infosecurity
EUROPE
SECURITYWORKSHOPS

Simon Crocker

SOC Advisory Services Lead, Cisco EMEAR

Discover the Secrets of the SOC

cisco

Agenda

SOC Overview

SOC Services

SOC Automation

Building a SOC

Agenda

SOC Overview

SOC Services

SOC Automation

Building a SOC

Why Build a SOC?

"There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked." [1]

[1] John Chambers, "What does the Internet of Everything mean for security?" WEF, January 21, 2015.

Q: What is most important in a SOC: people, process or technology?

The Shift from Control to Visibility

“Enterprises are transforming their security spending strategy in 2017, moving away from prevention-only approaches to focus more on detection and response [2]

[2] Gartner: http://www.gartner.com/newsroom/id/3638017

What is a SOC?

There are multiple available definitions of what a SOC might be.

It may be different from a CSIRT, a CDC or a CSC.

Q: Why does the name matter?

What Does a SOC Do?

Does it:

- Monitor?
- Investigate?
- Respond / Escalate?
- Inform / Advise?
- Hunt?
- Manage Platforms?
- Provide Security Assurance?

It DEPENDS… We've never seen two SOCs that are the same.

We See a Large Number of Unsuccessful SOCs

SOC Challenges:

- Bottom Up vs Top Down Approach
- Poor or inappropriate investment
- Insufficient skilled resources
- Poor fidelity
- Poorly managed expectations
- Broken delivery models

Agenda

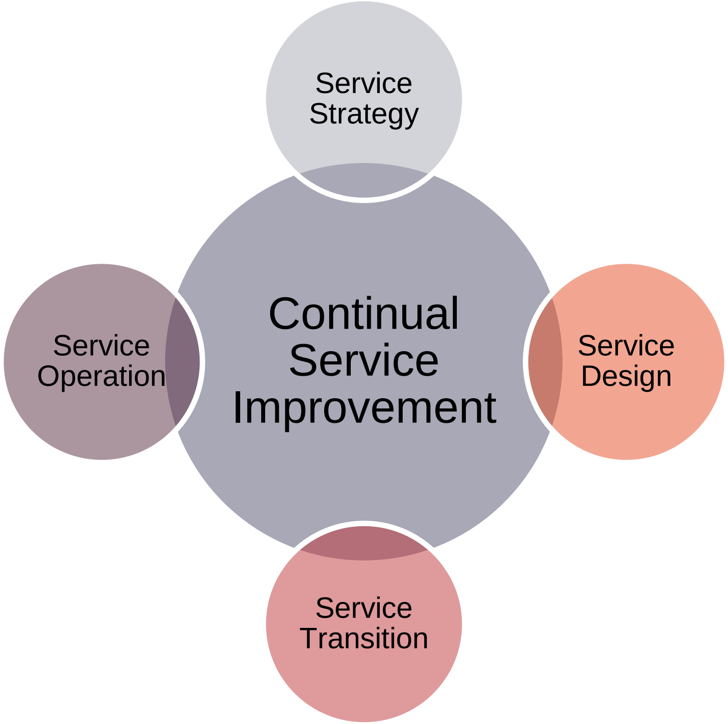
SOC Overview

SOC Services

SOC Automation

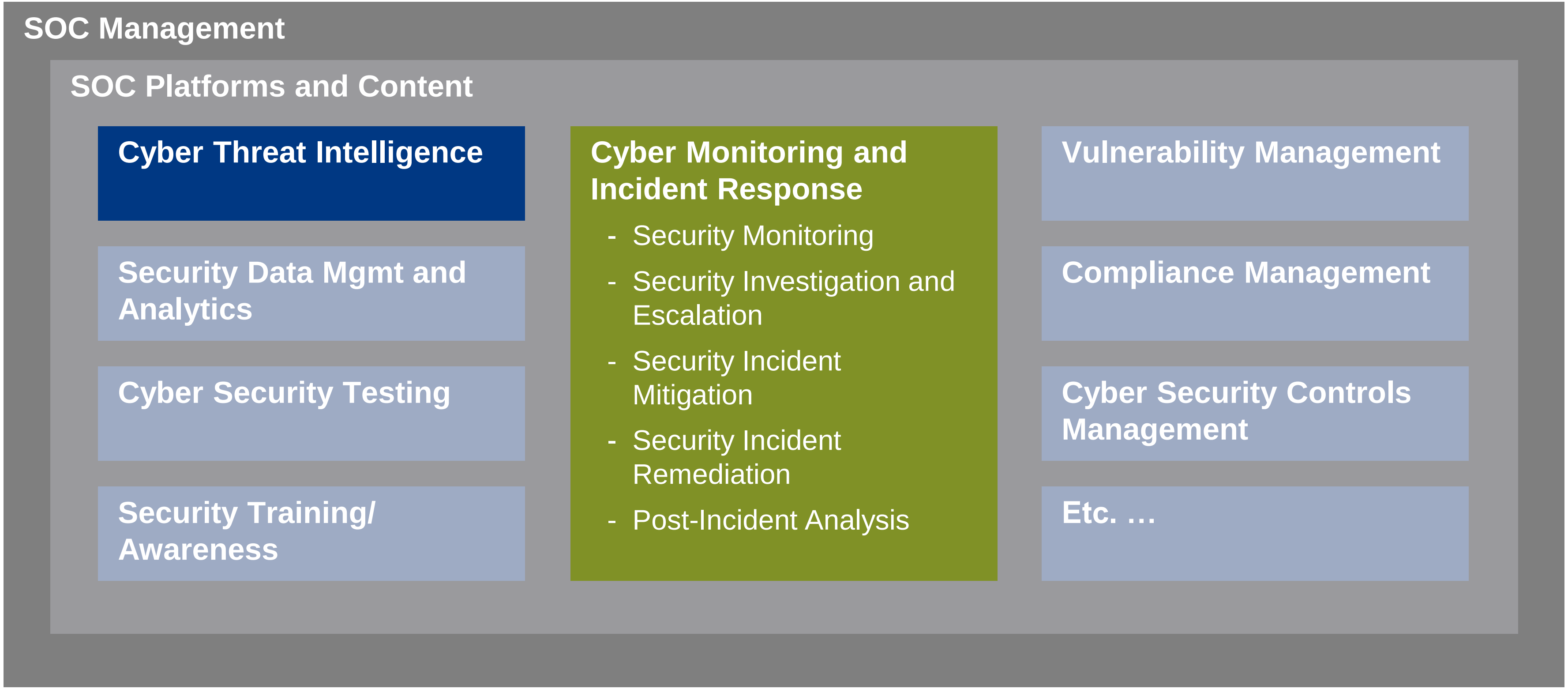
Building a SOC

Cisco's approach to developing new, or improving existing SOCs, is based on ITIL



Q: How many services does a SOC typically provide? 4, 6 or 12?

Example SOC Service Catalogue/Portfolio



SOC Management

SOC Platforms and Content

Cyber Threat Intelligence

Security Data Mgmt and Analytics

Cyber Security Testing

Security Training/ Awareness

Cyber Monitoring and Incident Response

- Security Monitoring
- Security Investigation and Escalation
- Security Incident Mitigation
- Security Incident Remediation
- Post-Incident Analysis

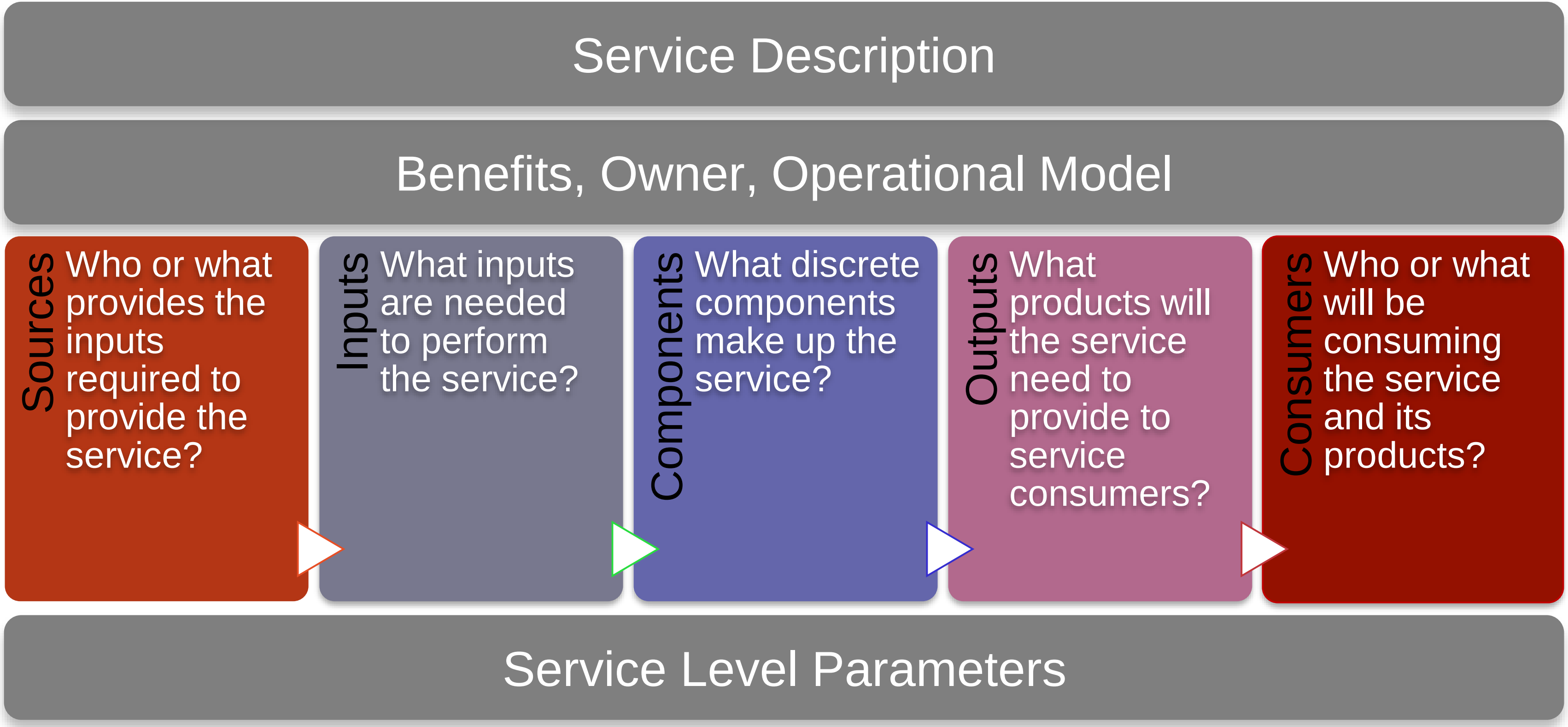
Vulnerability Management

Compliance Management

Cyber Security Controls Management

Etc. …

Service Specifications



Service Description

Benefits, Owner, Operational Model

Sources Who or what provides the inputs required to provide the service?

Inputs What inputs are needed to perform the service?

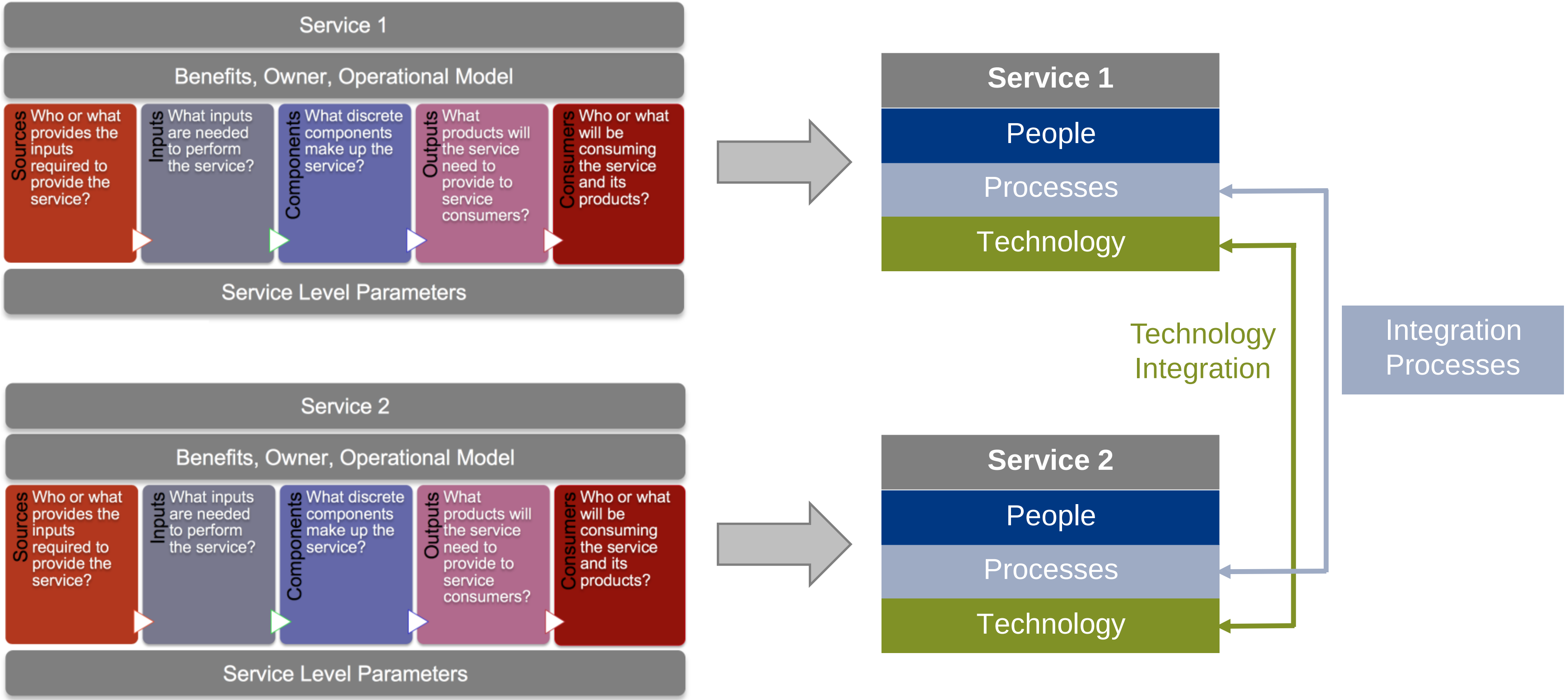
Components What discrete components make up the service?

Outputs What products will the service need to provide to service consumers?

Consumers Who or what will be consuming the service and its products?

Service Level Parameters

Service Specifications -> People, Processes, Technology



Service 1

Benefits, Owner, Operational Model

Sources: Who or what provides the inputs required to provide the service?

Inputs: What inputs are needed to perform the service?

Components: What discrete components make up the service?

Outputs: What products will the service need to provide to service consumers?

Consumers: Who or what will be consuming the service and its products?

Service Level Parameters

Service 2

Benefits, Owner, Operational Model

Sources: Who or what provides the inputs required to provide the service?

Inputs: What inputs are needed to perform the service?

Components: What discrete components make up the service?

Outputs: What products will the service need to provide to service consumers?

Consumers: Who or what will be consuming the service and its products?

Service Level Parameters

Service 1

People

Processes

Technology

Service 2

People

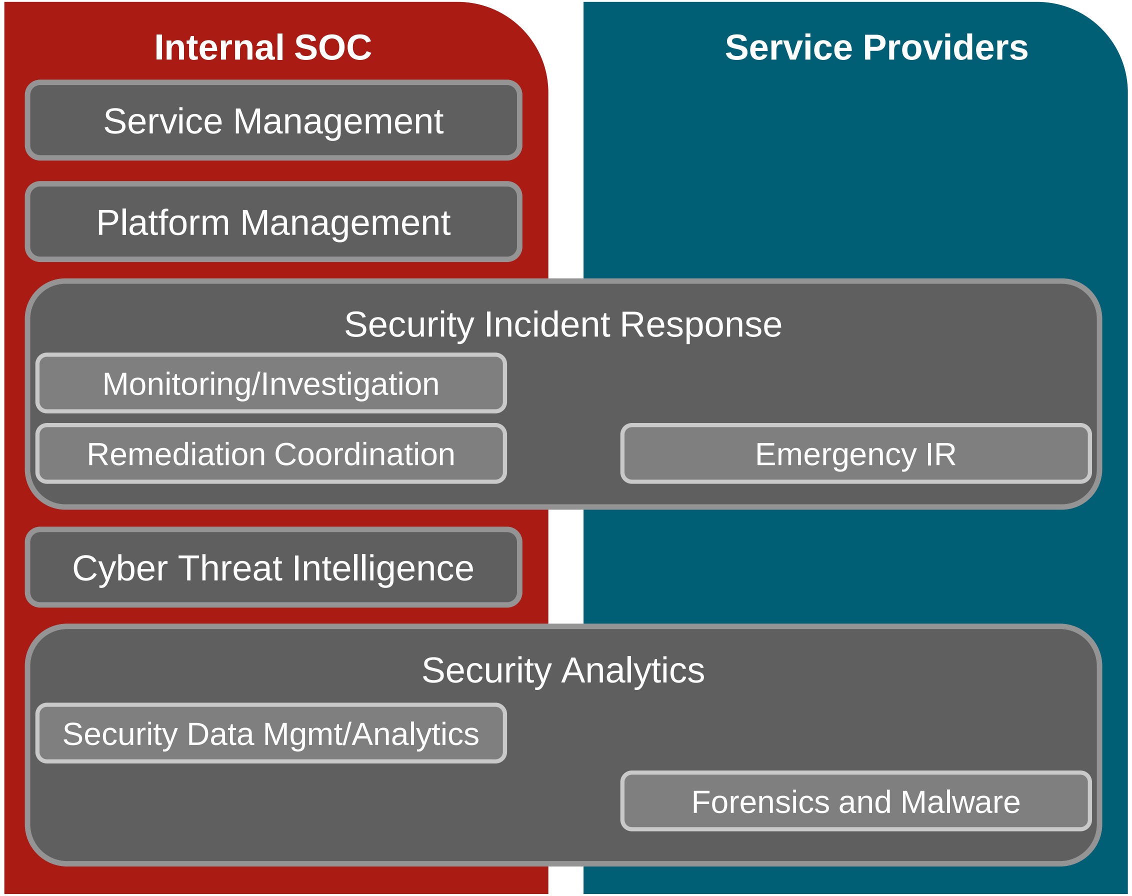
Processes

Technology

Technology Integration

Integration Processes

Operational Model: Predominantly Insourced



Internal SOC

Service Providers

Service Management

Platform Management

Security Incident Response

Monitoring/Investigation

Remediation Coordination

Emergency IR

Cyber Threat Intelligence

Security Analytics

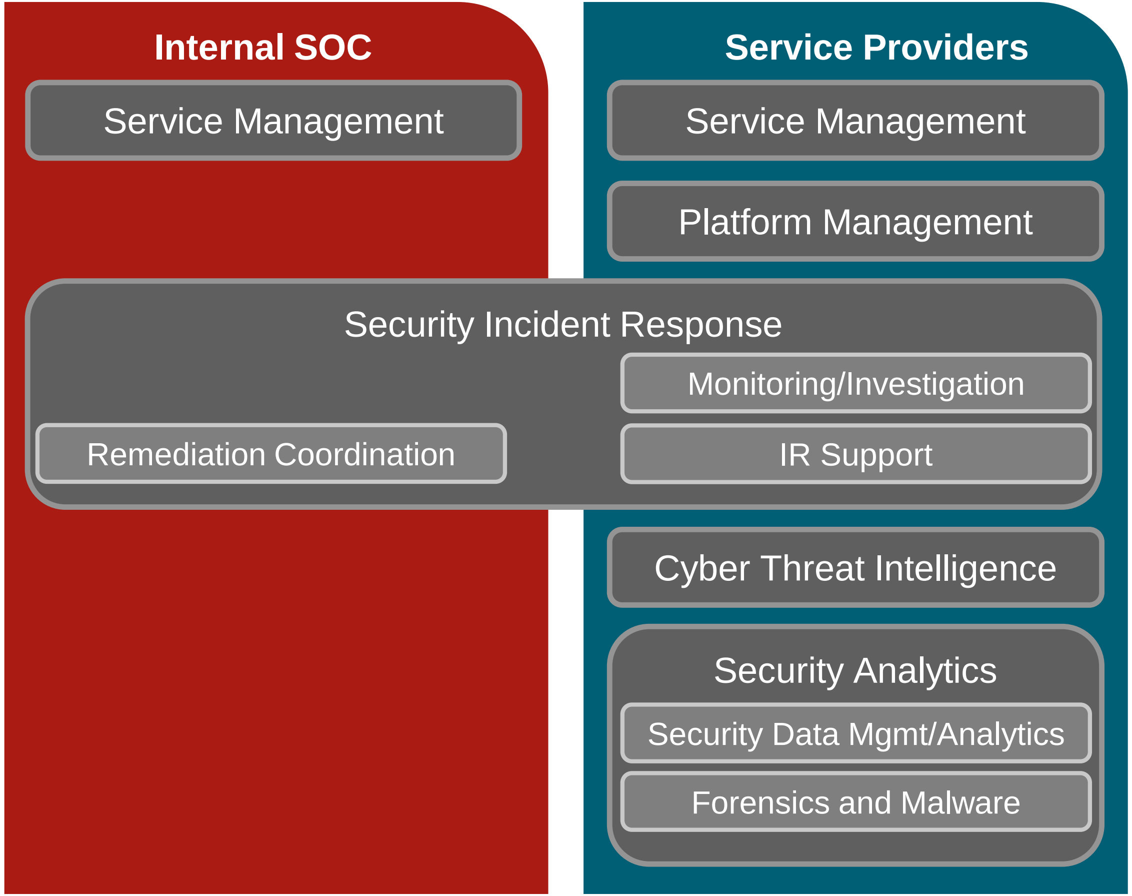
Security Data Mgmt/Analytics

Forensics and Malware

Most services provided by the internal SOC

Limited retainer based services from providers

Operational Model: Predominantly Outsourced



Core outsourced services provided by service providers

Supplementary services provided by internal operational resources

What Challenges does a Service Based Approach Help Solve?

SOC Challenges:

- Bottom Up vs Top Down Approach
- Poor or inappropriate investment
- Insufficient skilled resources
- Poor fidelity
- Poorly managed expectations
- Broken delivery models

Agenda

SOC Overview

SOC Services

SOC Automation

Building a SOC

How do I Automate my SOC?

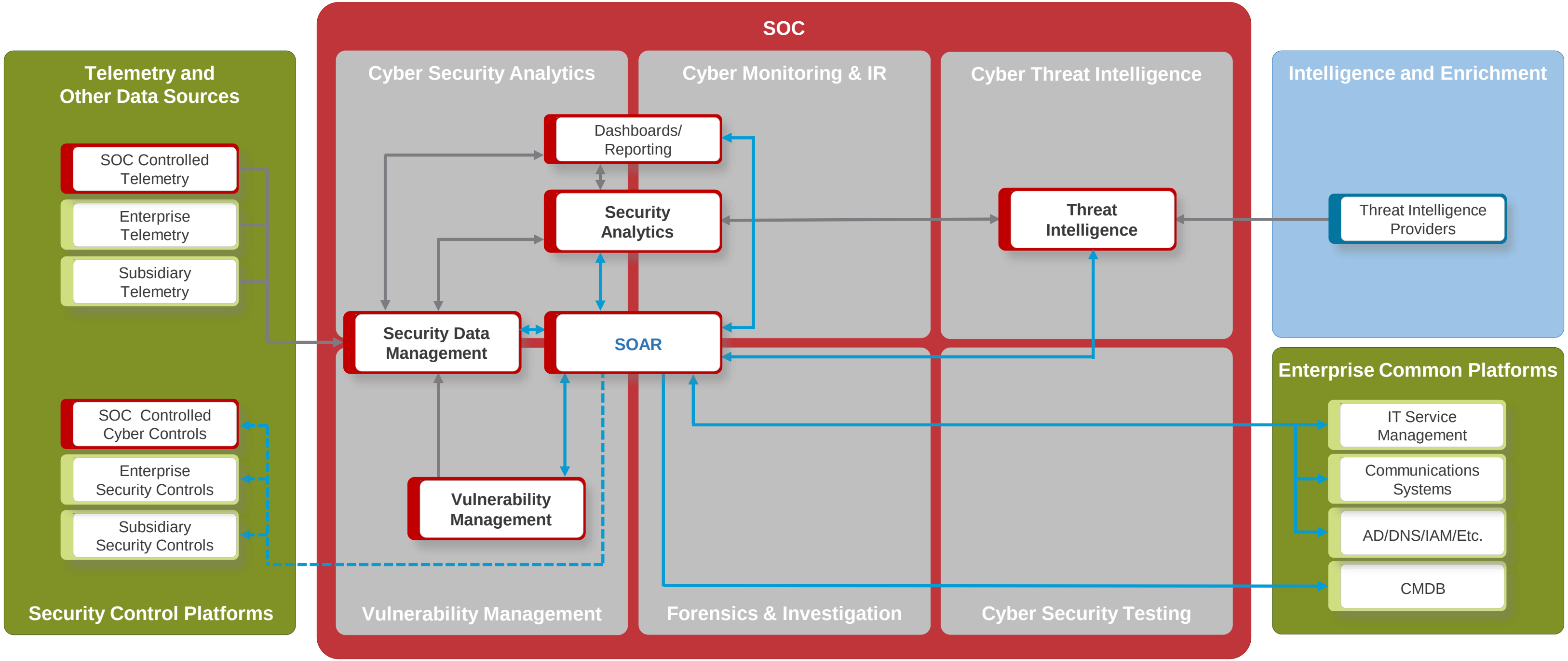
Market: SCM -> OCM -> SOAR

SOAR: Security Orchestration, Automation and Response/ Reporting

- Orchestrate end-to-end workflows
- Automate tasks using integration with other tools
- Respond automatically to security incidents
- Report key metrics and KPIs collected from the workflow

Native vs specialized platforms

SOAR in Action



What Challenges does SOAR Help Solve?

SOC Challenges:

- Bottom Up vs Top Down Approach
- Poor or inappropriate investment
- Insufficient skilled resources
- Poor fidelity
- Poorly managed expectations
- Broken delivery models

Agenda

SOC Overview

SOC Services

SOC Automation

Building a SOC

Building a SOC

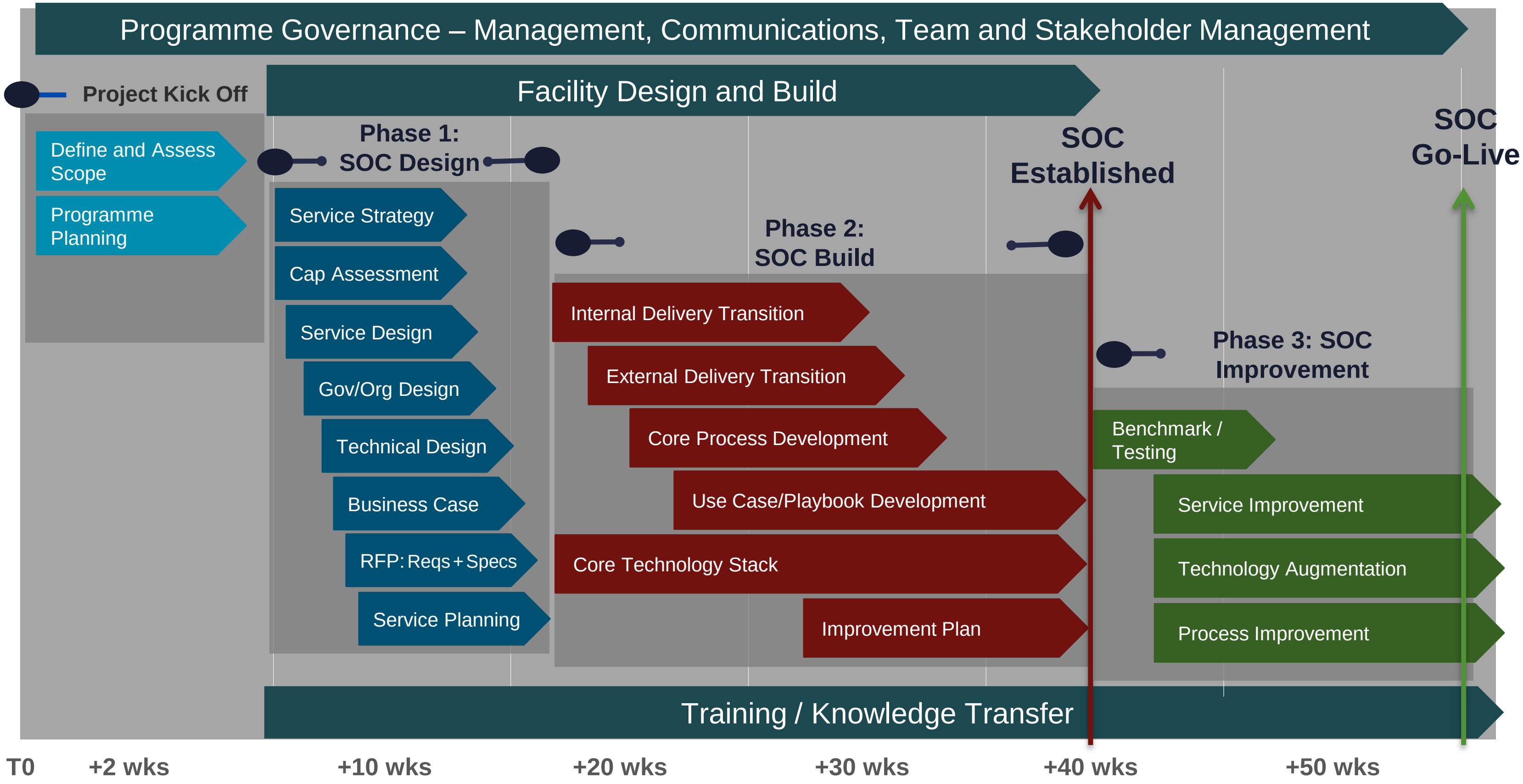
Three Phases:

1. Plan/Design
2. Build
3. Improve, and keep improving…

Q: Why is it vital for a SOC to keep improving?

Q: How long does it take to plan and build a SOC? 6 months, 12 months, 2 years?

Example SOC Roadmap



Programme Governance – Management, Communications, Team and Stakeholder Management

Project Kick Off

Define and Assess Scope

Programme Planning

Facility Design and Build

Phase 1: SOC Design

Service Strategy

Cap Assessment

Service Design

Gov/Org Design

Technical Design

Business Case

RFP: Reqs + Specs

Service Planning

Phase 2: SOC Build

Internal Delivery Transition

External Delivery Transition

Core Process Development

Use Case/Playbook Development

Core Technology Stack

Improvement Plan

SOC Established

Phase 3: SOC Improvement

Benchmark / Testing

Service Improvement

Technology Augmentation

Process Improvement

SOC Go-Live

Training / Knowledge Transfer

T0 +2 wks +10 wks +20 wks +30 wks +40 wks +50 wks

5 KEY TAKE AWAYS

5 KEY TAKE AWAYS

- SOCs face a number of challenges.
- SOCs often provide many different services.
- A top-down services based approach can help with the challenges.
- Automation can help with the challenges.
- SOCs must keep on improving.