



The bridge to possible

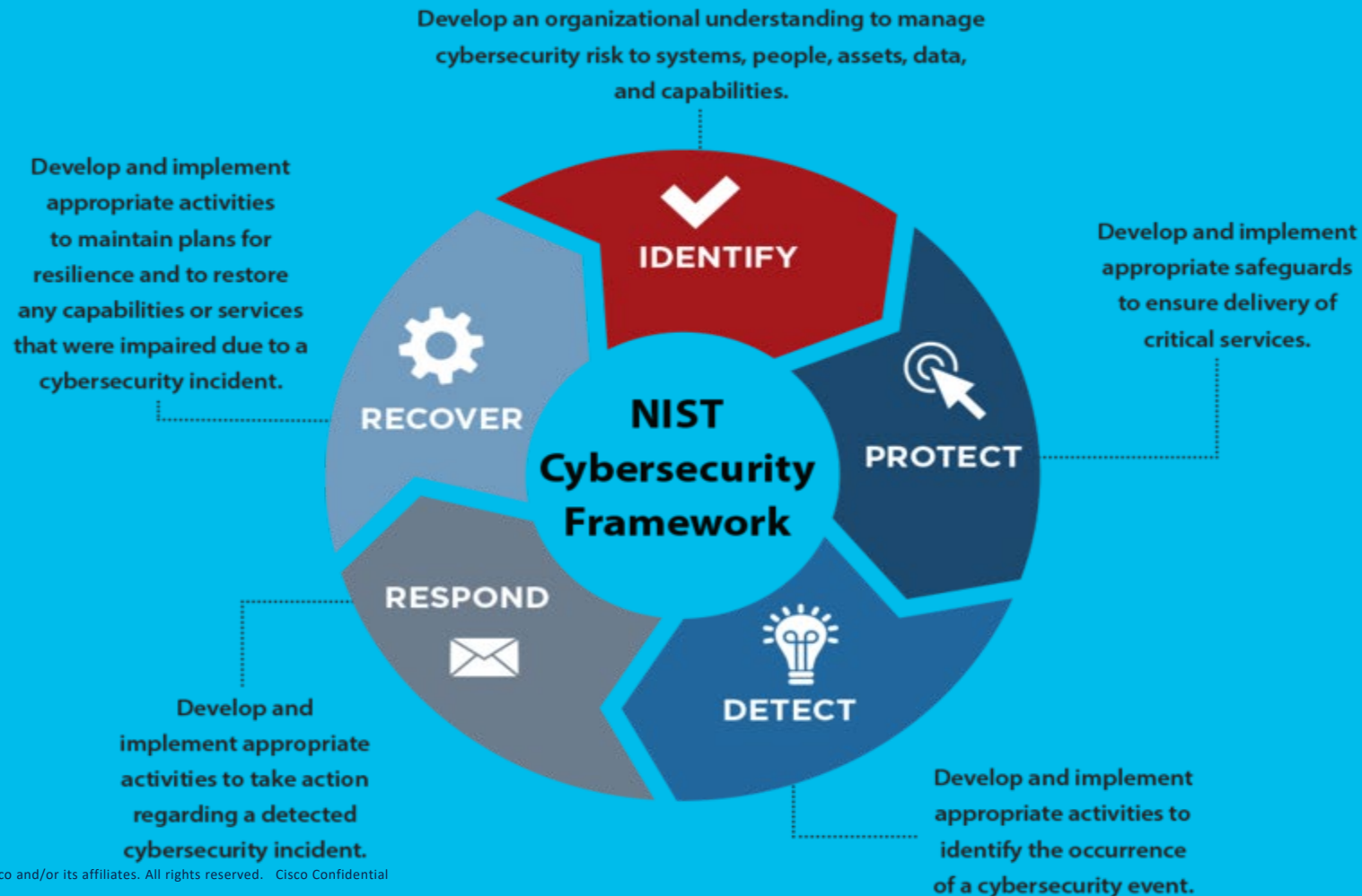
Security Services

Georgia Politopoulou

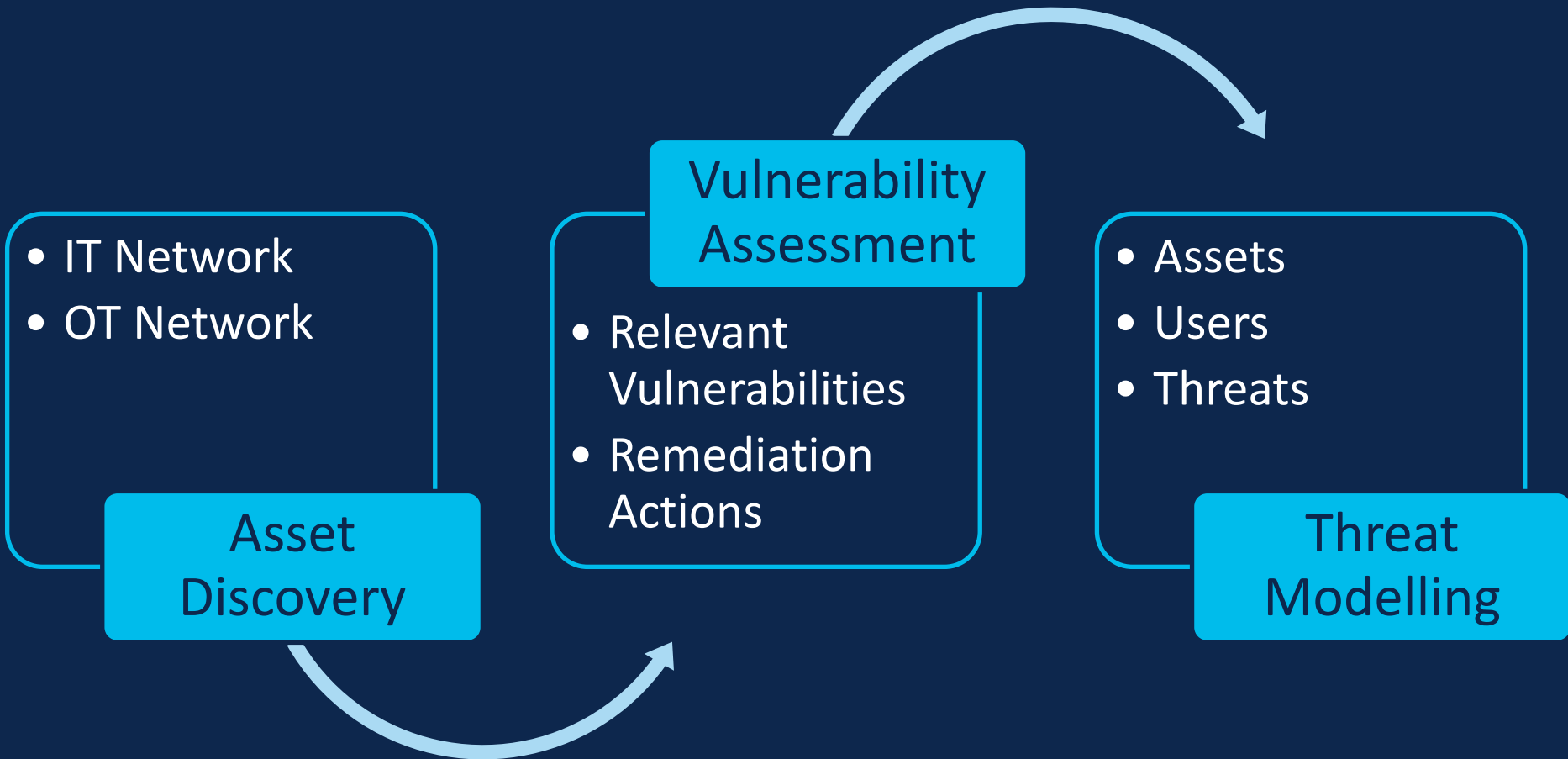
Business Development Manager

Agenta

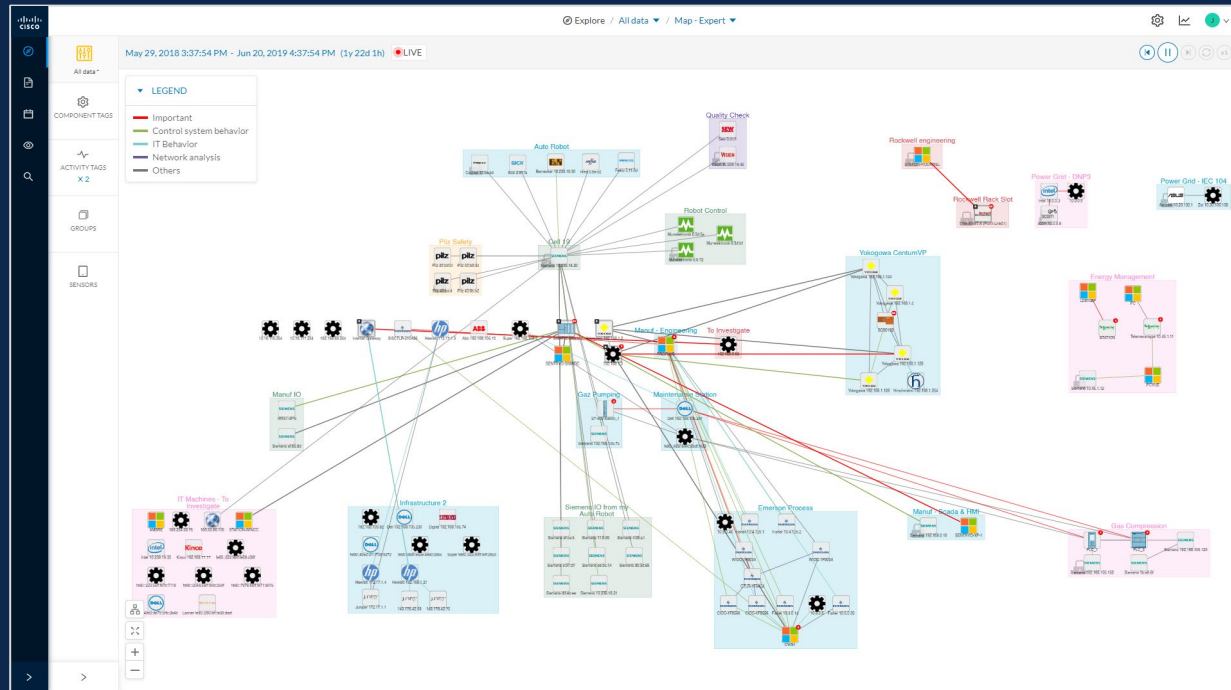
- Introduction to NIST framework
- Identify services
- Protect Services
- Detect, Respond & Recover Services



Identify



Communication | Map application flows



Visibility | Comprehensive asset inventory

Explore / All data / Component list

May 29, 2018 3:16:34 PM - Jun 20, 2019 4:16:34 PM (1y 22d 1h) LIVE


66 Components

1 2 3 4 > 20 / page

Component	Group	First activity	Last activity	IP	MAC	Tags	Flows	Vuln	Var	Vendor	OS
Dell 192.168.105.241	Maintenance Station	Apr 6, 2017 10:59:14 PM	Jun 18, 2019 12:23:34 AM	-	34:17ebd1c9:97	Read Var., Write Var., Engineering Station, Remote access	579	0	0	Dell Inc.	-
149.178.42.70	Infrastructure 2	Oct 5, 2017 6:03:16 PM	Jun 18, 2019 12:23:34 AM	-	2c:6bdf562a7:80	DNS Server, Public IP	38	0	0	Juniper Networks	-
232.108.116.118	-	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:34 AM	-	01:00:5e6c74:76	Multicast, Public IP	8	0	0	-	-
AMBRE	IT Machines - To Investigate	Apr 6, 2017 10:58:58 PM	Jun 18, 2019 12:23:34 AM	-	00:24:9b08:43:6f	Windows	7	0	0	Action Star Enterprise Co., Ltd.	-
10.16.116.254	-	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:34 AM	-	00:22e5c210a:86	Read Var., Write Var., Wireless IO Module, DeltaV	44	0	225	-	-
SIMATIC 300(1)	-	Apr 6, 2017 11:29:22 PM	Jun 18, 2019 12:23:34 AM	192.168.0.1	00:0e8c845b:a6	Read Var., PLC	25	10	13	Siemens AG A&D ET	-
10.8.0.6	-	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:34 AM	-	84:8f69e1a3:7b	Read Var., DNS Server, Time Server, Windows, DeltaV	16099	3	4	-	-
OWS1	Emerson Process	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:34 AM	-	d4:ae52aa:dc93	Read Var., Write Var., Windows, DeltaV	16071	3	113	Dell Inc.	Windows 7 or Windows Server 2008
239.192.24.4	-	Oct 5, 2017 6:03:14 PM	Jun 18, 2019 12:23:34 AM	239.192.24.4	01:00:5e40:18:04	Multicast, Public IP	17	0	0	-	-
Hirschmann 192.168.1.254	Yokogawa CentumVP	Oct 5, 2017 6:03:14 PM	Jun 18, 2019 12:23:34 AM	192.168.1.254	ec:74ba03:98:6b	Time Server	4	0	0	Hirschmann Automation and Control GmbH	-
Fisher 10.4.0.14	Emerson Process	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:34 AM	10.4.0.14	00:22e5c1f9a:54	Read Var., Write Var	35	0	16	Fisher-Rosemount Systems Inc.	-
WIOC-1F03A	Emerson Process	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:34 AM	10.5.0.22	00:22e5c1f90:18	Read Var., Write Var., DeltaV	41	0	28	Fisher-Rosemount Systems Inc.	-
IP02:1fff:b3b4b	-	Apr 6, 2017 10:59:14 PM	Jun 18, 2019 12:23:34 AM	IP02:1fff:b3b4b	33:33fff:b3b4b	Multicast, Public IP	2	0	0	IPv6 Multicast	-
IM151-3PN	Manuf IO	Apr 6, 2017 11:29:22 PM	Jun 18, 2019 12:23:34 AM	192.168.0.2	08:00:06:6b7f:16	IO Module	6	0	0	SIEMENS AG	-

Anomaly | List vulnerability identification

Component

**SIMATIC 300(1)**
IP: 192.168.0.1
MAC: 00:0e:8c:84:5b:a6

First activity
Apr 6, 2017 11:29:22 PM

Last activity
Jun 20, 2019 12:22:18 AM

Read Var

PLC

24
Flows

51
Events

13
Variables

Vulnerabilities

5

Basics

Security

Activity

Automation

Vulnerabilities

Credentials

Vulnerabilities

5

☐ **Multiple Siemens Products CVE-2017-12741 Denial of Service Vulnerability**
CVE-2017-12741
Several Industrial products are affected by a vulnerability that could allow remote attackers to conduct a Denial-of-Service (DoS) attack.
Solution
Siemens has released updates for several affected products, and recommends that customers update to the new version. Siemens is preparing further updates and recommends specific countermeasures until patches are available.
Published on November 23, 2017
Identified on this component on April 6, 2017
Identified vulnerable because of model-ref (6ES7 315-2EH13-0AB0)
Links
[Siemens Security Advisory](#)

☐ **SIMATIC S7-300 and S7-400 CPUs Denial of Service and Information Disclosure Vulnerabilities**
CVE-2016-9158
Successful exploitation of these vulnerabilities could lead to a denial-of-service condition or result in credential disclosure.
Solution
Siemens provides firmware version V3.X.14 for S7-300 CPUs that resolves CVE-2016-9158.
Published on December 16, 2016
Identified on this component on April 6, 2017
Identified vulnerable because of model-ref (6ES7 315-2EH13-0AB0)
Links
[www.siemens.com](#)
[ics-cert.us-cert.gov](#)
[www.securityfocus.com](#)

☒ **Multiple Denial of Service Vulnerabilities on Siemens devices using the PROFINET Discovery and**

7.8
score CVSS
Access Vector: Network
Access Complexity: Low
Authentication: None Required
Confidentiality Impact: None
Integrity Impact: None
Availability Impact: complete
Acknowledge ?

Explain why OK

7.8
score CVSS
Access Vector: Network
Access Complexity: Low
Authentication: None Required
Confidentiality Impact: None
Integrity Impact: None
Availability Impact: complete
Acknowledge ?

Explain why OK

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

8

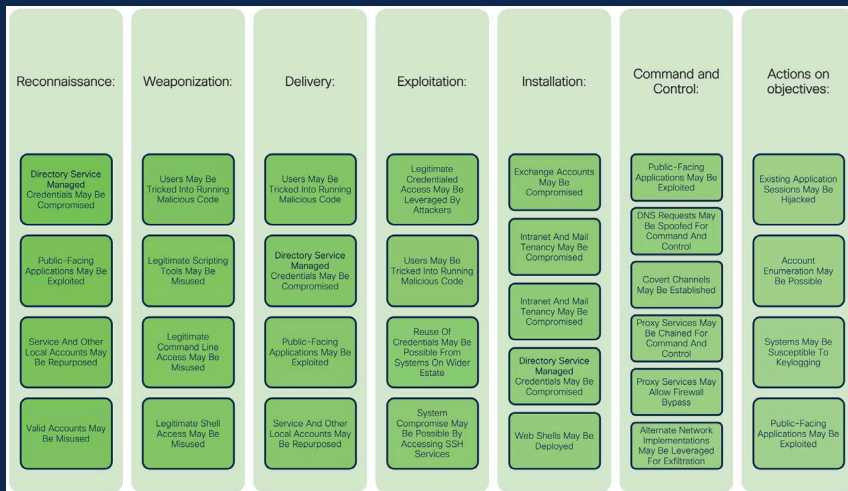
Threat Modelling

Start from business lead threats, and then translate into specific scenarios from which offensive and defensive use cases can be derived.

Cisco will work with your key stakeholders to identify business threats, tools and tactics of threats actors that are likely to target your business and compliance and risk visibility requirements.

In each scenario, Cisco will define the attack path, the data sources needed, the priorities, the actions that should be taken as well as any other required items.

Outcome will be a Threat profile for your organization that allows better targeting for in security investments



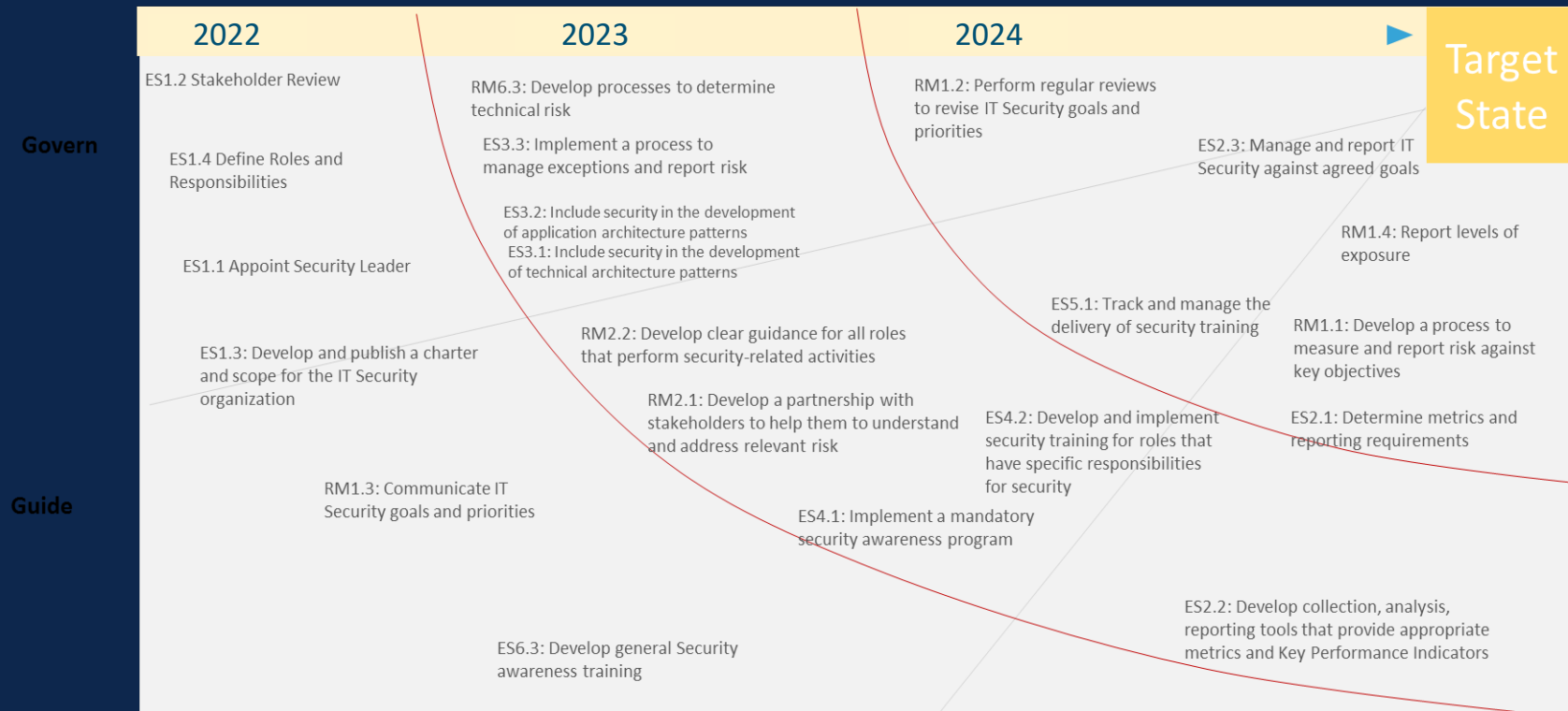
Example Scenarios

Initial Access	Foothold Achieved	Route	Pre-access Controls	Impact	Post-access Controls
Supply Chain Compromise	Authenticated 3 rd party VPN access	Unsecured Credentials	To discuss	Ability to access systems that they support	To discuss
Phishing	Authenticated access to management plane	Exploitation for Credential Access	To discuss	Manipulation of BGP or DNS service configuration	To discuss
Exploit Public Facing Application	Code execution on middleware or backend services	OS Credential Dumping	To discuss	Theft and modification of customer data	To discuss

Cyber Security Program Assessment

		Strategy (People)				Operations (Process)				Tactical (Technology)			
		Executive Management				Cybersecurity Intelligence				IT Risk Management			
		Cybersecurity Responsibility Charter & Governance				Cybersecurity Management Program Requirements				Cybersecurity & IT Assurance			
		Cybersecurity Management Program, Metrics & Reporting				Risk Management Program							
		Cybersecurity Architecture Strategy & Management				User Account, Solution Provisioning / Deployment				Cybersecurity Incident Response			
		Cybersecurity Education / Awareness Training				Regulatory & Internal Compliance Management							
Maturity Level Key	Level 0 Absent	Activity Log Management				Business Continuity & Disaster Recovery				Archiving & Records Management			
	Level 1 Initial	Threat / Activity Correlation & Analysis				Configuration & Patch Management				Vendor & 3 rd Party Management			
	Level 2 Managed	HR / Personnel Support				Vulnerability Management				Asset Management			
	Level 3 Defined	Legal Team Support				Application Development / Management							
	Level 4 Q. Managed	Physical Security Team Support				Asset Classification							
		Crisis Management Team Support				Identity & Access Management							
										Secure System			
										Secure Network			
										Secure Applications			
										Secure Network Topology			
										Network Segmentation / Zone Security			
										Secure Provisioning Capability			
										Mobile, Remote, BYOD & 3 rd Party Network Design			
										Data Privacy			
										Secure Application / Code Development for Internal Use			
										Directory Service / Identity Management			
										Data Storage Protection			
										Backup, Recovery & Archiving			
										Virtualized & Cloud Environments			
										Software Product Security			
										Encryption / Data Obfuscation			
										Data Exfiltration Defense			
										Authentication & Authorization			
										Cyber Intrusion Defenses			
										Malware Defenses			

Security Roadmap



Protect

Zero Trust

Securing access everywhere



What are enclaves and segmentation?



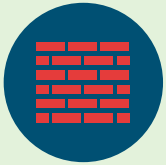
Assets with common
security goals



Applied set of security controls that meets
common requirements



Known characteristics
(systems, end-points, applications)



Secured physical or
virtual boundaries



Internally defined
communication



Explicitly defined and trusted
external communication



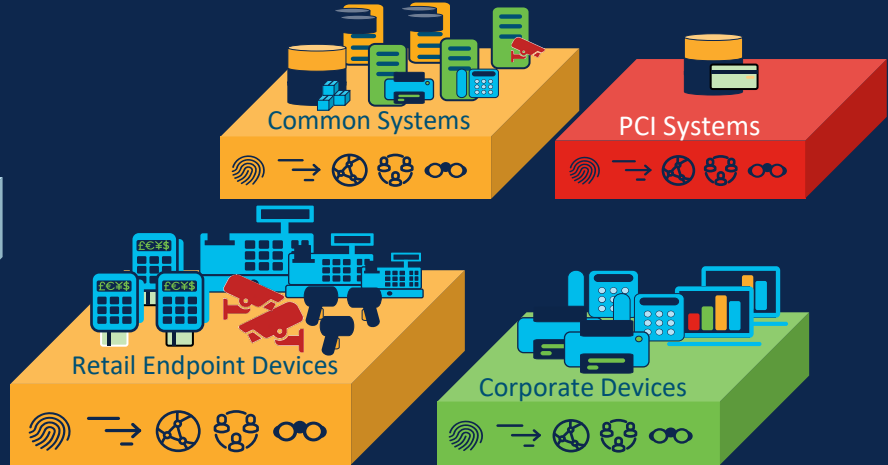
Single administrative
entity



Flat → Segmented



Flat Network



Segmented Network
using Enclaves



Identity & Trust



Policy Enforcement



Isolation



Availability

Visibility

Detect, Respond & Recover

Outcomes

1. SOC's Role in the customer's Overall Security Mission
2. Key Drivers for building the SOC
3. Key SOC Stakeholders
4. Consumers of the SOC services
5. SOC Vision and Mission statements
6. Core Principles that the SOC will operate under
7. Desired Goals and Outcomes of the SOC
8. High-level Operating Model
9. Three-year Strategic Roadmap to achieve the SOC's Goals
10. Target Service Capability/Maturity levels
11. High-level SOC Service Catalogue
12. Organisation Strategy to deliver the SOC services
13. Core Processes to deliver the SOC services
14. Technology Strategy to deliver the SOC services

SOC Services: Plan Package



Outcomes

1. SOC Strategy

Customer's key drivers, desired business outcomes, SOC requirements and specific situation explored and documented using a formal SOC strategy framework

Appropriate SOC Services Portfolio created which the SOC will deliver in order to meet the strategy

2. SOC Capability Assessment

Customer's existing SOC related capabilities assessed for suitability for the SOC strategy

Gaps and recommendations documented in the form of a roadmap

3. SOC Governance & Organizational Design

Comprehensive SOC Governance, Service, Operating Model and Organization Structure designs to deliver the strategy

4. SOC Technical Architecture Design

Comprehensive SOC Technical Architecture design, focussed on capabilities and integrations to deliver the strategy

5. SOC Process Development

Key Processes developed to deliver the strategy

SOC Services: Design Package



Cisco Talos Incident Response



Global Capabilities



Leading security technology
(Cisco Secure Endpoint, Umbrella,
Secure Network Analytics and more)



400+ dedicated responders
and intelligence researchers



Ability to reach across
the entire Cisco enterprise



Incident Commanders



Incident Response
Consultants



Red Team



Project Managers

A vendor agnostic approach

**We work with what you have,
no hidden costs or charges**

Whether you have Cisco gear, competitor gear, or you're lacking security infrastructure, we have you covered. Our competition might bring in their own tools and start charging you, but we don't.



Talos Incident Response Retainer Services



Emergency
Incident Response



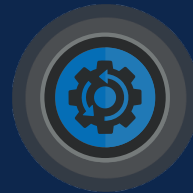
Intel on
Demand



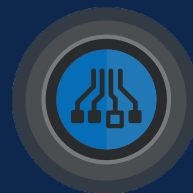
IR
Plans



IR
Playbooks



IR Readiness
Assessments



Network Security
Architecture
Assessment

Core Offer

Foundational



Tabletop
Exercises



Cyber Range
Training



Compromise
Assessments



Threat
Hunting



Pen
Testing



Purple
Team



Red
Team

Training

Threat Detection

Offensive

The Talos Incident Response Difference



Named, dedicated, certified, and seasoned incident response consultants



Largest private global threat intelligence & response organization in the world



Vendor agnostic, leveraging existing security investments



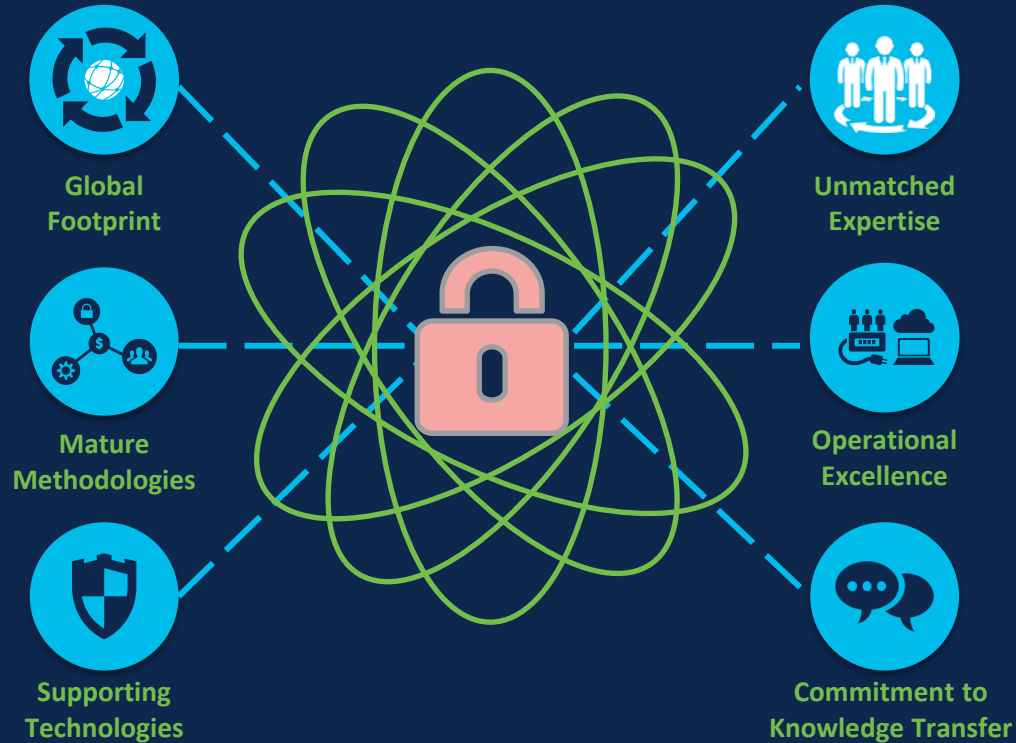
Proactive and reactive work from the same highly-qualified teams



Industry-leading tools and best practices from the #1 Cyber Security company in the world

Why Cisco?

Mature Delivery





The bridge to possible