In the Design and Operation of Security Operation Centres

A Comprehensive Approach

Nadhem AlFardan, PhD

Security Solutions Architect

Apr, 2017

Agenda

- Architecture
- Demo
- Methodology
- Predictive Analytics
- Demo

Security Challenges

Changing Business Models

IOE

25%

increase in an organization's cybersecurity risk due to IoE

CLOUD

5-10

times more cloud services are being used than known by IT

Dynamic Threat Landscape

60% data in breaches is stolen in **hours**

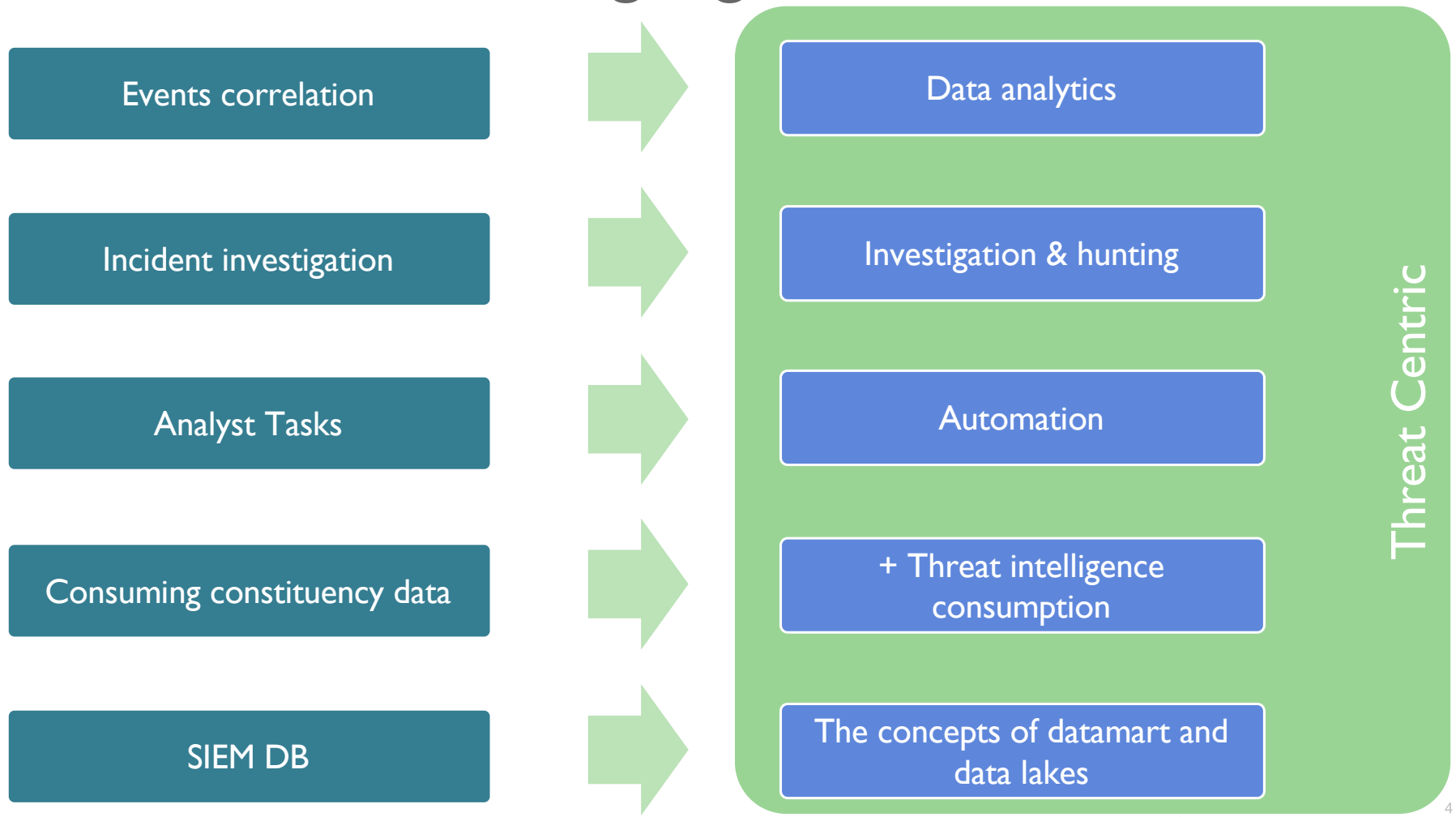
54% of breaches remain undiscovered for **months**

Complexity and Fragmentation

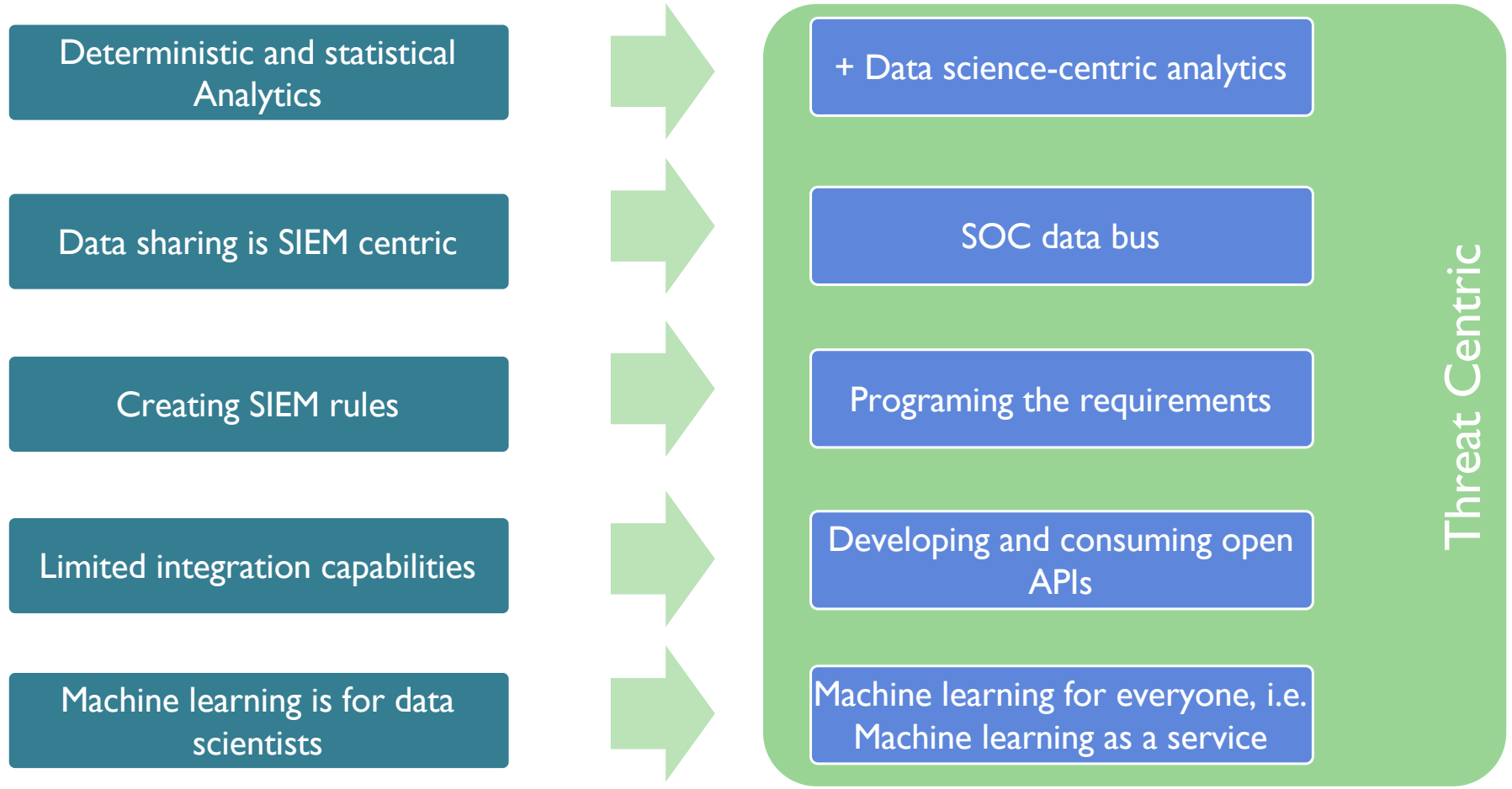
12x Demand for security talent

45 Security vendors for some customers

SOC – What is Changing?

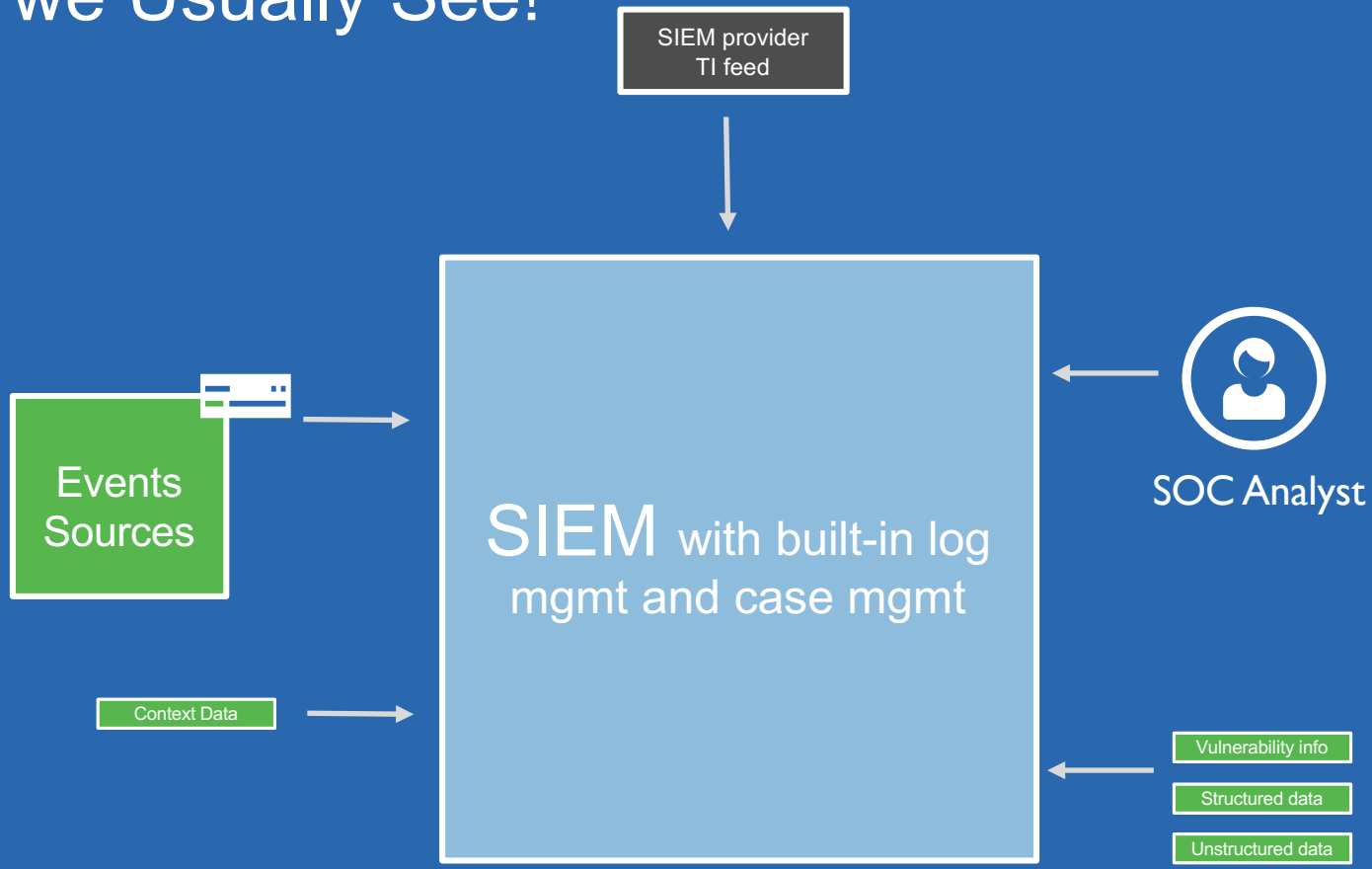


SOC – What is Changing?

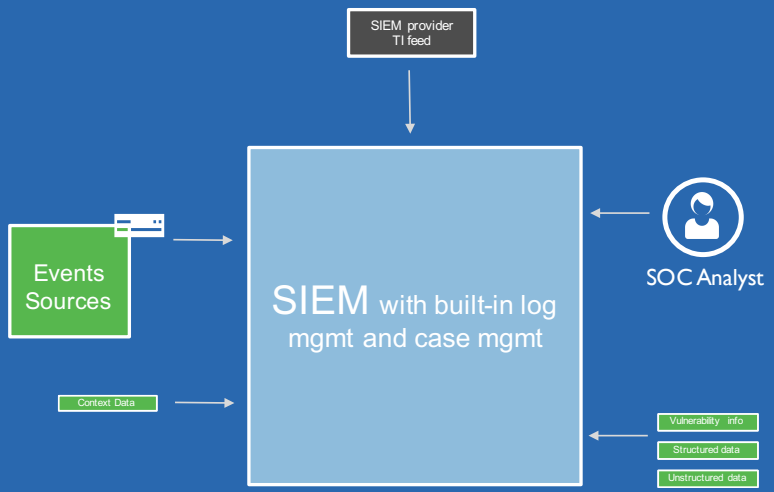


What *we* see

What we Usually See!



Then a Number of Artifacts are Attached



Technology
Design and Build

Policies

Standard Use
Cases

Processes

Support

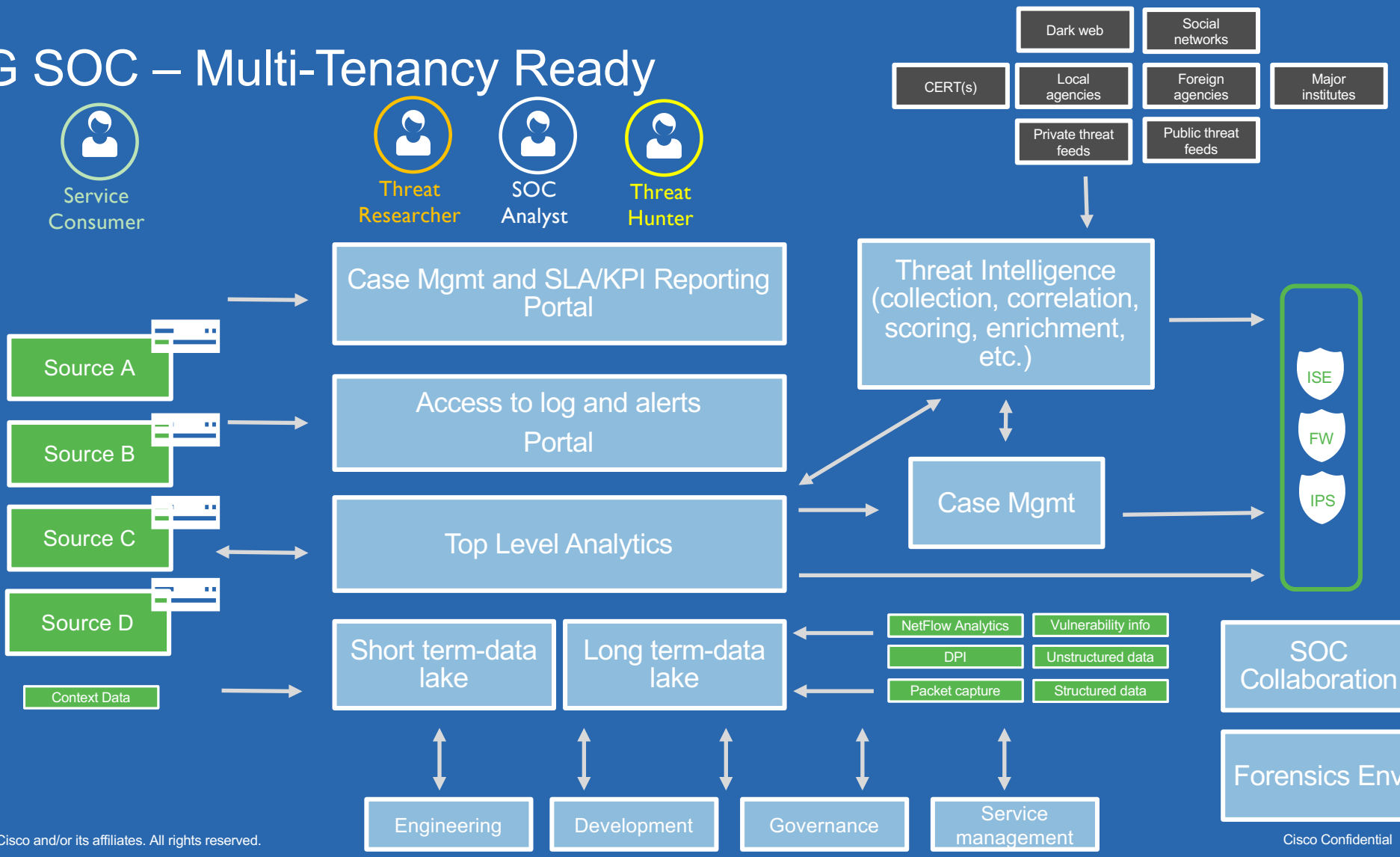
Procedures

Operation

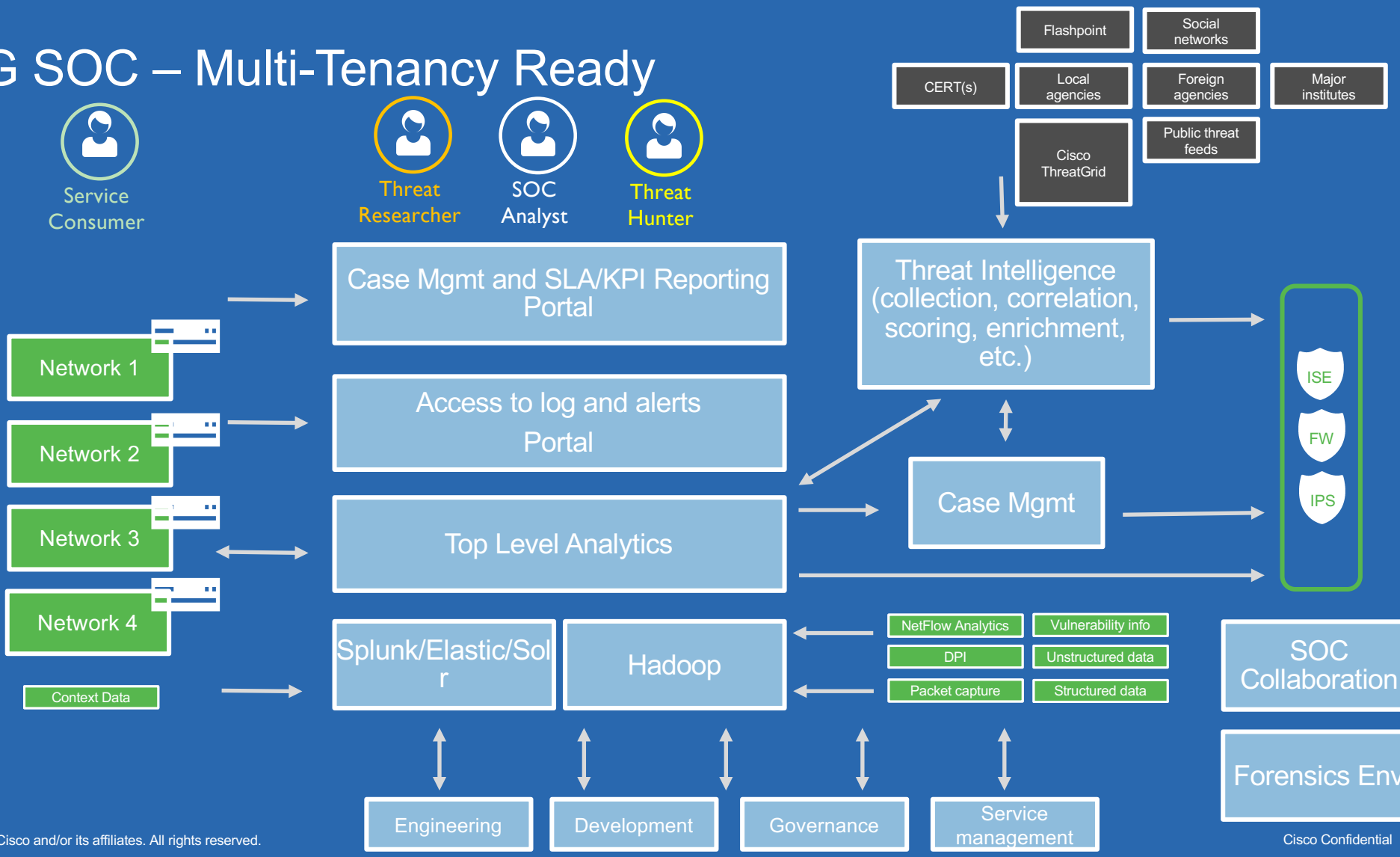
KT

What *we* want to see

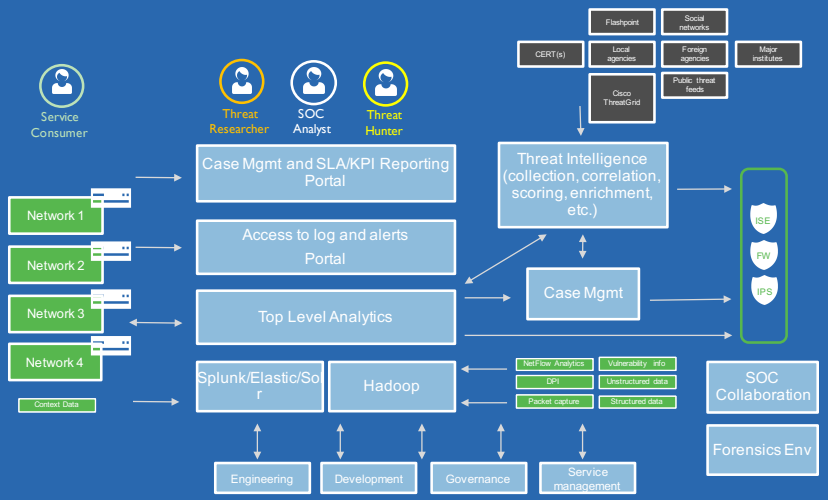
NG SOC – Multi-Tenancy Ready



NG SOC – Multi-Tenancy Ready



Structured Approach



Architecture Principles
Conceptual Architecture
Logical Architecture
Physical Architecture

DESIGN

PLAN

Service Strategy

Service Capabilities Assessment: People Systems Network Tools Processes

High Level Services Architecture

Services Catalogue Design

- Log Management Service
- Security Monitoring Service
- Incident Response Service
- Threat Intelligence and Research Service
- Vulnerability Management Service
- Threat Hunting
- Big Data Analytics
- Active Defense

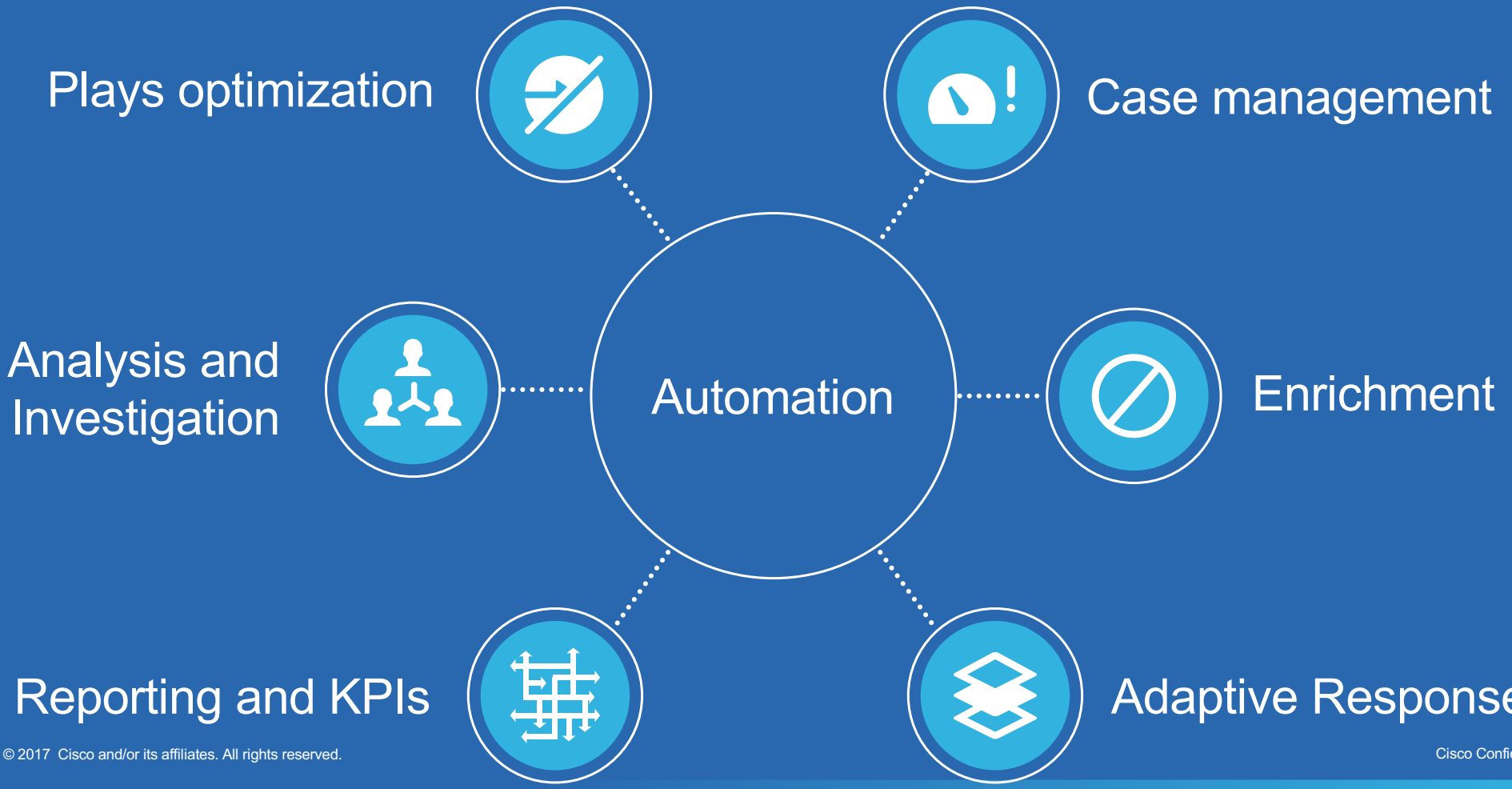
- Sources
- Inputs
- Components
- Outputs
- Procedures
- Processes
- KPIs/KRIs
- SLAs
- Pricing

- IR Program
- Emergency IR

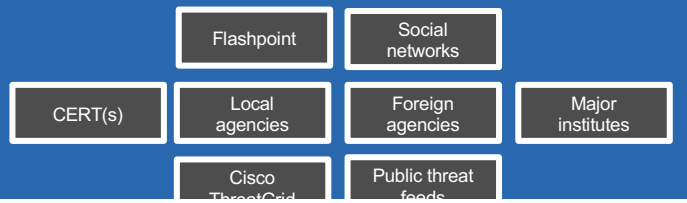
Threat Modelling

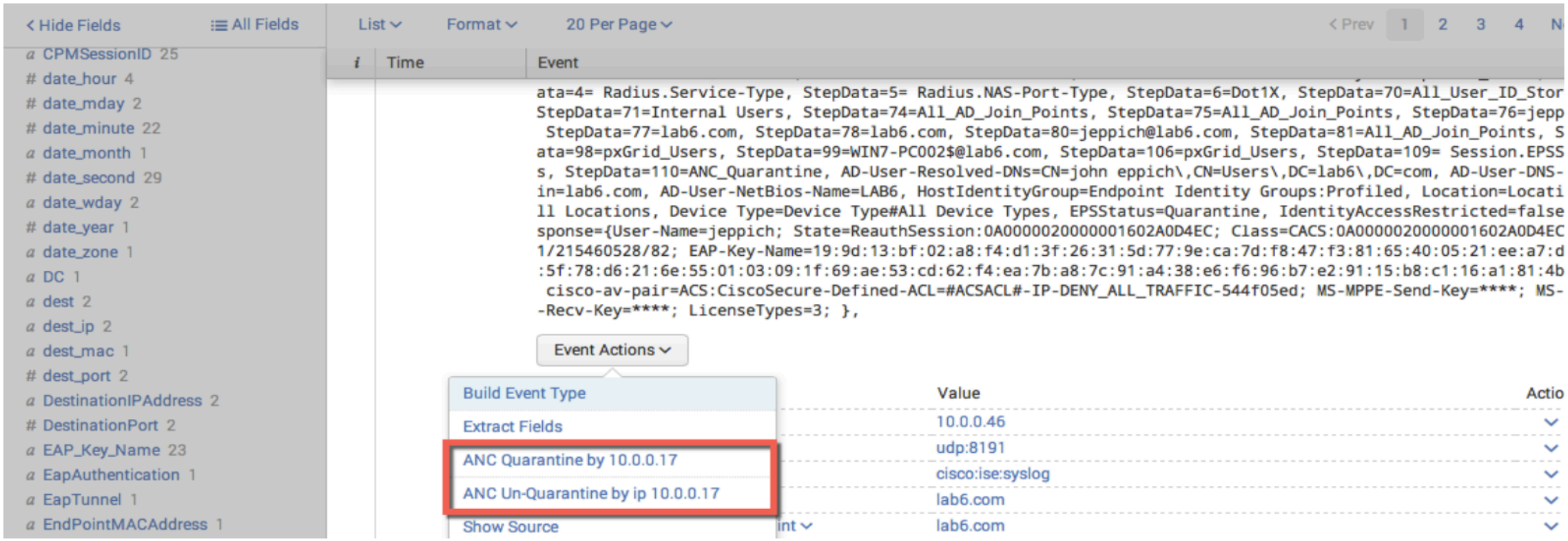
- Use Cases
- Plays

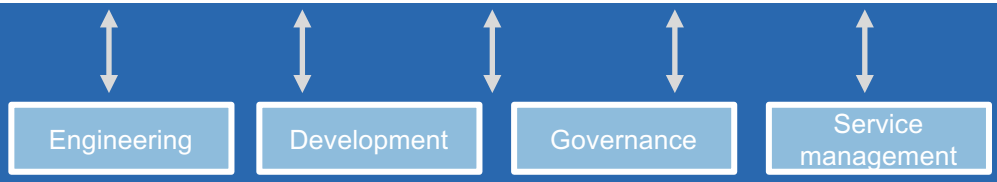
Automating the SOC Tasks



Mapping Technologies and Products







Confluence

Flashpoint | Social networks

20 Per Page ⌄ < Prev 1 2 3 4 5 6 7 8 9 ...

nt

```
.9.109.61 - - [05/Jan/2017:06:39:16] "GET /product.screen?productId=WC-SH-A02&JSESSIONID=SD0SL6FF7ADFF4953 HTTP 1.1" 200 3878 "http://www
com" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 349
```

Event Actions ⌄

	Field	Value	Actions
ected	✓ host ⌄	ip-10-0-1-207.ec2.internal	⌄
	✓ source ⌄	/tmp/splunk-testdata/test.log	⌄
	✓ sourcetype ⌄	TQDemoData	⌄
nt	JSESSIONID ⌄	SD0SL6FF7ADFF4953	⌄
	dest_ip ⌄	68.9.109.61	⌄
	field1 ⌄	68.9.109.61	
	field10 ⌄	349	
	field2 ⌄	-	
	field3 ⌄	-	⌄
	field4 ⌄	[05/Jan/2017:06:39:16]	⌄
	field5 ⌄	GET /product.screen?productId=WC-SH-A02&JSESSIONID=SD0SL6FF7ADFF4953 HTTP 1.1	⌄
	field6 ⌄	200	⌄
	field7 ⌄	3878	⌄
	field8 ⌄	http://www.google.com	⌄

Edit Tags

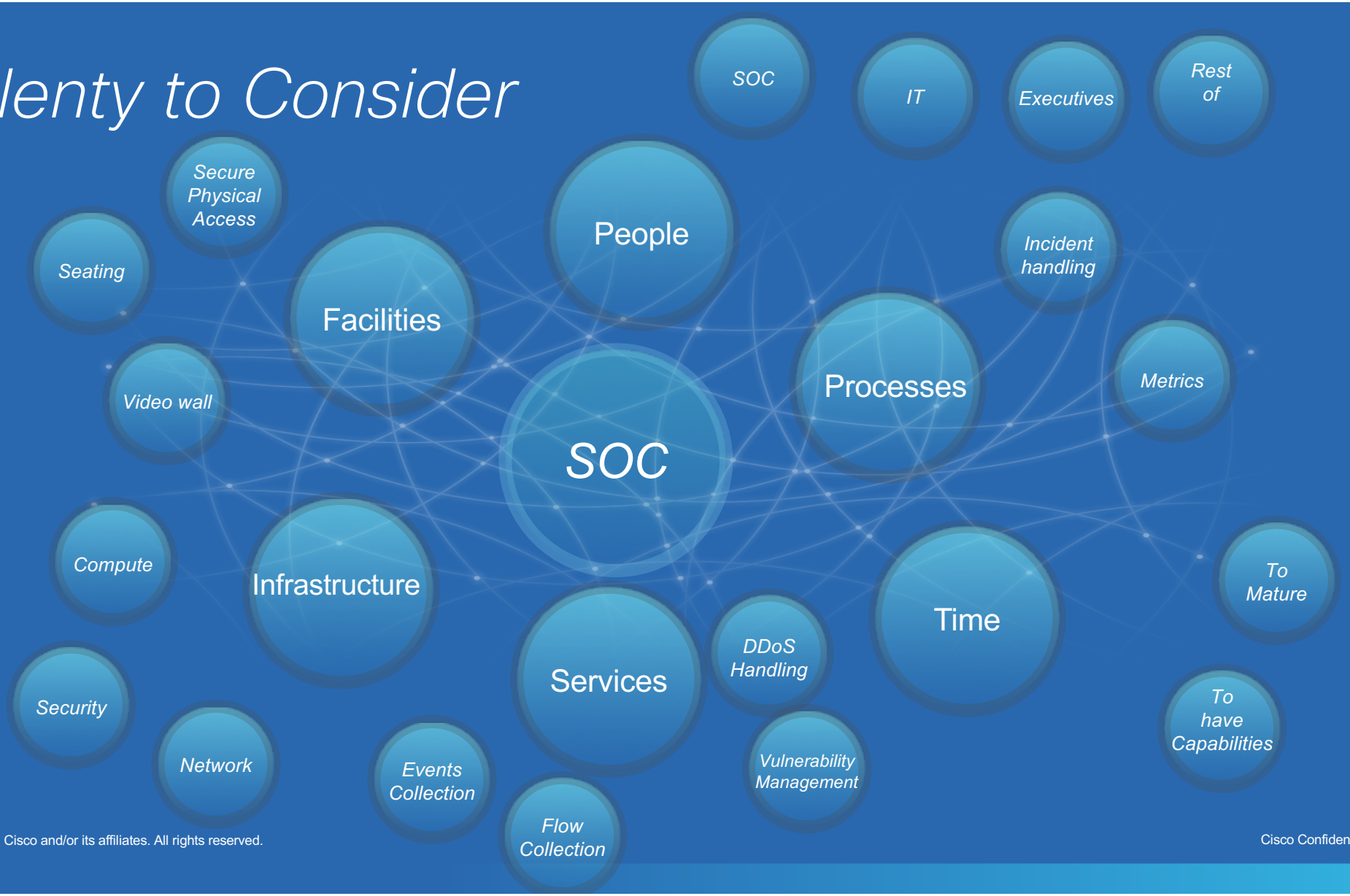
ThreatQ: Add IP Indicator

Engineering | Development | Governance | management

Demo

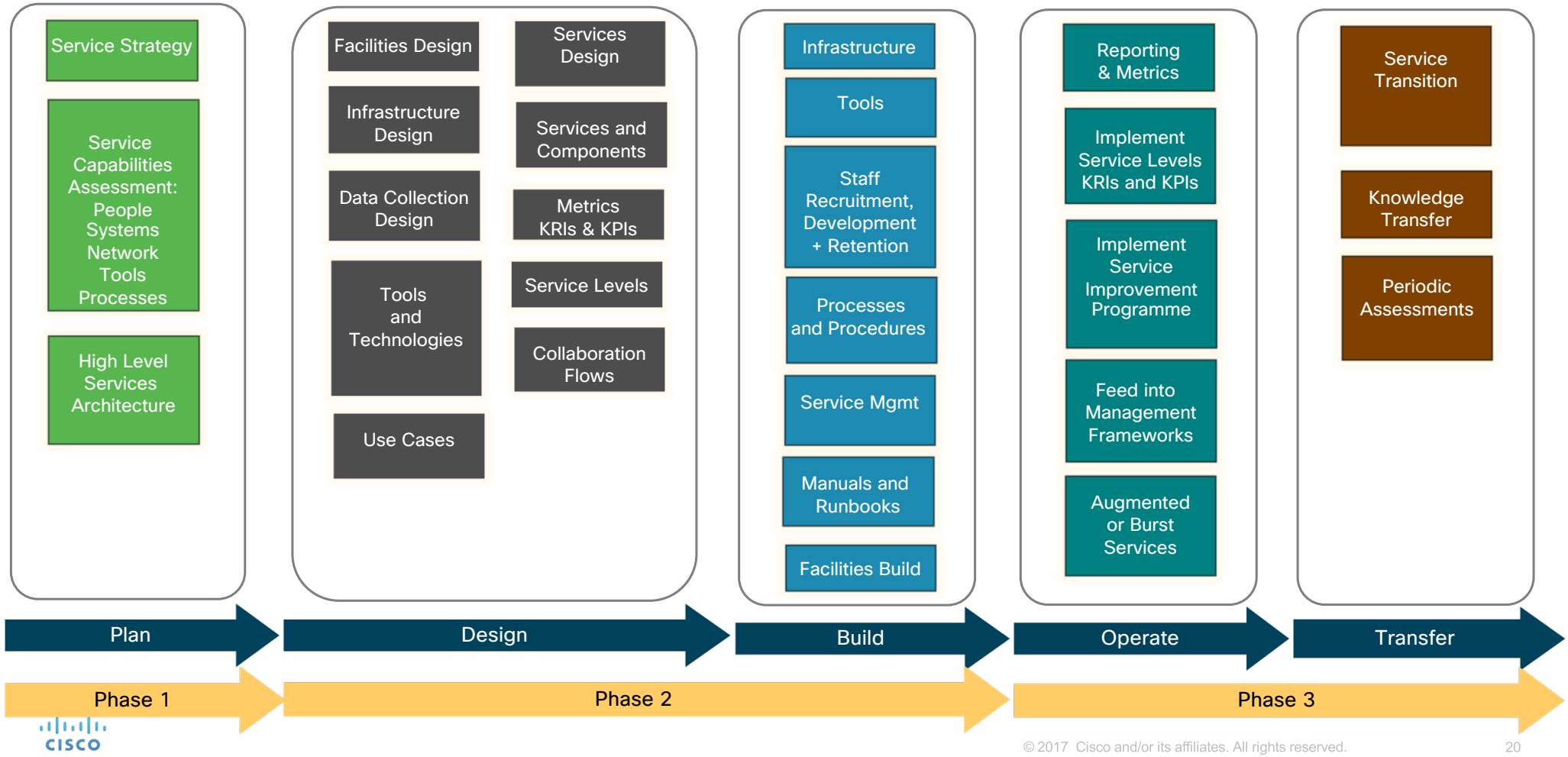
How to reach there?

Plenty to Consider



Establishing a SOC – A Phased Methodology

Cisco's Phased Methodology



A typical SOC service catalogue…

Service Management

- Business Service Management
- IT Service Management
- Operations Management
- HR Management

Security Incident Response

- Cyber Security Monitoring
- Cyber Security Investigation and Escalation
- Cyber Threat Hunting
- Cyber Security Incident Remediation
- Post-Incident Analysis

Cyber Security Analytics

- Security Data Management
- Security Analytics

Platforms and Content

- Platform Development
- Platform Engineering
- Platform Operations
- Content Management

Cyber Threat Intelligence

- Intelligence Collection, Evaluation and Collation
- Intelligence Analysis
- Intelligence Production
- Intelligence Reporting and Communications

… but some SOCs can include a wider range of services

Service Management

- Security Service Provider Management
- Cloud Security Services Management
- Vendor Management

Cyber Security Controls Management

- IAM
- Boundary control
- System and data integrity protections
- Cryptographic services
- Application security
- Others

Compliance Management

- Policy and standards development

Compliance scanning, validation and escalation

Compliance reporting

Audit and compliance support

Training and Testing

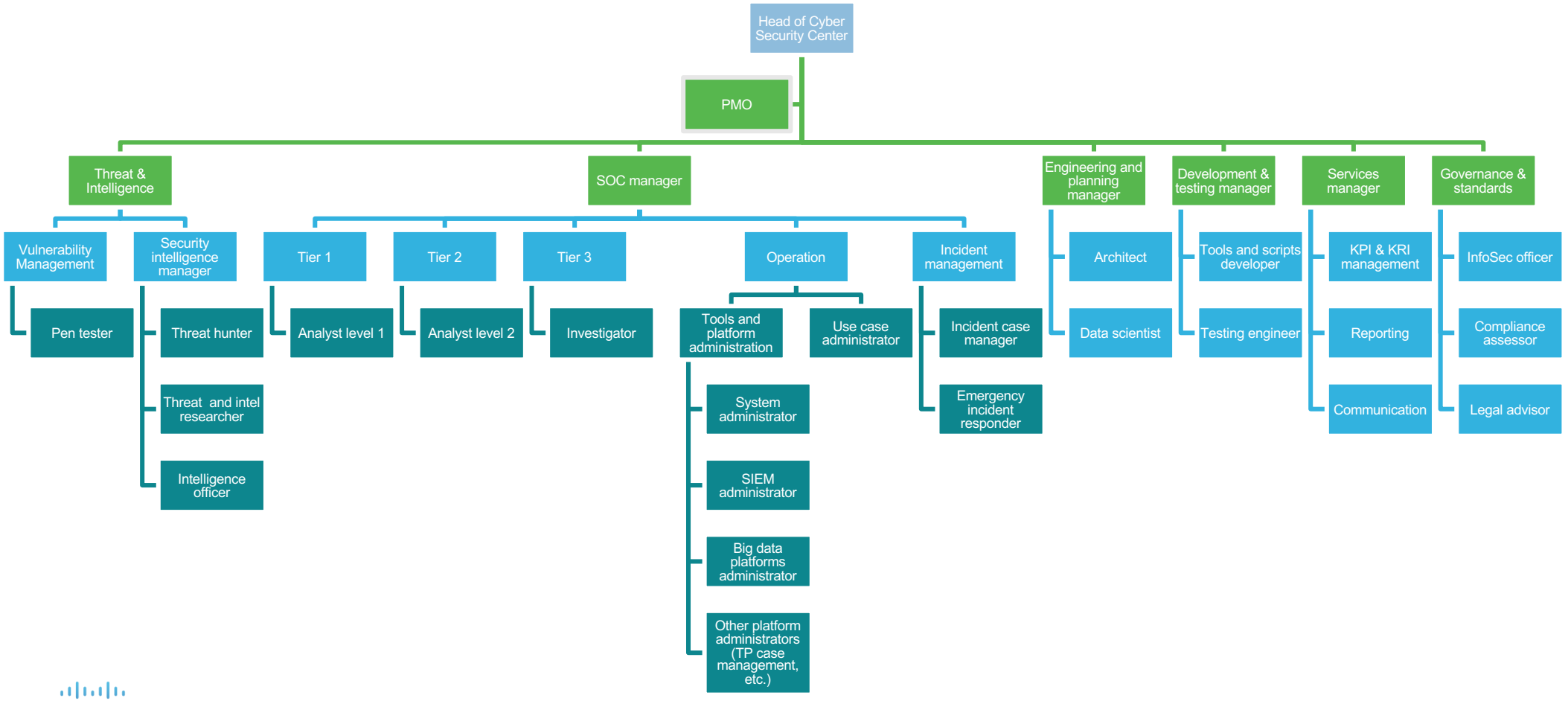
- Training Development
- Training Delivery
- Purple team and other testing services

Vulnerability Management

- Vulnerability Intelligence
- Vulnerability Scanning
- Vulnerability Escalation
- Vulnerability Remediation

The Team

Team Structure



Predictive Analytics

Machine learning (ML) is the science of getting computers to act without being explicitly programmed!

Andrew Ng, Associate Professor, Stanford University

Feature = numeric representation of raw data

Analytics Methods

Service Differentiator

	 Deterministic Rules-Based Analytics (DRB)	 Statistical Rules-Based Analytics (SRB)	 Data Science-Centric Analytics (DSC)
Examples	• Signature based detection • Alerting when predefined thresholds are exceeded • Identification of outbound communication to known C&C domains or IPs	• Unusual system changes such as from non-standard administrator accounts or bulk changes at unexpected times • Highlight abnormal levels of data export from critical systems	• Automated categorization of data, such identifying classified documents • Alert on suspicious activity gathering around a high value asset. For example, a classified asset is injected with malware, then logged into from a foreign IP, then proceeds to port scan the internal network
Characteristics	• Mature method of analysis • Covers a majority of known threats • Fast detection	• Anomaly detection based on historical context (i.e. highlighting atypical behavior) • Dynamic outlier detection independent of predefined thresholds	• Adaptive learning to automatically tune system for useful alerts • Clustering information around specific attributes to identify behavioral anomalies • Extrapolation of future threat behavior to reduce time to detect
Effort Required	• Creation of rules library based on current known threats • Ongoing maintenance and tuning of rules library	• Manual tuning of statistical parameters to reduce false positives and false negatives • Intimate knowledge of use cases and environmental data to create statistical models	• Automated tuning of model parameters to reduce false positives and false negatives • Broad understanding of use cases and intimate understanding of environmental data

DBR – Examp

Deterministic Rules-Based Analytics (DRB)

- Signature based detection
- Alerting when predefined thresholds are exceeded
- Identification of outbound communication to known C&C domains or IPs

- Mature method of analysis
- Covers a majority of known threats
- Fast detection

- Creation of rules library based on current known threats
- Ongoing maintenance and tuning of rules library

Top Notable Events

rule_name	sparkline	count
Threat Activity Detected		427
Default Account Activity Detected		284
Host With Multiple Infections		189
Geographically Improbable Access Detected		119
High Or Critical Priority Host With Malware Detected		93
Excessive Failed Logins		90
Insecure Or Cleartext Authentication Detected		31

Correlation Search

Search Name* Excessive Failed Logins

Application Context SA-AccessProtection

Description Detects excessive number of failed login attempts

Describes what kind of issues this search is intended to detect

Search* | datamodel "Authentication" "Failed_Authentication" search | stats values(Authentication.tag) as "tag",dc(Authentication.user)
"Authentication.app","Authentication.src" | rename "Authentication.app" as "app","Authentication.src" as "src" | where 'count'>=6

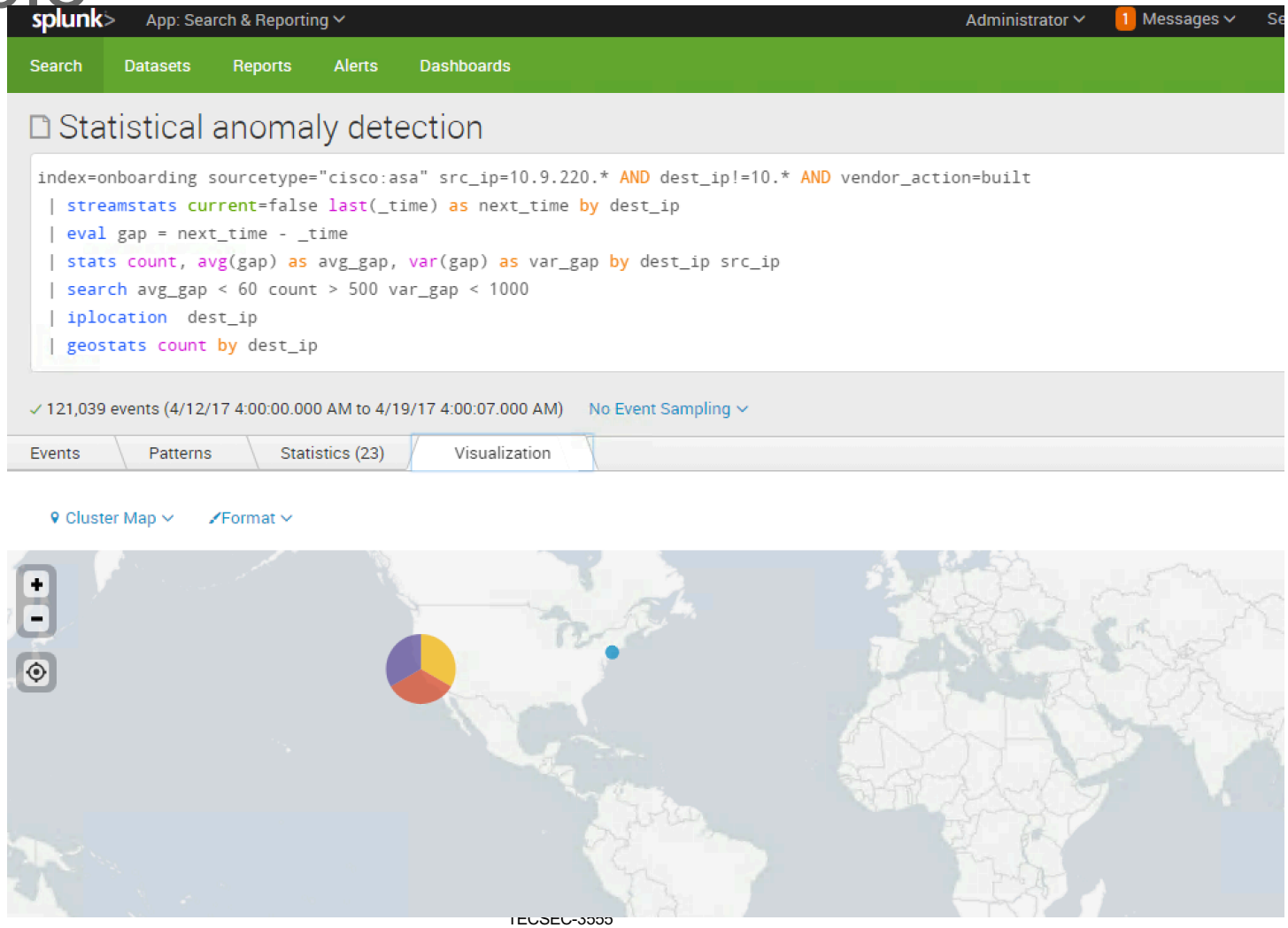
SBR – Example

Statistical Rules-Based Analytics (SRB)

- Unusual system changes such as from non-standard administrator accounts or bulk changes at unexpected times
- Highlight abnormal levels of data export from critical systems

- Anomaly detection based on historical context (i.e. highlighting atypical behavior)
- Dynamic outlier detection independent of predefined thresholds

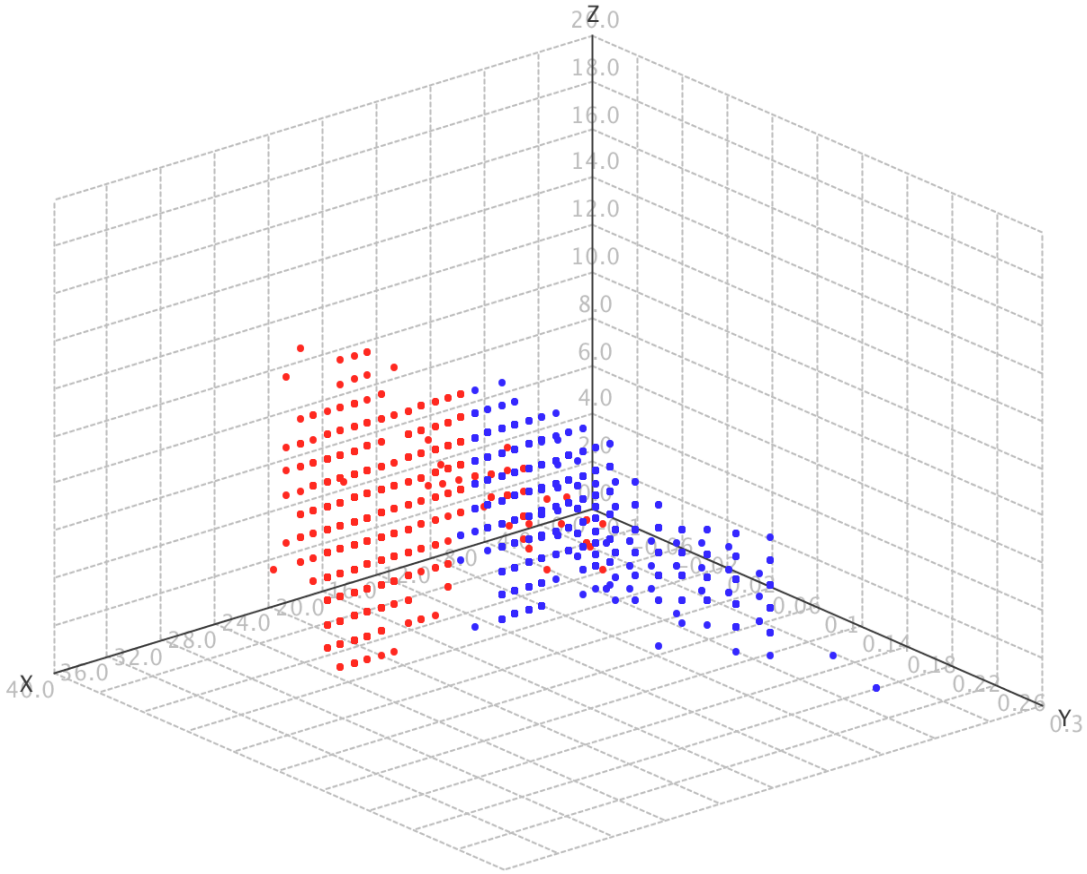
- Manual tuning of statistical parameters to reduce false positives and false negatives
- Intimate knowledge of use cases and environmental data to create statistical models



DSC – Example

Data Science-Centric Analytics (DSC)

- Automated categorization of data, such identifying classified documents
- Alert on suspicious activity gathering around a high value asset. For example, a classified asset is injected with malware, then logged into from a foreign IP, then proceeds to port scan the internal network
- Adaptive learning to automatically tune system for useful alerts
- Clustering information around specific attributes to identify behavioral anomalies
- Extrapolation of future threat behavior to reduce time to detect
- Automated tuning of model parameters to reduce false positives and false negatives
- Broad understanding of use cases and intimate understanding of environmental data



Demo


CISCO