Rochester Security Summit

Hacking and Defending XIoT

A hardware hacker and OT security expert share their perspectives on building, breaking and defending XIoT devices.

October 25, 2023

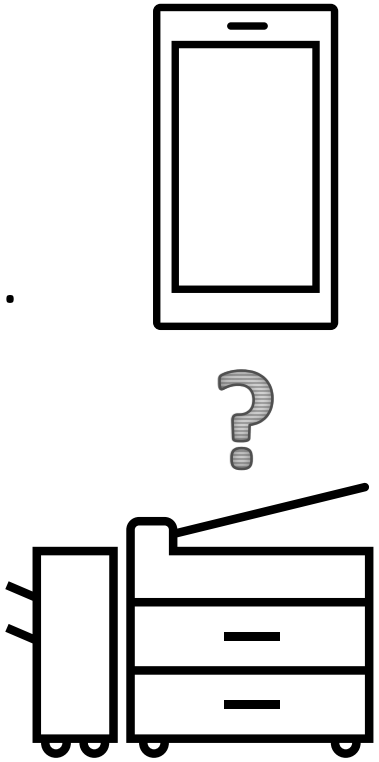
Introductions

- Zack Lehmann
- Senior Consultant
- ~5 years at SRA
- Focused on monitoring and detection in CPS/OT/XIoT

- Gabe Siftar
- 5 years at SRA, currently a Lead Scientist
- Previously spent 20 years as a design engineer for a medical device manufacturer
- Specializes in offensive security with a focus on XIoT, OT/ICS, and hardware devices

XIoT

XIoT Defined



There are many varying definitions of XIoT, and it can be subjective. Let's identify some basic criteria:

XIoT Devices:

- Are network-connected
- Often interact with the real world (sensors, actuators, etc)
- Serve an important function for the owner (often *ONLY* one)
- Often "security-challenged" – lack traditional cybersecurity capabilities
- Normally run firmware

Rule of thumb: If it runs EDR, it's probably *not* XIoT.

XIoT– “Extended Internet of Things”

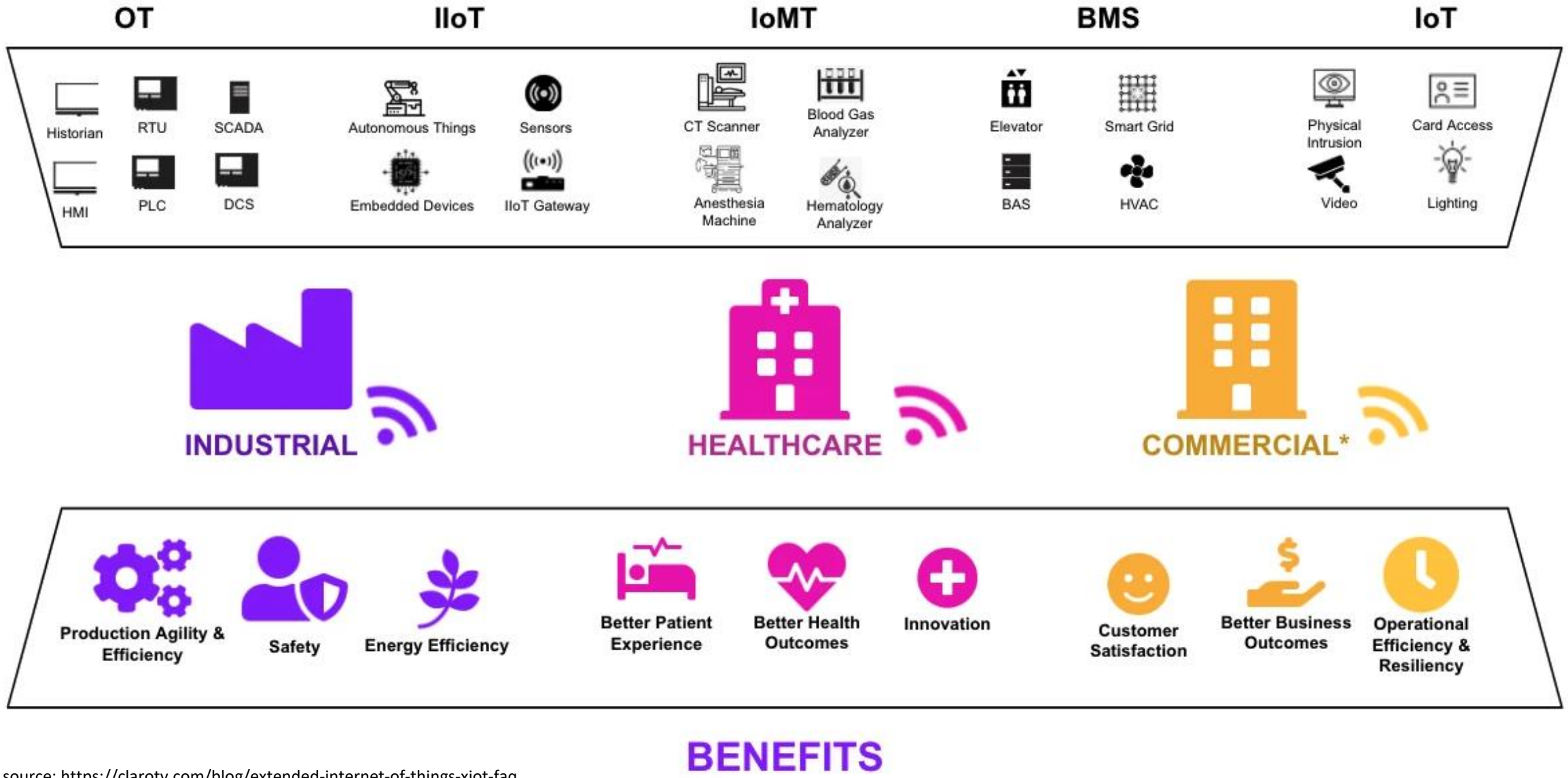
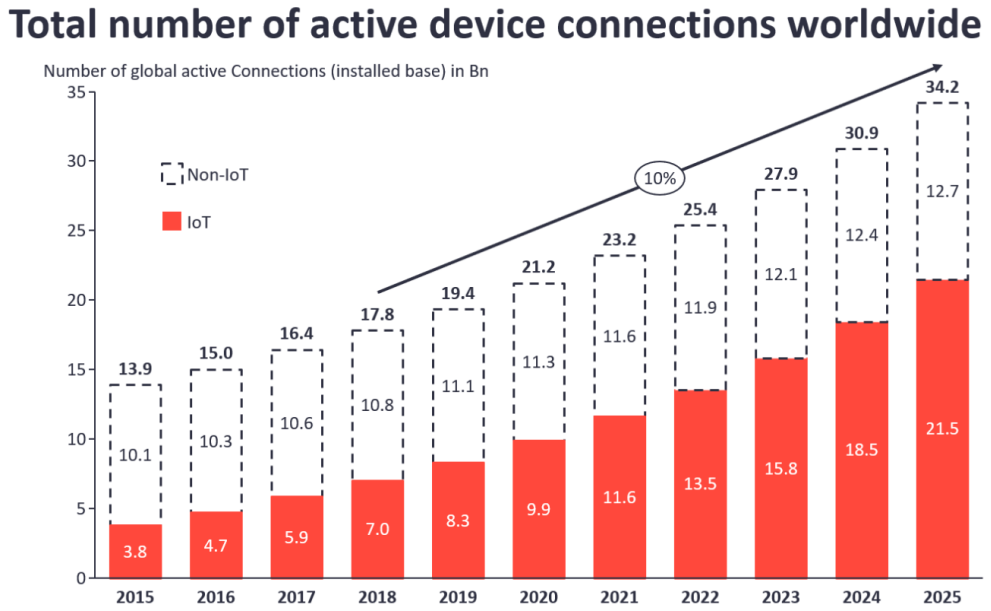


Image source: https://claroty.com/blog/extended-internet-of-things-xiot-faq

XIoT



Why should I care?

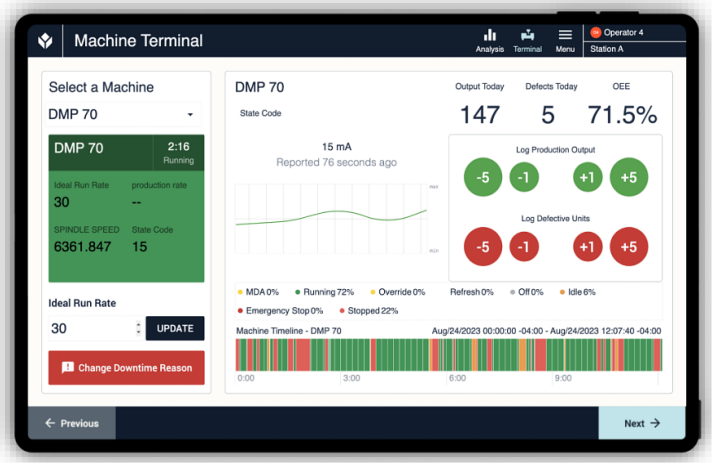
- Researchers are consistently identifying XIoT weaknesses
  "All you have to do is look"
- Increasingly deployed by the millions across all sectors
- Increasing dependency on XIoT devices
- Devices are often in the shadows, unaccounted for and unmaintained
- Relatively immature tools and practices
- Increasingly interesting to potential attackers

- Vulnerabilities
  - Akuvox E11 smart intercom – Claroty's Team82 discovered 13 vulnerabilities

- Attacks
  - QUIETEXIT – compromised SSH client commonly found on embedded devices. Attributed to APT29

Image Source: https://iot-analytics.com/wp/wp-content/uploads/2018/08/Number-of-global-device-connections-2015-2025-Number-of-IoT-Devices.png

XIoT Product Example



- Industrial Internet of Things (IIoT) Device
- Installed in settings such as water treatment or manufacturing facilities to provide:
  - Remote collection of operational data
  - Control of machine parameters
  - Extend existing input (sensing) or output capabilities
  - Enterprise integrations (ERP/MES)
  - Cloud integration capabilities to other IIoT devices with API's (e.g. digital scale)

Device: Tulip Edge IO https://tulip.co/products/edge-io/

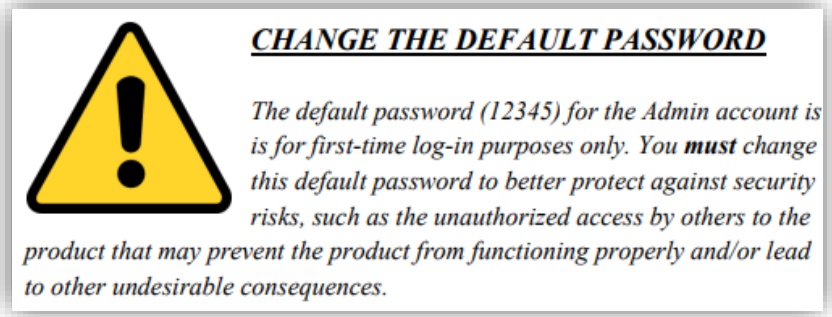
XIoT Security Threats & Weaknesses

Inherent (Introduced by manufacturers)

- Weak product security – devices often do not include common security features and capabilities
- Slow patch/update cycles
- Insecure default configurations
- Straight-up vulnerabilities (proprietary code or 3rd-party components)

Deployment-based (Introduced by end-users)

- Devices are deployed on enterprise networks rather than dedicated segments
- Insecure default configuration, e.g.:
  - Default password (often in user manual)
  - Unused features are left enabled, increasing attack surface
- Security features aren't always enabled or correctly configured
- Patches and updates made available by supplier not applied



https://us.hikvision.com/en/system/files_force/manual/20150119024136900.pdf

Attacking XIoT

Hacking Example

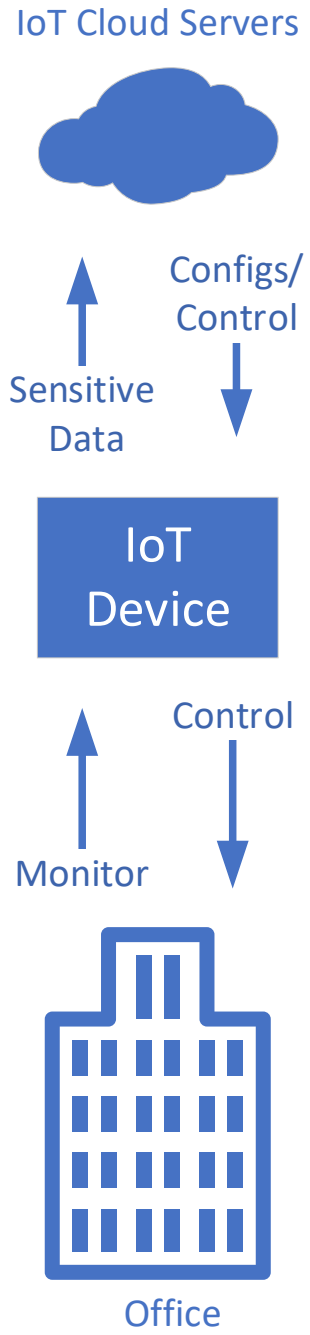
Device Tested: [Redacted due to pending responsible disclosure process]

Device Characteristics:

- Commonly found in enterprise and commercial settings
- Stores and transfers sensitive data
- Interfaces with the physical environment
- Communicates with cloud-based systems

Attack Objectives:

- Access to Sensitive Data (local and cloud)
- Denial of Service
- Manipulation of Control



Hacking Example - Findings

Vulnerability : Local access to sensitive data

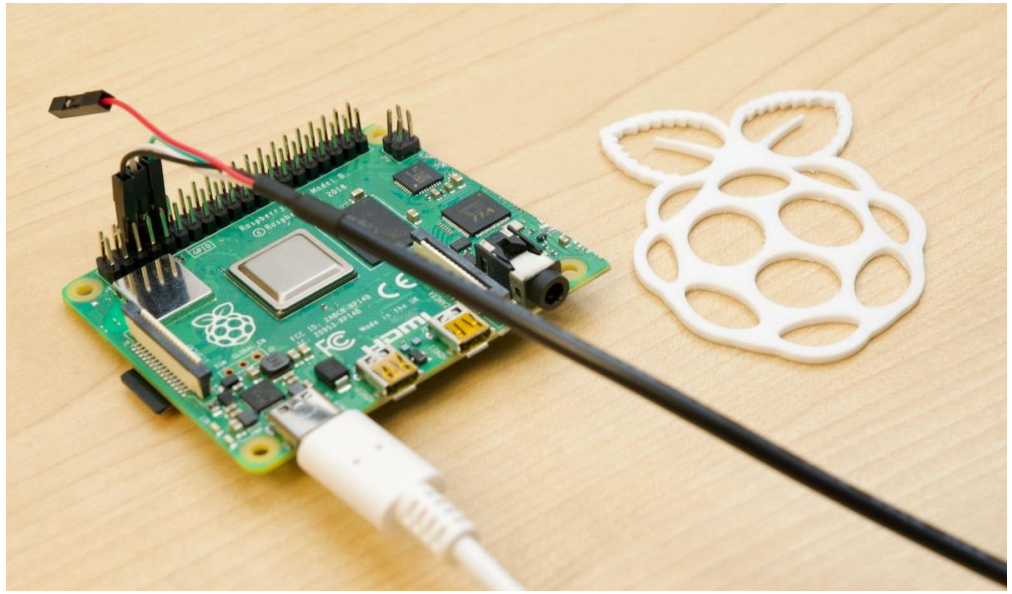
CVSS score: 7.6 (AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

Boot loader accessible via hardware serial console port with no authentication allowed full access to device memory.

- Dump memory
- Extract & reverse engineer file system
- Identify sensitive data
- PWN!

Impact:

- Full device access (ability to set root password)
- Control of any device function (root can do everything)
- Full ability to interact with the physical world
- Access to local sensitive data
- Impersonate device to access cloud resources



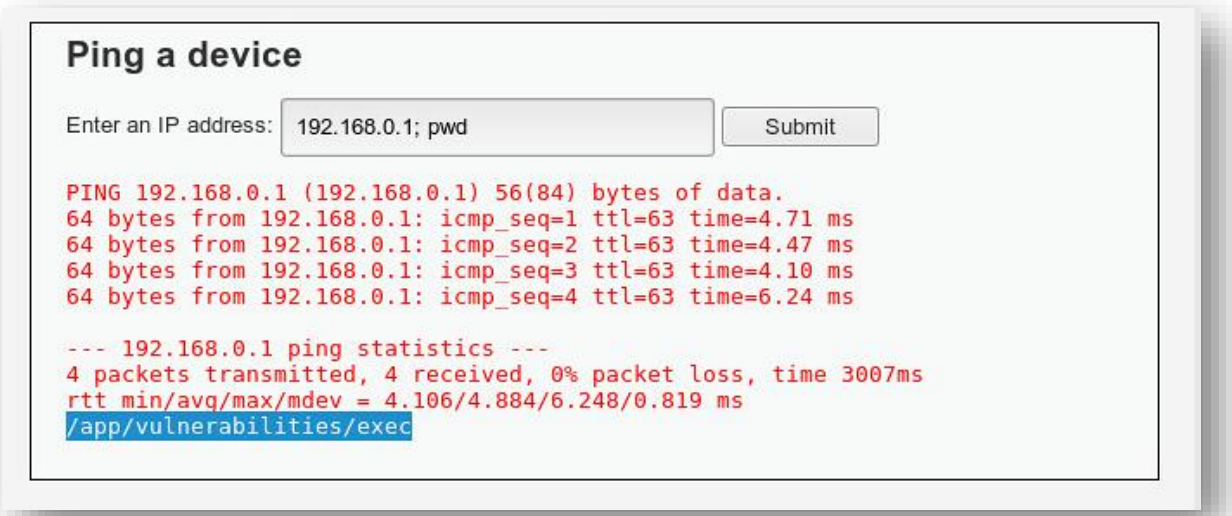
```
U-Boot 2018.09 (Oct 04 2018 - 05:36:06 -0700)

DRAM:  128 MiB
RPI Zero (0x900093)
MMC:   sdhci@7e300000: 0
Loading Environment from FAT... *** Warning - bad CRC, using default environment

In:    serial
Out:   vidconsole
Err:   vidconsole
Net:   No ethernet found.
starting USB...
USB0:   scanning bus 0 for devices... 2 USB Device(s) found
       scanning usb for storage devices... 0 Storage Device(s) found
Hit any key to stop autoboot:  0
U-Boot>
```

Image credits: https://www.jeffgeerling.com/blog/2021/attaching-raspberry-pis-serial-console-uart-debugging

Hacking Example - Findings

Vulnerability: Command Injection

CVSS score: 9.0 (AV:A/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)



Administrative web interface (requires authenticated access)

- Test all fields for potential injection flaws
- Identify unexpected behavior
- Weaponize
- Exploit (e.g. set root password -> connect via SSH -> control)

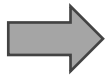
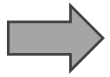
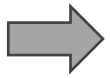
Impact:

- **Remote (local network)** control of device function (root can do everything)
- **Remote** ability to interact with the physical world
- **Remote** access to local sensitive data
- Impersonate device to access cloud resources

Image credit: https://chris-young.net/dvwa-command-injection/

Securing XIoT

XIoT Security – A Shared Responsibility

Manufacturer			Owner	
Practice	**Examples**		**Practice**	**Example**
Build secure by design products	Secure software development life cycle (SDLC) Penetration testing Software Bill of Materials (SBOM) Include recommended security features.		Procure secure devices	Purchasing standards, vendor and product evaluation, Manufacturer Disclosure Statement for Medical Device Security (MDS2)
Create user-facing cyber security guidance	IT Security Guide, Product Security Whitepapers		Secure deployment	Deploy according to manufacturer recommendations and industry best practices. Monitor and integrate with security tools.
Maintain product security	Track supply chain vulnerabilities, disclosure process, release products patches/updates, communicate		Maintain security	Create device inventory and establish visibility. Implement a patch/mitigation strategy (Tune in to vulnerability feeds)

A common conversation in XIoT security…

IT department: I have no idea what XIoT assets are out there!

Site Lead: I know exactly what's there, but I don't write it down.

Security department: (To site lead) Here's a platform where you can write it down.

Site Lead: I don't have time for that.

Security department: I guess we're on our own. ☹

Challenges with securing IoT devices

Decentralization

- Every site has their own IoT asset inventory
- Some sites have *multiple* asset inventories that include IoT devices

No enterprise security tool coverage

- No SCCM, Intune, etc.
- Sometimes security tool coverage exists but is limited

Network traffic looks different from IT

- Takes time to baseline and find signal in the noise

Some critical networks are unknown (or easily missed)

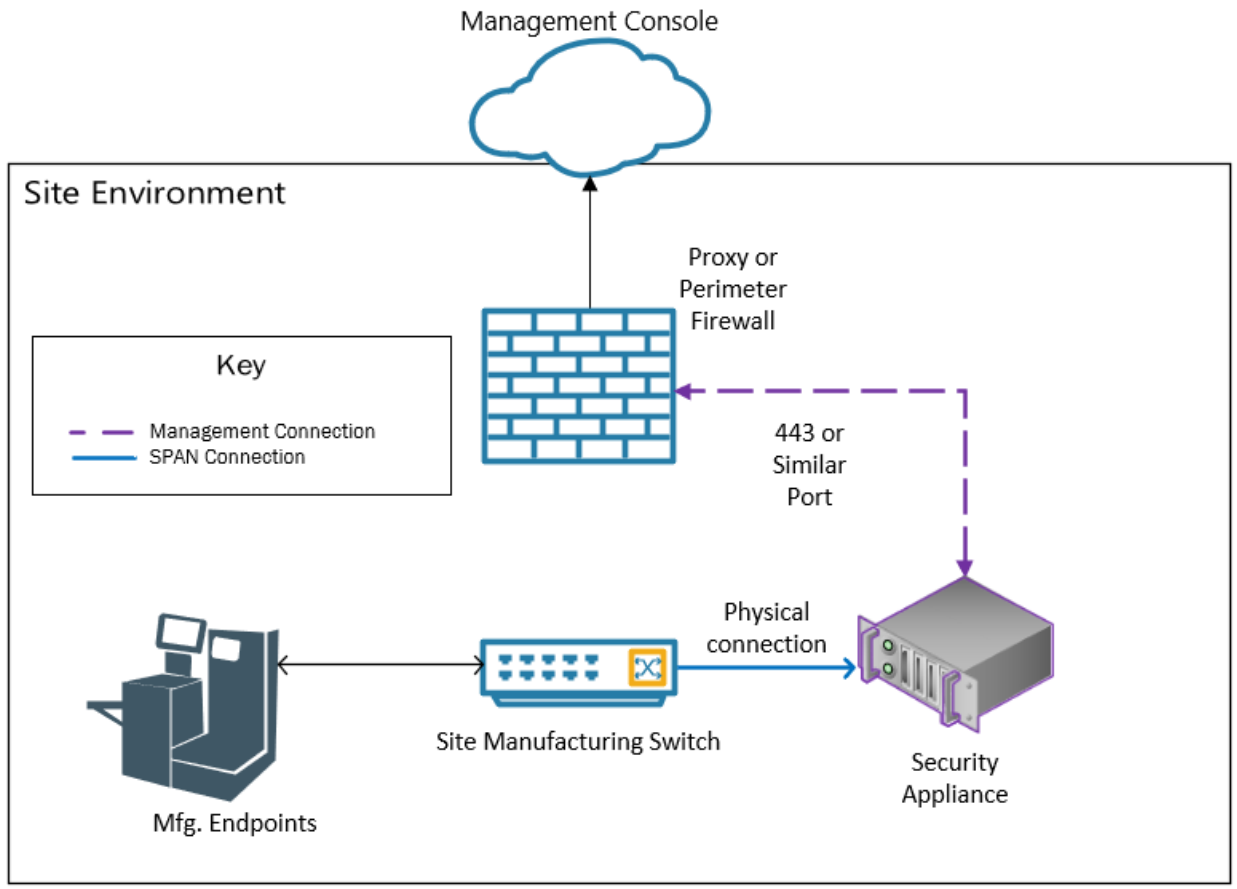
- After conversations with site personnel, the team will learn about different appliances or rooms that were previously unknown

No incentive to work on security issues

- Site IT folks do not have time devoted/budgeted for security

Defensive Tooling

- Lots of vendors moving into this space (lots of VC money)
- Common features:
  - Sensors on-prem, management console SaaS
  - Integrations with firewalls/security tools
  - Traffic analysis
  - OT, Healthcare, and XIoT device identification
  - Some vulnerability management
- Strengths:
  - Passive monitoring, no interruptions to XIoT devices
  - Quick time-to-value
- Weaknesses:
  - Hard to “master”
  - Deploying correctly takes *lots* of time and effort



Example of a deployment in a manufacturing environment

What do the Frameworks say?

New frameworks emerging every day, here are some that we looked at:

- NIST SP 1800-32A: Securing the Industrial Internet of Things
- Industry IoT Consortium Security Maturity Model and Security Framework
- IoT security institute smart cities & critical infrastructure framework

Some highlights:

- Authentication and Access Control
  - Every framework mentioned this early and often, both network and identity auth are options
- Behavioral Monitoring
  - Not monitoring people, looking for deviations in normal machine operations
- Log of Commands/Events
  - You should be logging important commands and events from IIoT devices, this record should be immutable
- Protection of Data
  - Includes both in transit and at rest
  - Data integrity (i.e., firmware)
- Response Plan
  - Plans should be routinely reviewed and tested

Conclusions in Practice

- Build strong relationships with site personnel
  - No security control will be effective without a partnership
- Access Control
  - Site personnel do not want this, requires strong relationships
- Gain visibility into IoT devices on your network using a centralized tool
  - Agents most likely not available for IoT devices
- Log as much as you can in a third-party platform
  - Expand collection of log sources
- Build and test a response plan
  - TTXs using IIoT scenarios are a great place to start