CUTAWAY SECURITY

INFOSEC CONSULTANTS

Prioritizing OT Security Efforts:

The Five Tactical Things to Accomplish While Leadership Defines a Security Program

Don C. Weber - @cutaway

Principal Consultant, Founder

© 2020 Cutaway Security, LLC. All Rights Reserved.

Don C. Weber / Cutaway Security, LLC

- SANS Instructor
  - ICS410: ICS / SCADA Security Essentials
  - Hosted: Accessing and Exploiting Control Systems
- ICS Security Assessments
- Penetration Testing
- Security Research

- https://www.cutawaysecurity.com
- https://www.linkedin.com/company/cutaway-security-llc

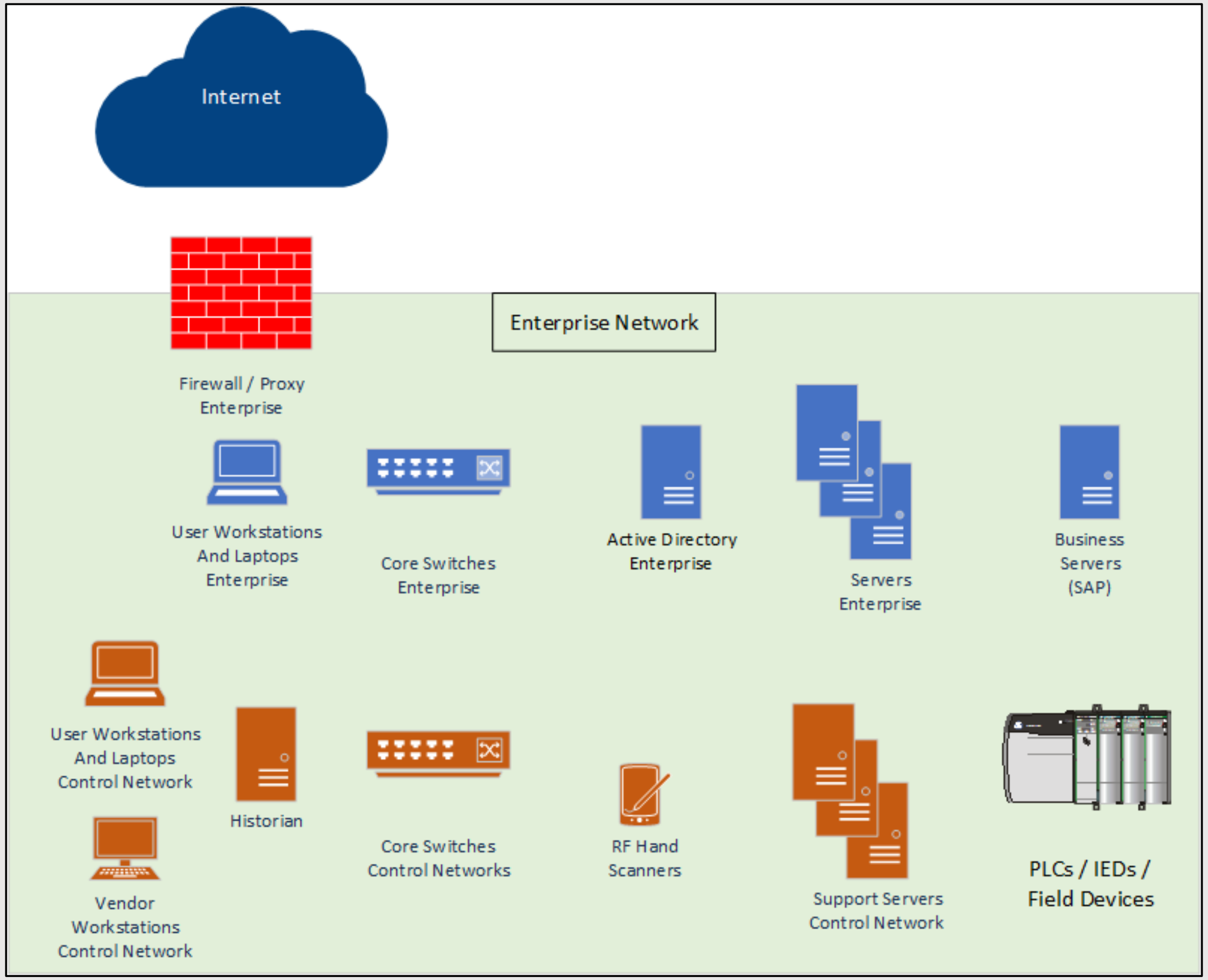
© 2020 Cutaway Security, LLC. All Rights Reserved.

Agenda

- Why are we here?
- Security Programs
- Approaches
- Strategic / Tactical / Operational
- Tactical Direction
- Desired State

© 2020 Cutaway Security, LLC. All Rights Reserved.

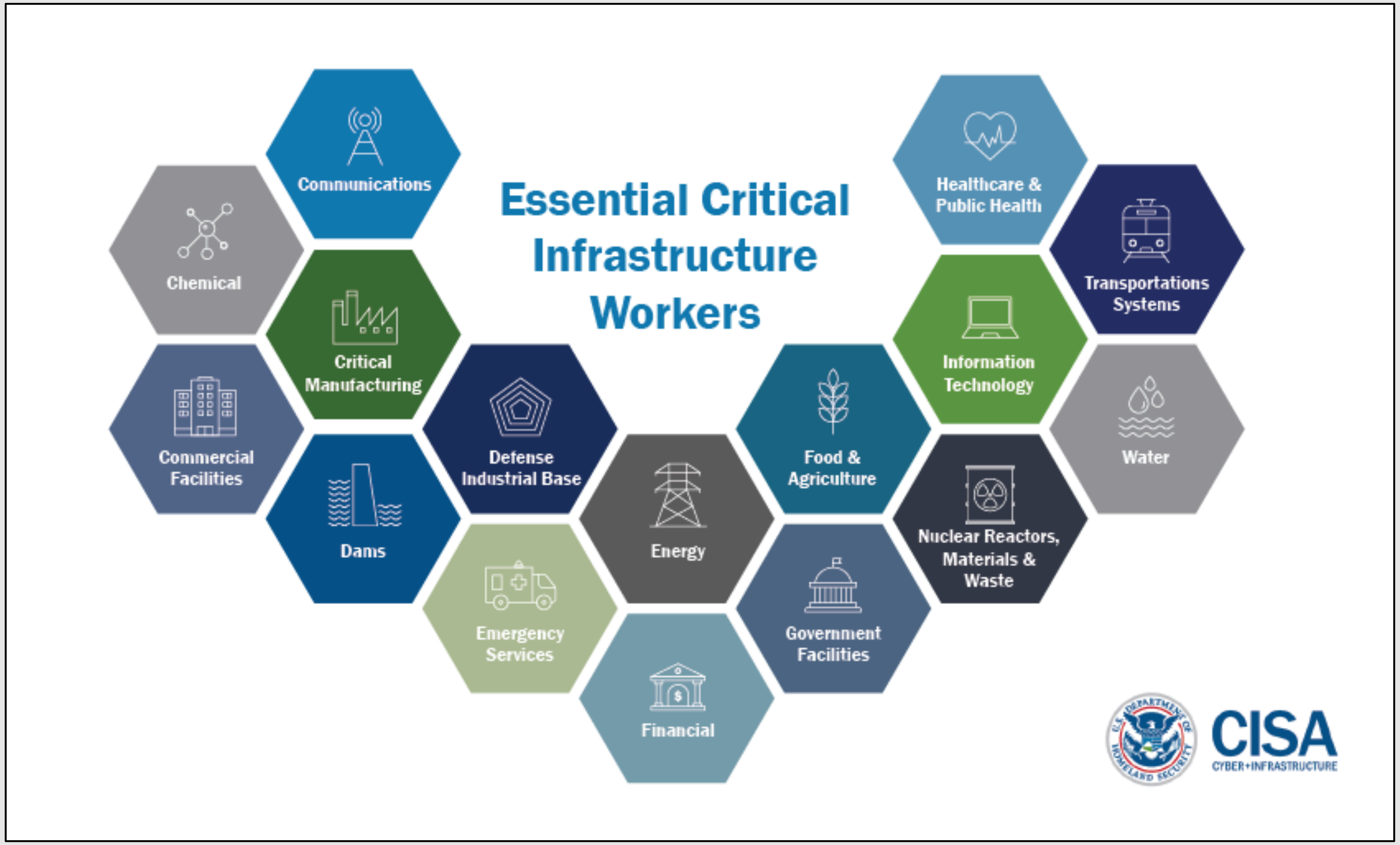
OT Worst Case Scenario


Internet
Firewall / Proxy Enterprise
Enterprise Network
User Workstations And Laptops Enterprise
Core Switches Enterprise
Active Directory Enterprise
Servers Enterprise
Business Servers (SAP)
User Workstations And Laptops Control Network
Historian
Core Switches Control Networks
RF Hand Scanners
Support Servers Control Network
PLCs / IEDs / Field Devices
Vendor Workstations Control Network

© 2020 Cutaway Security, LLC. All Rights Reserved.

OT / ICS Security Programs

- Critical Infrastructure
  - Defined for you
- Non-Critical Infrastructure
  - Fend for yourself



Source: https://www.cisa.gov/identifying-critical-infrastructure-during-covid-19

© 2020 Cutaway Security, LLC. All Rights Reserved.

Cybersecurity Program Guidance

- ISO 27001 – Information Security Management
- NIST 800-53 - Recommended Security Controls for Federal Information Systems and Organizations
  - NIST 800-82r2 - Guide to Industrial Control Systems (ICS) Security
- NIST Cyber Security Framework – a framework to help organizations achieve a better understanding of itself with the goal of improved management to reduce cybersecurity risk.

© 2020 Cutaway Security, LLC. All Rights Reserved.

NIST CSF for OT

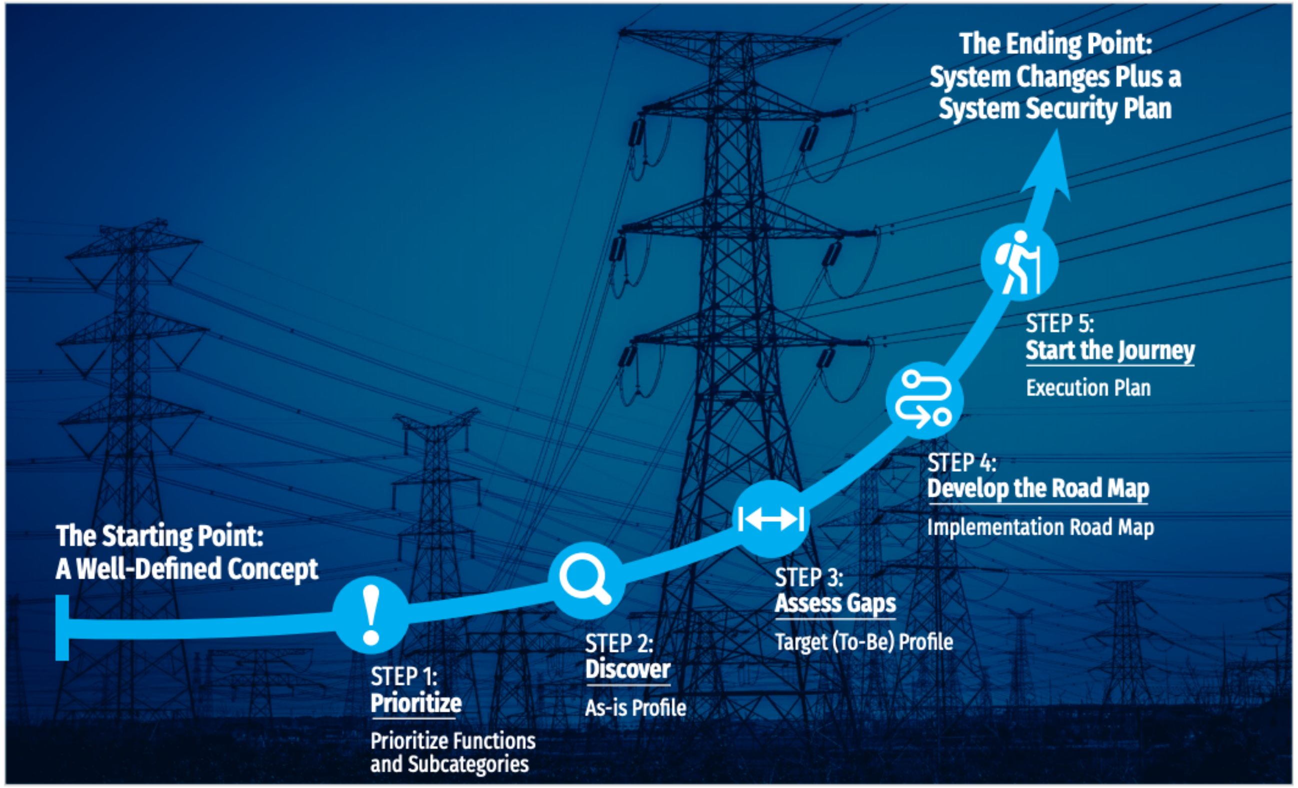


Figure 2. NIST CSF Gap Assessment Process Overview

SANS White Paper: Security by Design: A Systems Road Map Approach by Barb Filkins

Source: https://www.sans.org/reading-room/whitepapers/analyst/security-design-systems-road-map-approach-39370

© 2020 Cutaway Security, LLC. All Rights Reserved.

Strategic Ordering of NIST Functions

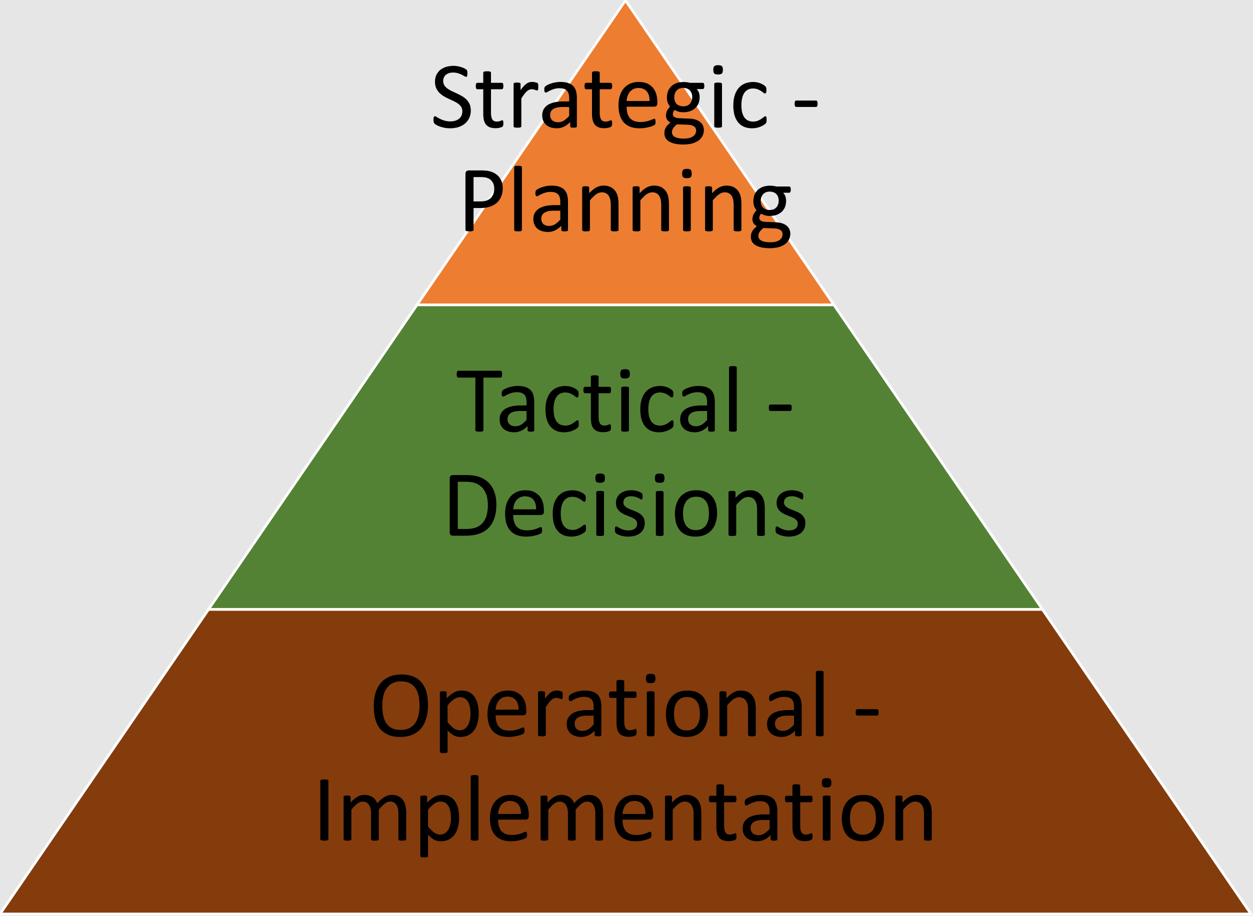
1. Protect – most efficient risk reduction via network architecture
2. Recover – set requirements, obtain management buy-in, test
3. Identify – asset inventory
4. Respond – no sense in detecting if you are not ready to take action
5. Detect – gather information about activity

Ordering the NIST CSF Functions for Efficient Risk Reduction
by Dale Peterson, Digital Bond

Source: https://dale-peterson.com/2020/04/23/ordering-the-nist-csf-functions-for-efficient-risk-reduction/

© 2020 Cutaway Security, LLC. All Rights Reserved.

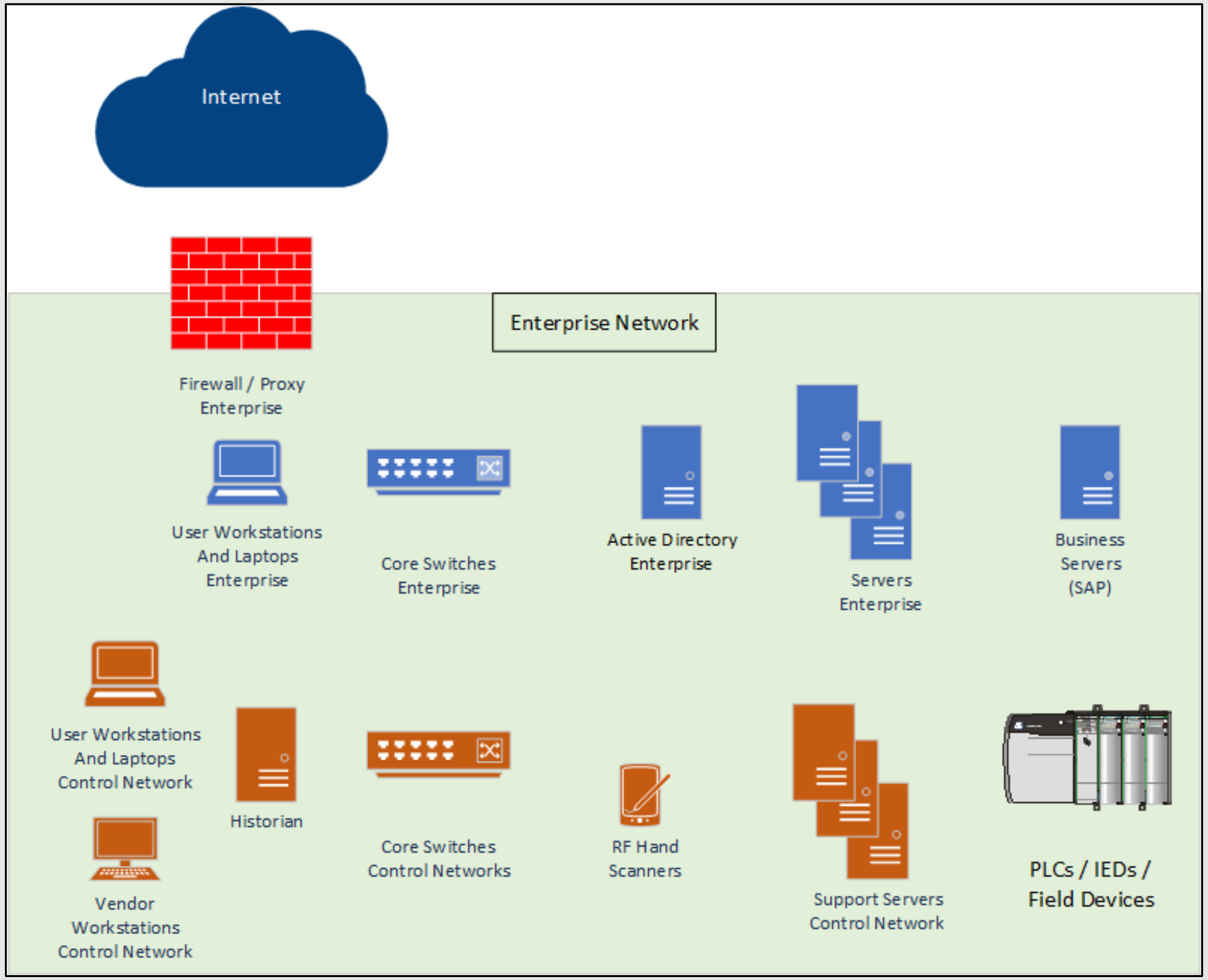
Decision Pyramid



Strategic - Planning

Tactical - Decisions

Operational - Implementation


Internet
Enterprise Network
Firewall / Proxy Enterprise
User Workstations And Laptops Enterprise
Core Switches Enterprise
Active Directory Enterprise
Servers Enterprise
Business Servers (SAP)
User Workstations And Laptops Control Network
Historian
Vendor Workstations Control Network
Core Switches Control Networks
RF Hand Scanners
Support Servers Control Network
PLCs / IEDs / Field Devices

© 2020 Cutaway Security, LLC. All Rights Reserved.

IT / OT Security Effort Prioritization

- Segmentation and Isolation
- Access Control
- Logging and Monitoring
- Asset Inventory
- Incident Response and Recovery

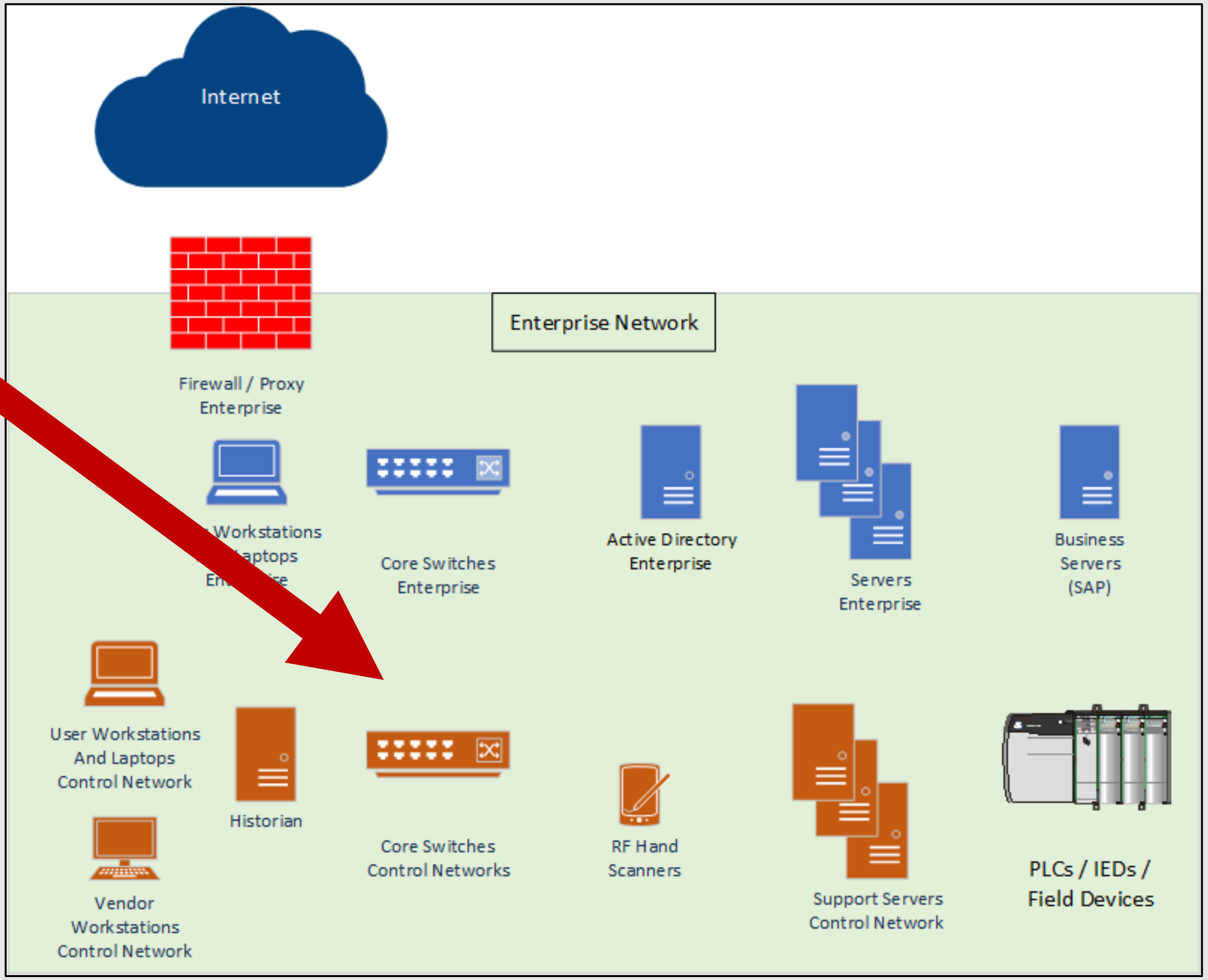
Tactical ICS Security Starts Here

© 2020 Cutaway Security, LLC. All Rights Reserved.

Network Segmentation / Isolation

- Segmentation and Isolation
- Access Control
- Logging and Monitoring
- Asset Inventory
- Incident Response and Recovery

Start With: Enforcement Boundary Between Purdue Level 3 and 4

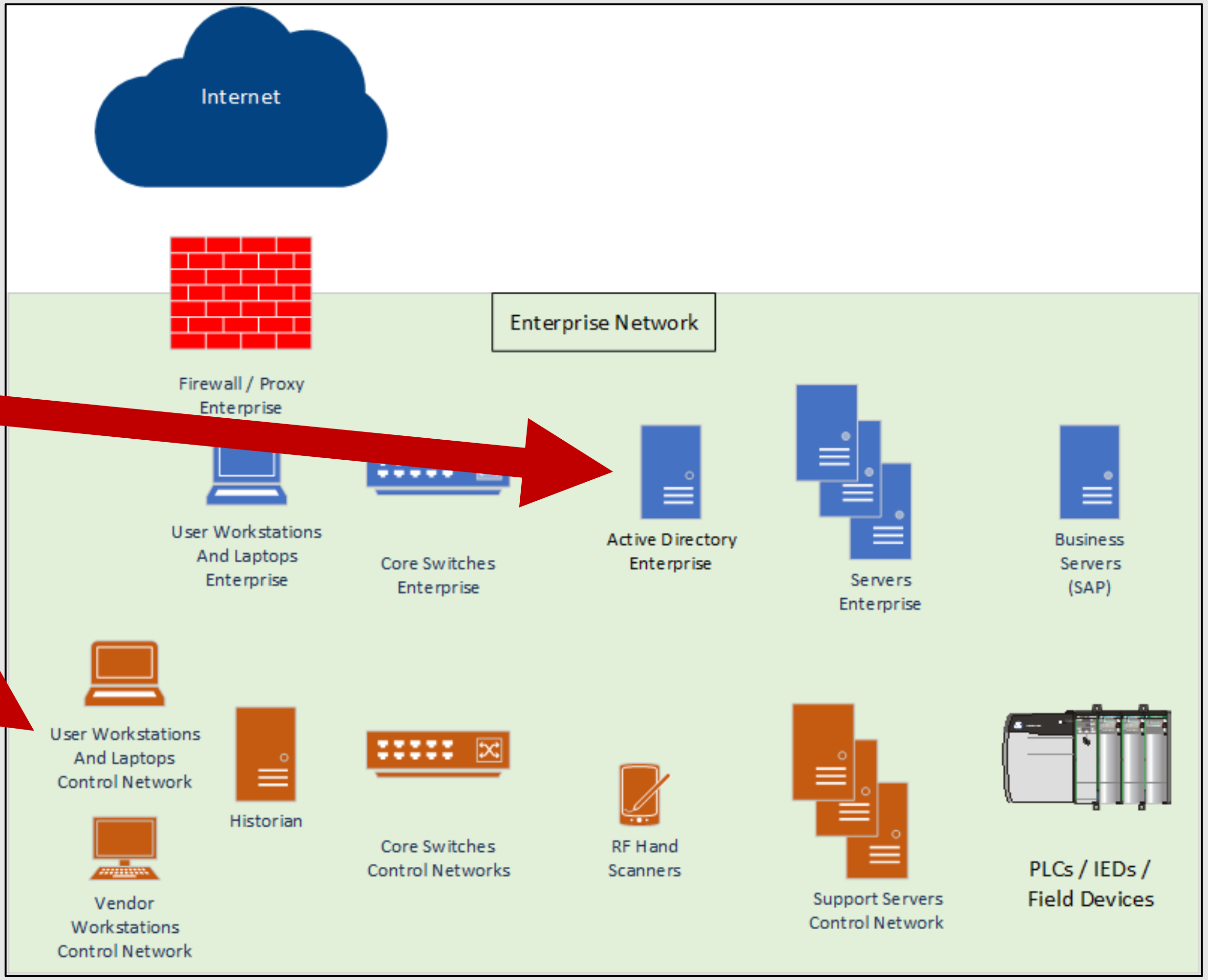

Internet
Firewall / Proxy Enterprise
Enterprise Network
Workstations Laptops Enterprise
Core Switches Enterprise
Active Directory Enterprise
Servers Enterprise
Business Servers (SAP)
User Workstations And Laptops Control Network
Historian
Core Switches Control Networks
RF Hand Scanners
Support Servers Control Network
PLCs / IEDs / Field Devices
Vendor Workstations Control Network

© 2020 Cutaway Security, LLC. All Rights Reserved.

Access Control

- Segmentation and Isolation
- Access Control
- Logging and Monitoring
- Asset Inventory
- Incident Response and Recovery

Start With: Separate Enterprise and Control Accounts and Integrator / Vendor Access

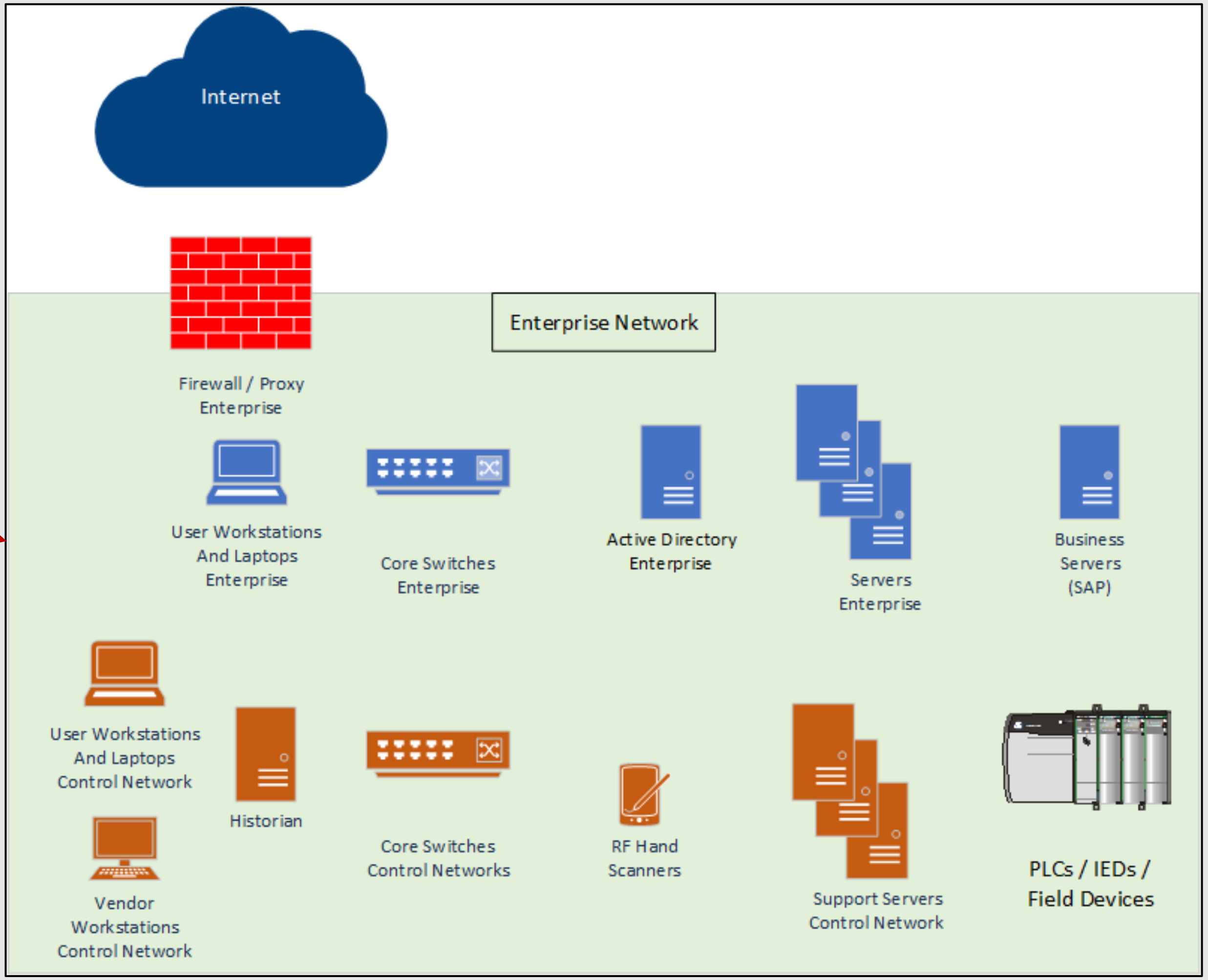


© 2020 Cutaway Security, LLC. All Rights Reserved.

Logging and Monitoring

- Segmentation and Isolation
- Access Control
- Logging and Monitoring
- Asset Inventory
- Incident Response and Recovery

All The Things!!


Internet
Enterprise Network
Firewall / Proxy Enterprise
User Workstations And Laptops Enterprise
Core Switches Enterprise
Active Directory Enterprise
Servers Enterprise
Business Servers (SAP)
User Workstations And Laptops Control Network
Historian
Vendor Workstations Control Network
Core Switches Control Networks
RF Hand Scanners
Support Servers Control Network
PLCs / IEDs / Field Devices

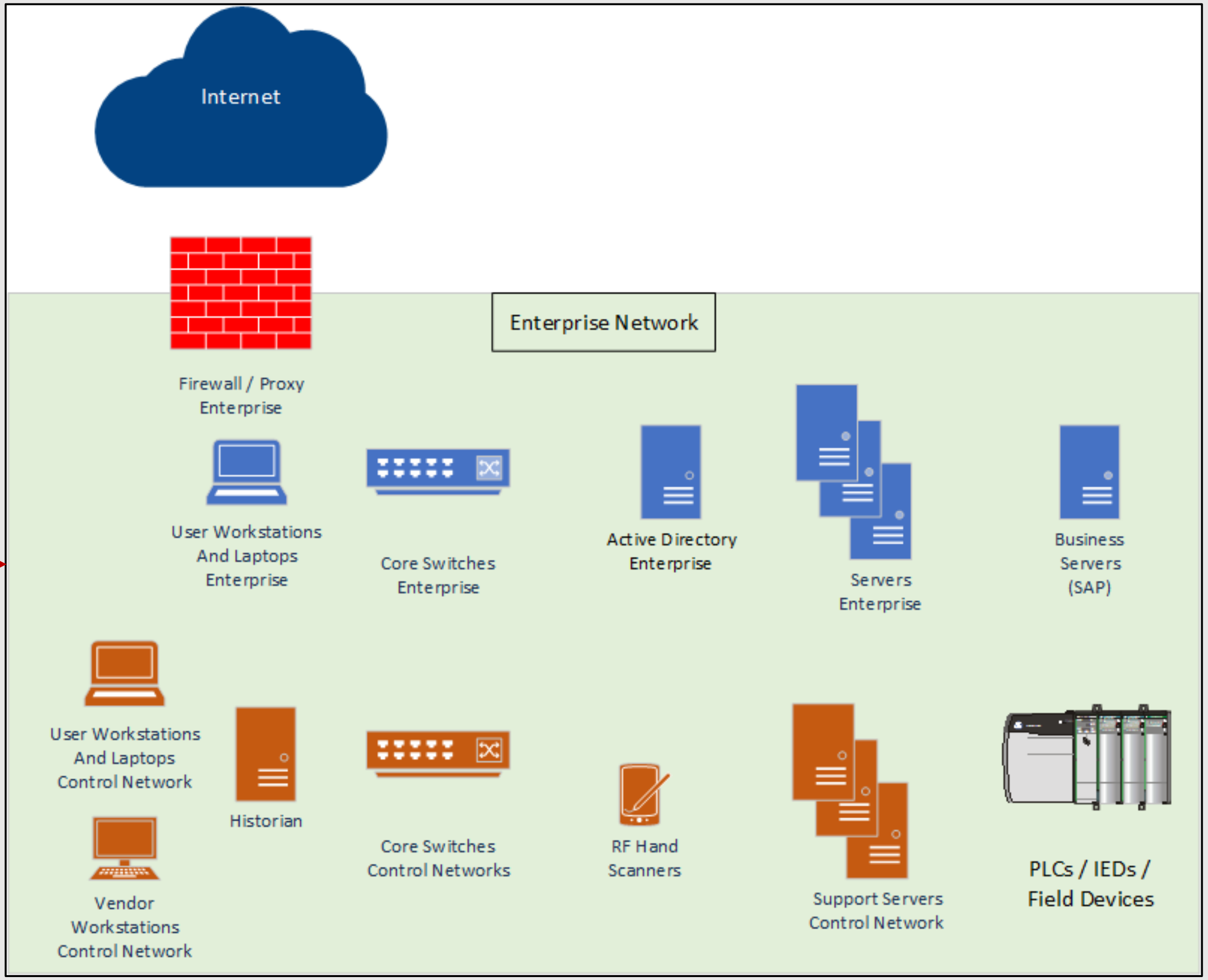
Start With: Increase Master Server Local Log Sizes and Centralize

© 2020 Cutaway Security, LLC. All Rights Reserved.

Asset Inventory

- Segmentation and Isolation
- Access Control
- Logging and Monitoring
- Asset Inventory
- Incident Response and Recovery

All The Things!!


Internet
Enterprise Network
Firewall / Proxy Enterprise
User Workstations And Laptops Enterprise
Core Switches Enterprise
Active Directory Enterprise
Servers Enterprise
Business Servers (SAP)
User Workstations And Laptops Control Network
Historian
Core Switches Control Networks
RF Hand Scanners
Support Servers Control Network
PLCs / IEDs / Field Devices
Vendor Workstations Control Network

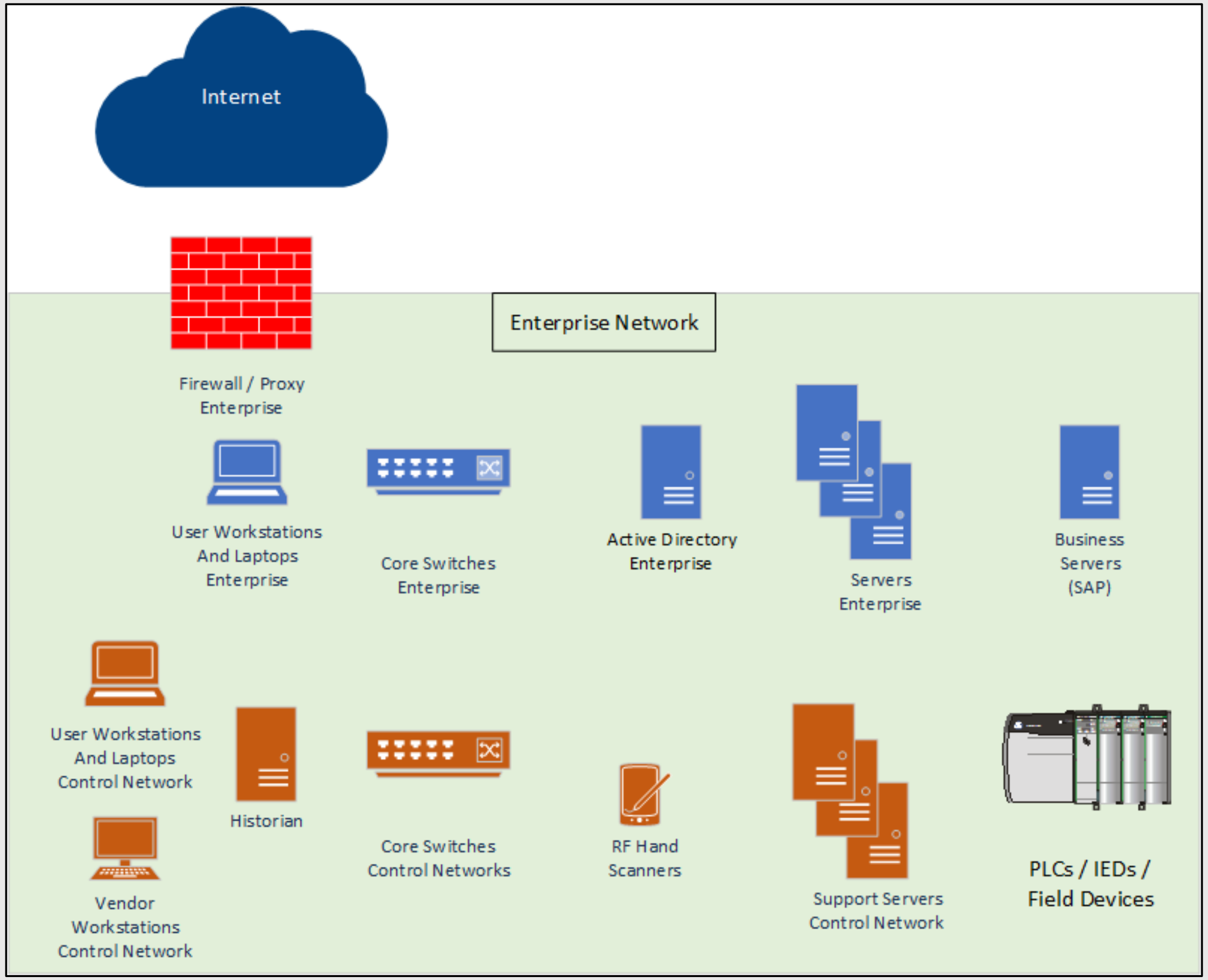
Start With: Passive Information Gathering using Netflow / PCAP

© 2020 Cutaway Security, LLC. All Rights Reserved.

Incident Response

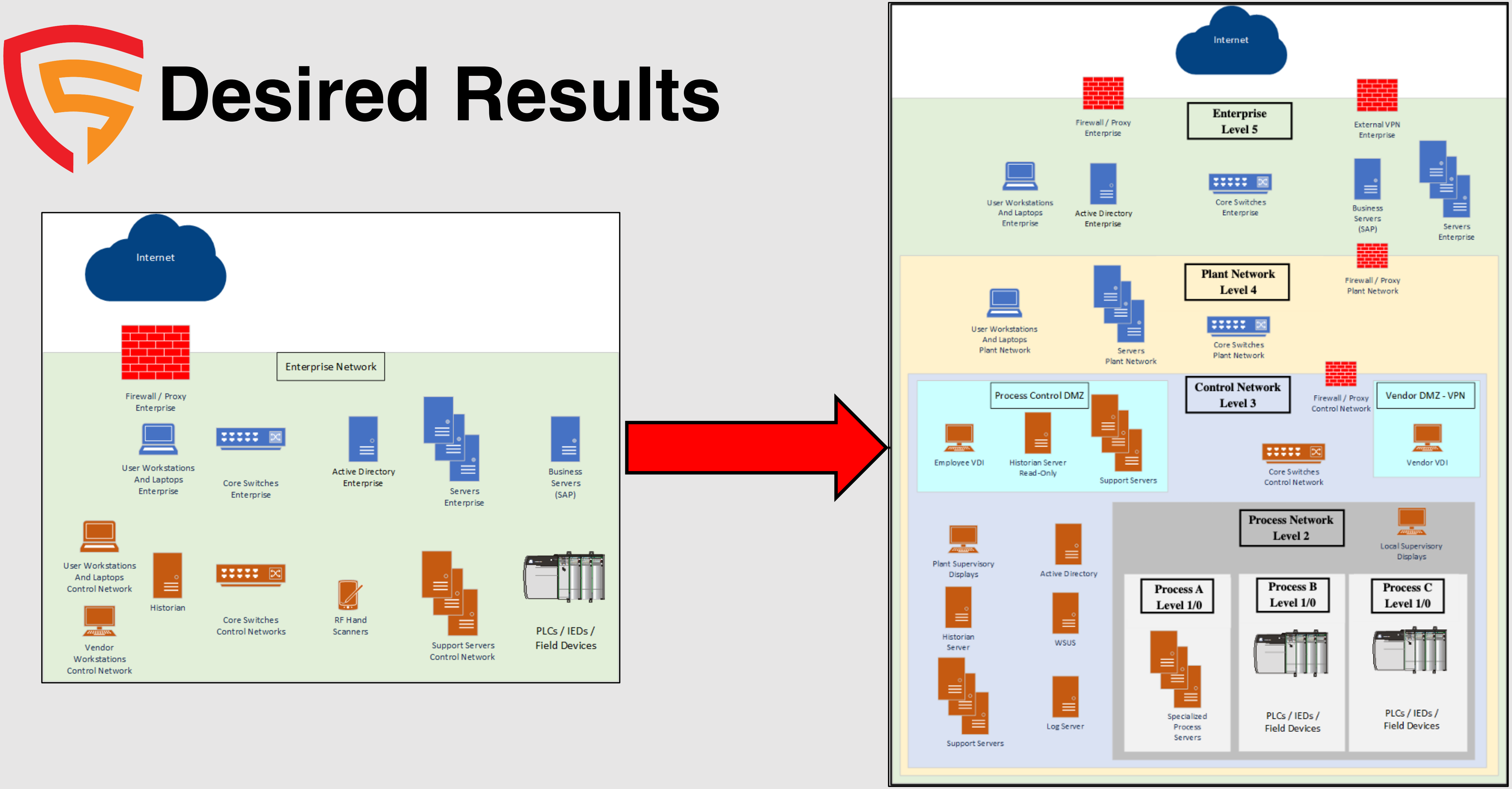
- Segmentation and Isolation
- Access Control
- Logging and Monitoring
- Asset Inventory
- Incident Response and Recovery

Start With: Table-Top Training Exercises with IT / IT Sec / OT Teams


Internet
Enterprise Network
Firewall / Proxy Enterprise
User Workstations And Laptops Enterprise
Core Switches Enterprise
Active Directory Enterprise
Servers Enterprise
Business Servers (SAP)
User Workstations And Laptops Control Network
Historian
Core Switches Control Networks
RF Hand Scanners
Support Servers Control Network
PLCs / IEDs / Field Devices
Vendor Workstations Control Network

© 2020 Cutaway Security, LLC. All Rights Reserved.

Desired Results



© 2020 Cutaway Security, LLC. All Rights Reserved.

Conclusion

- Management needs to provide strategic guidance.
- OT / IT teams need to gather information to feed into the strategic process.
- OT / IT teams need to secure the control networks during the strategery.

© 2020 Cutaway Security, LLC. All Rights Reserved.

CUTAWAY SECURITY

INFOSEC CONSULTANTS

Don C. Weber - @cutaway

don@cutawaysecurity.com
https://www.cutawaysecurity.com

© 2020 Cutaway Security, LLC. All Rights Reserved.