ▶ PaaS
  - AWS
  - Azure
  - Google
  - ...
- ▶ SaaS
  - O365
  - SFDC
  - Akamai
  - Security tools
  - ...
- ▶ Private and hybrid environments



# Onboard Necessary Data Sources

This is what we recommend to get started

## ES Req'd Data Sources

- Network/Host IDS
- DNS
- Antivirus
- Email
- Web Proxy
- Firewall
- Vulnerability Scanning
- Active Directory
- VPN
- \*\*\*Assets and Identities is  
KEY\*\*\*

## Ideal

- Sysmon
- CLI and Powershell logging
- UF's on all Endpoints
- Full NGE data
- Full enrichment in ES

# Adopt an Alerting and Detection Strategy



Define your approach for detection and response to known/unknown threats

Risk based approach

Sufficient coverage & visibility of the tactics and techniques

Ability to disrupt and contain the risk (threat/adversary) sooner

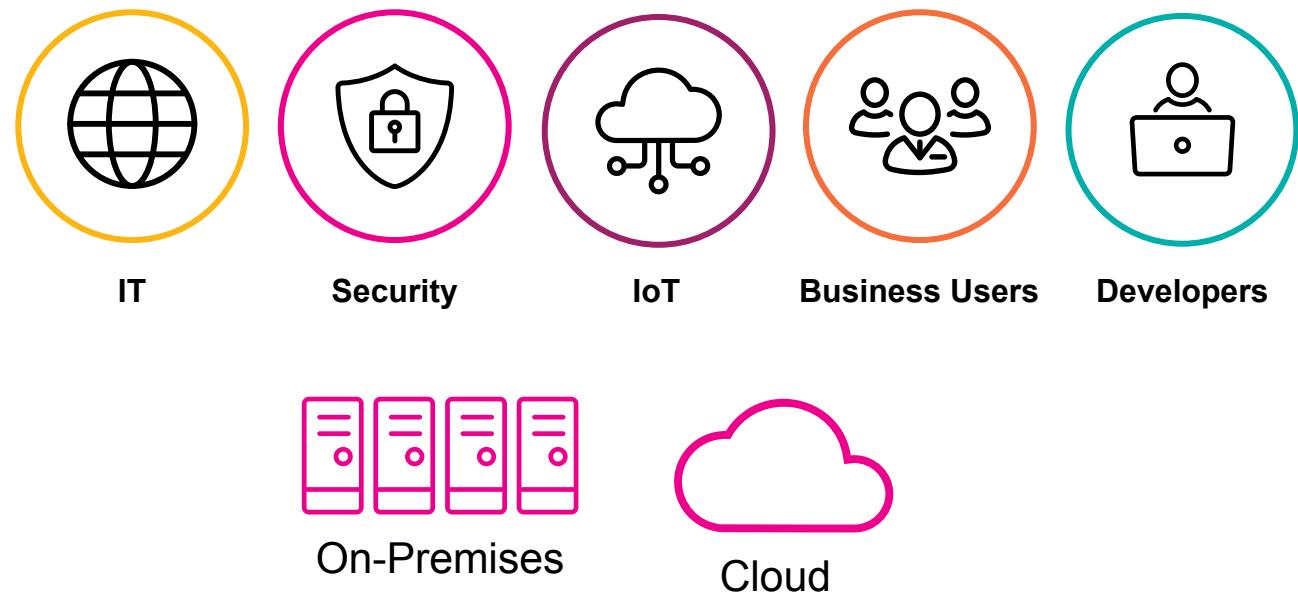
**Be transparent** – create awareness through reports and metrics | **Visibility**



# Various Alerting and Detection Strategies

Strengthen defenses by integrating existing security infrastructure together so that each part is an active participant

- Diamond Model for Intrusion Analysis
- Mitre Att&ck
- CIS
- Palantir

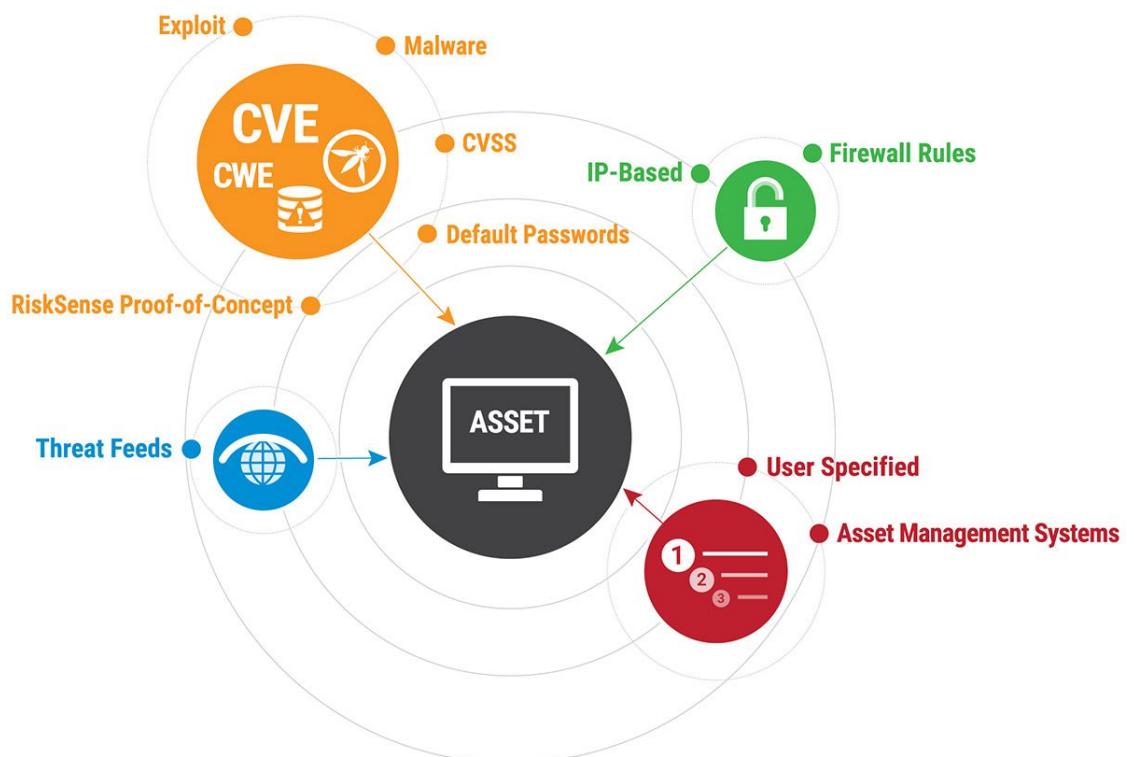




# Considerations For Risk Based Alerting

A new'ish concept with a twist

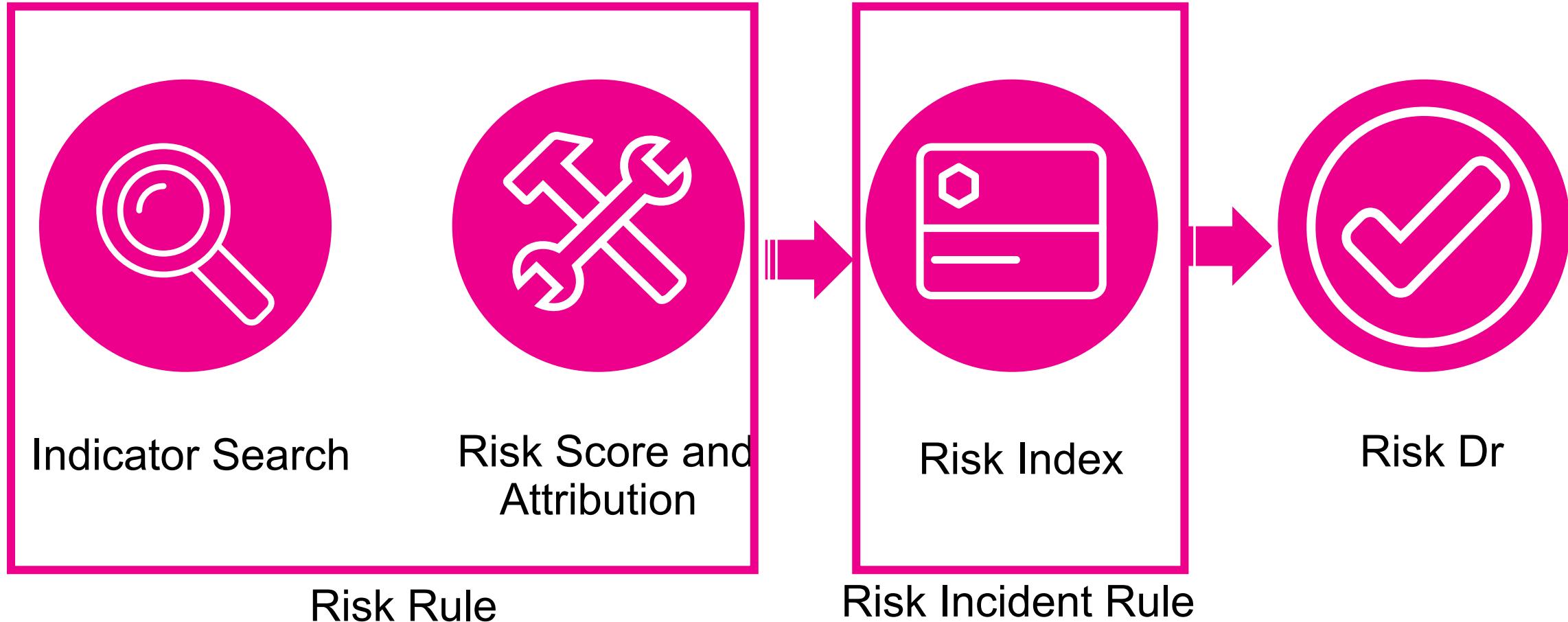
- ▶ Alert fatigue anyone....
- ▶ Threat Intel
  - Create attributions for matches
  - Dynamic score based on feed, asset/identity, or other context
- ▶ IDS/AV
  - Map the IDS vendor categories into ATT&CK / Kill chain phases
  - Dynamic score based on category, asset/identity, or other context
- ▶ Behavioral Anomaly attributions (SSE and ESCU)
- ▶ Outlier attributions – leveraging ML
- ▶ 3rd party Integrations to include their risk attributions, like WHOIS





# A Risk Driven Approach To Alerting

Mindset Shift: Cast a Wide Net



Not every alert (detection) should be a notable



# Aim To Disrupt And Contain

Ensure you can respond faster and reduce dwell times

- ▶ CIS Top 20 (really, accomplishing the top 4 is a big deal)
- ▶ ASD Essential 8
- ▶ Lockheed Martin Kill Chain
- ▶ ...

INTERCONNECTED SECURITY STACK

AUTOMATION AND ORCHESTRATION

MACHINE LEARNING TO AUGMENT HUMAN SKILLS

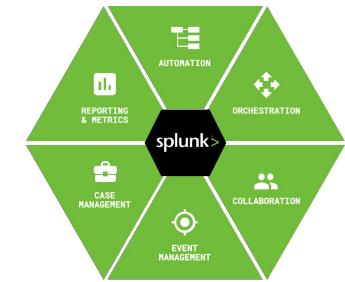


Splunk Enterprise Security™



ADAPTIVE RESPONSE

splunk®  
phantom



Splunk User Behavior Analytics™

# Use Cases Oh My...

---

Different detection methods? What about selection criteria?



# Machine Learning / Artificial Intelligence

## Use Case Methods

### Baselining / historical

- Collects data, creates model, evaluate against the model
- Creates a baseline of what is "normal" and then measures any changes against that model

Utilizes very sophisticated algorithms, but is not easily customized with custom use cases/queries

### Lateral Movement

- Splunk uses 45+ Anomaly classifications based off existing logs that UBA puts into various threat models
- Via unsupervised ML these use cases are created based off the available data
- Detects anomalous changes that are indicative of lateral movement

### Data Exfiltration

- Again utilizing unsupervised ML we can detect changes in endpoint behavior and definitively output the results to the user as anomalies that indicate data exfil
- Anomalies are not necessarily false positives, they are changes in the behavior that have not been seen before

# Heuristic And Static

## Use Case Methods

### Human based

- ▶ Require extensive tuning
- ▶ Can generate more false positives
- ▶ Allows for highly/easily customized rules
- ▶ Logic is entirely up to you

These types of queries are generally not “intelligent” like ML or AI, the logic is entirely up to us. It’s not generated on the fly.

### Mimikatz

- This is a point detection that looks for specific terms, powershell executions and event IDs
- Still very effective
- Generates few false positives

Point detections like this are great at finding very specific events

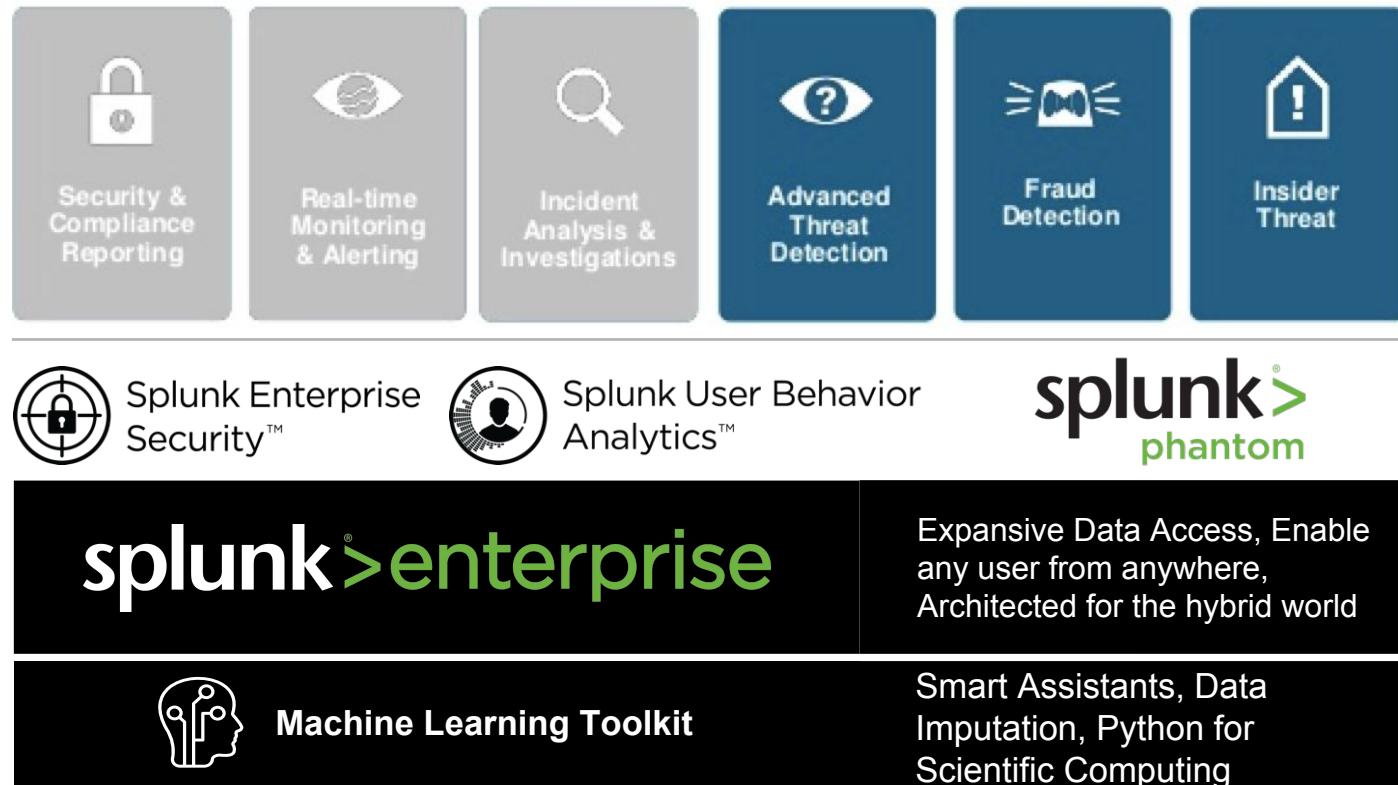
### Brute Force

- A little harder to solve because we want to successive failures followed by a singular success
- Requires extensive tuning
- Requires effective logic to tune down the noise and give actual brute force detections.

# Shhhh, Keep Down The Noise

Selection is key

- ▶ Be strategic
  - Don't pick a use case just to have a use case
- ▶ Pick only use cases that are high value and high fidelity
- ▶ If you can't action the use case you probably don't need it
  - What does the alert tell the analyst
- ▶ Event sequencing is awesome, use it!



# Validation, Validation, Validation

---

How do you know your security monitoring program really works?

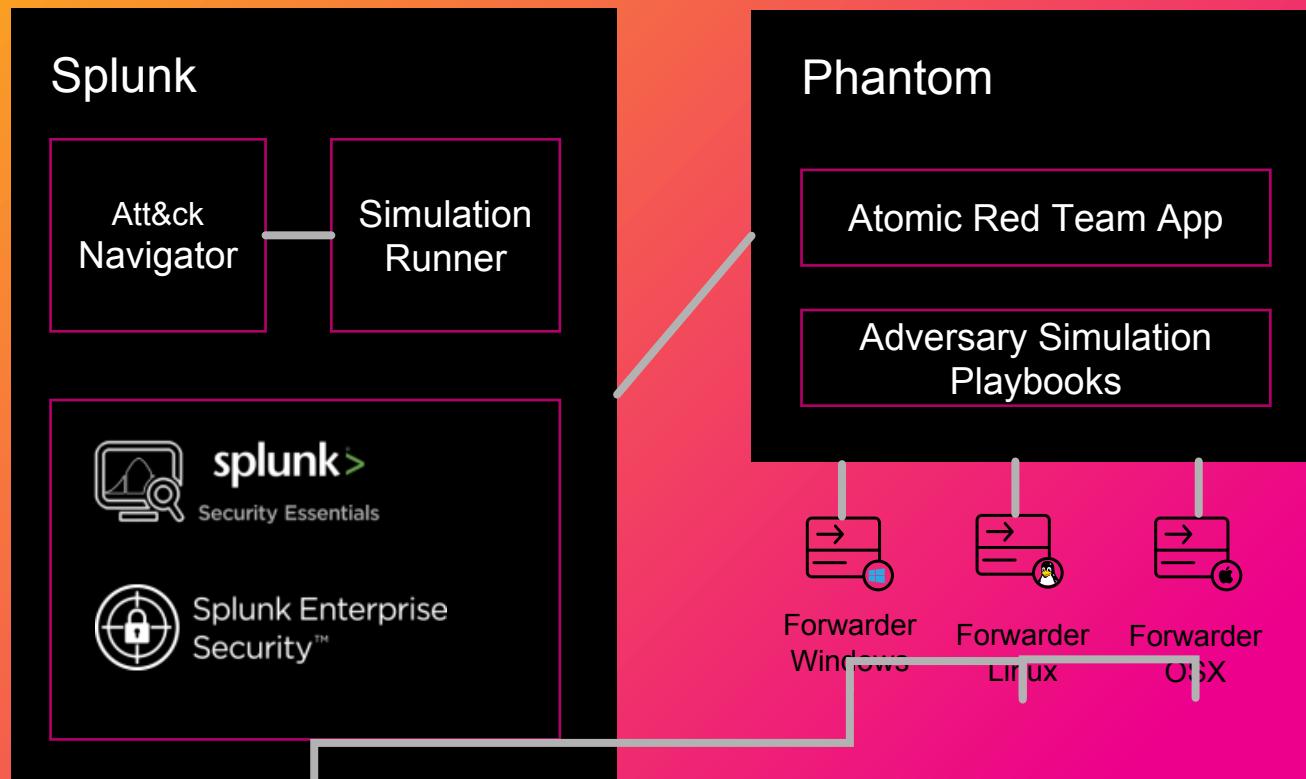


# I Made A Rule So I'm Good, Right?

- ▶ Confirm that your rules and correlation searches actually do what they're supposed to do
- ▶ Regression testing: does what you did 6 months ago still work?
- ▶ You don't wanna miss a thing....don't miss widely known vulns
- ▶ Identify your blind spots
- ▶ Oh yeah Splunk detects that...Show me the money!



# A Framework For Security Content Validation



Red Canary + Phantom = One Approach

# Purple Teaming The Splunky Way

Phantom as the testing engine

- ▶ We have lots of controls that can frustrate our adversaries
- ▶ Somehow they still achieve success
- ▶ Adversary simulation can help

# Maturity, Our Favorite Thing!!!

---

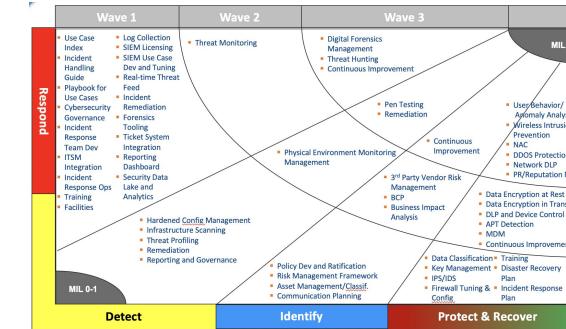
Am I like a 5 year old or a teenager or a seasoned vet



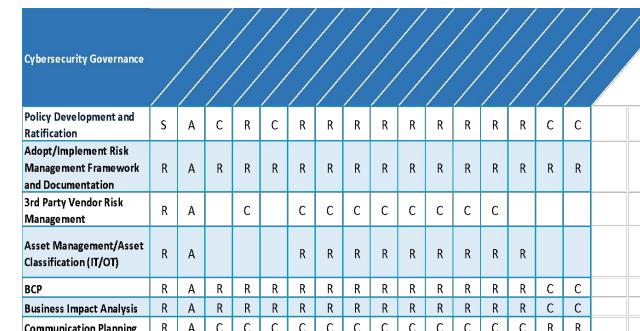
# Move Up The Maturity Scales

This is the time to be critical of one's SOC, self assess with some cadence

- ▶ Identify your current position
  - Know Thyself!!!
  - Define responsibilities (RACI is your friend)
- ▶ Define your strategic path
  - Align business goals with strategic security plan
- ▶ Identify skill/tooling gaps
  - Where do you need more coverage, prioritize
- ▶ Create a plan for a path forward
  - Create budgetary plans
- ▶ Define timelines

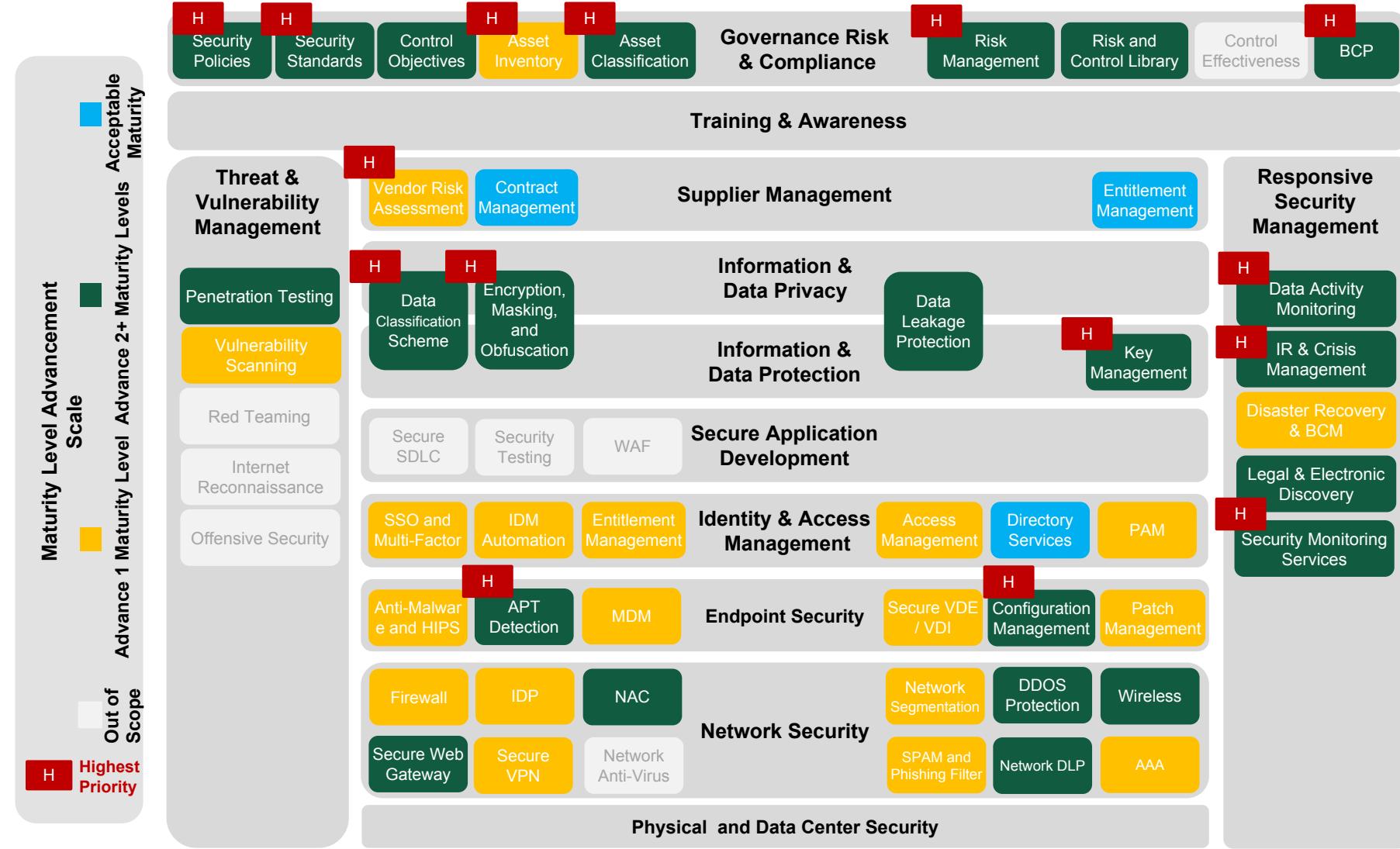


CSIRT Operations	Priority	NIST Mapping	Implementation Timeline						
			1	2	3	1	2	3	1
Use Case index based on Florida AST risk	H	ID.RA, ID.RM, DE.CM, DE.AE				\$60			
Incident Handling Procedure Guide	H	RS.RP, RS.DO				\$100			
Playbook development for identified use cases	H	RS.AN, RS.ML, DE.AE				\$50	\$75	\$75	
Cybersecurity Command and Governance	H	RS.IM				\$60			
Cybersecurity Incident Response Team Design and Build	H	PR.P, DE.AE, DE.DP, RS.RP, RS.OI, RS.ML, DE.CM, DE.AE				\$120			
ITSM Integration	H	DE.AE, B.CM, B.OV, DE.CM				\$40			
Incident Response Operations	H	DE.AE				\$100			10 3 3
Threat Monitoring	H	DE.AE				\$75	\$75	1	
Digital Forensics Management	M	RS.AN				\$75			2
Threat Hunting	M	DE.AE				\$75			2
Training	H	PR.PT				\$80	\$80	\$80	
CSIRT Facilities Build	M	RS.IM				\$250	\$75	\$75	
Continuous Improvement	H	PR.PP							



# Prioritization Of Objectives – One Approach

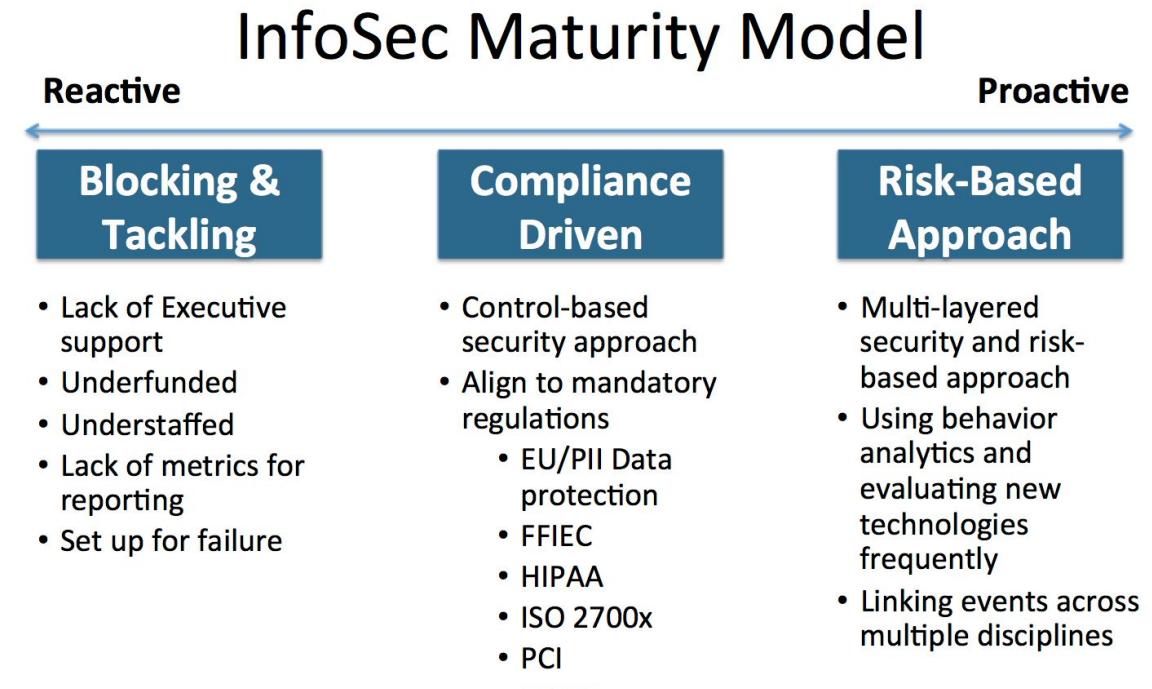
Lots of noise out here, focus on what matters most for your organization



# Increased Maturity = Increased Protection

Don't go at it alone, look to industry for objective measuring sticks

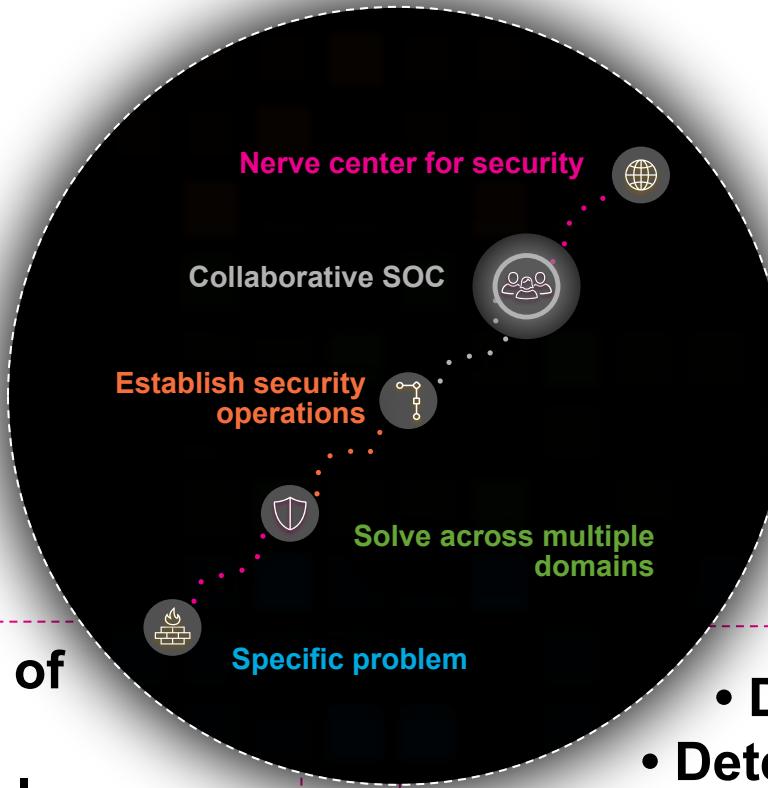
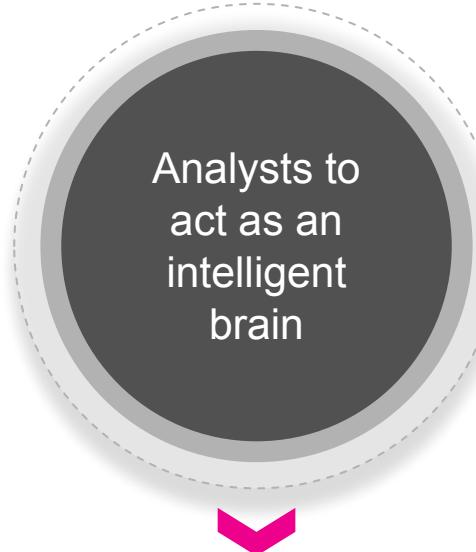
- ▶ Progress up the Kill Chain for more advanced response and detections
  - Requires additional data sources you may not have
- ▶ Use Mitre Att&ck as a guide for expansion of coverage and capabilities
- ▶ Diamond Model to increase Maturity
- ▶ Conduct internal assessments using the Capability Model Maturity Integration (CMMI) or Capability to Maturity Model (C2M2)
- ▶ Utilize industry standards
- ▶ Be prepared, conduct tabletops, etc.



*Source: Blue Lava*

# Measure Your SOC Maturity (Continuously)

Using a data analytics driven SOC to enhance resiliency



- Gathering data from all areas of an organization
- Automatically sifting through logs
- Prioritizing the risks
- Alerting on & preventing attacks before they can be executed or cause costly damage

- Discovery & prioritization of events
- Determination of risk level
- Identification of assets affected and execution of the appropriate response
- Detailed visibility at the local and network levels



# Demonstrate Value

Quantify your CSM program, putting data in the context of business (your customer)

## Utilize best practices

- For creating correlation searches, to architecture
- Know your customer

## Focus on fidelity (quality)

- Less noise, less searches and more efficiency, more relevant alerts, better data enrichment and correlations, faster time to action

## Communicate risks

- Know your assets (HVA)
- Understand your vulnerabilities
- Assess your threats

Risk: Assets | Threats | Vulnerabilities

“Value is in the eyes of the customer. The customer doesn’t always readily look in the right direction, so it’s our job to help them see the entire picture.”

Mark Hunter



## Executive reports (metrics)

- We need their support
- They need data to help support us
- Enable decision making

Dashboards and rich visualizations

# Key Takeaways

TLDR

1. Enable your people – biggest bang for \$
2. Be transparent – quantify security and leverage metrics for your benefit (security == risks)
3. Purple teaming – forewarn is forearm, practice makes perfect....
4. Participate in community – share lessons learned
5. Avoid complacency – Continuously seek opportunities for improvement and refinement
6. Focus on business outcomes

# Sources

Links, Conf talks, and shout-outs

▶ Our .conf2018 Talk:

- [https://static.rainfocus.com/splunk/splunkconf18/sess/1523538581536001Pq3N/finalPDF/SEC1672\\_BuildingASecurityMonitoring\\_Final%20%281%29\\_15385960547480012LOM.pdf](https://static.rainfocus.com/splunk/splunkconf18/sess/1523538581536001Pq3N/finalPDF/SEC1672_BuildingASecurityMonitoring_Final%20%281%29_15385960547480012LOM.pdf)

▶ Qmulos

- <https://www.qmulos.com/>
- <https://github.com/palantir/alerting-detection-strategy-framework>
- <https://medium.com/palantir/alerting-and-detection-strategy-framework-52dc33722df2>

▶ Jim Apger and Stuart McIntosh – Say Goodbye to Your Big Alert Pipeline...

- [https://static.rainfocus.com/splunk/splunkconf18/sess/1523456018499001lxCD/finalPDF/SEC1479\\_SayGoodbyeToYourBig\\_Final\\_1538509127390001SxPF.pdf](https://static.rainfocus.com/splunk/splunkconf18/sess/1523456018499001lxCD/finalPDF/SEC1479_SayGoodbyeToYourBig_Final_1538509127390001SxPF.pdf)

▶ Tim Frazier, Dave Herrald and Kyle Champlin – Simulating the Adversary

- [https://static.rainfocus.com/splunk/splunkconf18/sess/1522696002986001hj1a/finalPDF/Simulating-the-Adversary-Test-1244\\_1538791048709001YJnK.pdf](https://static.rainfocus.com/splunk/splunkconf18/sess/1522696002986001hj1a/finalPDF/Simulating-the-Adversary-Test-1244_1538791048709001YJnK.pdf)

# Q&A

---

.conf19  
splunk>



# Making machine data accessible, usable and valuable to everyone.

.conf19<sup>®</sup>

splunk<sup>®</sup>>

Thank  
You!