

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



Dynamic Threat Landscape



Complexity and Fragmentation



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

60% data in breaches is stolen in hours

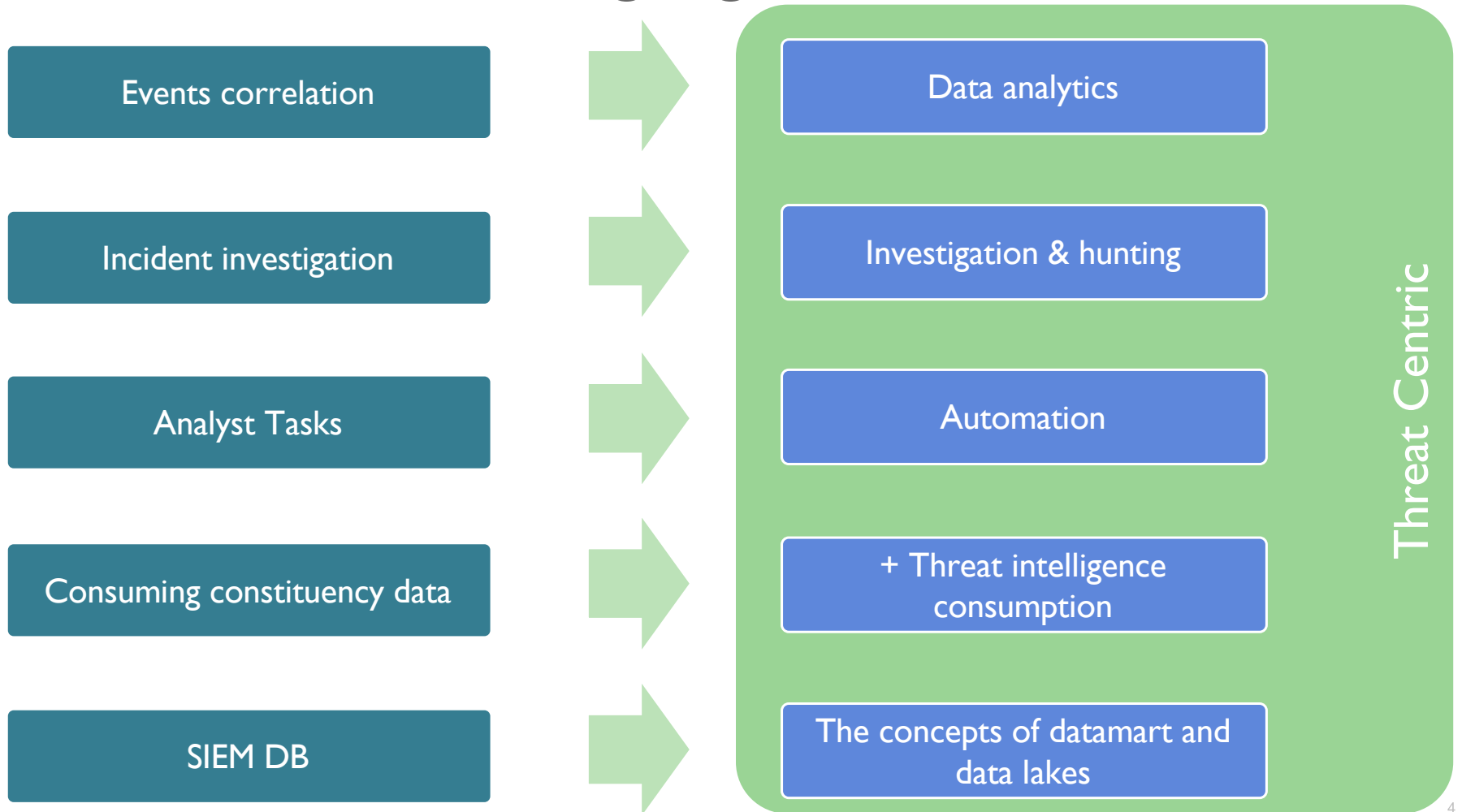


54% of breaches remain undiscovered for months

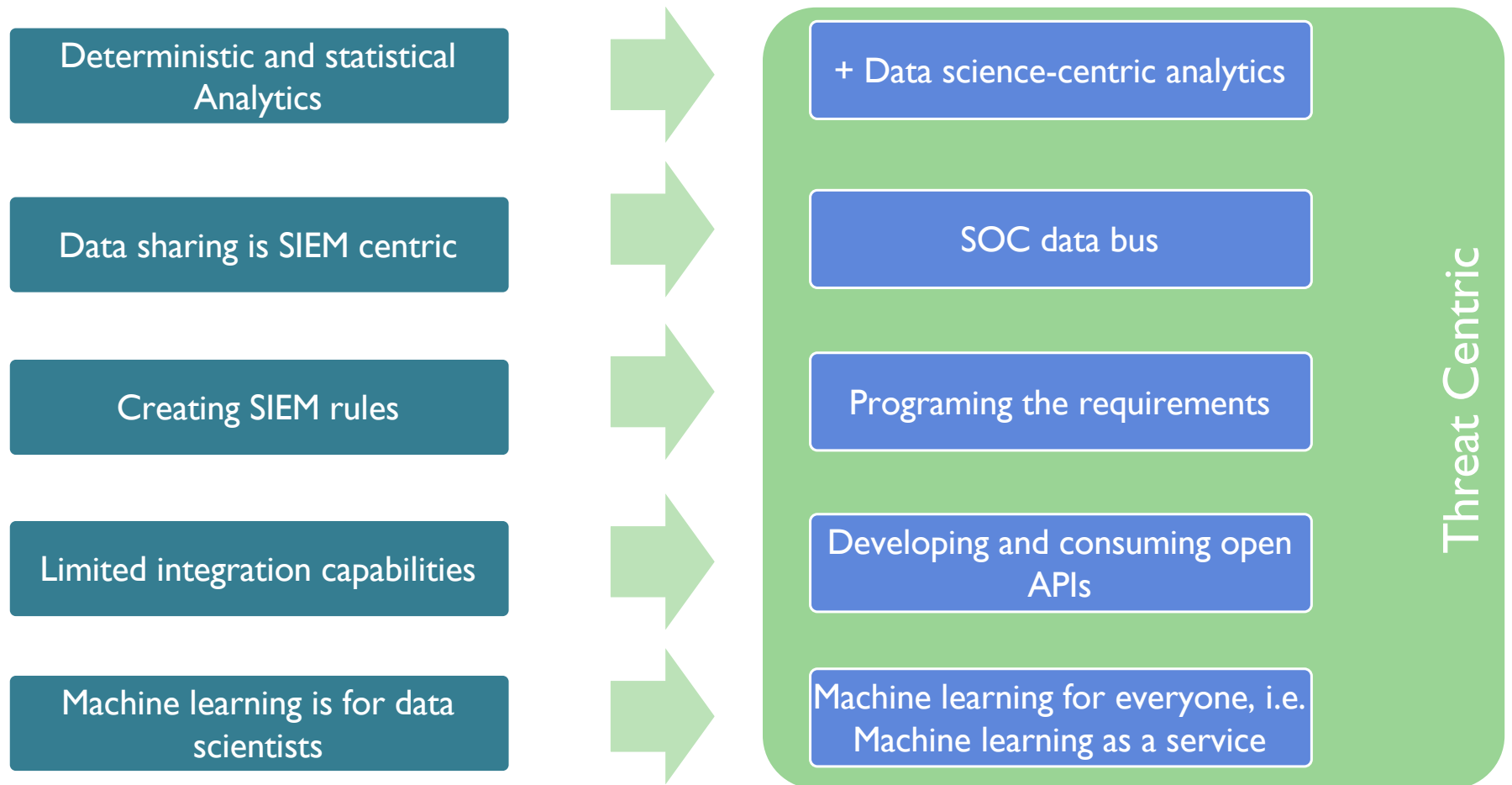
12x Demand for security talent

45 Security vendors for some customers

SOC – What is Changing?

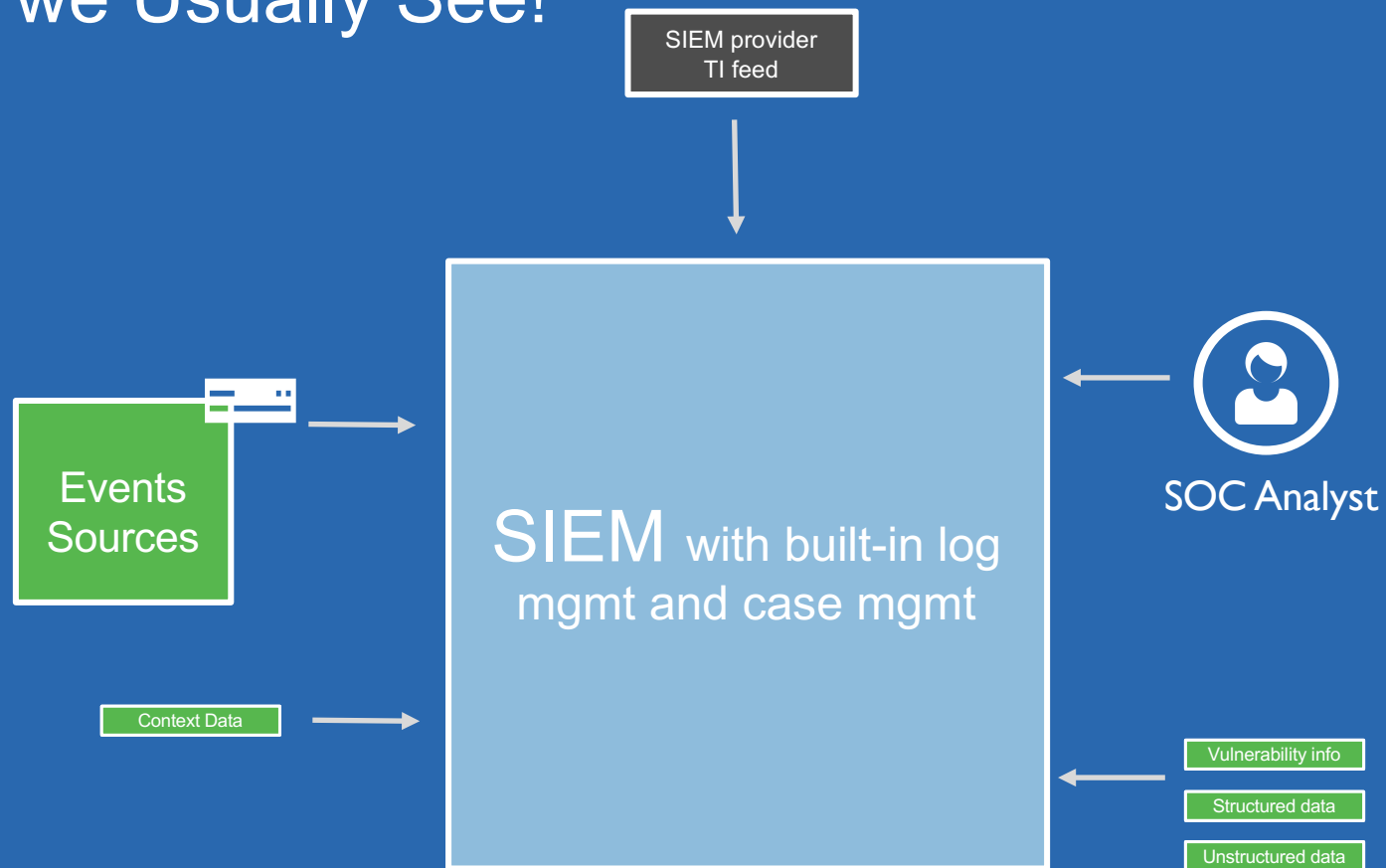


SOC – What is Changing?

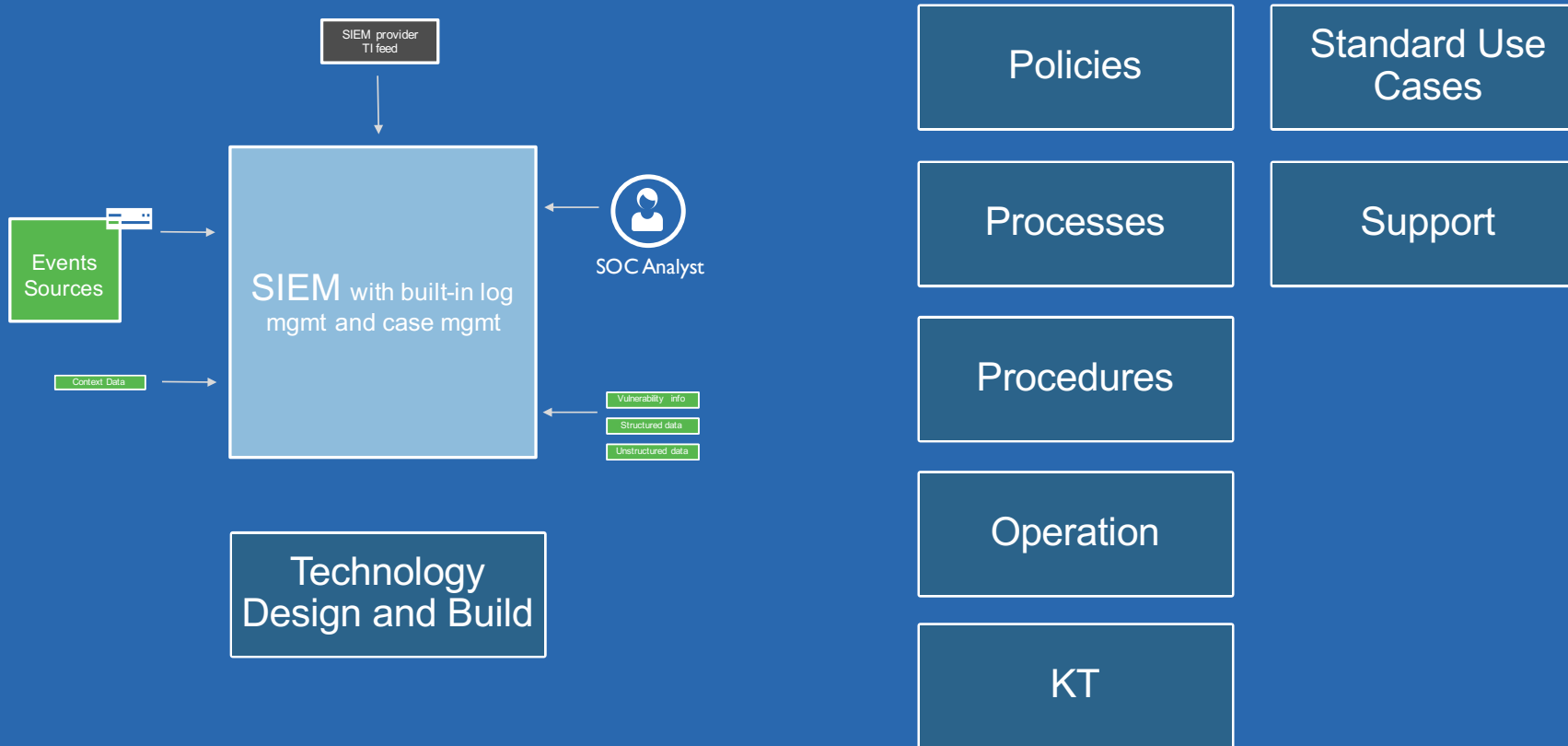


What we see

What we Usually See!

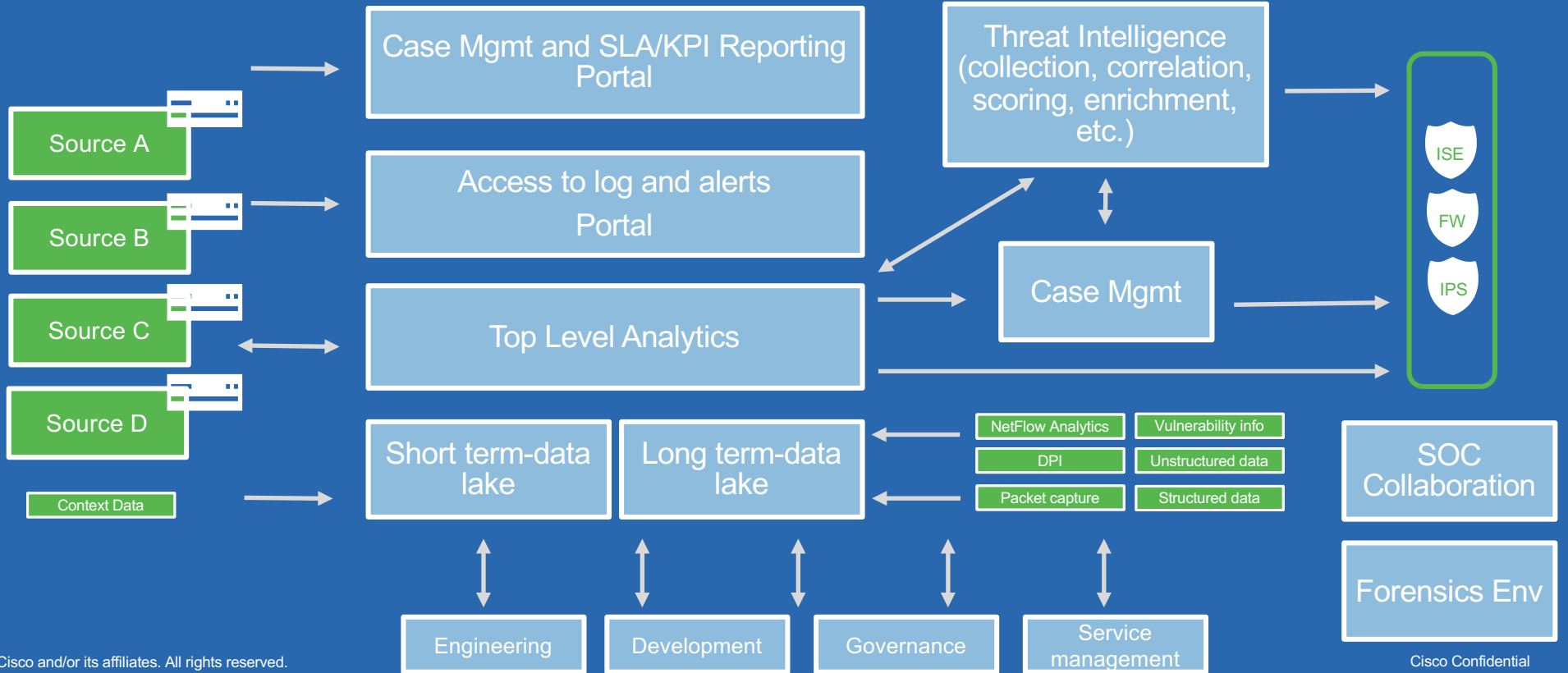


Then a Number of Artifacts are Attached

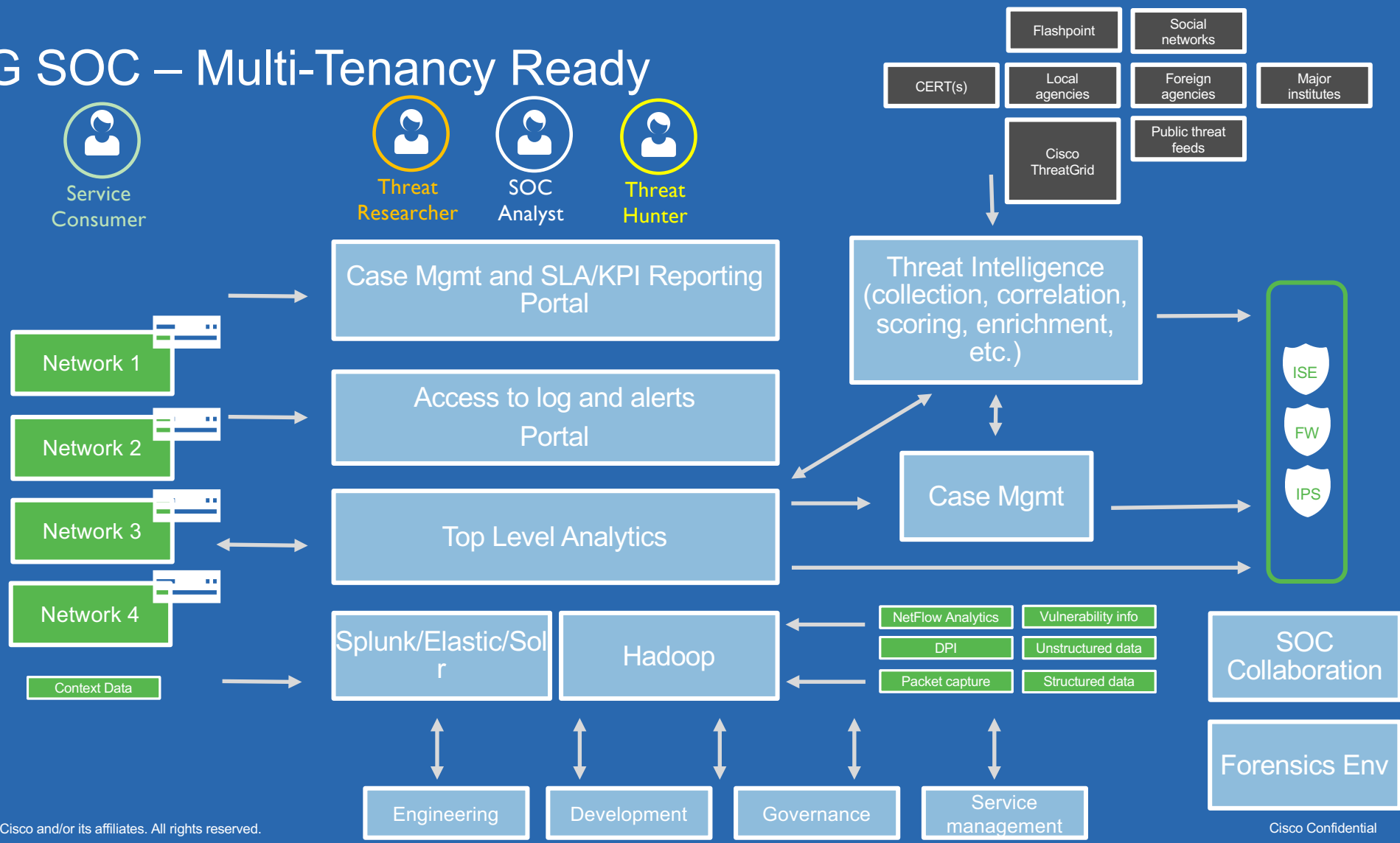


What we want to see

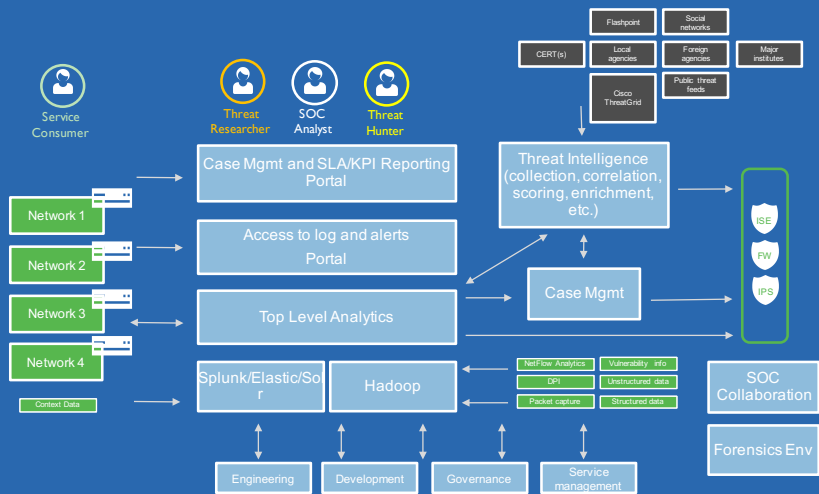
NG SOC – Multi-Tenancy Ready



NG SOC – Multi-Tenancy Ready



Structured Approach

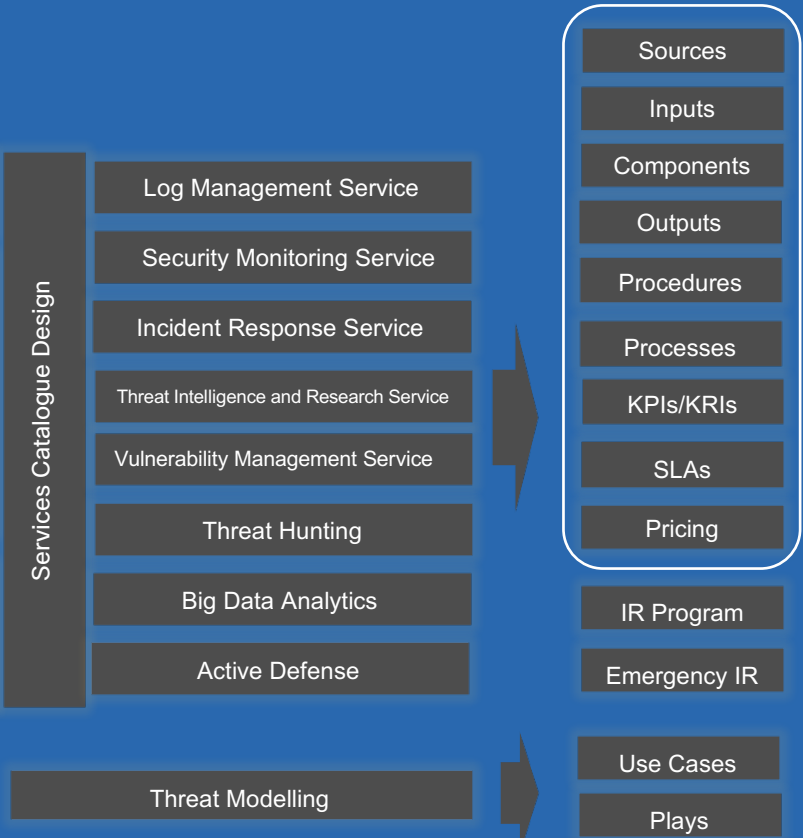


Architecture Principles
 Conceptual Architecture
 Logical Architecture
 Physical Architecture

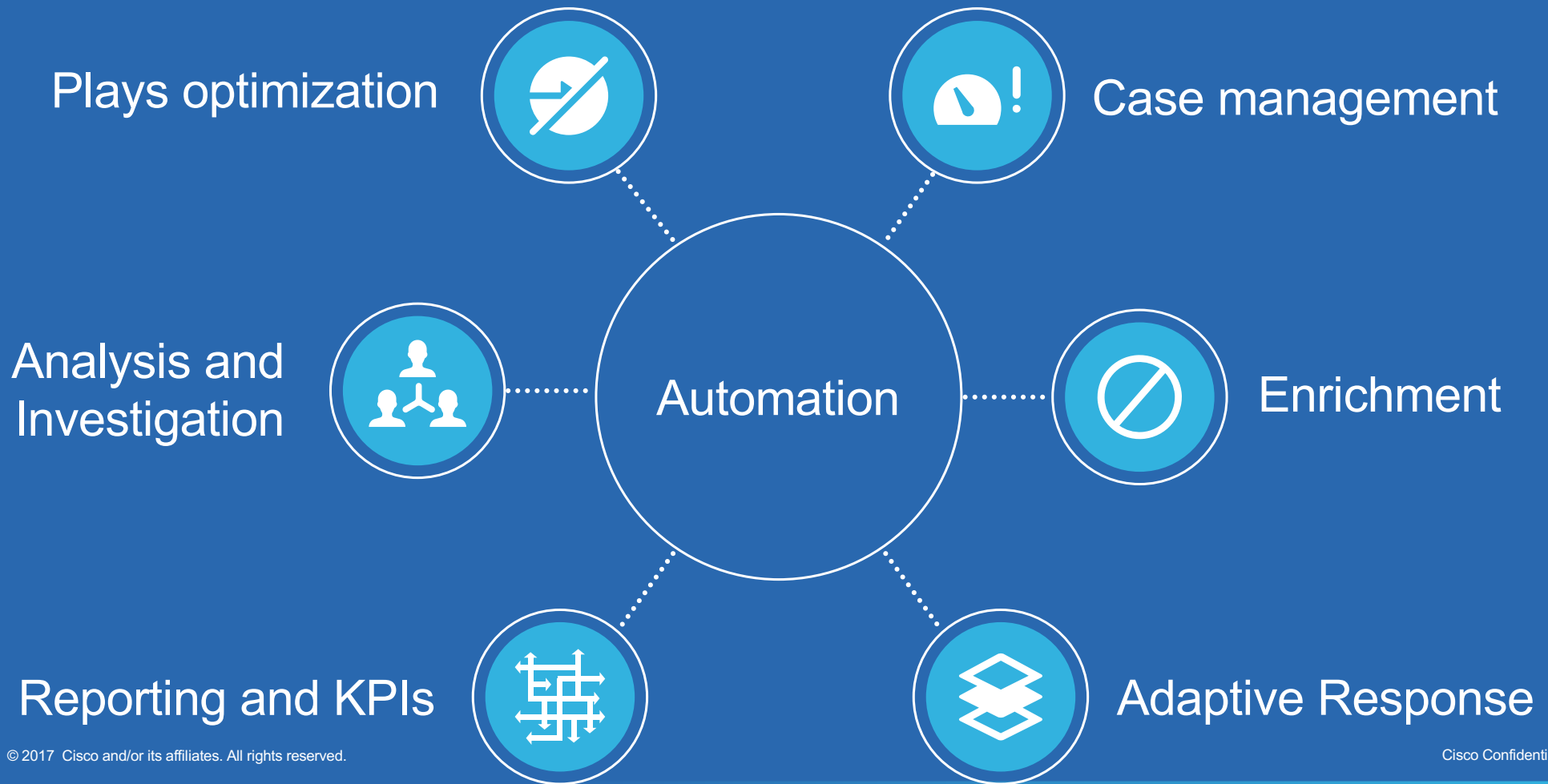
PLAN

Service Strategy
 Service Capabilities Assessment: People Systems Network Tools Processes
 High Level Services Architecture

DESIGN



Automating the SOC Tasks



Mapping Technologies and Products



< Hide Fields All Fields List Format 20 Per Page < Prev 1 2 3 4 N

Fields List:

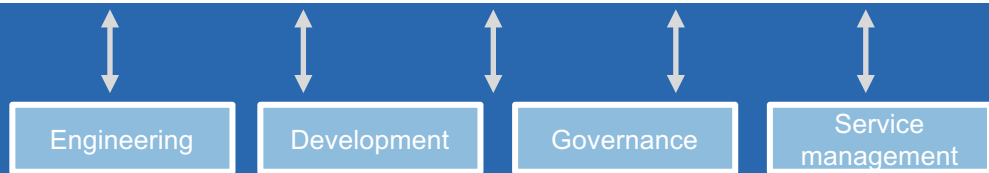
- a CPMSessionID 25
- # date_hour 4
- # date_mday 2
- # date_minute 22
- a date_month 1
- # date_second 29
- a date_wday 2
- # date_year 1
- a date_zone 1
- a DC 1
- a dest 2
- a dest_ip 2
- a dest_mac 1
- # dest_port 2
- a DestinationIPAddress 2
- # DestinationPort 2
- a EAP_Key_Name 23
- a EapAuthentication 1
- a EapTunnel 1
- a EndPointMACAddress 1

Event Log Entry:

```
ata=4= Radius.Service-Type, StepData=5= Radius.NAS-Port-Type, StepData=6=Dot1X, StepData=70=All_User_ID_Stor
StepData=71=Internal Users, StepData=74=All_AD_Join_Points, StepData=75=All_AD_Join_Points, StepData=76=jep
StepData=77=lab6.com, StepData=78=lab6.com, StepData=80=jepich@lab6.com, StepData=81=All_AD_Join_Points, S
ata=98=pxGrid_Users, StepData=99=WIN7-PC002$@lab6.com, StepData=106=pxGrid_Users, StepData=109= Session.EPSS
s, StepData=110=ANC_Quarantine, AD-User-Resolved-DNS=CN=john eppich\CN=Users\,DC=lab6\,DC=com, AD-User-DNS-
in=lab6.com, AD-User-NetBios-Name=LAB6, HostIdentityGroup=Endpoint Identity Groups:Profiled, Location=Locati
ll Locations, Device Type=Device Type#All Device Types, EPSSStatus=Quarantine, IdentityAccessRestricted=false
sponse={User-Name=jepich; State=ReauthSession:0A0000020000001602A0D4EC; Class=CACS:0A0000020000001602A0D4EC
1/215460528/82; EAP-Key-Name=19:9d:13:bf:02:a8:f4:d1:3f:26:31:5d:77:9e:ca:7d:f8:47:f3:81:65:40:05:21:ee:a7:d
:5f:78:d6:21:6e:55:01:03:09:1f:69:ae:53:cd:62:f4:ea:7b:a8:7c:91:a4:38:e6:f6:96:b7:e2:91:15:b8:c1:16:a1:81:4b
cisco-av-pair=ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-DENY_ALL_TRAFFIC-544f05ed; MS-MPPE-Send-Key=****; MS-
-Recv-Key=****; LicenseTypes=3; },
```

Event Actions:

Action	Value	Action
Build Event Type		
Extract Fields	10.0.0.46	▼
ANC Quarantine by 10.0.0.17	udp:8191	▼
ANC Un-Quarantine by ip 10.0.0.17	cisco:ise:syslog	▼
Show Source	lab6.com	▼



Confluence

Flashpoint

Social networks

20 Per Page v

< Prev 1 2 3 4 5 6 7 8 9 ...

ent
68.9.109.61 - - [05/Jan/2017:06:39:16] "GET /product.screen?productId=WC-SH-A02&JSESSIONID=SD0SL6FF7ADFF4953 HTTP 1.1" 200 3878 "http://www.google.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 v

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

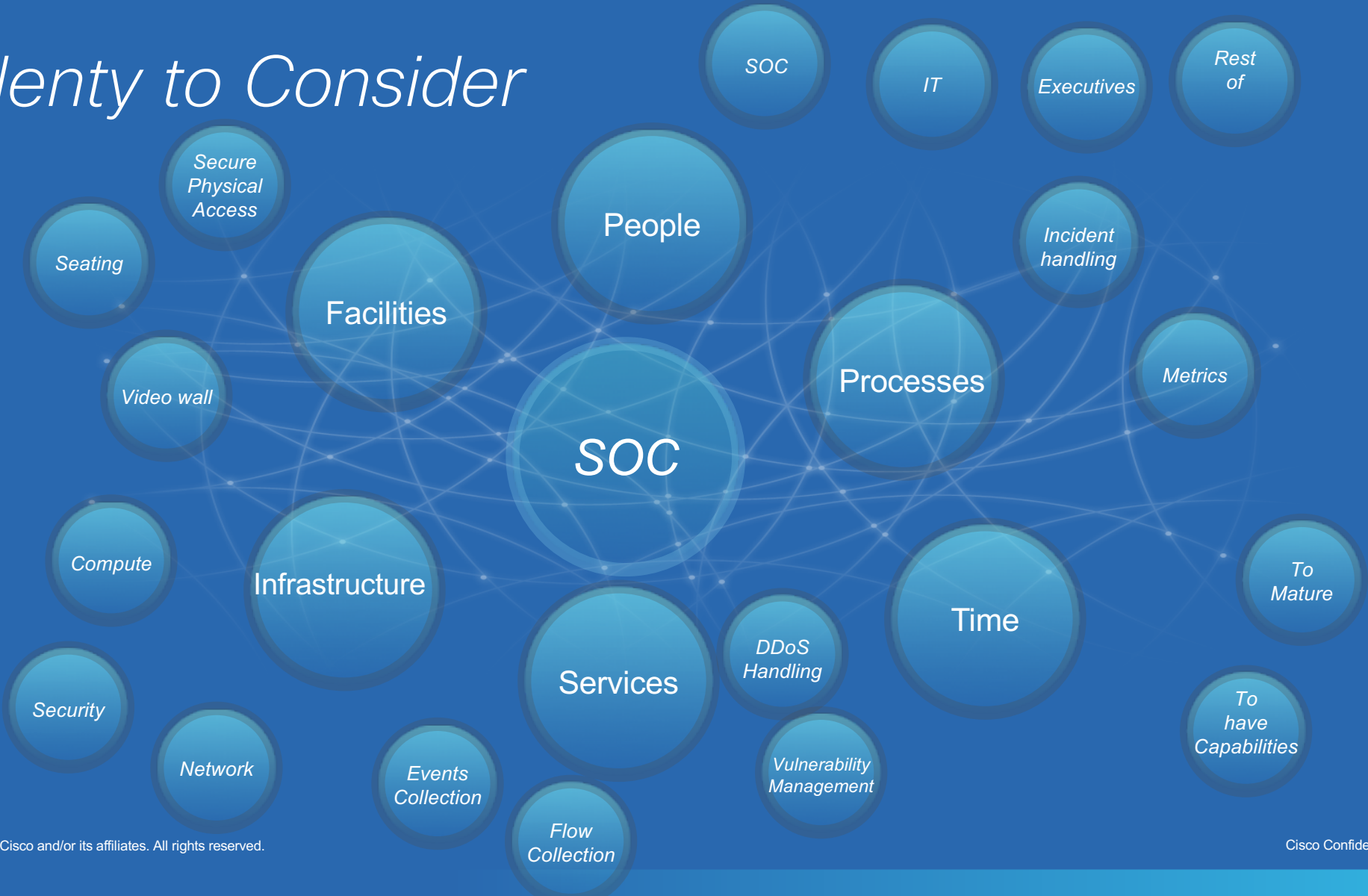
Edit Tags

ThreatQ: Add IP Indicator

Demo

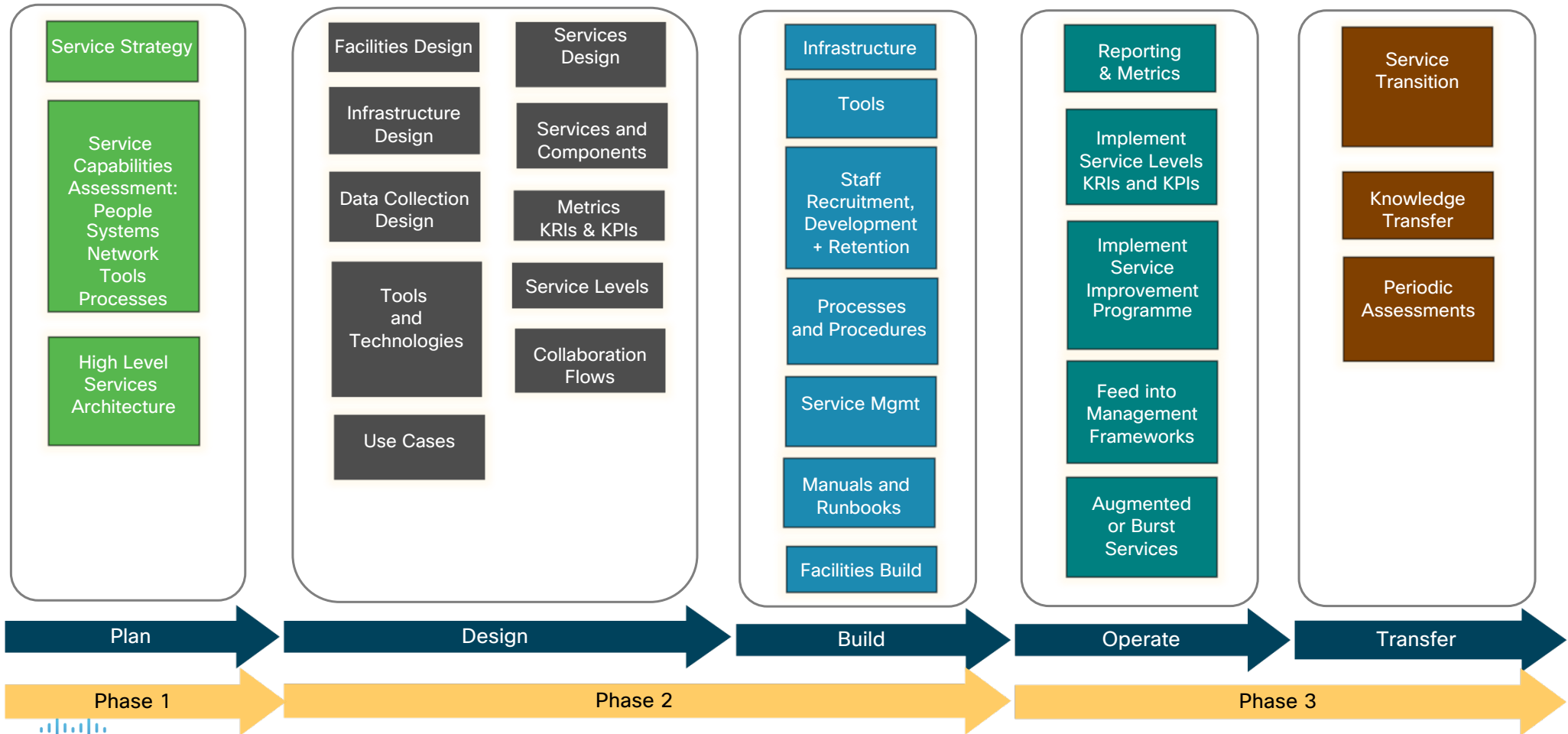
How to reach there?

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

Platforms and Content

- Platform Development
- Platform Engineering
- Platform Operations
- Content 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

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

Compliance Management

- Policy and standards development
- Compliance scanning, validation and escalation
- Compliance reporting
- Audit and compliance support

Cyber Security Controls Management

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

Training and Testing

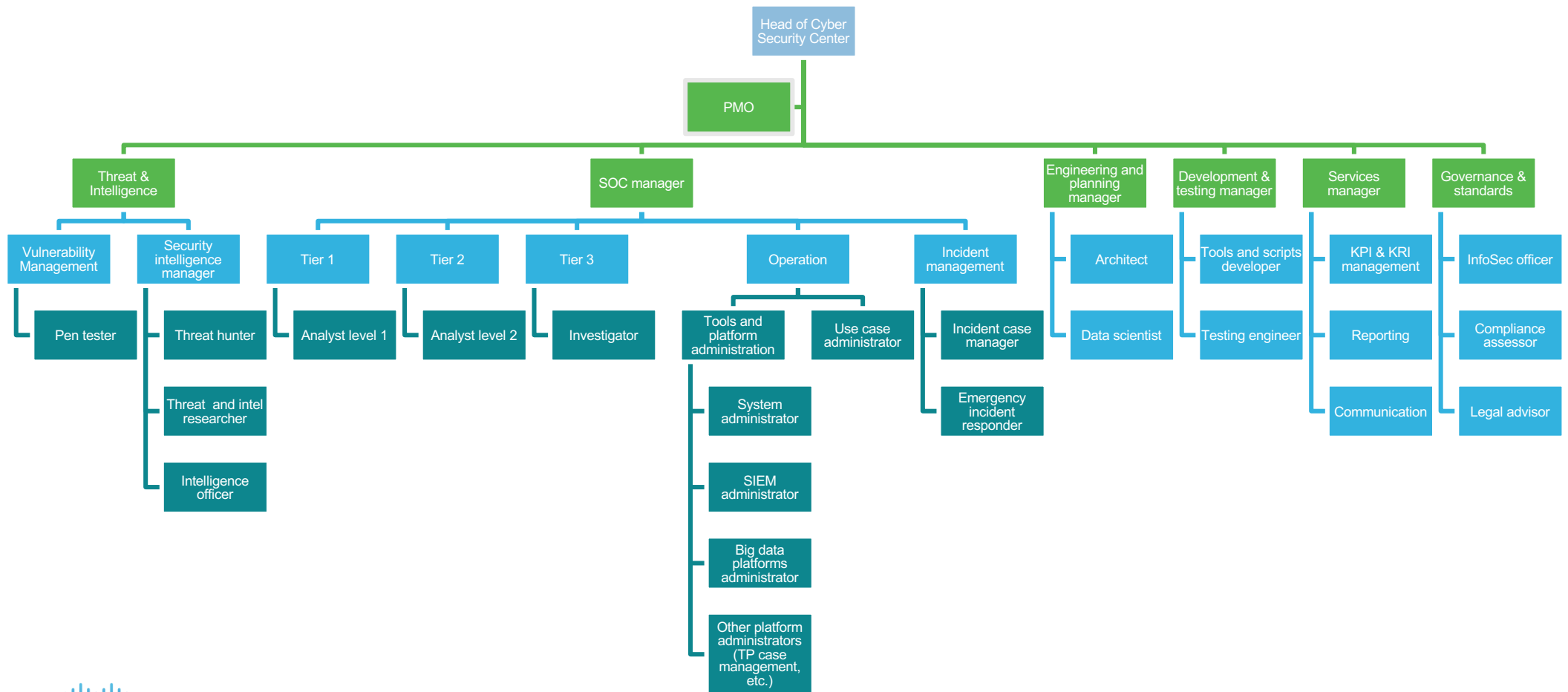
- Training Development
- Training Delivery
- Purple team and other testing services

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 as 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

A screenshot of the Splunk web interface. The top navigation bar includes "Search", "Datasets", "Reports", "Alerts", and "Dashboards". The main content area is titled "Statistical anomaly detection" and contains a search query:

```
index=onboarding sourcetype="cisco:asa" src_ip=10.9.220.* AND dest_ip!=10.* AND vendor_action=built | streamstats current=false last(_time) as next_time by dest_ip | eval gap = next_time - _time | stats count, avg(gap) as avg_gap, var(gap) as var_gap by dest_ip src_ip | search avg_gap < 60 count > 500 var_gap < 1000 | iplocation dest_ip | geostats count by dest_ip
```

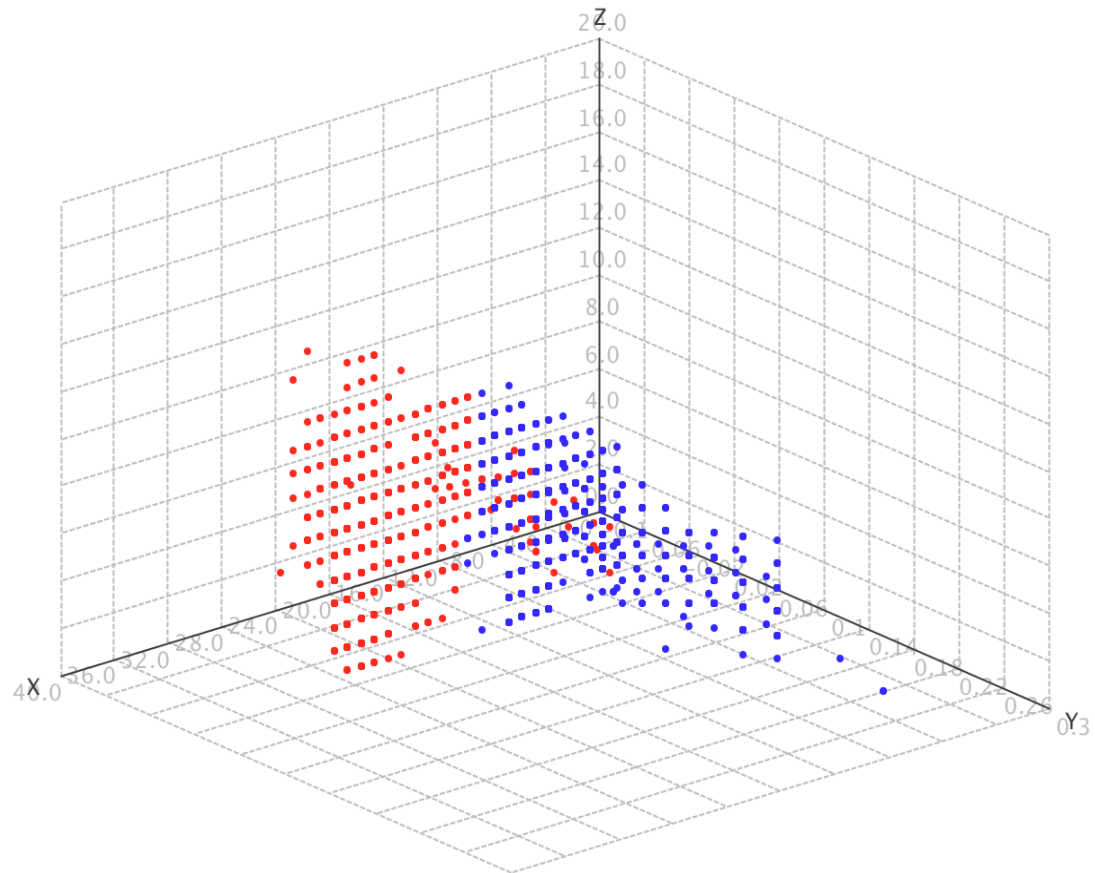
 Below the query, it shows "121,039 events (4/12/17 4:00:00.000 AM to 4/19/17 4:00:07.000 AM) No Event Sampling". The interface has tabs for "Events", "Patterns", "Statistics (23)", and "Visualization". Under "Visualization", there are options for "Cluster Map" and "Format". A map of the world is displayed with a pie chart overlay on the North America region, indicating a geographic distribution of data points.

DSC – Example



Data Science-Centric
Analytics (DSC)

- Automated categorization of data, such as 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



© 2017 Cisco and/or its affiliates. All rights reserved.

31

Demo

