Building a Security Monitoring Strategy With Splunk

Session 1672

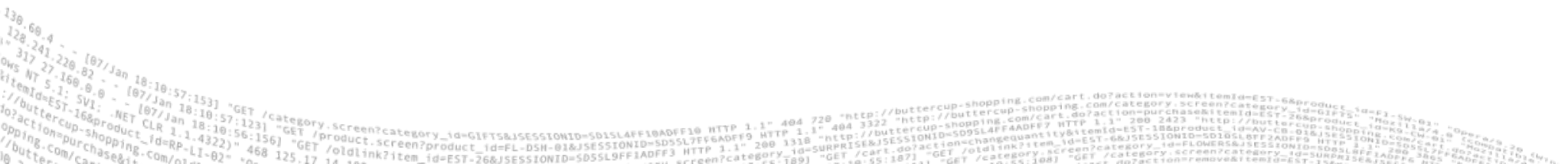
Paul D'Avilar | Splunk
Paul Pelletier | Splunk

October 2018 | Version 1.0

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.



Building a Security Monitoring Strategy With Splunk

Gain visibility as well as resiliency

splunk> .conf18

Personal Information

- Paul D'Avilar
  - Security Consultant at Splunk
  - 1+ year with Splunk
  - 14+ years security markets
- Paul Pelletier
  - Sr. Security Consultant at Splunk
  - 1+ year with Splunk
  - 17+ years security markets
  - Formerly with Capgemini and Schneider Electric and I even owned my own MSSP for a while

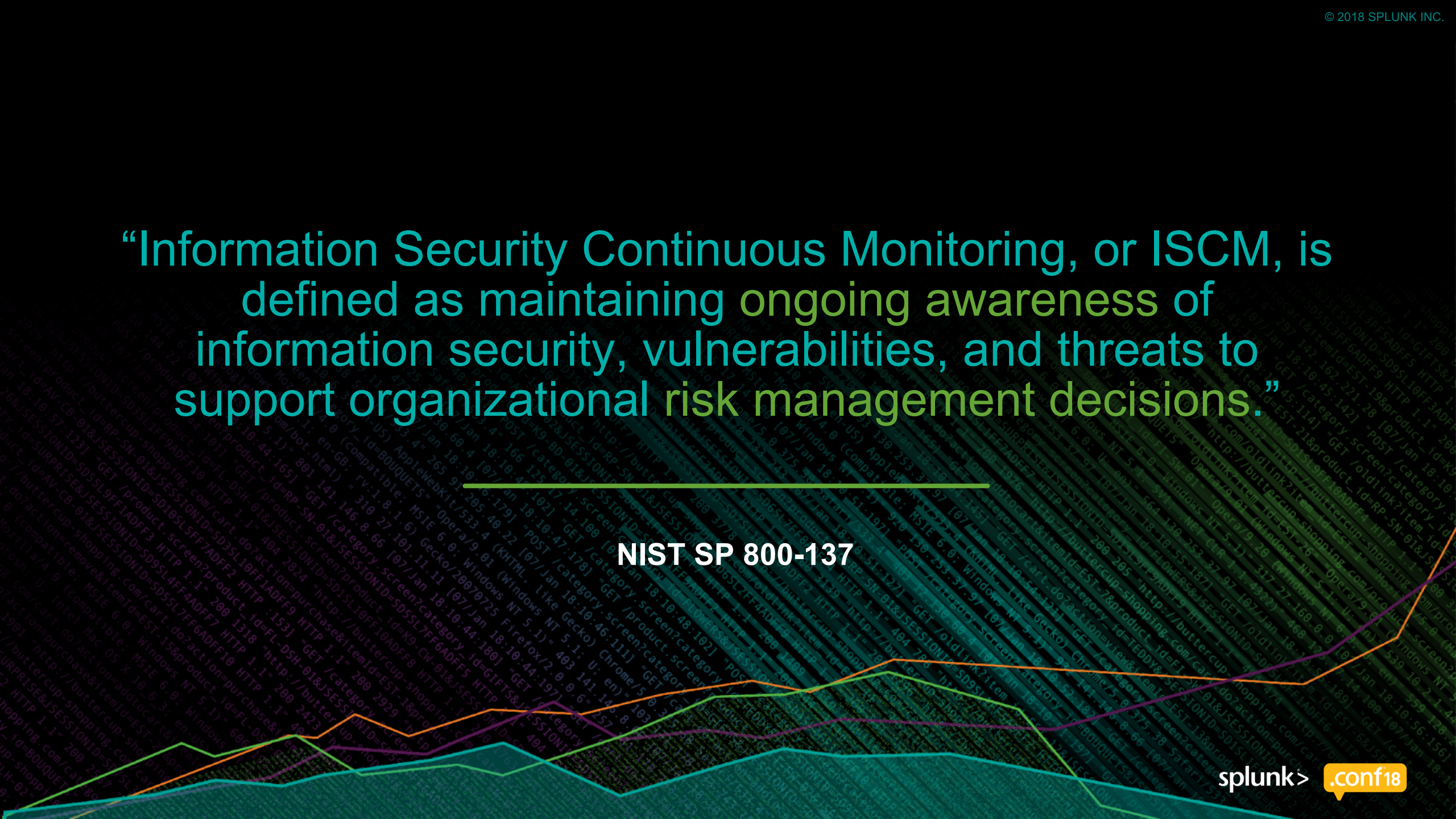
Agenda

The outline for building a security monitoring program

- Identifying objectives – why are you doing security monitoring
- Developing a framework for the prioritization of objectives
- Security Maturity
- Operationalization priorities
- Closing the loop

"Information Security Continuous Monitoring, or ISCM, is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions."

NIST SP 800-137



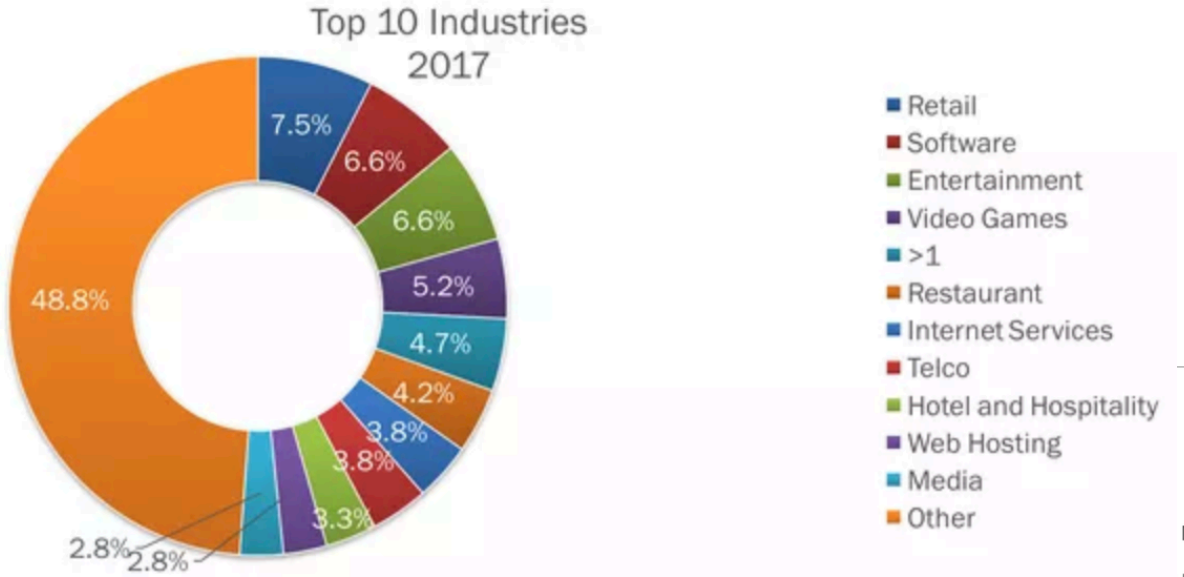
Misconceptions About Security Monitoring

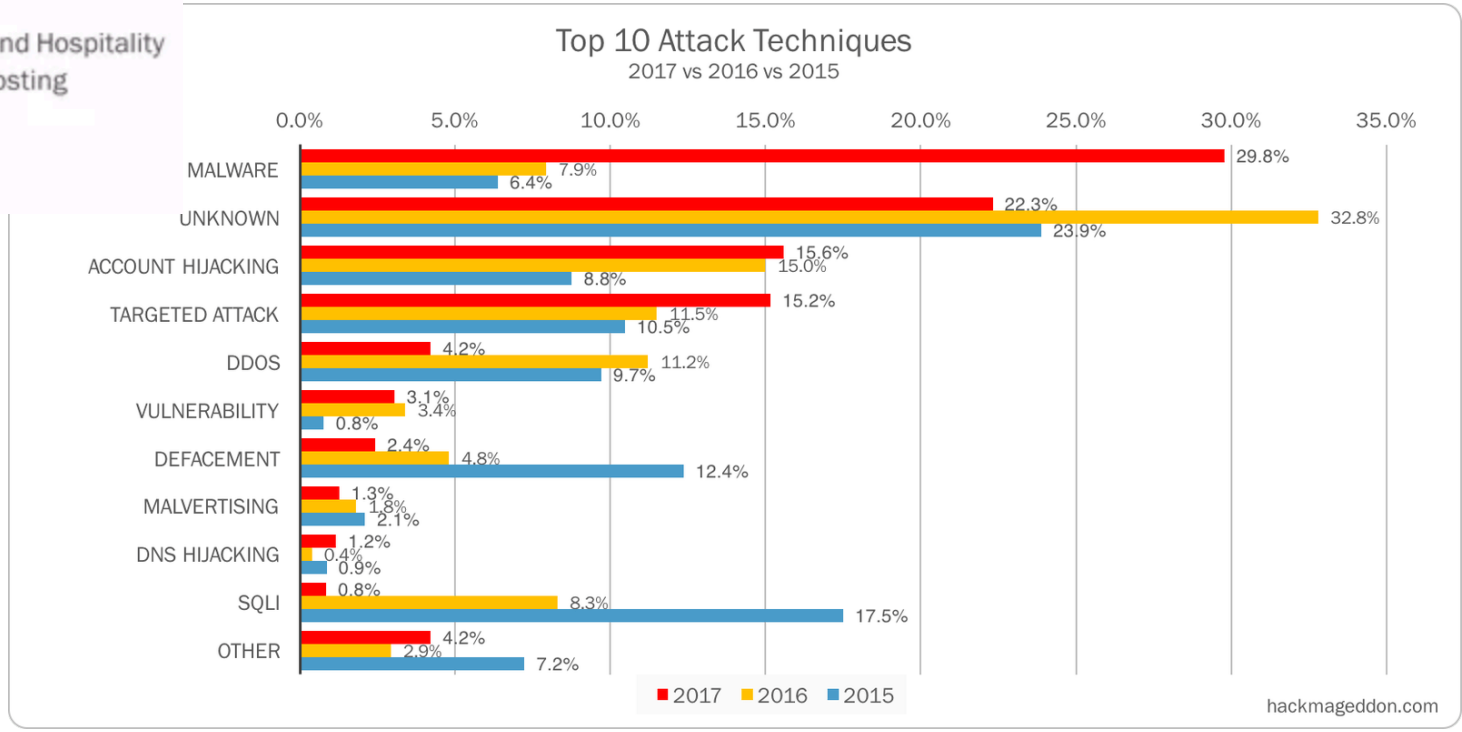
Security monitoring is not hard, just missed understood

- Security monitoring is too hard, too expensive, and too time consuming; continuous monitoring is dead/old news, too much data, we are focusing on AI and ML
- We encrypt everything or at least what is important, so why do we need to do monitoring; the data is garbage
- Monitoring is a compliance only activity, which we are already doing with our quarterly reviews; compliance is security
- We are not a target/no one is interested in us (we are not like the big guys), we are in a sweet spot (not too small, not too big)
- We do preventative security/FWs everywhere, full network segmentation, what else do we need to?

...

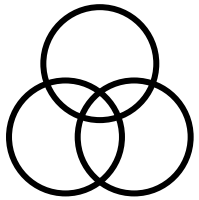
What are the Stats Saying?



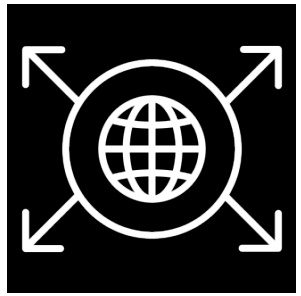


splunk> .conf18

Why is this so Hard?



Machine data is real time, messy and unpredictable



Requires massive scale

You don’t always know which questions to ask

What's the Point of Security Monitoring?

Supports the creation and sustainability of value

Identify & protect assets (crown jewels)

Visibility

Security Ops / Incident Response
Alert and investigate processes

Alignment

Cyber Hygiene
Compliance

Close the decision to take action (Tell me what I need to act on)	Risks/ Security posture (What are my vulnerabilities)

splunk> Platform for Machine Data

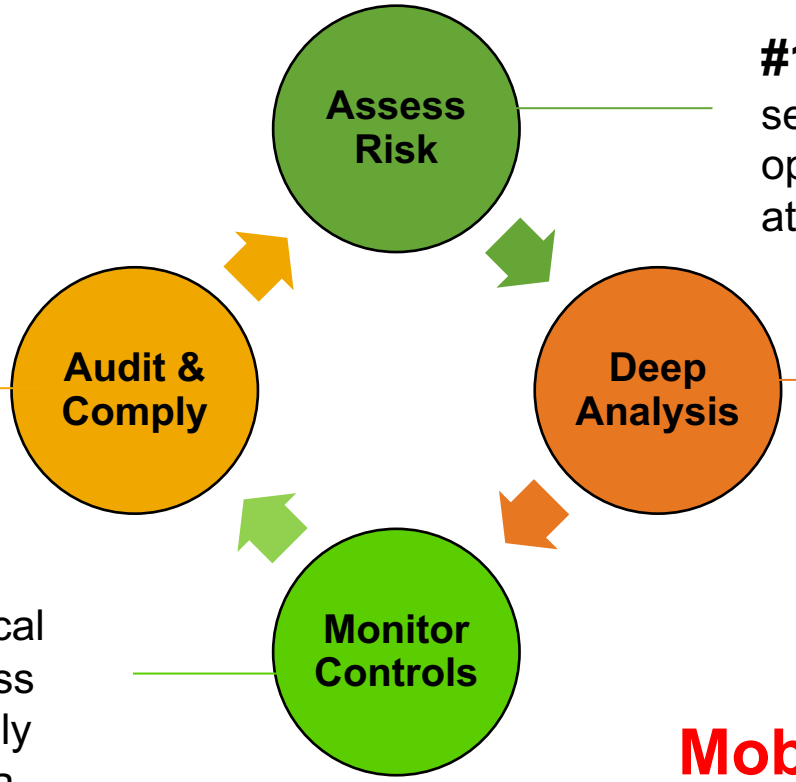
Platform based approach is needed to achieve the objectives for security monitoring

Top 4 Use Cases for Security Monitoring

Data Breaches

Targeted Attacks

E-Crime & Malware



#1 Faster 1st level triage on ALL security attacks with less resources as opposed to reviewing only a subset of attacks

#2 Faster deep dive investigation on security incidents that require further proactive and reactive analysis

#3 Faster implementation of critical security controls (ex: CIS Top 20) across ALL layers of the organization, ultimately resulting in full enterprise visibility and a reduction in risks

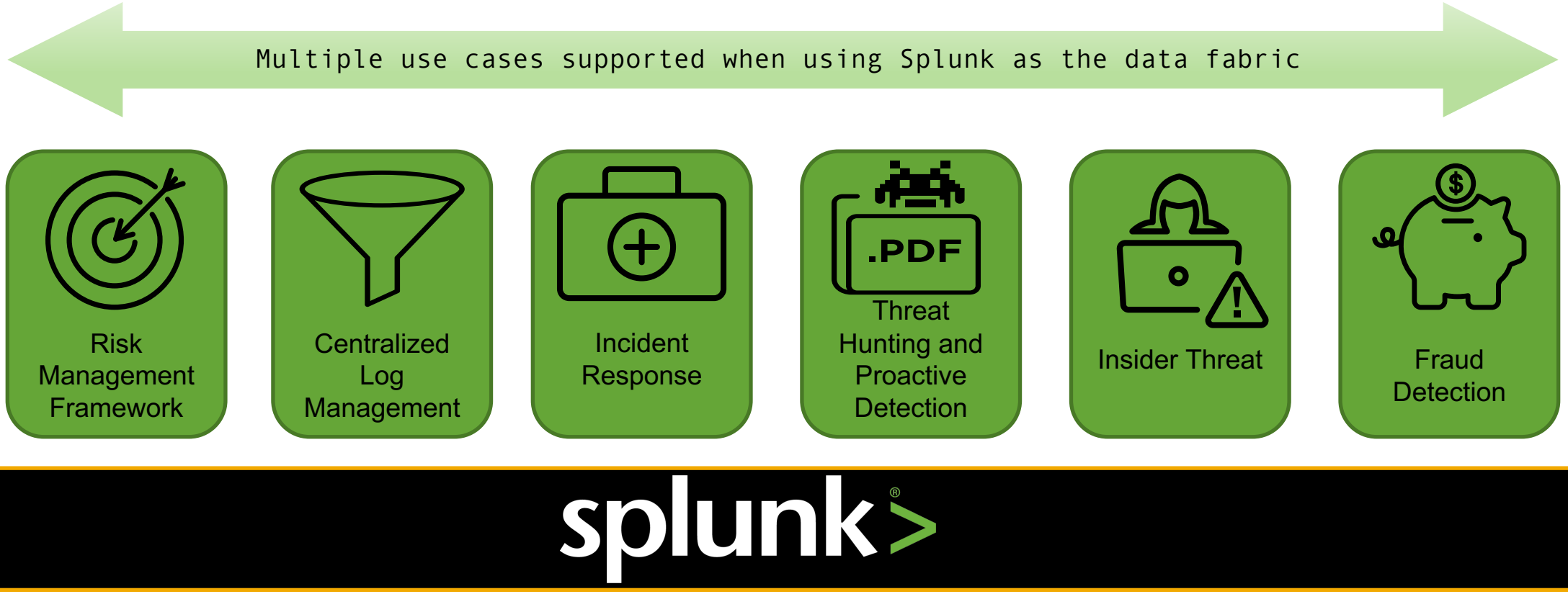
#4 Continuous compliance on ALL components and policies resulting in faster and simpler audits

Web Threats

Mobile & IOT Vulnerabilities

Scams & Social Media

Top 4 Use Cases for Security Monitoring

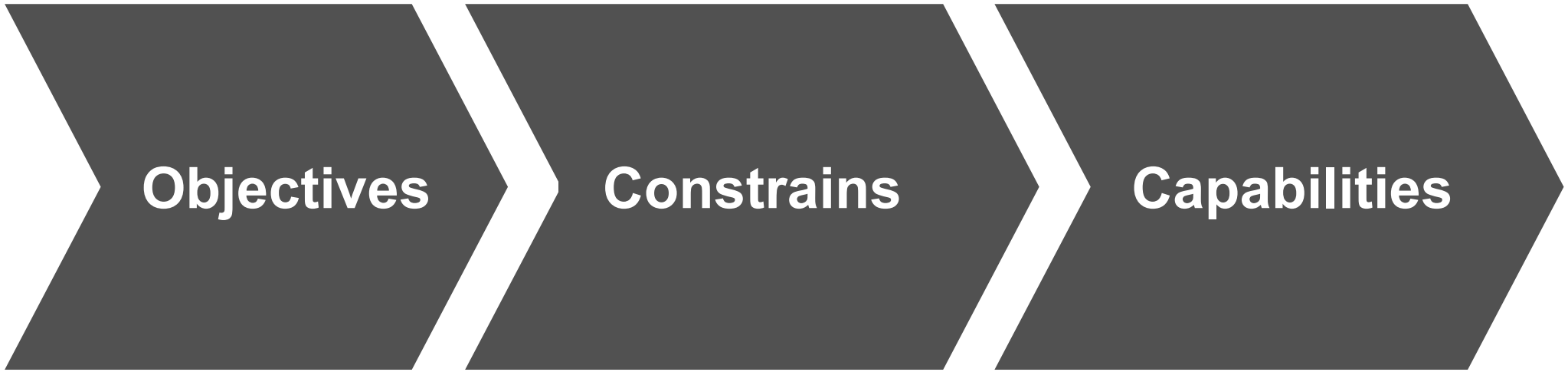


Prioritize

Assess the capabilities of the organization to achieve defined objectives and augment as needed, build on a solid foundation and prioritize

How/Framework

Layout a roadmap for operationalizing capabilities to achieve objectives based on 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

Where to Start

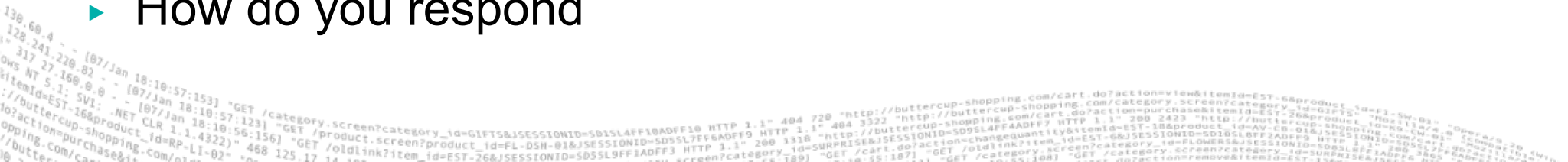
Understand what you are trying to achieve, understand your maturity

- Identity key drivers/ key motivations and support for security monitoring (define a set of objectives)
  - Operations/ Incident Response
  - Laws/Regulations (cost of non compliance)
  - ….
- Think about resiliency
  - We all know it is not if but when, but beyond surviving, we should plan to succeed in carrying out our organizational priorities
- Continuous improvements
  - Assess where you are now and define a target (and a strategy to get there)
  - Metrics
- Accountability
  - Build a program that is measurable, focus on what is effective vs. fancy (being good on paper vs. being real)

4 Important Things to Consider

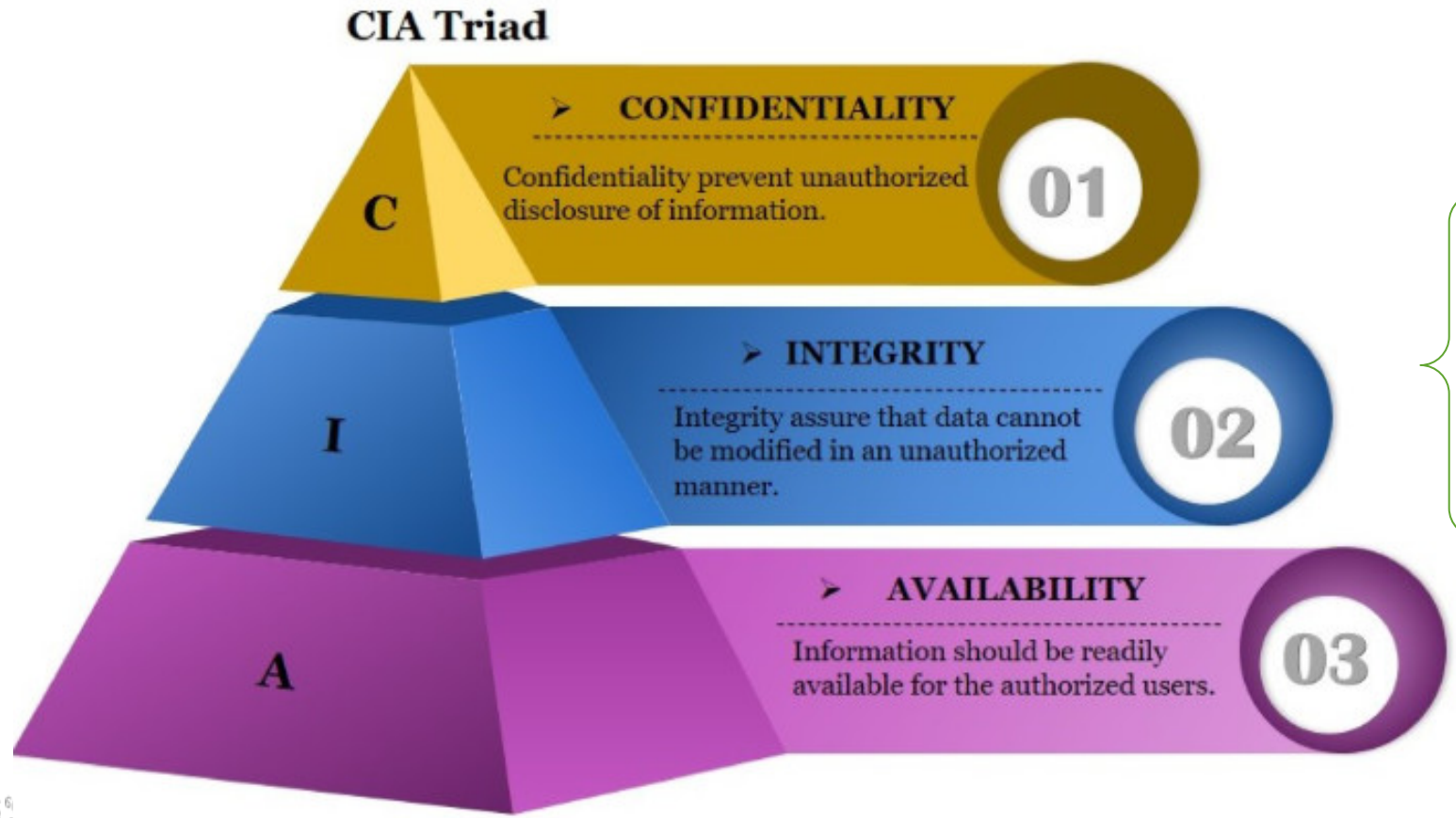
Lots of noise out here, focus on what matters most for your organization – get the basics right

- What data do I need to protect/monitor?
  - Can I get information from my network devices?
  - Endpoint security suites
  - Specific applications
- Compliance and Business Requirements
  - Understand the business or company you are trying to secure and the strategy of your IT Security Program
- Define your continuous monitoring policies and intervals
- How do you respond



Don’t Forget the Fundamentals are Still Relevant

All the standards, frameworks, guidance, recommendations are generally providing approaches for achieving basic security objectives



Additional Considerations:

- Non-reputation
- Resiliency
- You have to protect your data and your customers

Laws & Regulations

Security and compliance vary across, however the challenges similar

- Public sector
  - Federal Information Security Modernization Act (FISMA)
  - Defense Acquisition Regulations Supplement (DFARS)
  - Continuous Monitoring/Risk Management Framework (ConMon/RMF)
  - North American Electric Reliability Corporation - Critical Infrastructure Protection (NERC CIP)
- Commercial
  - Payment Card Industry Data Security Standard (PCI DSS)
  - Gramm-Leach-Bliley Act (GLBA)
  - Sarbanes-Oxley Act (SOX)
  - Health Insurance Portability and Accountability Act (HIPAA)
- International
  - General Data Protection Regulation (GDPR)

Standards/Frameworks

Guidance for addressing the challenges of complying with complex and overlapping regulatory requirements

- NIST
  - SP-800-53
  - SP-800-171
  - SP-800-37
  - Cyber Security Framework
- ISO
  - 27001
  - 27032
  - 22301
- Industry
  - HITRUST
  - ISA62443
  - NERC/CIP

Splunk

Splunk Measures

High Level Requirement	SOX	GLBA	HIPAA	FISMA	NERC	ISO17799	PCI	FIPS200
Audit and Log Security Events	•	•	•	•	•	•	•	AU
Timely Monitoring and Review Centralized Log Management/SIEM	•	A A	•	• I	• I	• I	• •	CM /CA AU
Access and Privilege Management (Individual Accounts, Complex Passwords, Least Privilege, 90 Day change, Min Password...)		A	•	•	•	•	•	AC/ IA
Asset Inventory/Classification (High/Medium/Low, Workstation, Server)		A	•	•	•	•		FIP S 199
IDS/IPS (Perimeter Defenses)		A		I	I	I	•	SI
Anti-Virus Software (Unix is often excluded)				•	•	•	•	SI
Encrypt Sensitive Data in Transit		A	A	•	I	I	•	SC

Ideally one product for all

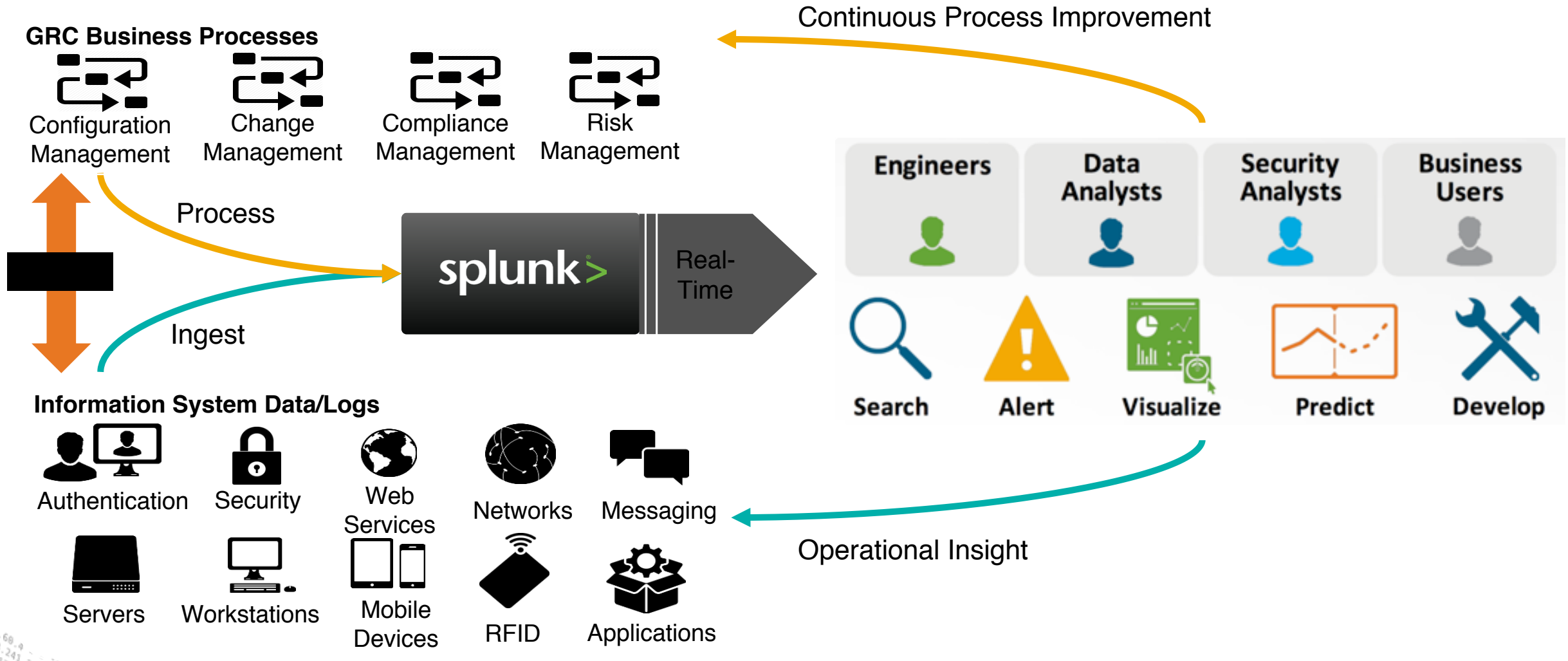
Source: SANS

● = Required
I = Implied
A = As appropriate to the org

splunk> .conf18

Where Does Splunk Fit in to all of This?

Highly-scalable platform for aggregation, automation, and analysis at scale



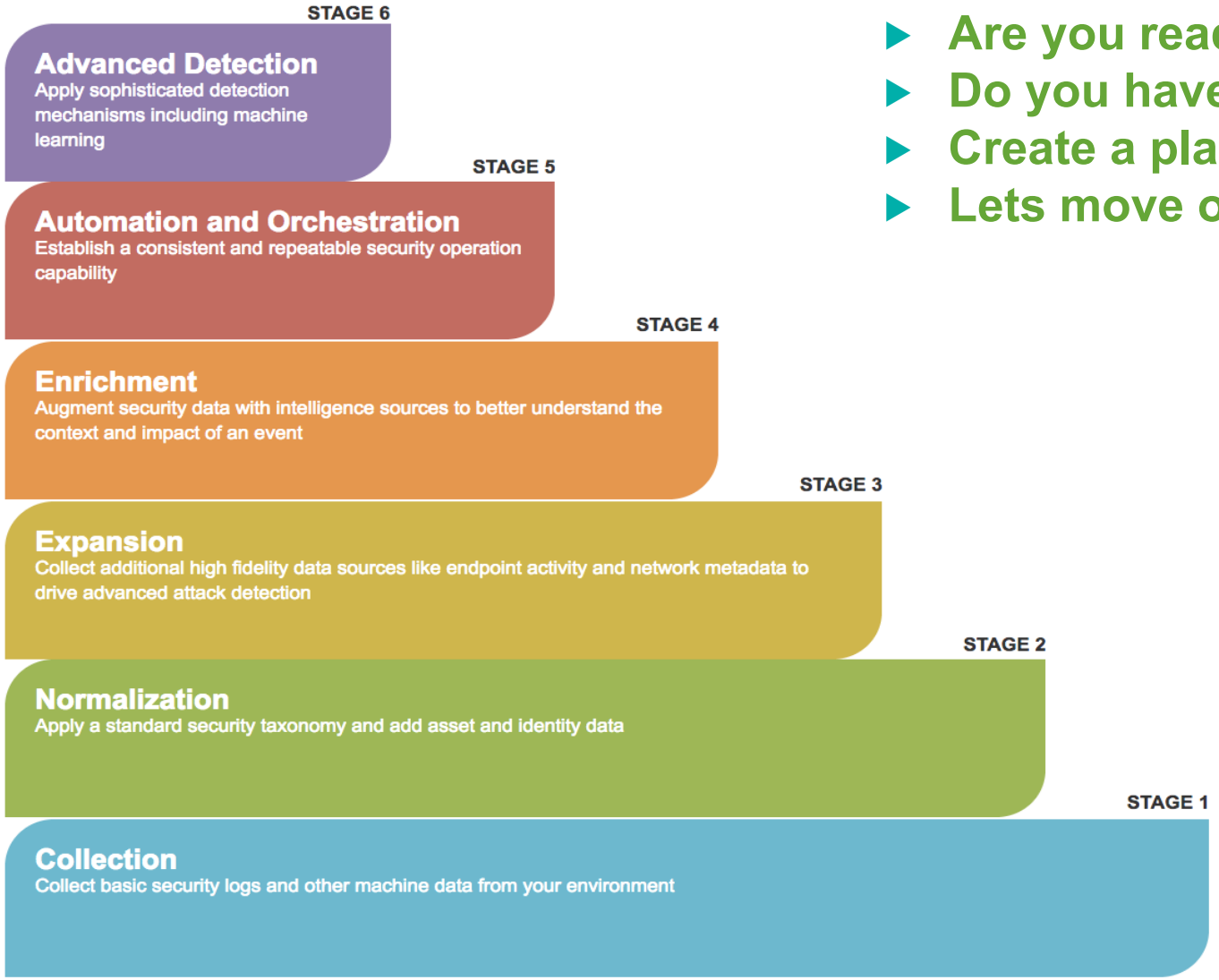
Security Maturity

We all need to define a starting point, a target, and timeframe to get there

Where are You?

It's all about Maturity

Security Data Journey

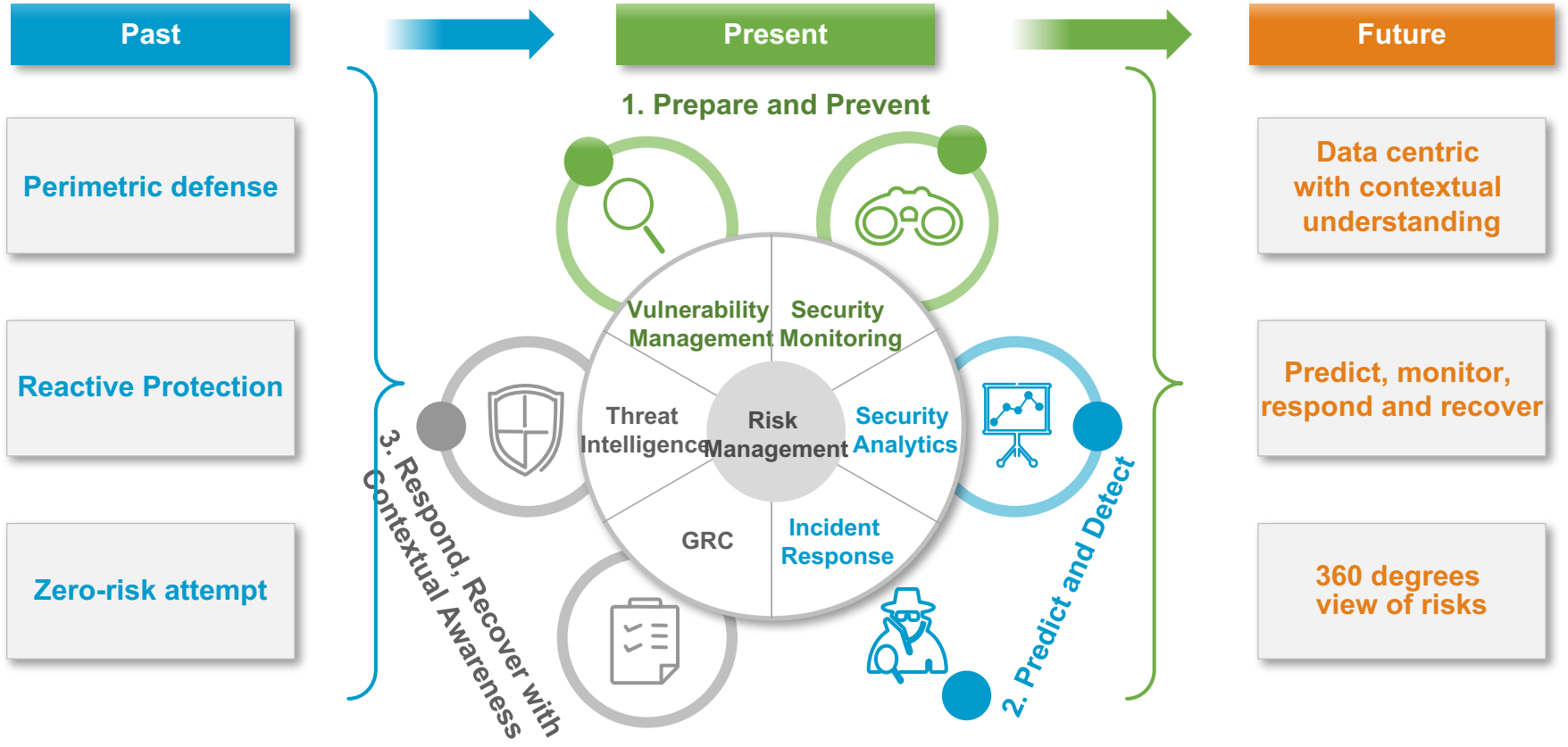


- Are you ready for stage 3?
- Do you have all the appropriate data sources?
- Create a plan, perform a self assessment
- Lets move on up to Stage 4 or 5 or 6!

splunk> .conf18

The Security Monitoring Journey

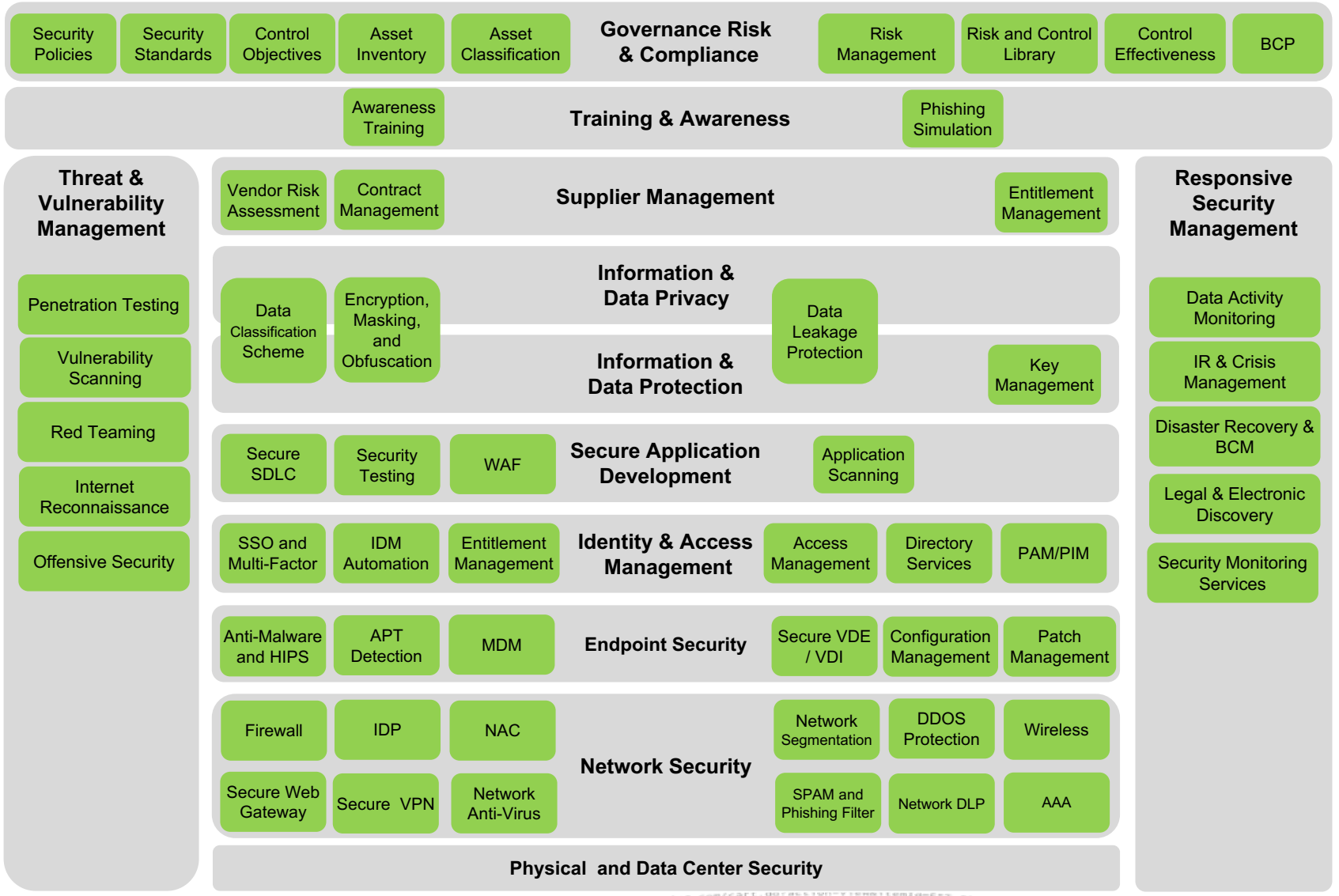
Organizations are moving beyond the traditional perimeter and are looking at security monitoring differently.



splunk> .conf18

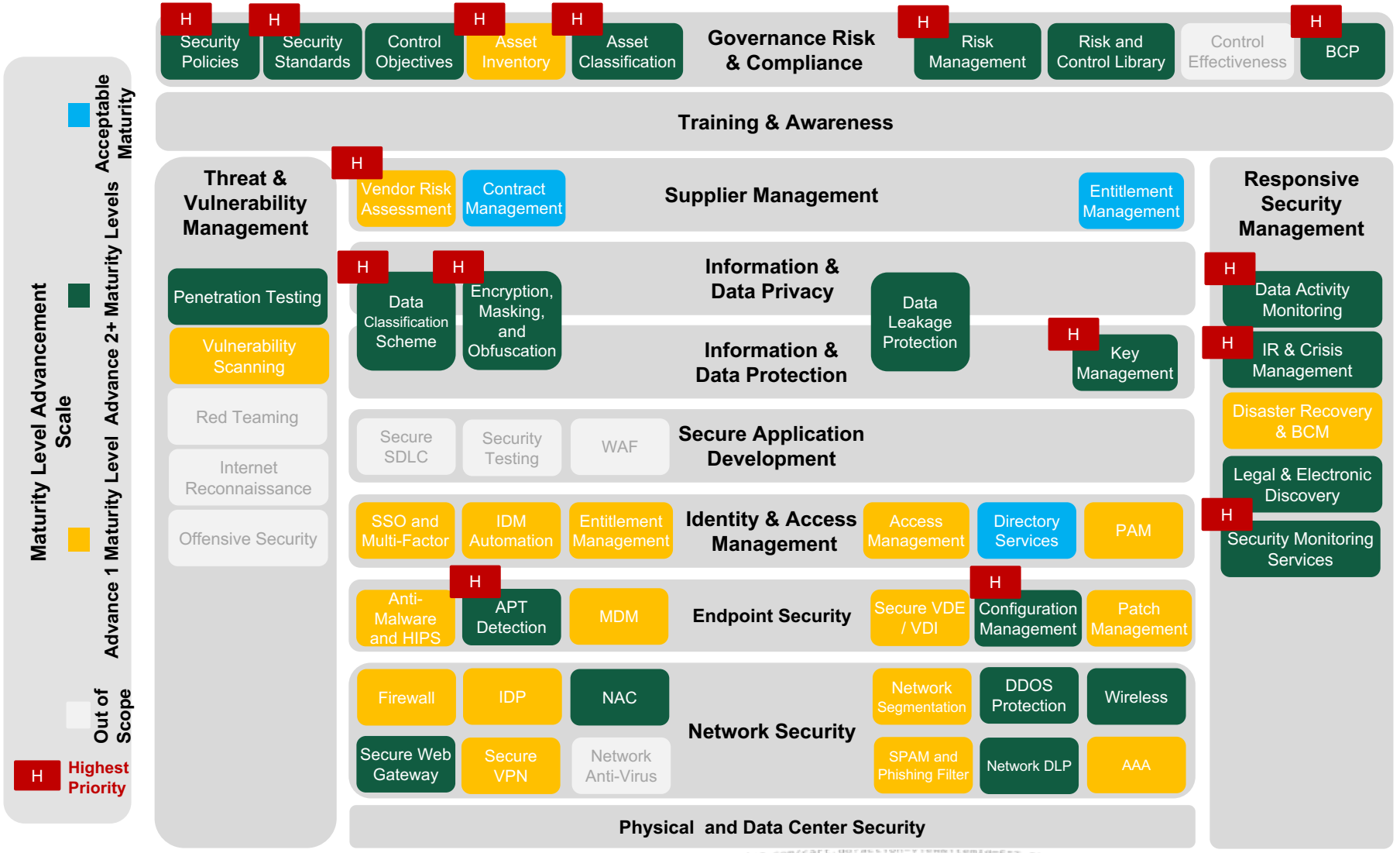
Data Sources and Silos

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



Example Prioritization of Objectives

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



splunk> .conf18

Splunk Vision for Security Resiliency

Using a Data Analytics Driven SOC

Analysts to act as an intelligent brain

- 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

situational awareness to respond to intrusions before assets are at risk

- 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

Operationalize

Outcomes driven

Use Case 1: **Compliance Reporting**

PCI / HIPAA

Questions:

- Do we have all compliance related stuff logged and data retained?
- Is my organization compliant today with an external regulation?
- Does everyone follow my internal compliance requirements e.g. my security policy?
- Who, When, Where, What, Why questions?

Key Data Sources:

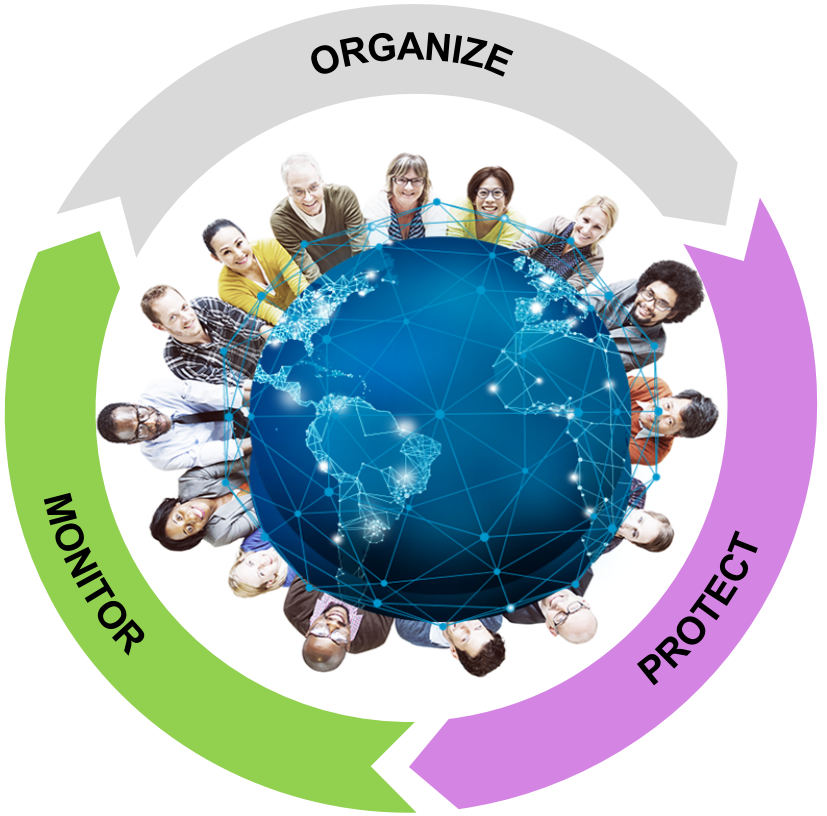
All data associated with compliance / policy requirements i.e. firewalls, proxy, endpoint, AD, AAA, VPN, etc.

Use Case 2: **Data Privacy (GDPR)**

EU General Data Protection Regulation

Questions:

- Who has accessed which personal data record?
- Can I prove that personal data was deleted after the processing was done?
- When and how has consent been given for authorization for processing?
- In the even of an attack:
  - Can I quickly investigate if data has leaked?
  - Can I determine which individual(s) have had data leaked?
  - Can I find all involved systems and users involved in the attack?
- How can I prove that I deployed proper security controls and that they have been active?
- How can I prove that at the point of the breach all systems have been patched? That regular password changes happened?



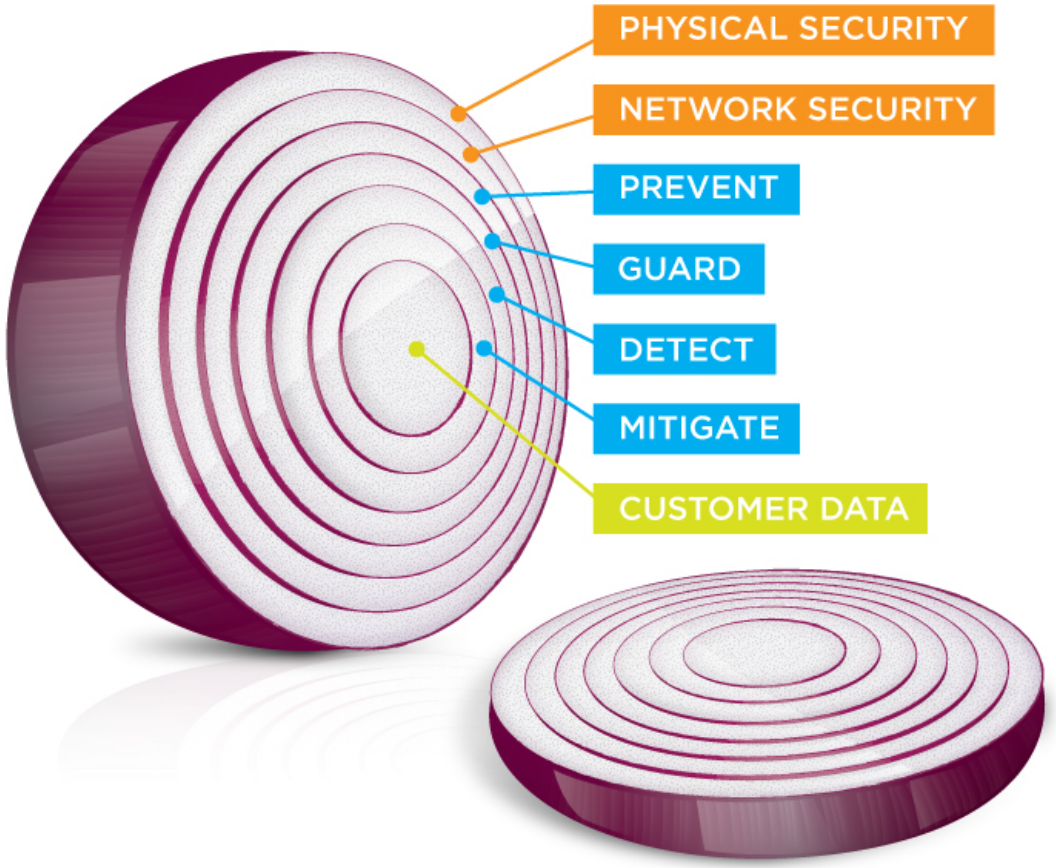
Key Data Sources:

All data is security relevant – not just the data of PD systems and applications

Use Case 3: **Defense in Depth Investigations**

Questions:

- What security controls has a user bypassed/breached?
- What notable events have been triggered within Splunk ES?
- Who else was involved?
- Whose machine is it? Where is the machine located? What is the source/destination? What network is it located on?



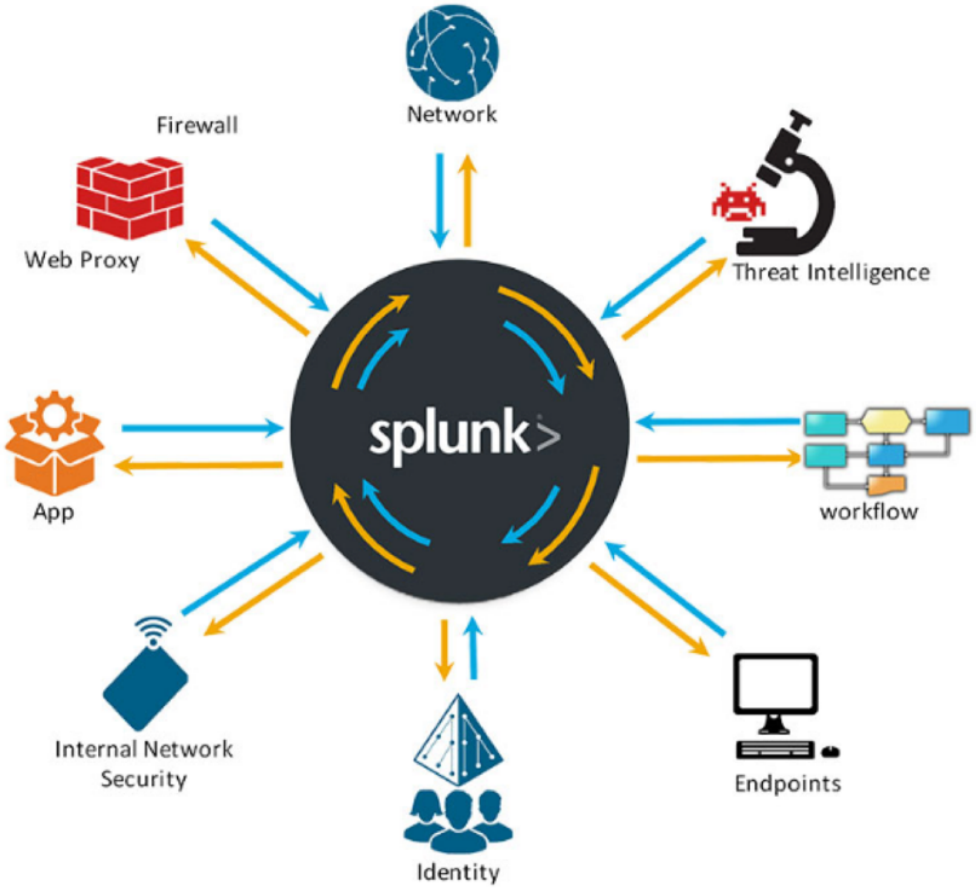
Key Data Sources:

Firewall, Proxy, (H)IPS/(H)IDS, Endpoint, NGAV, DLP, CMDB, AAA, File Access, Badge Data

Use Case 4: **Analytics Driven Security Monitoring**

Questions:

- How does an incident impact or influence my business?
- Who is that user and what are they doing?
- What other events can be correlated in relation to this root event?
- Is that really high severity?
- Which security barriers are effective and which need enhancements/ elimination?



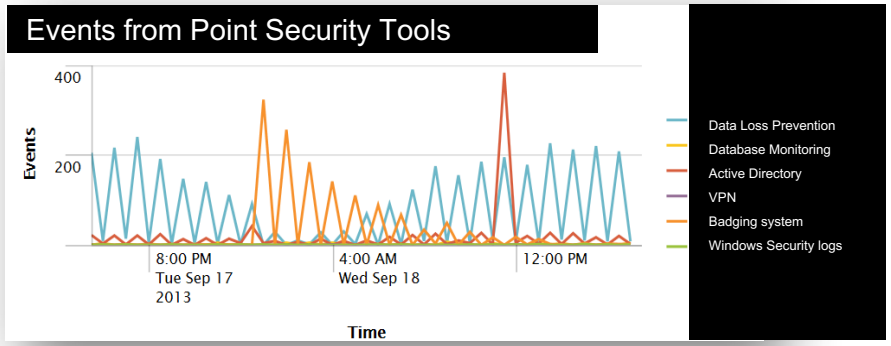
Key Data Sources:

All Security Data is relevant; Firewall, Proxy, (H)IPS/(H)IDS, Endpoint, NGAV, DLP, CMDB, AAA, File Access, Badge Data

Use Case 5: **Insider Threat Detection and Response**

Questions:

- Can I establish a baseline ‘normal’ for a peer group and/or look for outliers/anomalies?
- How can I correlate against specific actions?
- Risk scoring to identify low-severity events that in aggregate are high severity
- Determine “initial triggers” that then initiate closer monitoring
- I want to initiate automated remediation via custom scripts or playbooks



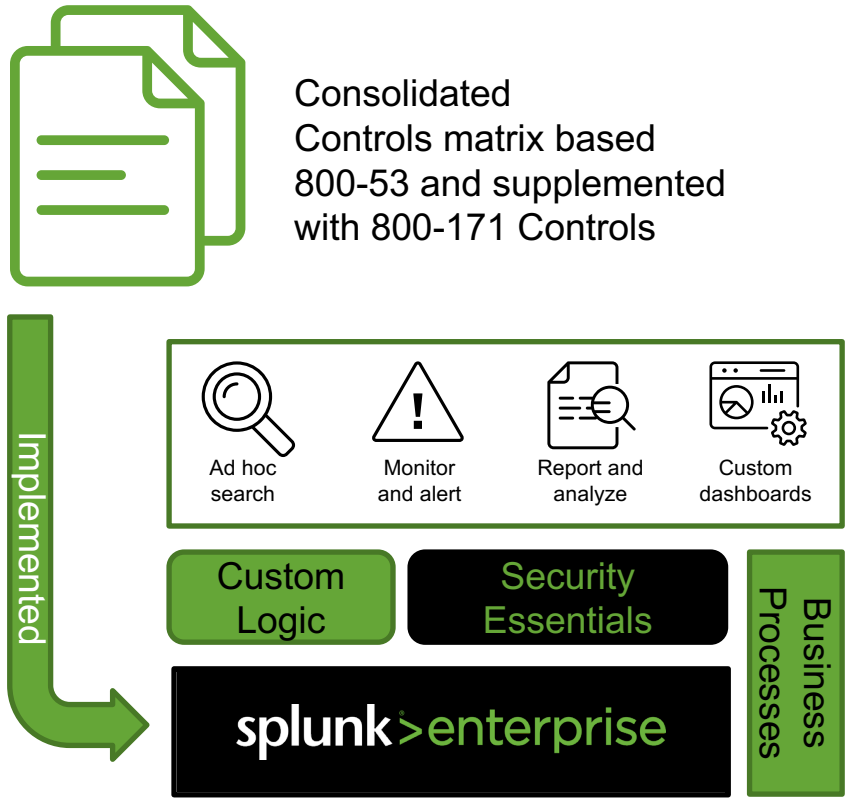
Sample Splunk Summary Index				
User	Data Loss Prevention risk score	Database Monitoring risk score	HR profile risk score	Splunk Total
John Doe	0	2	0	**2**
Fred Haxor	6	9	15	**30**
Jen Smith	1	2	0	**3**

Key Data Sources:

All Security Data is relevant; HR Data, Firewall, Proxy, (H)IPS/(H)IDS, Endpoint, NGAV, DLP, CMDB, AAA, File Access, Badge Data

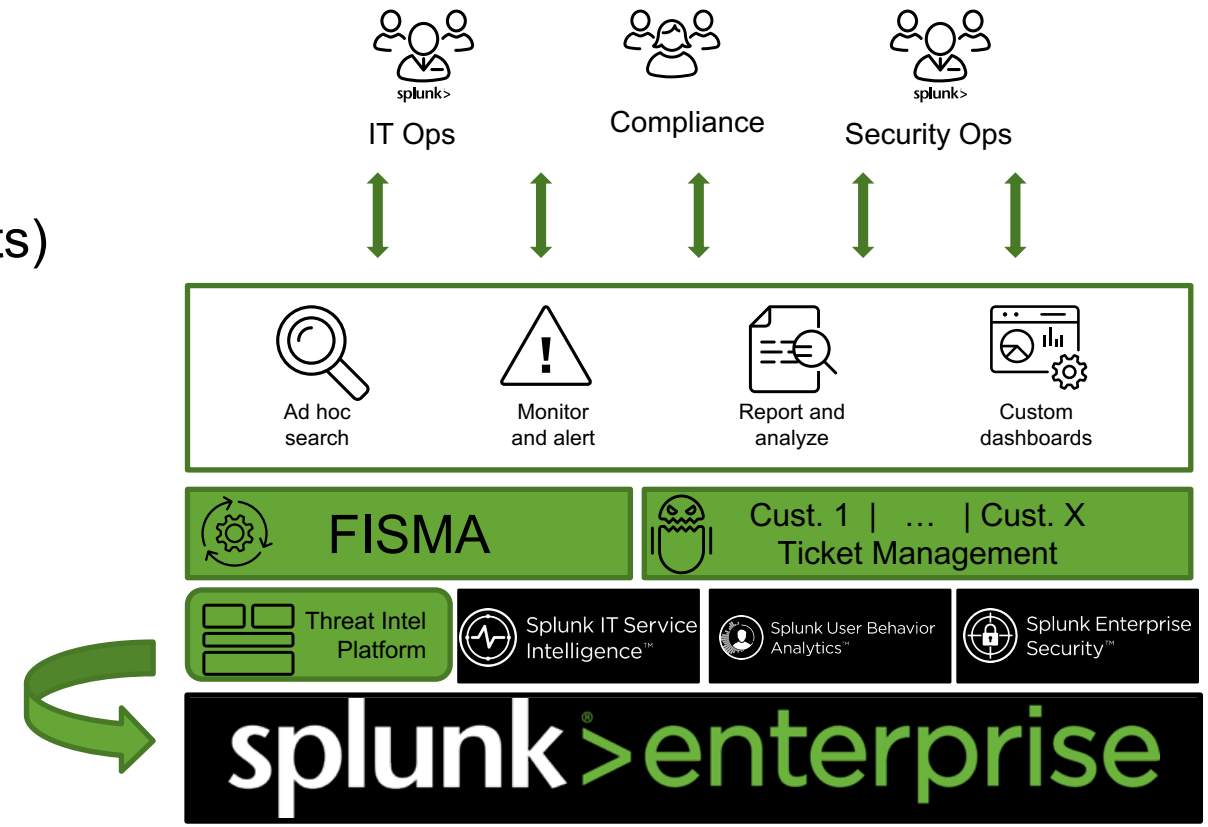
Profile 1: Subsidiary that Provides Services to Gov't (Housing Gov't Data)

- Objectives:
  - Demonstrate that access to gov't data (CUI) is restricted to only individuals with the need to know
  - Support audit readiness
  - FISMA ready (not required but future proofing)
- Constrains:
  - Need to use shared services and share some information with the parent
  - Adherence to 800-171
- Capabilities:
  - Limited staff (No dedicated security professionals
  - Basic set of tools (mainly for operational support)



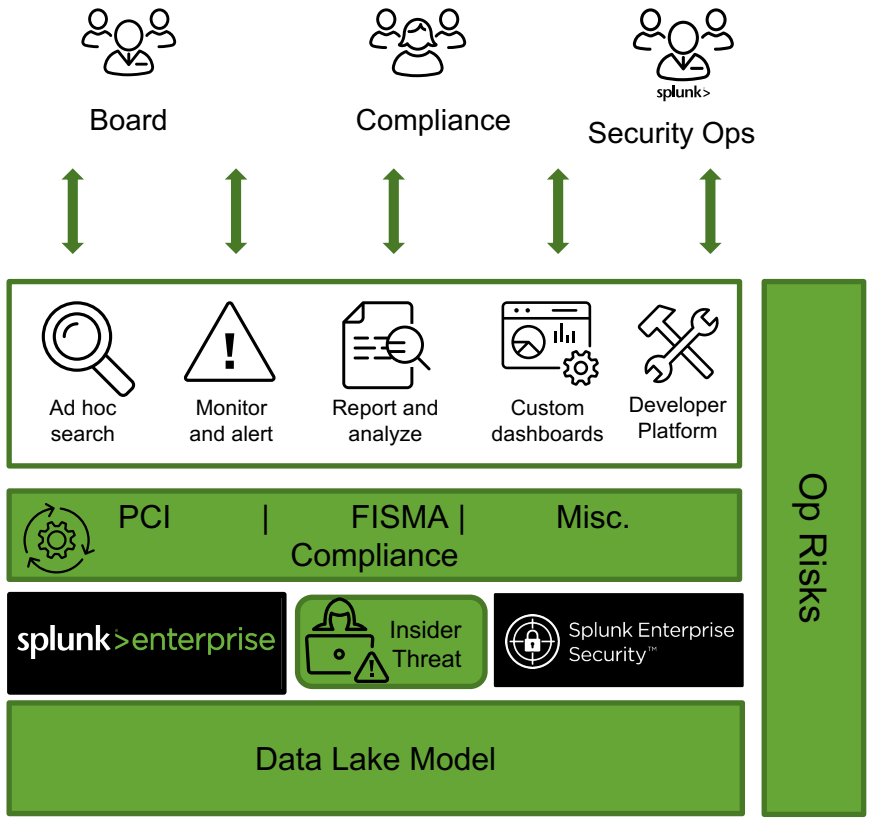
Profile 2: Managed Infrastructure and Security Services

- Objectives:
  - Increase visibility and accountability
  - Audit support (tons of data calls)
  - Support incident response and preparedness
  - Consistency in investigation and response
  - Simply IT and Security Ops (to many starter kits)
  - Metrics (to mature SLA as well as maturity)
- Constrains:
  - Federal and non-gov't customers
  - Contractor managed
  - FISMA, SSAE 18 SOC I & II
  - Geographically spread out (national centers)
- Capabilities:
  - Dedicated SOC (with varying experience)
  - Dedicated threat intel team



Profile 3: Financial Services (Securitization)

- Objectives:
  - Increase visibility and accountability
  - Support audit readiness
- Constrains:
  - Federal and non-gov't customers
  - Highly compartmentalized
  - FISMA, SOX
  - Geographically spread out (international centers)
- Capabilities:
  - Dedicated SOC
  - Unlimited budget (?)



Next Steps

Key Takeaways

1. It’s not as complex as you think
2. Determine your maturity level
3. Create a plan and roadmap for your security journey
4. Define specific use cases based on your data, compliance and business requirements
5. Gain visibility into security posture and maintain near real-time awareness of deviations
6. Operationalize all of this and create relevant playbooks and begin monitoring and responding with Splunk!

The Splunk Portfolio

Splunk Premium Solutions

Splunk IT Service Intelligence™

Splunk Enterprise Security™

Splunk User Behavior Analytics™

Phantom®

Rich Ecosystem of Apps & Add-Ons

amazon web services

cisco

paloalto NETWORKS

TANIUM™

box

kepware

puppet

>enterprise

>cloud

splunk> Platform for Machine Data

Forwarders	Syslog/ TCP	Mobile	IoT Devices	Network Wire Data	Hadoop	Relational Databases	Mainframe Data

Consider a Security Use Case Workshop

This Workshop helps you increase the effectiveness of your security monitoring and identify ways to improve your security posture. Our experts aid in identifying and customizing the security queries (use cases) to maximize the opportunities to improve your security posture, align with your business needs and risk priorities. The Workshops focus on identifying use cases that improve your ability to:

- Monitor your network attack surface
- Conduct advanced threat monitoring on the endpoint
- Conduct advanced threat monitoring in the network
- Monitor key cyber terrain
- Monitor your policy violations
- Conduct network health monitoring
- Monitor for "first seen" or anomalouse\ activity
- Monitor user behavior

Use Case Workshops help your organization by:

✓ Helping to develop a roadmap with your organization to increase your visibility into high risk activity

✓ Implementing a security monitoring framework that will help you reduce noise and focus your investigations

✓ Allowing us to help you discover the most effective monitoring strategy to support your business and processes

“Most mature SIEM users report that their most valuable use cases were site-specific, custom or at least heavily customized”

– Anton Chuvakin, Research VP Gartner

http://blogs.gartner.com/anton-chuvakin/2015/12/02/starting-a-siem-project-from-vendor-use-case-content-win-or-fail/

Thank You

Don't forget to rate this session in the .conf18 mobile app

Q&A

Paul D'Avilar | Speaker
Paul Pelletier | Speaker

What is continuous security monitoring?

Talking Points/Notes

- The objective of a continuous monitoring program is to determine if the complete set of planned, required, and deployed security controls within an information system or inherited by the system continue to be effective over time in light of the inevitable changes that occur. - The NIST CM FAQ
- Promotes the concept of near real-time risk management and ongoing information system authorization through the implementation of robust continuous monitoring processes; (800-37)
- …to support consistent, well-informed, and ongoing security authorization decisions (through continuous monitoring), transparency of security and risk management-related information, and reciprocity; (800-37)

NIST

Talking Points/Notes

- Under F[illegible]A, the National Institute of Standards and Technology (NIST) is requi[illegible] publish key security standards and guidelines
- [illegible] Task Force Transformation Initiative Interagency Working Group
  - Formed in April 2009
    - Representatives from NIST, DOD, ODNI
    - Produced a unified information security framework for the federal government
    - Standards and guidance covering risk management, security categorization, security controls, security assessment procedures, and security authorization process
- NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach (RMF)

PCI

Talking Points/Notes

- A stand[illegible]at was developed jointly by Visa, Mastercard, Discover to secure payn[illegible]ystems in retail environments.
- 6[illegible] tenants
  - Build and maintain a secure network
  - Protect Cardholder data
  - Maintain a vulnerability management program
  - Implement strong access control measures
  - Maintain an information security program