Network Perception

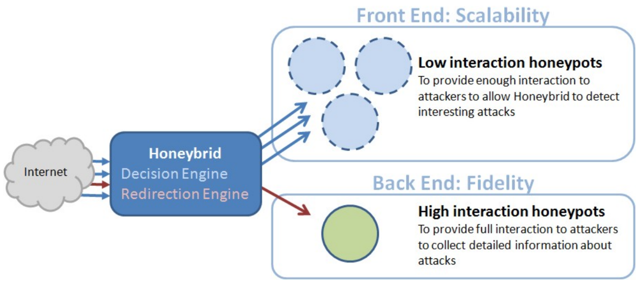
IFIP Meeting
Jan. 30, 2020
Robin Berthier

Agenda

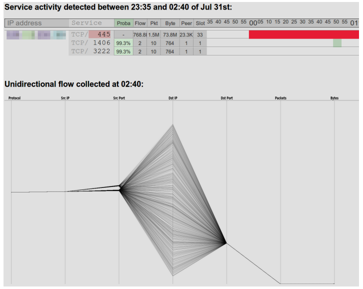
- Background
- **Industry Perspective**
  - Challenges
  - Culture of Resiliency
  - Best Practices
  - Compliance as a stepping stone
  - Pro-active approaches
  - Technology and automation
- **R&D Perspective**
  - Continuous independent network monitoring
  - NP Platform architecture
  - Configuration parsers
  - Network model
  - Topology visualization
  - Path analysis
  - Research roadmap
- Summary

Background

- Univ. of Maryland College Park – PhD with Michel Cukier
  - **Nfsight**: Netflow visualization platform
  - **Honeybrid:** dynamically-scaling honeypot framework
- Univ. of Illinois in Urbana-Champaign – Postdoc with Bill Sanders
  - **Amilyzer**: first IDS for smart meters
  - **NetAPT**: firewall analysis
- Network Perception – Co-founder and President
  - **NP-View**: offline network audit
  - **NP-Live**: continuous network device monitoring platform


Front End: Scalability
Low interaction honeypots
To provide enough interaction to attackers to allow Honeybrid to detect interesting attacks
Internet
Honeybrid
Decision Engine
Redirection Engine
Back End: Fidelity
High interaction honeypots
To provide full interaction to attackers to collect detailed information about attacks

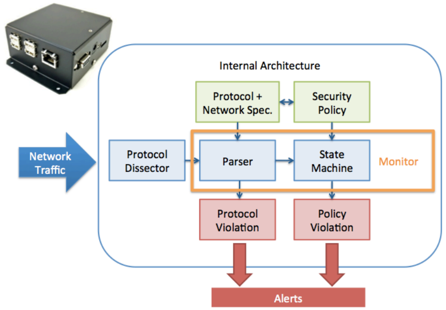
http://honeybrid.sourceforge.net


Service activity detected between 23:35 and 02:40 of Jul 31st:

IP address	Service	Proba	Flow	Pkt	Byte	Peer	Slot
[redacted]	TCP/ 445	-	768.8I	1.5M	73.8M	23.3K	33
	TCP/ 1406	99.3%	2	10	764	1	1
	TCP/ 3222	99.3%	2	10	764	1	1

Unidirectional flow collected at 02:40:

http://nfsight.sourceforge.net



Background (cont.)

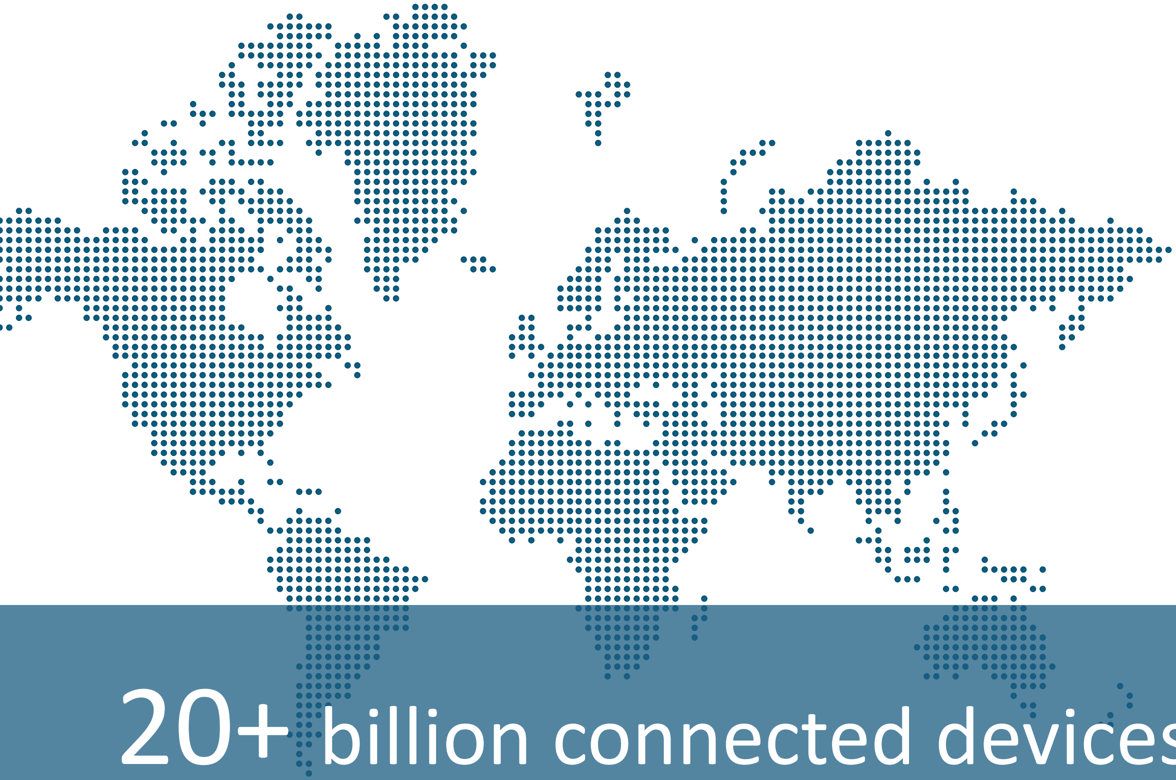
- Network Perception was launched by a team of researchers and industry experts from the University of Illinois in Urbana-Champaign in 2014

Mission: to support critical infrastructure in checking the correct implementation of cybersecurity and compliance best practices

- Leveraging 6 years of collaboration with electric utilities
  - – Technology developed at TCIPG, an $18-million cybersecurity research project for the power grid, funded by DHS and DOE
  - – Feature set developed through collaboration with users and auditors
  - – 100+ deployments in the US

INDUSTRY PERSPECTIVE

Challenges



20+ billion connected devices in 2020

30% yearly increase

Challenges

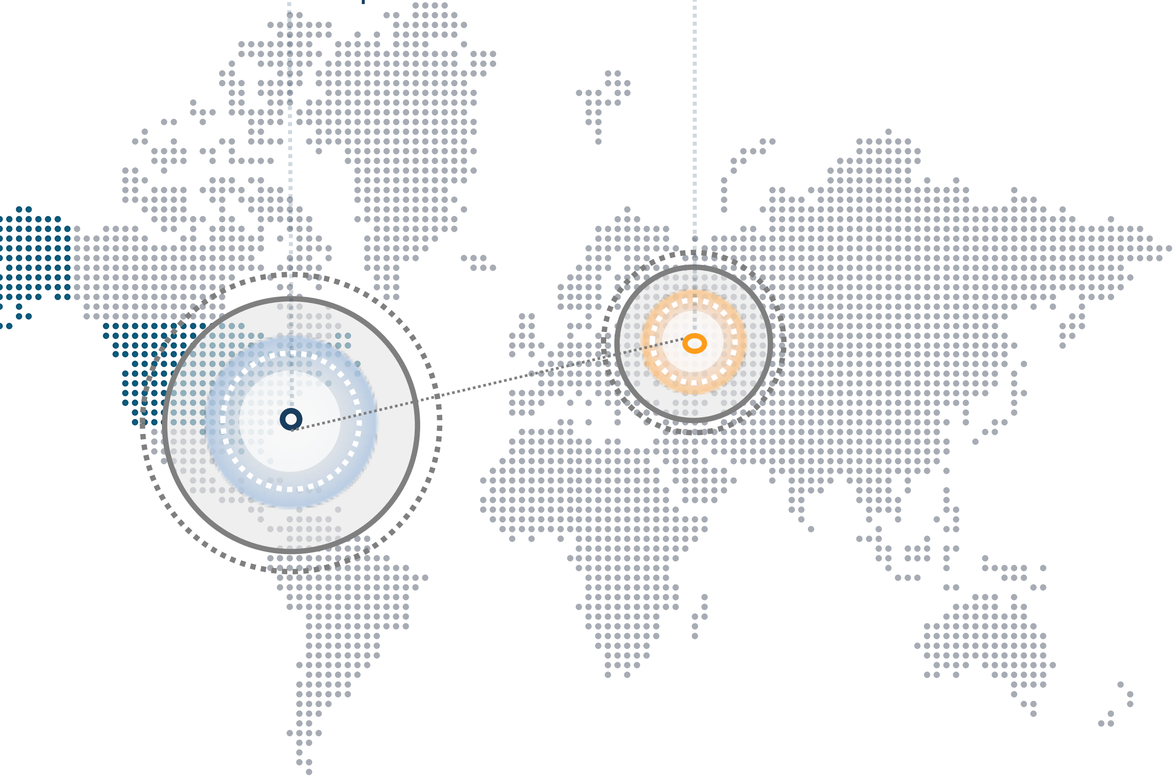
53,000 confirmed security incidents in 2018

28% insider job

2017+
WannaCry ransomware cyber attack affecting ICS ($4B loss)

2018
Compromise of M.E.Doc by NotPetya: Maersk network down

Challenges



2018
US Navy information compromised via contractors

2018
VPN Filter malware targeting critical infrastructure in Ukraine

2017+
WannaCry ransomware cyber attack affecting ICS ($4B loss)

2018
Compromise of M.E.Doc by NotPetya: Maersk network down

Attack surface
keeps increasing
while security threats
keep evolving

EVOLUTION OF NETWORK SECURITY

1 PROTECTION

2 DETECTION

3 REGULATION

4 BEST PRACTICES

EVOLUTION OF NETWORK SECURITY

1 PROTECTION

2 DETECTION

3 REGULATION

4 BEST PRACTICES

Towards a Culture of Resilience: Compliance + Best Practices

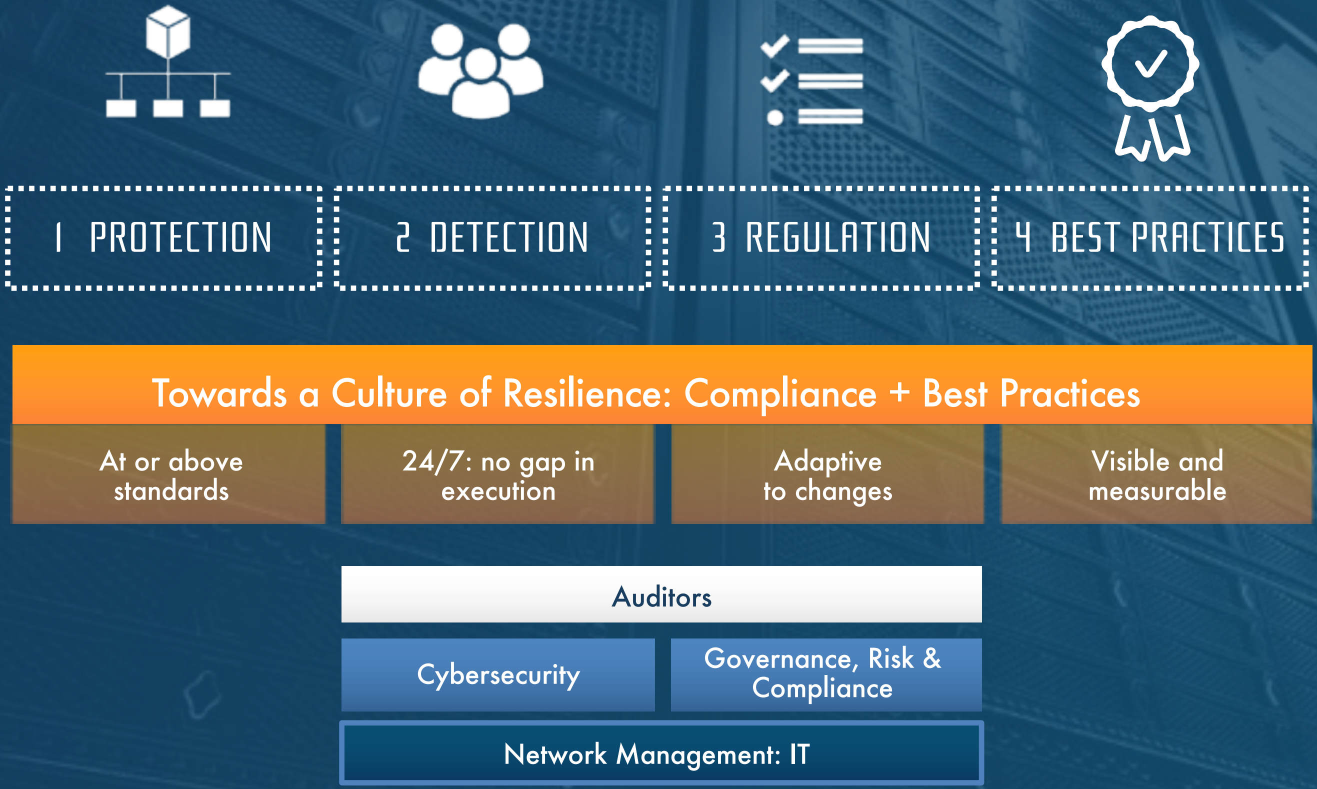
At or above standards

24/7: no gap in execution

Adaptive to changes

Visible and measurable

EVOLUTION OF NETWORK SECURITY



1 PROTECTION

2 DETECTION

3 REGULATION

4 BEST PRACTICES

Towards a Culture of Resilience: Compliance + Best Practices

At or above standards

24/7: no gap in execution

Adaptive to changes

Visible and measurable

Auditors

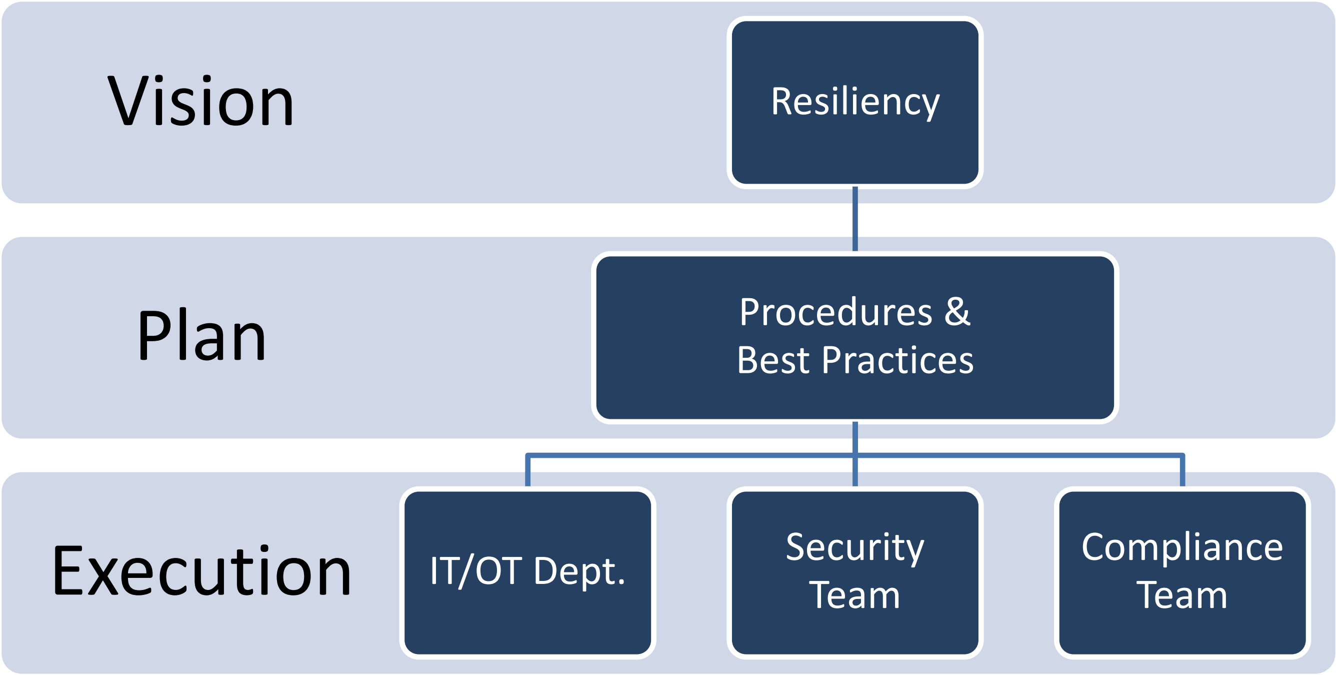
Cybersecurity

Governance, Risk & Compliance

Network Management: IT

The Alignment Challenge

“Ability to continuously deliver the intended outcome despite adverse cyber events”



Best Practices

*“Procedure that has been shown by **research and experience** to produce **optimal results** and that is established or proposed as **a standard** suitable for widespread adoption”*

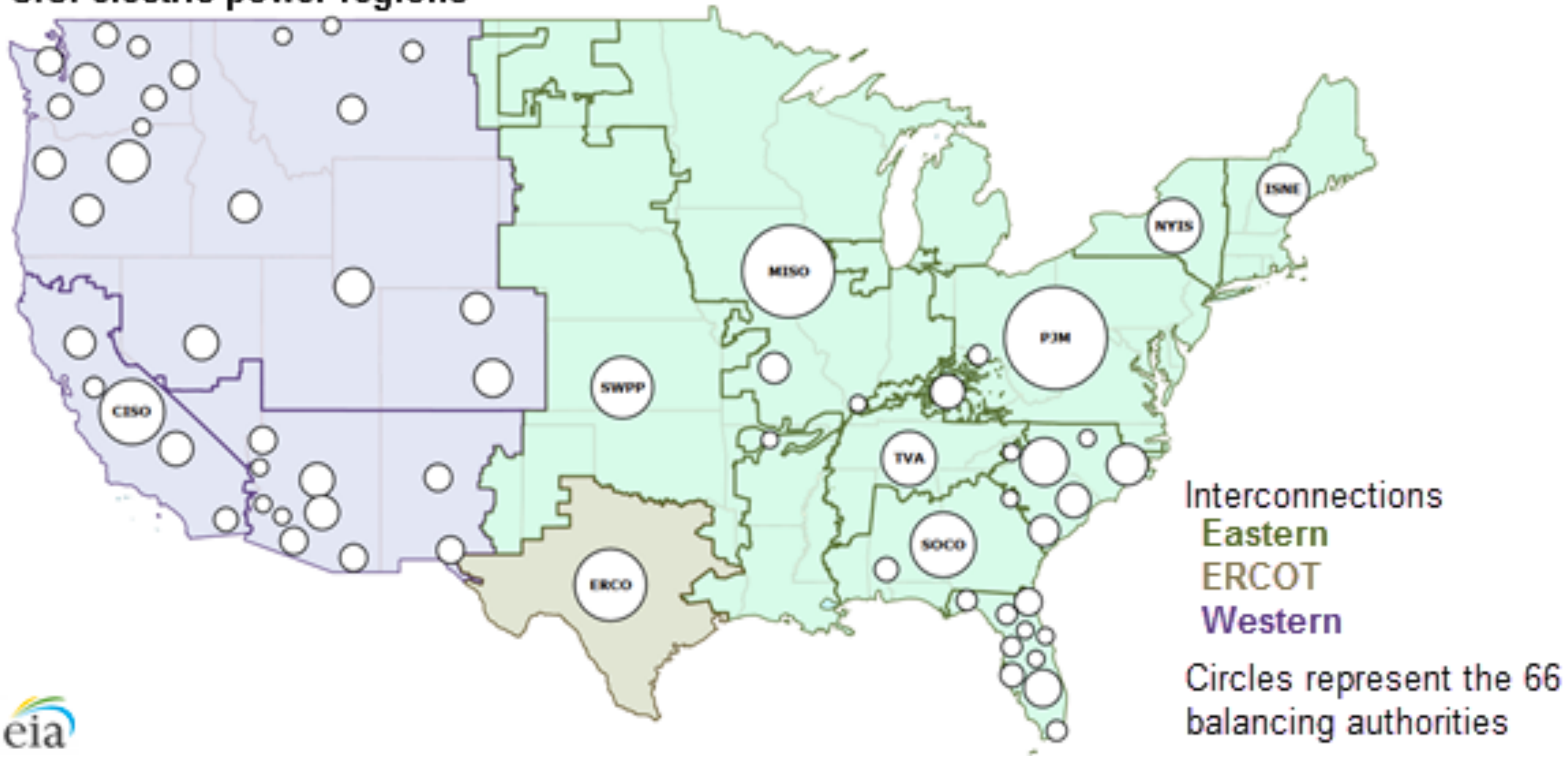
Independent

Measurable

Usable

The US Electric Industry

U.S. electric power regions

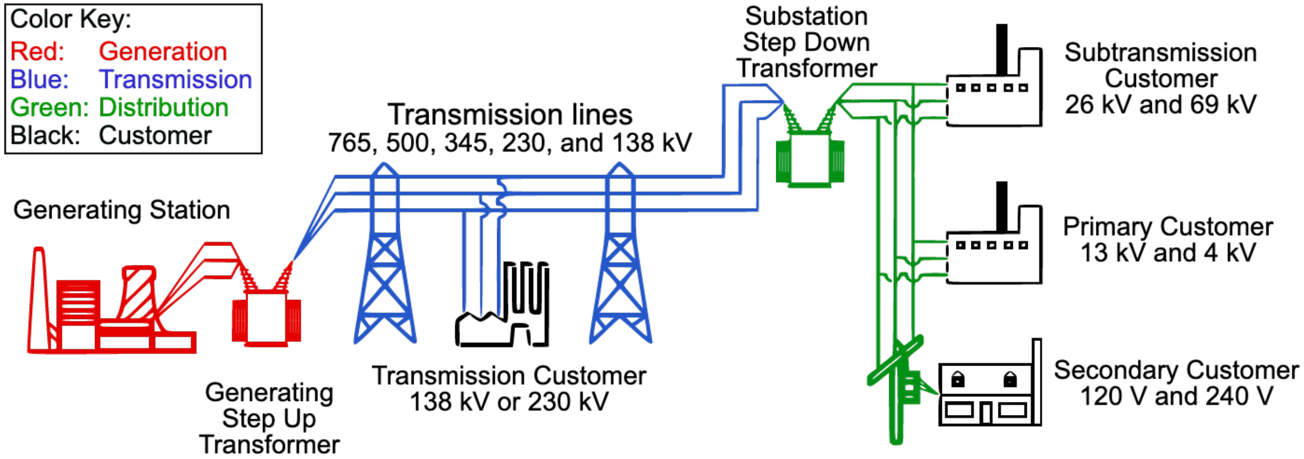


Circles represent the 66 balancing authorities

Note: A balancing authority ensures, in real time, that power system demand and supply are finely balanced.

Source: https://www.eia.gov/todayinenergy/detail.php?id=27152

The US Electric Industry (cont.)

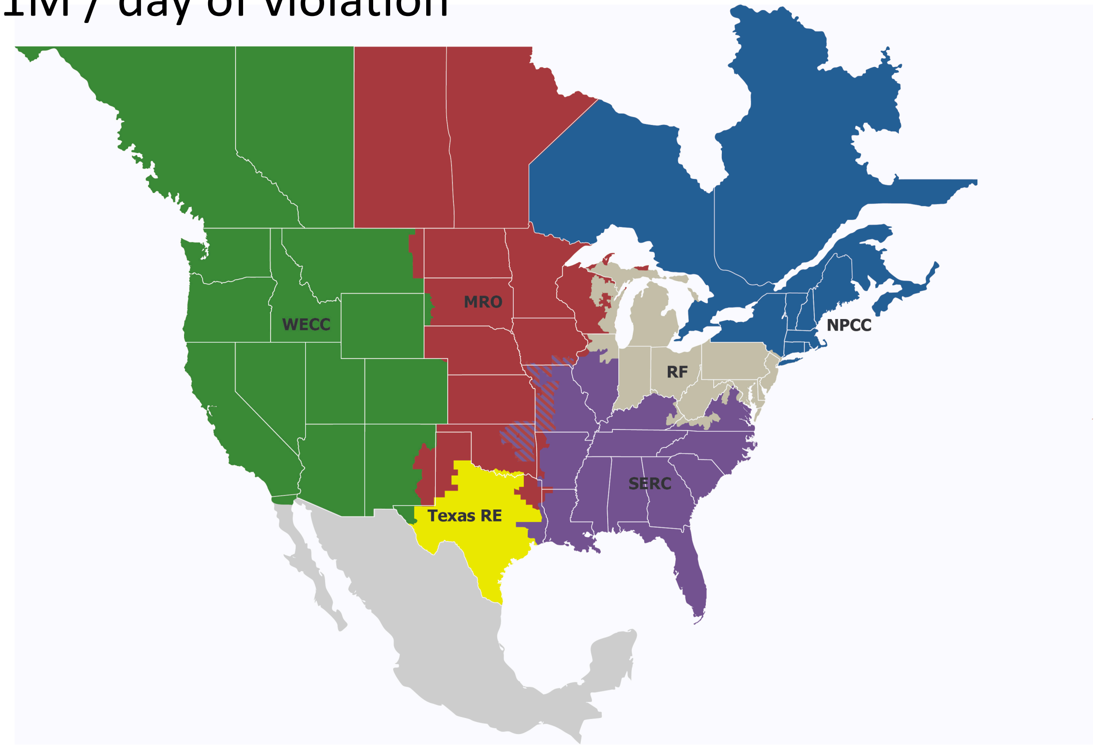


Balancing Authority	105
Distribution Provider	388
Generation Owner	972
Generation Operator	921
Planning Authority / Planning Coordinator	71
Reliability Coordinator	16
Resource Planner	168
Response Sharing Group	15
Transmission Owner	326
Transmission Operator	175
Transmission Provider	200
Transmission Service Provider	78

1,454 registered entities

NERC Regulation

- **FERC**: Federal Energy Regulatory Commission
  - Energy Policy Act of 2005
- **NERC**: North American Electric Reliability Corporation
  - **C**ritical **I**nfrastructure **P**rotection reliability standards enforced since 2008
  - Up to $1M / day of violation



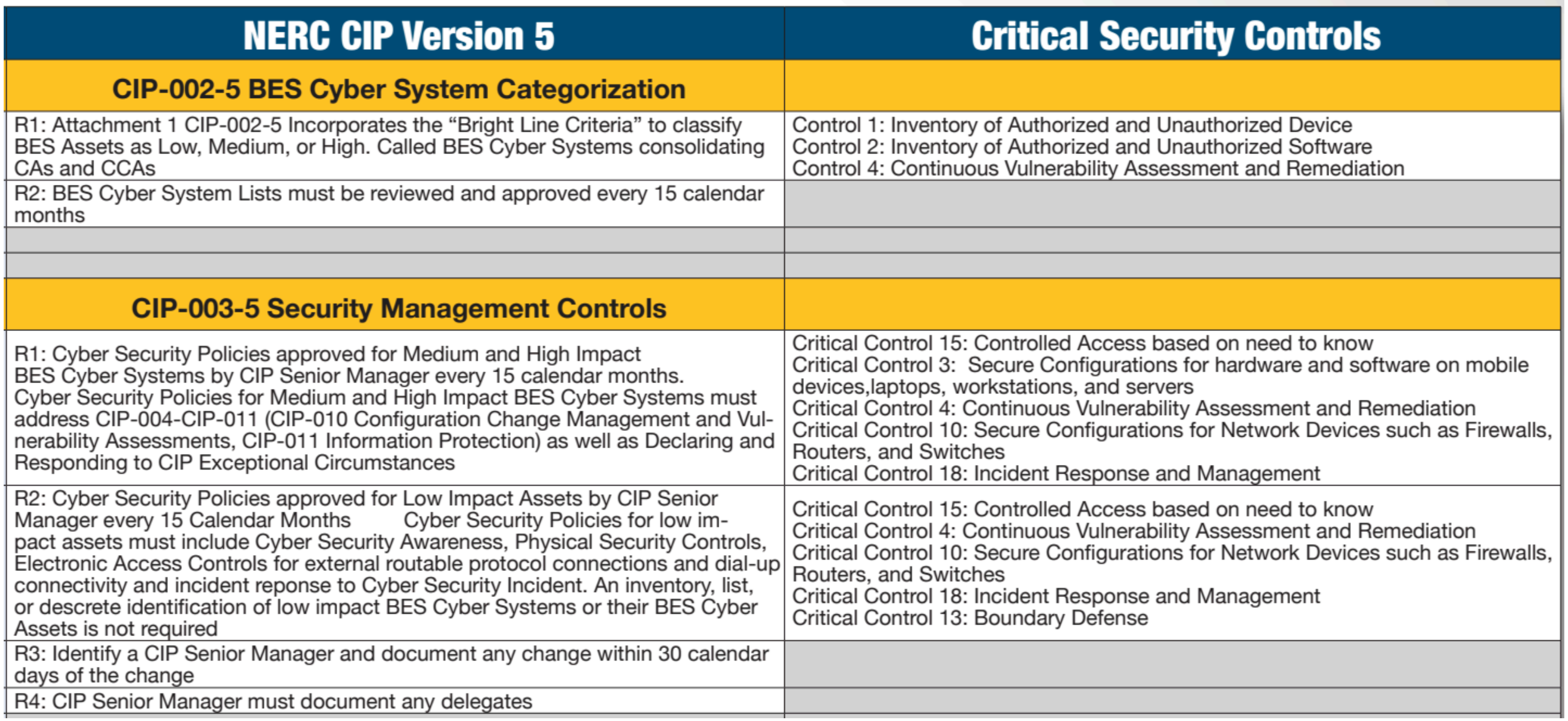
NERC Regulation (cont.)

CIP-002-5.1a	Cyber Security - BES Cyber System Categorization
CIP-003-7	Cyber Security - Security Management Controls
CIP-004-6	Cyber Security - Personnel & Training
CIP-005-5	Cyber Security - Electronic Security Perimeter(s)
CIP-006-6	Cyber Security - Physical Security of BES Cyber Systems
CIP-007-6	Cyber Security - System Security Management
CIP-008-5	Cyber Security - Incident Reporting and Response Planning
CIP-009-6	Cyber Security - Recovery Plans for BES Cyber Systems
CIP-010-2	Cyber Security - Configuration Change Management and Vuln. Assessments
CIP-011-2	Cyber Security - Information Protection
CIP-014-2	Physical Security

Compliance as a Steppingstone

	Compliance	Best Practices
Asset inventory	**CIP-002-5**: BES Cyber System Categorization	Expand inventory to include all IT/OT assets
Network access policy	**CIP-003-7**: Security Management Controls **CIP-005-5**: Electronic Security Perimeters	Adopt NIST 800-41 guideline on network policy for every firewall Review network segmentation across all business units
Change tracking	**CIP-010-2**: Configuration Change Management and Vulnerability Assessments	Include mandatory quality control through independent review for every changes

Mapping Compliance with Security Controls



NERC CIP Version 5	Critical Security Controls
CIP-002-5 BES Cyber System Categorization	
R1: Attachment 1 CIP-002-5 Incorporates the “Bright Line Criteria” to classify BES Assets as Low, Medium, or High. Called BES Cyber Systems consolidating CAs and CCAs	Control 1: Inventory of Authorized and Unauthorized Device Control 2: Inventory of Authorized and Unauthorized Software Control 4: Continuous Vulnerability Assessment and Remediation
R2: BES Cyber System Lists must be reviewed and approved every 15 calendar months	
CIP-003-5 Security Management Controls	
R1: Cyber Security Policies approved for Medium and High Impact BES Cyber Systems by CIP Senior Manager every 15 calendar months. Cyber Security Policies for Medium and High Impact BES Cyber Systems must address CIP-004-CIP-011 (CIP-010 Configuration Change Management and Vulnerability Assessments, CIP-011 Information Protection) as well as Declaring and Responding to CIP Exceptional Circumstances	Critical Control 15: Controlled Access based on need to know Critical Control 3: Secure Configurations for hardware and software on mobile devices,laptops, workstations, and servers Critical Control 4: Continuous Vulnerability Assessment and Remediation Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches Critical Control 18: Incident Response and Management
R2: Cyber Security Policies approved for Low Impact Assets by CIP Senior Manager every 15 Calendar Months Cyber Security Policies for low impact assets must include Cyber Security Awareness, Physical Security Controls, Electronic Access Controls for external routable protocol connections and dial-up connectivity and incident reponse to Cyber Security Incident. An inventory, list, or descrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required	Critical Control 15: Controlled Access based on need to know Critical Control 4: Continuous Vulnerability Assessment and Remediation Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches Critical Control 18: Incident Response and Management Critical Control 13: Boundary Defense
R3: Identify a CIP Senior Manager and document any change within 30 calendar days of the change	
R4: CIP Senior Manager must document any delegates	

Source:https://www.sans.org/media/critical-security-controls/nerc-cip-mapping-sans20-csc.pdf

Compliance Toolset

Momentum CYBER

Risk Assessment & Visibility

- AXONIUS
- Balbix
- cavirin
- Coalition
- cyber OBSERVER
- CyberCube
- cyberGRX
- cytegic
- DELVE LABS
- eclypsium
- FIREMON
- innoSec INNOVATING SECURITY
- KENNA Security
- NEHEMIAH SECURITY
- NOPSEC
- OPAQ Networks
- Outpost24
- panaseer
- PREVALENT
- REDSEAL
- riskrecon
- RiSKSENSE TRANSFORMING CYBER RISK MANAGEMENT
- SKYBOX SECURITY
- tenable
- UpGuard
- VENAFI
- zeguro

Security Ratings

- ARCEO.AI
- BITSIGHT
- corax
- COWBELL CYBER
- FICO
- GUIDEWIRE
- NormShield
- Panorays
- PREVALENT
- RiskLens
- riskrecon
- SecurityScorecard

Pen Testing & Breach Simulation

- ATTACKIQ
- Cobalt
- CRONUS CYBER TECHNOLOGIES
- CYBERHAT
- CYCOGNITO
- CYMULATE
- DEPTH SECURITY
- Komodo CONSULTING making security simple
- MAZEBOLT
- NOPSEC
- PCYSYS
- PICUS SECURITY
- RAPID7
- SafeBreach
- SCYTHE
- VERODIN Security. Instrumented.
- XM | DEFENSE BY OFFENSE

GRC

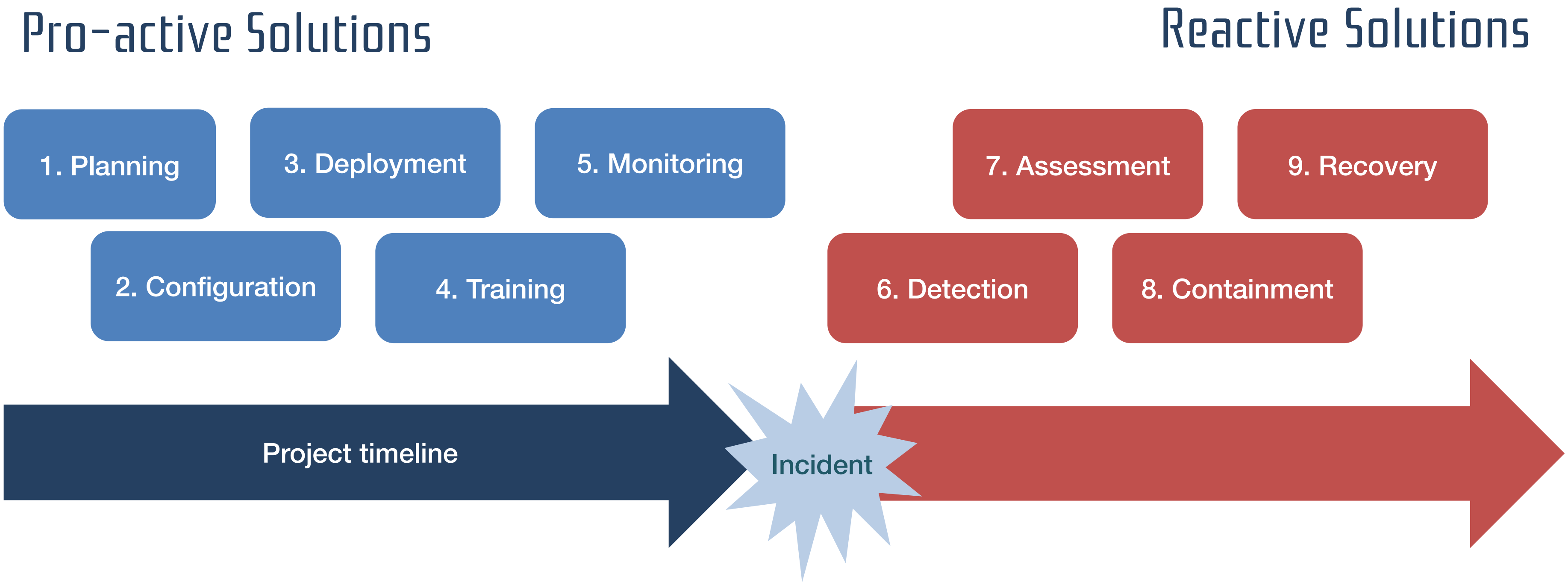
- algosec
- Apptega
- esecure
- Galvanize
- InformationShield
- LockPath
- MetricStream
- netwrix
- Onspring
- RESOLVER
- riskonnect
- RSA
- SAI GLOBAL
- tufin

Security Awareness & Training

- Barracuda
- COFENSE
- CyberVista
- IMMERSIVELABS
- IRONSCALES
- KnowBe4 Human error. Conquered.
- PHISHLABS
- proofpoint
- RANGEFORCE
- SANS
- SECURITY INNOVATION
- SAC the security awareness COMPANY

Source: https://momentumcyber.com/docs/CYBERscape.pdf

Understanding Toolset Scope



Pro-active Solutions

Reactive Solutions

1. Planning

2. Configuration

3. Deployment

4. Training

5. Monitoring

6. Detection

7. Assessment

8. Containment

9. Recovery

Project timeline

Incident

Technology Vetting Checklist

At or above standards

24/7: no gap in execution

Adaptive to changes

Visible and measurable

- ❑ Industry standards and third-party integration supported
- ❑ Value proposition aligned with resiliency objectives
- ❑ Leverages automation and smart workflows for continuous compliance
- ❑ User experience validated by all stakeholders
- ❑ Reports are actionable and include relevant measurements

Industry Perspective: Summary

- Government and organizations are moving towards a **culture of resilience** in which risk-based approaches are the norm.
- Cybersecurity is everyone's responsibility. Compliance can be a **pro-active steppingstone** towards improving resiliency.
- Best practices should be **independent**, **measurable**, and **usable**. Understanding the barriers to adoption is key to succeed.

R&D PERSPECTIVE

“If you really want to protect your network, you really have to know your network”

Rob Joyce – Chief, NSA TAO (Tailored Access Operation)

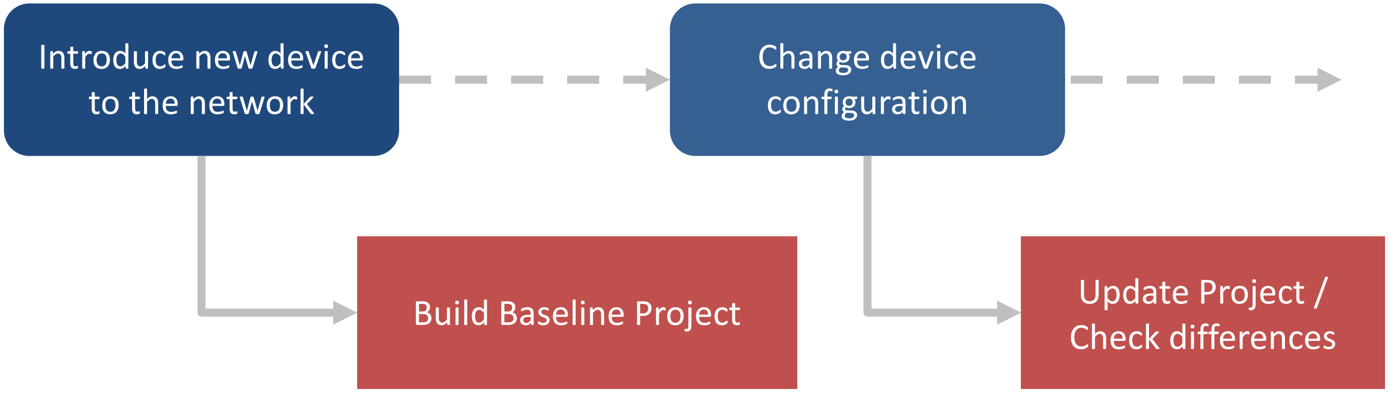
Source: USENIX ENIGMA 2016 https://youtu.be/bDJb8WOJYdA

Why is this still a challenge?

- Growing network complexity
- Variety of proprietary firewall technologies requiring expert knowledge
- Network devices prone to misconfiguration
- Time-consuming tasks to manually review configurations and to ensure compliance with best practices and regulatory standards
- Question keeping practitioners up at night: “Did we miss anything?”

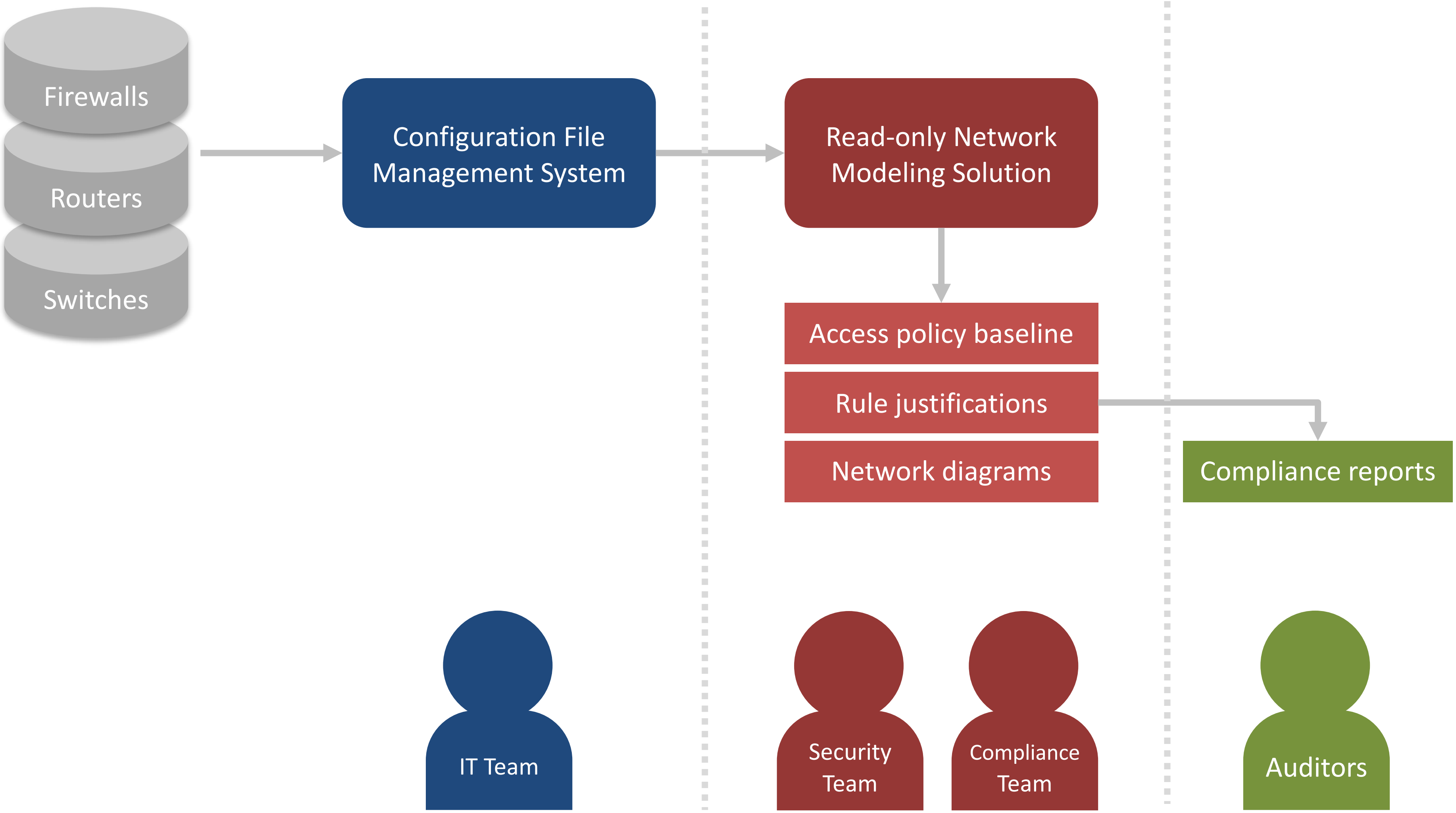
Network Device Change Management

- **Objectives**:
  - – Document implementation and adherence to best practices:
    - Security reports and internal processes
    - Compliance reports
  - – Leverage automation to reduce likelihood of human errors



Introduce new device to the network
Change device configuration
Build Baseline Project
Update Project / Check differences

Separation of Duties



Firewalls

Routers

Switches

Configuration File Management System

Read-only Network Modeling Solution

Access policy baseline

Rule justifications

Network diagrams

Compliance reports

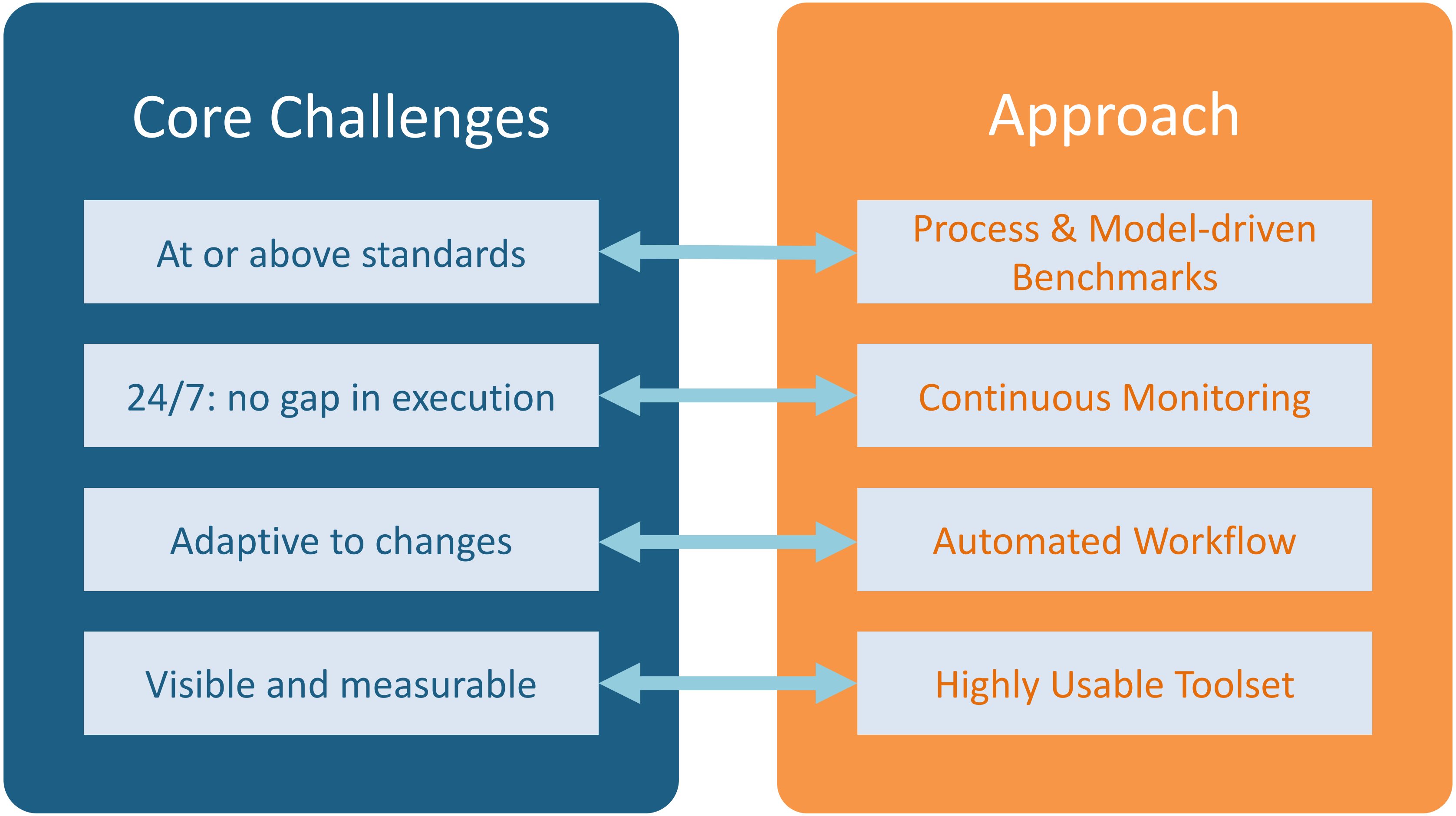
IT Team

Security Team

Compliance Team

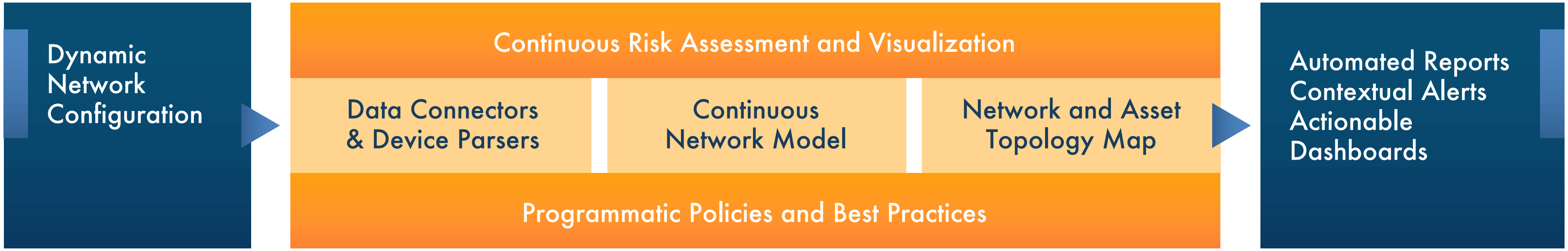
Auditors

Being Pro-Active



Core Challenges	Approach
At or above standards	Process & Model-driven Benchmarks
24/7: no gap in execution	Continuous Monitoring
Adaptive to changes	Automated Workflow
Visible and measurable	Highly Usable Toolset

Configuration Monitoring Workflow



Dynamic Network Configuration

Continuous Risk Assessment and Visualization

Data Connectors & Device Parsers

Continuous Network Model

Network and Asset Topology Map

Programmatic Policies and Best Practices

Automated Reports
Contextual Alerts
Actionable Dashboards

Check Point
SOFTWARE TECHNOLOGIES LTD.

paloalto
NETWORKS

WatchGuard

SEL SCHWEITZER ENGINEERING LABORATORIES

CISCO

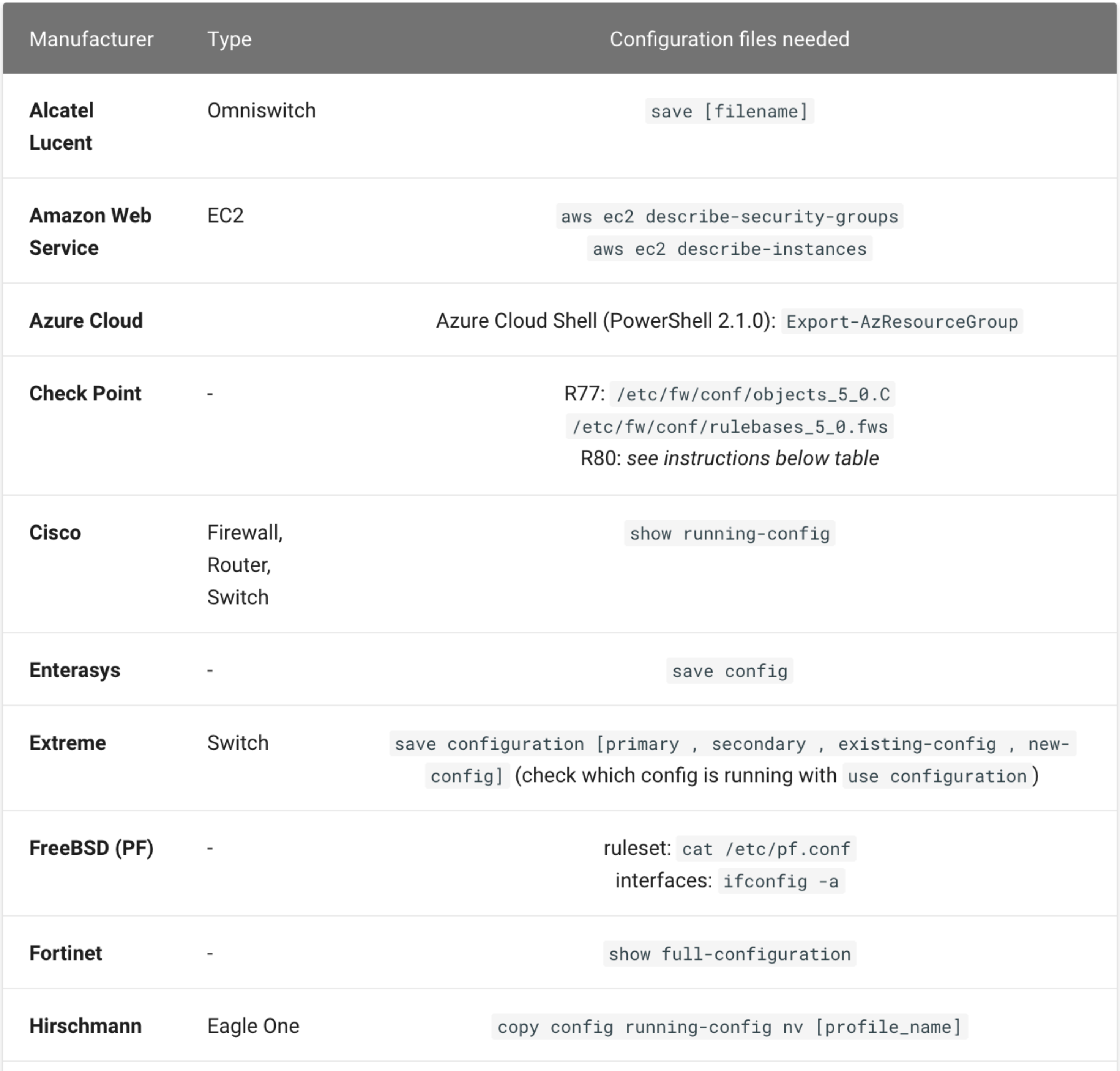
JUNIPER
NETWORKS

FORTINET

Standalone

Server

Cloud

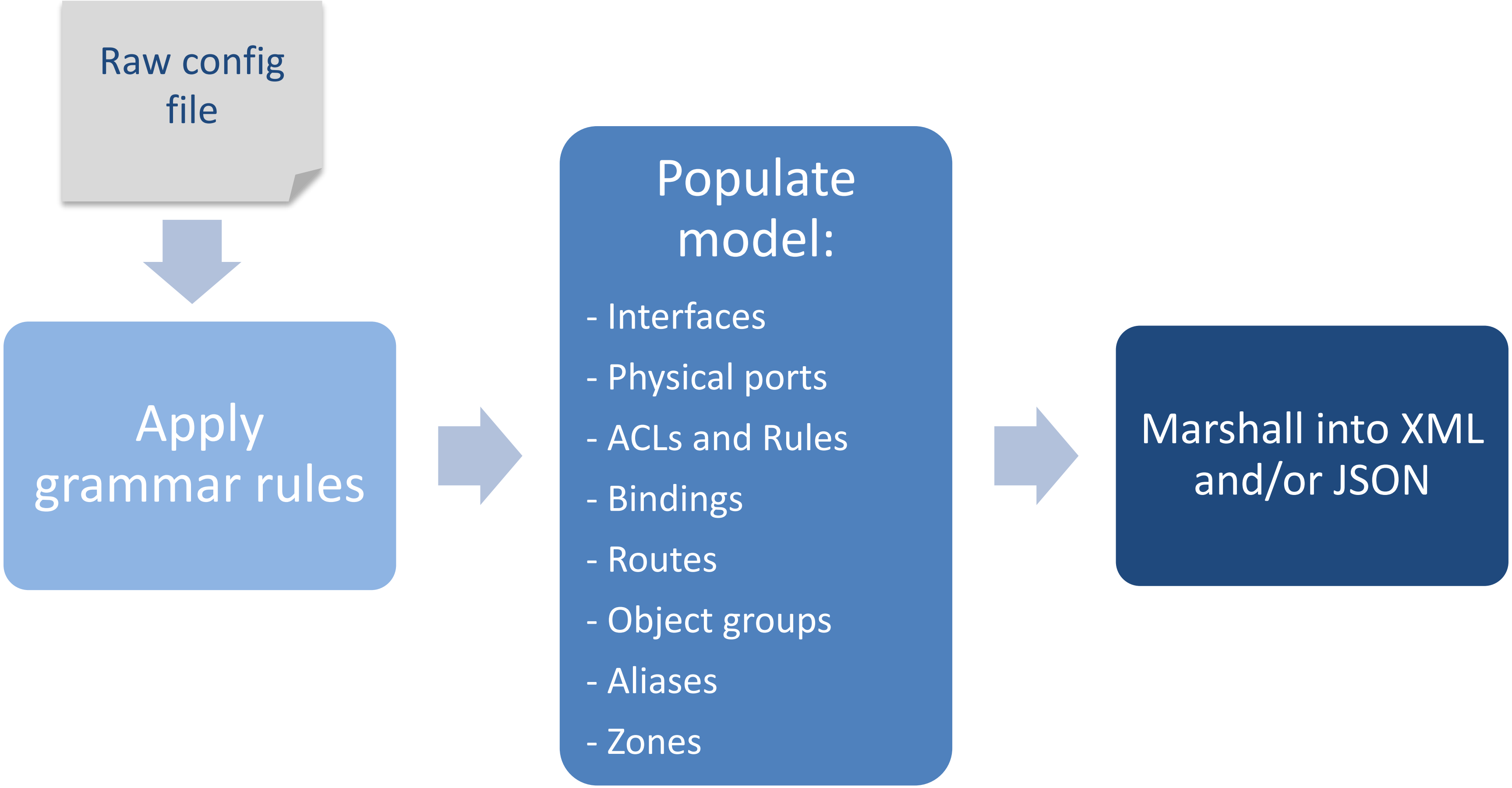


Manufacturer	Type	Configuration files needed
Alcatel Lucent	Omniswitch	`save [filename]`

Amazon Web Service	EC2	`aws ec2 describe-security-groups`
		`aws ec2 describe-instances`

Azure Cloud		Azure Cloud Shell (PowerShell 2.1.0): `Export-AzResourceGroup`
Check Point	-	R77: `/etc/fw/conf/objects_5_0.C` `/etc/fw/conf/rulebases_5_0.fws` R80: *see instructions below table*
Cisco	Firewall, Router, Switch	`show running-config`
Enterasys	-	`save config`
Extreme	Switch	`save configuration [primary , secondary , existing-config , new-config]` (check which config is running with `use configuration`)
FreeBSD (PF)	-	ruleset: `cat /etc/pf.conf` interfaces: `ifconfig -a`
Fortinet	-	`show full-configuration`
Hirschmann	Eagle One	`copy config running-config nv [profile_name]`

Configuration Parsers



Raw config file

Apply grammar rules

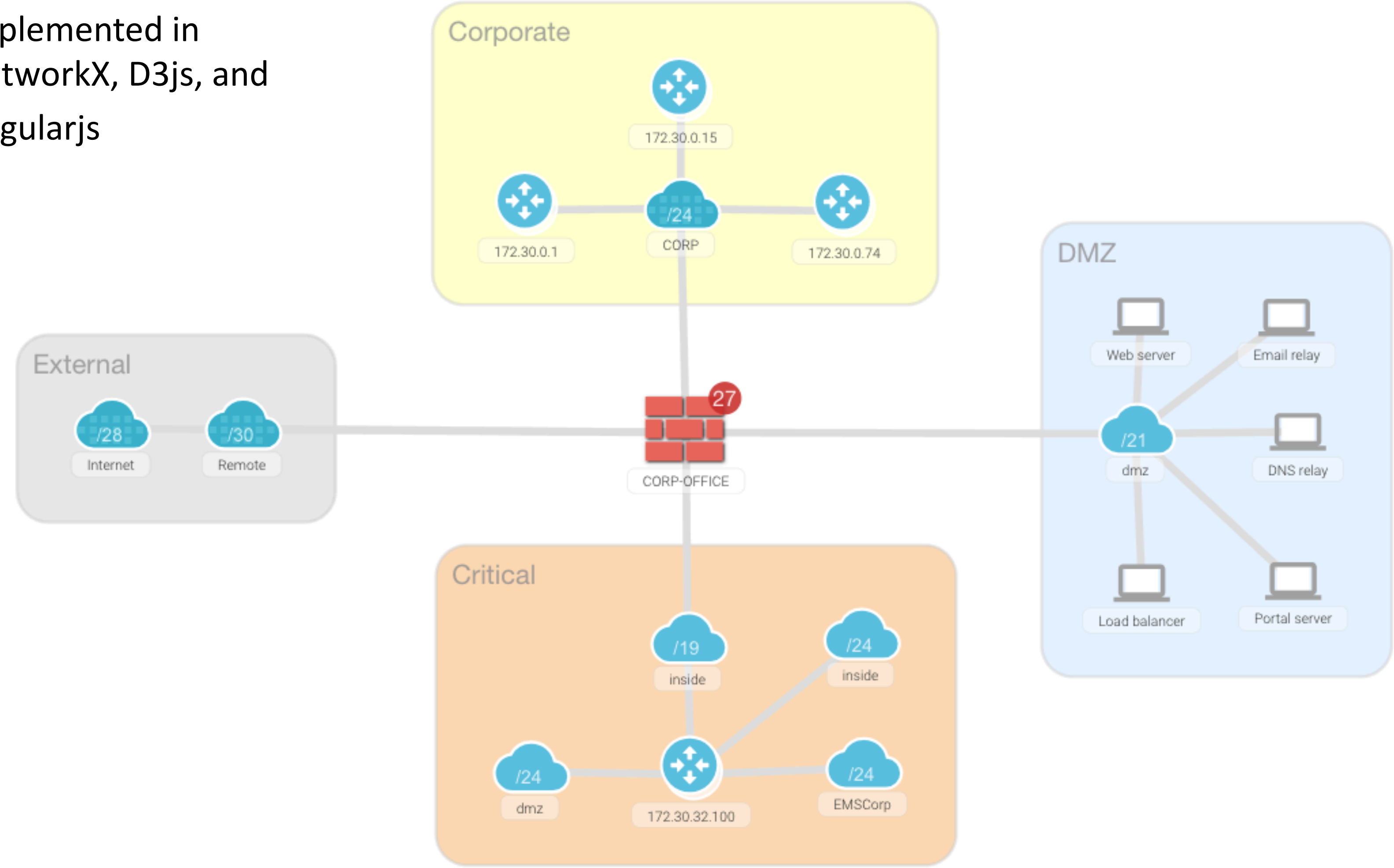
Populate model:

- Interfaces
- Physical ports
- ACLs and Rules
- Bindings
- Routes
- Object groups
- Aliases
- Zones

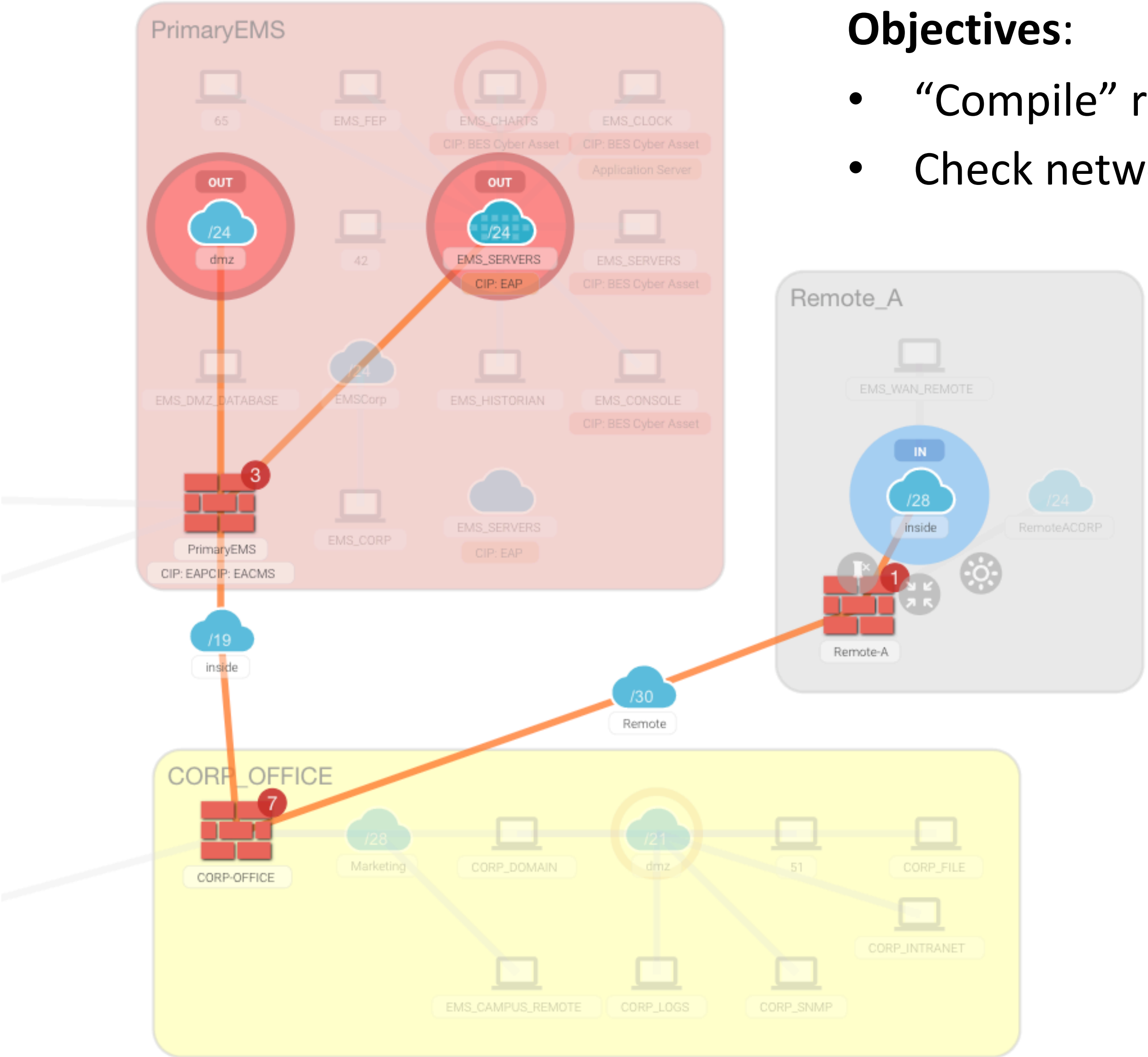
Marshall into XML and/or JSON

Topology Visualization

Implemented in NetworkX, D3js, and Angularjs



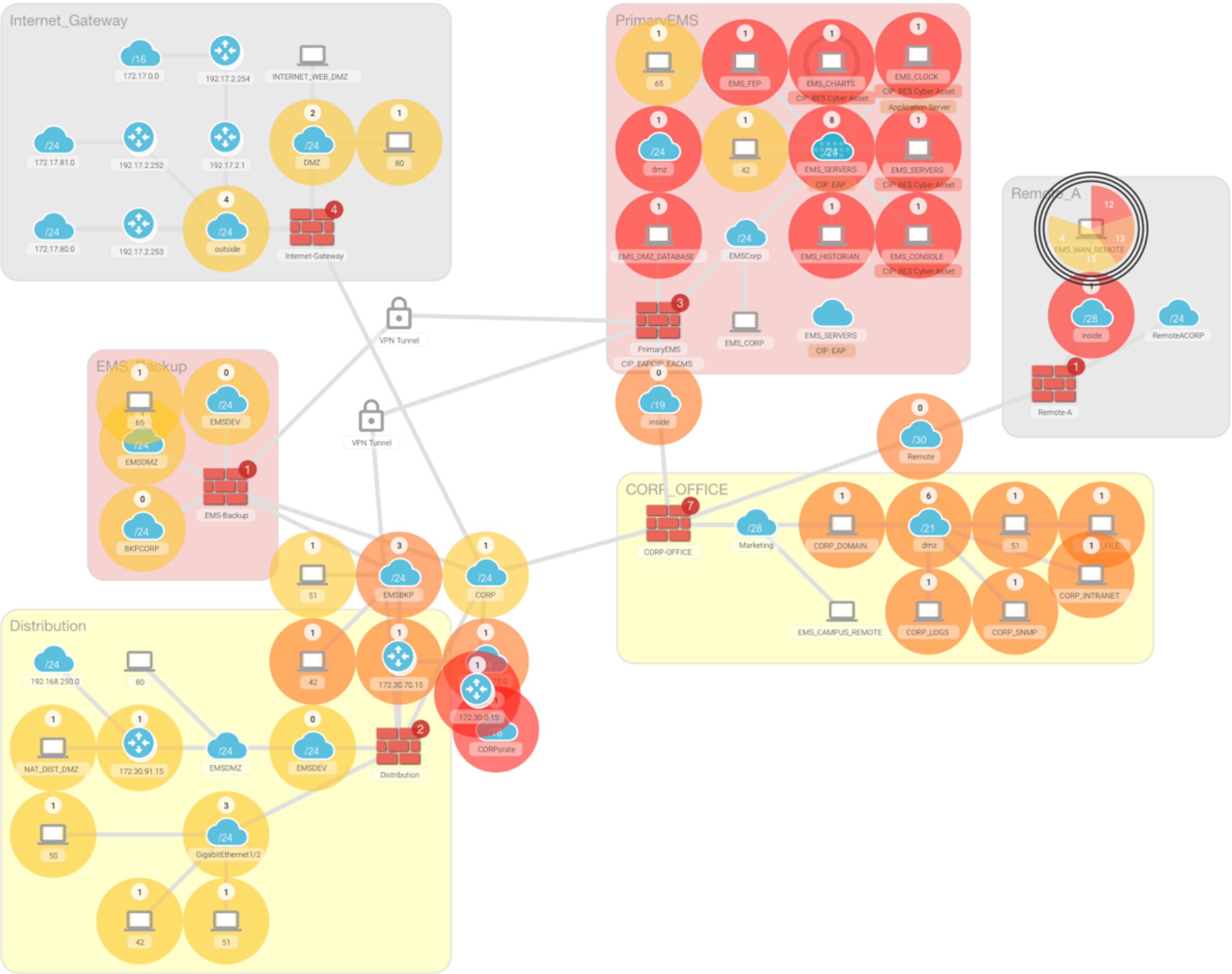
Path Analysis



Objectives:

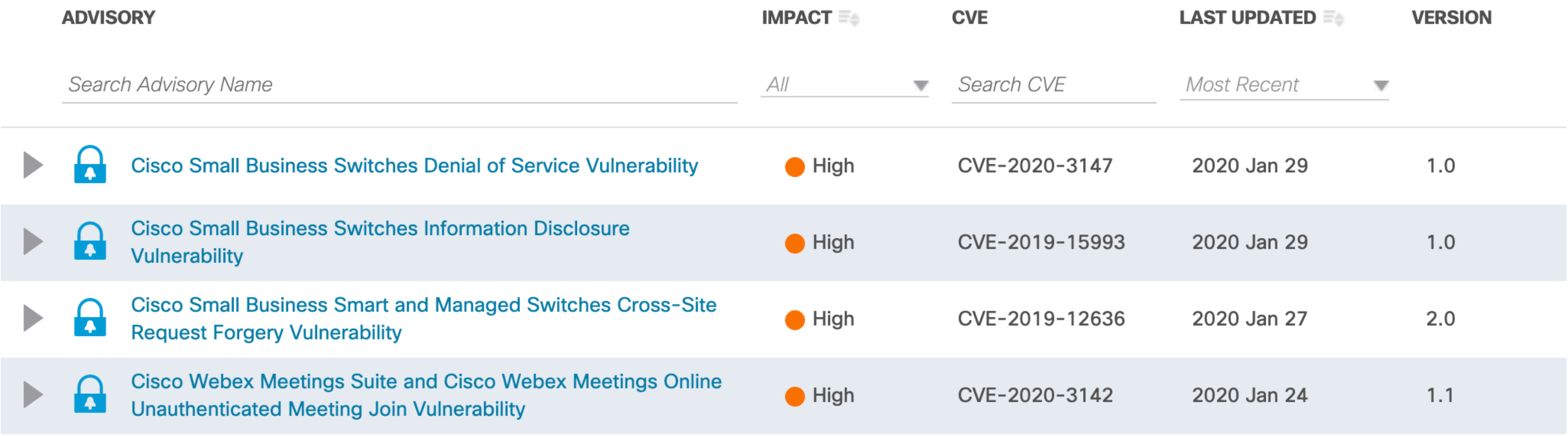
- “Compile” ruleset into paths
- Check network segmentation

Steppingstone Access Map



Vulnerability Exposure

- Network scanner import
  - Nmap
  - Nessus
  - Nexpose
- Security advisories import from device manufacturers



ADVISORY	IMPACT	CVE	LAST UPDATED	VERSION
Search Advisory Name	All ▼	Search CVE	Most Recent ▼	
Cisco Small Business Switches Denial of Service Vulnerability	● High	CVE-2020-3147	2020 Jan 29	1.0
Cisco Small Business Switches Information Disclosure Vulnerability	● High	CVE-2019-15993	2020 Jan 29	1.0
Cisco Small Business Smart and Managed Switches Cross-Site Request Forgery Vulnerability	● High	CVE-2019-12636	2020 Jan 27	2.0
Cisco Webex Meetings Suite and Cisco Webex Meetings Online Unauthenticated Meeting Join Vulnerability	● High	CVE-2020-3142	2020 Jan 24	1.1

Automated Report

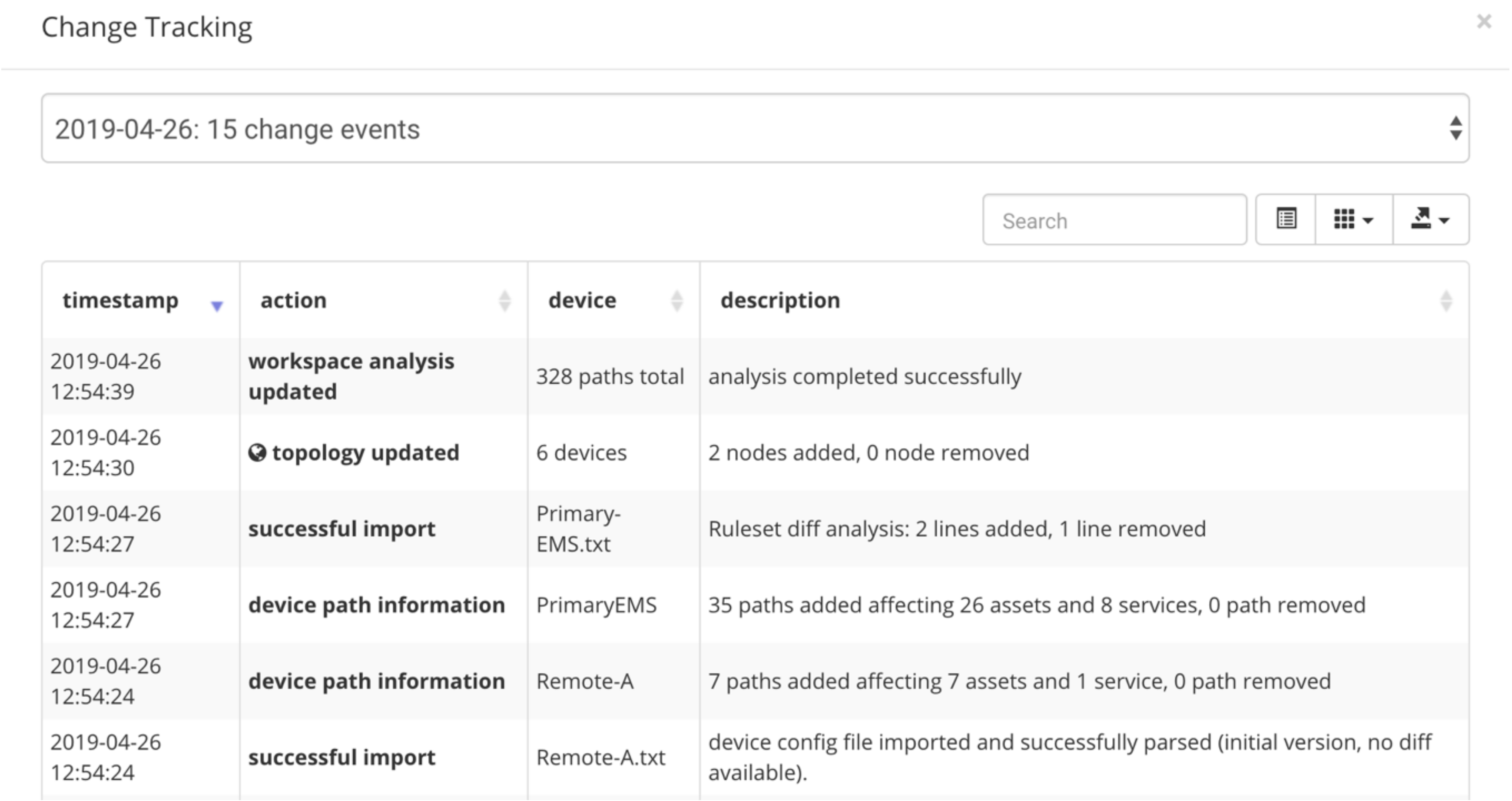
• **Executive Summary**	Findings and recommendations		
• **Ruleset Check**			
– Misconfigurations	E.g., invalid interfaces		
– Object groups	Empty and unused groups		
– Access rules	Unused rules, missing justifications	CIP-003 R1.1.3	CIP-005 R1.3
– Assets	Missing hostnames		
• **Risks Assessment**	Overly permissive rules, risky ports	CIP-003 R1.1.3	CIP-005 R1.3
• **Path Analysis**			
– Network topology	Network zones and criticality		CIP-005 R1.1
– Connectivity matrix	Network segmentation	CIP-003 R1.1.3	R1.2
– Intermediate systems	Jump hosts		R2.1
– Explicit deny by default	Ensure white listing approach		R1.3
• **Next Steps**			

Ruleset Check

- Misconfigurations
  - Duplicate or invalid IP addresses
  - Invalid network zones
  - Invalid interface configuration (e.g., unused security levels)
  - Rules for equipment no longer in service
- Object groups
  - Empty object groups
  - Unused object groups
- Access rules
  - Unused rules (e.g., ACL not bound to an interface)
  - Missing rule descriptions
- Assets
  - Missing hostnames
  - Incomplete asset inventory

Continuous Monitoring

Objective: 24/7 alignment with best practices and regulations



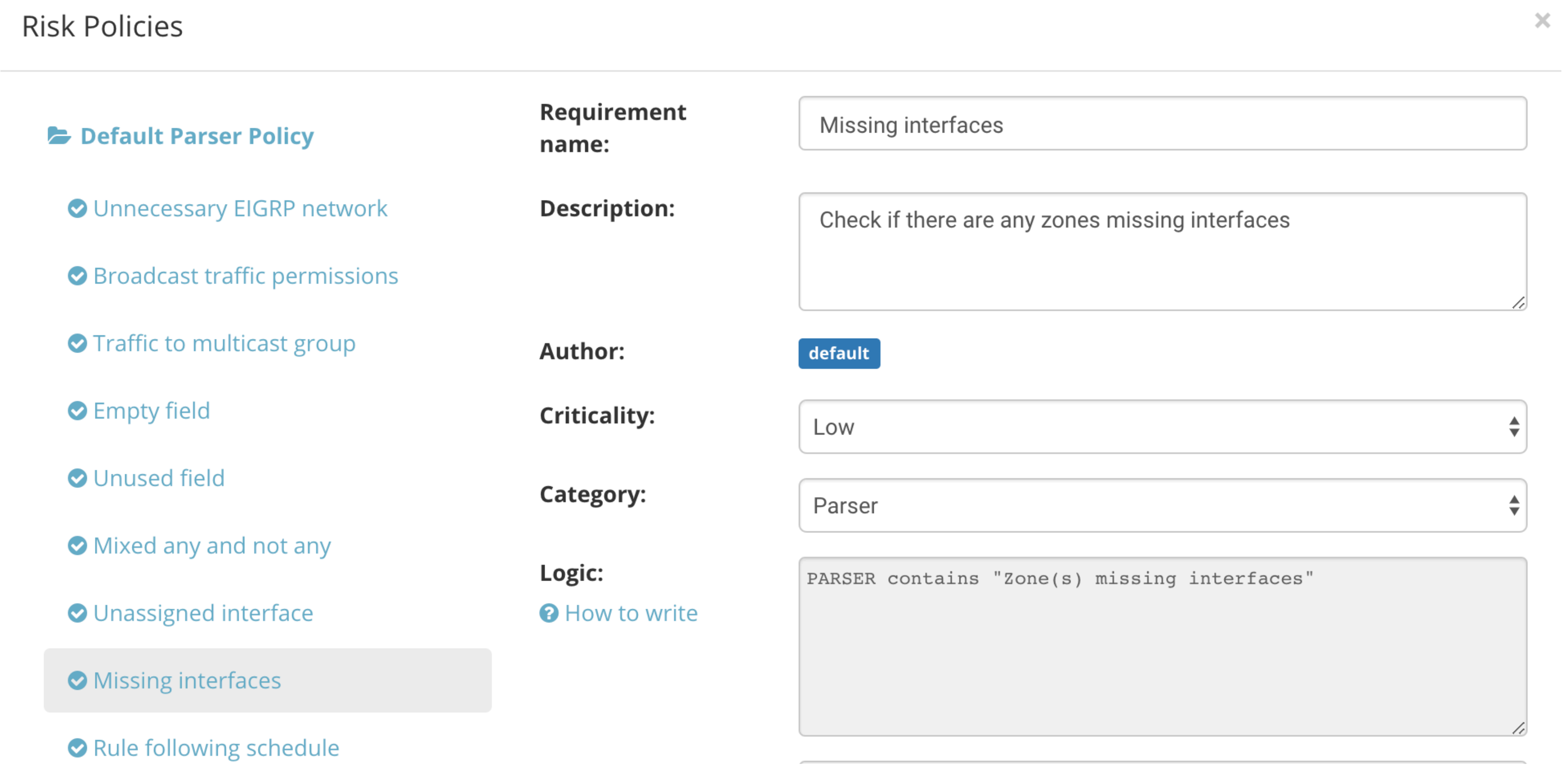
Change Tracking

2019-04-26: 15 change events

timestamp	action	device	description
2019-04-26 12:54:39	**workspace analysis updated**	328 paths total	analysis completed successfully
2019-04-26 12:54:30	**topology updated**	6 devices	2 nodes added, 0 node removed
2019-04-26 12:54:27	**successful import**	Primary-EMS.txt	Ruleset diff analysis: 2 lines added, 1 line removed
2019-04-26 12:54:27	**device path information**	PrimaryEMS	35 paths added affecting 26 assets and 8 services, 0 path removed
2019-04-26 12:54:24	**device path information**	Remote-A	7 paths added affecting 7 assets and 1 service, 0 path removed
2019-04-26 12:54:24	**successful import**	Remote-A.txt	device config file imported and successfully parsed (initial version, no diff available).

Policy Management

- Library of policy requirements:
  - Logic implemented using YARA
  - Pattern matching available for CONFIG, RULE, PATH, PARSER LOGS



Risk Policies ×

Default Parser Policy

- ✓ Unnecessary EIGRP network
- ✓ Broadcast traffic permissions
- ✓ Traffic to multicast group
- ✓ Empty field
- ✓ Unused field
- ✓ Mixed any and not any
- ✓ Unassigned interface
- ✓ Missing interfaces
- ✓ Rule following schedule

Requirement name: Missing interfaces

Description: Check if there are any zones missing interfaces

Author: default

Criticality: Low

Category: Parser

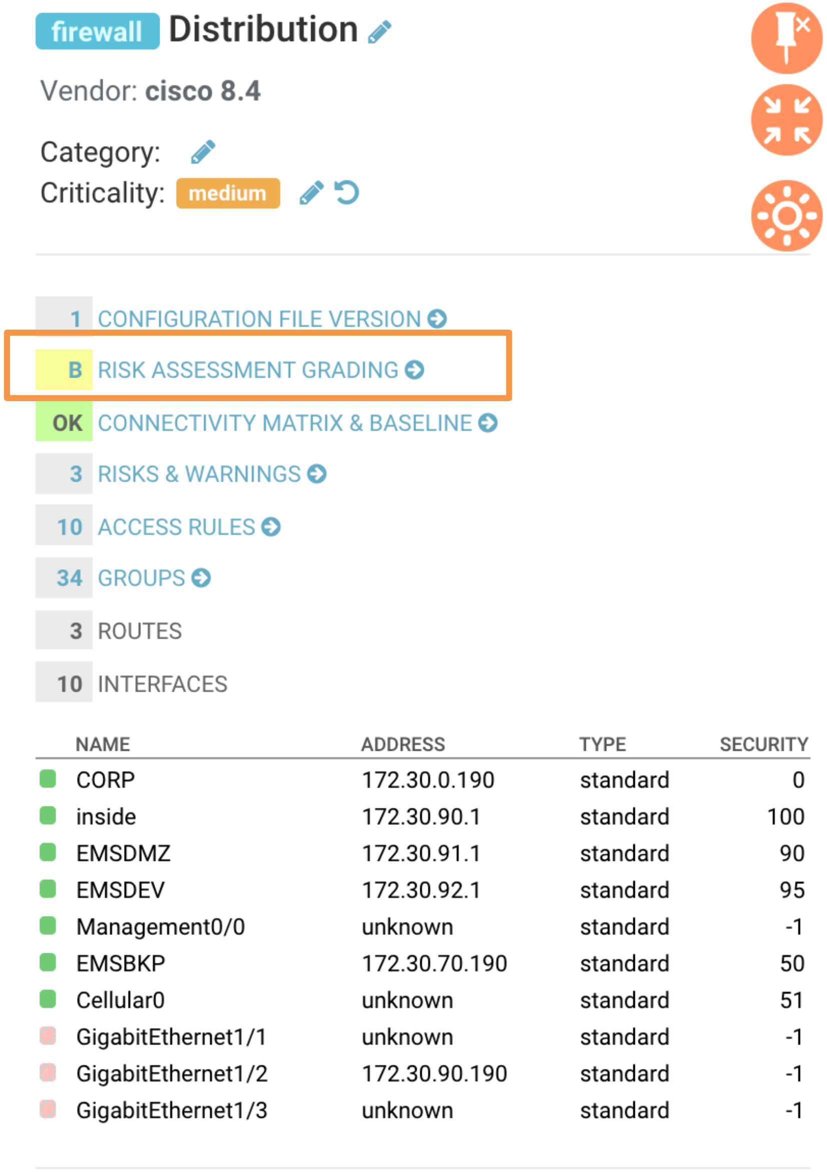
Logic:

? How to write

```
PARSER contains "Zone(s) missing interfaces"
```

Policy Management

- Risk assessment grading:



firewall **Distribution**

Vendor: **cisco 8.4**

Category:

Criticality: medium

1 CONFIGURATION FILE VERSION

B RISK ASSESSMENT GRADING

OK CONNECTIVITY MATRIX & BASELINE

3 RISKS & WARNINGS

10 ACCESS RULES

34 GROUPS

3 ROUTES

10 INTERFACES

	NAME	ADDRESS	TYPE	SECURITY
🟩	CORP	172.30.0.190	standard	0
🟩	inside	172.30.90.1	standard	100
🟩	EMSDMZ	172.30.91.1	standard	90
🟩	EMSDEV	172.30.92.1	standard	95
🟩	Management0/0	unknown	standard	-1
🟩	EMSBKP	172.30.70.190	standard	50
🟩	Cellular0	unknown	standard	51
🟥	GigabitEthernet1/1	unknown	standard	-1
🟥	GigabitEthernet1/2	172.30.90.190	standard	-1
🟥	GigabitEthernet1/3	unknown	standard	-1

Summary

- A **culture of resilience** is changing the way critical infrastructures are organized and brings more resources to dedicated security and compliance groups
- Regulation is now leveraged as a **steppingstone** towards best practices
- Dedicated security and compliance teams are growing and need **highly-usable solutions** to address the increasing complexity of today's networks
- Usability and automation are still critically needed to improve **network situational awareness** in industrial sectors

Network Perception

Robin Berthier
rgb@network-perception.com
(773) 830-4061