(ISC)² WEBINARS
SECURITY BRIEFINGS

Security Secrets: Why Leading SOC Teams Have Cloud-y Vision

Matthias Maier, Product Marketing Director, Splunk;

Brandon Dunlap, Moderator



splunk>
turn data into doing.™



Housekeeping for Today's Webinar

- Please submit questions via the "Questions" tab – we will address as many questions as possible during the webinar
- Please rate the webinar upon completion
- Should you experience the presentation slide deck freezing, please refresh your browser
- CPEs will be submitted on (ISC)^2 members' behalf within 5 business days *(must have minimum 45-minute viewing time)*



Agenda

- The Cloud and DevOps Attack Surface
- The Future Of People and Technology in SecOps
- 4 Secrets to Building Modern SecOps
  - SOC in the Cloud
  - DevOps Agility in Detection Engineering
  - Multi-Cloud Services Monitoring
  - Embedding the SOC into DevOps and the CI/CD Lifecycle

“The Cloud”

DevOps and Cloud Services

Cloud Is Not Just Office Apps

1. **Digital Transformation**
   Demanded by Customers & Business Stakeholders
2. **DevOps (CI / CD Pipeline)**
   More frequent releases, Faster release times – Attack Surface WITHIN CI / CD
3. **Extensive Use Of Cloud Services**
   Loosely Coupled Microservices and Serverless Functions, Many Providers/Vendors – Attack Surface With Multi Cloud Services
4. **Modern Security Operations Ready for the Cloud Age**
   Cover new technologies with an expanded attack surface
   Need to work agile to keep the pace with DevOps (CI / CD)

Survey

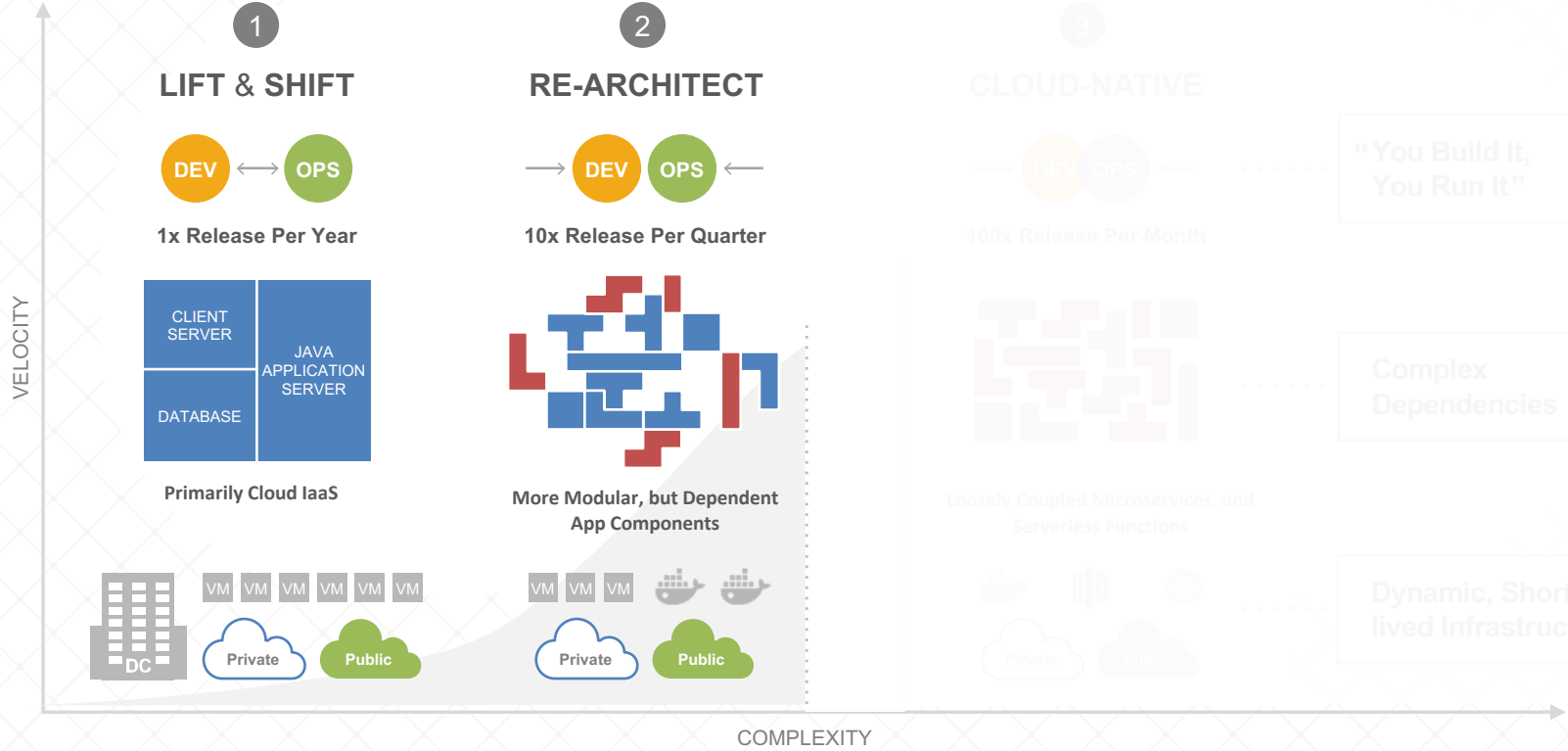
How many cloud infrastructure and service providers do you use across your company?

- ❑ None
- ❑ 1-5
- ❑ 6-20
- ❑ 20-50
- ❑ 50+

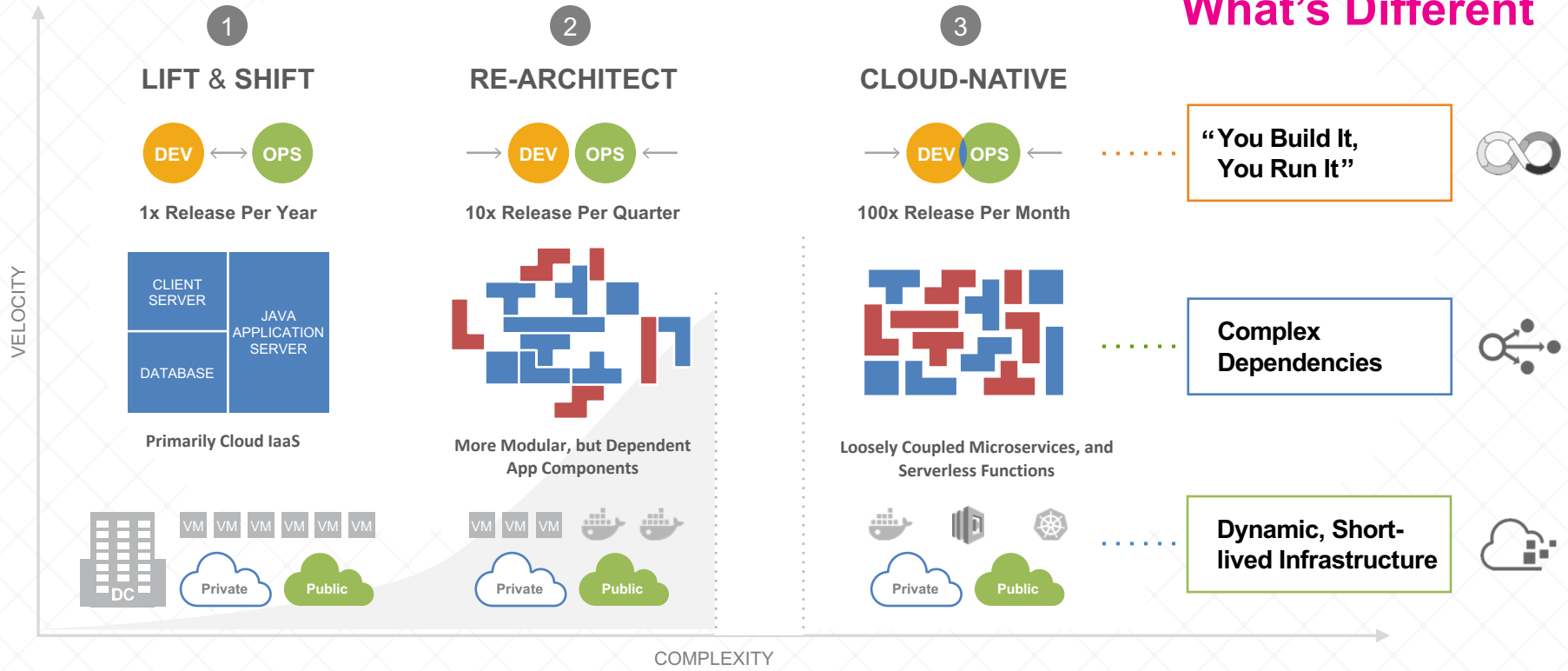
Cloud is a Critical Enabler of Transformation, but Increases Complexity



Cloud is a Critical Enabler of Transformation, but Increases Complexity



Cloud is a Critical Enabler of Transformation, but Increases Complexity



Amazon Textract

Easily extract text and data from virtually any document

Get Started with Amazon Textract

FEATURED BLOG

Use Amazon A2I with Amazon Textract

Easily build-in human review to Textract workflows with Amazon A2I.

Learn more »

Amazon Textract is a service that automatically extracts text and data from scanned documents. Amazon Textract goes beyond simple optical character recognition (OCR) to also identify the contents of fields in forms and information stored in tables.

Many companies today extract data from documents and forms through manual data entry that's slow and expensive or through simple optical character recognition (OCR) software that requires manual customization or configuration. Rules and workflows for each document and form often need to be hard-coded and updated with each change to the form or when dealing with multiple forms. If the form deviates from the rules, the output is often scrambled and unusable.



What is Amazon Textract (1:49)

Cloud is a Critical Enabler of Transformation, but Increases Complexity



In a mid-sized to large organization, all phases are available at the same time

Looking Into Every Nook and Cranny

The Attack Surface

Survey

Do you feel your cloud provider offers higher security standards or lower than you would operate yourself?

- ❑ Lower Standards
- ❑ Similar Standards
- ❑ Higher Standards

Shared Responsibility = You own Data & Security

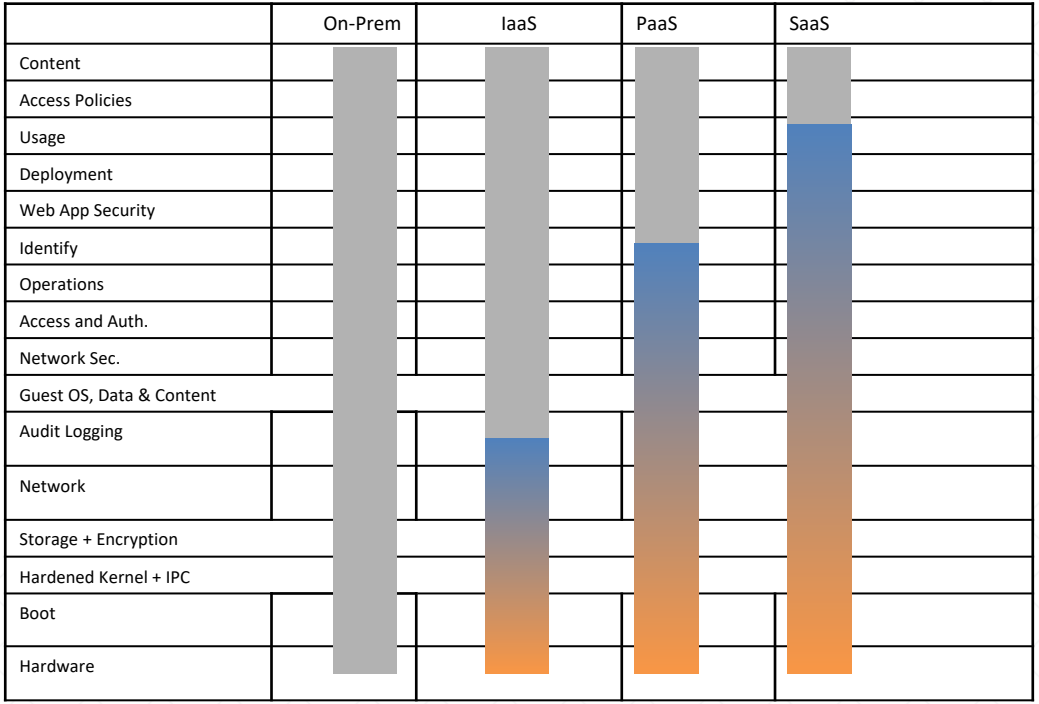
= Cloud Provider Responsibility

= Customer Responsibility

Understanding Shared Responsibility

- The **boundaries change** based on the services selected by the customer

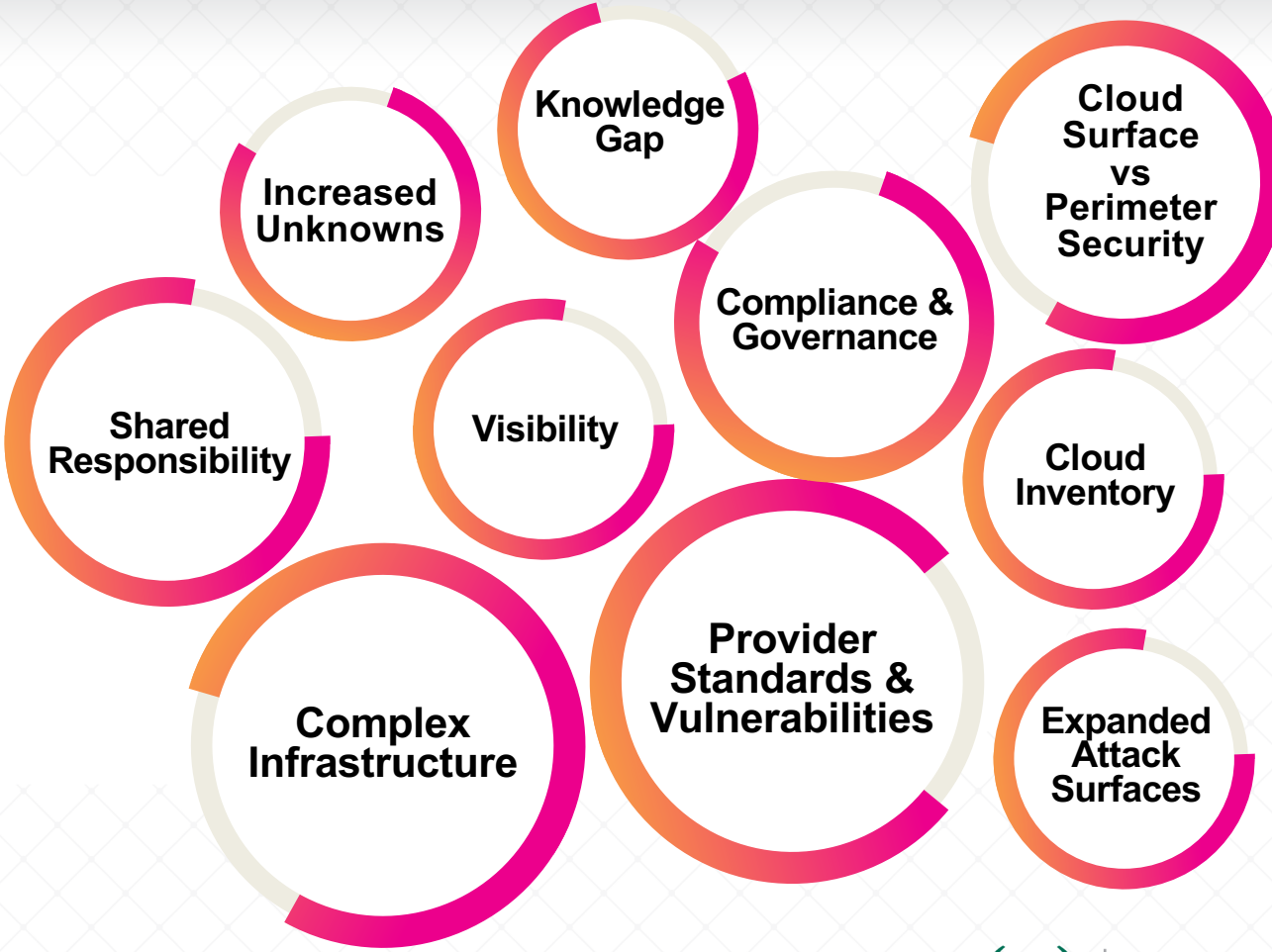
Workplace	CI / CD Platforms & Code Repositorys	Infrastructure as Code (IaC)
Office 365	Jenkins	puppet
workday.	GitHub	ANSIBLE
salesforce	Travis CI	HashiCorp Terraform



What's the impact for Security Operations Teams?

Common Challenges & Threats

Challenges of Cloud Security Operations



MITRE Cloud Matrix

Cloud-based techniques for AWS, GCP, Azure, Azure AD, Office 365, SaaS

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impact
Drive-by Compromise	Account Manipulation	Valid Accounts	Application Access Token	Account Manipulation	Account Discovery	Application Access Token	Data from Cloud Storage Object	Transfer Data to Cloud Account	Resource Hijacking
Exploit Public-Facing Application	Create Account		Redundant Access	Brute Force	Cloud Service Dashboard	Internal Spearphishing	Data from Information Repositories		
Spearphishing Link	Implant Container Image		Revert Cloud Instance	Cloud Instance Metadata API	Cloud Service Discovery	Web Session Cookie	Data from Local System		
Trusted Relationship	Office Application Startup		Unused/Unsupported Cloud Regions	Credentials in Files	Network Service Scanning		Data Staged		
Valid Accounts	Redundant Access		Valid Accounts	Steal Application Access Token	Network Share Discovery		Email Collection		
	Valid Accounts		Web Session Cookie	Steal Web Session Cookie	Permission Groups Discovery				
					Remote System Discovery				
					System Information Discovery				
					System Network Connections Discovery				

An Analytics-Driven Security Approach

Aligns to Security Maturity Journey

Investigate



Establish an investigative data platform and correlate events across the entire stack

Monitor



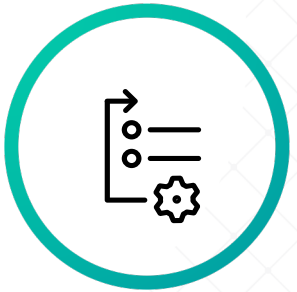
Use the same data platform across infrastructure, apps and services to proactively monitor and report across teams

Analyze



Enable machine learning (ML) and artificial intelligence (AI) for deeper analysis, predict issues and proactive threat hunting

Act



Automate tasks and orchestrate workflows for fast response and countering threats

Survey

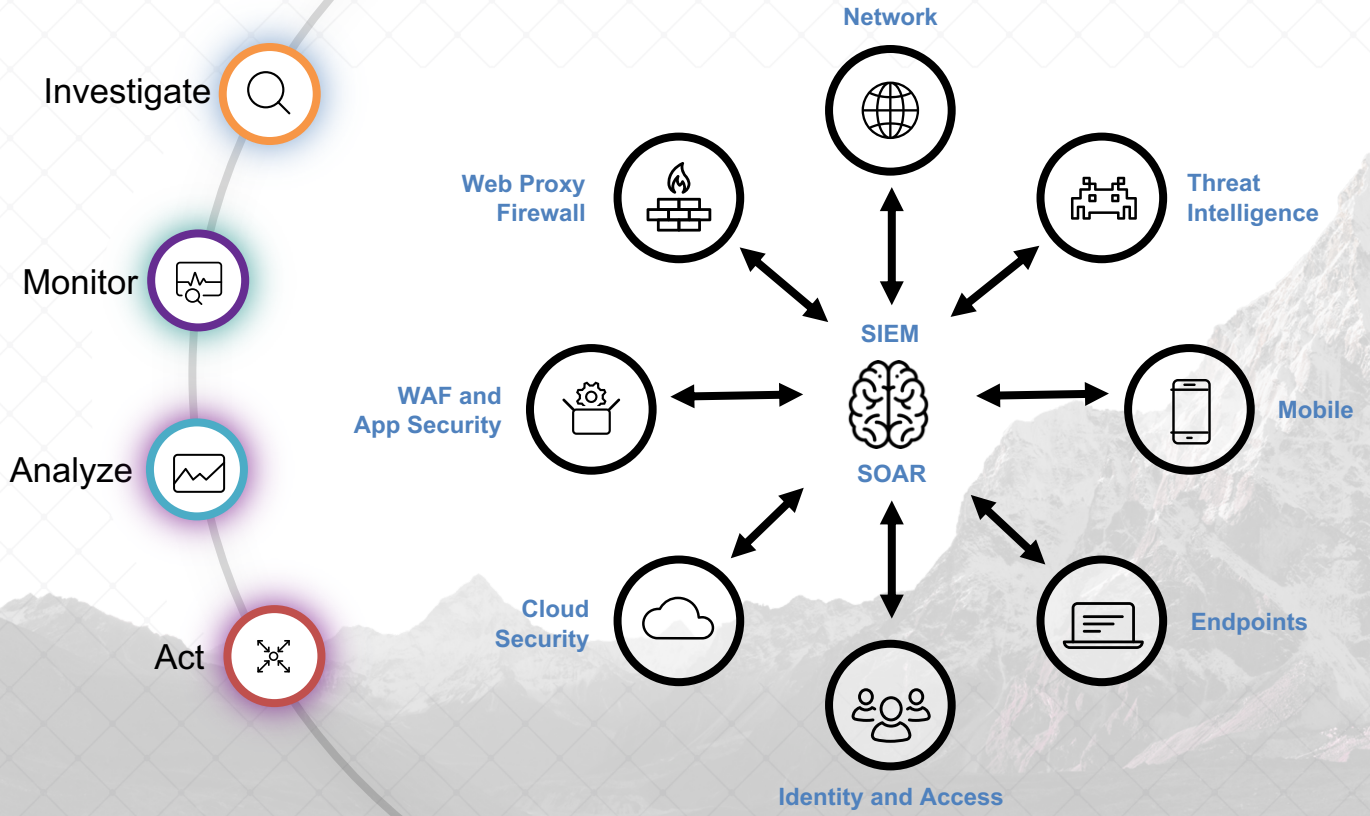
Does your organization increase your security headcounts when it adds new cloud providers and services?

- ❑ Yes
- ❑ No

The Future Of Security Operations (SecOps)

People, Process & Technology

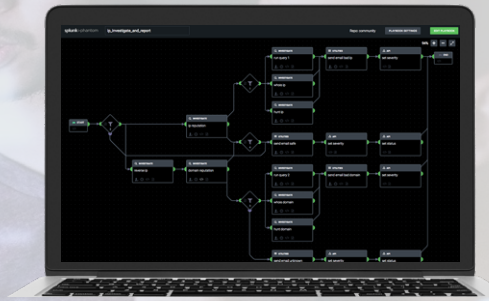
Security Nerve Center



New Roles in Security Operations

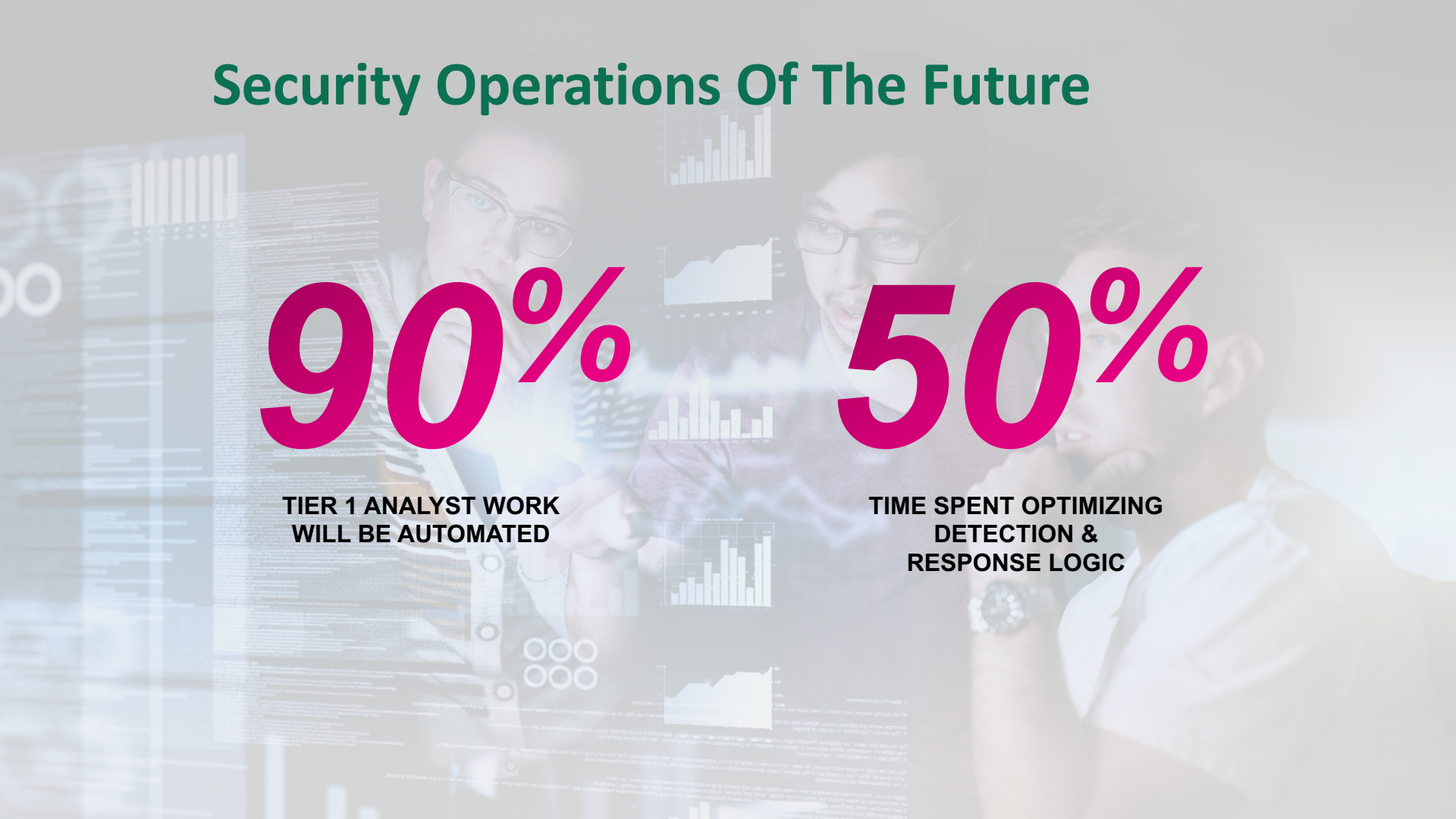


Security Content Developer



Automation Engineer

Security Operations Of The Future



90%

TIER 1 ANALYST WORK WILL BE AUTOMATED

50%

TIME SPENT OPTIMIZING DETECTION & RESPONSE LOGIC

4 secrets

Splunk Customers Building Modern SecOps

SOC in the Cloud

Agility in Detection Engineering

Multi Cloud Services Monitoring

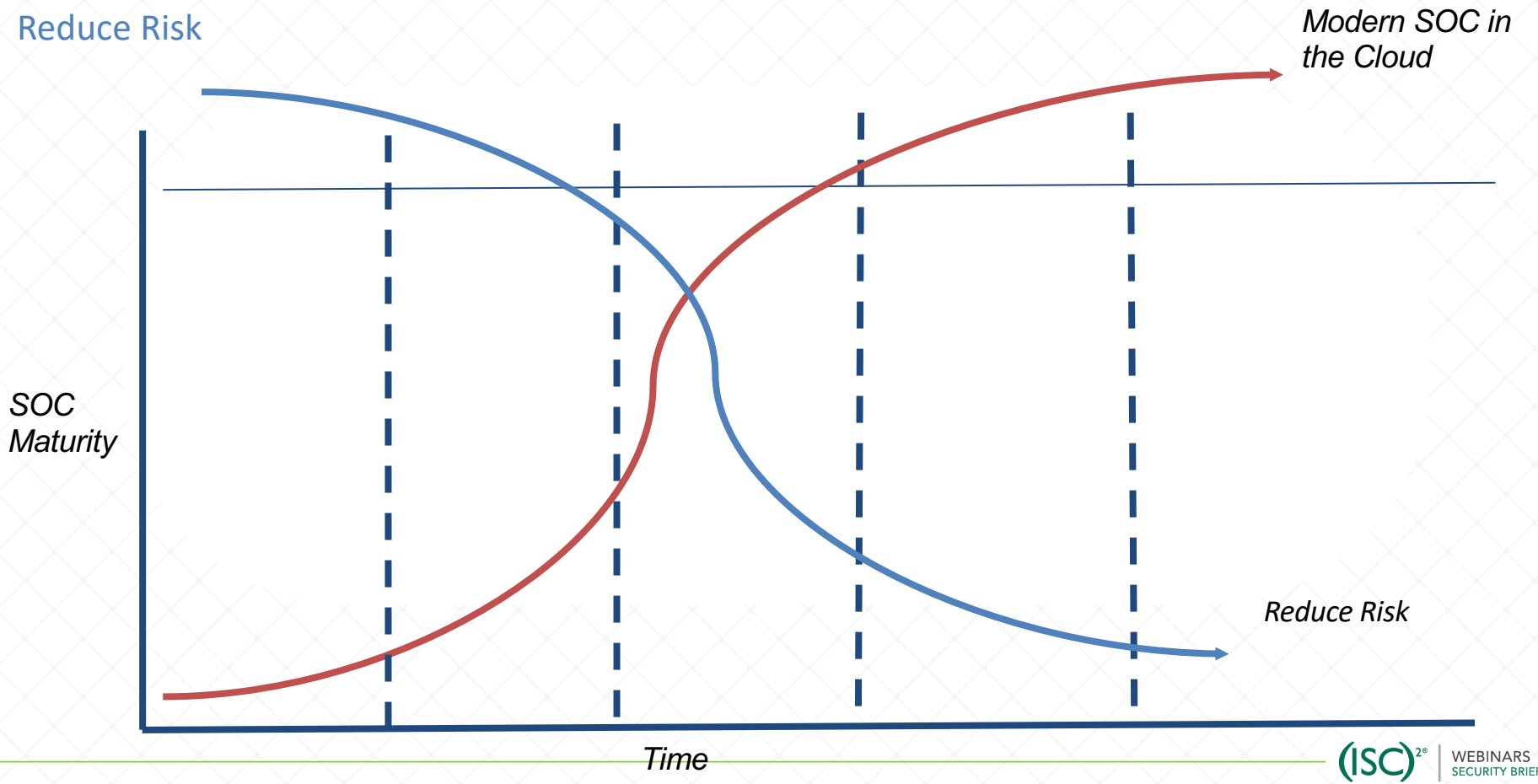
Embedded in DevOps



How To Mature The SOC & Mitigate Cyber Risks Faster

Mature the SOC Faster in the Cloud

Reduce Risk



Security Operations on Splunk Cloud

Accelerate your Cloud Journey

Time to Value



SIEM Deployment in Days not in weeks or months

Easy to Scale



Upmost scalability and agility tied to provisioning on demands HW & SW

Upmost Flexibility



Ingest any data, from any layer (hybrid cloud) at any speed & volume – Highest SecOPS Performance

Lower TCO

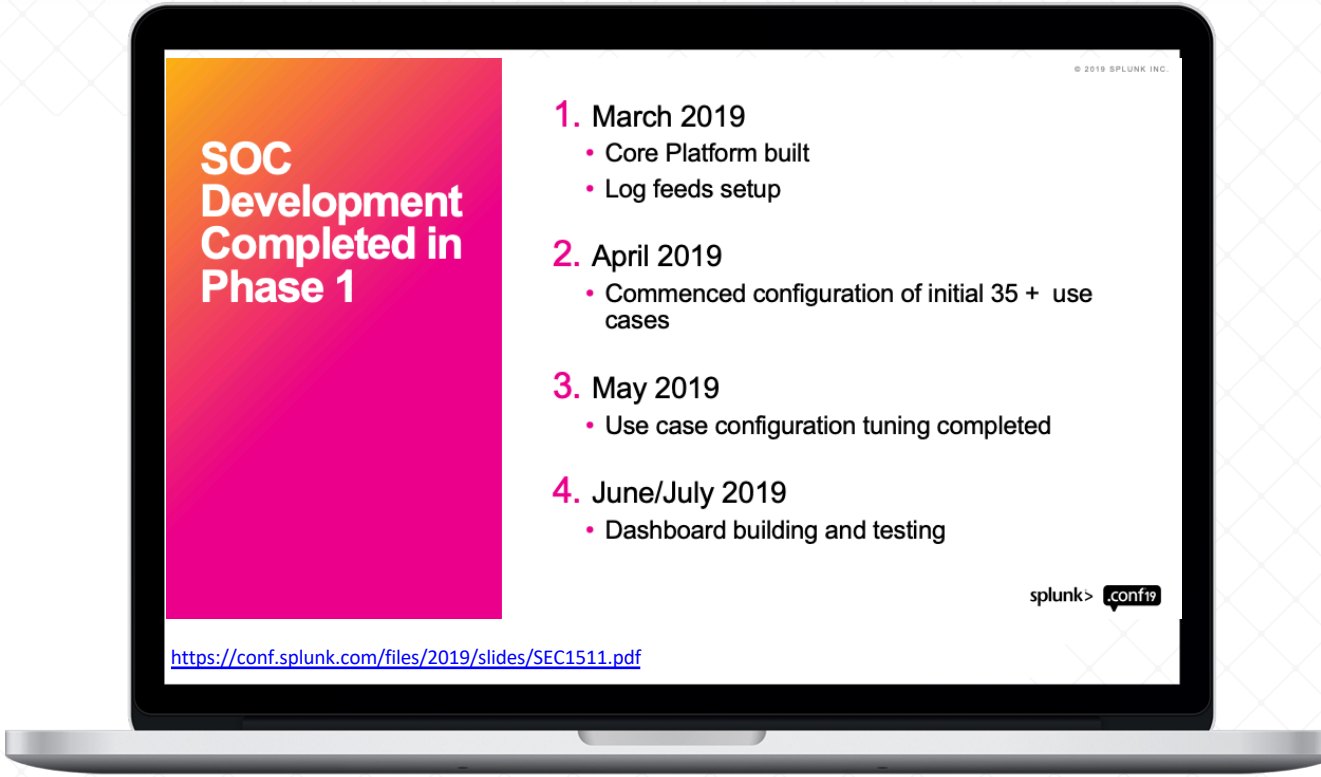


No upfront investment in resources like hardware, software and people

Johnson Matthey



Johnson Matthey



4 secrets

Splunk Customers Building Modern SecOps

SOC in the Cloud

Agility in Detection Engineering

Multi Cloud Services Monitoring

Embedded in DevOps

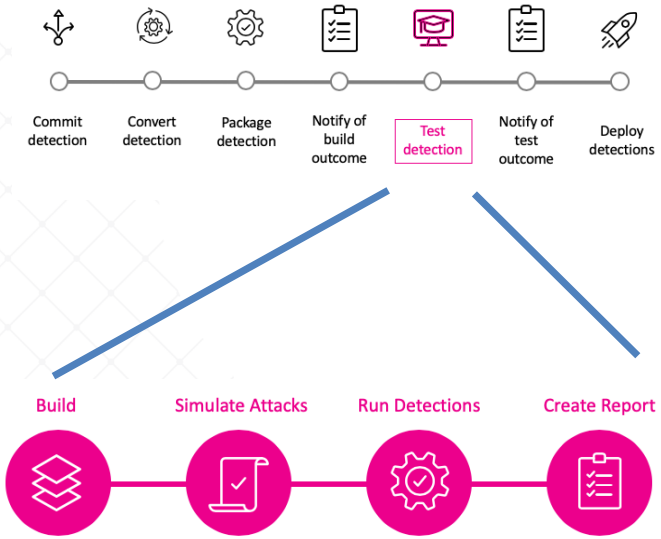


DevOps (CI / CD) Principles Within The SOC

Detection Engineering

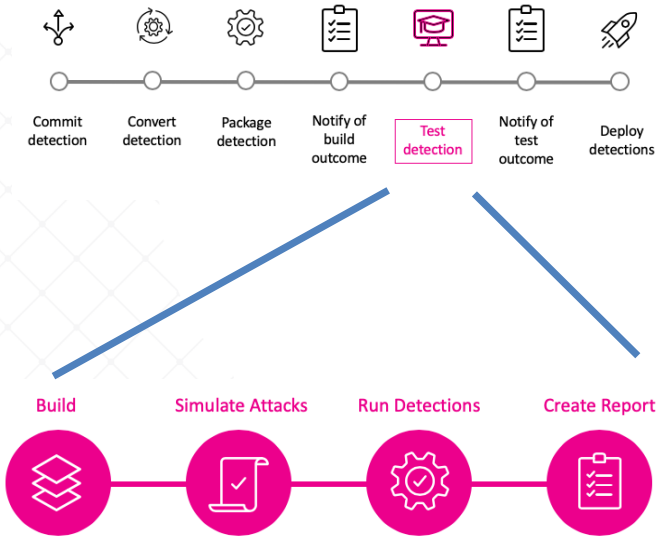
How do you know your MITRE (Cloud) ATT&CK detections work?

Agile Detection Engineering



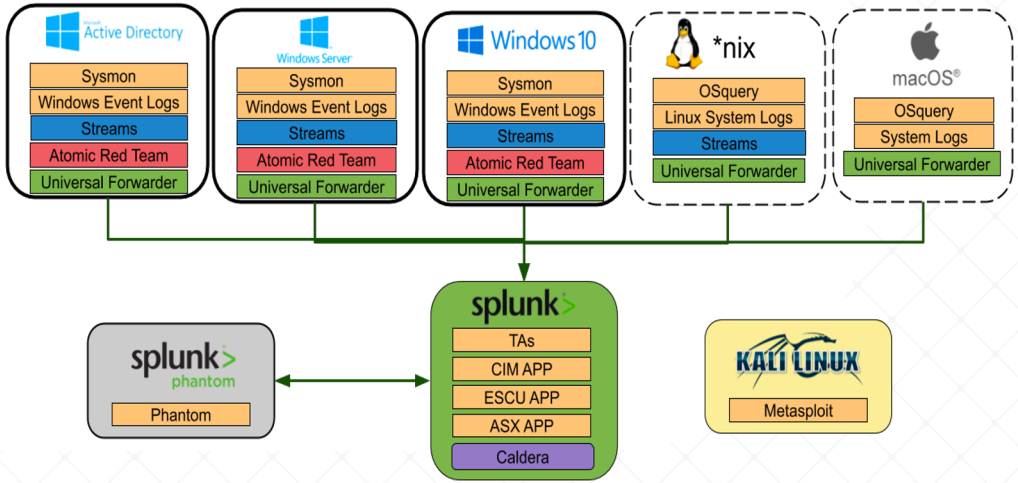
How do you know your MITRE (Cloud) ATT&CK detections work?

Agile Detection Engineering



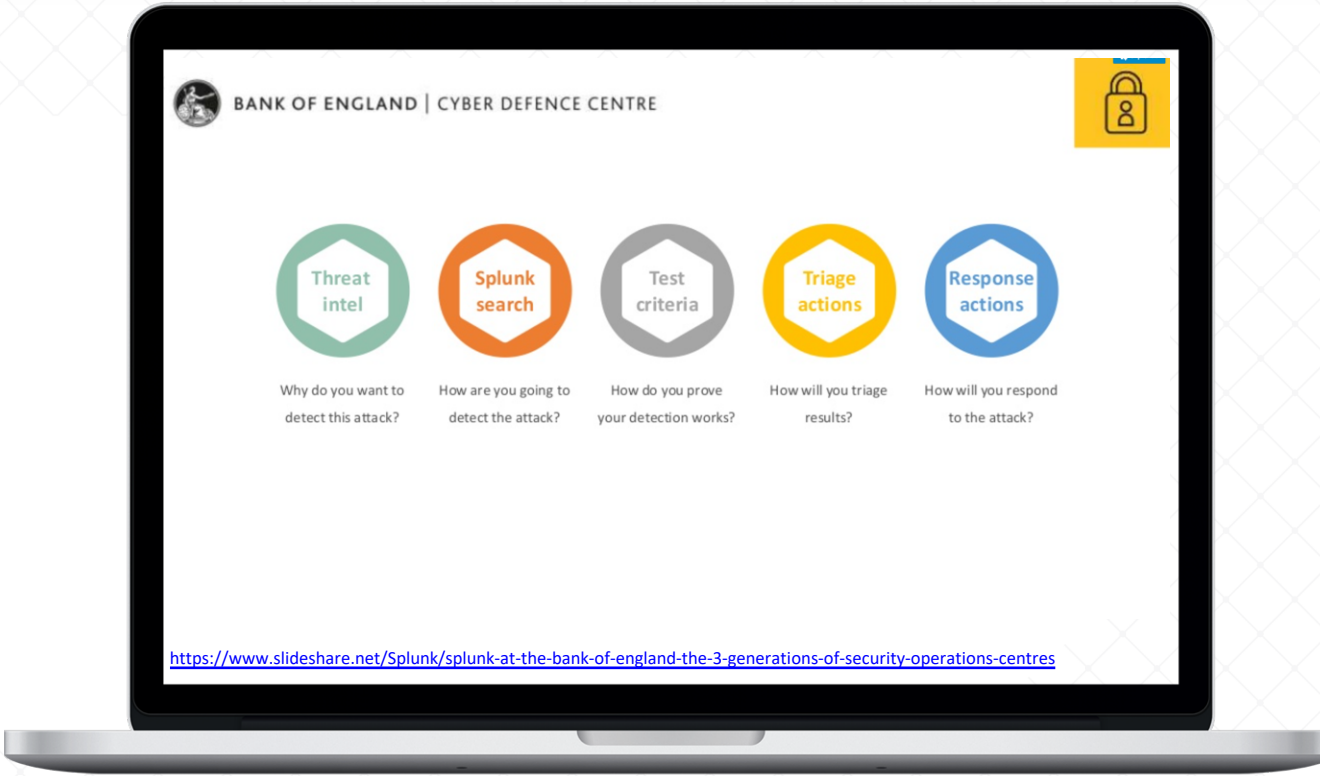
- Splunk Attack Range (Open Source)

Test Detections Including Adversary Simulation

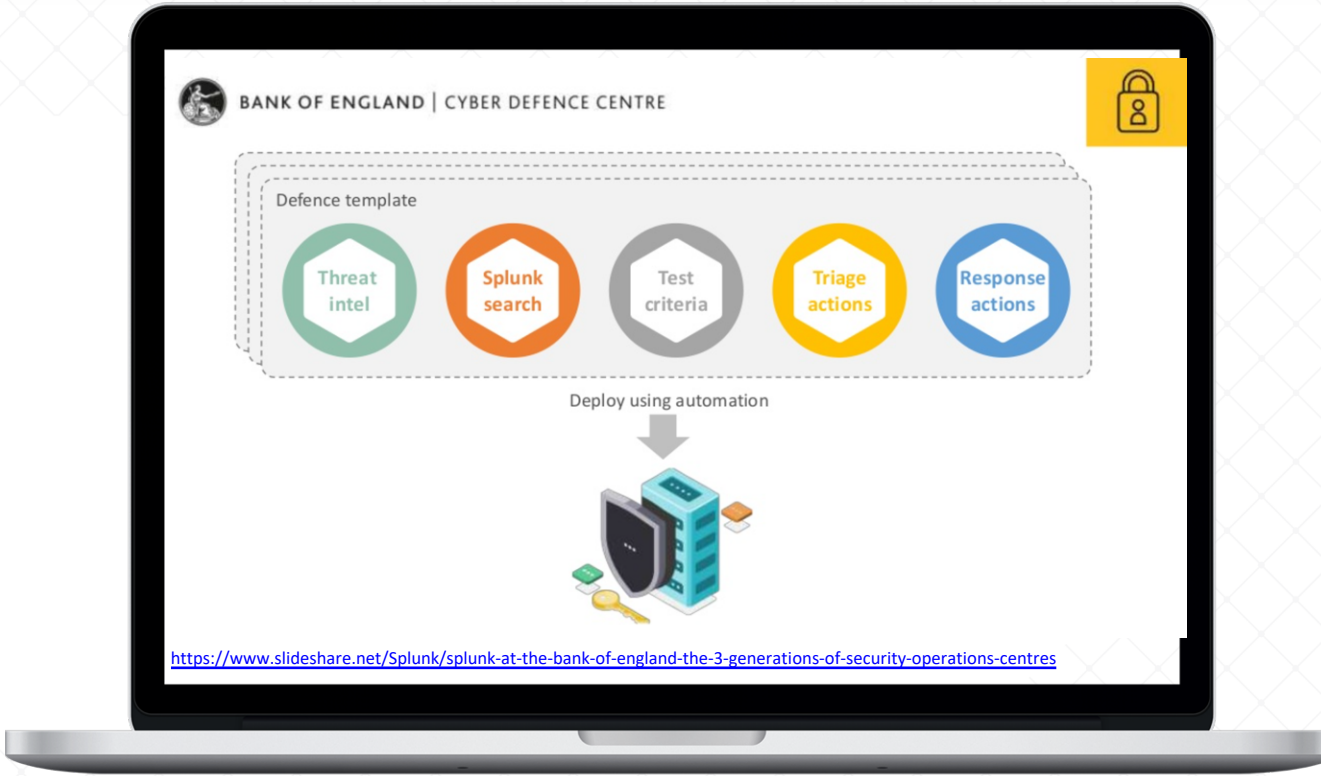


Git: https://github.com/splunk/attack_range
Whitepaper: Using Splunk Attack Range to Simulate and Collect Attack Data:
https://www.splunk.com/en_us/form/using-splunk-attack-range-to-simulate-and-collect-attack-data.html

Bank Of England



Bank Of England



4 secrets

Splunk Customers Building Modern SecOps

SOC in the Cloud

Agility in Detection Engineering

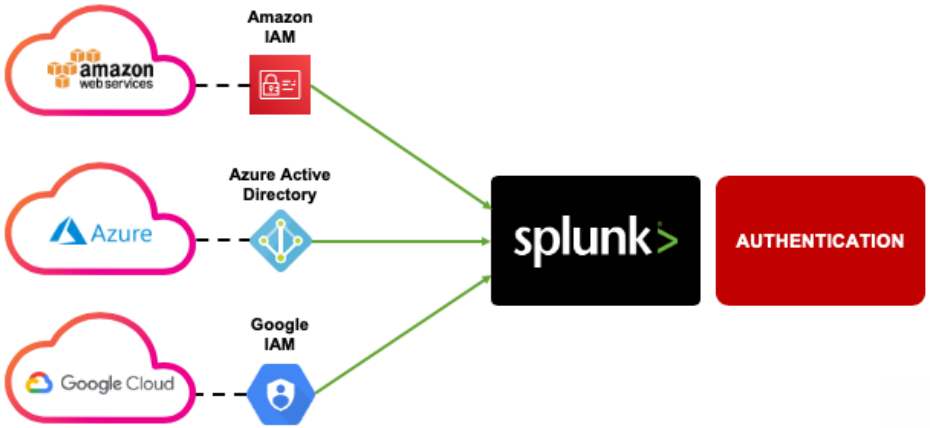
Multi Cloud Services Monitoring

Embedded in DevOps



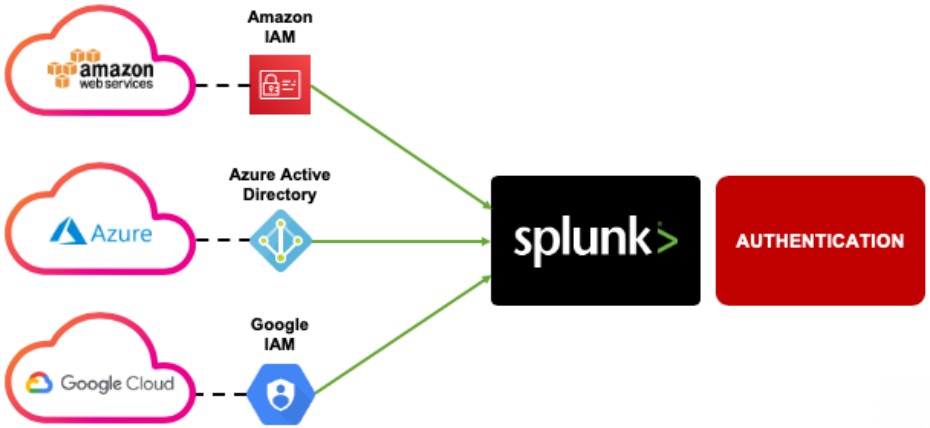
Splunk Multi-Cloud Monitoring Example: Auth

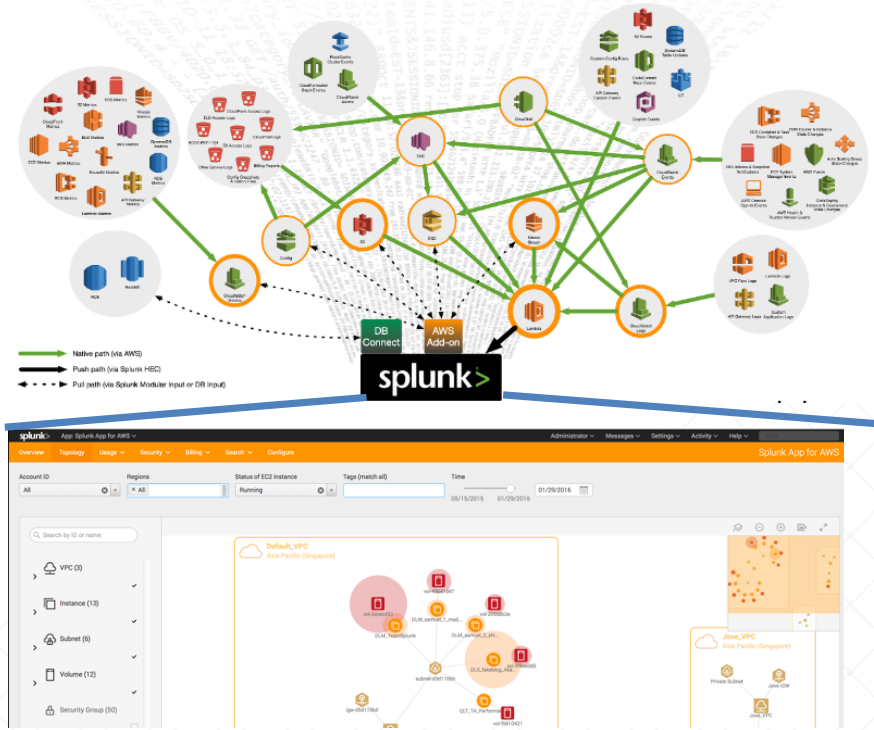
Highlight user behavior across cloud instances



Splunk Multi-Cloud Monitoring Example: Auth

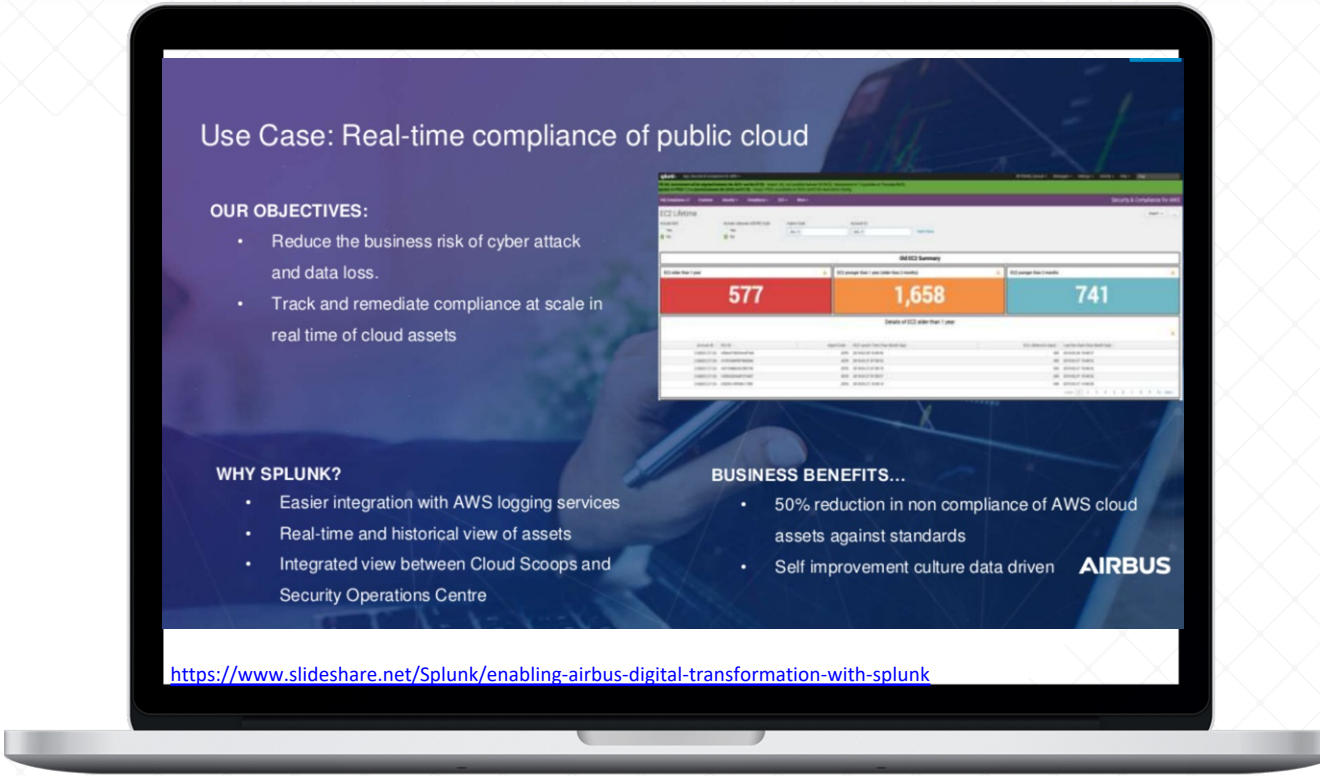
Highlight user behavior across cloud instances





amazon web services

Airbus



https://www.slideshare.net/Splunk/enabling-airbus-digital-transformation-with-splunk

4 secrets

Splunk Customers Building Modern SecOps

SOC in the Cloud

Agility in Detection Engineering

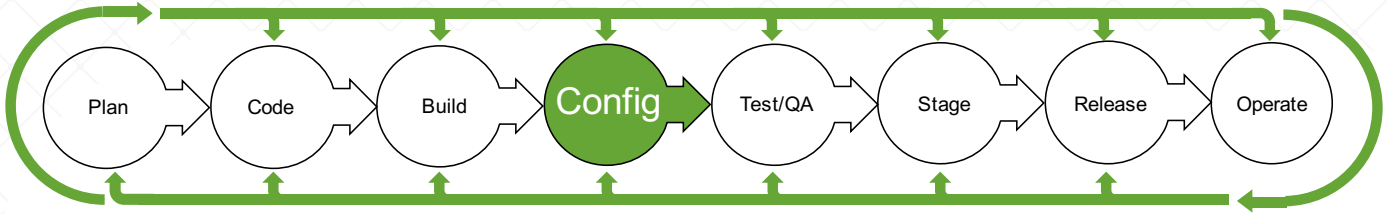
Multi Cloud Services Monitoring

Embedded in DevOps



(ISC)² WEBINARS SECURITY BRIEFINGS

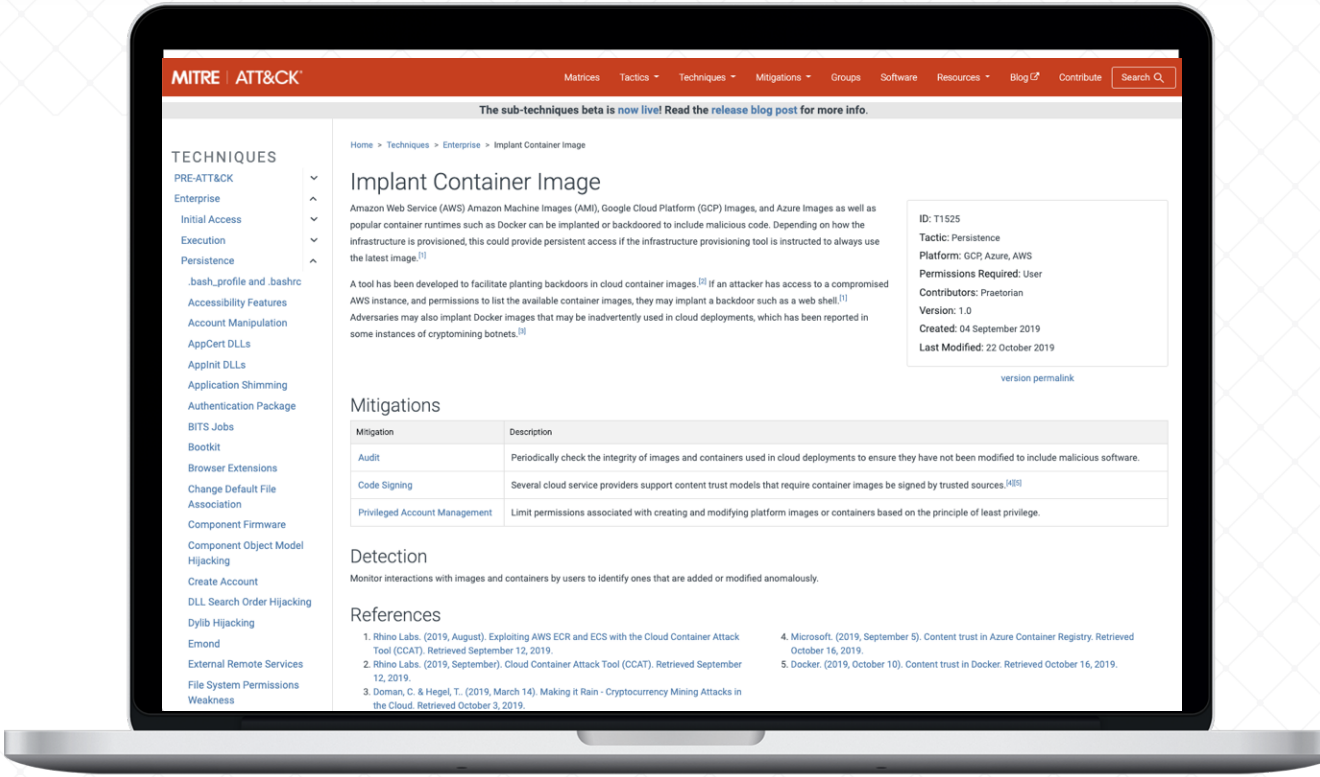
DevSecOps: Real-time Risk Scoring



- **Ensure use of "known good images" and/or configuration code**
  - …and track by user ID for audit compliance
- Audit and report on configuration drift from staging to production
- Audit and report on manual configuration activity on staging or production
- Audit deployment instance configurations
  - ..and include any diffs in test system

Detecting Implant Container Image

- MITRE Cloud ATT&CK T1525



https://attack.mitre.org/techniques/T1525/

Detecting Implant Container Image

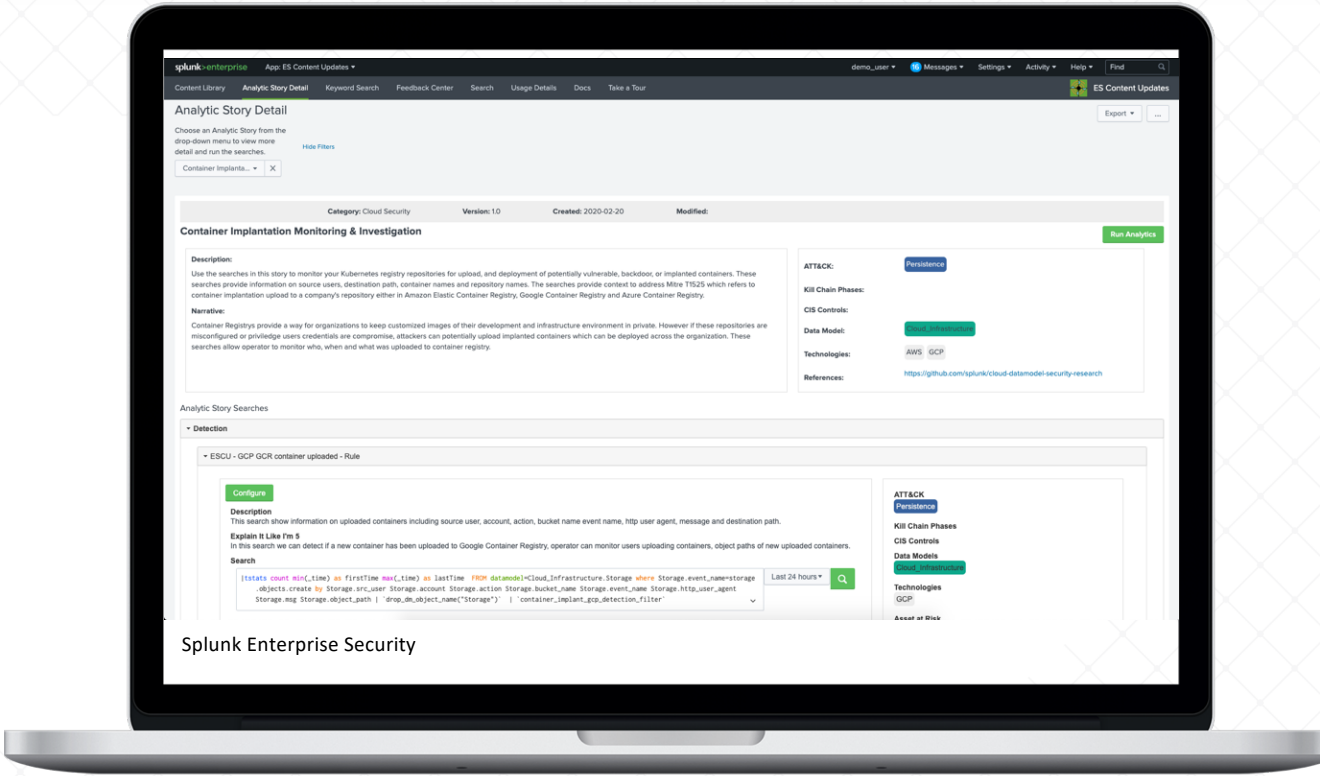
- MITRE Cloud ATT&CK T1525



https://www.youtube.com/watch?v=PgzNib37g0M&feature=youtu.be

Detecting Implant Container Image

- MITRE Cloud ATT&CK T1525



Splunk Enterprise Security

4 secrets

Splunk Customers Building Modern SecOps

SOC in the Cloud

Agility in Detection Engineering

Multi Cloud Services Monitoring

Embedded in DevOps



Taking data to everything

Splunk helps organizations leverage their data to reduce operational complexity and securely enable the shift to the cloud.

Investigate



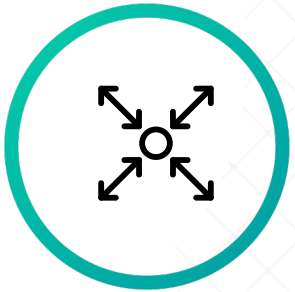
Monitor



Analyze



Act



Thank You

Please leave your feedback & comments in the “Rate This” tab



Thank you for attending this webinar!

Stay Connected!

Update your email preferences to receive news about upcoming (ISC)² webinars, publications & more!

www.isc2.org/connect

