RSA®Conference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: 49273

Here, There and Everywhere – How to Harness Your Value Chain Security Beast!

Edna Conway

Chief Security Officer, Global Value Chain

CISCO

Agenda
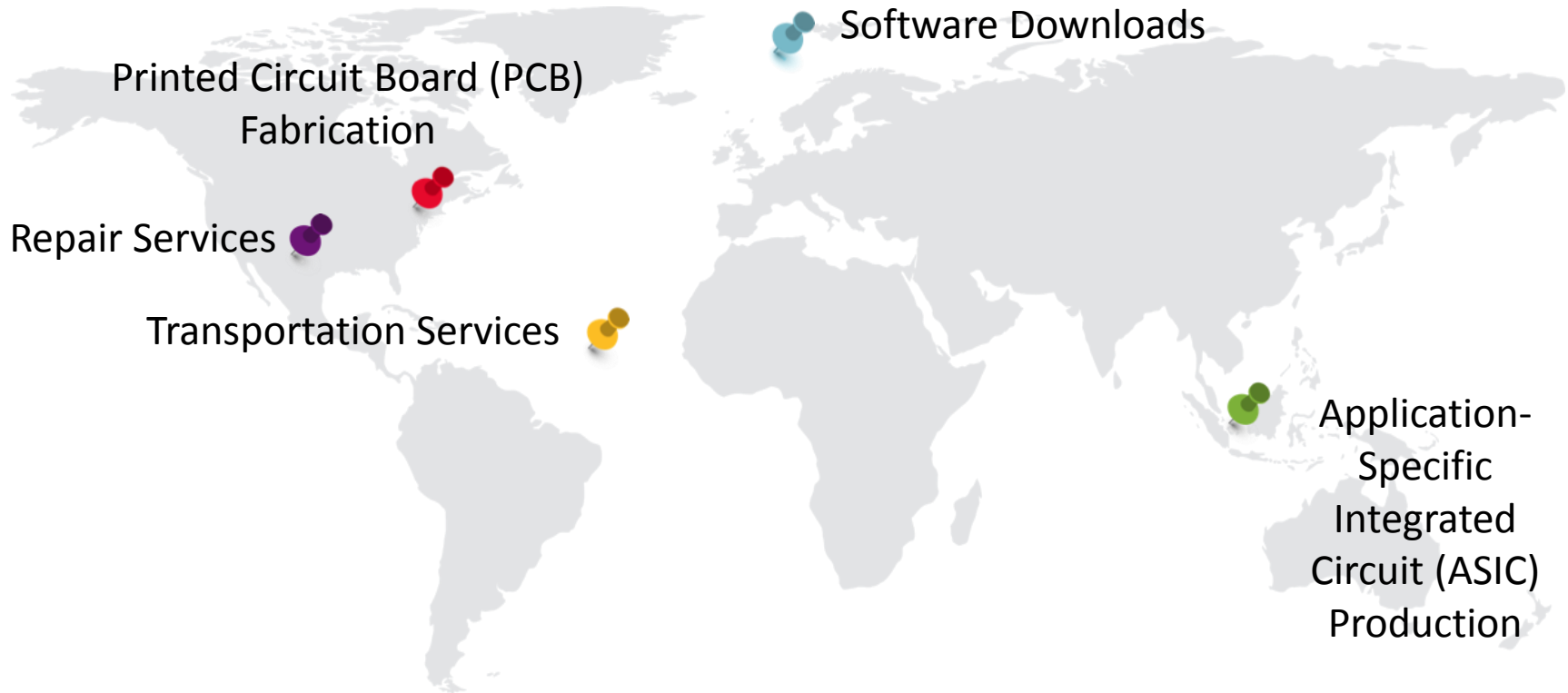
The IT Value Chain Beast

Security Built In Is the Answer

Pervasive Value Chain Security

Winning Together

RSAConference2016

Today's IT Value Chain Beast

Software Downloads

Printed Circuit Board (PCB) Fabrication

Repair Services

Transportation Services

Application-Specific Integrated Circuit (ASIC) Production

CISCO

RSA Conference2016

Today's IT Value Chain Beast

ASIC Production

RSAConference2016
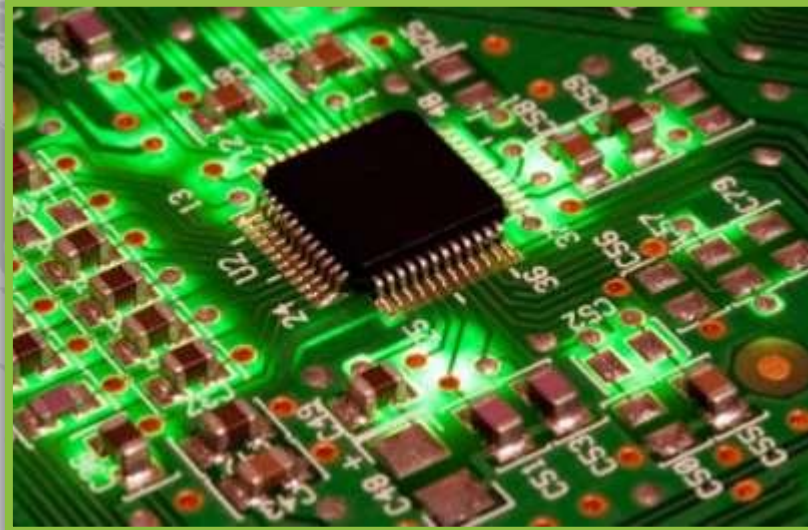
Today's IT Value Chain Beast

Repair Services

CISCO

RSAConference2016

Today's IT Value Chain Beast

Transportation Services
7 Point Container Inspection
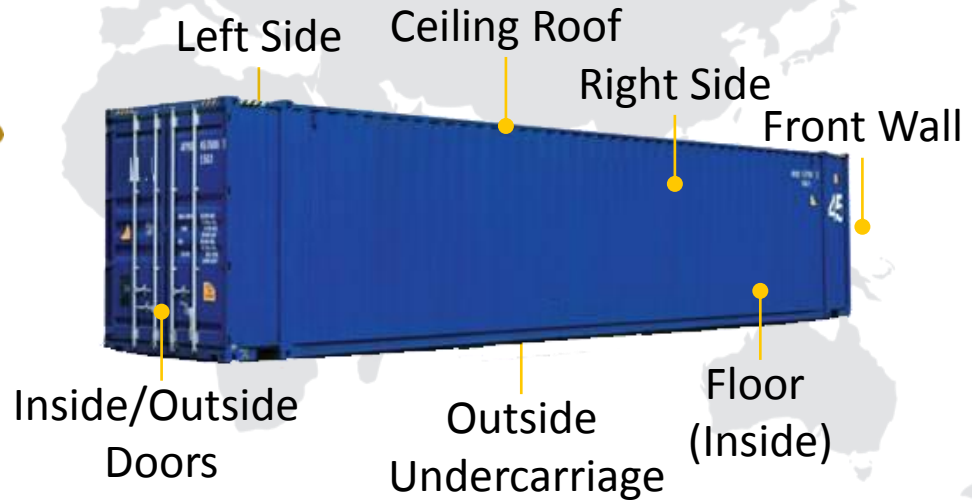
Left Side

Ceiling Roof

Right Side

Front Wall

Inside/Outside
Doors

Outside
Undercarriage

Floor
(Inside)

Today's IT Value Chain Beast

PCB Fabrication

CISCO

RSAConference2016

Today's IT Value Chain Beast

Software Downloads

RSAConference2016
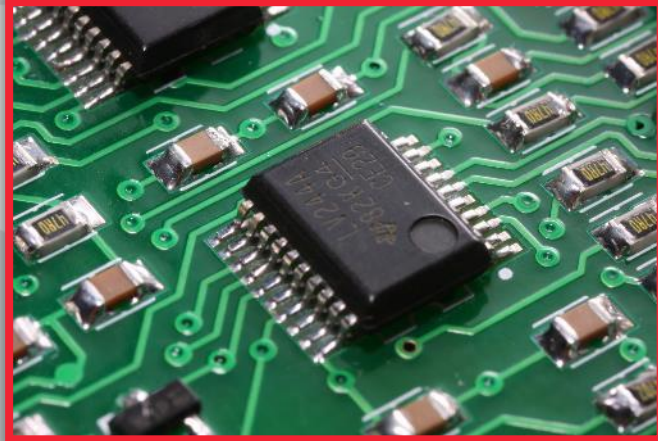
The Risk of Non- Alignment

The Risk of Non- Alignment

RSAConference2016

What Is the IT Value Chain?

Design/Develop → Plan/Order → Source → Make → Quality → Delivery → Sustain → End of Life
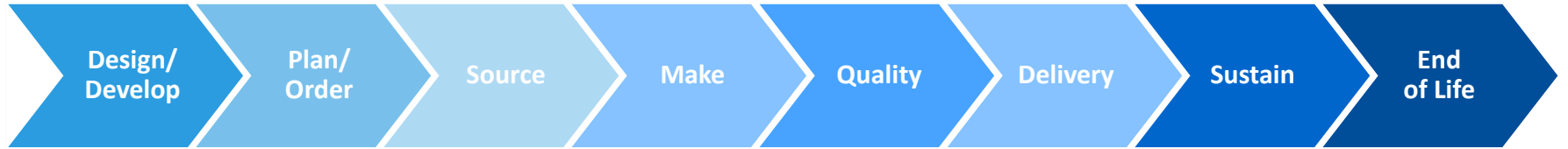
What Are the Threats to the IT Value Chain?

Manipulation
Unauthorized Control

Espionage
Unauthorized Visibility

Disruption
Denial of Service

RSAConference2016

What Exposures Arise from IT Value Chain Threats?

Manipulation
Unauthorized Control

Espionage
Unauthorized Visibility

Disruption
Denial of Service

TAINT = alteration allowing unauthorized control or content visibility

COUNTERFEIT = raw materials, software or finished goods which are not authentic
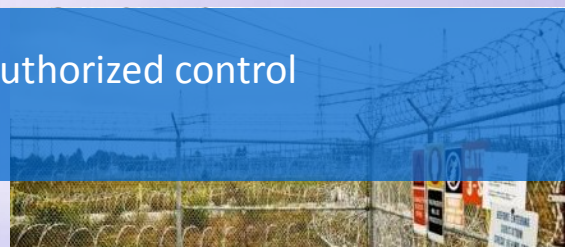
IP MISUSE = unauthorized access to IP, allowing unfair business competition and increased risk to end users

RSAConference2016

Value Chain Security
Making Security Pervasive

Secure Development

Information and Security Technology Innovation

Physical Security Practices

Logical Security Processes

| Design/ Develop | Plan/ Order | Source | Make | Quality | Delivery | Sustain | End of Life |

CISCO

RSA Conference2016
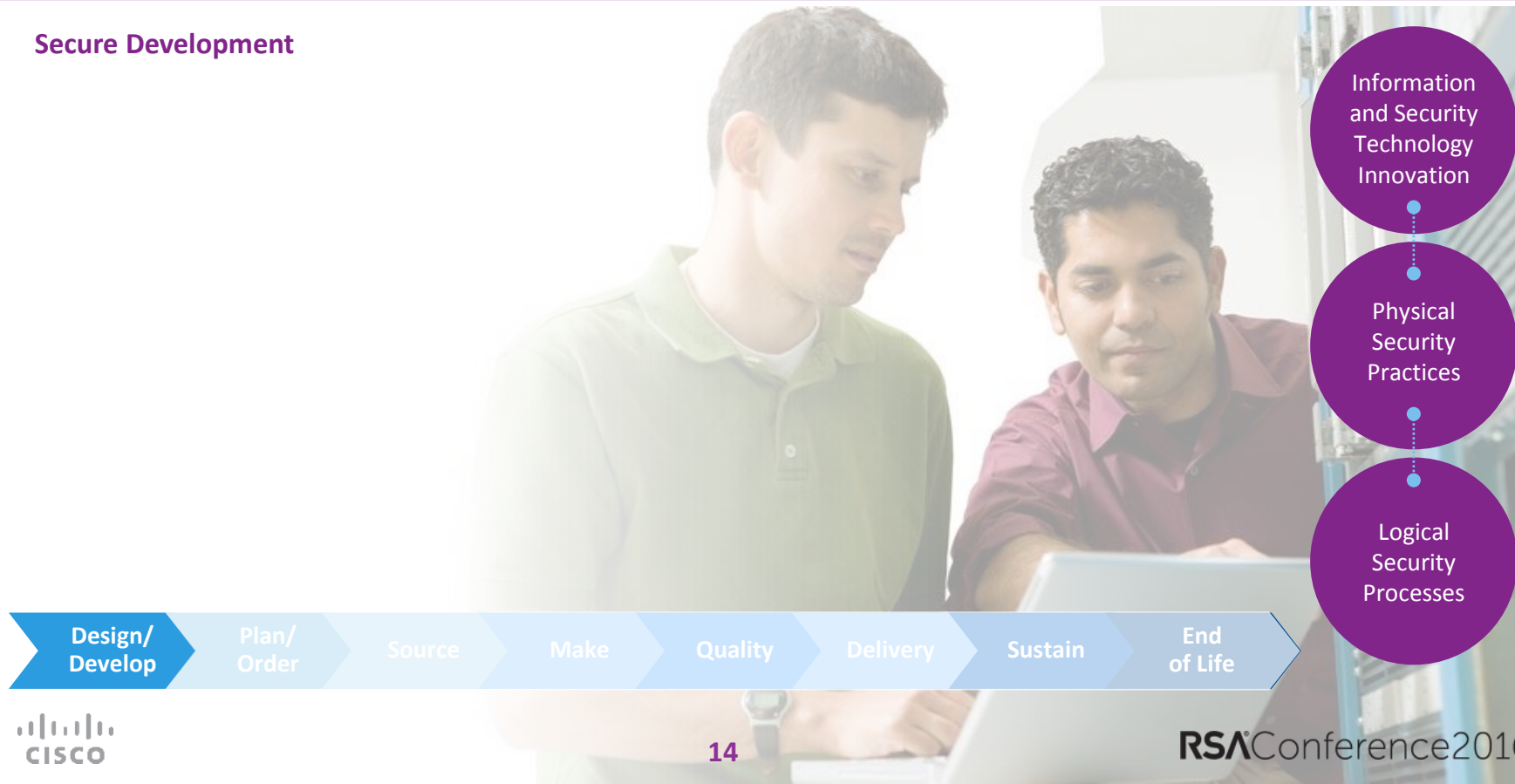
Value Chain Security

Making Security Pervasive

Secure Development

Information Exchange and Access Controls

Information and Security Technology Innovation

Physical Security Practices

Logical Security Processes

| Design/ Develop | Plan/ Order | Source | Make | Quality | Delivery | Sustain | End of Life |

RSAConference2016

Value Chain Security
Making Security Pervasive

Secure Development

Information Exchange and Access Controls

Physical Plant Security

Information and Security Technology Innovation

Physical Security Practices

Logical Security Processes

Design/ Develop	Plan/ Order	Source	Make	Quality	Delivery	Sustain	End of Life

RSAConference2016

Value Chain Security
Making Security Pervasive

Secure Development

Information Exchange and Access Controls

Physical Plant Security

Talent Security and Integrity

Information and Security Technology Innovation

Physical Security Practices

Logical Security Processes

| Design/ Develop | Plan/ Order | Source | Make | Quality | Delivery | Sustain | End of Life |

CISCO

RSAConference2016

Value Chain Security
Making Security Pervasive

Secure Development

Information Exchange and Access Controls

Physical Plant Security

Talent Security and Integrity

Supplier Resiliency and Crisis Management

Information and Security Technology Innovation

Physical Security Practices

Logical Security Processes

Design/ Develop	Plan/ Order	Source	Make	Quality	Delivery	Sustain	End of Life

RSA Conference2016

Value Chain Security
Making Security Pervasive

Secure Development

Information Exchange and Access Controls

Physical Plant Security

Talent Security and Integrity

Supplier Resiliency and Crisis Management

Protection of High Value/IP Containing Components and Finished Goods

Information and Security Technology Innovation

Physical Security Practices

Logical Security Processes

| Design/ Develop | Plan/ Order | Source | Make | Quality | Delivery | Sustain | End of Life |

RSA Conference2016

Value Chain Security
Making Security Pervasive

Secure Development

Information Exchange and Access Controls

Physical Plant Security

Talent Security and Integrity

Supplier Resiliency and Crisis Management

Protection of High Value/IP Containing
Components and Finished Goods

Logistics Security

Information and Security Technology Innovation

Physical Security Practices

Logical Security Processes

Design/ Develop	Plan/ Order	Source	Make	Quality	Delivery	Sustain	End of Life

CISCO

RSAConference2016

Value Chain Security
Making Security Pervasive

Secure Development

Information Exchange and Access Controls

Physical Plant Security

Talent Security and Integrity

Supplier Resiliency and Crisis Management

Protection of High Value/IP Containing Components and Finished Goods

Logistics Security

Fabrication Security

Information and Security Technology Innovation

Physical Security Practices

Logical Security Processes

Design/ Develop	Plan/ Order	Source	Make	Quality	Delivery	Sustain	End of Life

RSAConference2016

Value Chain Security
Making Security Pervasive

Secure Development

Information Exchange and Access Controls

Physical Plant Security

Talent Security and Integrity

Supplier Resiliency and Crisis Management

Protection of High Value/IP Containing Components and Finished Goods

Logistics Security

Fabrication Security

Scrap Management

Information and Security Technology Innovation

Physical Security Practices

Logical Security Processes

Design/ Develop	Plan/ Order	Source	Make	Quality	Delivery	Sustain	End of Life

CISCO

RSAConference2016

Value Chain Security
Making Security Pervasive

Secure Development

Information Exchange and Access Controls

Physical Plant Security

Talent Security and Integrity

Supplier Resiliency and Crisis Management

Protection of High Value/IP Containing
Components and Finished Goods

Logistics Security

Fabrication Security

Scrap Management

Service Security

Information and Security Technology Innovation

Physical Security Practices

Logical Security Processes

Design/ Develop	Plan/ Order	Source	Make	Quality	Delivery	Sustain	End of Life

RSAConference2016

Value Chain Security
Making Security Pervasive

Secure Development

Information Exchange and Access Controls

Physical Plant Security

Talent Security and Integrity

Supplier Resiliency and Crisis Management

Protection of High Value/IP Containing Components and Finished Goods

Logistics Security

Fabrication Security

Scrap Management

Service Security

End of Life Security Management
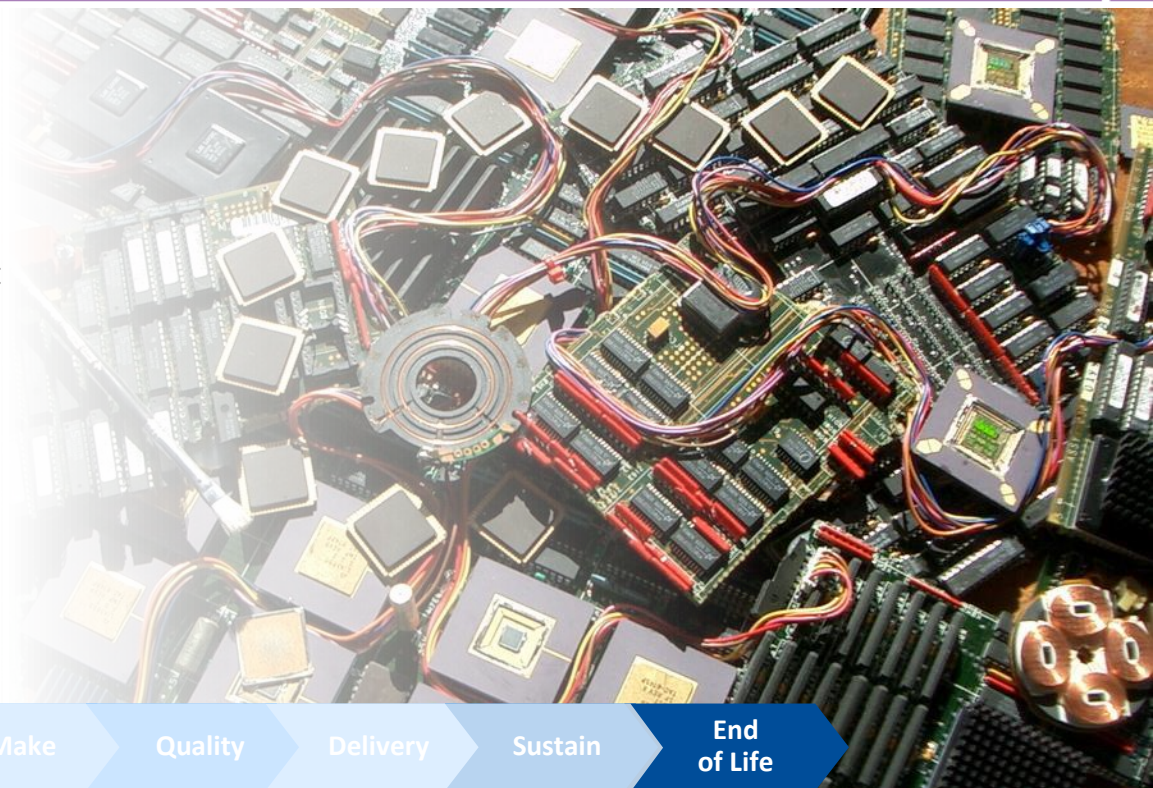
| Design/ Develop | Plan/ Order | Source | Make | Quality | Delivery | Sustain | End of Life |

cisco

RSAConference2016

RSAConference2016

Leveraging Security Technology and Process

Bone Pile

VS

Tracked Inventory

02

RSAConference2016

Leveraging Security Technology and Process

Guard/Door

vs

Biometric Access

Physical Scans

RSAConference2016

Value Chain Security
Applying A Winning Formula

1   An Adaptable Security Architecture   Flexible Requirements

2   A Coordinated Deployment Plan   The Value Chain Ecosystem

3   Metrics that Embrace Security   Scorecard

4   Trust but Verify   Audit Template

5   Join the Industry Discussion   Global Collaboration

CISCO

RSAConference2016

Value Chain Security

Adaptable Pervasive Security

Anti-Taint

Anti-Counterfeit

Intellectual Property Protection

>1200 security requirements

SR2 SR1

SR3

Key Requirements

Defined Categories

11 Domains

>180 Requirements

Mapped to Specific Activity

RSAConference2016
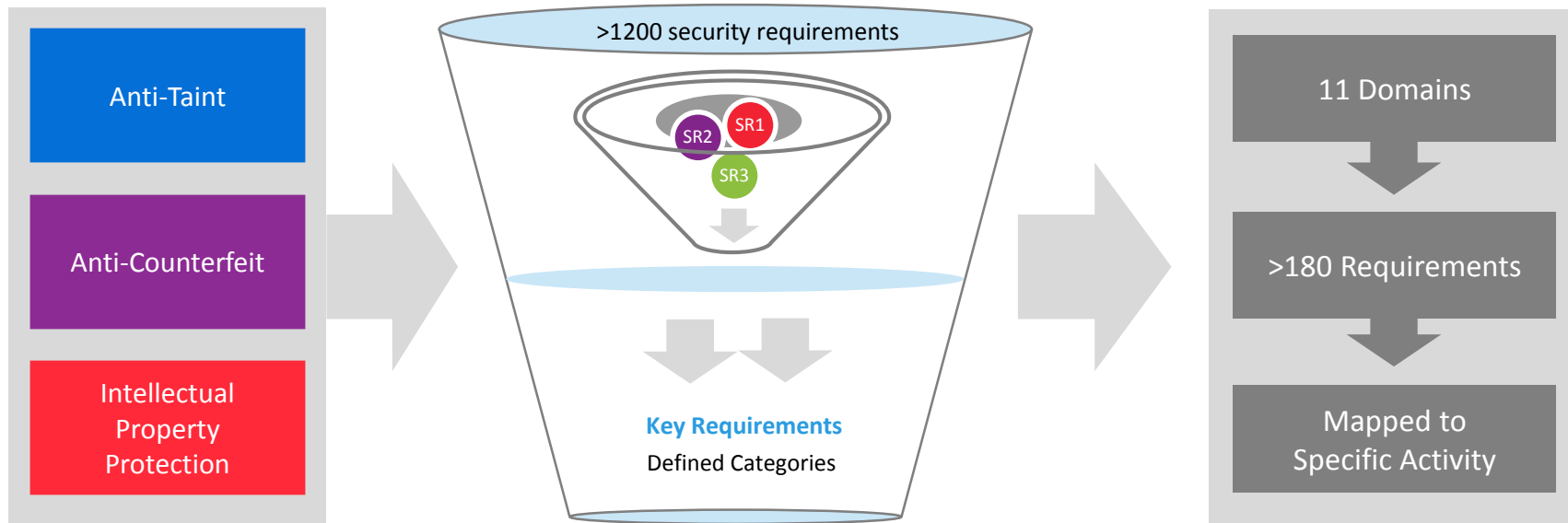
Value Chain Security

Adaptable Pervasive Security

Domains

1	Security Governance		7	Physical and Environmental Security
2	Security in Manufacturing and Operations		8	Personnel Security
3	Asset Management		9	Information Protection
4	Security Incident Management		10	Security Engineering and Architecture
5	Security in Service Management		11	Third-Tier Partner Security
6	Security in Logistics and Storage			

RSAConference2016

Value Chain Security
Adaptable Pervasive Security

Domain	Sub Domain	Requirement Description	Direct Fulfillment (final assembly, Prototype and test)	PCB Assembly (PCBA Prototype)	Design/ Development	Transportation	Warehousing / Hubbing	Destruction/ Recycling	Failure Analysis	Channel Partners
Security in Manufacturing and Operations	Security in Inventory Mangmt.	Supplier must produce a written report on the results of the cycle counts that identifies the individuals who performed the activity. The results of all cycle counts must be reconciled and discrepancies must be reported to Cisco immediately.	✔	✔			✔			
Asset Management	Media Protection and Disposal	Cisco IP and/or Confidential Information must not be stored in removable Media unless authorized in writing by Cisco.	✔	✔	✔	✔	✔		✔	✔
Information Protection	Information System Logging and Monitoring	Supplier must monitor Information Systems for: a. attacks and indicators of potential attacks; b. unusual transactions that could indicate unauthorized access to Cisco IP or Confidential Information; c. unexpected changes to system configurations and privileges; and d. unauthorized local, network and remote connections.	✔	✔	✔	✔	✔	✔	✔	✔

Value Chain Security
A Coordinated Deployment Plan

- **Engineering**
- **Supply Chain Operations**
- **Technical Services**

- **Engineering**
- **Supply Chain Operations**
- **Technical Services**

- **Engineering**
- **Supply Chain Operations**
- **Quality Assurance**
- **Technical Services**
- **Repair and Refurbishment**

- **Engineering**
- **Services Operations**
- **Services Logistics**

Design/ Develop → **Plan/ Order** → **Source** → **Make** → **Quality** → **Delivery** → **Sustain** → **End of Life**

- **Sales**
- **S&OP**
- **Order Management**
- **Global Planning and Fulfillment**

- **Supply Chain Operations**
- **Technical Services**
- **Repair and Refurbishment**

- **Supply Chain Logistics**
- **Global Channel/ Distribution**
- **Services Logistics**
- **Reverse Logistics**

- **Reverse Logistics**

CISCO

RSAConference2016

SCO Security Audit Dashboard

Site Category	Partner	Country
(All)	(All)	(All)

Rating Legend

Exemplary = Zero findings, best in class

Acceptable = No significant finding(s)

Needs Improvement = Significant finding(s) identified

Deficient = Substantial lack of foundational security. Consider a (SIP)

Site Category	Partner	Site	Rating as of Audit	Findings Status
ASIC				Open: 0 Closed: 0
				Open: 6 Closed: 0
				Open: 9 Closed: 0
				Open: 6 Closed: 0
				Open: 7 Closed: 0
				Open: 7 Closed: 0
				Open: 5 Closed: 0

RSAConference2016

Category	Metric	Global	Direct Fulfillment	PCBA
Top level	Cost Savings			
	Cost per Placement			
	Innovation			
	Non-Material Spend			
	Financial Health			
	Sustainability			
	Business Continuity Plan			
	Time to Recover			
	Security			
	Data Governance			
	Subtotal	Actual: __	Actual: __	Actual: __
	Percentage	__%	__%	__%

RSAConference2016

Value Chain Security
One IT Industry Voice

Global Collaboration

Join the Industry Discussion

Industry/Government Guidelines

A truly layered approach requires addressing security in the value chain across the industry and with governments worldwide

ISO/IEC 15408	ISO/IEC 27036 Part 3	ISO/IEC 20243

Common Criteria

ISO

ISO

THE Open GROUP

Combating Crime and Terrorism Collaboratively

Certifications

International certifications obtained by Cisco and our value chain partners reflect our commitment to protect against terrorism, smuggling, and other criminal activities

Tier 3 Partner in US Customs and Border protection	Canada's Border Services Agency's Partners in Protection Program	EU Authorized Economic Operator Program

C-TPAT
Custom-Trade Partnership Against Terrorism

Canada Border Services Agency

AEO

European Commission

Value Chain Security

Applying A Winning Formula

🔒 Unified Security Architecture

🔺 The Value Chain Ecosystem

📈 Audit Dashboard

📋 Scorecard

🤝 Global Collaboration

CISCO

RSAConference2016