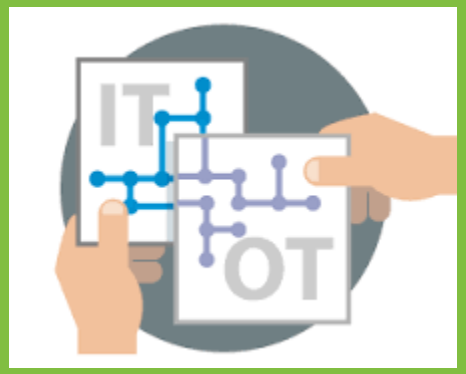
CB Pacific Company Overview

Industrial Technology Solutions

CB Pacific



Cybersecurity Fundamentals & Trends for OT Platforms

Securing SCADA & OT Platforms Product & Technology Workshops

Apr/May 2023

CB Pacific

Introductions

- Greg Santos – CB Pacific Account Manager
- Brad Frayo – CB Pacific Account Manager
- Sheriane Evans – CB Application Engineer
- Pete Miller – CB Application Engineer
- Prasad Pai – GE Director of Automation Product Portfolio
- Alec Granger – GE Product Manager
- Mark Fusick – CB Pacific Account Manager

Agenda

Cyber Security Framework

- Greatest Risks for SCADA Systems
- OT Security Foundations:
  - Identify, Protect, Detect, Respond, Recover
- Challenges in Industrial Operations

Greatest Risks for SCADA Systems

Flat Networks

- Sites with no segmentation and firewall rules.
- OT hardware on the IT Network
- Only segmentation is logical with no access control exposing the network across SCADA platform

Limited Biz Integration

- Infrastructure without abilities to integrate with Biz Apps to modernize operations (IoT meters, GIS, CMMS, Energy Mgmt, ERP, Data Lakes, etc).
- Limiting adoption of new technologies and strategic digital transformation initiatives.

Remote Access

- IT based Remote Access (VPN) was extended to OT environment without considering OT use cases
- No Security at endpoints or required visibility and audit trail to comply with audits.

Remote Sites Security

- Small remote sites (3-5 IP enabled devices) did not have any security at the edge.
- Any changes or network access to remote sites was not tracked and no security was enforced at the edge.

Lack of Access Control

- Lack of Identity Management and Access Controls across all sites. Limited implementation of Active Directory.
- User and Password management was a major maintenance hassle. Lack of accountability as operators and supervisors were sharing passwords.

Asset Management

- Lack of OT asset monitoring. Do not have any visibility of rogue devices connected to the OT network.
- No anti-virus or Endpoint Detection and Response solutions.
- No asset baselining and application behavior monitoring.

Cyber Security Framework

#1 – Identify

POLL#1

Question 1

Do you have an OT Cybersecurity Plan?

Question 2

Is your OT environment segmented from IT environment?

Question 3

Do you know how many SCADA assets you have on your network?

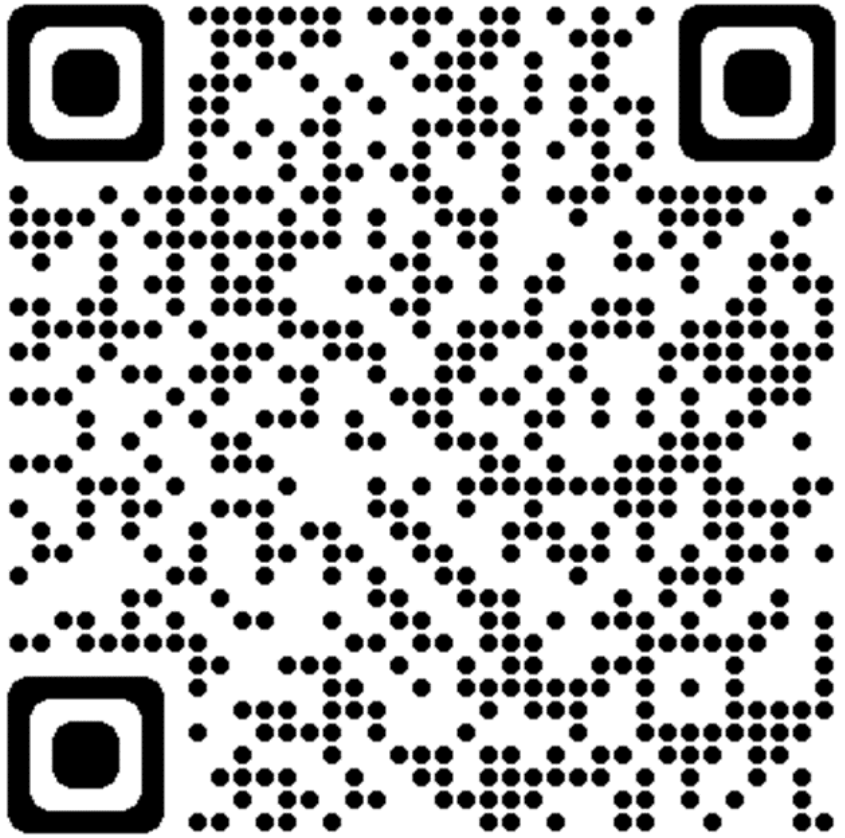
Question 4

Do you know the software version and patch state of all the devices on your network?

Question 5

Would you be interested in knowing where all your assets are in the network and how to mitigate risk across your environment?

CBPacific



OT Cyber Threat Assessment Program (CTAP) Deliverable:

FORTINET

Operational Technology Assessment Report

Prepared For
New Bay Energy
Prepared By
John Smith
Fortinet
Report Date
Sep 15, 2022

Executive Summary

We aggregated key findings from our OT assessment within the Executive Summary below. While the highlights are listed below, a more detailed view of each section follows. Be sure to review the Recommended Actions page at the end of this report for actionable steps your organization can take to protect your OT assets, validate industrial application usage, and identify potentially susceptible OT hosts.

Security

4,172 Application Vulnerability Attacks Detected

3 Malware and/or Botnets Discovered

6 Devices Attempting External Connection

Note that any threats observed within this report have potentially bypassed your existing network security controls, so they should be considered active risks until otherwise fully reconciled.

Applications

84 Total OT Applications Detected

8 Remote Access Applications Detected

32.0% Percentage of OT Traffic

Applications in use within OT environments should be constrained and monitored. Understanding the industrial applications within your network can help define corporate use policies, set access controls on airgapped networks, and minimize unnecessary chatter.

Utilization

2.7GB Total Bandwidth Used

13 Total OT Devices Detected

364.0MB Average OT Bandwidth Per Day

Understanding overall utilization on your OT network can help with capacity planning and streamlining network traffic over time.

Recommendations

- [x] **1. Quarantine Botnet Hosts**
  Botnet activity was detected on at least one host within your network. You should immediate quarantine any botnet hosts (e.g. remove them from the network) and investigate any associated breach activity.
- [x] **2. Reconcile External Remote Access**
  It is not uncommon to use remote access applications to access industrial systems. However, you should audit the remote access applications listed in this report to ensure that only legitimate access is occurring within your OT segment.
- [x] **3. Audit Devices Communicating Externally**
  Devices within an OT environment are normally air-gapped or isolated into specific industrial segments on the network. While running the assessment, we detected devices attempting to communicate externally; this may indicate malicious C&C activity and is worthy of additional investigation.
- [x] **4. Verify Firmware on OT Devices**
  We detected OT specific application attacks on your network. Verify that potentially affected devices are running the latest firmware and are not an exposure risk to application vulnerabilities.
- [x] **5. Audit High Risk Hosts for Attack Susceptibility**
  Some hosts on your network are exhibiting a high degree of suspicious behavior (which could include originating lateral attacks, potential malware installation, or botnet activity detected). Review the hosts most at risk, and quarantine those devices until you can determine the root cause of the suspicious behavior.

CB Pacific

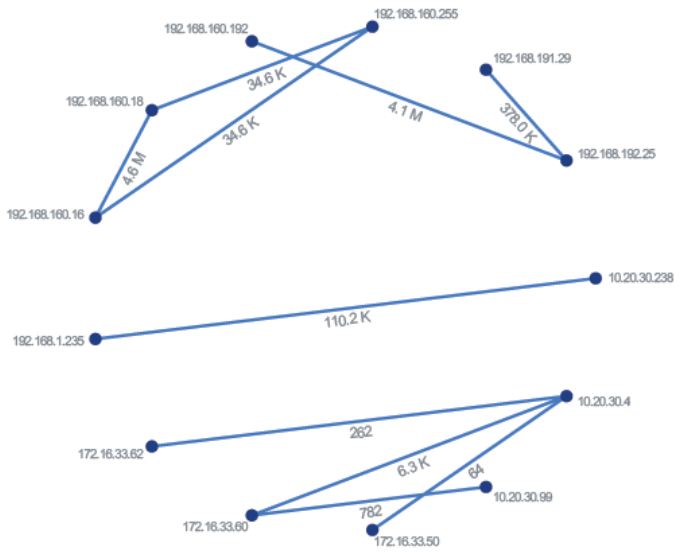
Security

Quick Stats

- **4,172** application vulnerability attacks detected
- **3** malware and/or botnets discovered
- **6** devices attempting external connection
- **6** OT application vulnerability attacks detected

Activity Between OT Devices

Understanding activity derived from the industrial network can be useful when trying to troubleshoot application communications between devices. The visualization below tracks OT device application log counts (which in turn indicates a higher degree of activity). Note that only OT device activity is shown (any host sending/receiving industrial application traffic) and that certain industrial protocols can use multiple function calls over a single extended session.



Applications

Quick Stats

- **84** total OT applications detected
- **8** remote access applications detected
- **32.0%** percentage of OT traffic
- **69%:31%** IT vs. OT Application Mix
- **185** IT applications detected
- **269** total applications detected

High Risk Applications

The FortiGuard research team assigns a risk rating of 1 to 5 to an application based on the application behavioral characteristics. The risk rating can help administrators to identify the high risk applications quickly and make a better decision on the application control policy. Applications listed below were assigned a risk rating of 4 or higher.

#	Risk	Application	Category	Technology	Users	Bandwidth	Sessions
1	5	Proxy.HTTP	Proxy	Network-Protocol	26	332.08 MB	93,688
2	4	Citrix.Receiver	Remote.Access	Client-Server	11	8.25 MB	2,945
3	4	RDP	Remote.Access	Client-Server	4	41.83 MB	200
4	4	VNC	Remote.Access	Client-Server	1	25.53 KB	180
5	4	Splashtop	Remote.Access	Client-Server	1	306.63 KB	18
6	4	Windows.Powershell	Remote.Access	Client-Server	1	9.81 KB	2

High Risk Industrial Applications

Industrial applications which are classified as high risk should be investigated. This table shows the highest risk industrial applications detected on your OT network sorted by risk rating. Typically, industrial applications by their very nature are lower risk, but if there are industrial applications with risk ratings 4+, you should investigate further.

#	Risk	Application	Category	Technology	Bandwidth	Sessions
1	3	IEC.60870.5.104_Control.Functions.Unnumbered	Industrial	Client-Server	6.31 MB	3,688
2	3	Vedeer-Root.ATG.Access	Industrial	Client-Server	5.25 MB	2,475

A Closer Look at "Bad Stuff"

- Depending on the assessment type, we define "bad stuff" as…
  - » NGFW = malware/botnets & high risk applications
  - » Email = malware/botnets, malicious URLs, & impersonations
  - » SD-WAN = malware/botnets & unusual cloud app usage

- So, **what percentage** of total assessments do you think we find "bad stuff" in (e.g. bypassing security controls)?

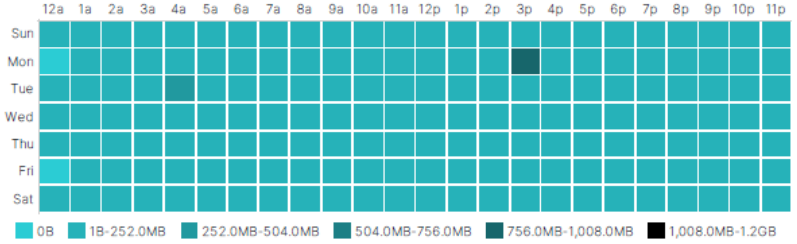
Utilization

Quick Stats

- **2.7GB** total bandwidth used
- **13** total OT devices detected
- **364.0MB** average OT bandwidth per day
- **68%:32%** IT vs. OT bandwidth mix
- **99%:1%** IT vs. OT session mix

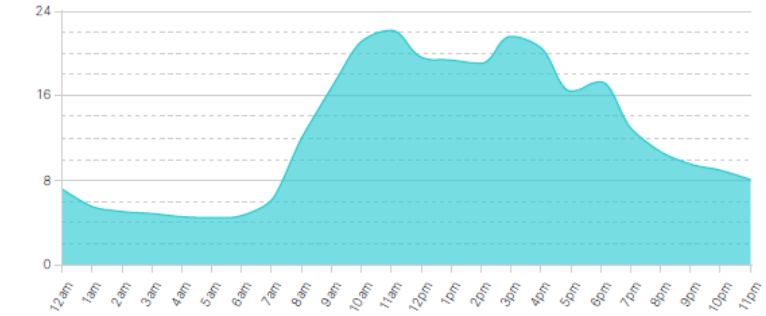
OT Application Bandwidth Utilization

By looking at OT bandwidth usage when distributed over an average day, administrators can better understand their organizational ISP connection and interface speed requirements. Bandwidth can also be optimized on an application basis (using throttling), specific hosts can be prioritized during peak traffic times, and firmware updates can be rescheduled outside of working hours.



Average Log Rate by Hour

Understanding average log rates is extremely beneficial when sizing a security environment from a performance standpoint. Higher average log rates applied to specific hours usually indicate peak traffic usage and throughput. Calculating enterprise-wide log rates can also help when sizing for upstream logging/analytics devices such as FortiAnalyzer. Keep in mind, the log rates presented here are with the full logging capabilities of the FortiGate enabled and will include all log types (traffic, anti-virus, application, IPS, web and system events).



Cyber Security Framework

#2 – Protect

POLL#2

Question 1

Do you have concerns with legacy OT equipment that is not “patchable”?

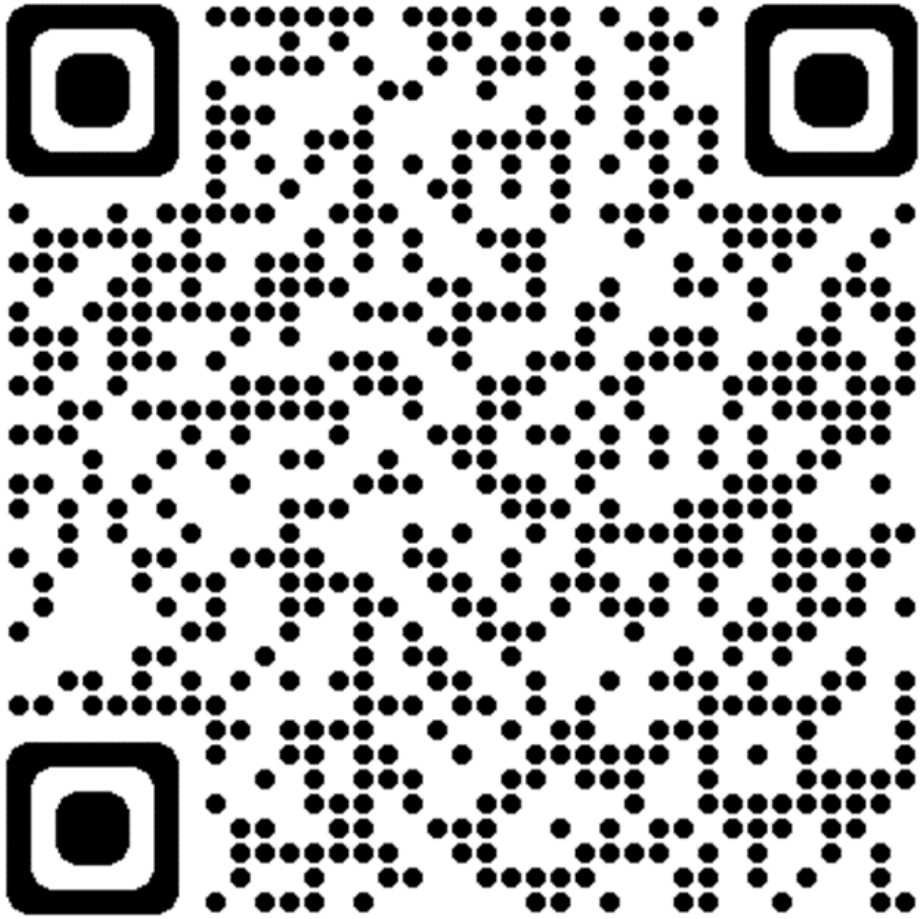
Question 2

Have your OT systems ever gone down due to issues with IT patch management?

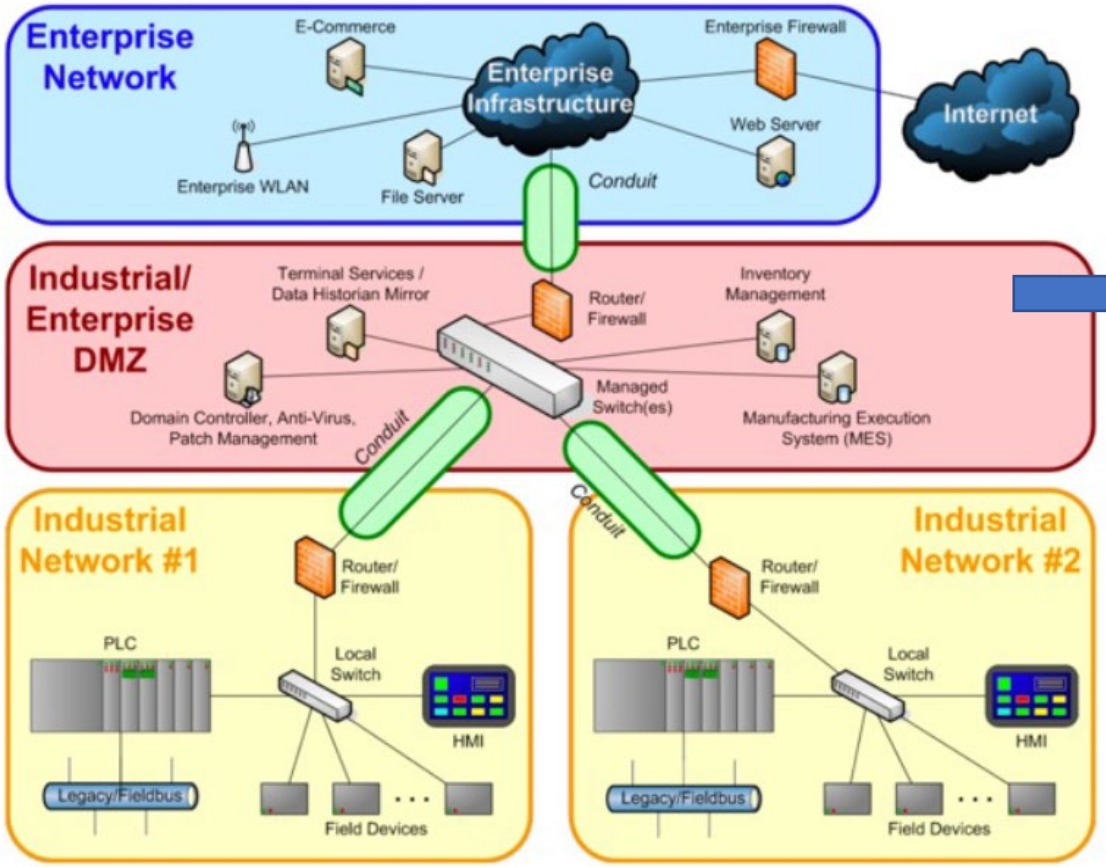
Question 3

Does your organization have multifactor authentication (MFA or 2FA) deployed on all access to OT systems or hardware technologies?

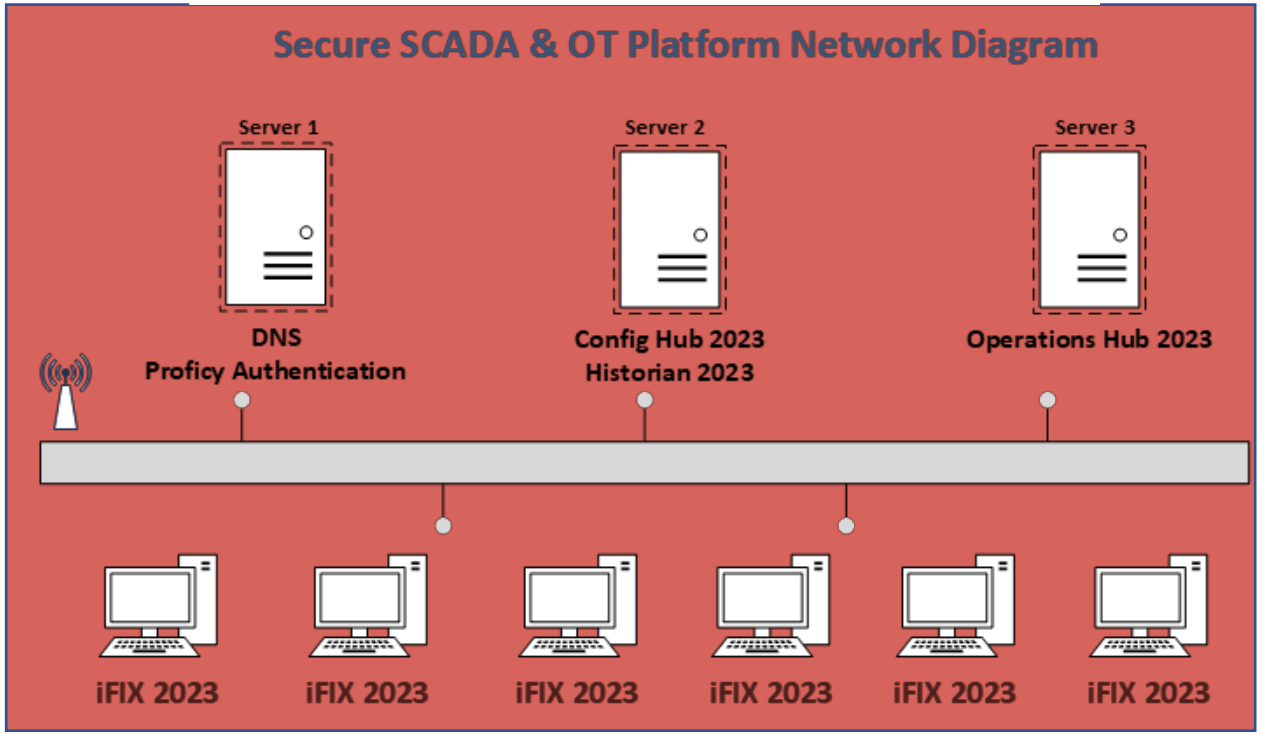
CB Pacific



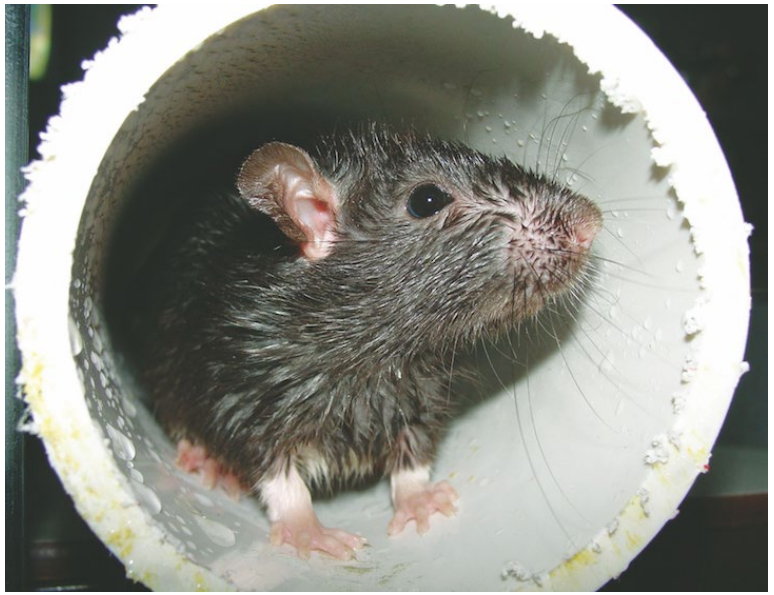
OT Cybersecurity Solutions: Segmentation

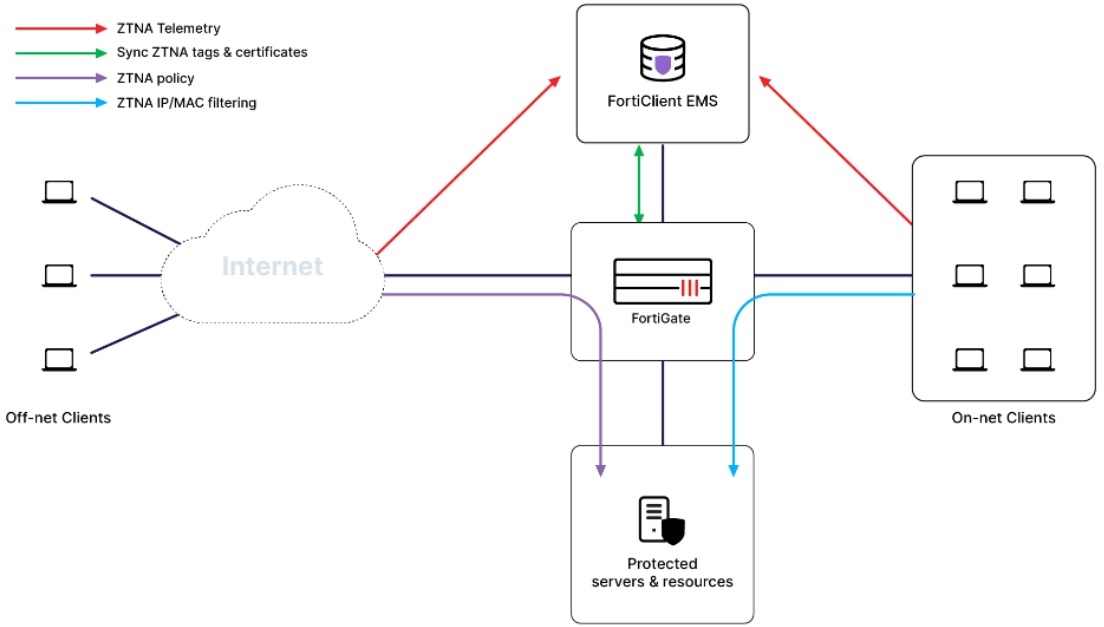


Manufacturing Example



VPN vs ZTNA





Validate the Device - Verify User - Limit Access and Privileges

Cyber Security Framework

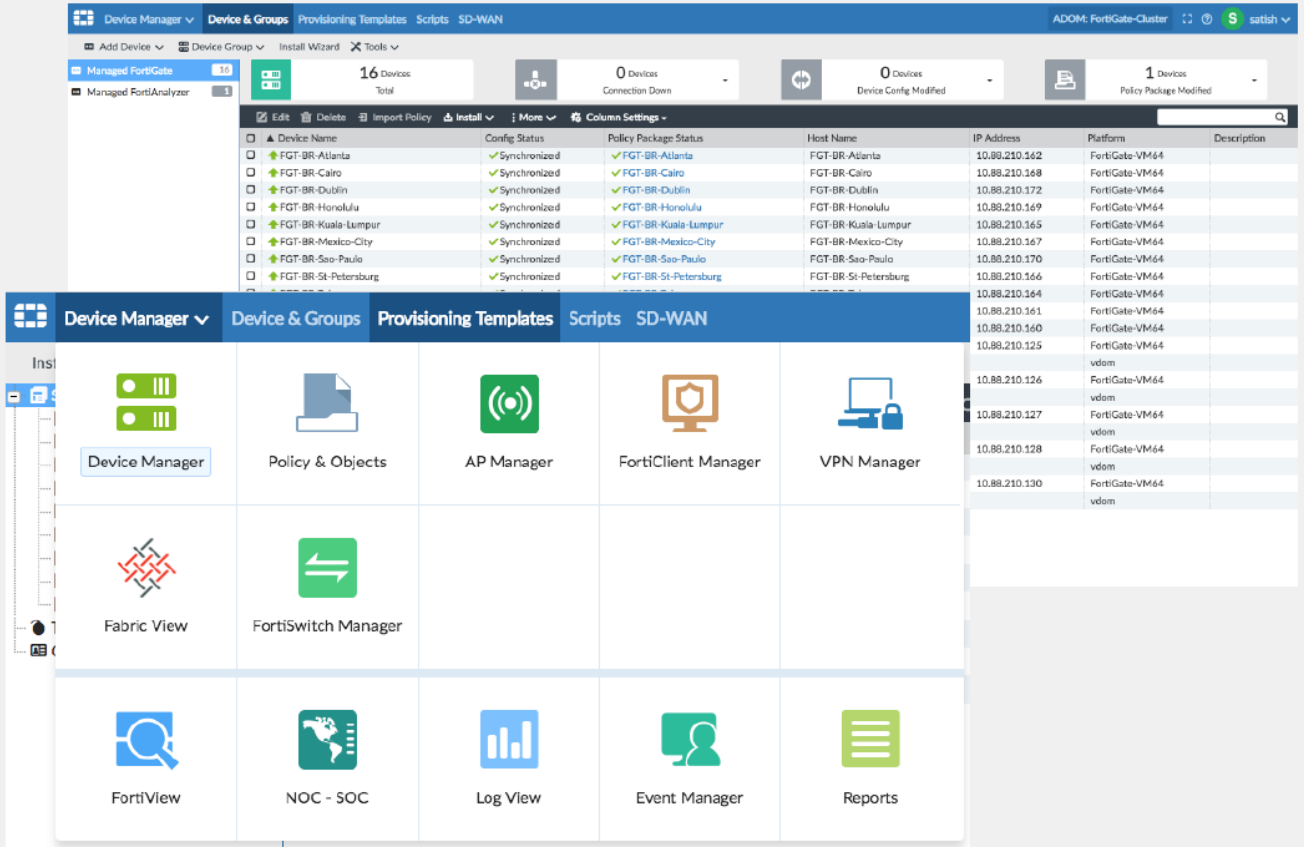
1 Identify | 2 Protect | 3 Detect | 4 Respond | 5 Recover

#3 - Detect

Single Pane of Glass

Enterprise Grade Management

- Centralized policy creation and element management
- Complete Security Fabric Integration



Cyber Security Framework

1 Identify | 2 Protect | 3 Detect | 4 Respond | 5 Recover

#4 - Respond

Follow your plan.

Update Cybersecurity Policy and Plan with Lessons Learned

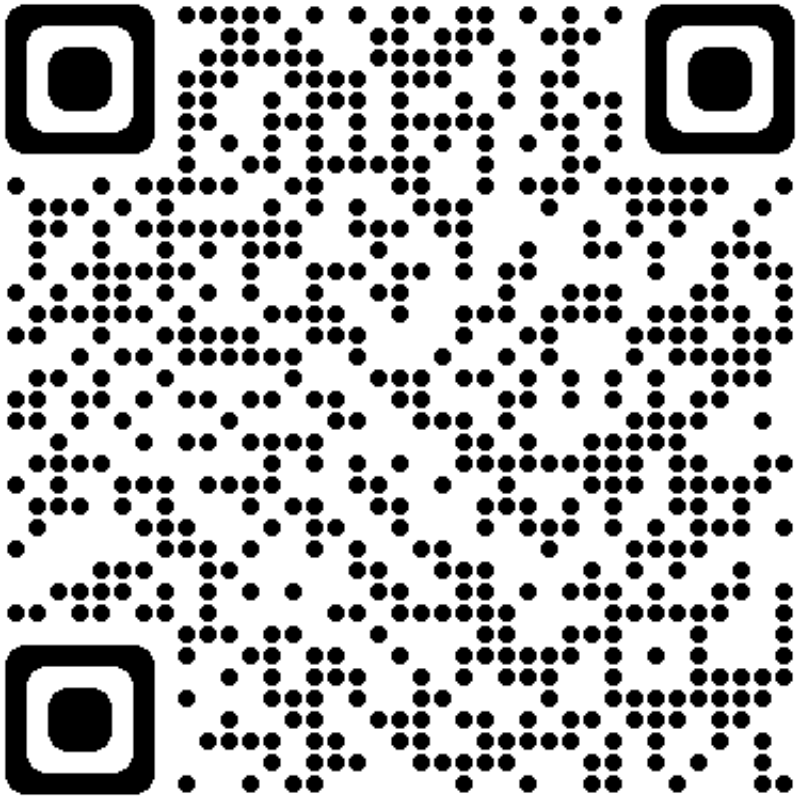
Test your plan

Cyber Security Framework

1 Identify | 2 Protect | 3 Detect | 4 Respond | 5 Recover

#5 – Recovery

POLL

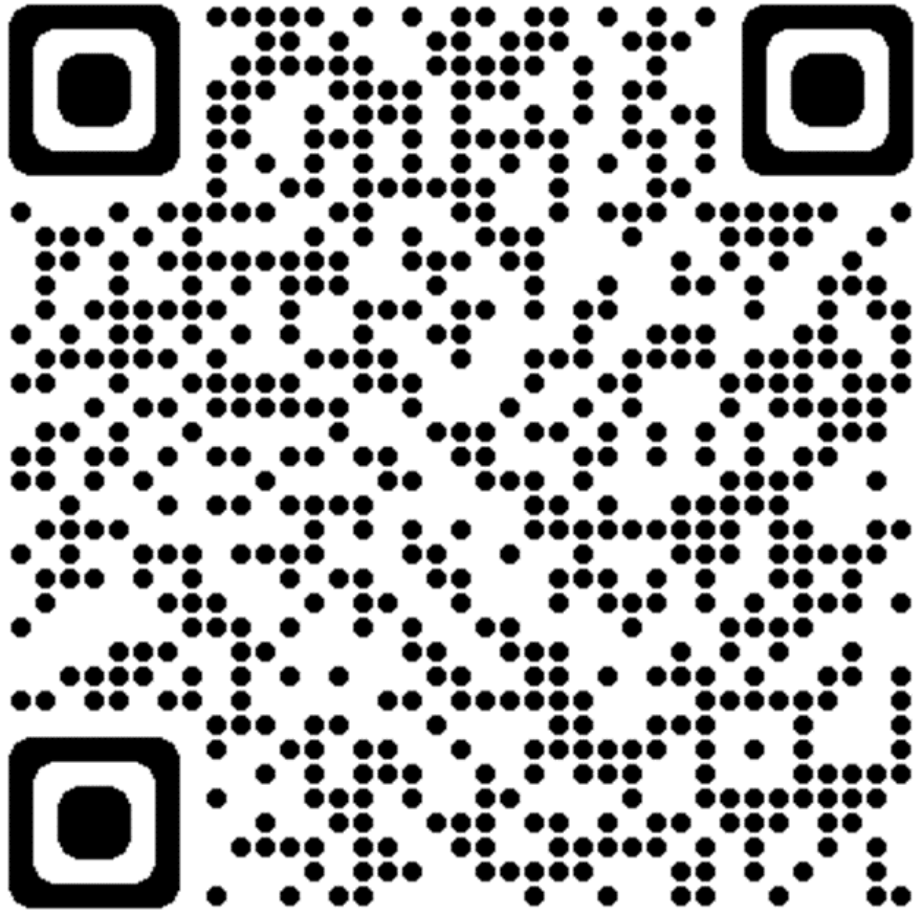


Question 1

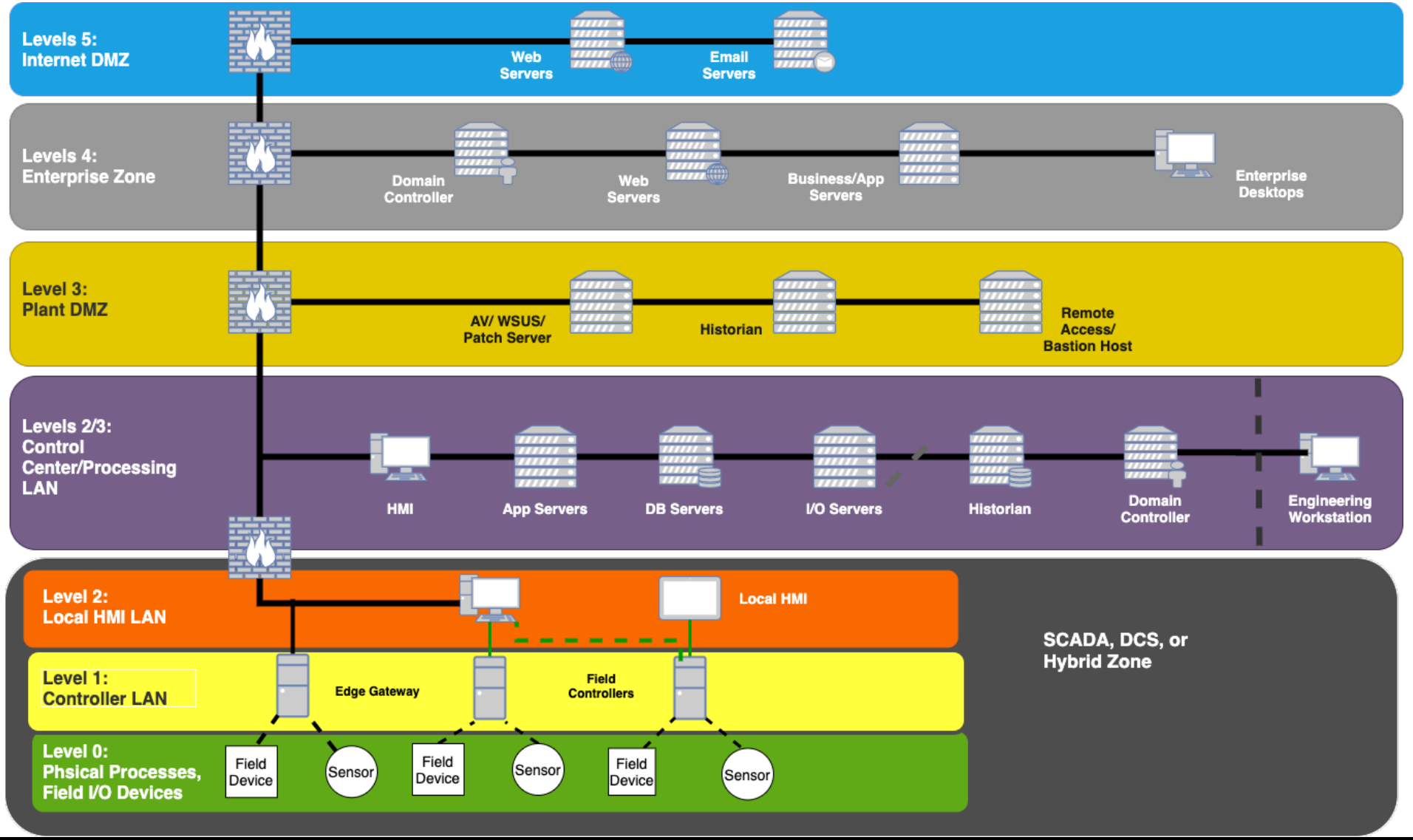
Are you backing up all your OT data on a regular basis, including storing one recent backup offsite?

Question 2

Has your organization ever been hacked?



OT Security Management meets Purdue Model



AUVESY-MDT

FORTINET

NOZOMI NETWORKS

OPSWAT.

MOXA

Source: AWS OT Security Management

CBPacific

Challenges for Industrial Operations

Real concerns operations face with their cybersecurity.

- Required to comply with numerous regulations
- Increasing number and sophistication of attacks
- Increasing public awareness of cost of attack or sabotage
- Loss of safety, production, or reputation can ruin a company
- Most Industrial Control Systems lack minimal intrusion protection
- Cost of non-compliance can be staggering
- Large Companies are often targeted due to the value of the data.
- All large-scale breaches of publicly traded companies involve law enforcement at the federal level, the FBI, Department of Homeland Security and other agencies

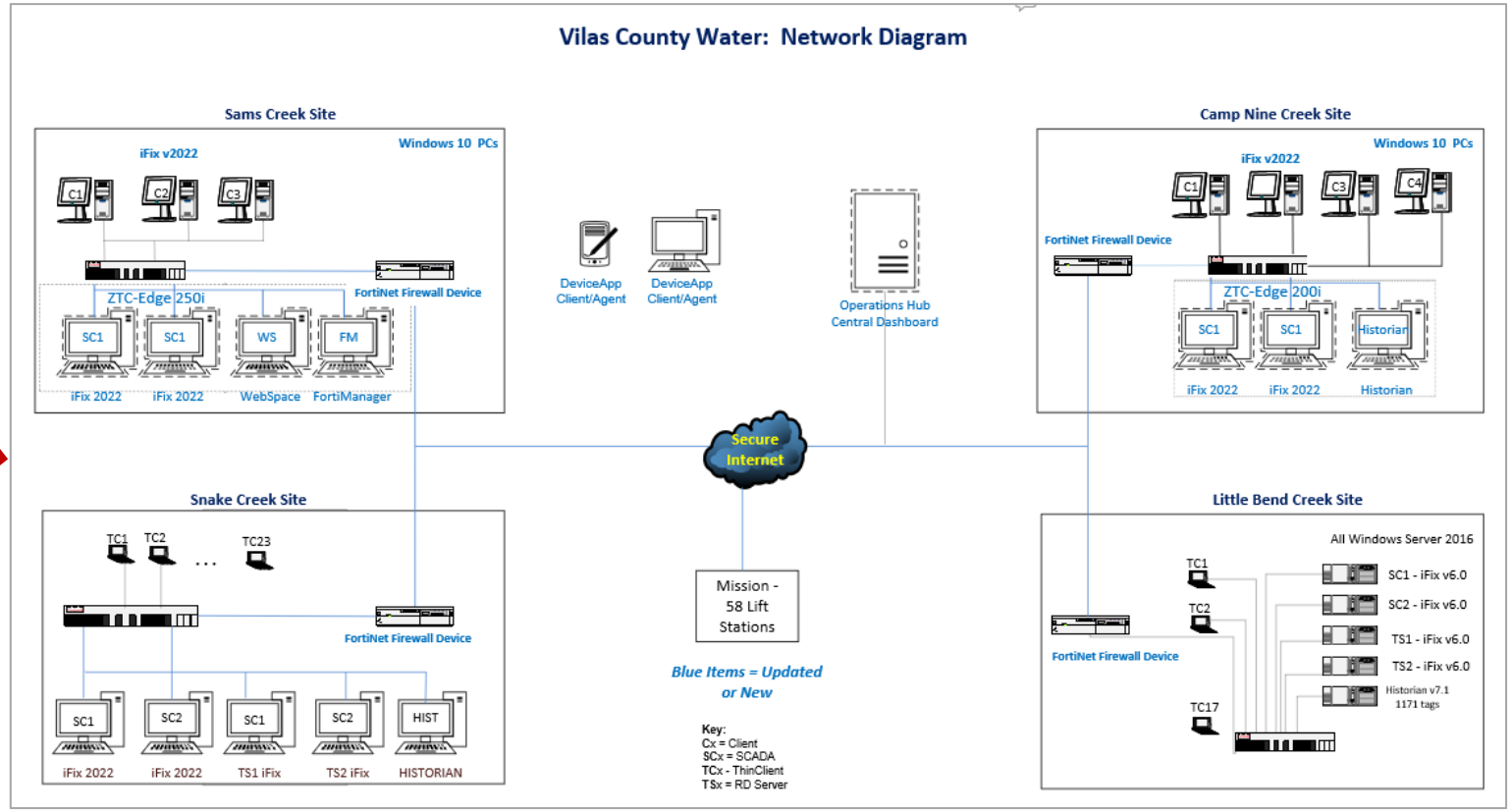
Questions?

Other items to think about:

- How do you handle on/off-boarding of vendors/employees with OT remote access?
- How do you manage version control, are you required by an outside body to maintain it?
- When was the last time you performed a risk assessment?

Benefits and Offers (50% Off)

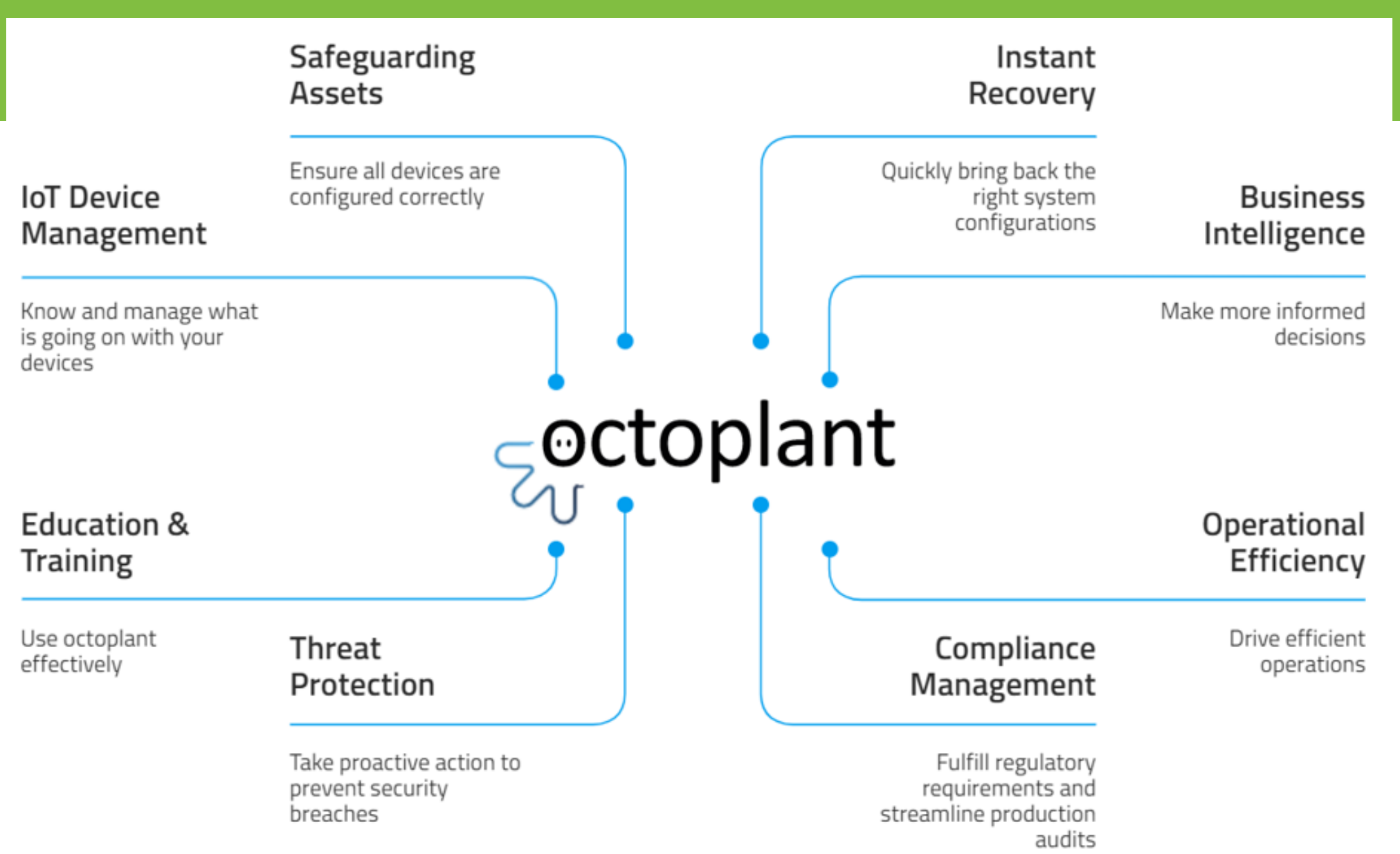
- **OT Cyber CTAP or**
- **GE SCADA & Historian Migration Roadmap**
  - › We & partners come onsite and build your roadmap:
  - › **Deliverable** will be a Logical Network Diagram
- **GE Training Offer**
  - › Unlimited Online Training Modules



Appendix

https://csrc.nist.gov/News/2022/guide-to-operational-technology-ot-security

https://www.cisa.gov/resources-tools/resources/ics-recommended-practices

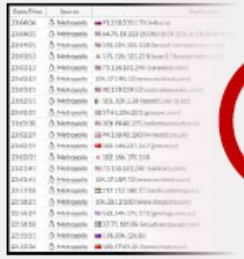

Safeguarding Assets
Ensure all devices are configured correctly
Instant Recovery
Quickly bring back the right system configurations
IoT Device Management
Know and manage what is going on with your devices
Business Intelligence
Make more informed decisions
octoplant
Education & Training
Use octoplant effectively
Operational Efficiency
Drive efficient operations
Threat Protection
Take proactive action to prevent security breaches
Compliance Management
Fulfill regulatory requirements and streamline production audits

Conducting an OT Assessment

1

INSTALL FORTIGATE FIREWALL

Deploy in Sniffer Mode or Inline to minimize disruption to existing network.



2

MONITOR TRAFFIC LOGS

Collect log traffic locally or to remote server for approximately 3-7 days.

3

REVIEW SECURITY REPORT

Investigate findings and review risks with your organization.

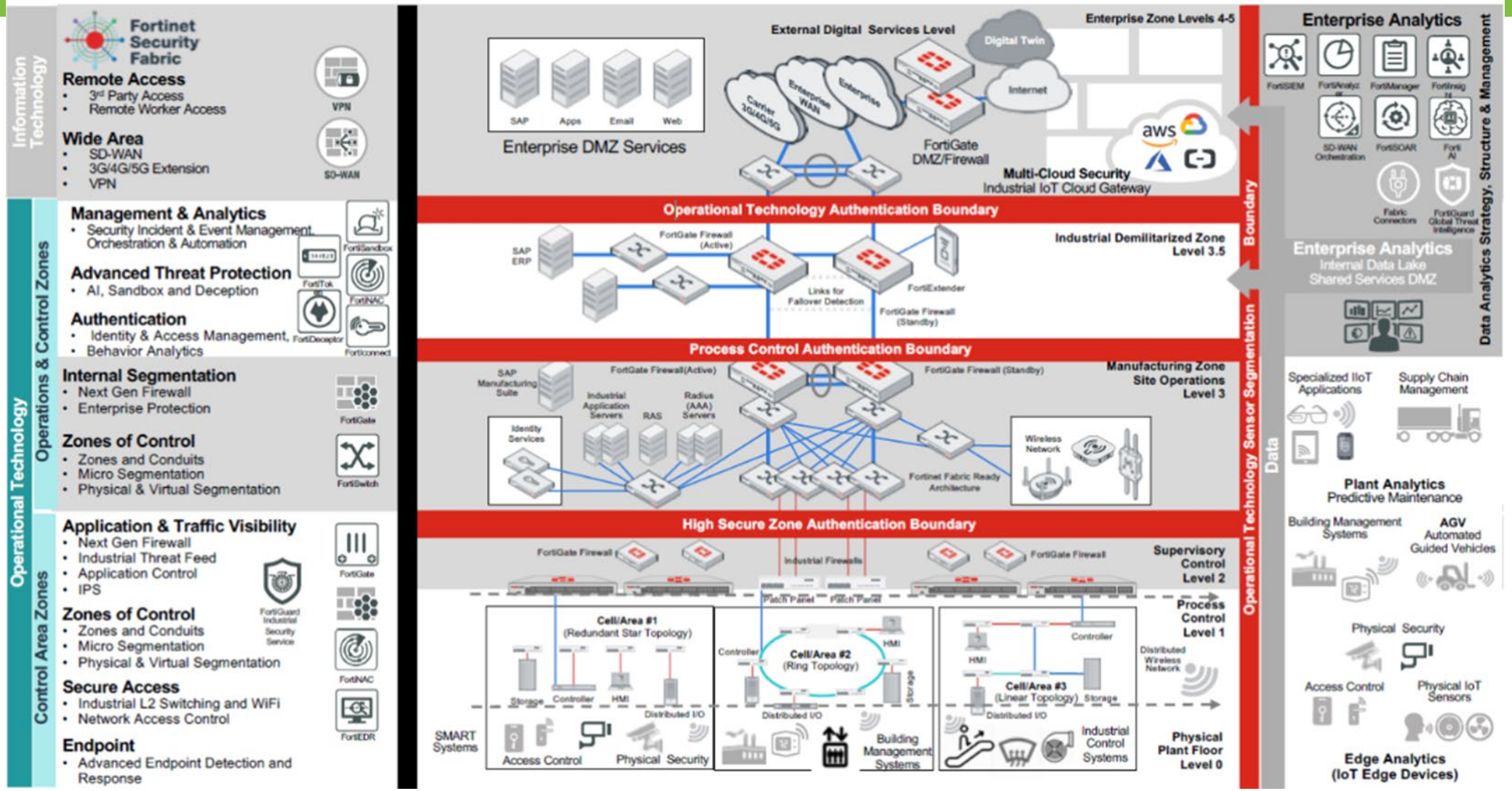
BENEFITS

- Evaluate FortiGate in your network
- Experience the value of FortiGuard
- Receive an assessment report!

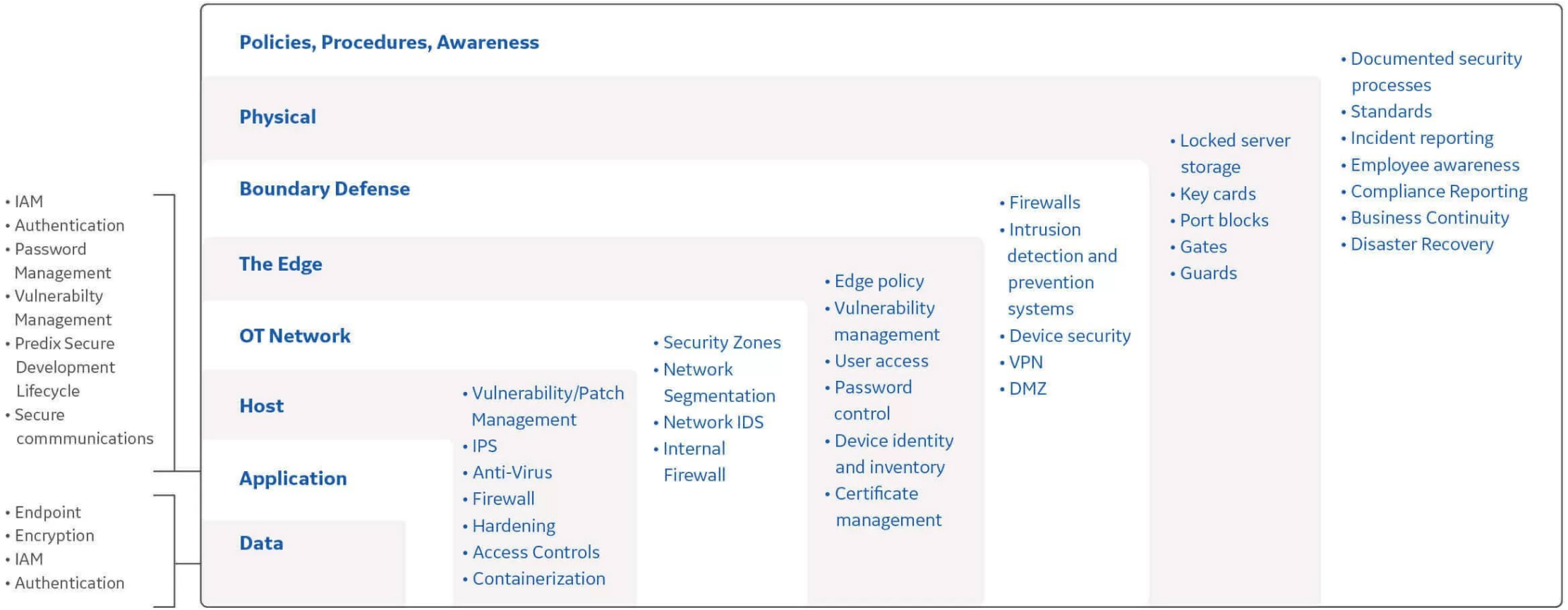
CB Pacific

ENHANCED Purdue INDUSTRIAL Architecture

Standards-based Framework with Fortinet Security Fabric



Defense in depth



CBPacific

Cybersecurity

- **Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA)**
- **National Institute of Standards and Technology (NIST)**
- **American Water Works Association (AWWA)**
- **International Organization for Standardization (ISO), 62443**
- **International Society of Automation/International Electrotechnical Commission (ISA/IEC)**
- **EPA has provided an optional Checklist that PWSs (or states) may use to conduct an assessment of recommended cybersecurity practices and controls.**