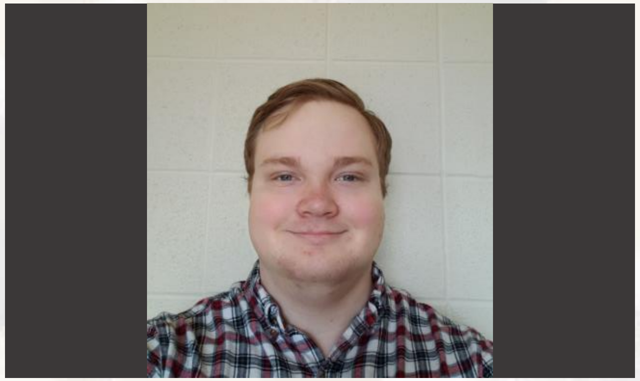
THE PROJECT IS SPONSORED BY DEPARTMENT OF DEFENSE NATIONAL CENTER OF ACADEMIC EXCELLENCE IN CYBERSECURITY (NCAE-C) CURRICULUM AND RESEARCH 2020 PROGRAM

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

Reaching Towards the Future of Manufacturing

Students Research Team



Wesley Larrabee (CEE) - Team Lead/Hardware Engineer

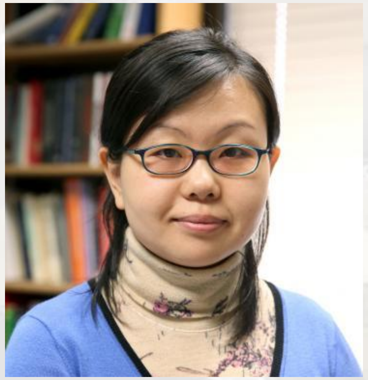
Scott Bresnahan (CNIT) - AWS Engineer/5G Engineer

Michael Laffin (CEE) - Hardware Engineer

Neil Borden (CNIT) - AWS/Network Security Engineer

Lee Kottke (CNIT) - AWS/Network Security Engineer

Advisory Board



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

Agenda

- Problem Statement
- Equipment and Software
- Implementations
- Case Studies and Demos
- Testing Policies
- Lessons Learned

WHAT PROBLEMS AFFECT A MANUFACTURE?

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

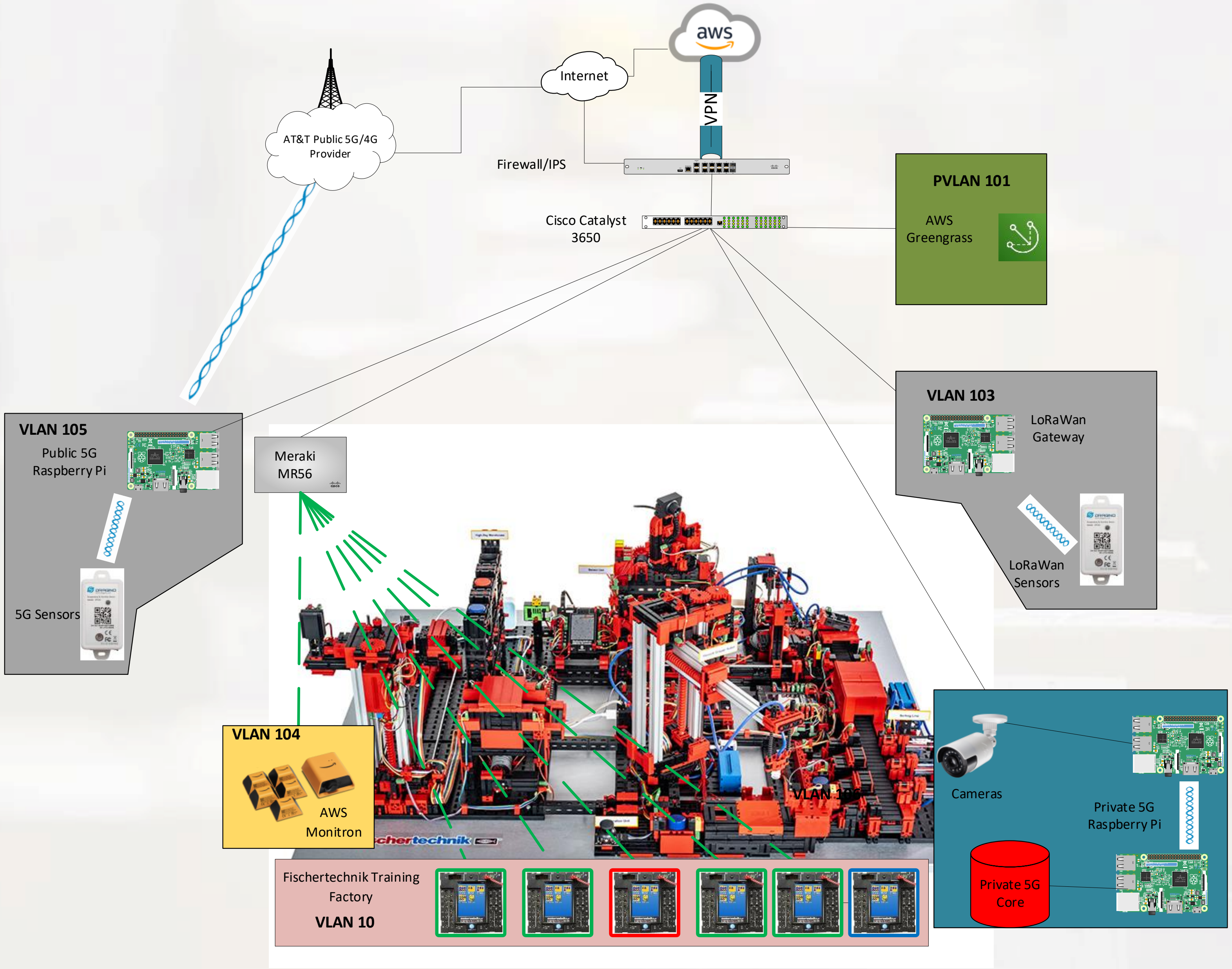
CYBERSECURITY RELATED ATTACKS POSE A THREAT TO THE FUTURE OF MANUFACTURING.

HOW DO WE SOLVE THESE ISSUES?

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

FACTORY IN THE LAB

OUR NETWORK


aws
Internet
VPN
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
Cameras
Private 5G Raspberry Pi
Private 5G Core
Fischertechnik Training Factory
VLAN 10

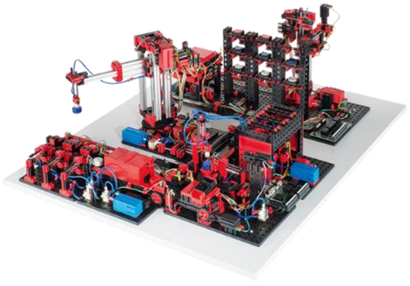
EQUIPMENT

AWS Monitron

Meraki MX84

Raspberry Pi 5G Hat

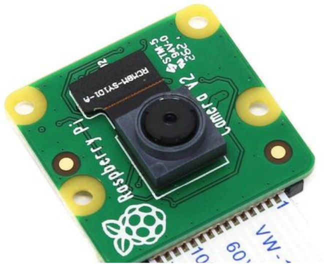
LoRaWAN Raspberry Pi



Fishertechnic Factory Floor

Private 5G Raspberry Pi

Edge Computing Raspberry Pi



Raspberry Pi Cameras

SOFTWARE

Amazon Web Services

DUO Multifactor

Open5GS

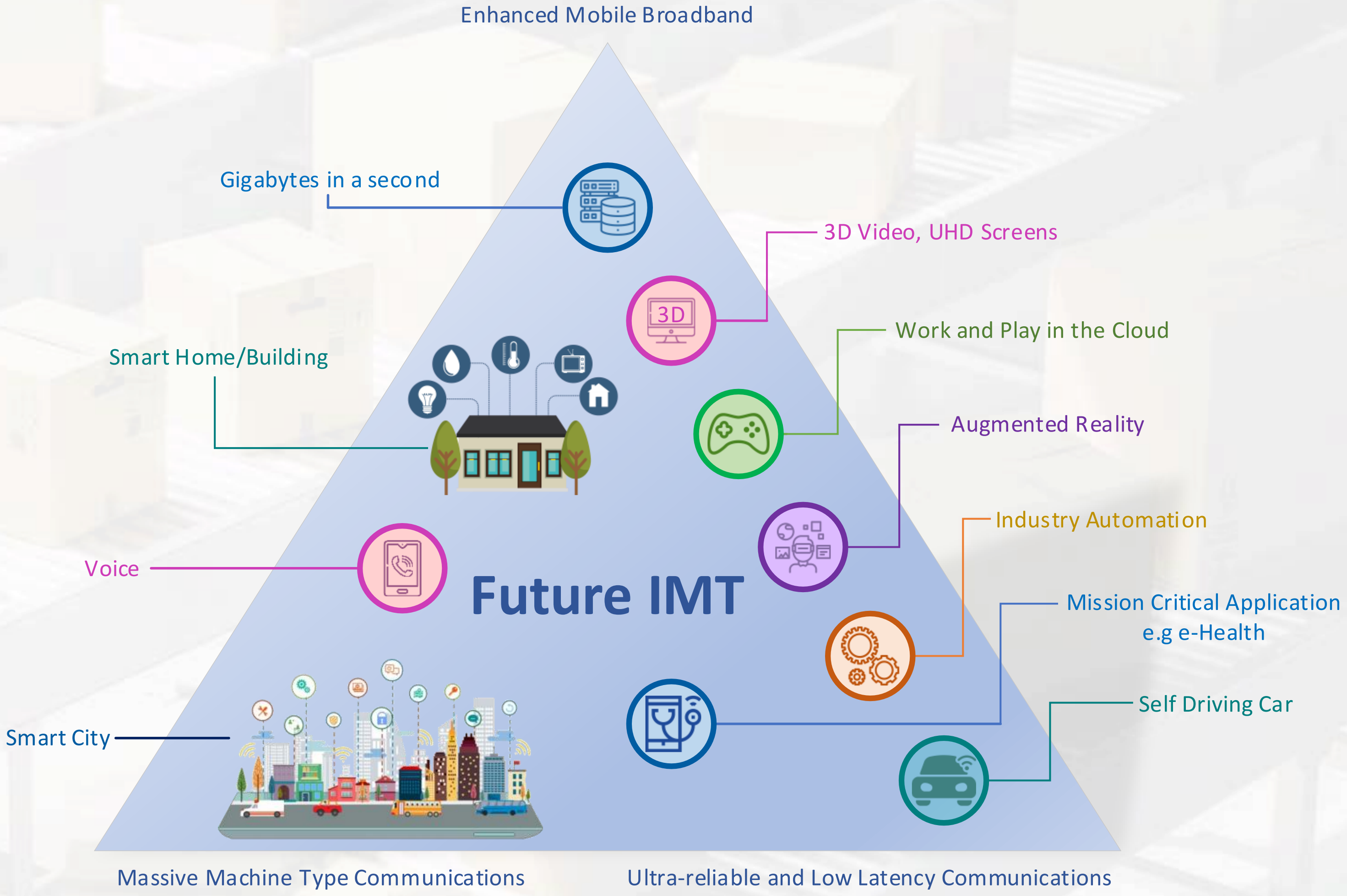
Edge Impulse

UERANSIM

Cisco Meraki Cloud

MAIN GOALS OF 5G

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

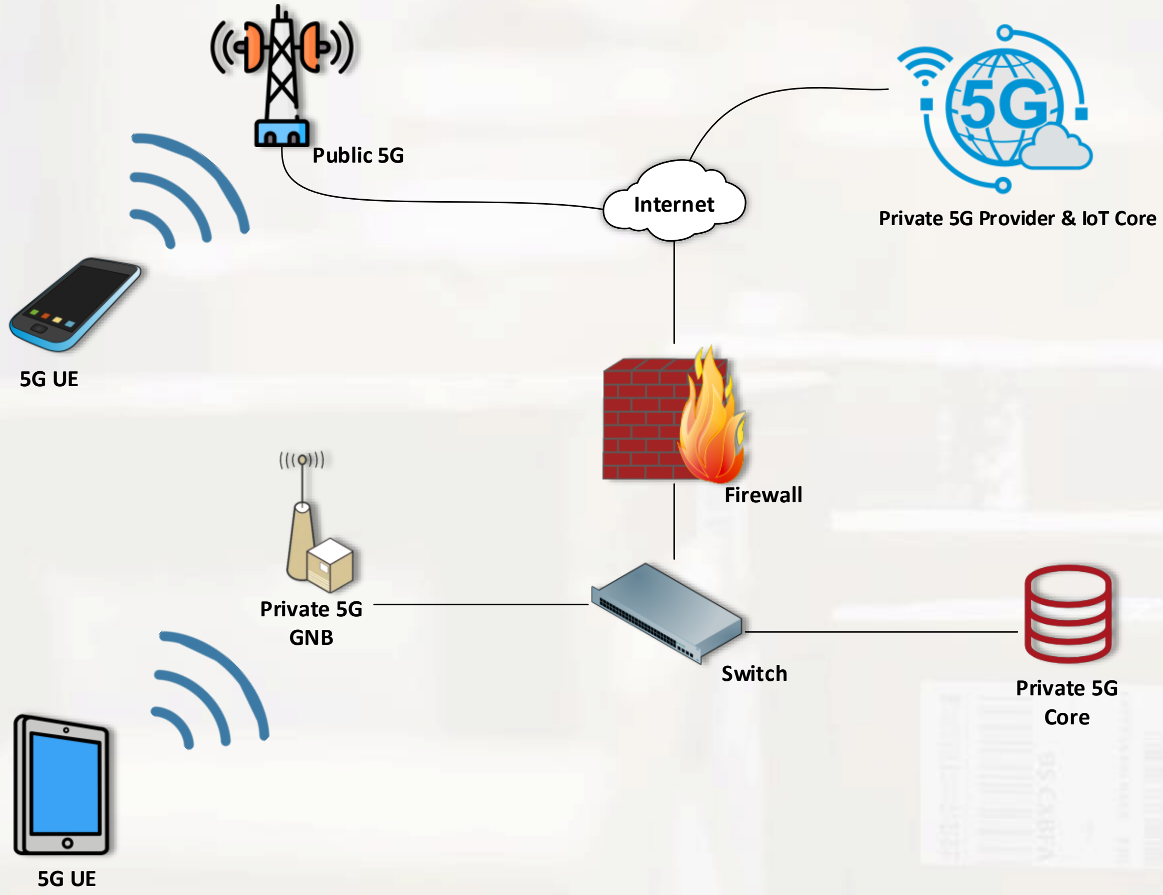


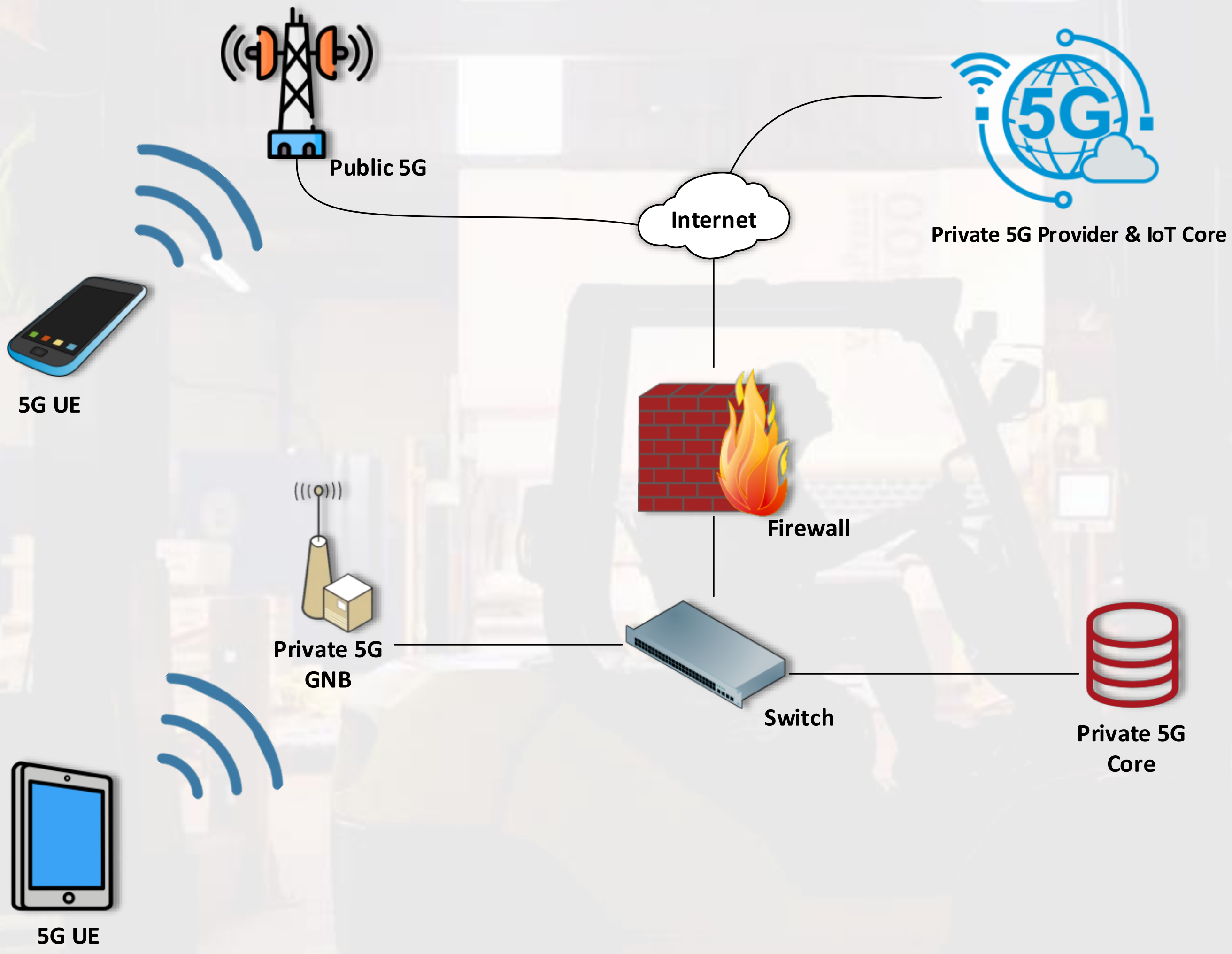
Enhanced Mobile Broadband
Gigabytes in a second
3D Video, UHD Screens
3D
Work and Play in the Cloud
Smart Home/Building
Augmented Reality
Industry Automation
Voice
Future IMT
Mission Critical Application e.g e-Health
Self Driving Car
Smart City
Massive Machine Type Communications
Ultra-reliable and Low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

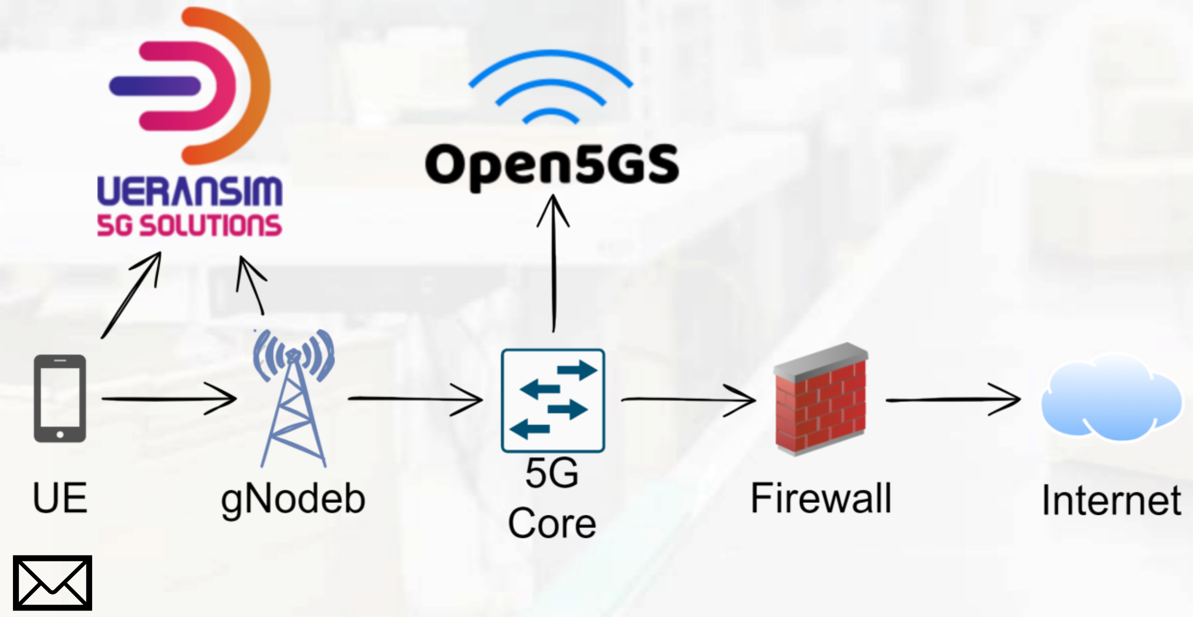
- On-Premise
- Cloud
- Managed Services

Open5GS

aws

cisco

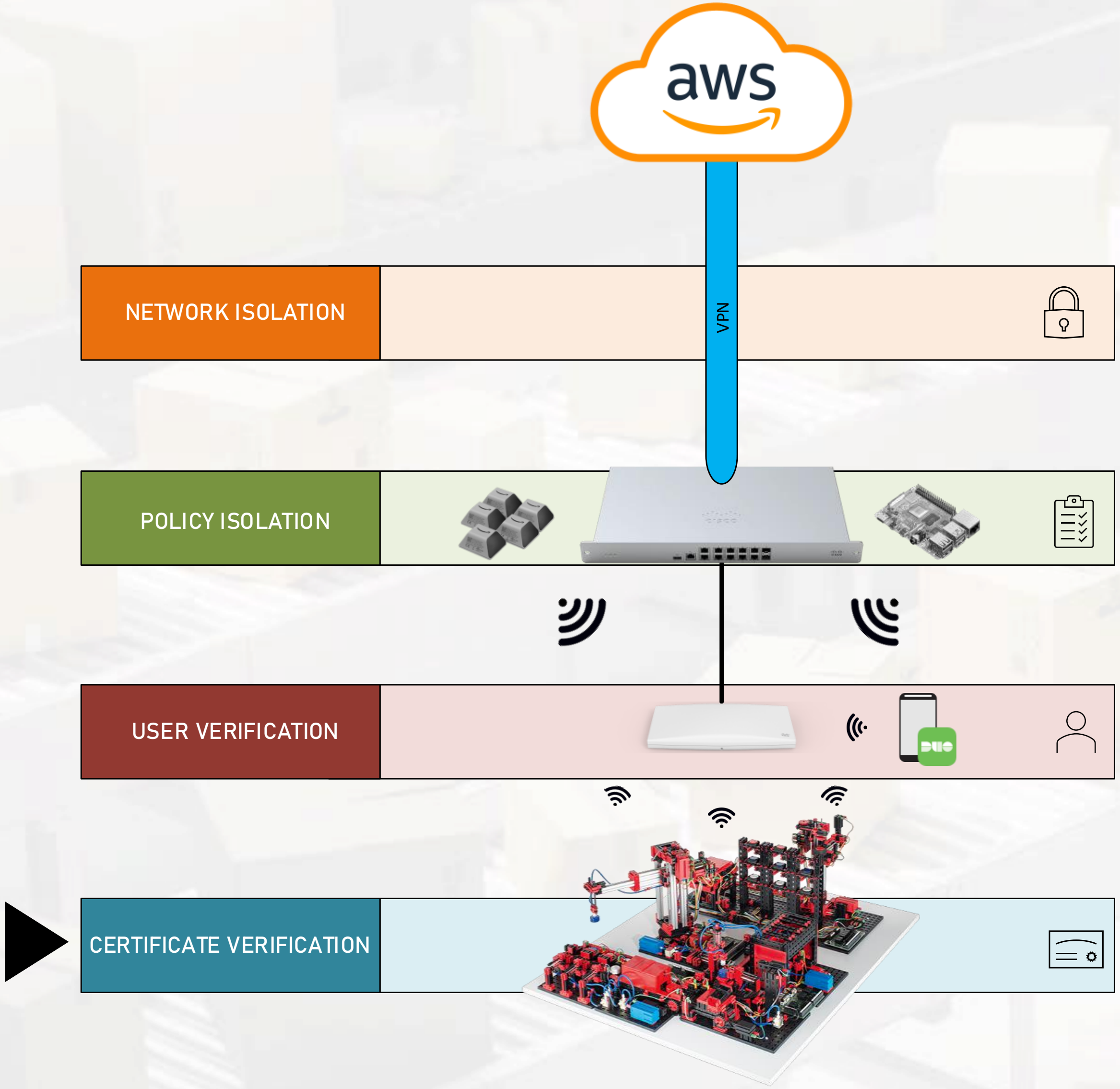
IMPLEMENTATION OF PRIVATE 5G (EMULATED)



- **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.

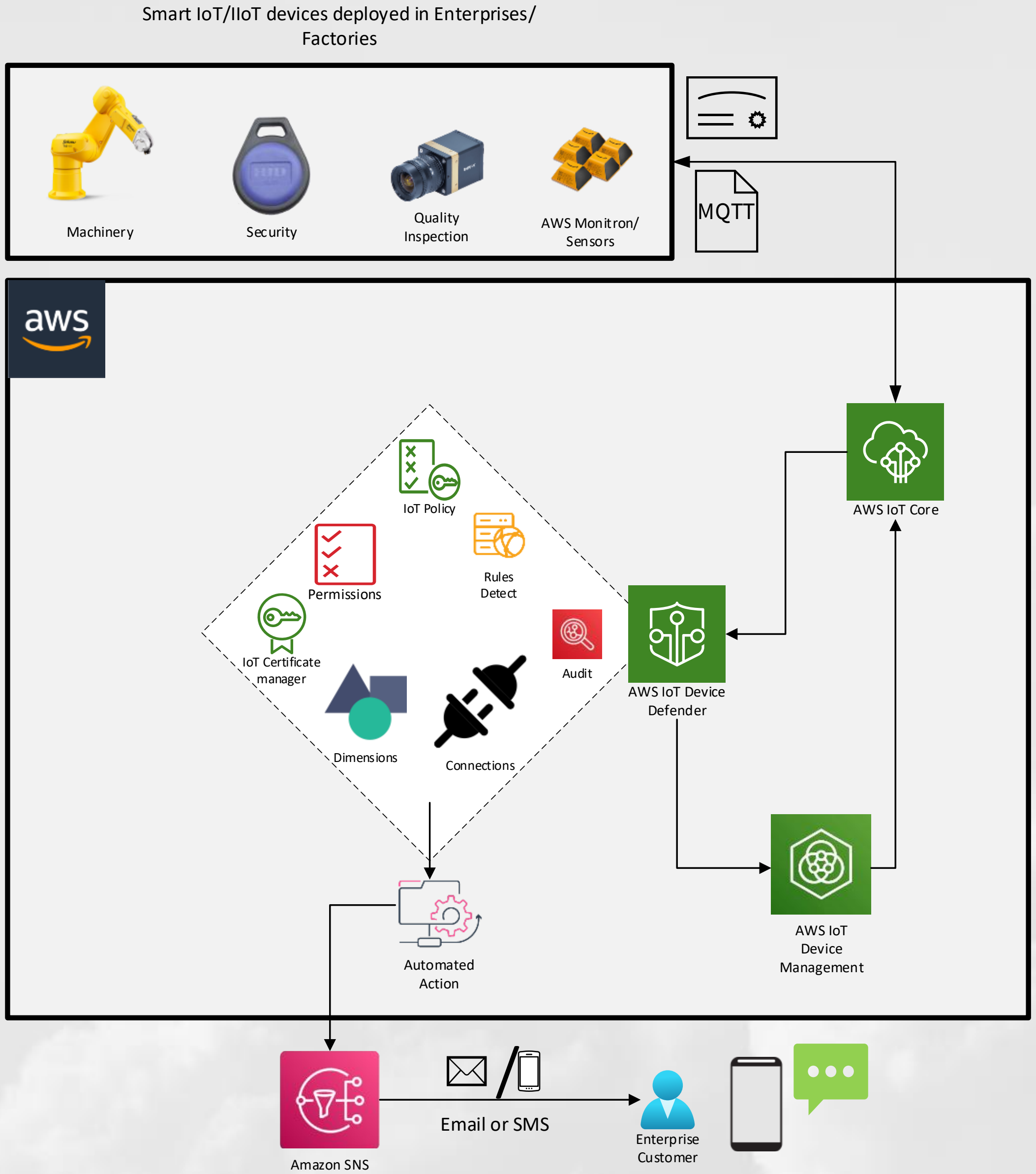
DESIGN – SECURITY: ZERO TRUST



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

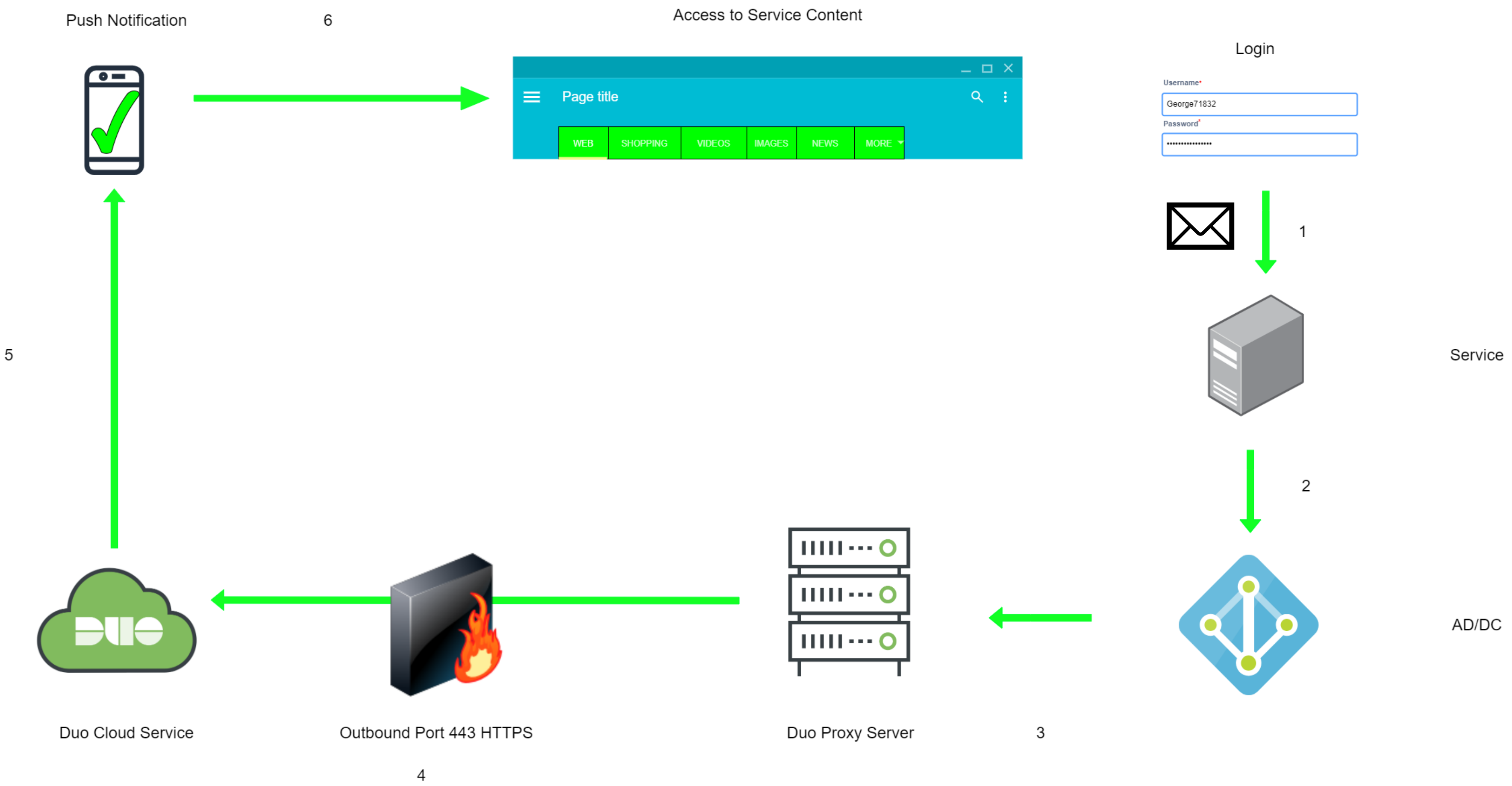
DESIGN – SECURITY:

CLOUD SECURITY ZERO TRUST



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

DUO MFA



Push Notification

6

Access to Service Content

Login

Username*

George71832

Password*

1

Service

5

2

AD/DC

Duo Cloud Service

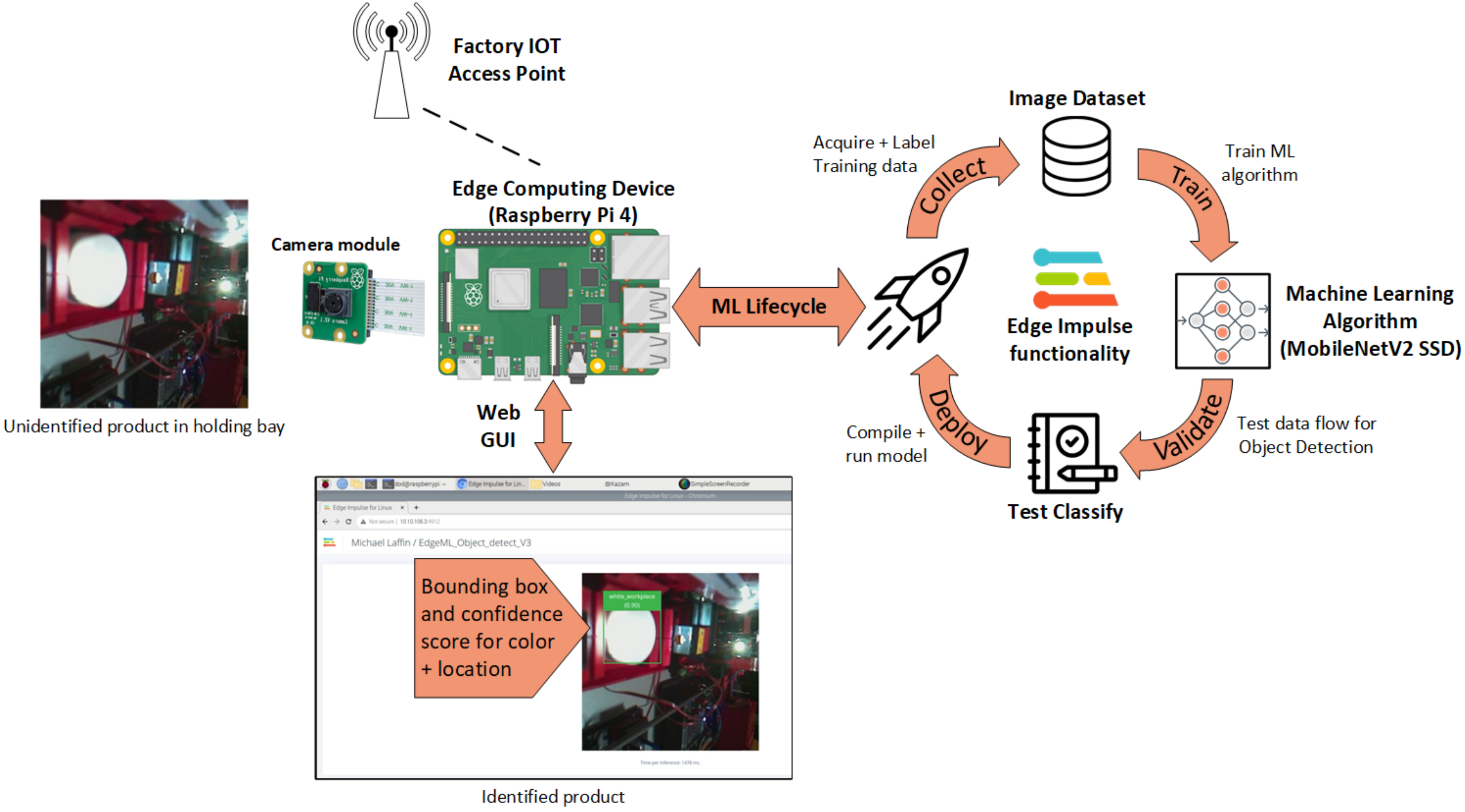
Outbound Port 443 HTTPS

Duo Proxy Server

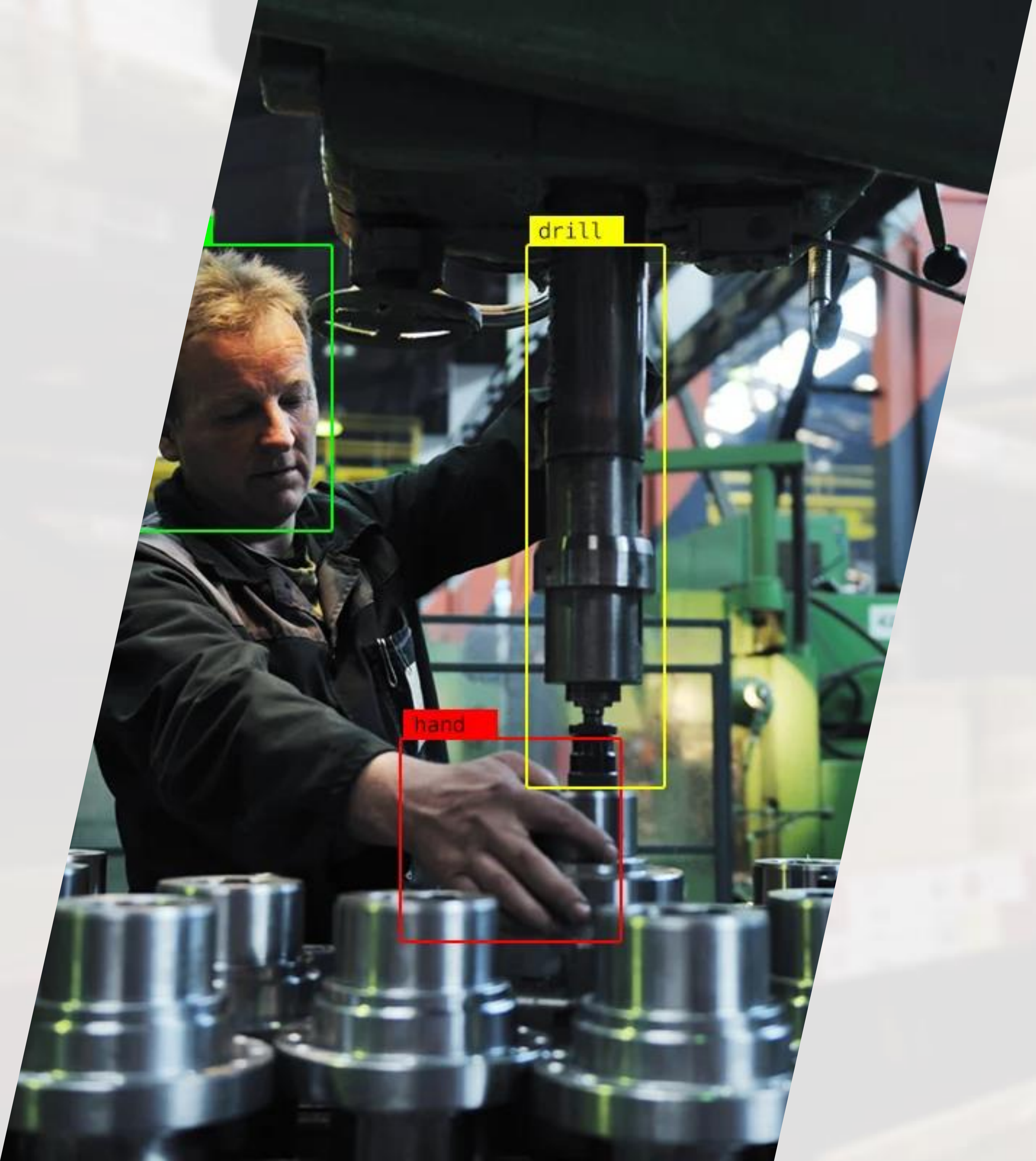
3

4

DESIGN – EDGE COMPUTING + MACHINE LEARNING



CASE STUDIES



Case Study 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

Case Study 2

Predictive Maintenance

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

Case Study 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.

Case Study 4

Improve Productivity

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

Testing

NETWORK CONNECTIVITY

IOT CORE CONNECTIVITY

SECURITY

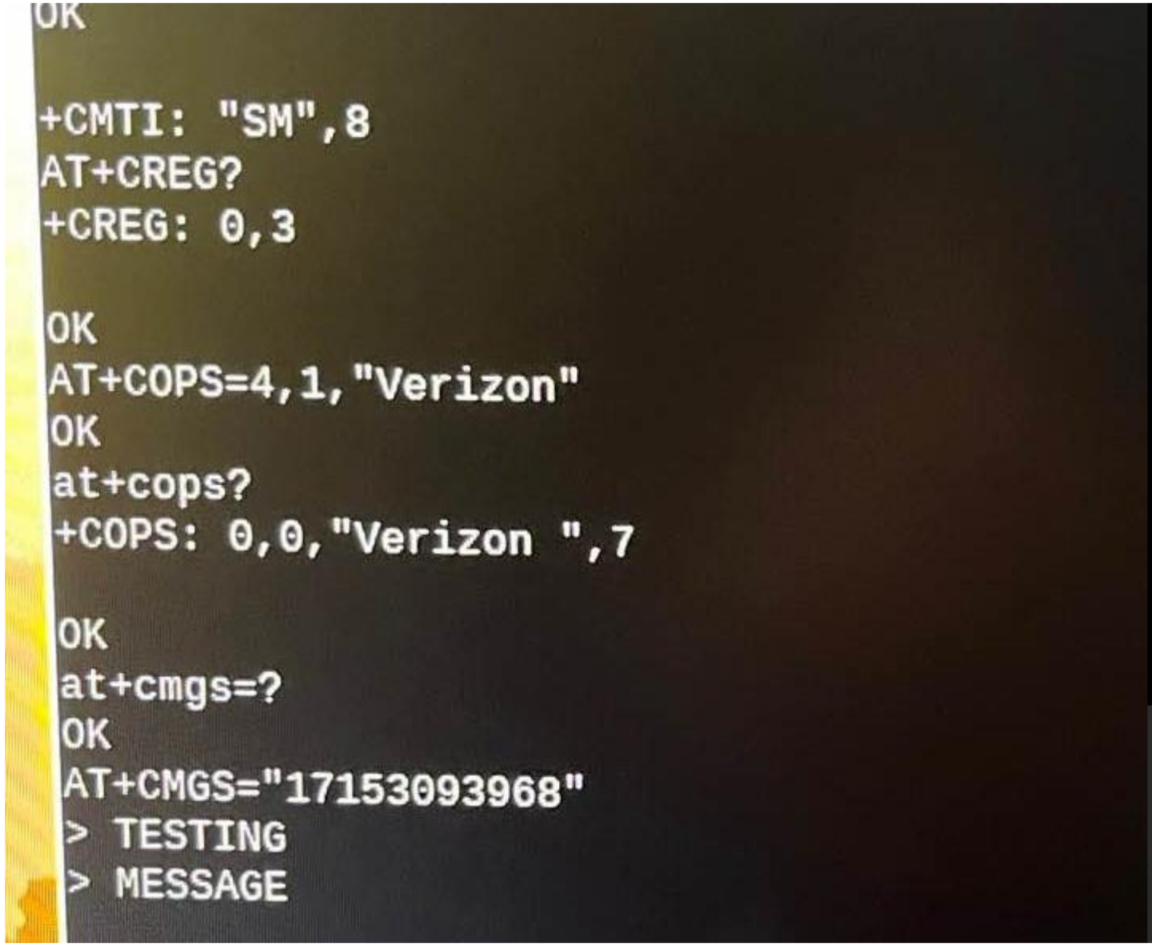
QUALITY

PREDICATIVE MAINTENANCE

INVENTORY MANAGEMENT

PRODUCTIVITY

TESTING– PUBLIC 5G

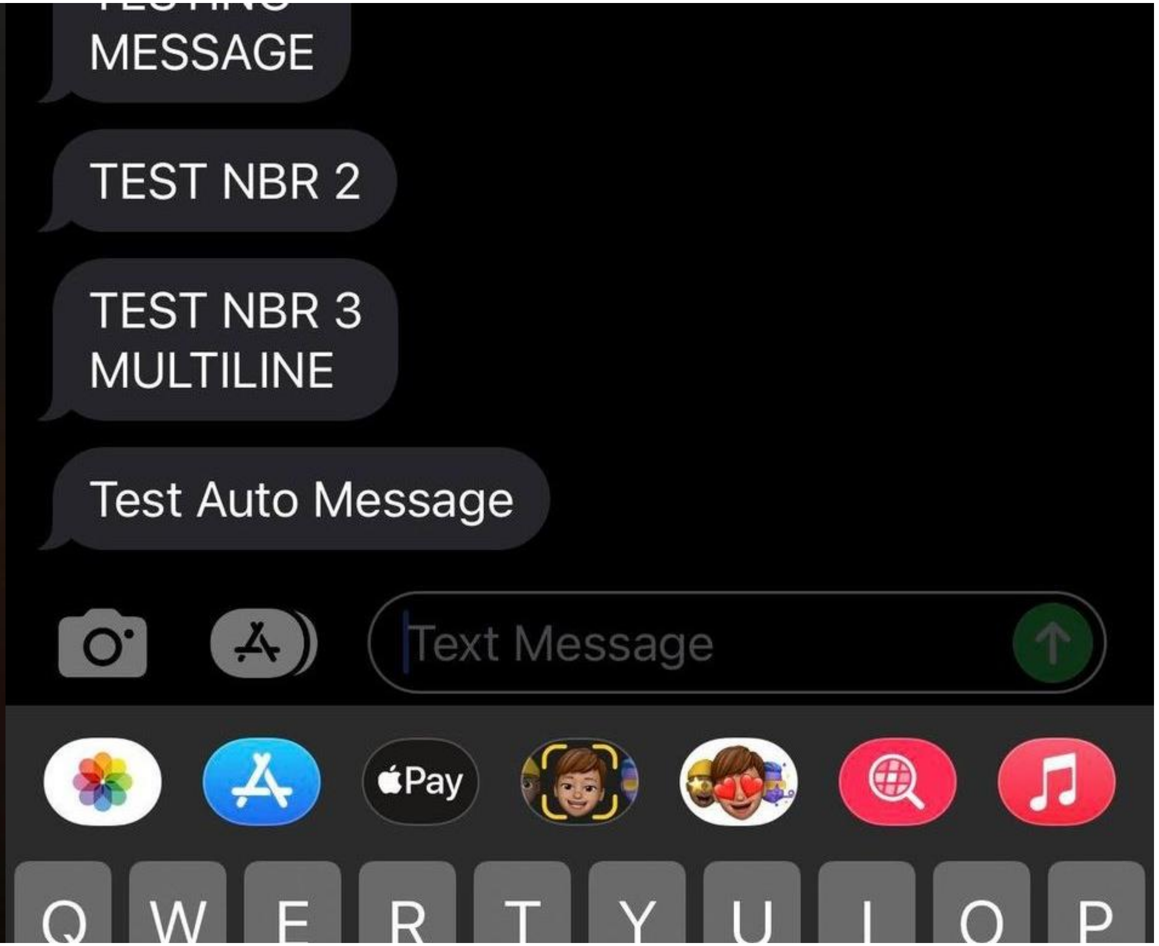


```
OK

+CMTI: "SM",8
AT+CREG?
+CREG: 0,3

OK
AT+COPS=4,1,"Verizon"
OK
at+cops?
+COPS: 0,0,"Verizon ",7

OK
at+cmgs=?
OK
AT+CMGS="17153093968"
> TESTING
> MESSAGE
```



TESTING
MESSAGE

TEST NBR 2

TEST NBR 3
MULTILINE

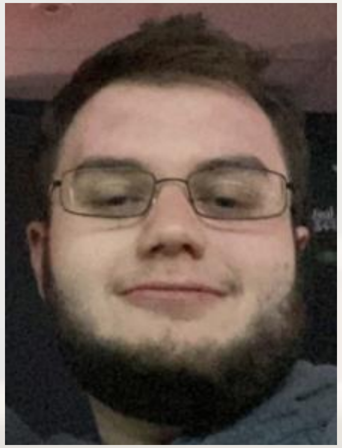
Test Auto Message

DUO DEMONSTRATION & TESTING

IOT SECURITY PENTEST/AUDIT

White Hat Hacker Team

Who we are:



Matthew Korte – Hardware and Firmware vulnerabilities expert

Chris Caravella – Wireless Network and Cloud vulnerabilities Pen tester

Andrew Hanson – OpenVAS, NMAP, Metasploit Engineer

Industry Advisors: Sam Gibson and Brian Halbach

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.

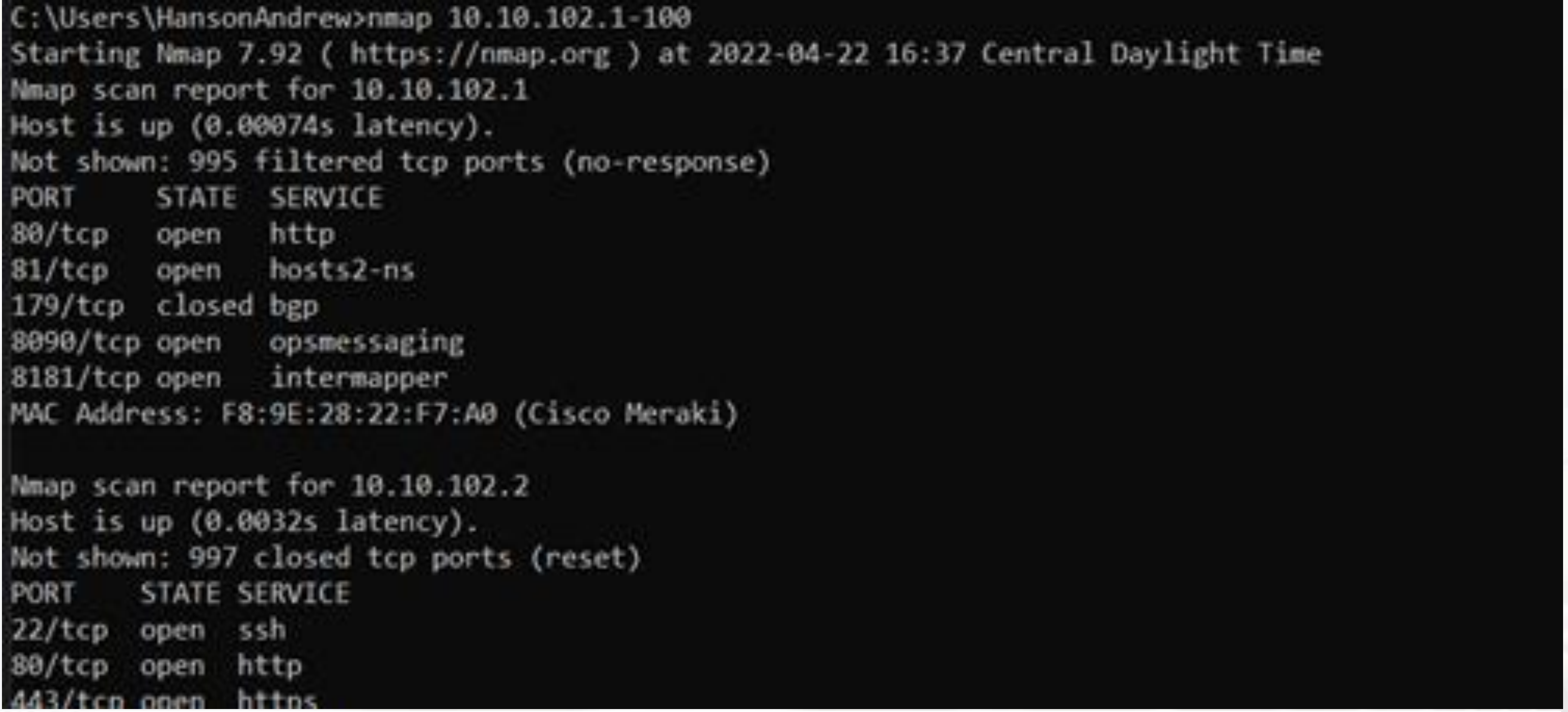
What we’ve done:

- Took inventory of the on-premise network devices/assets
    - 4x Raspberry Pi 4
    - Meraki Firewall MX84
    - Meraki AP MR56
    - Cisco 3650 Catalyst Switch
    - Various informational sensors

- Looked through the data flow of the network for policies used
    - Zero Trust
    - Least Privilege
    - Verified Users
    - Identifying certificates

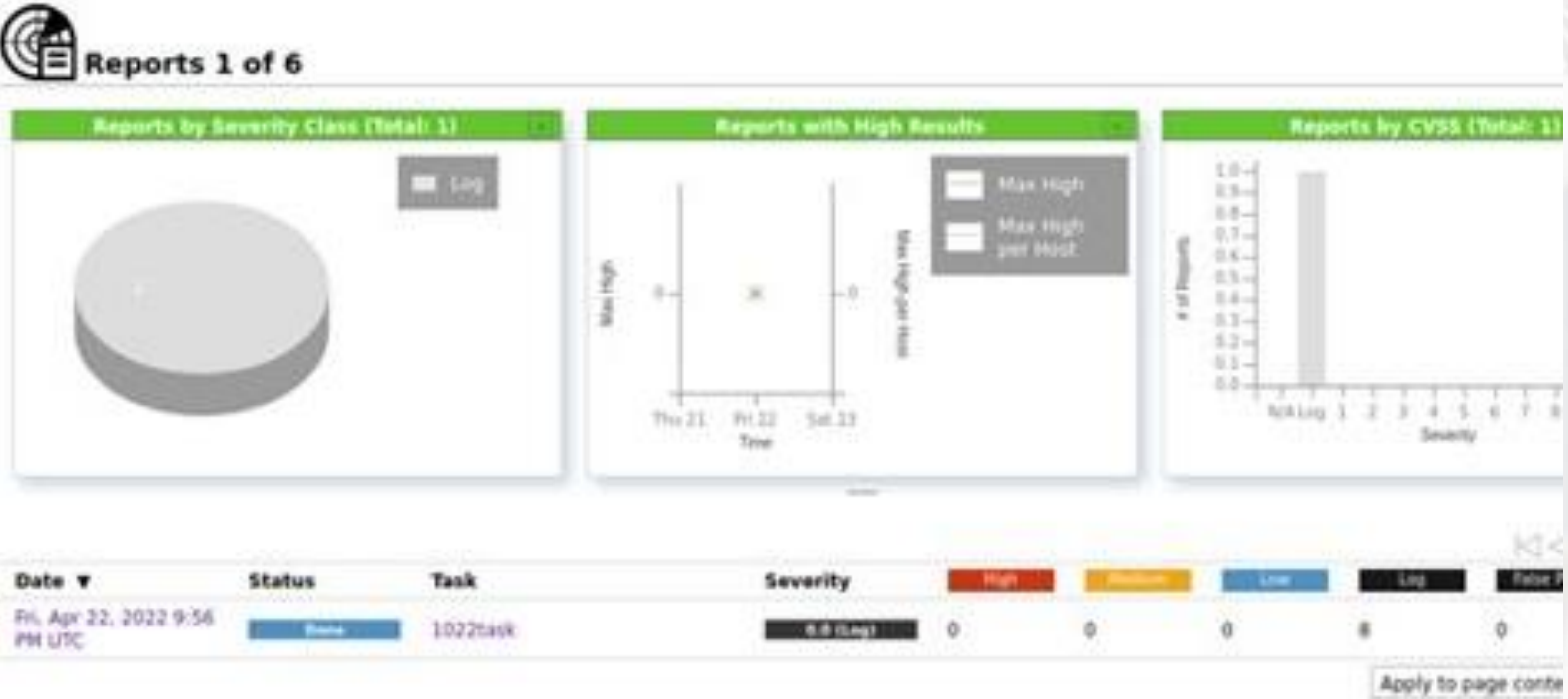
The Audit

- 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

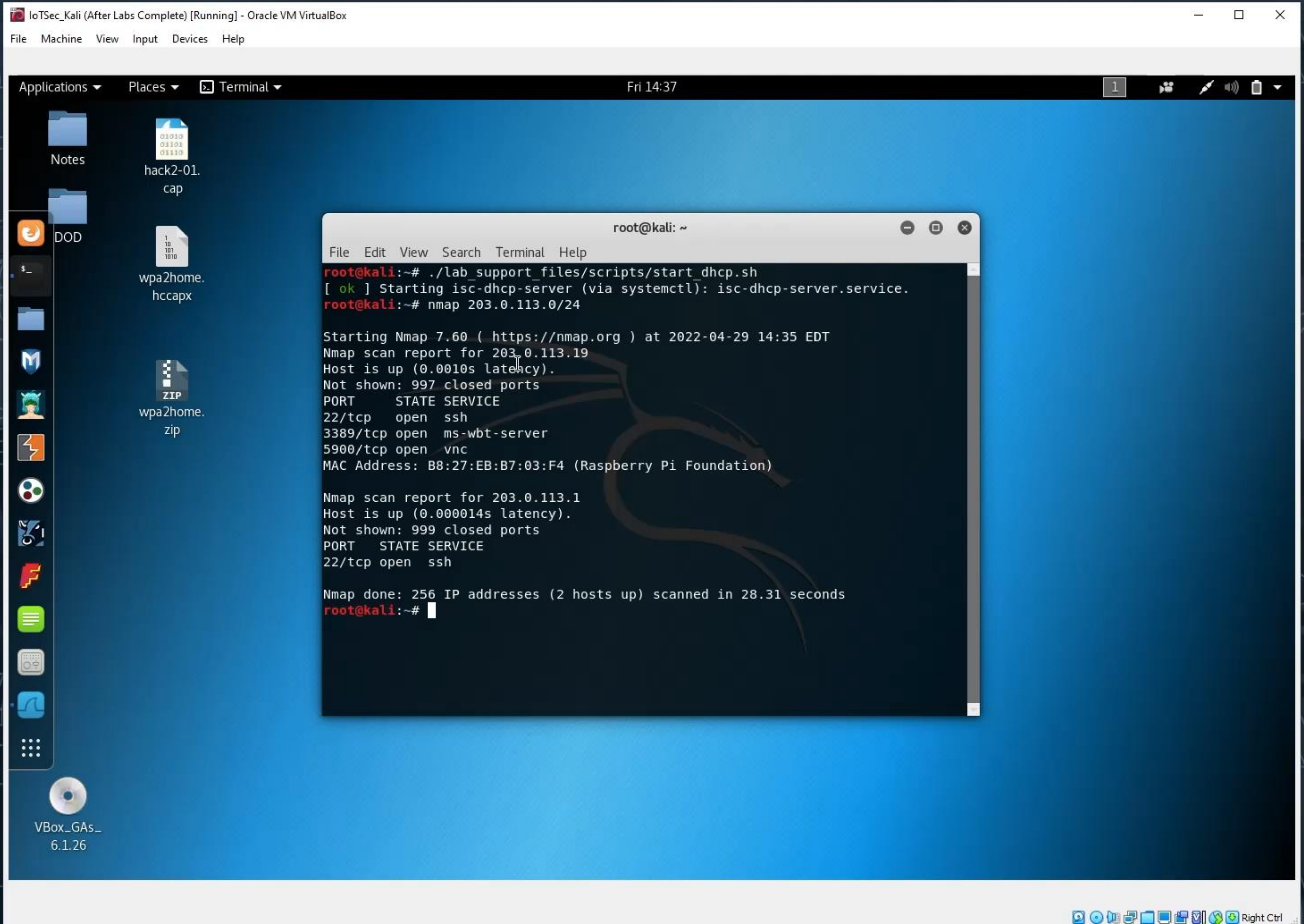
Date ▼	Status	Task	Severity	High	Medium	Low	Log	False P
Fri, Apr 22, 2022 9:56 PM UTC	Done	1022task	0.0 (Log)	0	0	0	8	0

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.


IoTSec_Kali (After Labs Complete) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Fri 14:37
Notes
DOD
hack2-01.cap
wpa2home.hccapx
wpa2home.zip
VBox_GAs_6.1.26
root@kali: ~
File Edit View Search Terminal Help
Right Ctrl

```
root@kali:~# ./lab_support_files/scripts/start_dhcp.sh
[ ok ] Starting isc-dhcp-server (via systemctl): isc-dhcp-server.service.
root@kali:~# nmap 203.0.113.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2022-04-29 14:35 EDT
Nmap scan report for 203.0.113.19
Host is up (0.0010s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
3389/tcp open  ms-wbt-server
5900/tcp open  vnc
MAC Address: B8:27:EB:B7:03:F4 (Raspberry Pi Foundation)

Nmap scan report for 203.0.113.1
Host is up (0.000014s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (2 hosts up) scanned in 28.31 seconds
root@kali:~# 
```

AWS Auditing

AWS Security Hub

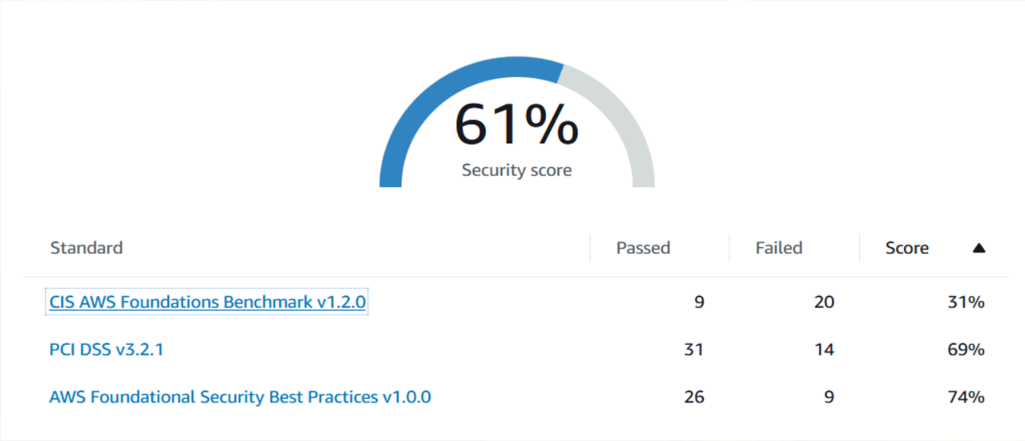
- Look for Best Practice Security

AWS Inspector

- Look for network reachability

Results:

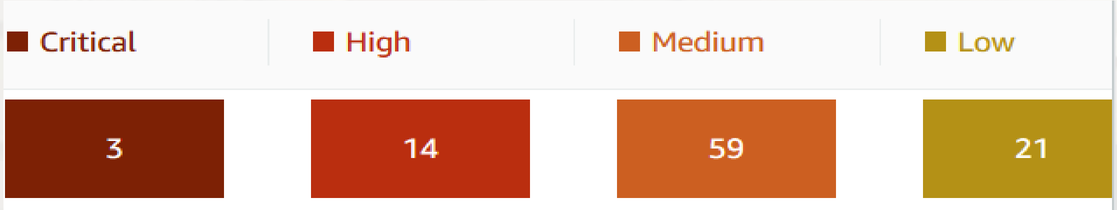
- IoT devices were secured through their serial ports and other means of unauthorized access.
- We were able to capture a WPA2 handshake from the Wi-Fi.
- The security on user's accounts and external connections are secure, no access was granted besides what was allowed by the router and firewalls.



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%



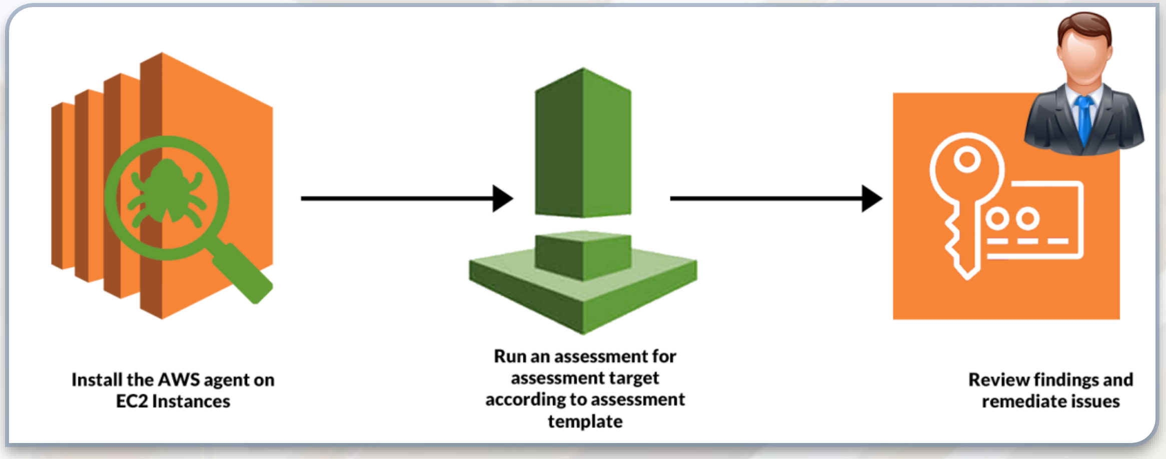
■ Critical	■ High	■ Medium	■ Low
3	14	59	21

AWS Security hub

- 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

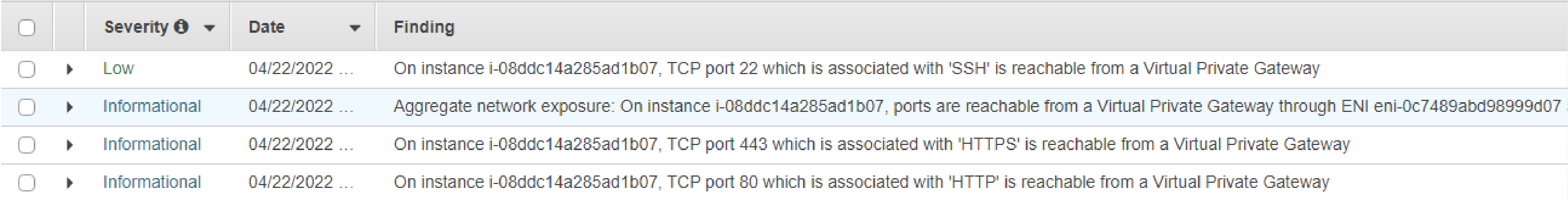
- For the assessment run we conducted only one low severity risk was detected.



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

Lesson Learned

- Wesley
  - Better understanding of working in a mix discipline group
  - First time leading a project
- Lee
  - Hired as a Network Security Engineer for Smart Manufacturing thanks to this project.
- Neil
  - Zero Trust
  - 5G/IoT Technologies
- Scott
  - Private 5G Configuration
  - Zero Trust
  - AWS Configuration
- Michael
  - Edge Impulse

Lesson Learned – White Hat Hacker

- Chris C.
  - Improved research skills
  - Wireless LANs
  - Auditing

- Matt
  - Usefulness of CVE database
  - Raspberry pi firmware vulnerabilities

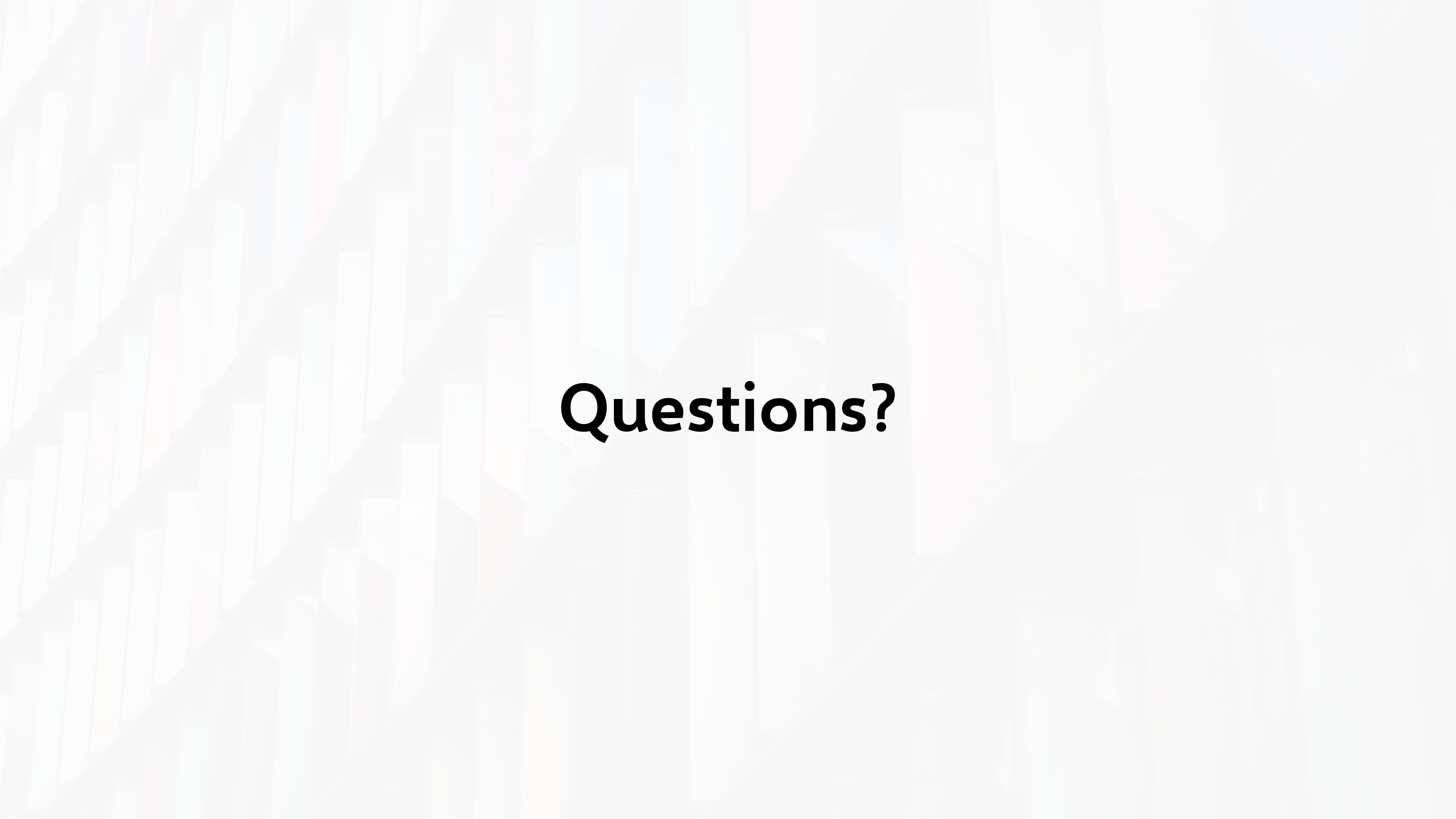
- Andrew
  - Recon for Vulnerabilities
  - Auditing Process

- Chris P.
  - Project Management
  - BLE Sniffing & Blocking

- Emily
  - Zigbee Sniffing with Raspberry Pi Zigbee Bridge
  - AWS Auditing Process

- Jordan
  - LoRa research process
  - AWS Auditing Process

Thank you



Questions?