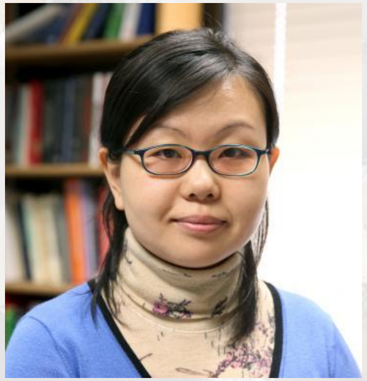
THE PROJECT IS SPONSORED BY DEPARTMENT OF DEFENSE NATIONAL CENTER OF ACADEMIC EXCELLENCE IN CYBERSECURITY (NCAE-C) CURRICULUM AND RESEARCH 2020 PROGRAM

BUILDING A SMART SECURE MANUFACTURING TESTBED USING ZERO TRUST MODEL, MACHINE LEARNING AND 5G

Reaching Towards the Future of Manufacturing

Faculty Team



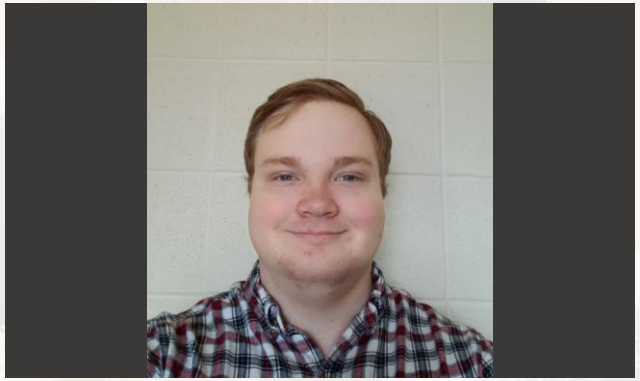
Holly Yuan: CNIT/CyROC Director, UW-Stout

Brandon Cross: Lecturer – CNIT, UW-Stout

Wei Shi: Computer & Electrical Engineering Program Director, UW-Stout

Aaron Bialzik: Manufacturing Outreach Center Director

Students Research Team



Wesley Larrabee (CEE) - Team Lead/Hardware Engineer

Scott Bresnahan (CNIT) - AWS Engineer/5G Engineer

Michael Laffin (CEE) - Hardware Engineer

Neil Borden (CNIT) - AWS/Network Security Engineer

Lee Kottke (CNIT) - AWS/Network Security Engineer

Agenda

- Problem Statement
- Equipment and Software
- Implementations
- Case Studies and Demos
- Pen Testing & Auditing
- Q&A

WHAT PROBLEMS AFFECT A MANUFACTURE?

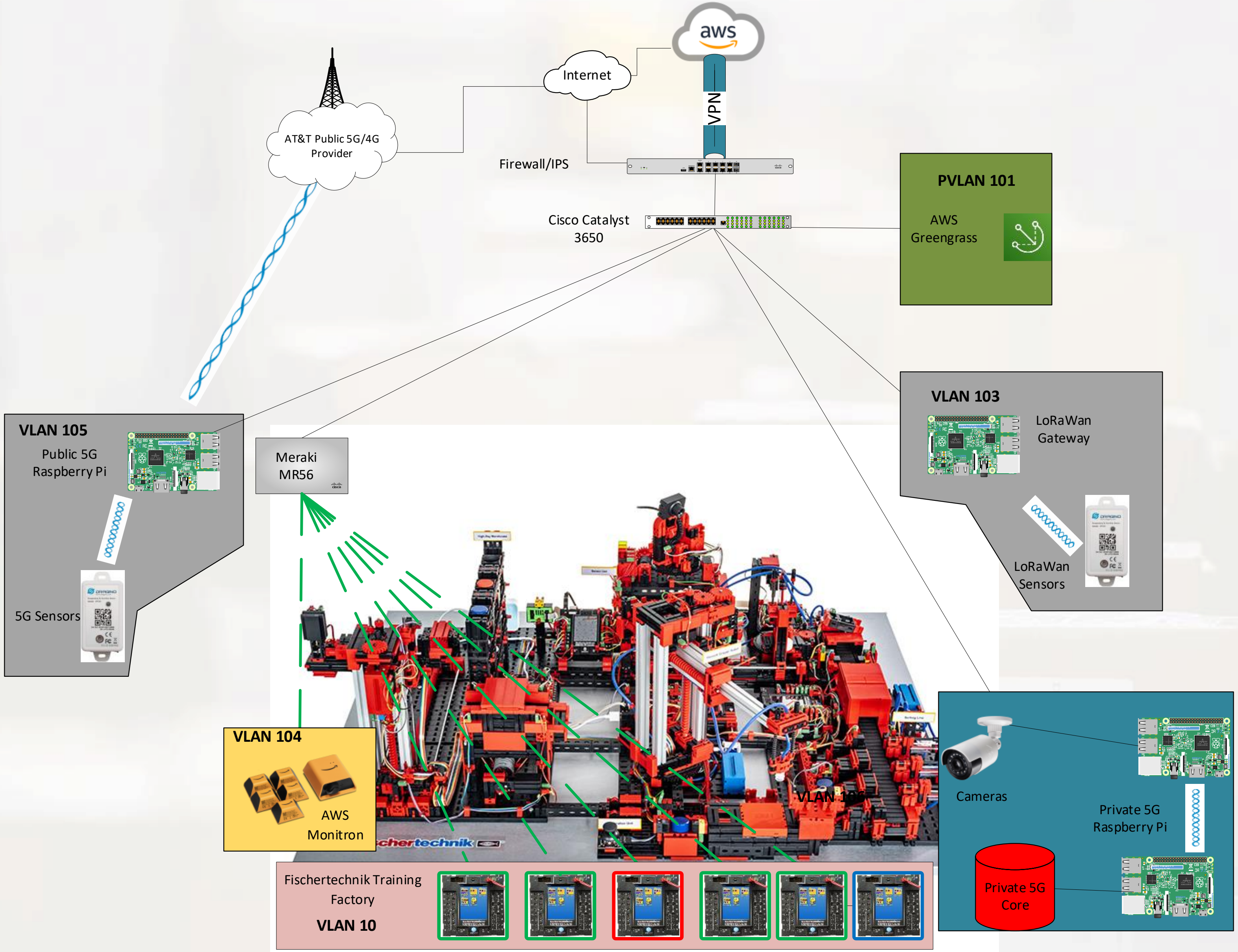
5G, IIOT AND AI IS IMPACTING THE FUTURE AND GROWTH OF MANUFACTURING.

CYBERSECURITY RELATED ATTACKS POSE A THREAT TO THE FUTURE OF MANUFACTURING.

HOW DO WE SOLVE THESE ISSUES?

- 5G PROTOCOL
- ZERO TRUST
- EDGE COMPUTING
- ARTIFICIAL INTELLIGENCE

OUR NETWORK


aws
VPN
Internet
AT&T Public 5G/4G Provider
Firewall/IPS
Cisco Catalyst 3650
PVLAN 101
AWS Greengrass
VLAN 105
Public 5G Raspberry Pi
5G Sensors
Meraki MR56
VLAN 103
LoRaWan Gateway
LoRaWan Sensors
VLAN 104
AWS Monitron
VLAN 106
Cameras
Private 5G Raspberry Pi
Private 5G Core
fischertechnik
Fischertechnik Training Factory
VLAN 10

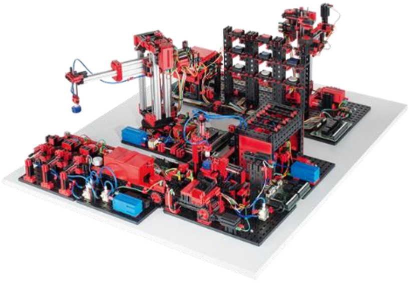
EQUIPMENT

AWS Monitron

Meraki MX84

Raspberry Pi 5G Hat

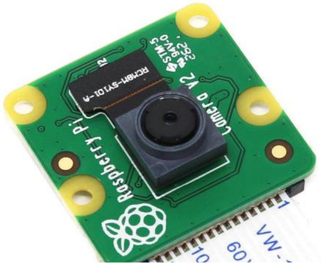
LoRaWAN Raspberry Pi



Fishertechnic Factory Floor

Private 5G Raspberry Pi

Edge Computing
Raspberry Pi



Raspberry Pi Cameras

SOFTWARE

Amazon Web Services

DUO Multifactor

Open5GS

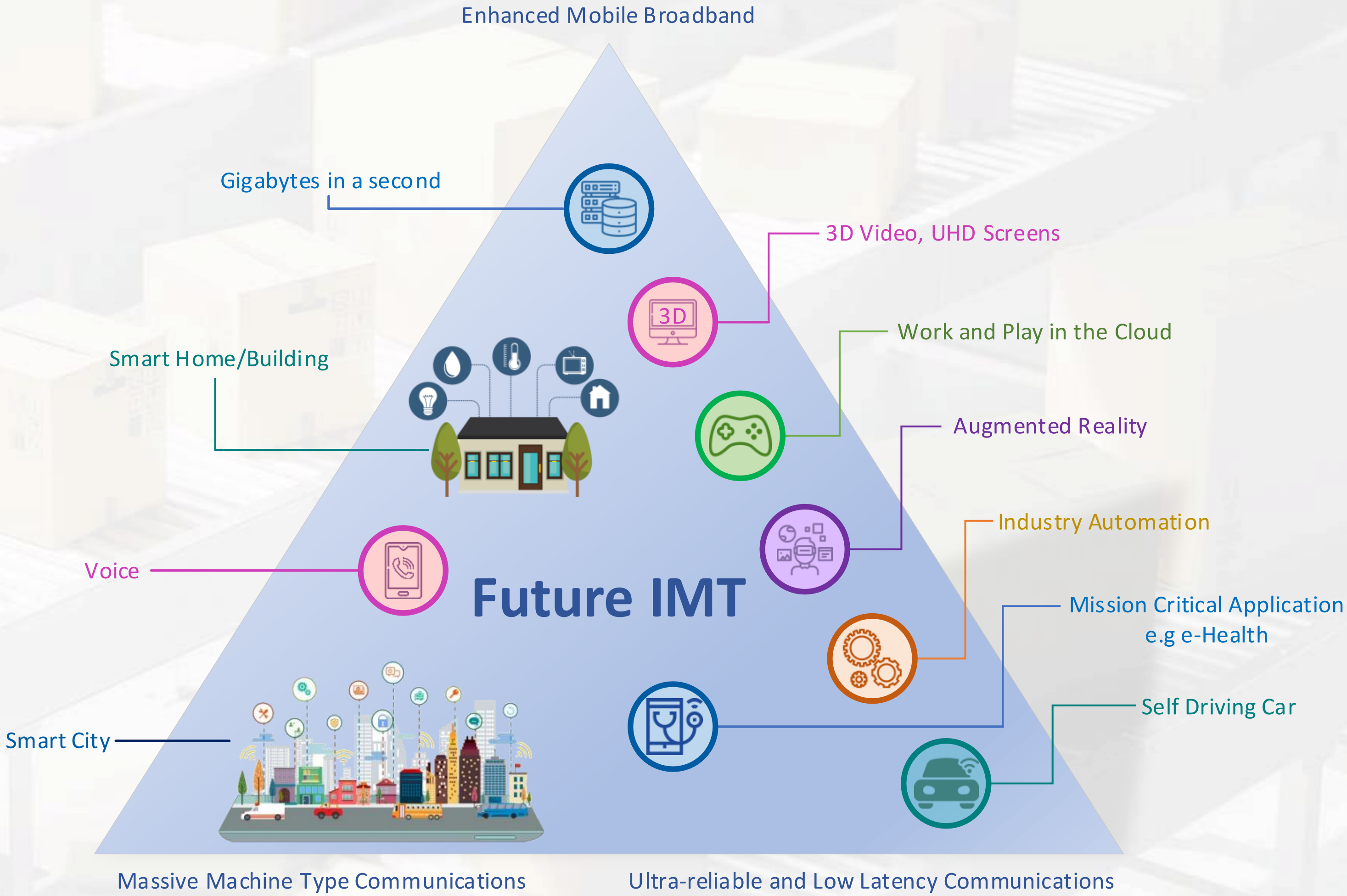
Edge Impulse

UERANSIM

Cisco Meraki Cloud

MAIN GOALS OF 5G

- **Enhanced Mobile Broadband (eMBB)**
- **Ultra-Reliable Low-Latency Communications (uRRLC)**
- **Massive Machine-Type Communications (mMTC)**



Enhanced Mobile Broadband
Gigabytes in a second
3D Video, UHD Screens
3D
Work and Play in the Cloud
Smart Home/Building
Augmented Reality
Industry Automation
Voice
Future IMT
Mission Critical Application e.g e-Health
Self Driving Car
Smart City
Massive Machine Type Communications
Ultra-reliable and Low Latency Communications

BENEFITS OF PRIVATE 5G IN MANUFACTURING

500% FASTER THAN 4G LTE

1MS LATENCY

MORE DEVICES PER NETWORK

INCREASED AVAILABILITY

INCREASED RELIABILITY

INCREASED SECURITY

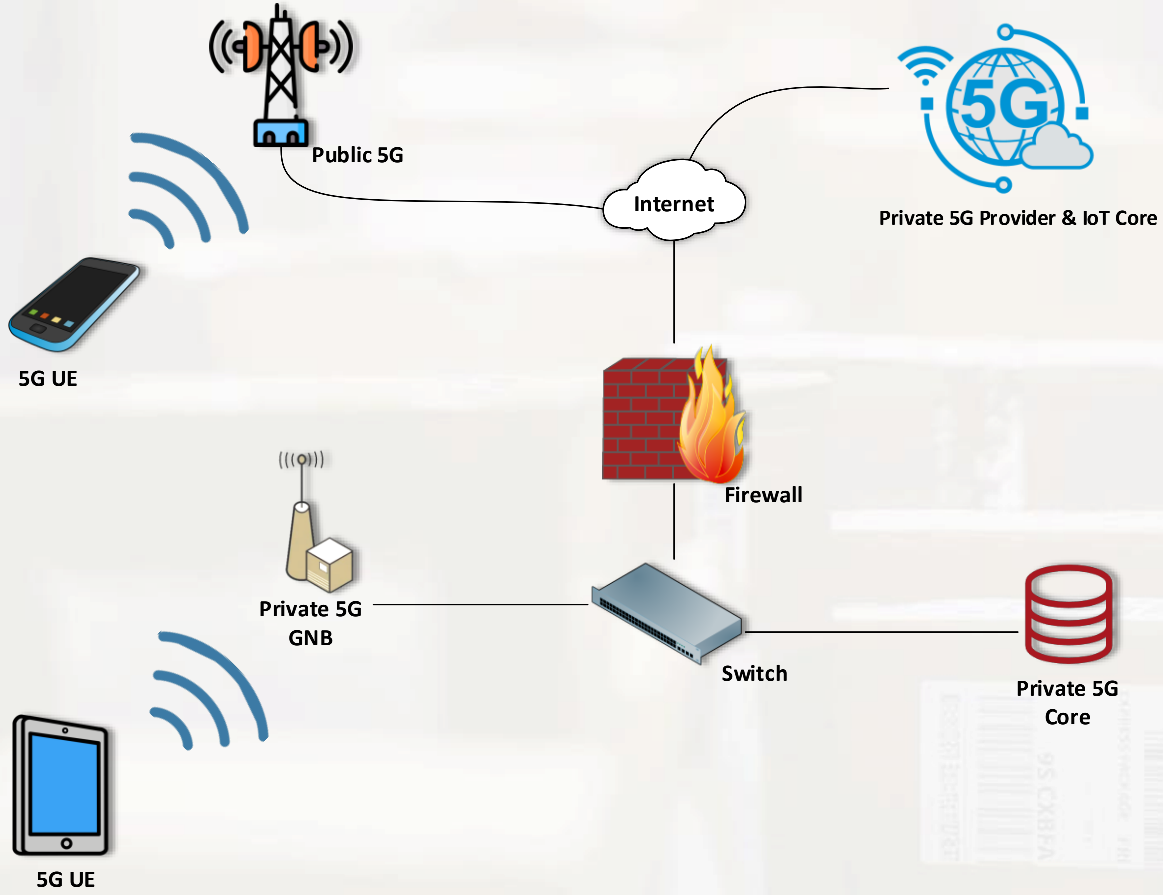
INCREASED MOBILITY

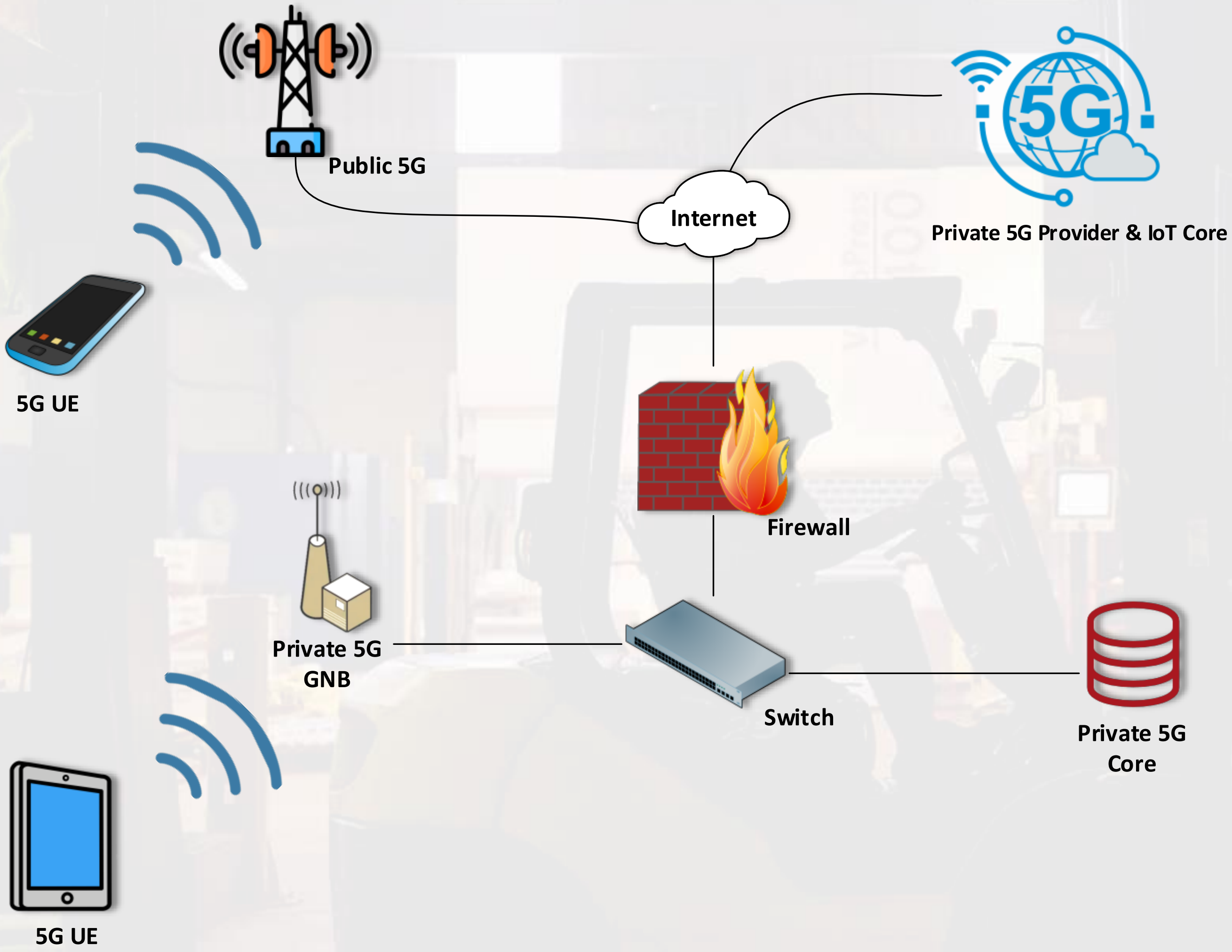
NETWORK SPLICING

INCREASED AUTOMATION AI & IOT FUNCTIONALITY

INCREASED FLEXIBILITY

DESIGN – PUBLIC 5G





PRIVATE 5G

Next generation of global wireless standard.

Multi-Gbps data speeds

Ultra-Low Latency

Reliability

Increased Network Capacity/Availability

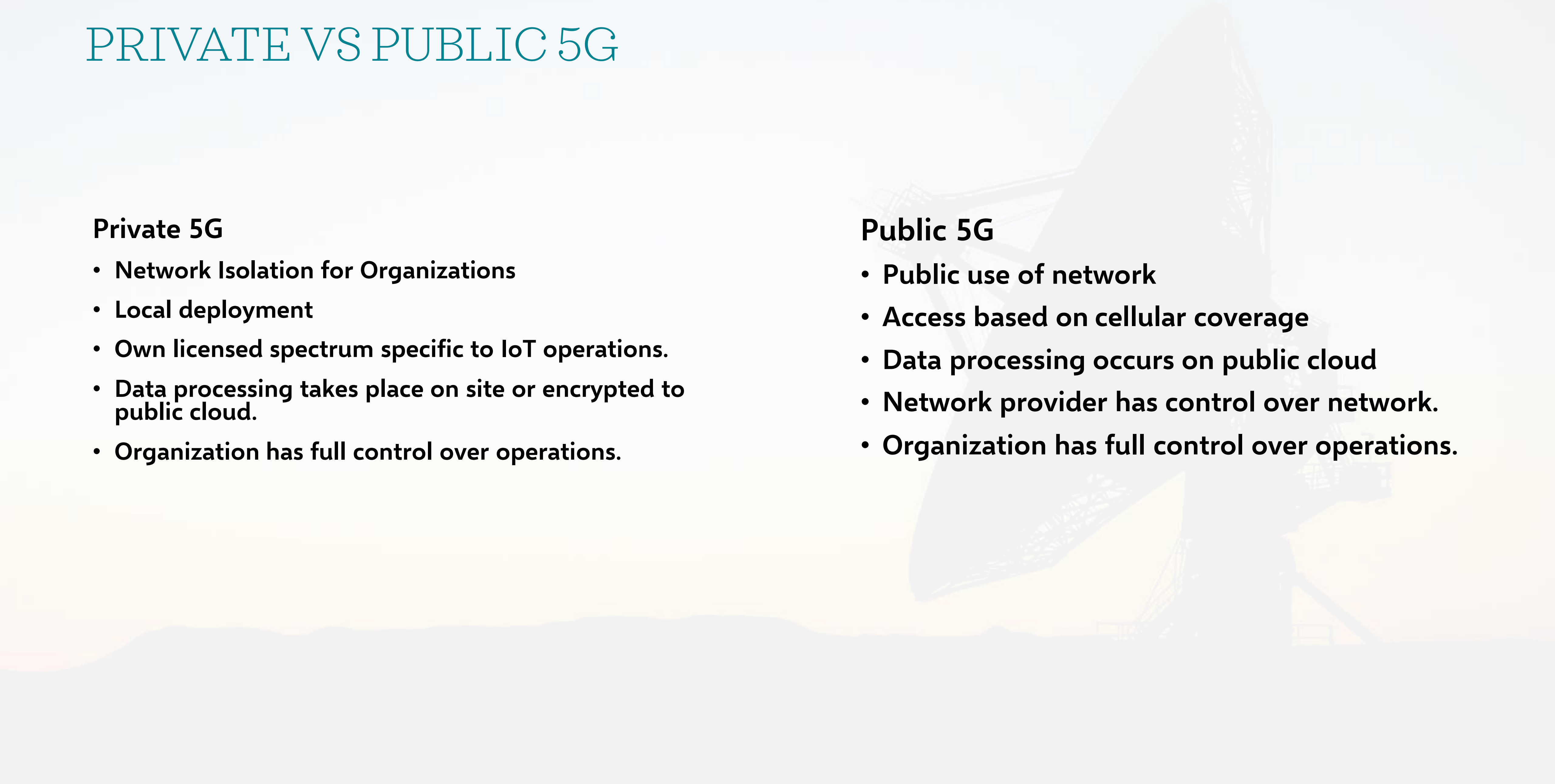
PRIVATE VS PUBLIC 5G

Private 5G

- Network Isolation for Organizations
- Local deployment
- Own licensed spectrum specific to IoT operations.
- Data processing takes place on site or encrypted to public cloud.
- Organization has full control over operations.

Public 5G

- Public use of network
- Access based on cellular coverage
- Data processing occurs on public cloud
- Network provider has control over network.
- Organization has full control over operations.



5G VS WI-FI 6

TYPES OF PRIVATE 5G IMPLEMENTATION

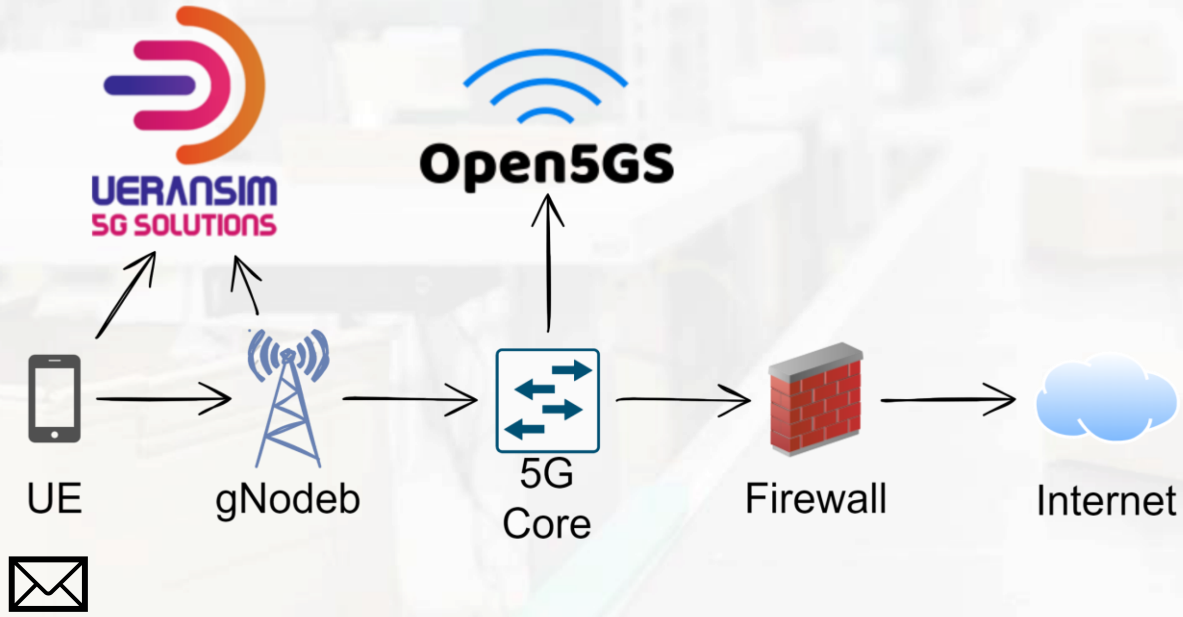
- On-Premise
- Cloud
- Managed Services

Open5GS

aws

cisco

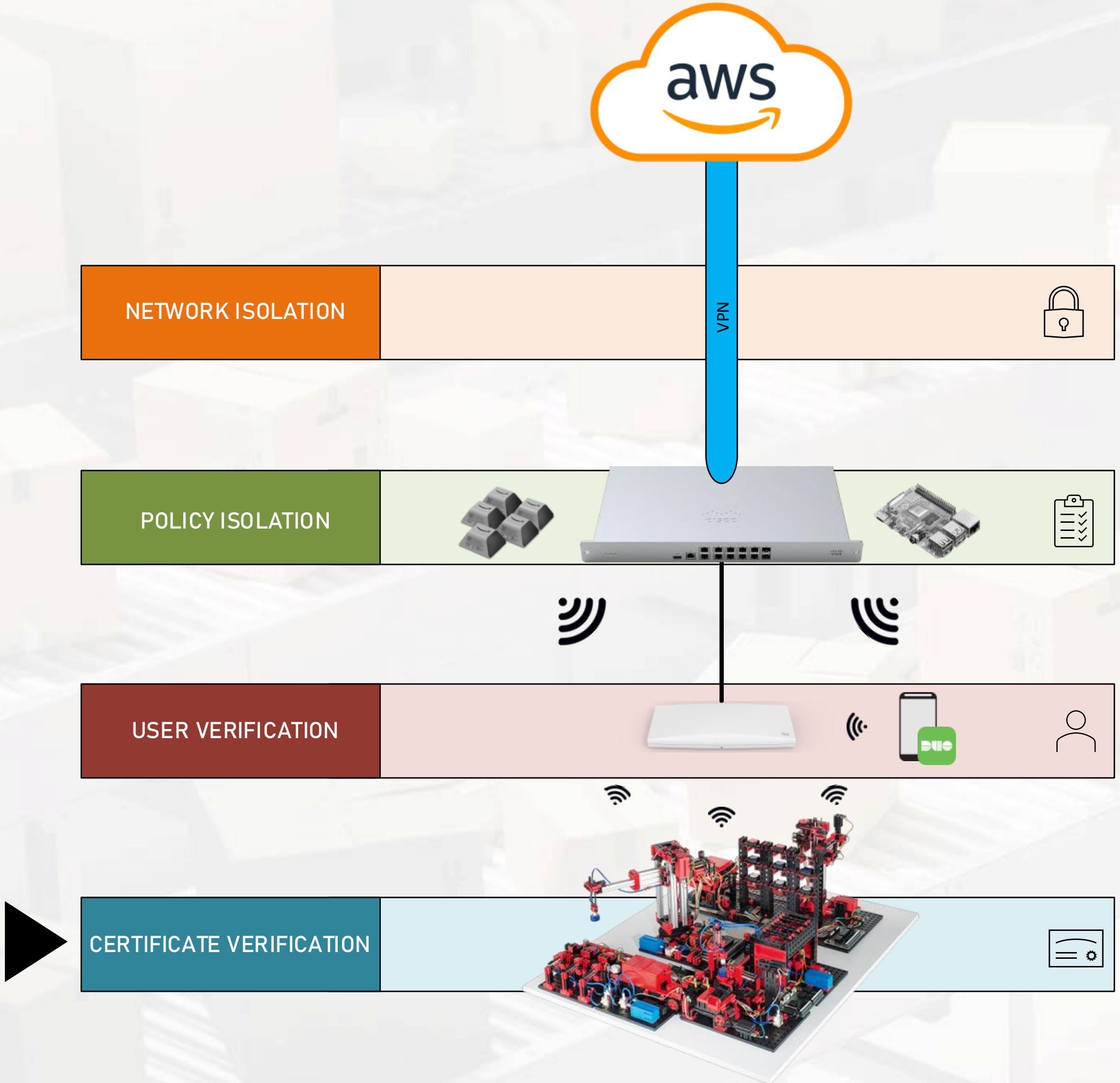
IMPLEMENTATION OF PRIVATE 5G (EMULATED)



- **5G Core Emulation done through Open5GS**
  - Brains of the operation.

- **5G UE and RAN (gNodeB) emulation done through UERANSIM**
  - This is emulating a cell phone and a base station.

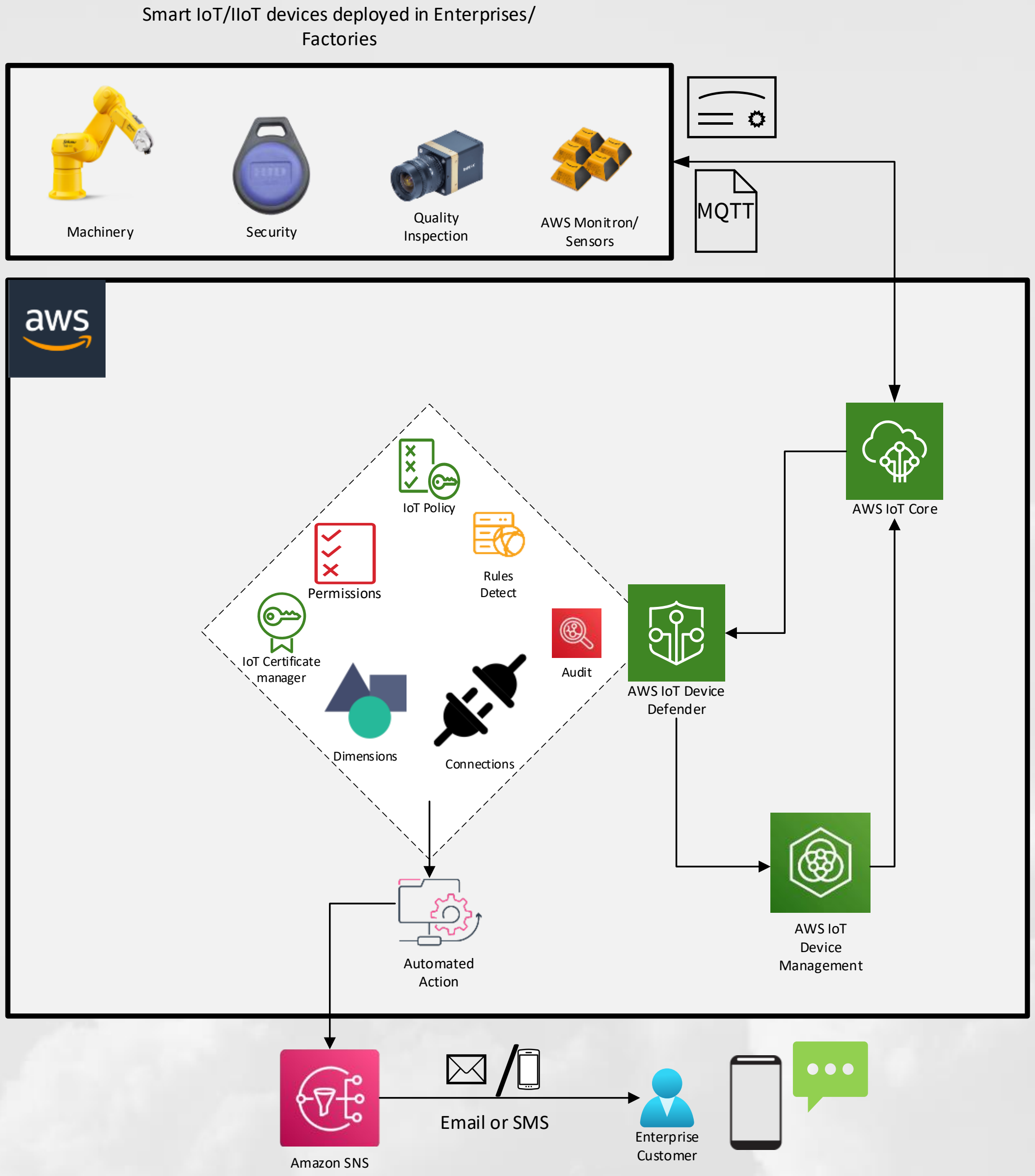
DESIGN – SECURITY: ZERO TRUST



- ✓ Zero trust → Never trust, Always Verify!
- Device Access Isolated
- Least Privilege

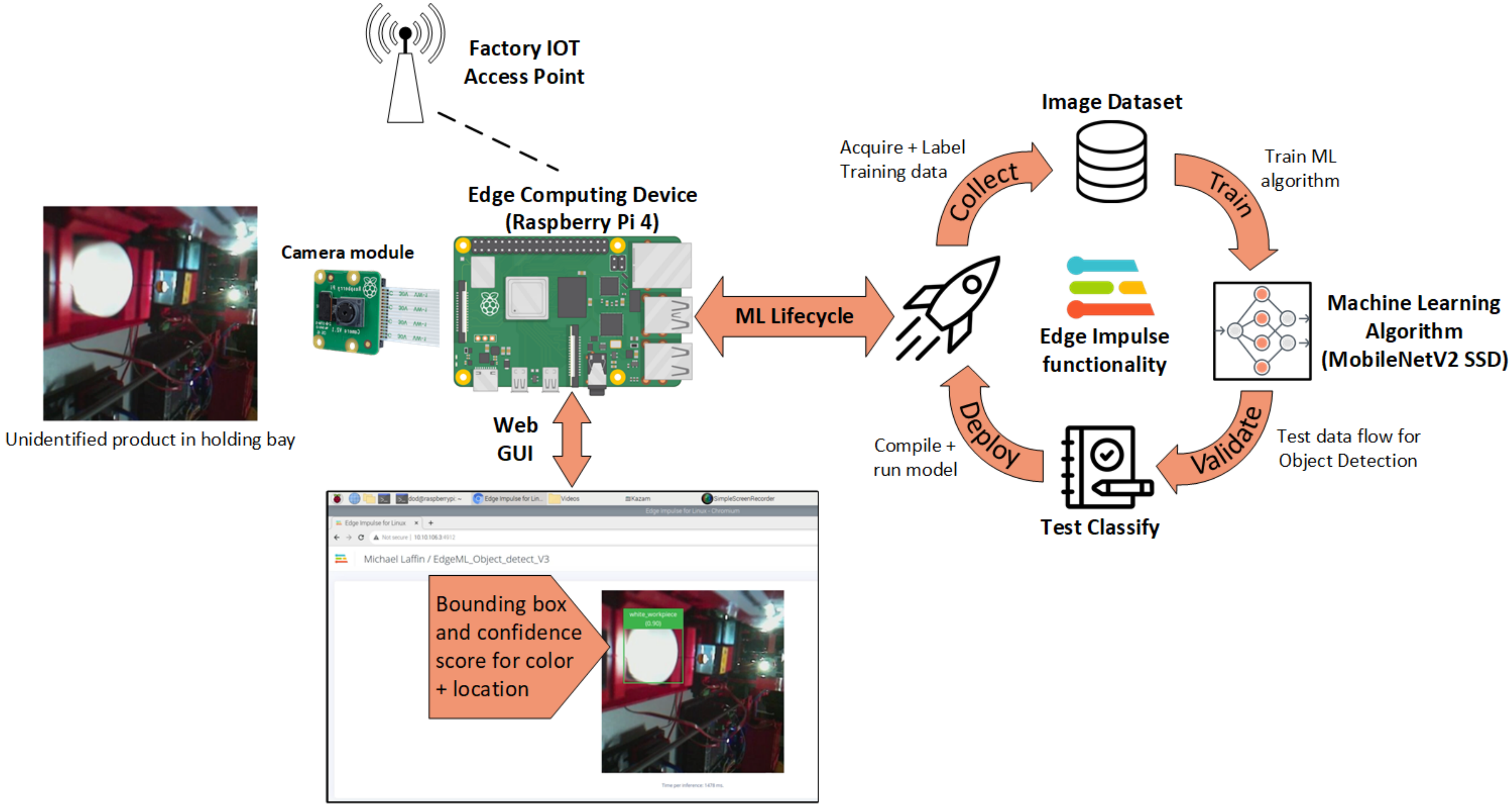
DESIGN – SECURITY:

CLOUD SECURITY ZERO TRUST



- Certificates to Identify
- Follow “Least Privilege”
- Don’t Trust User Based on Network Location

DESIGN – EDGE COMPUTING + MACHINE LEARNING



Factory IOT Access Point

Edge Computing Device (Raspberry Pi 4)

Camera module

Unidentified product in holding bay

ML Lifecycle

Web GUI

Bounding box and confidence score for color + location

Identified product

Image Dataset

Acquire + Label Training data

Collect

Train

Train ML algorithm

Edge Impulse functionality

Machine Learning Algorithm (MobileNetV2 SSD)

Validate

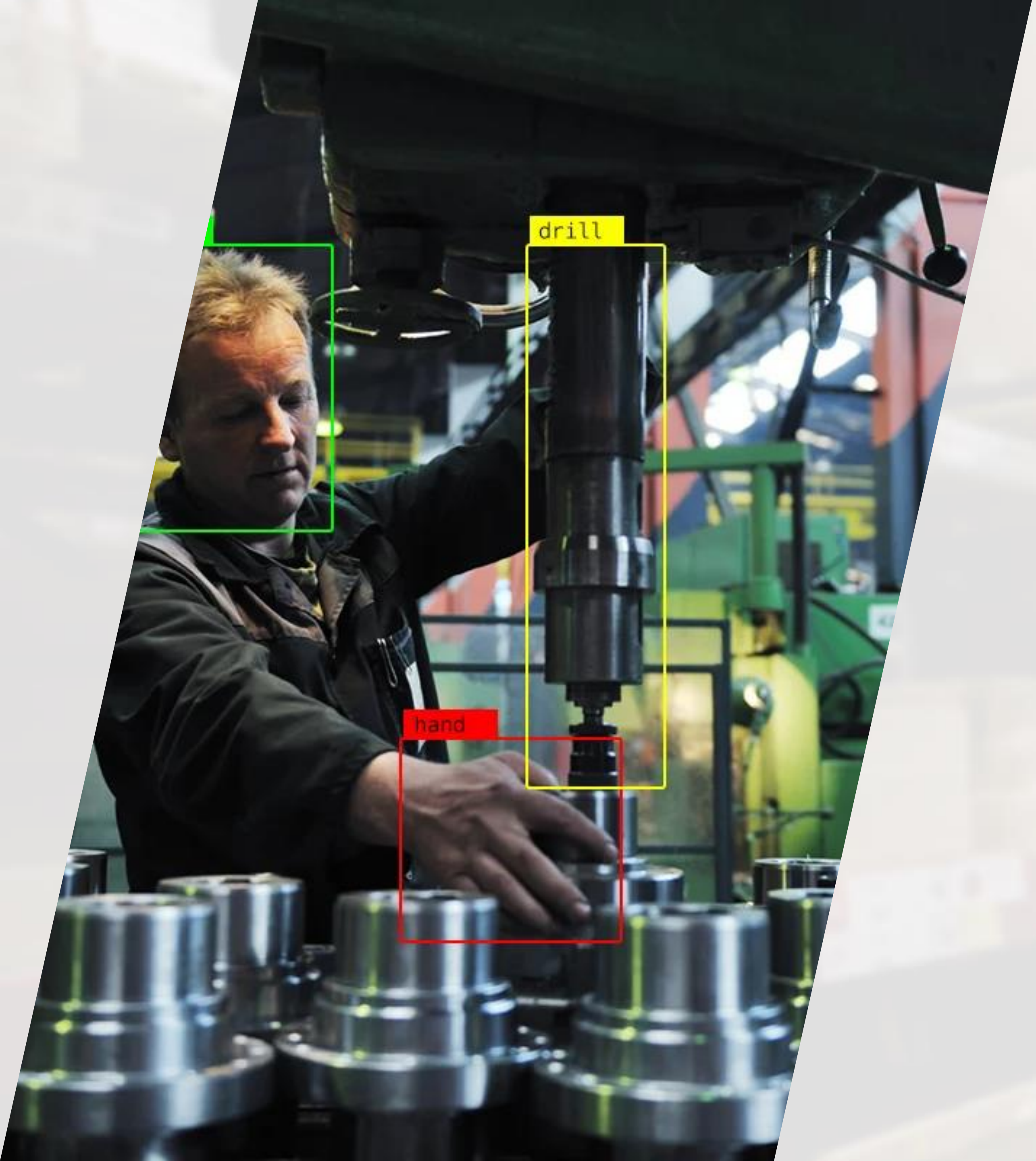
Test data flow for Object Detection

Test Classify

Deploy

Compile + run model

LIVE DEMO



USE CASE 1

Edge Machine Learning for Quality Control

- Local (edge) processing reduces Cloud network traffic and security risks
- Identify product color and location within dynamic visual environment

USE CASE 2

Predictive Maintenance

- Predict time to fail
- Plan maintenance downtime
- Save time and money with little to no unscheduled downtime.

USE CASE 3

Inventory Management

- IIoT can be utilized to keep track of exactly what, where, and when a product is within the factory, including when it's coming into or out of the factory.
- Using wireless technologies, track packages through the shipping process
- AI/ML can be utilized to use current and previous inventory records to predict and notify you when you’ll run out of a certain product or input.

USE CASE 4

Improve Productivity

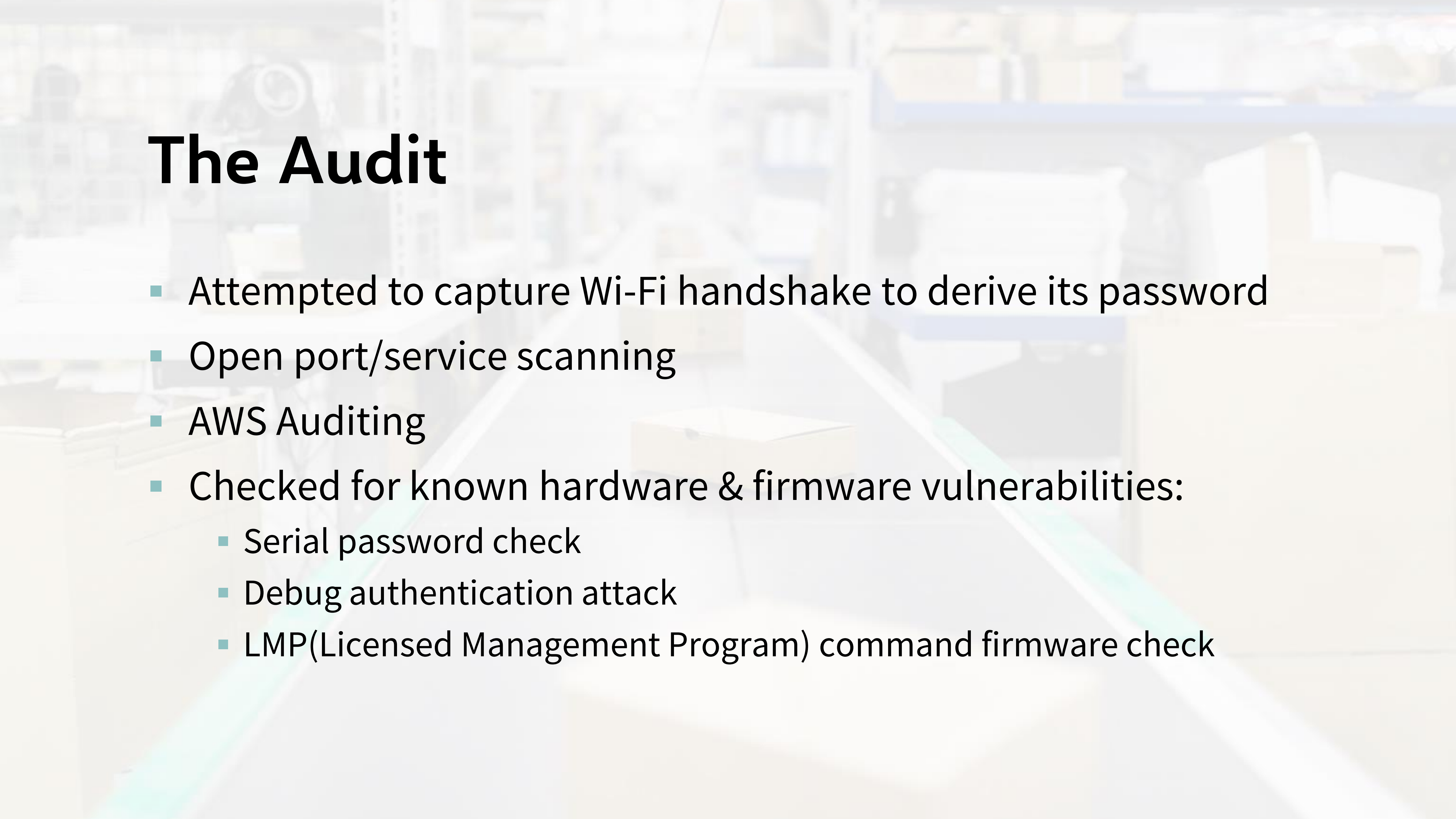
- By using Next-Generation 5G, Data transfer between IIOT Devices is faster, and more reliable than prior mobile technologies.

IOT SECURITY PENTEST/AUDIT

White Hat Hacker Team

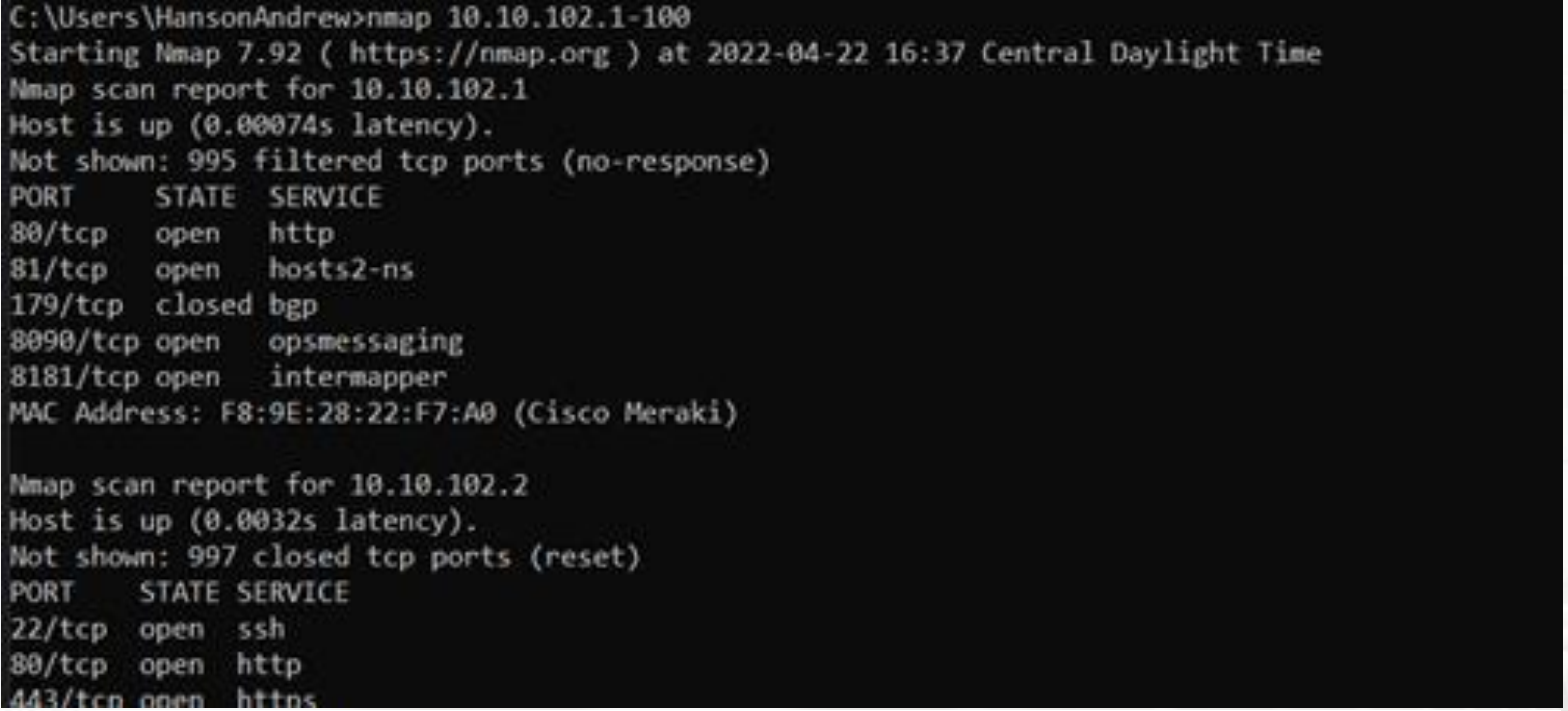
Goals

- Our goal is to pen test and audit the SMART Manufacturing team’s network for vulnerabilities and risks to ensure adequate security measures are in place.
- Provide the SMART manufacturing team with a report of our findings to further improve their network.



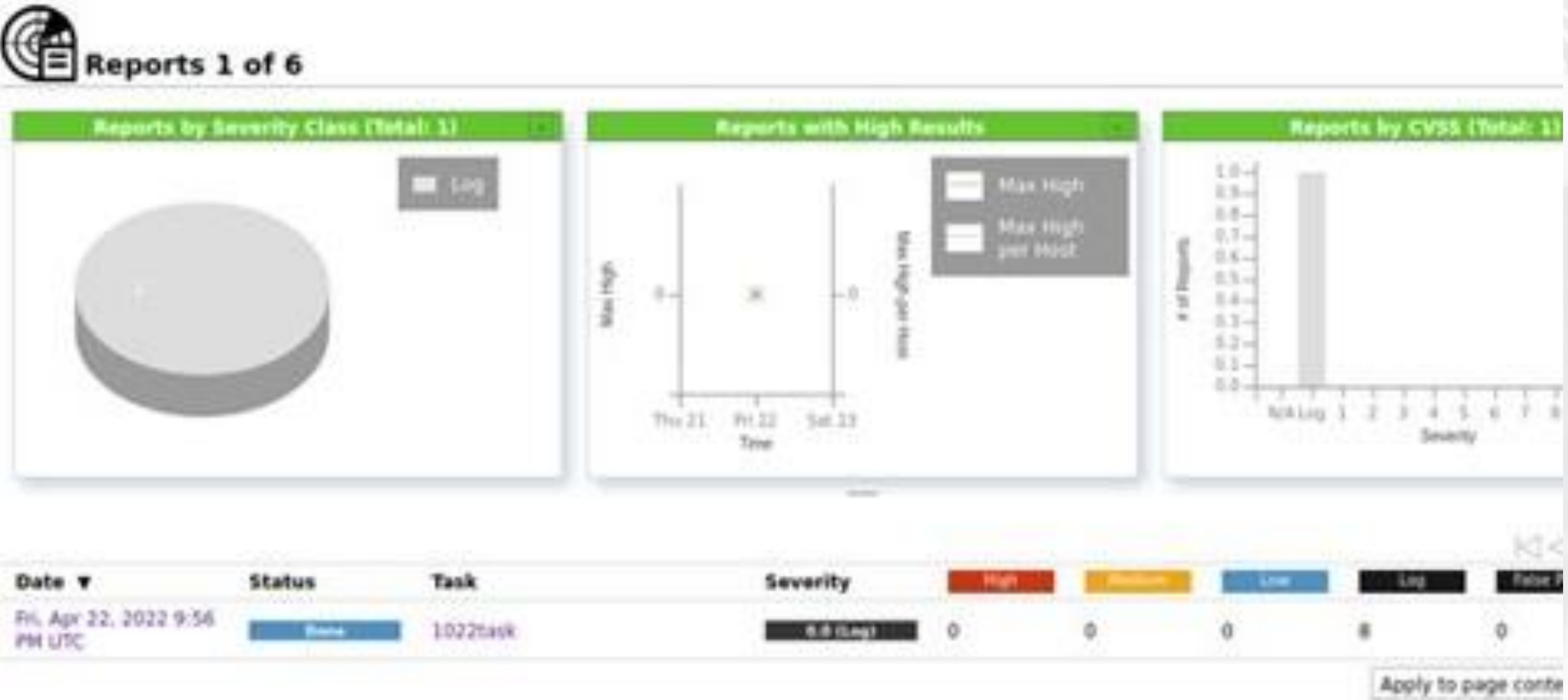
The Audit

- Attempted to capture Wi-Fi handshake to derive its password
- Open port/service scanning
- AWS Auditing
- Checked for known hardware & firmware vulnerabilities:
  - Serial password check
  - Debug authentication attack
  - LMP(Licensed Management Program) command firmware check



```
C:\Users\HansonAndrew>nmap 10.10.102.1-100
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-22 16:37 Central Daylight Time
Nmap scan report for 10.10.102.1
Host is up (0.00074s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE  SERVICE
80/tcp   open   http
81/tcp   open   hosts2-ns
179/tcp  closed bgp
8090/tcp open   opsmessaging
8181/tcp open   intermapper
MAC Address: F8:9E:28:22:F7:A0 (Cisco Meraki)

Nmap scan report for 10.10.102.2
Host is up (0.0032s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
```



Reports 1 of 6

Date ▼	Status	Task	Severity	High	Medium	Low	Log	False P
Fri, Apr 22, 2022 9:56 PM UTC	Done	1022task	0.0 (Log)	0	0	0	8	0

OpenVas and NMAP Scans

- NMAP Scan
  - Nothing Found from External connection
  - Scan from internal connection found devices, but only in same VLAN.
    - Services were password protected
- OpenVAS Tests
  - Scans didn't detect vulnerabilities on devices
    - Both Cisco machines

WPA2 Cracking

Demonstration of Airmon-ng Suite running through a raspberry pi to capture a 4-way handshake.

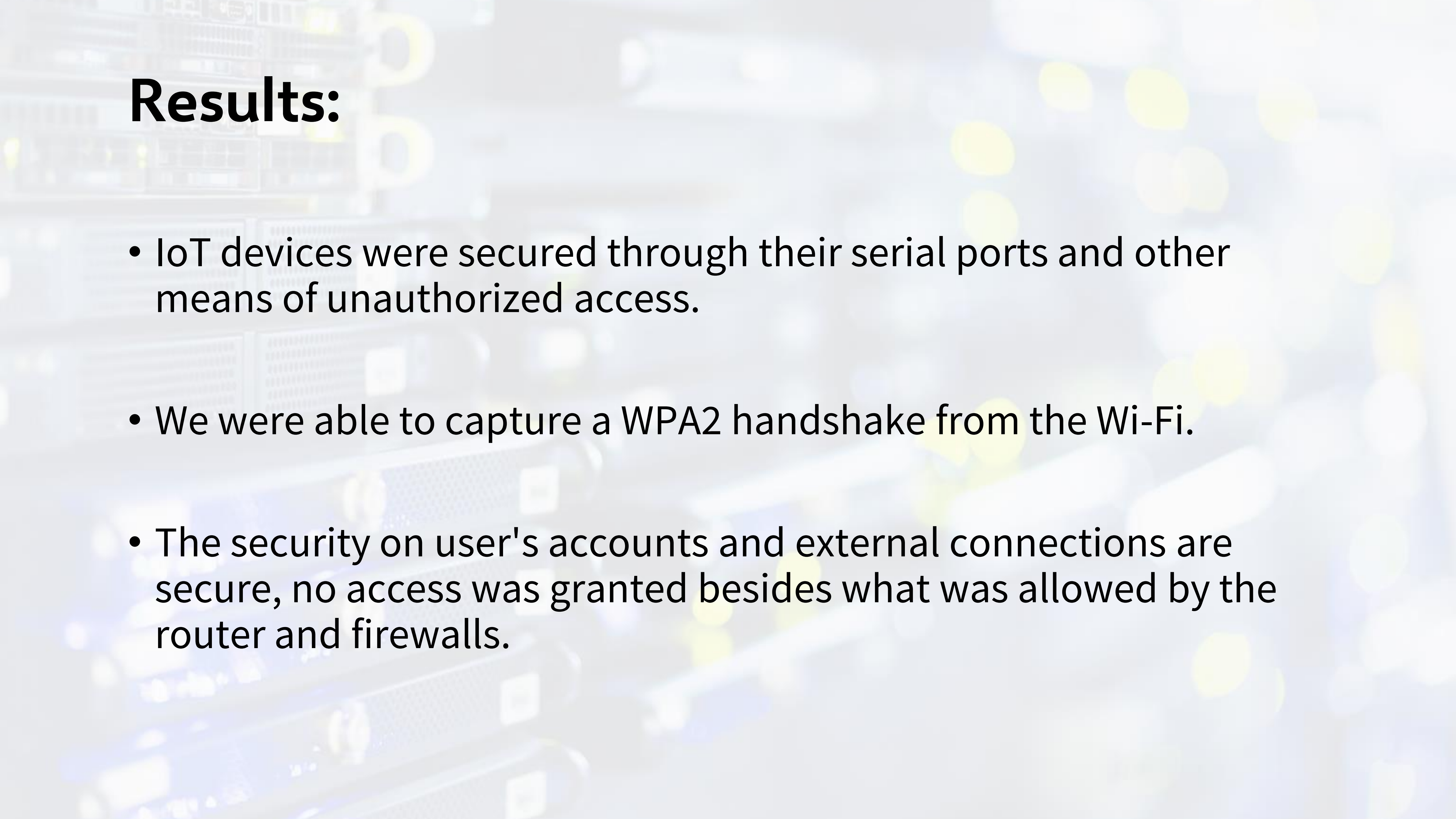
AWS Auditing

AWS Security Hub

- Look for Best Practice Security

AWS Inspector

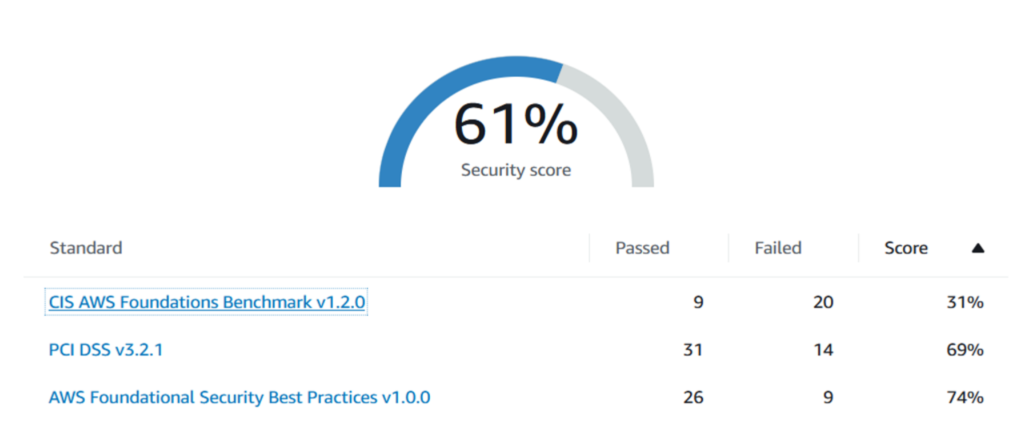
- Look for network reachability



Results:

- IoT devices were secured through their serial ports and other means of unauthorized access.
- We were able to capture a WPA2 handshake from the Wi-Fi.
- The security on user's accounts and external connections are secure, no access was granted besides what was allowed by the router and firewalls.

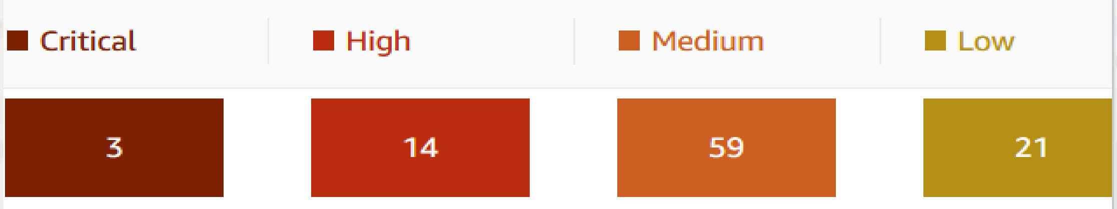
AWS Security hub



61%

Security score

Standard	Passed	Failed	Score ▲
CIS AWS Foundations Benchmark v1.2.0	9	20	31%
PCI DSS v3.2.1	31	14	69%
AWS Foundational Security Best Practices v1.0.0	26	9	74%

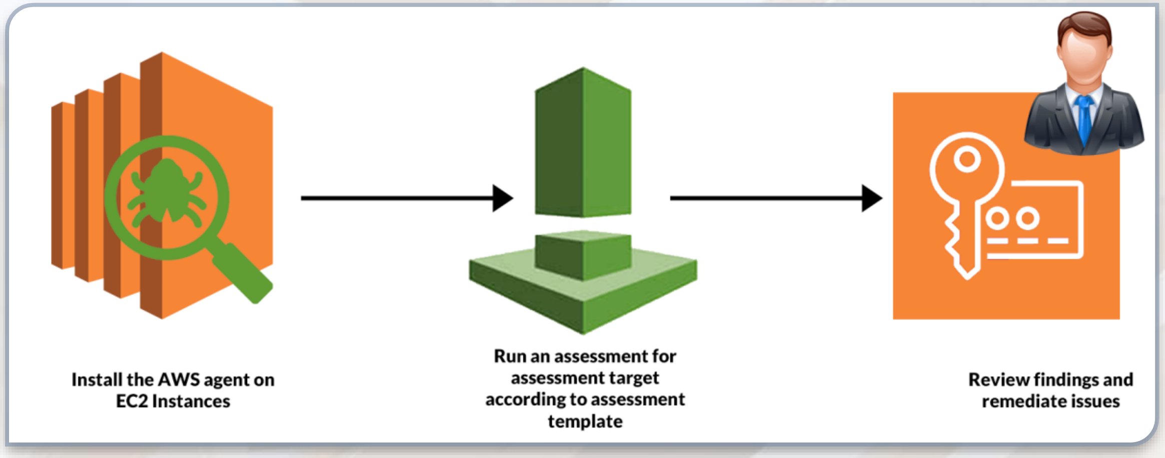


Critical	High	Medium	Low
3	14	59	21

- Of those failed compliance standard, only 3 were of critical severity:
  - Automatic Security services not being enabled.
  - Server-side encryption not being enabled.
  - Hardware MFA should be enabled for the root user

AWS Inspector

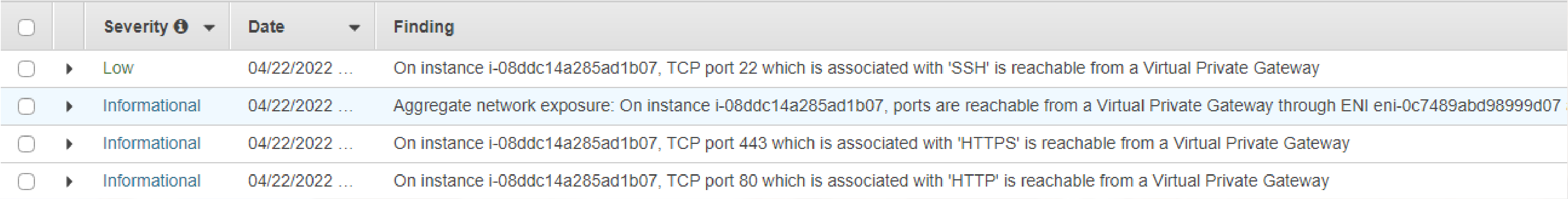
- For the assessment run we conducted only one low severity risk was detected.



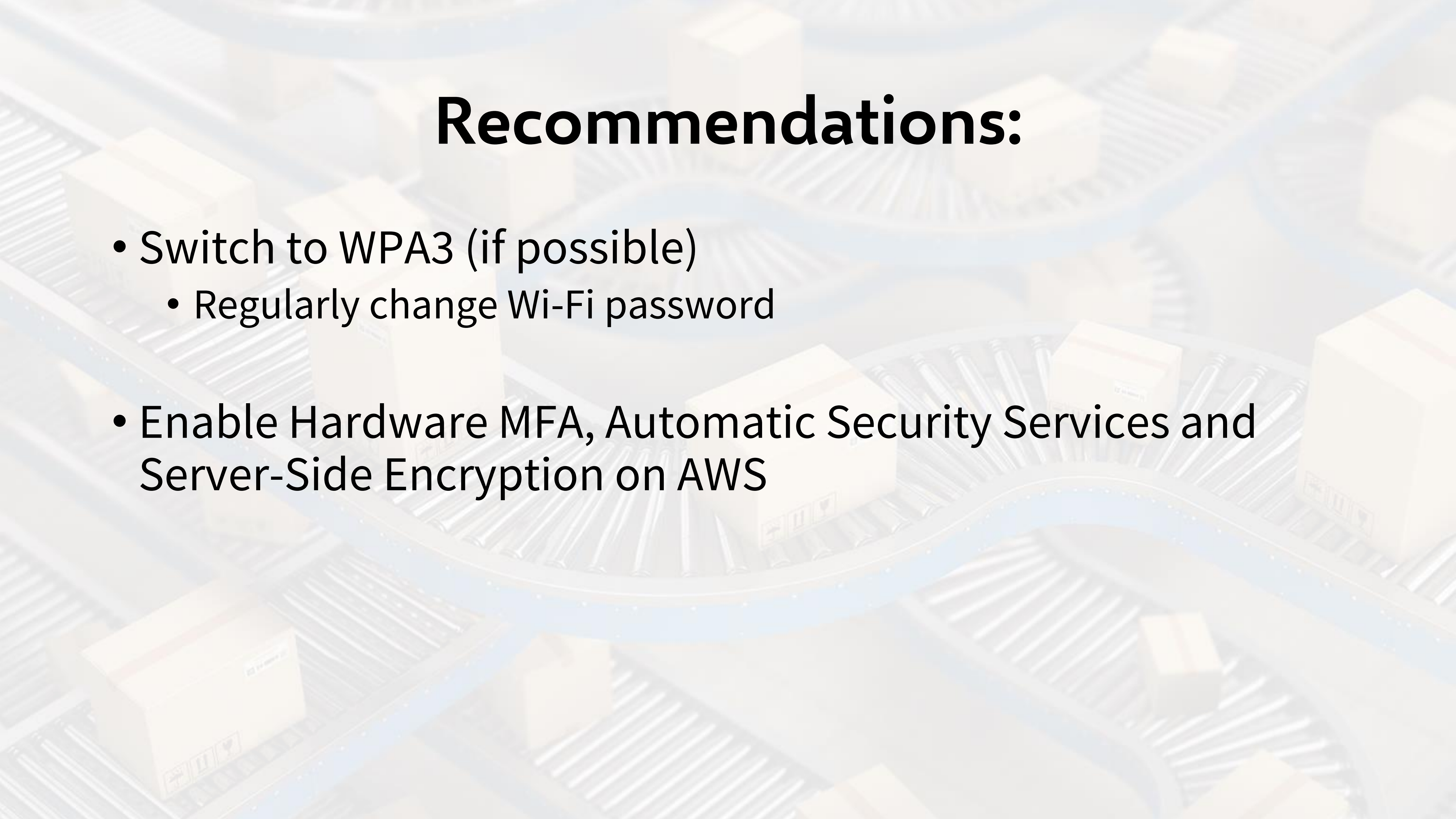
Install the AWS agent on EC2 Instances

Run an assessment for assessment target according to assessment template

Review findings and remediate issues



□		Severity	Date	Finding
□	▸	Low	04/22/2022 ...	On instance i-08ddc14a285ad1b07, TCP port 22 which is associated with 'SSH' is reachable from a Virtual Private Gateway
□	▸	Informational	04/22/2022 ...	Aggregate network exposure: On instance i-08ddc14a285ad1b07, ports are reachable from a Virtual Private Gateway through ENI eni-0c7489abd98999d07
□	▸	Informational	04/22/2022 ...	On instance i-08ddc14a285ad1b07, TCP port 443 which is associated with 'HTTPS' is reachable from a Virtual Private Gateway
□	▸	Informational	04/22/2022 ...	On instance i-08ddc14a285ad1b07, TCP port 80 which is associated with 'HTTP' is reachable from a Virtual Private Gateway



Recommendations:

- Switch to WPA3 (if possible)
  - Regularly change Wi-Fi password
- Enable Hardware MFA, Automatic Security Services and Server-Side Encryption on AWS

Thank you

DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA

NATIONAL CENTERS OF ACADEMIC EXCELLENCE
IN CYBERSECURITY

UNIVERSITY OF WISCONSIN
STOUT

Questions?

Contact: Dr. Holly Yuan

yuanh@uwstout.edu