CISCO
SECURE

The bridge to possible

Cisco’s Approach to SOC

Softprom Security Forum Baku

Kirill Sulima

Technical Solutions Architect, Cisco GSSO

April 2024,

Know your speaker

Kirill Sulima - ksulima@cisco.com

- Based in Kazakhstan (for the last 34 years ☺)
- Covering CIS countries + Caucasus cluster
- 7 years and 5 months at Cisco (7 of them at Cisco Advanced Services (CX))

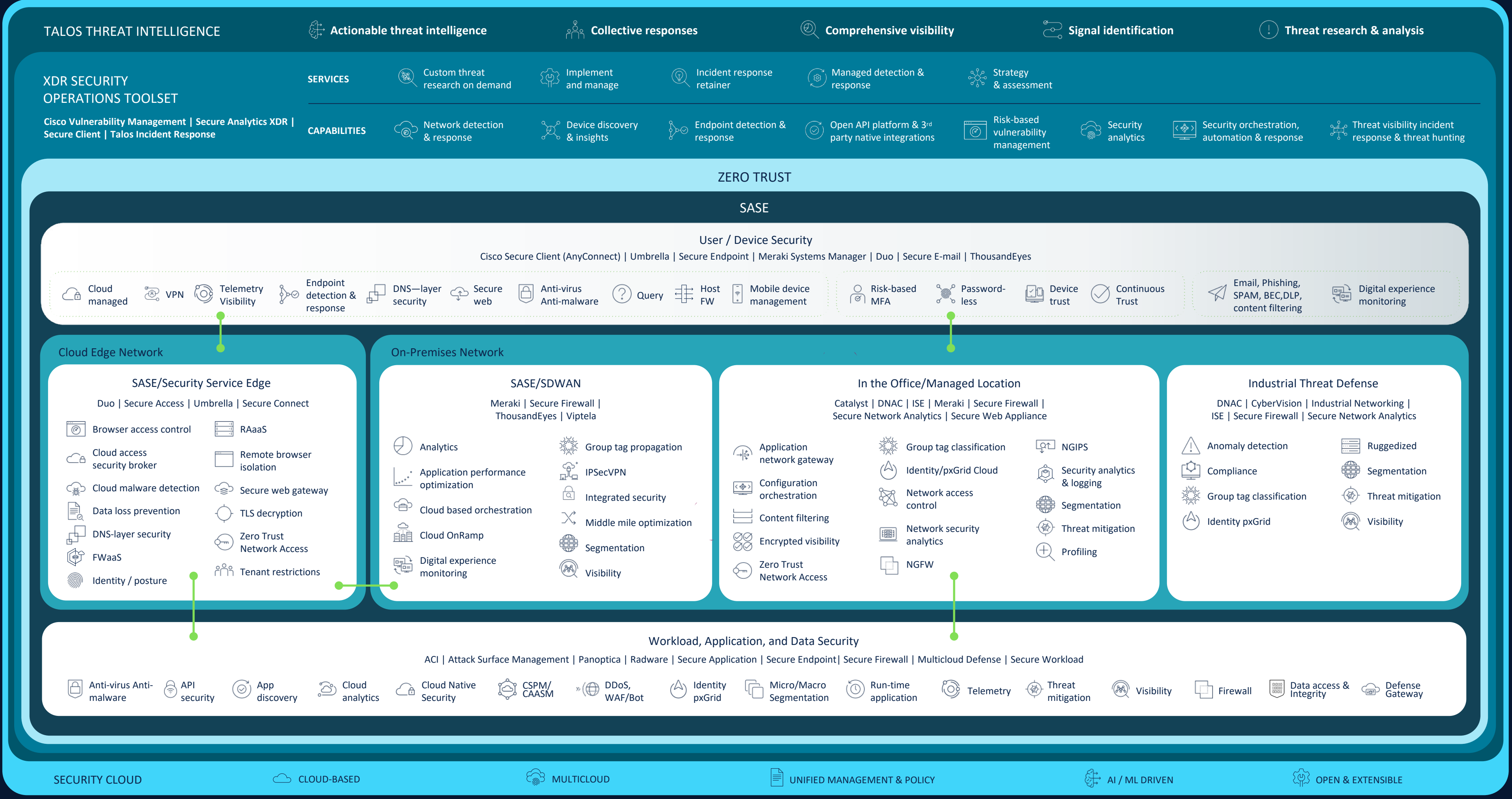
Agenda

- What is SOC?
- How Cisco could help me with my SOC journey?
- Cisco Talos
- Cisco SOC Advisory Services
- Case Studies
- Cisco SOC Implementation Services

Before we start discussing our approach to SOC…

Security Reference Architecture

cisco.com/go/sra



TALOS THREAT INTELLIGENCE

Actionable threat intelligence | Collective responses | Comprehensive visibility | Signal identification | Threat research & analysis

XDR SECURITY OPERATIONS TOOLSET

Cisco Vulnerability Management | Secure Analytics XDR | Secure Client | Talos Incident Response

SERVICES

- Custom threat research on demand
- Implement and manage
- Incident response retainer
- Managed detection & response
- Strategy & assessment

CAPABILITIES

- Network detection & response
- Device discovery & insights
- Endpoint detection & response
- Open API platform & 3rd party native integrations
- Risk-based vulnerability management
- Security analytics
- Security orchestration, automation & response
- Threat visibility incident response & threat hunting

ZERO TRUST

SASE

User / Device Security

Cisco Secure Client (AnyConnect) | Umbrella | Secure Endpoint | Meraki Systems Manager | Duo | Secure E-mail | ThousandEyes

- Cloud managed
- VPN
- Telemetry Visibility
- Endpoint detection & response
- DNS—layer security
- Secure web
- Anti-virus Anti-malware
- Query
- Host FW
- Mobile device management
- Risk-based MFA
- Password-less
- Device trust
- Continuous Trust
- Email, Phishing, SPAM, BEC,DLP, content filtering
- Digital experience monitoring

Cloud Edge Network

SASE/Security Service Edge

Duo | Secure Access | Umbrella | Secure Connect

- Browser access control
- Cloud access security broker
- Cloud malware detection
- Data loss prevention
- DNS-layer security
- FWaaS
- Identity / posture
- RAaaS
- Remote browser isolation
- Secure web gateway
- TLS decryption
- Zero Trust Network Access
- Tenant restrictions

On-Premises Network

SASE/SDWAN

Meraki | Secure Firewall | ThousandEyes | Viptela

- Analytics
- Application performance optimization
- Cloud based orchestration
- Cloud OnRamp
- Digital experience monitoring
- Group tag propagation
- IPSecVPN
- Integrated security
- Middle mile optimization
- Segmentation
- Visibility

In the Office/Managed Location

Catalyst | DNAC | ISE | Meraki | Secure Firewall | Secure Network Analytics | Secure Web Appliance

- Application network gateway
- Configuration orchestration
- Content filtering
- Encrypted visibility
- Zero Trust Network Access
- Group tag classification
- Identity/pxGrid Cloud
- Network access control
- Network security analytics
- NGFW
- NGIPS
- Security analytics & logging
- Segmentation
- Threat mitigation
- Profiling

Industrial Threat Defense

DNAC | CyberVision | Industrial Networking | ISE | Secure Firewall | Secure Network Analytics

- Anomaly detection
- Compliance
- Group tag classification
- Identity pxGrid
- Ruggedized
- Segmentation
- Threat mitigation
- Visibility

Workload, Application, and Data Security

ACI | Attack Surface Management | Panoptica | Radware | Secure Application | Secure Endpoint| Secure Firewall | Multicloud Defense | Secure Workload

- Anti-virus Anti-malware
- API security
- App discovery
- Cloud analytics
- Cloud Native Security
- CSPM/ CAASM
- DDoS, WAF/Bot
- Identity pxGrid
- Micro/Macro Segmentation
- Run-time application
- Telemetry
- Threat mitigation
- Visibility
- Firewall
- Data access & Integrity
- Defense Gateway

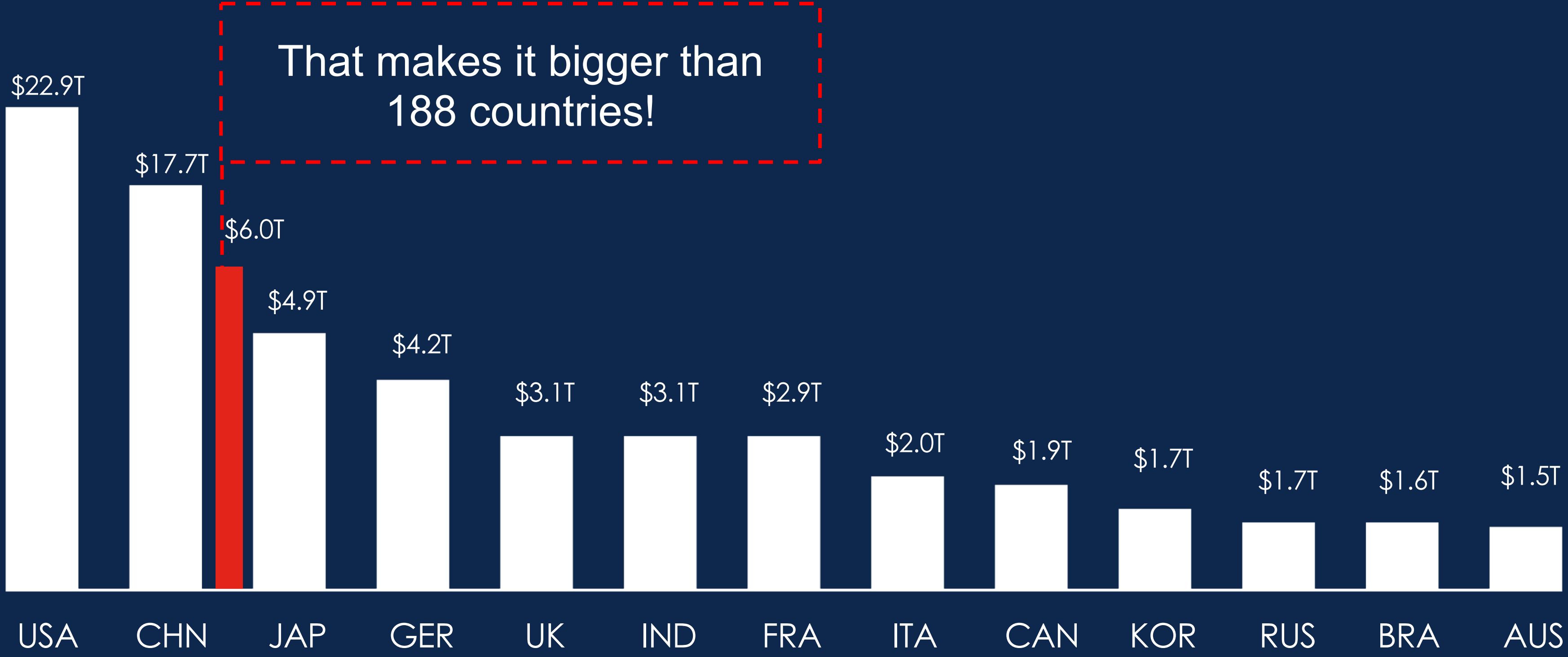
SECURITY CLOUD

CLOUD-BASED | MULTICLOUD | UNIFIED MANAGEMENT & POLICY | AI / ML DRIVEN | OPEN & EXTENSIBLE

splunk>
a CISCO company
CISCO

Now let’s talk about SOC ☺

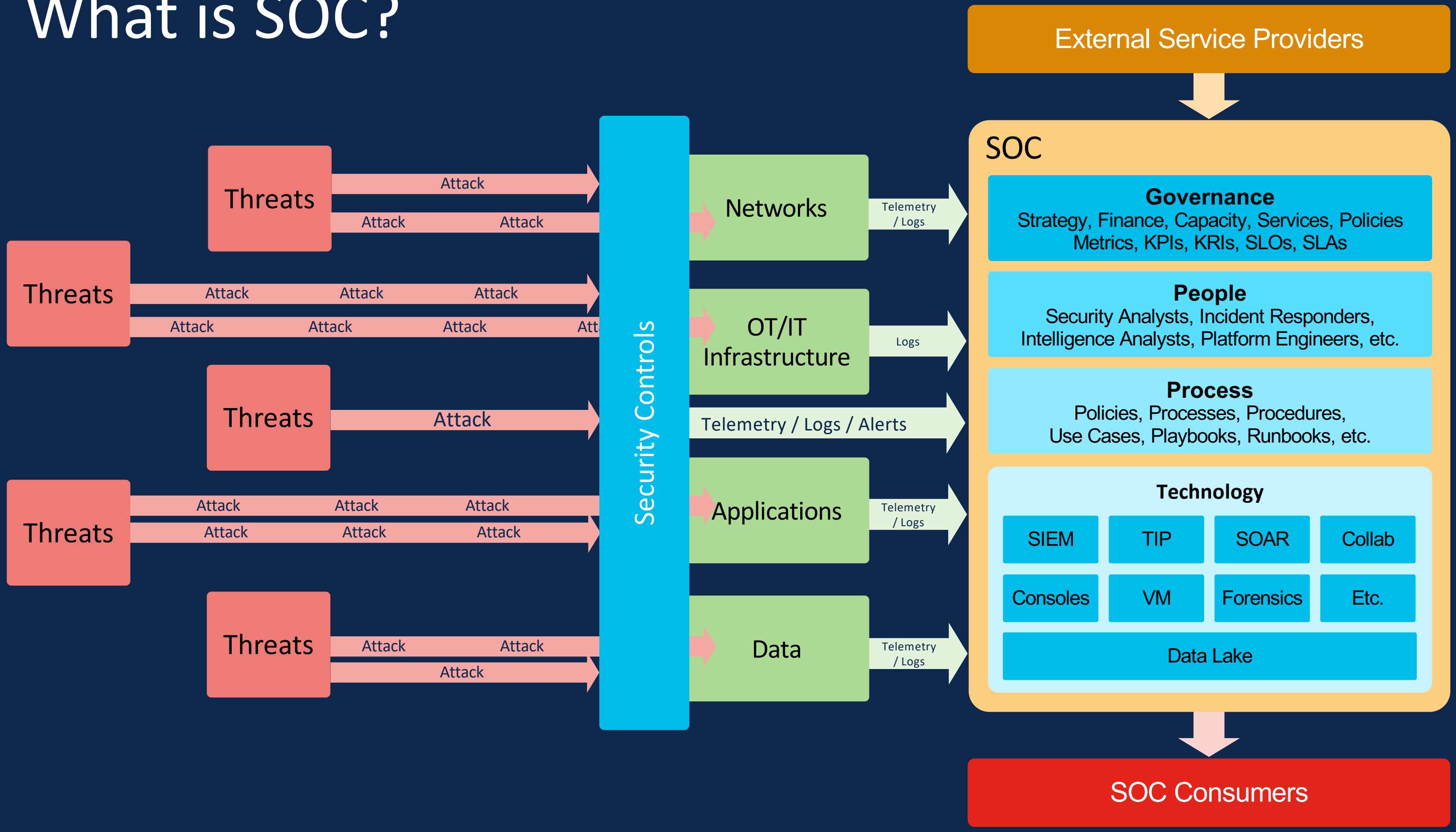
If Cybercrime were a Country...



That makes it bigger than 188 countries!

Source: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

What is SOC?



Threats

Attack

Attack Attack

Threats

Attack Attack Attack

Attack Attack Attack Att

Threats

Attack

Threats

Attack Attack Attack

Attack Attack Attack

Threats

Attack Attack

Attack

Security Controls

Networks

Telemetry / Logs

OT/IT Infrastructure

Logs

Telemetry / Logs / Alerts

Applications

Telemetry / Logs

Data

Telemetry / Logs

External Service Providers

SOC

Governance
Strategy, Finance, Capacity, Services, Policies
Metrics, KPIs, KRIs, SLOs, SLAs

People
Security Analysts, Incident Responders,
Intelligence Analysts, Platform Engineers, etc.

Process
Policies, Processes, Procedures,
Use Cases, Playbooks, Runbooks, etc.

Technology

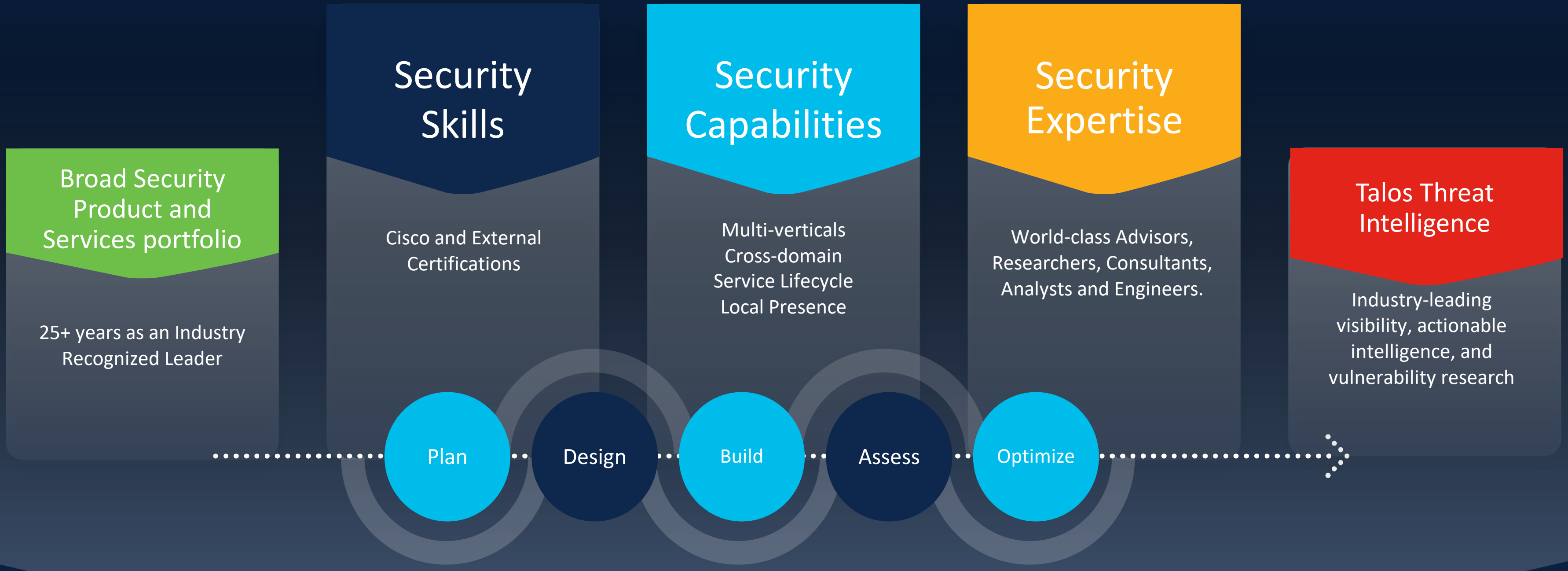
SIEM | TIP | SOAR | Collab

Consoles | VM | Forensics | Etc.

Data Lake

SOC Consumers

Why choose Cisco for Security Services ?



Broad Security Product and Services portfolio

25+ years as an Industry Recognized Leader

Security Skills

Cisco and External Certifications

Security Capabilities

Multi-verticals
Cross-domain
Service Lifecycle
Local Presence

Security Expertise

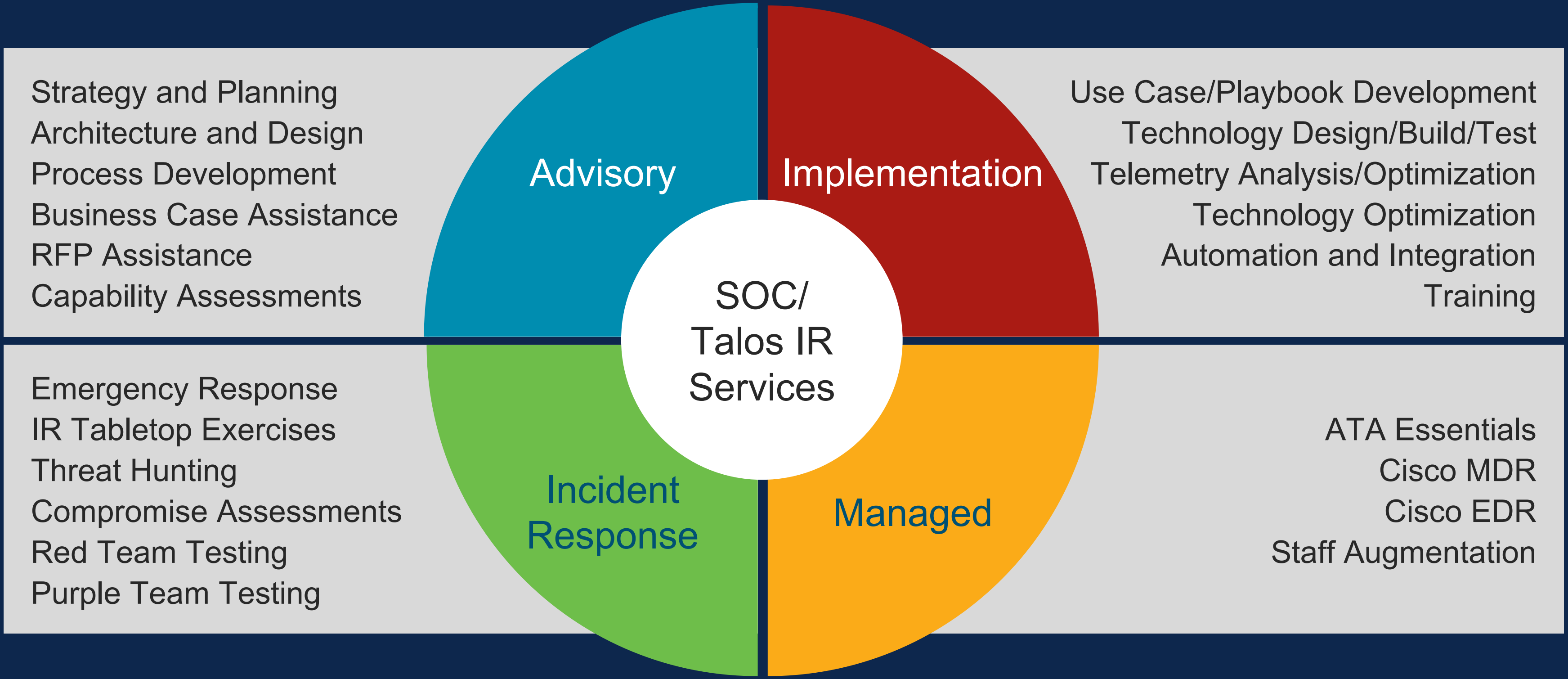
World-class Advisors, Researchers, Consultants, Analysts and Engineers.

Talos Threat Intelligence

Industry-leading visibility, actionable intelligence, and vulnerability research

Comprehensive services value throughout the lifecycle

How could Cisco help me with my SOC journey?



Strategy and Planning
Architecture and Design
Process Development
Business Case Assistance
RFP Assistance
Capability Assessments

Use Case/Playbook Development
Technology Design/Build/Test
Telemetry Analysis/Optimization
Technology Optimization
Automation and Integration
Training

Emergency Response
IR Tabletop Exercises
Threat Hunting
Compromise Assessments
Red Team Testing
Purple Team Testing

ATA Essentials
Cisco MDR
Cisco EDR
Staff Augmentation

Cisco Talos

Services

Intelligence Collection

Primary and secondary sources of threat intel

- Product telemetry
- Talos IR engagements
- Vulnerability research
- Intelligence partnerships
- Cutting-edge threat research
- Honeypots and spam traps

200+

Vulnerabilities discovered per year

60+

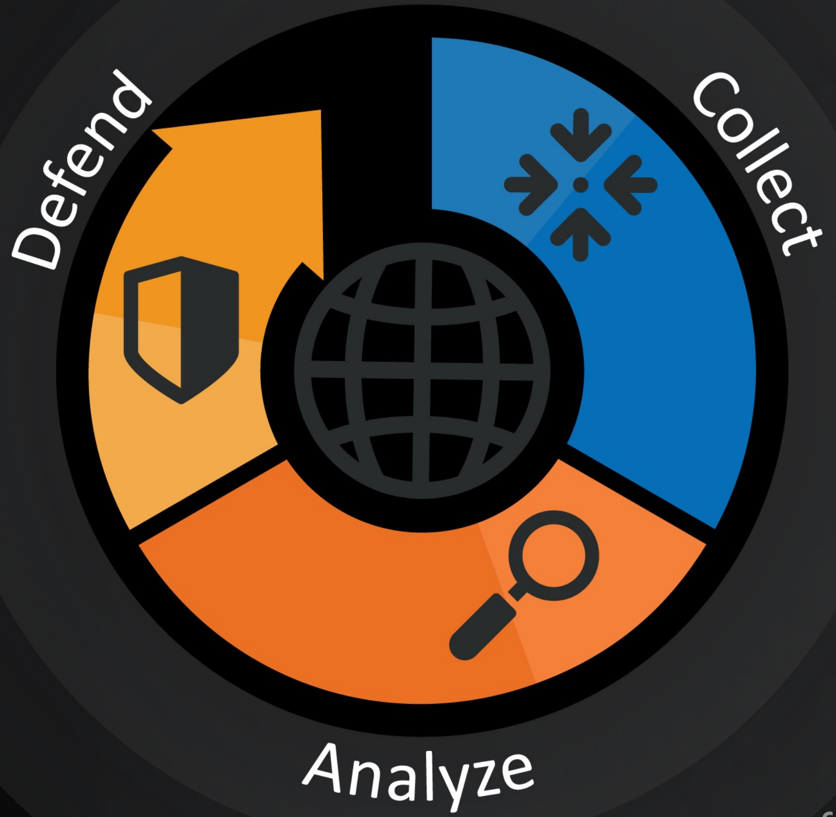
Government and law enforcement partnerships

45k

critical infrastructure endpoints monitored in Ukraine

Talos powers the Cisco portfolio with comprehensive intelligence

Every customer environment,
every event, every single day,
all around the world

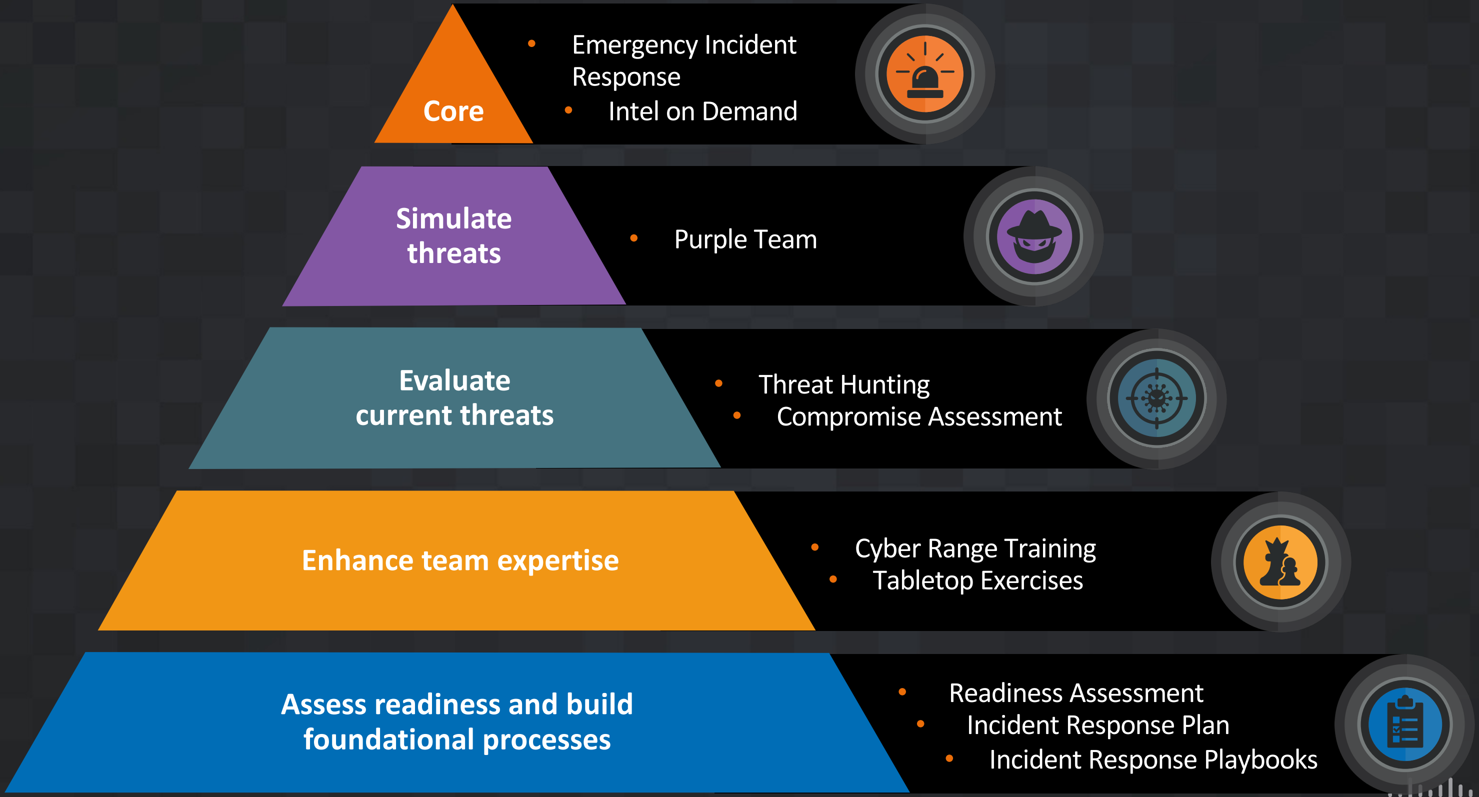


Cisco Talos Incident Response

Services overview

Talos Incident Response Retainer

Services to fortify your readiness and defense



Core

- Emergency Incident Response
- Intel on Demand

Simulate threats

- Purple Team

Evaluate current threats

- Threat Hunting
- Compromise Assessment

Enhance team expertise

- Cyber Range Training
- Tabletop Exercises

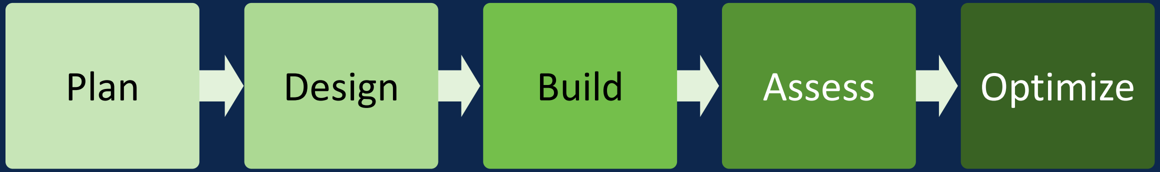
Assess readiness and build foundational processes

- Readiness Assessment
- Incident Response Plan
- Incident Response Playbooks

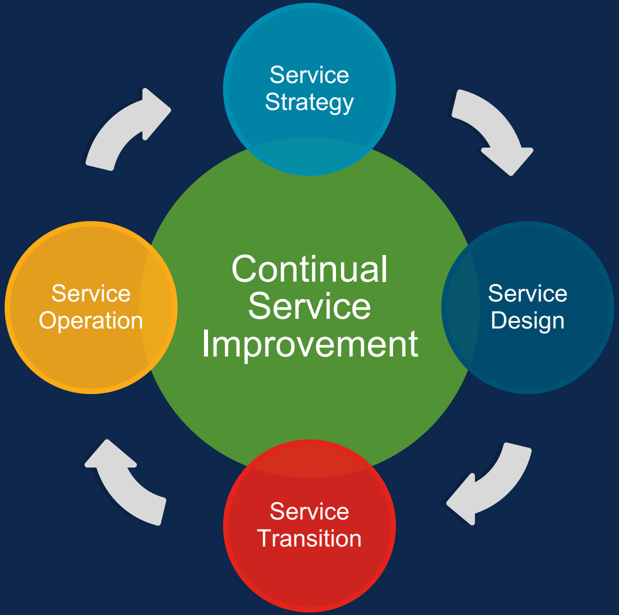
Cisco SOC

Advisory Services

Cisco SOC Advisory Services have a comprehensive portfolio of SOC Services covering all phases of the SOC lifecycle:



Cisco uses a top-down, services-oriented approach to develop new, or improve existing SOCs



The Run

Start

SOC Service Strategy

- Stakeholders -> Business alignment
- Drivers
- Services -> Subcomponents
- Operating model
- HL Organizational design
- Core Processes
- High Level Technology
- Align expectation to budget

Definition

SOC Service Design

- Benefit
- Trigger
- Input
- Output
- Process
- KPI
- Target C&M
- Responsibilities

Structure

SOC Governance & Organizational Design

- Organization
- Job Roles
- Define Customer / Consumer
- Reporting (who/when/what)
- Define cooperation (SLA / OLA)

Onboarding

Recruting

Process development

Playbooks & Use Case

Technical Design & Implementation

Learning & Delivery

Improve (Frameworks) TH, UC

Measure / Report

Explore System Environment

Communicate

Analyse (SLA &OLA / KPI)

Finish ?

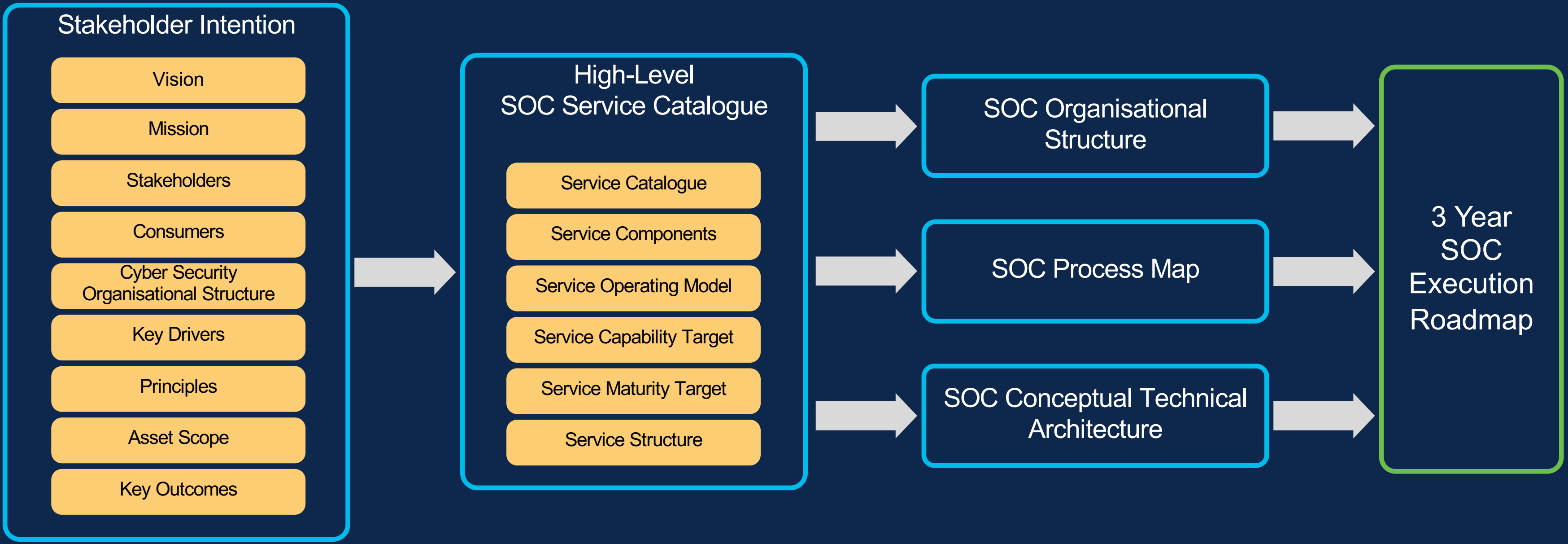
Back to Start (CSI)

Assessment

Adjust Roadmap

Automation

Components of SOC Strategy



Stakeholder Intention

- Vision
- Mission
- Stakeholders
- Consumers
- Cyber Security Organisational Structure
- Key Drivers
- Principles
- Asset Scope
- Key Outcomes

High-Level SOC Service Catalogue

- Service Catalogue
- Service Components
- Service Operating Model
- Service Capability Target
- Service Maturity Target
- Service Structure

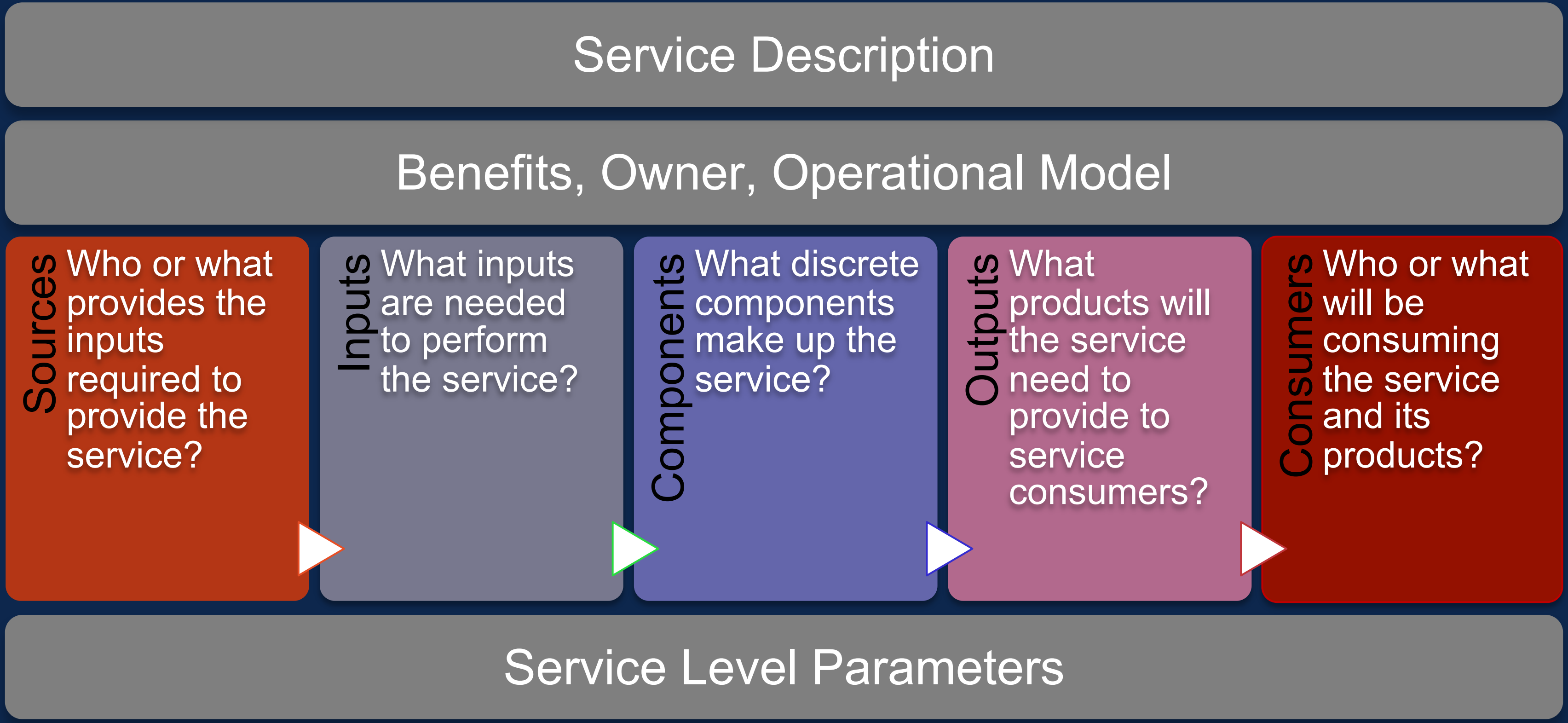
SOC Organisational Structure

SOC Process Map

SOC Conceptual Technical Architecture

3 Year SOC Execution Roadmap

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?

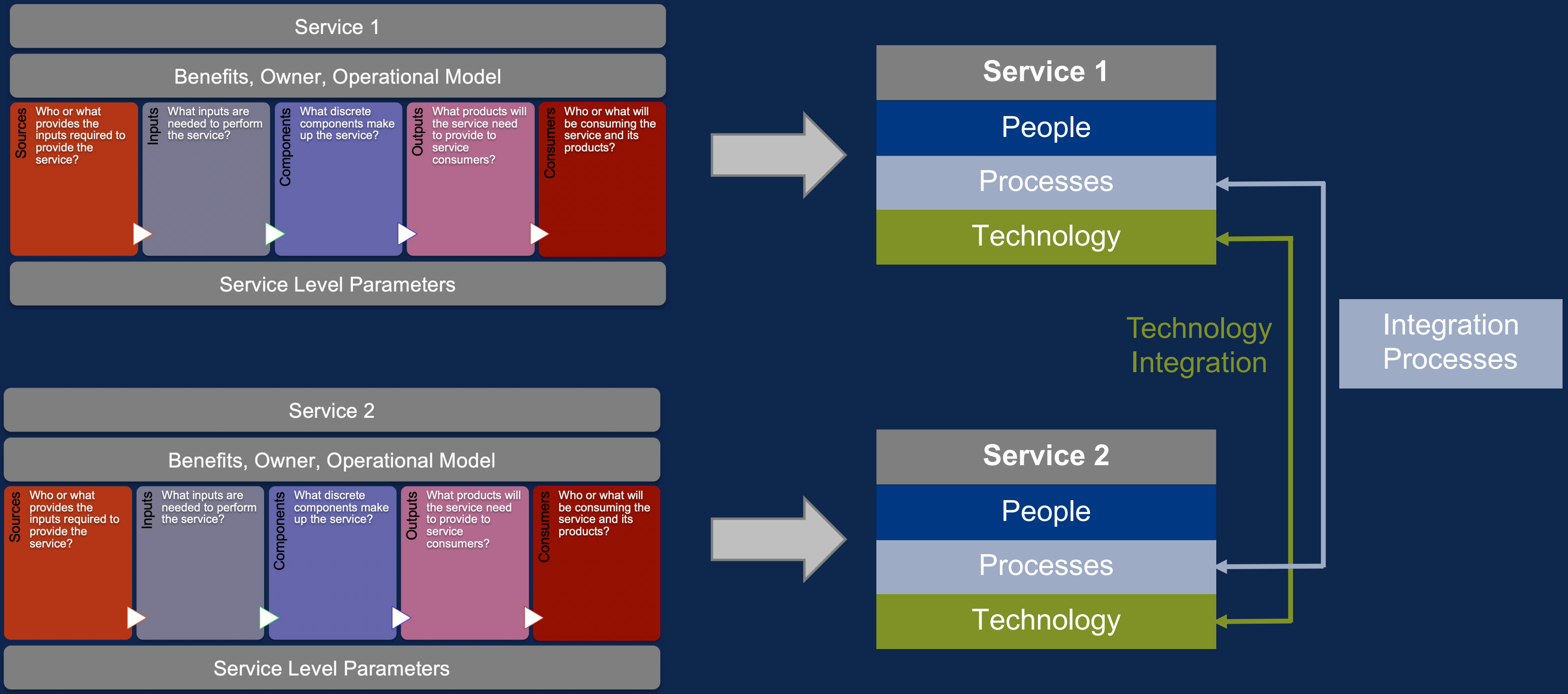
Components: What discrete components make up the service?

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, Process, 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

Case Study #1
Existing SOC – What Cisco Advisory Services can do for you here?

SOC Capabilities

Strategy & Governance

- SOC Strategy
- SOC Governance
- SOC Service Design
- SOC Financial Model

Architecture & Technology

- SOC Architecture
- SOC Telemetry
- SIEM/Security Analytics
- Security Automation & Orchestration
- Contextual Information
- Usecase Framework
- Threat Intelligence
- Metrics & Reporting

People & Organization

- Organization Structure, Roles, & Responsibilities
- Staffing
- Sourcing
- Training & Development

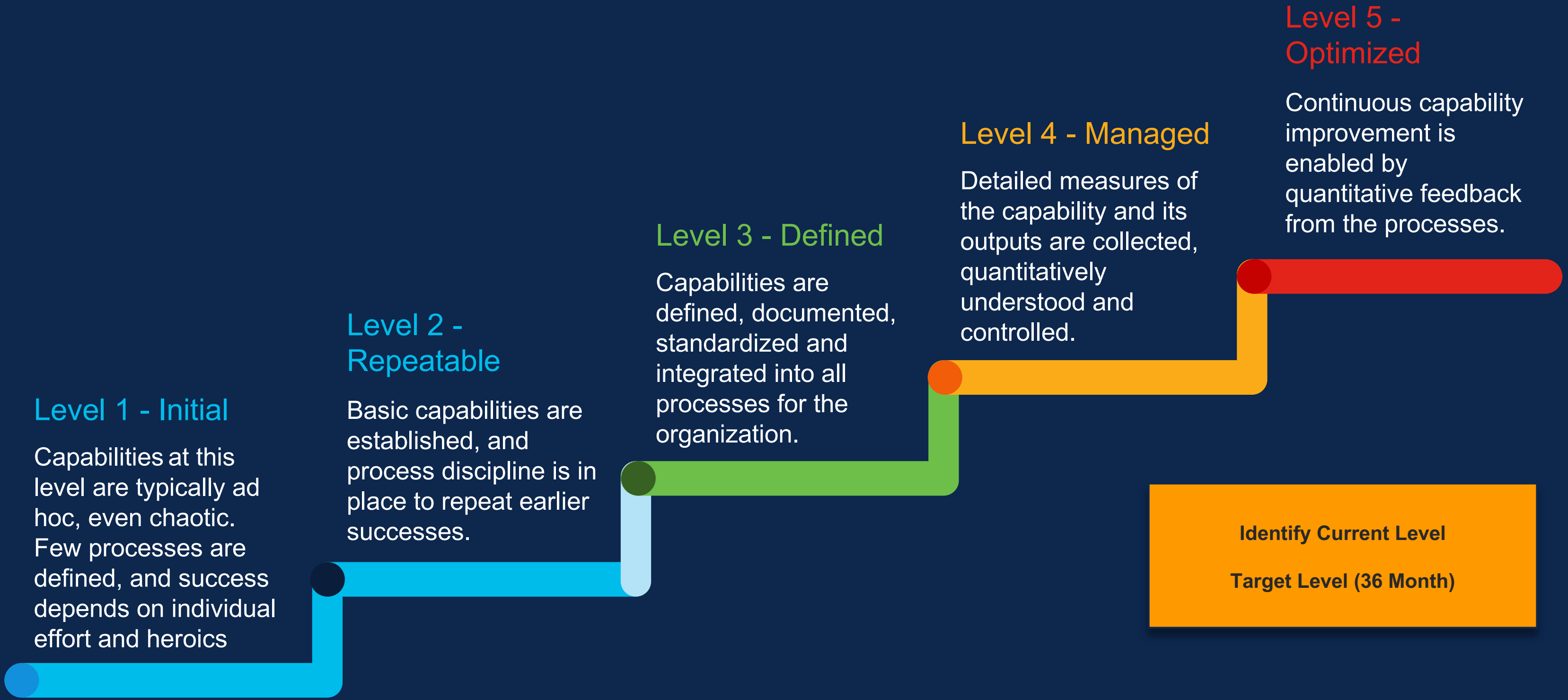
Process & Procedures

- Core SOC Processes
- Incident Playbooks
- Process Integration

SOC Services

- Security Monitoring
- Analysis & Investigation
- Incident Remediation
- Threat Intelligence
- Threat Hunting
- Platform Management
- Services Management

SOC Maturity Assessment - CMMI



Level 1 - Initial

Capabilities at this level are typically ad hoc, even chaotic. Few processes are defined, and success depends on individual effort and heroics

Level 2 - Repeatable

Basic capabilities are established, and process discipline is in place to repeat earlier successes.

Level 3 - Defined

Capabilities are defined, documented, standardized and integrated into all processes for the organization.

Level 4 - Managed

Detailed measures of the capability and its outputs are collected, quantitatively understood and controlled.

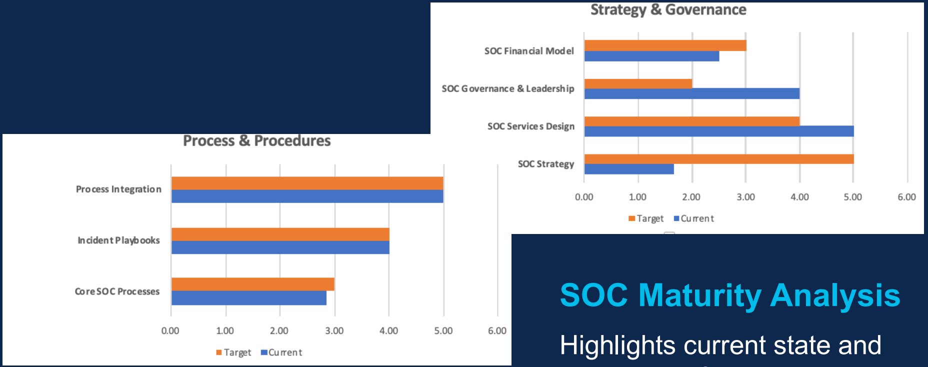
Level 5 - Optimized

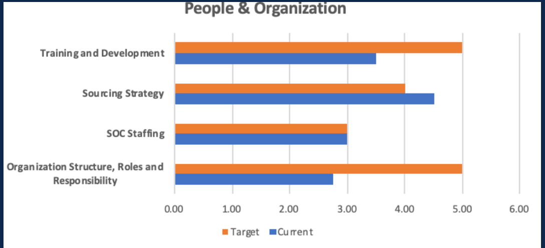
Continuous capability improvement is enabled by quantitative feedback from the processes.

Identify Current Level

Target Level (36 Month)

SOC Maturity Assessment – Output



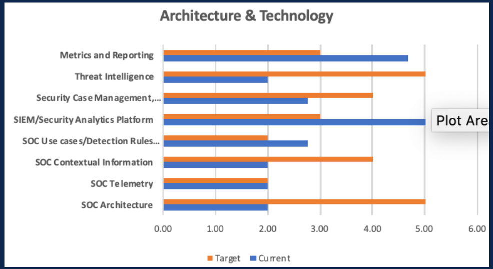


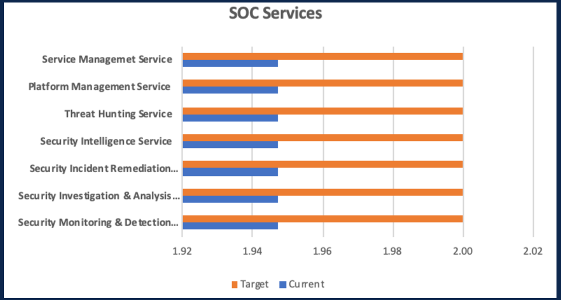
SOC Gap Assessment Report

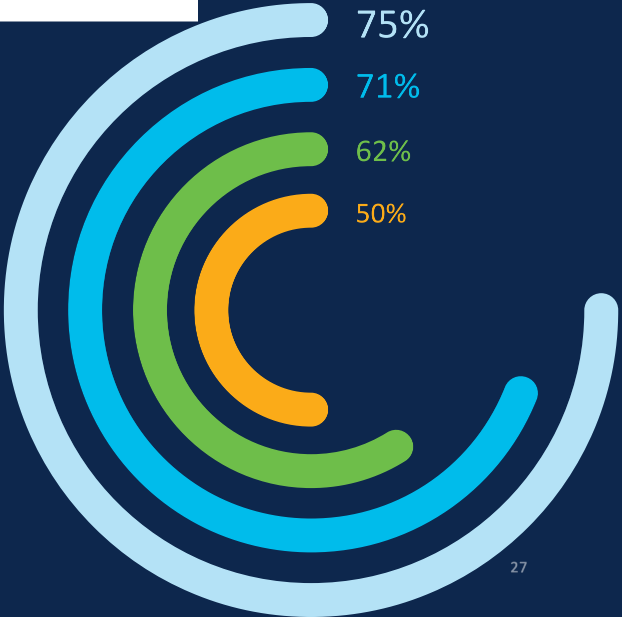
Highlights Key Findings & Recommendations to reach Target

SOC Maturity Analysis

Highlights current state and target state for individual capabilities/Domains





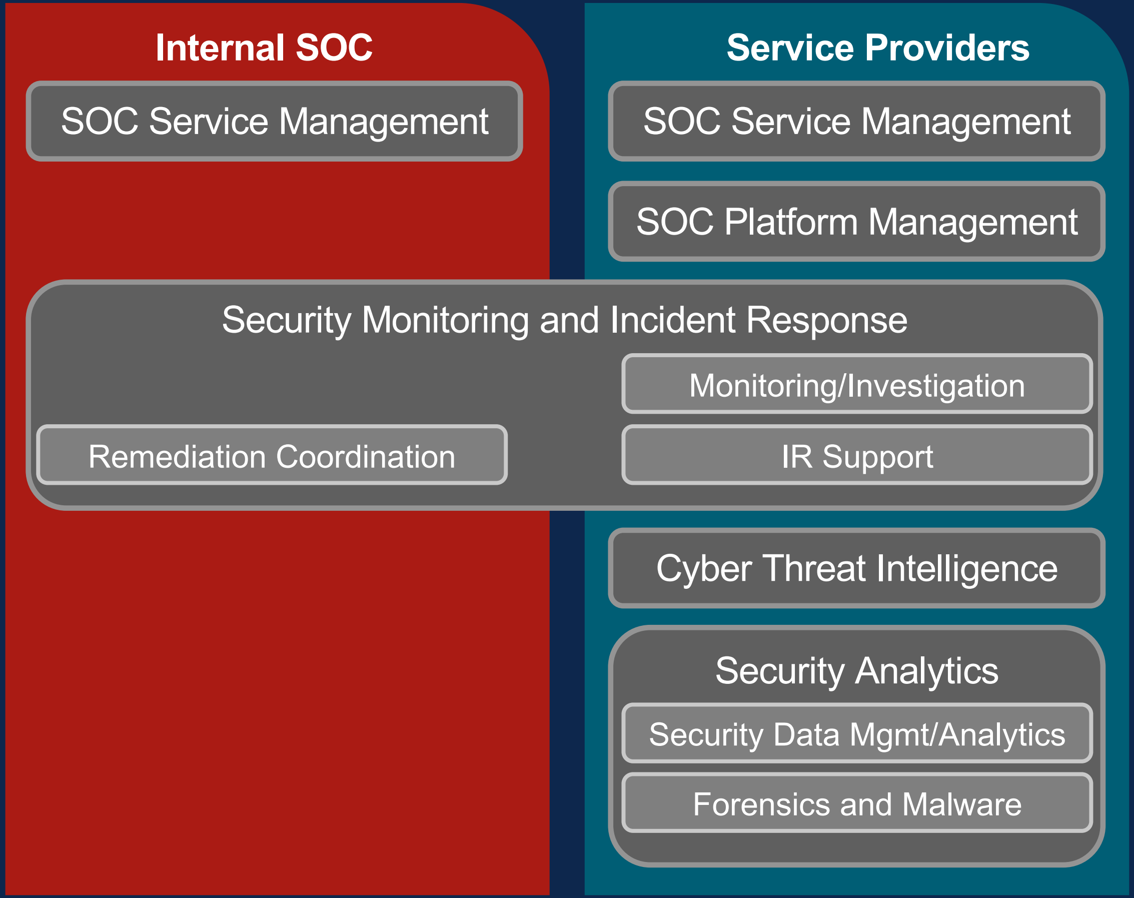


Case Study #2
Green Field SOC – predominantly outsourced SOC – Cloud Delivered

Operational Model: Predominantly Outsourced

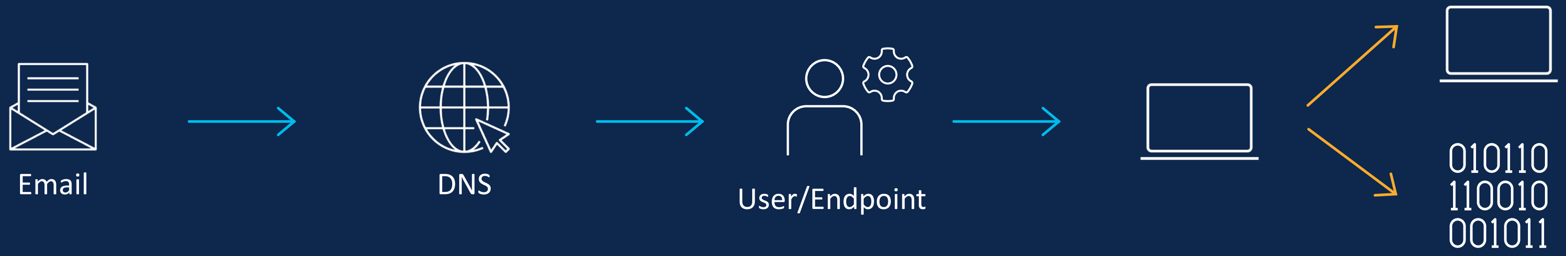
Core outsourced services provided by service providers

Supplementary services provided by internal operational resources



Sample Technology stack based on Cisco Products

Most attacks use a sequence like this…



You need a solution that sees deeply across the entire attack chain

Cisco XDR

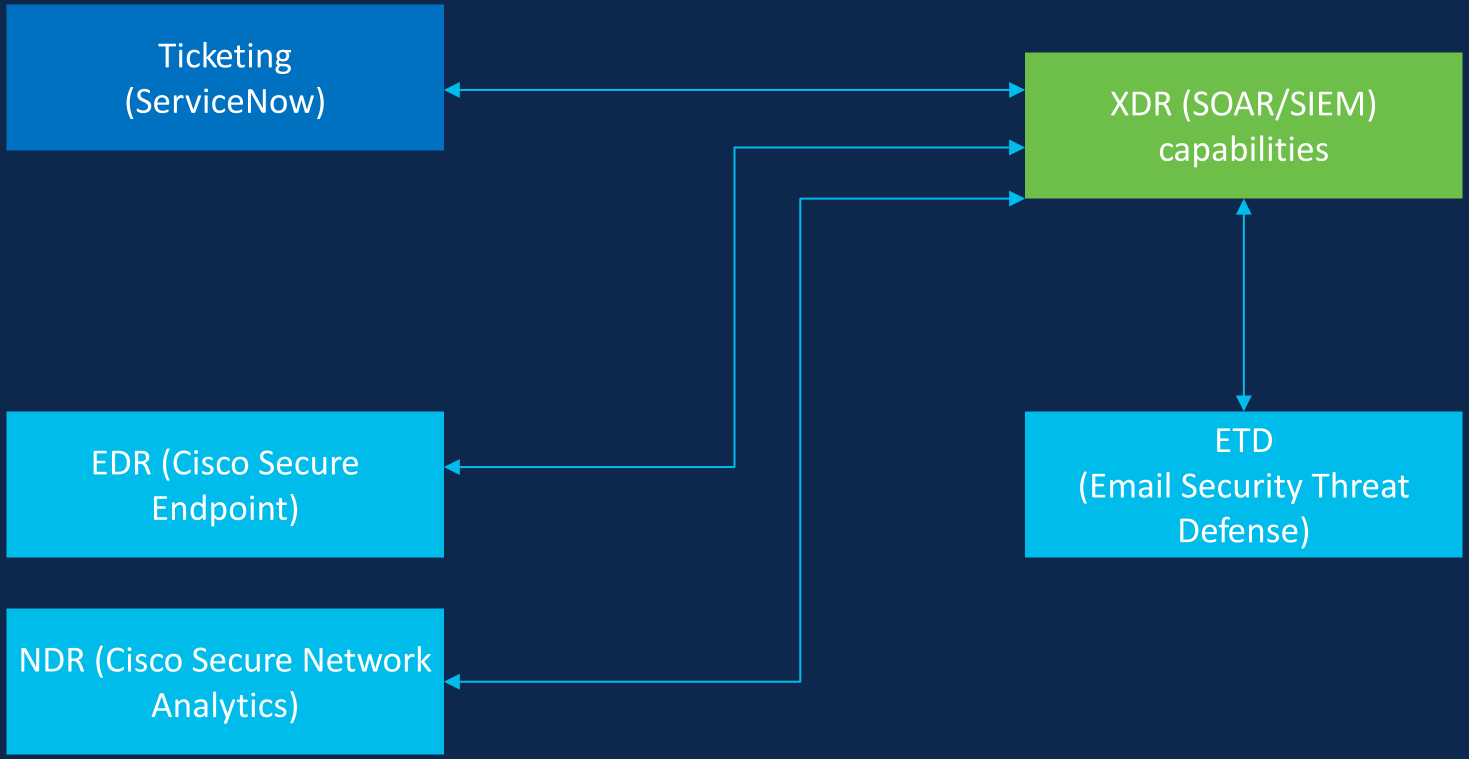
Built on the Cisco Security Cloud platform

Cisco Breach Protection

Extended Detection & Response

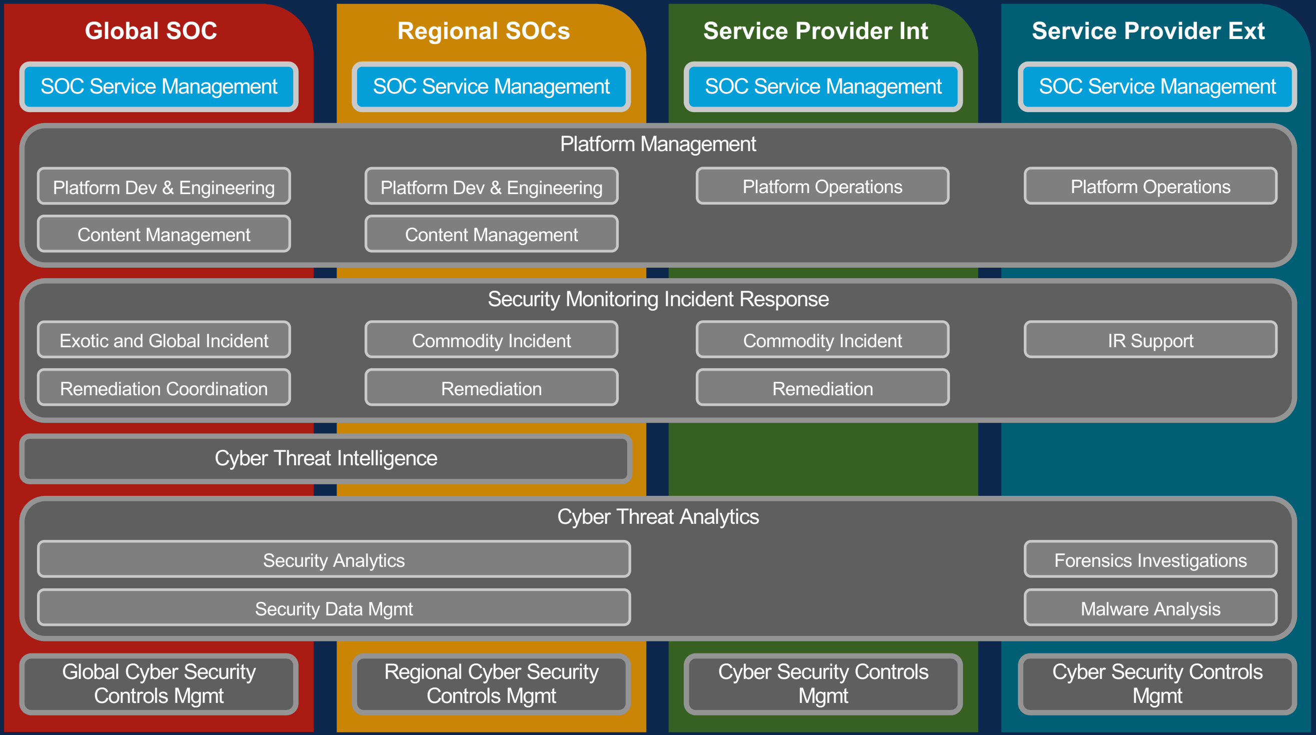
Ransomware Recovery

Premier	All features in Advantage	Managed extended detection & response (MXDR) delivered by Cisco CX
Advantage	All features in Essentials	Integrations with extensive list of third-party tools
Essentials	Native integration of full Cisco security portfolio	Talos and third-party threat intelligence enrichment


Ticketing (ServiceNow)
XDR (SOAR/SIEM) capabilities
EDR (Cisco Secure Endpoint)
ETD (Email Security Threat Defense)
NDR (Cisco Secure Network Analytics)

Case Study #3
Green Field Inhouse SOC (Internal MDR) – On-prem Delivered

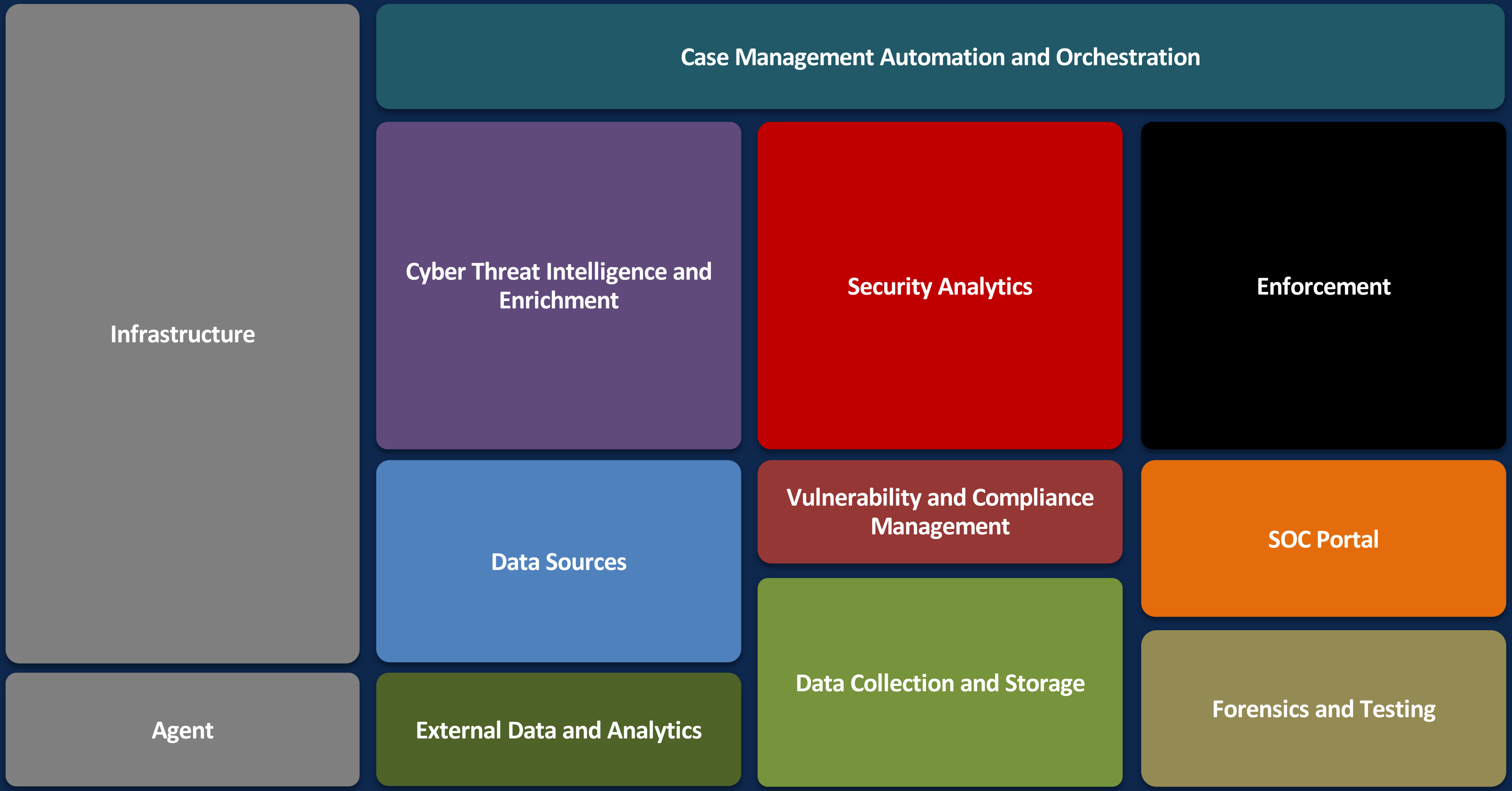
Operational Model: Federated Model



Services federated between central/regional SOCs, as well as internal and external service providers

Cisco SOC

Implementation Services



Infrastructure

Agent

Case Management Automation and Orchestration

Cyber Threat Intelligence and Enrichment

Security Analytics

Enforcement

Data Sources

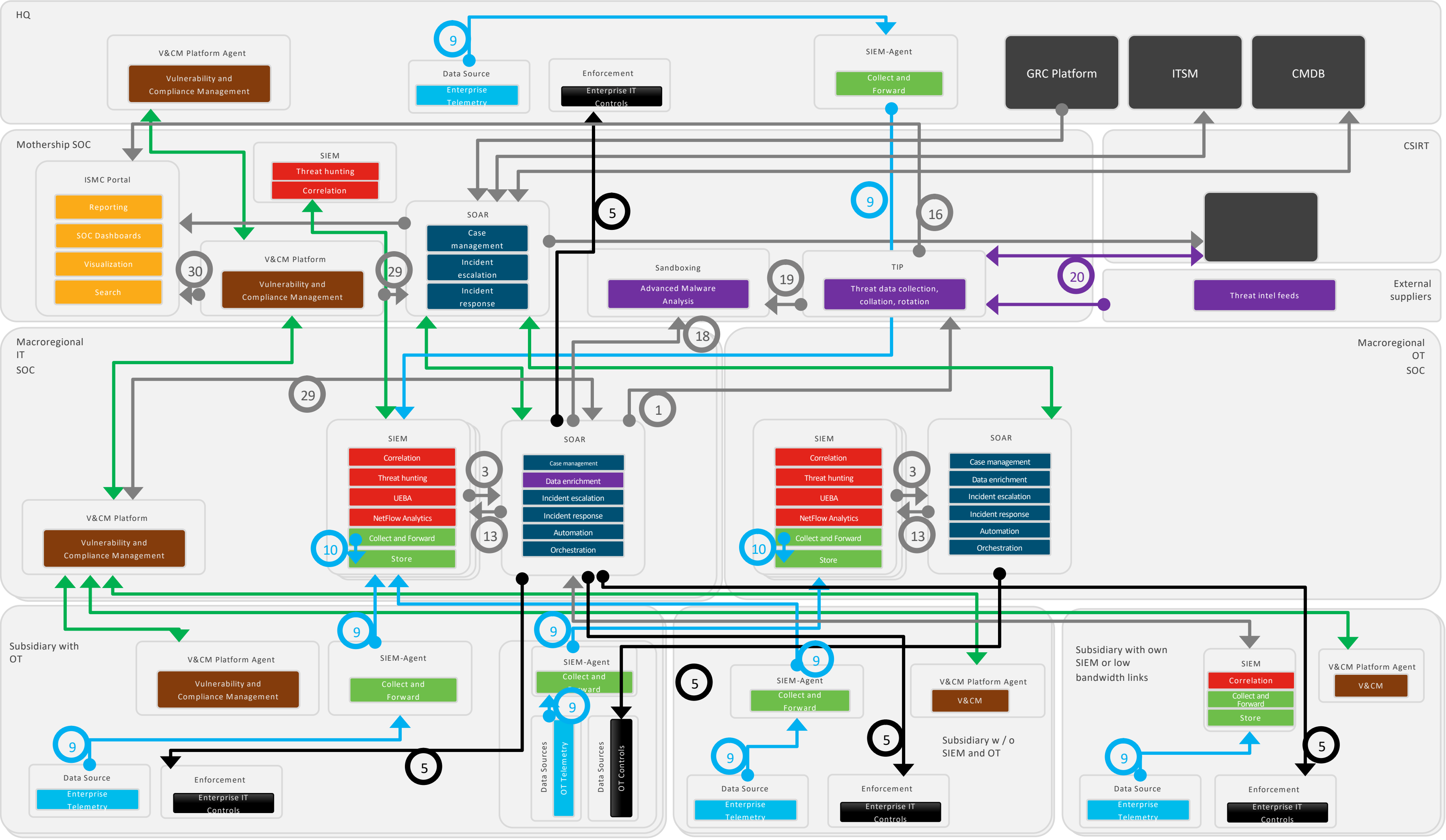
External Data and Analytics

Vulnerability and Compliance Management

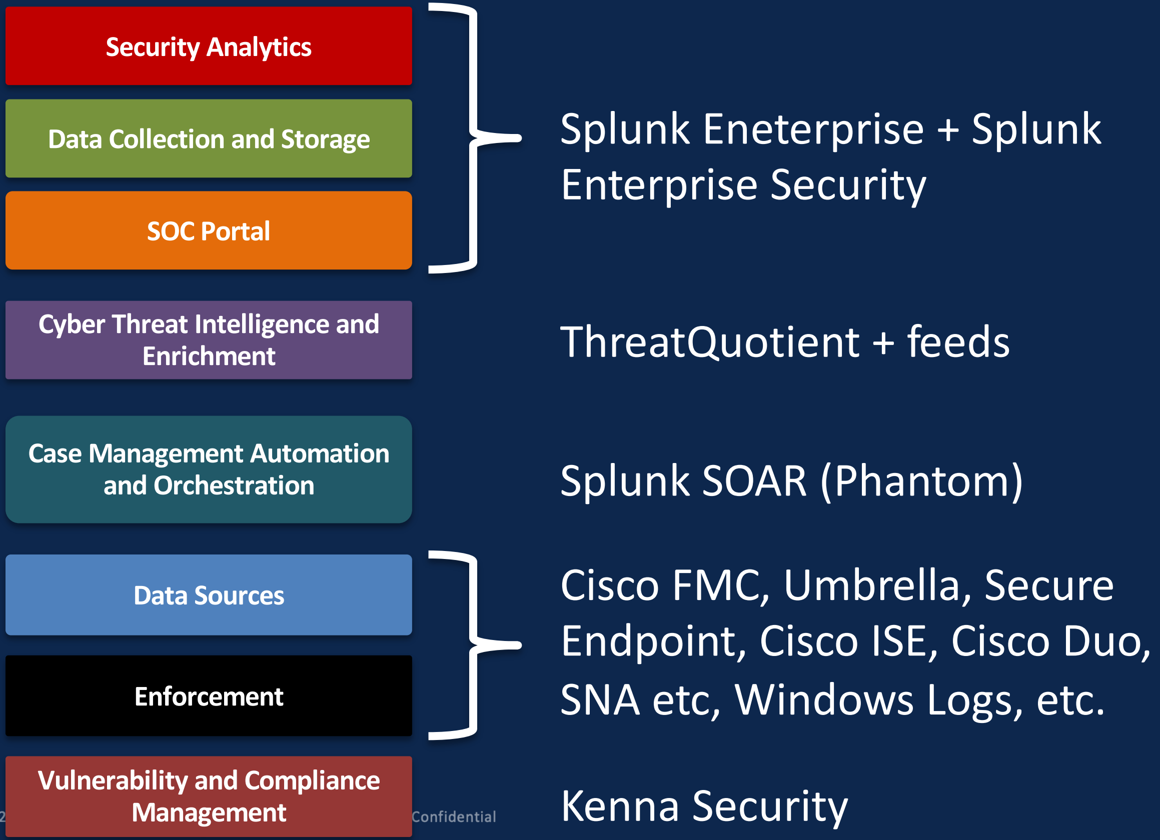
Data Collection and Storage

SOC Portal

Forensics and Testing


HQ
V&CM Platform Agent
Vulnerability and Compliance Management
9
Data Source
Enterprise Telemetry
Enforcement
Enterprise IT Controls
SIEM-Agent
Collect and Forward
GRC Platform
ITSM
CMDB
Mothership SOC
CSIRT
ISMC Portal
Reporting
SOC Dashboards
Visualization
Search
SIEM
Threat hunting
Correlation
SOAR
Case management
Incident escalation
Incident response
V&CM Platform
Vulnerability and Compliance Management
30
29
5
9
16
Sandboxing
Advanced Malware Analysis
19
TIP
Threat data collection, collation, rotation
20
Threat intel feeds
External suppliers
18
Macroregional IT SOC
Macroregional OT SOC
29
1
SIEM
Correlation
Threat hunting
UEBA
NetFlow Analytics
Collect and Forward
Store
10
3
13
SOAR
Case management
Data enrichment
Incident escalation
Incident response
Automation
Orchestration
SIEM
Correlation
Threat hunting
UEBA
NetFlow Analytics
Collect and Forward
Store
10
3
13
SOAR
Case management
Data enrichment
Incident escalation
Incident response
Automation
Orchestration
V&CM Platform
Vulnerability and Compliance Management
Subsidiary with OT
V&CM Platform Agent
Vulnerability and Compliance Management
9
SIEM-Agent
Collect and Forward
9
SIEM-Agent
Collect and Forward
9
Data Sources
OT Telemetry
Data Sources
OT Controls
5
9
Data Source
Enterprise Telemetry
Enforcement
Enterprise IT Controls
5
9
SIEM-Agent
Collect and Forward
V&CM Platform Agent
V&CM
9
Data Source
Enterprise Telemetry
5
Enforcement
Enterprise IT Controls
Subsidiary w / o SIEM and OT
Subsidiary with own SIEM or low bandwidth links
SIEM
Correlation
Collect and Forward
Store
V&CM Platform Agent
V&CM
9
Data Source
Enterprise Telemetry
5
Enforcement
Enterprise IT Controls

Services to technology mapping



Security Analytics

Data Collection and Storage

SOC Portal

Splunk Eneterprise + Splunk Enterprise Security

Cyber Threat Intelligence and Enrichment

ThreatQuotient + feeds

Case Management Automation and Orchestration

Splunk SOAR (Phantom)

Data Sources

Enforcement

Cisco FMC, Umbrella, Secure Endpoint, Cisco ISE, Cisco Duo, SNA etc, Windows Logs, etc.

Vulnerability and Compliance Management

Kenna Security

Splunk Chapter

Splunk Security

Differentiation

Scalable Platform

Gain visibility into hidden risks and attacks to identify the root cause of threats faster with Splunk's platform powered with AI capabilities.

Detection Power

Prioritize risk with RBA for a 50% reduction in false positives & access 1,500+ out-of-the-box detections crafted by industry experts.

Industry Leadership

Analyst recognized history of industry leadership in security operations across Gartner, IDC and Forrester.

Partners & Apps

Leverage a network of 2,200+ global security partners and 2,800+ partner and community-built apps to build a solution for any use case.

The Splunk Community

Solve problems faster with Splunk’s vast user community of 250,000 forum users addressing 57,000 questions per month to tackle any security challenge.

Apps & Add-ons

Built for Splunk Enterprise Security Users

Splunk ES Content Update (ESCU)

provides 1,500+ pre-built security detections as pre-packaged Security Content Library updates to help security practitioners address ongoing time-sensitive threats, attack methods, and other security issues.

Splunk App for PCI Compliance

provides a top-down and bottom-up view of your organization's current PCI compliance status to monitor, investigate, and report on compliance with Payment Card Industry Data Security Standards (PCI DSS).

Splunk App for Fraud Analytics

is an anti-fraud solution that uses the detection and investigation power of Splunk Enterprise Security (ES) and Risk Based Alerting to improve alert fidelity and your anti-fraud strategy.

OT Security Add-on for Splunk

enables organizations that operate assets, networks, and facilities across both IT and OT environments to to improve threat detection, incident investigation, and response.

Apps & Add-ons

Built for Splunk Platform Users

- **Splunk Security Essentials (SSE)** allows you to browse, bookmark and deploy ESCU analytic stories from the Security Content Library with just a few clicks to enhance searches in your Splunk environment. Also provides automatic mapping of data and security detections to the MITRE ATT&CK® and Cyber Kill Chain® frameworks.

- **Compliance Essentials for Splunk** streamlines continuous monitoring efforts, improves cybersecurity posture, and addresses the requirements of different National Institute of Standards and Technology (NIST)-based control frameworks, including the following: Risk Management Framework (RMF), Cybersecurity Maturity Model Certification (CMMC), Defense Federal Acquisition Regulation Supplement (DFARS) and the Office of Management (OMB) M-21-31 MEMORANDUM.

- **InfoSec App for Splunk** relies on accelerated data models and the Common Information Model (CIM) to provide a consistent and normalized view into the event data that you'll bring into Splunk. This app can help you address basic security use cases, including monitoring and security investigations.

- **The Splunk AI Assistant*** makes SPL more accessible, enabling users to create SPL queries from plain English, and view plain English explanations of any well-formed SPL searches. **The Splunk AI Assistant is available as a preview and is not officially supported.*

- **Splunk Mobile App** allows users to access your Splunk data anywhere at any time. Get notified with actionable alerts and make decisions faster with dashboards and reports at your fingertips.

- **Splunk Machine Learning Toolkit** helps you apply a variety of machine-learning techniques and methods, such as classification (predicting a yay or nay), regression, anomaly detection, and outlier detection against your data. In v5.4 or higher you can upload pre-trained ONNX models for inferencing in MLTK.

- **Splunk Security for SAP Solutions** Splunk Security for SAP solutions, an SAP Endorsed App, helps organizations reduce business risk by protecting SAP applications and data with Splunk.

CISCO

The bridge to possible