RSACONFERENCE2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Cisco Unified Security Metrics: Measuring Your Organization's Security Health

SESSION ID: SEC-W05

Hessel Heerebout

Manager, Application Security and Governance
Cisco
@InfoSec_Metrics

#RSAC

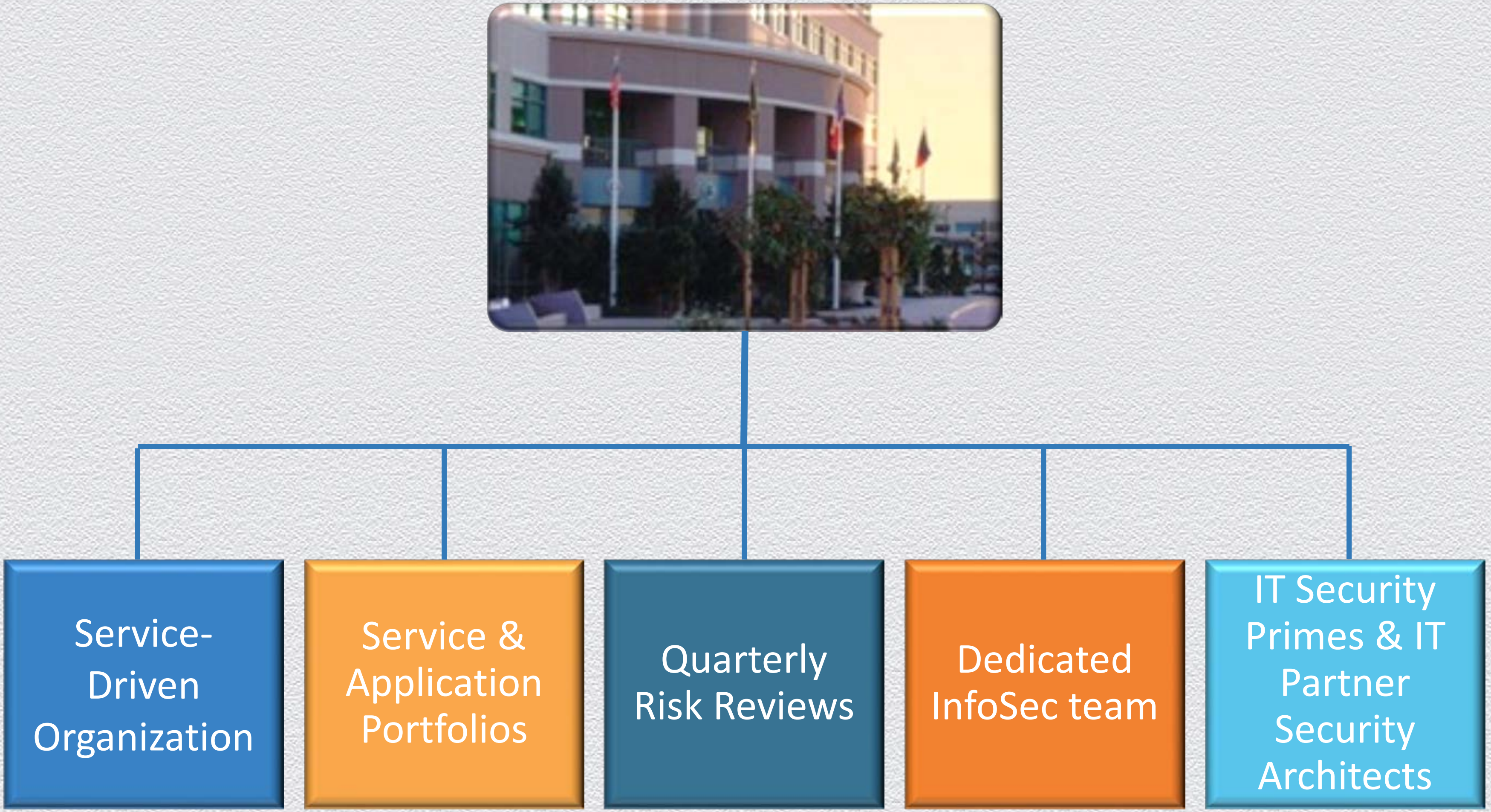
You will take away…

… a framework to set up a Security Metrics program for your organization…

Topics for Today's Discussion

- The Cisco IT Environment and Historical Security Issues
- Unified Security Metrics: How We Improved Cisco's Security Posture
- Some Practical Examples
- Early Success and Lessons Learned
- Q+A

IT Environment at Cisco



Service-Driven Organization

Service & Application Portfolios

Quarterly Risk Reviews

Dedicated InfoSec team

IT Security Primes & IT Partner Security Architects

Why? A Historical Problem

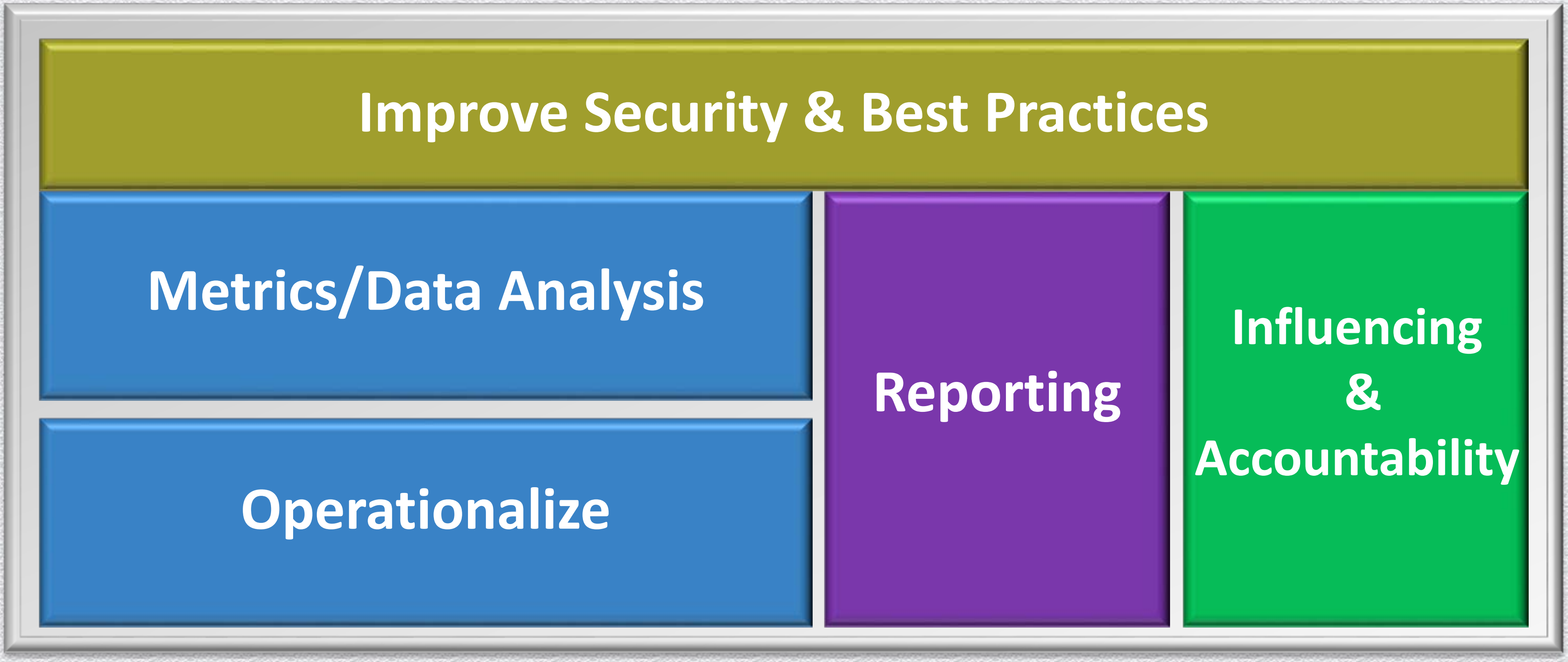
- Inconsistent security analysis, metrics and communication
- Passive, ***ad hoc*** approach to security from Business and IT
  - A focused, accelerated security initiative led to the creation of Unified Security Metrics (USM)…

"What is my security posture today and what should I do to improve it?"

IT Service Owner

How Cisco Executed the Plan

Unified Security Metrics Framework



Improve Security & Best Practices

Metrics/Data Analysis

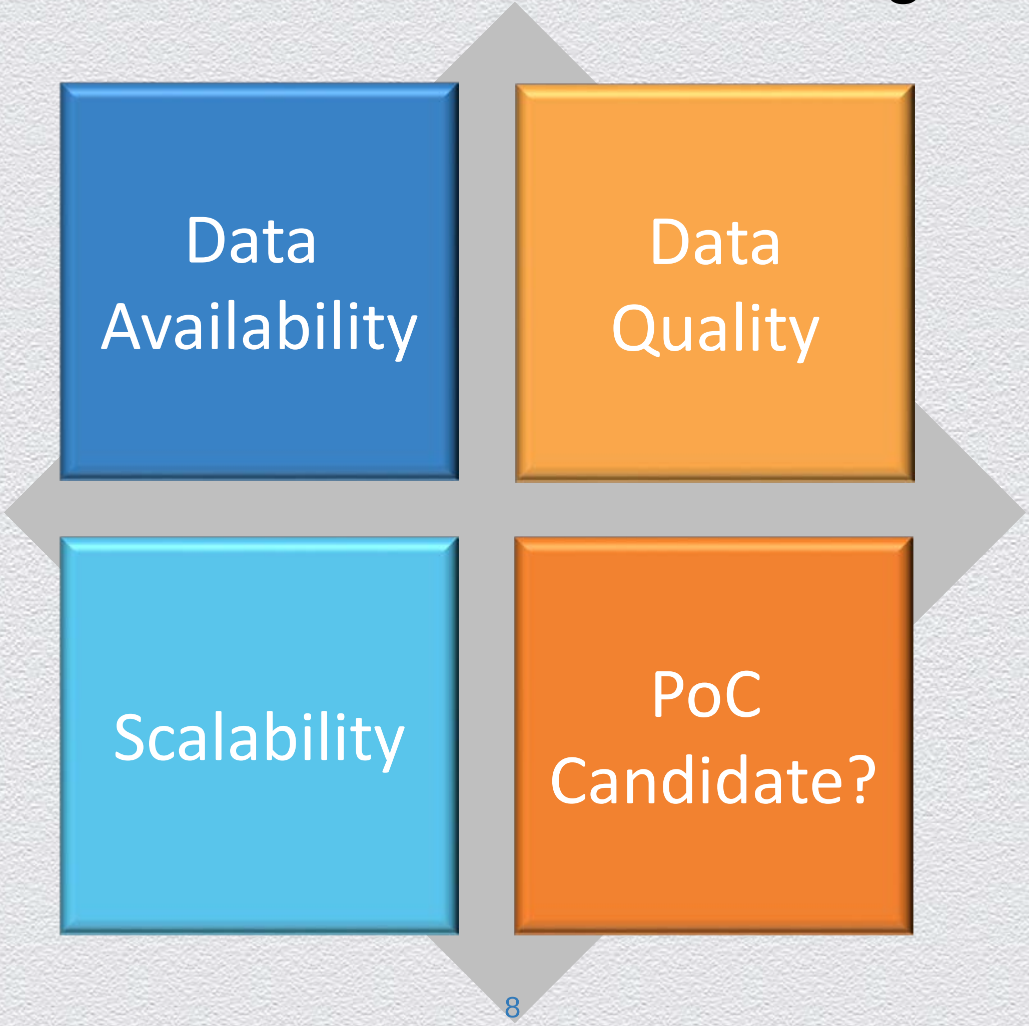
Operationalize

Reporting

Influencing & Accountability

Assessing the Landscape

Performed a Feasibility Analysis of Existing Data Sources and Ranking



Data Availability

Data Quality

Scalability

PoC Candidate?

Feasibility Analysis...

Data Availability

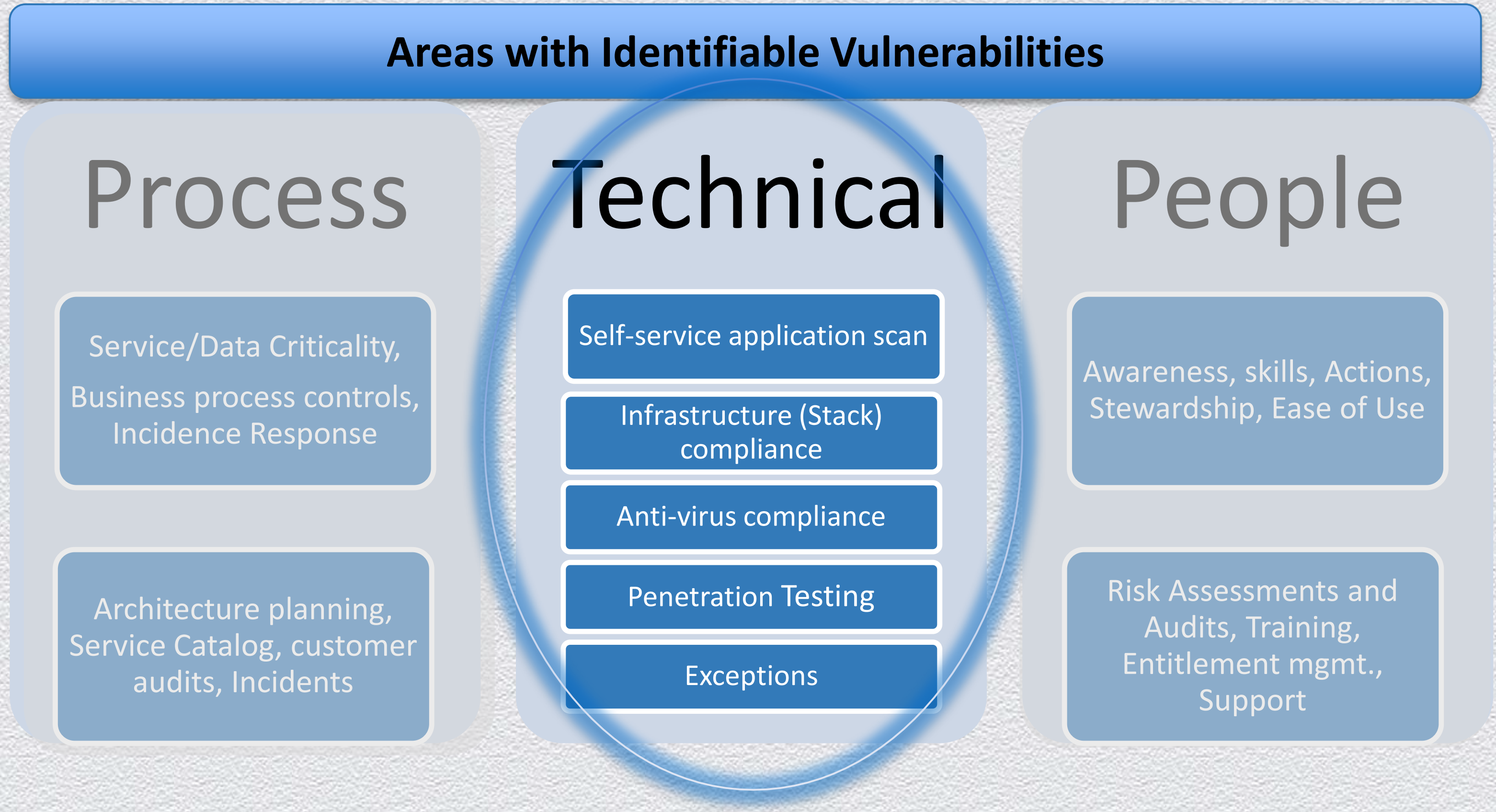
Data Quality

Scalability

PoC Candidate?

Questions	Type	Measure	Feasibility: Data Availability	Feasibility: Data Quality	Feasibility: Scalability	Feasible for PoC?
Does the service have a risk rating and data classification captured in service catalog?	Process	Actual risk rating, data classification	70%	70%	Manual	Yes
OS vulnerability / Patching compliance - Periodic OS vulnerability scanning?	Technical	# and severity of OS vulnerabilities	100%	100%	Partly Automated	Yes
What percentage of app developers and/or administrators trained on appropriate security topics?	People	total # of administrators, % of administrators trained	65%	50%	Manual	Yes

Focused on Technical Measurements (5)



Areas with Identifiable Vulnerabilities

Process

Service/Data Criticality,

Business process controls, Incidence Response

Architecture planning, Service Catalog, customer audits, Incidents

Technical

Self-service application scan

Infrastructure (Stack) compliance

Anti-virus compliance

Penetration Testing

Exceptions

People

Awareness, skills, Actions, Stewardship, Ease of Use

Risk Assessments and Audits, Training, Entitlement mgmt., Support

The Metrics Defined

- We focused on two metrics:
  - Vulnerability metric
  - On-time Closure metric
- Metrics summarized at the service-level

Service	Vulnerability Metric		On-Time Closure Metric	
Name	**Total Vulnerabilities**	**Pass Rate**	**% Closed on Time**	**Trend**
SQC	52	2 out of 5	68	↗

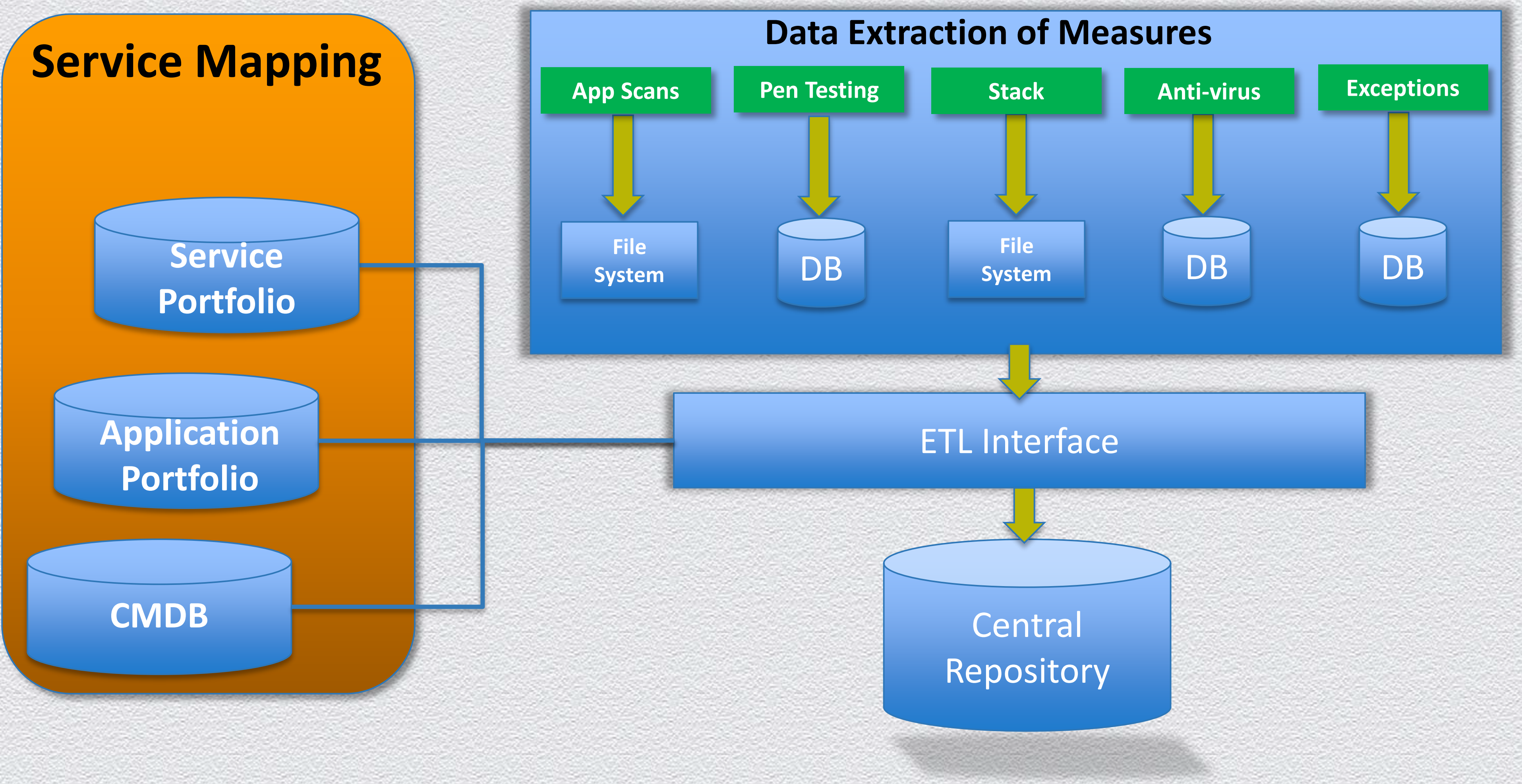
Pass Rate Legend

🔴 Immediate < 50% pass
🟡 Short Term 50-80% pass
🟢 Compliant >80% pass

Closed Vulnerability Legend

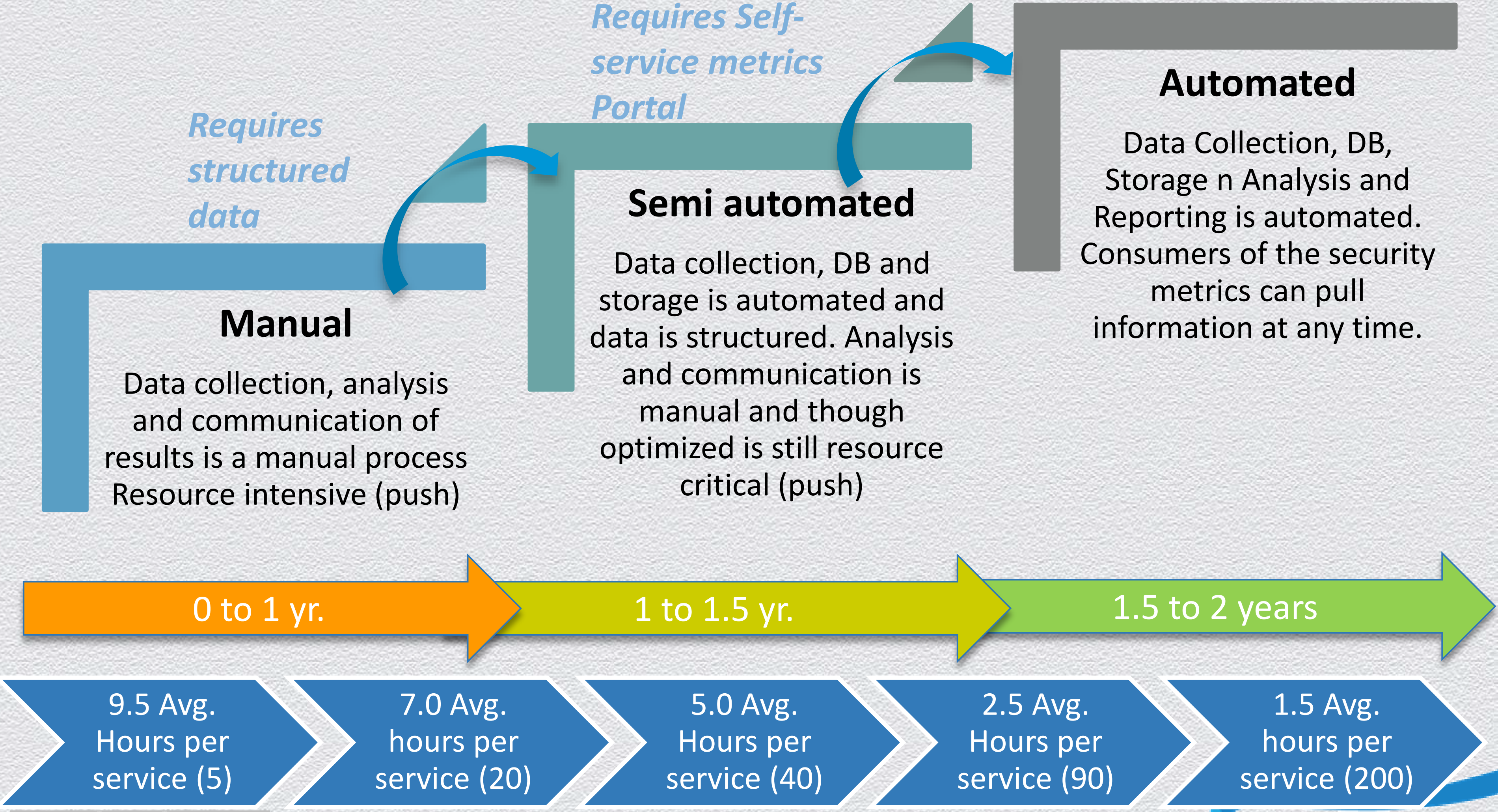
🔴 <50% closed on-time
🟡 50-80% closed on-time
🟢 >80% closed on-time
→ Direction indicates change

Linking the Data



Note: All data sources manually extracted initially and then automated during the scaling and optimization processes.

Scaling Up USM Security Maturity



Requires structured data

Manual

Data collection, analysis and communication of results is a manual process Resource intensive (push)

Requires Self-service metrics Portal

Semi automated

Data collection, DB and storage is automated and data is structured. Analysis and communication is manual and though optimized is still resource critical (push)

Automated

Data Collection, DB, Storage n Analysis and Reporting is automated. Consumers of the security metrics can pull information at any time.

0 to 1 yr.

1 to 1.5 yr.

1.5 to 2 years

9.5 Avg. Hours per service (5)

7.0 Avg. hours per service (20)

5.0 Avg. Hours per service (40)

2.5 Avg. Hours per service (90)

1.5 Avg. hours per service (200)

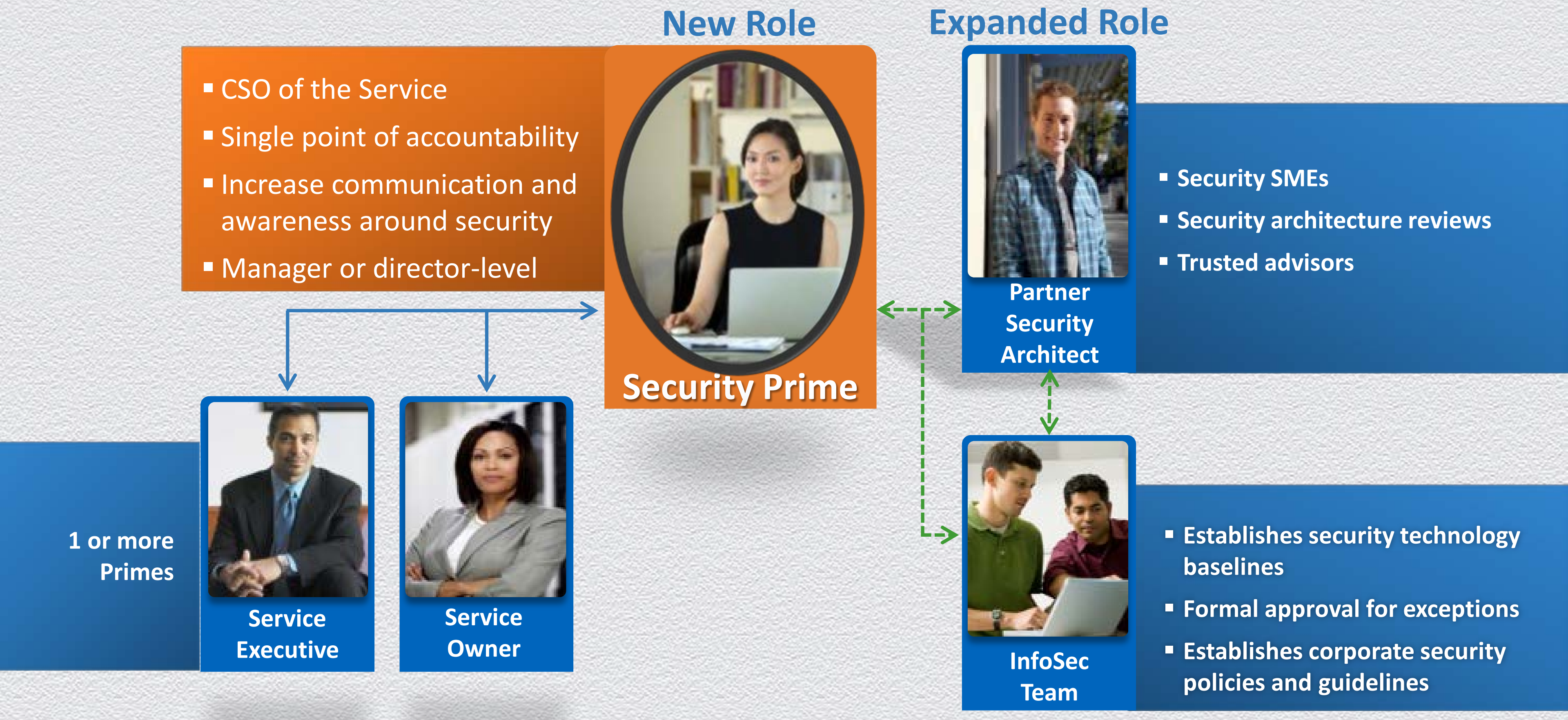
Lessons Learned

> *"99% of all Compromises required moderate-to-little sophistication."*
>
> *2013 Verizon Breach Report*

- What worked…
  - Focused on security hygiene and not "Risk"
  - Automation and optimization
  - Started small and built confidence & trust across stakeholders
  - Consistent stakeholder communications and follow-up interactions
  - The new Security Prime role*

- Challenges to overcome…
  - Stakeholders understanding the Vulnerability Metric
  - Correlating un-structured data required cap investment (API's, etc.)
  - Overloaded certain downstream processes

New and Expanded Roles



New Role

Expanded Role

- CSO of the Service
- Single point of accountability
- Increase communication and awareness around security
- Manager or director-level

Security Prime

Partner Security Architect

- Security SMEs
- Security architecture reviews
- Trusted advisors

InfoSec Team

- Establishes security technology baselines
- Formal approval for exceptions
- Establishes corporate security policies and guidelines

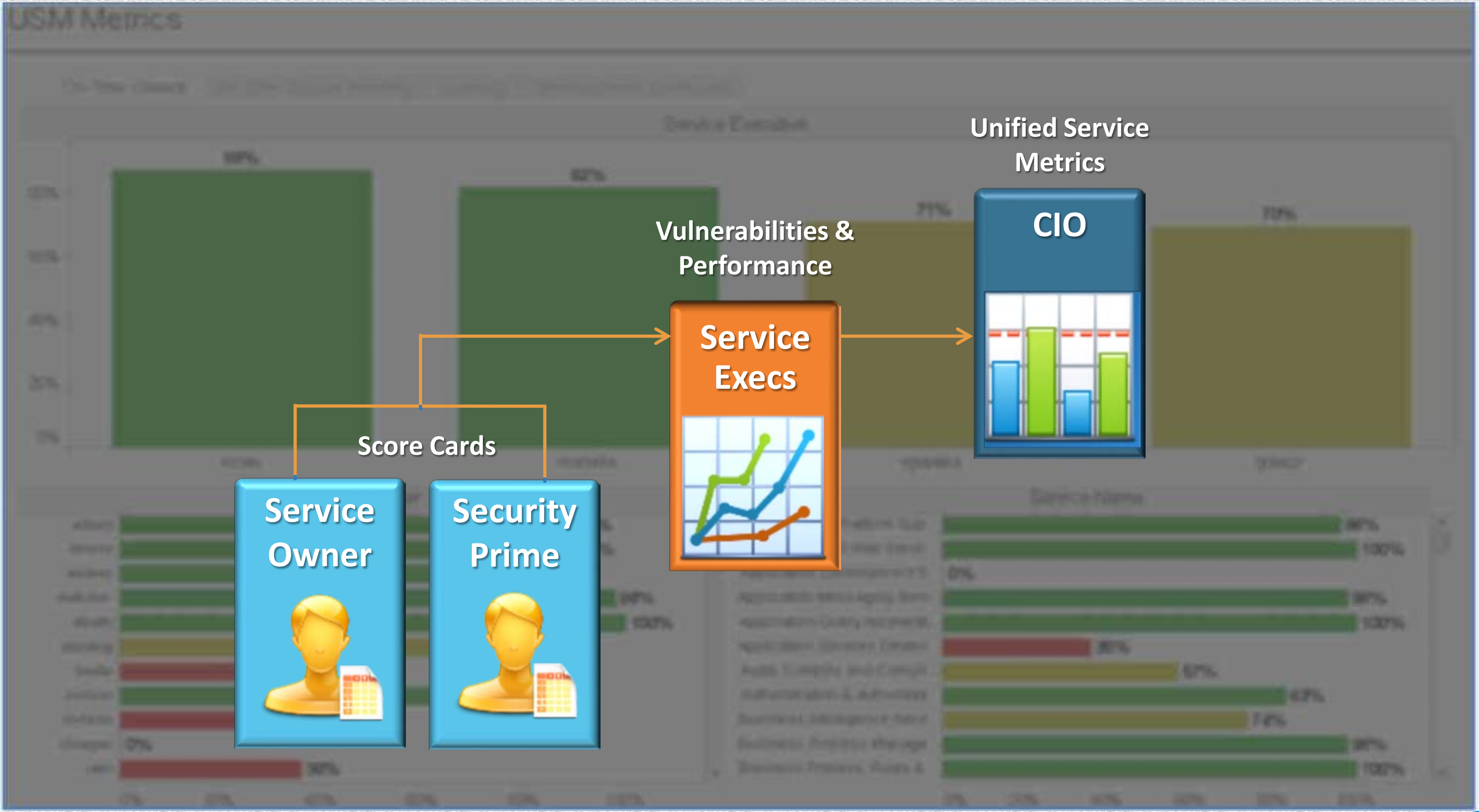
1 or more Primes

Service Executive

Service Owner

Governance & Accountability

Leverage Existing Quarterly Reporting



Unified Service Metrics

CIO

Vulnerabilities & Performance

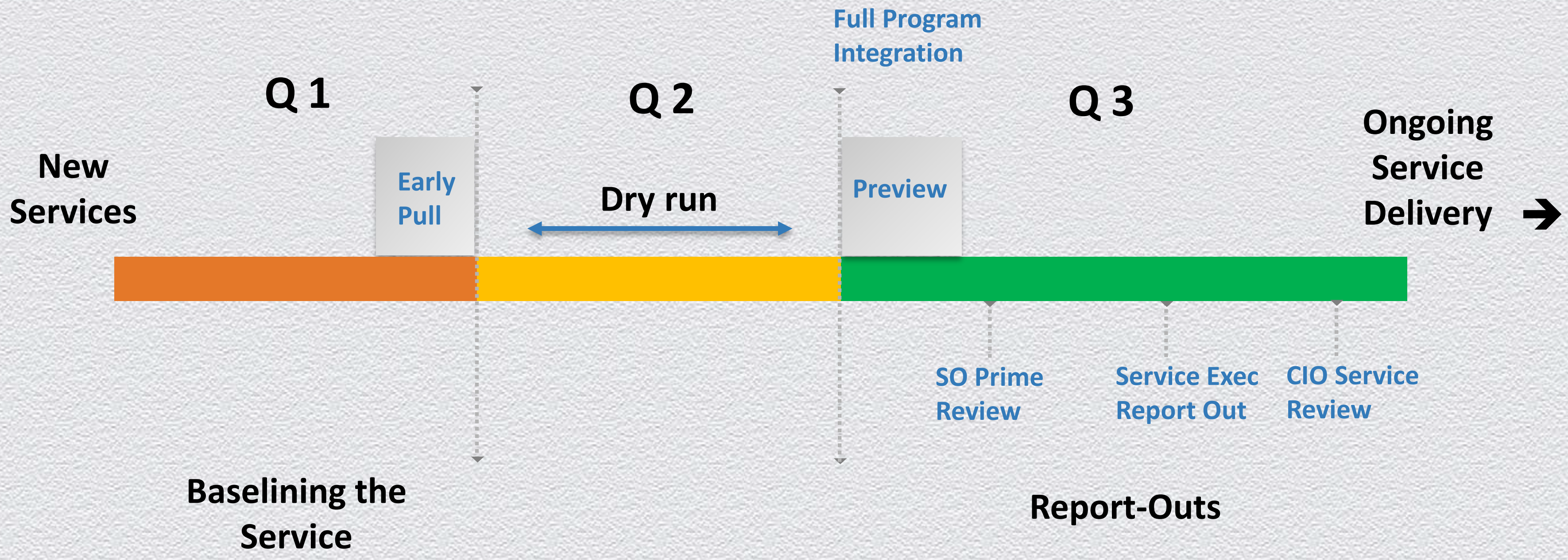
Service Execs

Score Cards

Service Owner

Security Prime

USM Program Integration and Reporting Timelines



New Services

Q 1

Early Pull

Baselining the Service

Q 2

Dry run

Full Program Integration

Q 3

Preview

SO Prime Review

Service Exec Report Out

CIO Service Review

Report-Outs

Ongoing Service Delivery ➔

Program Success

Before USM:

- Ad hoc approach to security across the service portfolio →
- Unable to manage and assess security vulnerabilities due to lack of measures →
- Marginal executive attention on internal security vulnerabilities →

Since USM:

- Shared Accountability: driving the conversation with service owners & other key stakeholders
- USM measures in place, we are able to quantify Cisco's security health: 65% reduction in vulnerabilities and On-time closure improvement from 15% to 80% within one year
- Increased Security investment (+50%) and support of the next phase of USM development

Final Thoughts…

- Done right, it works!
  - Get buy-in from upper management
  - Build the partner teams creating security synergy and governance
  - Embrace talent outside your immediate security/IT organization
  - Use measurements that are meaningful, accessible, quantifiable, and ***actionable***
- Start small and ***build trust*** across stakeholders
- Leverage "IT As a Service" building blocks
- Score results and score them objectively
- Report results using existing reporting structures wherever possible

Thank You!

Q&A