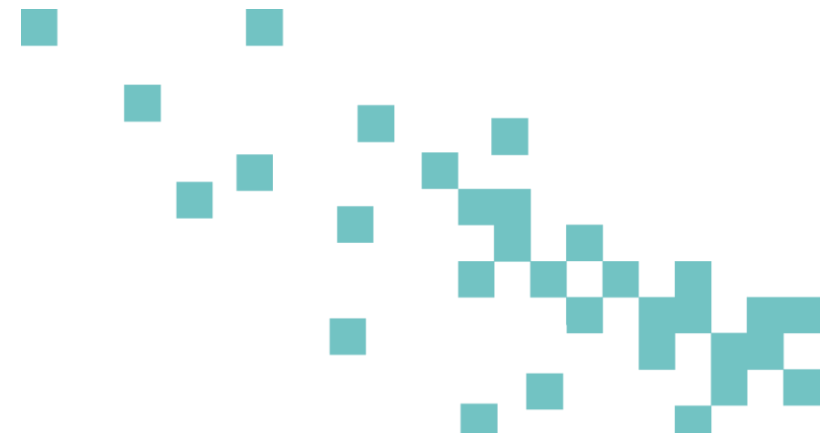
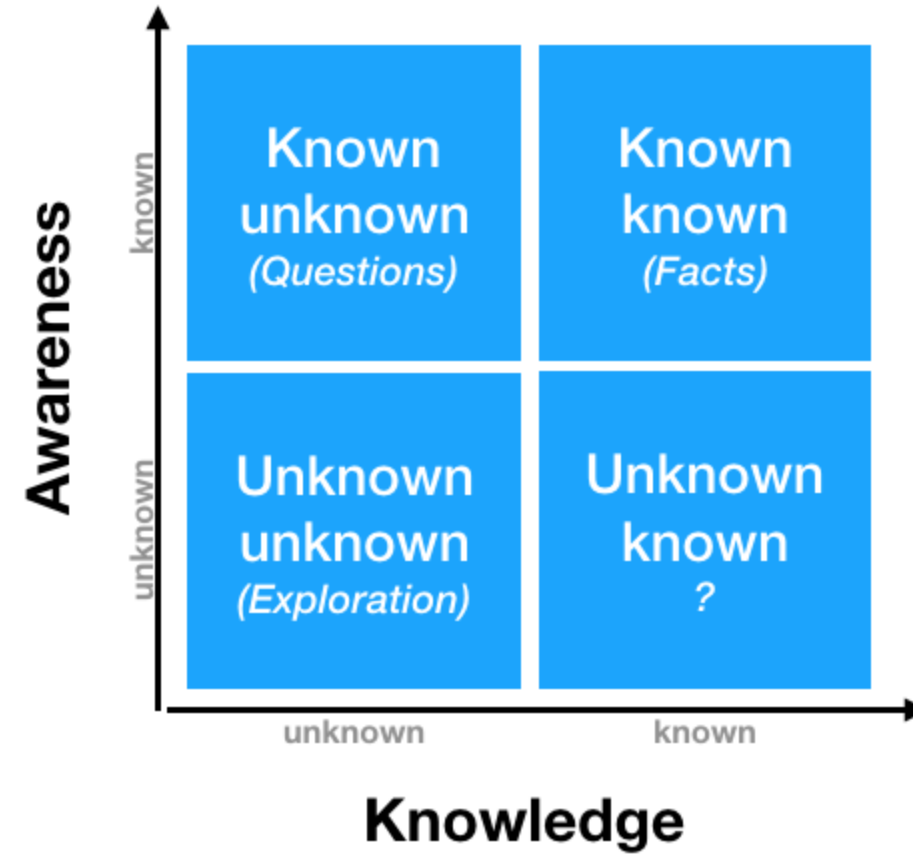


# Secure Connected Assets

Adrian Byrne CIO  
University Hospital Southampton





# Every Connected Device



## See every single asset

We need to see every single device in our environment regardless of location and type



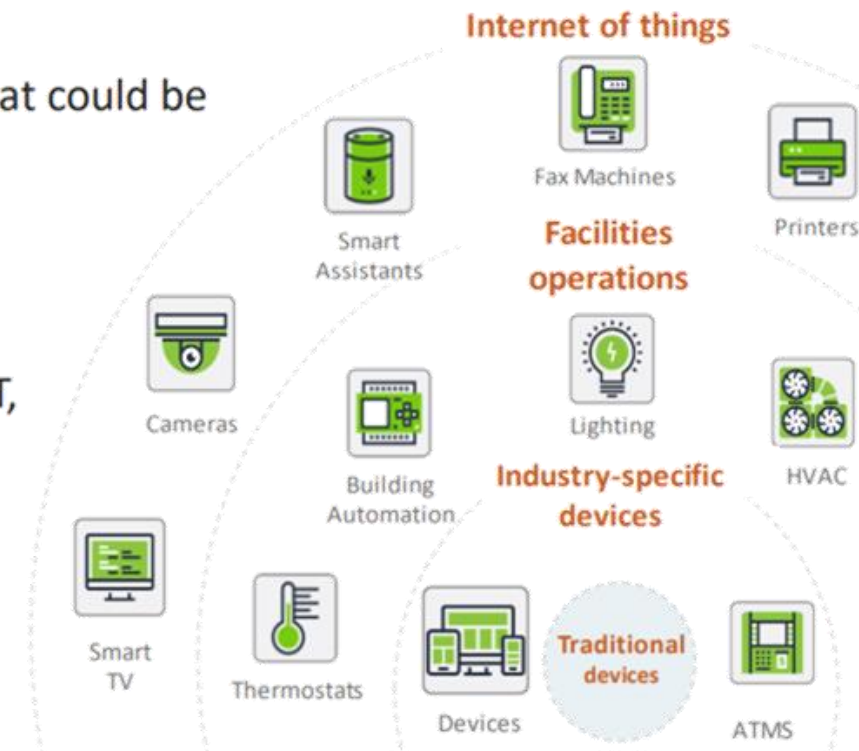
## Know vulnerabilities

We need to know if these devices have a vulnerability that could be exploited







## Map our estate to DSPT

Understand how are estate maps to all parts of the DSPT, Even legacy Operating Systems



Proprietary and Confidential

# How many devices !

					
	Workstations	Office	Facility	IoT	Medical
Total	15,711	3,795	565	8,476	1,384
Incidents	8,347	153	73	337	508
Vulnerabilities	15,327	1,118	226	2,971	1,021

*What sort of information do we really see for these devices?*

# What do we know about them?

## DEVICE INFORMATION

Mac Address : 00:80:92:6A:D0:F7  
 Business Function 1 :  
 Business Function 2 :  
 Business Function 3 :  
 Device Description : Glucose Monitor  
 Manufacturer : Abbott  
 Model Name/No. : Precision Pro  
 Serial No. : KDAA282-A0101  
 OS Type : Mac OS X  
 FQDN : dhcpclient.suhtad.suht.swest.nhs.uk  
 IP Binding Source : TOPOLOGY  
 DHCP :  
 DHCP Hostname : DHCPCLIENT  
 Has PHI : Yes  
 Vertical-Specific Protoc Abbott-Precision

What is it?



How is it connected

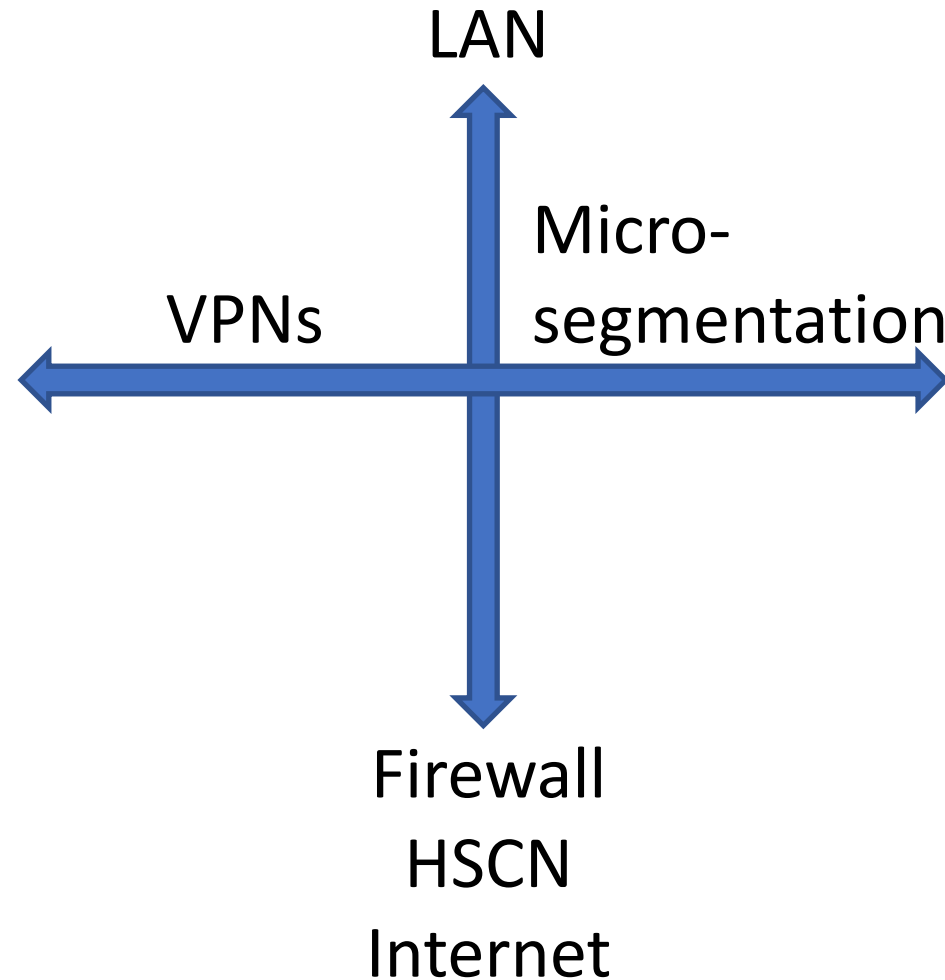
## CONNECTIVITY

SCE Sensor : ordr-main-sensor  
 IP Address : Offline (last IP = 172.22.160.17) [DHCP]  
 Subnet : 172.22.160.0/19  
 VLAN : VLAN0303(303)  
 Access Type : WIRELESS  
 Network Device : 172.22.0.22 (RHMARUBAMC\_NW)  
 WLAN SSID : UHSFTcorp  
 WLAN AP : uhs-nw-c-4.suhtad.suht.swest.nhs.uk  
 First Seen : 26/07/2022 08:48:38  
 Last Seen : 02/02/2023 22:59:00  
 Region/Location : ICU-MAIN | ICU-MAIN  
 Nw Location :

# North and South - East and West

Some have “flat” VPN  
Across a whole site/org

One of UHS suppliers was  
Insisting on a flat VLAN



# See every asset

## We have about 100 cameras on the network



Just  
firmware?

Dashboard Device Security Network

Devices Device Users Limited Visibility Utilization Utilization Schedule

### Device List

Total 113 Devices match 1 filter

hikvision Filter Saved Queries

Clear all criteria Any visible field has substring of 'hikvision' ...

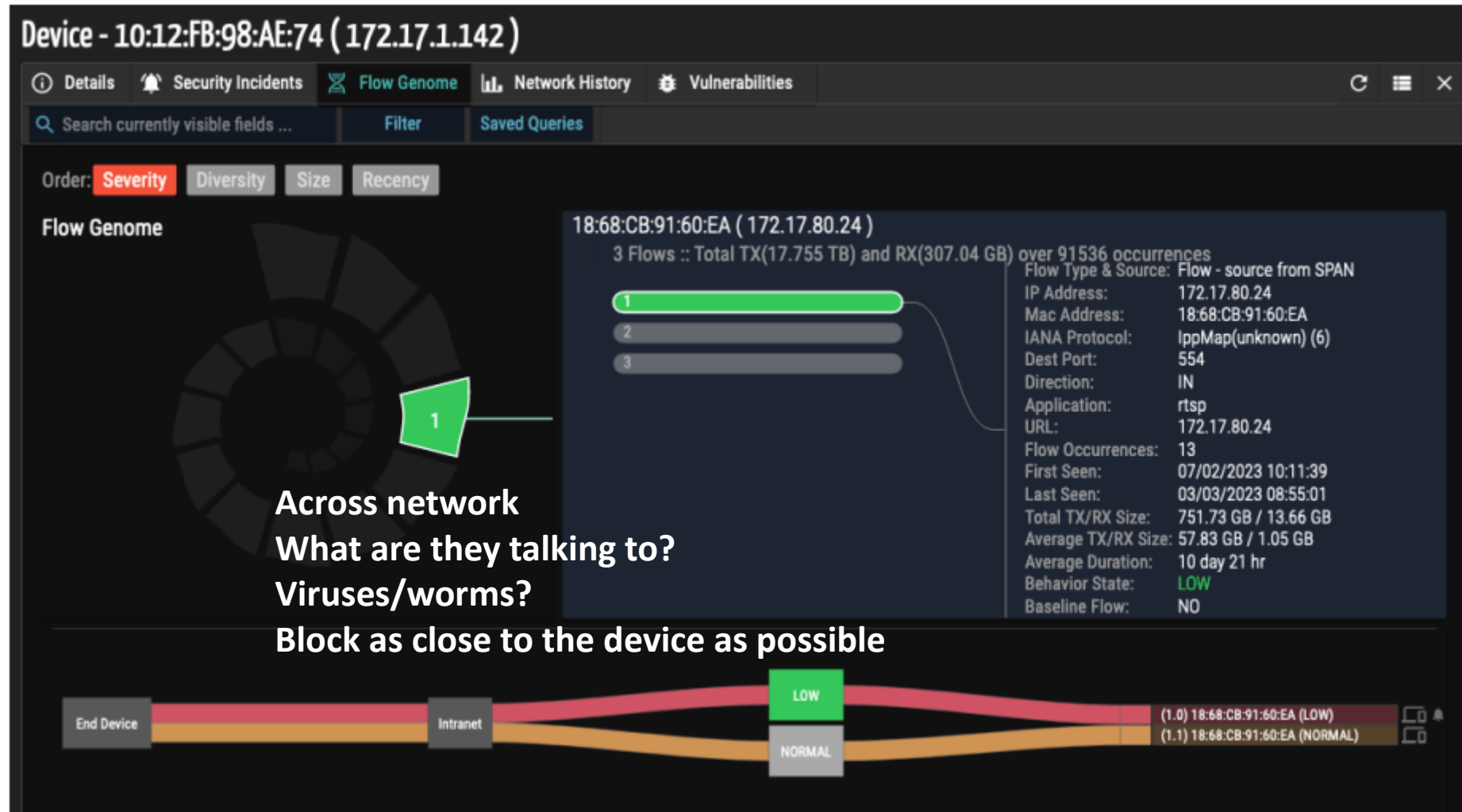
No.	Risk	Device Name	IP Address	Device
1	low	10:12:FB:98:AE:74	172.17.1.142	Network Camera
2	normal	10:12:FB:98:AF:18	172.17.1.144	Network Camera
3	low	18:68:CB:0F:F4:60	172.17.10.151	Network Camera
4	normal	18:68:CB:72:96:F5	192.168.1.103	Network Camera
5	normal	18:68:CB:72:96:FE	192.168.1.104	Network Camera
6	low	18:68:CB:72:97:05	192.168.1.101	Network Camera
7	normal	18:68:CB:72:97:0A	192.168.1.102	Network Camera
8	low	18:68:CB:85:2A:1A	172.17.10.152	Network Camera
9	low	18:68:CB:89:62:8A	172.17.10.153	Network Camera
10	low	18:68:CB:8A:10:D2	172.17.10.154	Network Camera
11	normal	18:68:CB:8A:10:D3	172.17.10.155	Network Camera
12	low	18:68:CB:91:60:EA	172.17.10.156	NVR
13	low	18:68:CB:92:7F:8E	172.17.10.157	NVR
14	low	28:57:BE:51:EC:C5	172.17.95.88	Network Camera

What VLAN's and Subnets are these in?

VLAN	Count	Subnet	Count
MED-VLAN-09(9)	1	13.80.0.0/24	1
SEC-CCTV-13(13)	1	13.83.0.0/24	1
SERVICES-VLAN(9)	6	13.84.0.0/24	1
SGH-10-SERVICES(9)	2	172.17.1.128/25	6
SGH-NWLE-84-SECURITY(11)	1	172.17.10.128/25	2
SRV-VLAN-09(9)	2	172.17.104.128/25	2
SVC-VLAN-08(8)	59	172.17.11.128/25	2
SVC-VLAN-09(9)	6	172.17.12.128/25	1
SVC-VLAN-10(10)	2	172.17.14.0/25	2

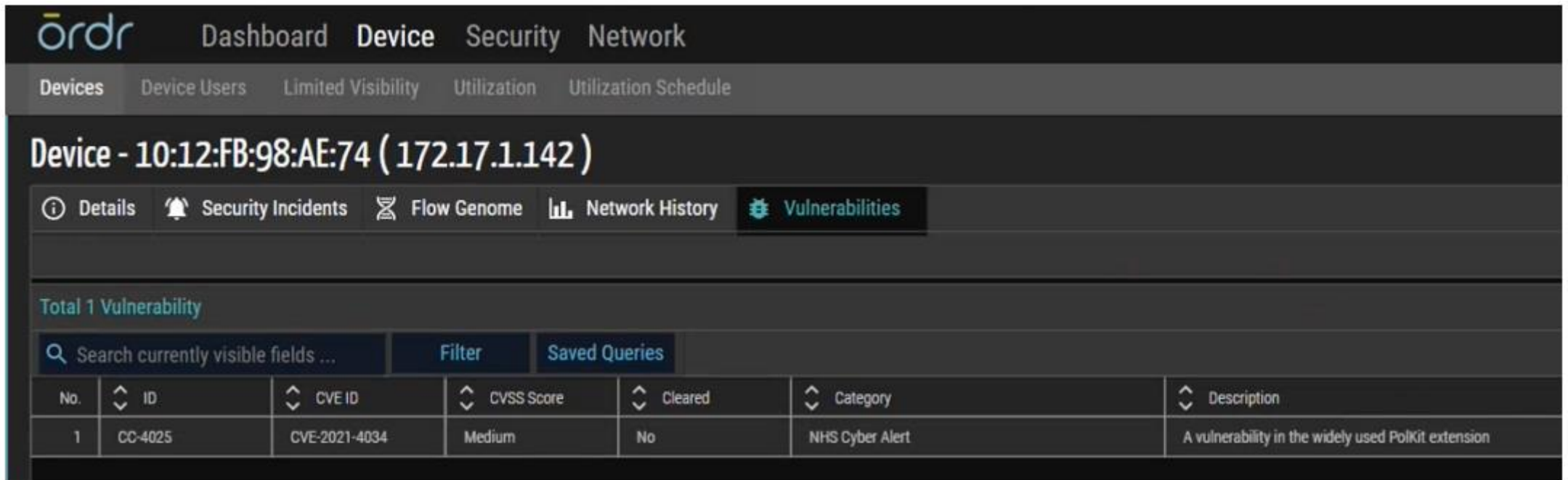
What else is in this vlan?

# Identify anomalous behaviour



# Are there any known vulnerabilities

Or known NHS cyber alerts applicable to any device?



Dashboard Device Security Network

Devices Device Users Limited Visibility Utilization Utilization Schedule

Device - 10:12:FB:98:AE:74 ( 172.17.1.142 )

Details Security Incidents Flow Genome Network History **Vulnerabilities**

Total 1 Vulnerability

Search currently visible fields ... Filter Saved Queries

No.	ID	CVE ID	CVSS Score	Cleared	Category	Description
1	CC-4025	CVE-2021-4034	Medium	No	NHS Cyber Alert	A vulnerability in the widely used PolKit extension

# Unsupported operating systems?

All Outdated OS Alarms Vulnerability List as of 03/03

Total 15 entries when expanded per device

Search currently visible fields ... Filter Saved Queries

No.	ID	CVE ID	Severity	Cleared	Category	Description	IP Address	Device Type	Device Profile	Info	Actions
1			LOW	No	Outdated OS	Outdated OS in use - Windows XP	172.16.1.31	Workstation	DFI-Workstation		
2			LOW	No	Outdated OS	Outdated OS in use - Windows XP	10.168.227.232	Nuclear Medical	GE-Xeleris-Nuclear Medical		
3											
4											
5			LOW	No	Outdated OS	Outdated OS in use - Windows XP					
6			LOW	No	Outdated OS	Outdated OS in use - Windows XP					
7											
8			LOW	No	Outdated OS	Outdated OS in use - Windows XP		Ultrasound	GE-Vivid S6-Ultrasound		
9			LOW	No	Outdated OS	Outdated OS in use - Windows XP		Server	Supramicro-Server		
10			LOW	No	Outdated OS	Outdated OS in use - Windows XP	10.168.223.125	X-ray Angiograph	Siemens-Axiom-Artis-X-ray		
11			LOW	No	Outdated OS	Outdated OS in use - Windows XP		Carescape Centi	GE-MP100-Carescape Centi		
12			LOW	No	Outdated OS	Outdated OS in use - Windows XP	192.168.122.31	Carescape Centi	GE-Carescape Central Stati		
13			LOW	No	Outdated OS	Outdated OS in use - Windows XP	172.17.81.30	Carescape Centi	GE-MP100-Carescape Centi		
14			LOW	No	Outdated OS	Outdated OS in use - Windows XP	172.17.82.5	Carescape Centi	GE-MP100-Carescape Centi		

# Medical Devices



**450 equipment types**

**Around 11-15 are considered connectable to EPR  
(ECGs, Scanners etc)**

**Currently about 5% blood glucose tests cannot be tracked  
as just taken as “stat”**

# Medical Devices - Patching



Medicines & Healthcare products  
Regulatory Agency



**You can't just patch them under normal policy**

**MHRA locks down versions with accreditation**



# Medical Devices - Interfacing



**Interfacing gives you bidirectional  
Demographics ↔ Results**

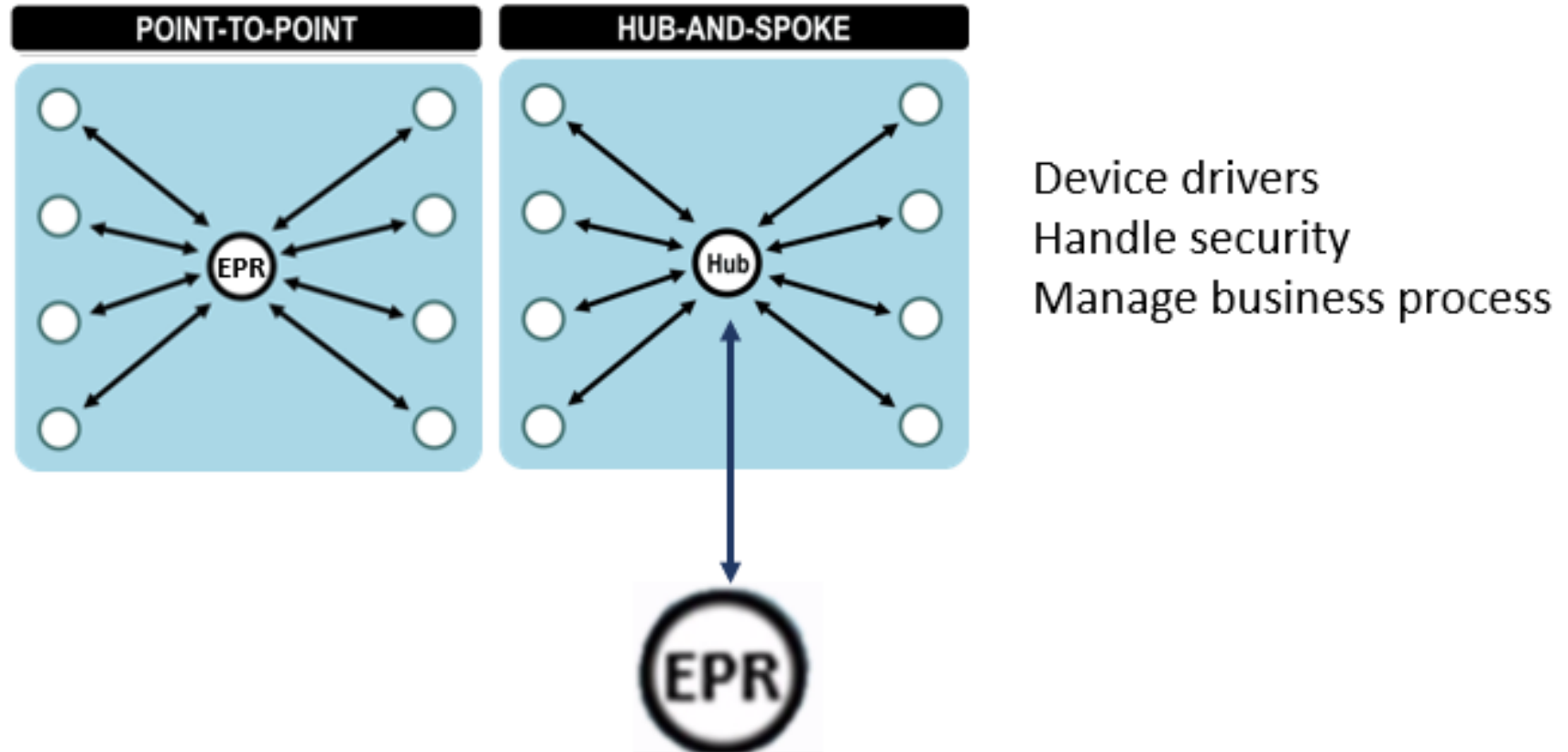
**2D barcode gives you off line capability**



**Can link to a staff ID also – e.g. badge scan**



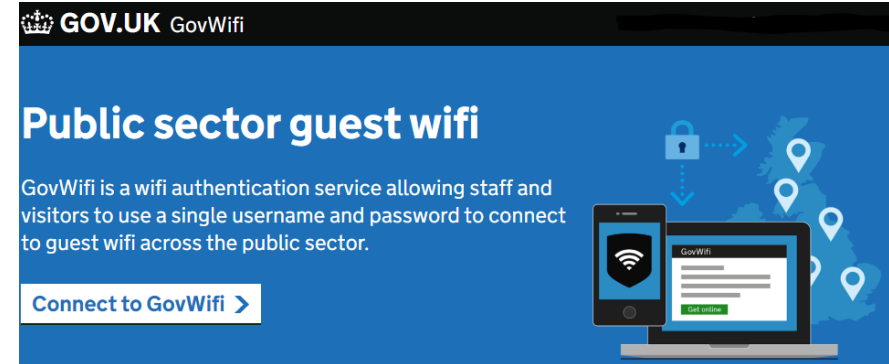
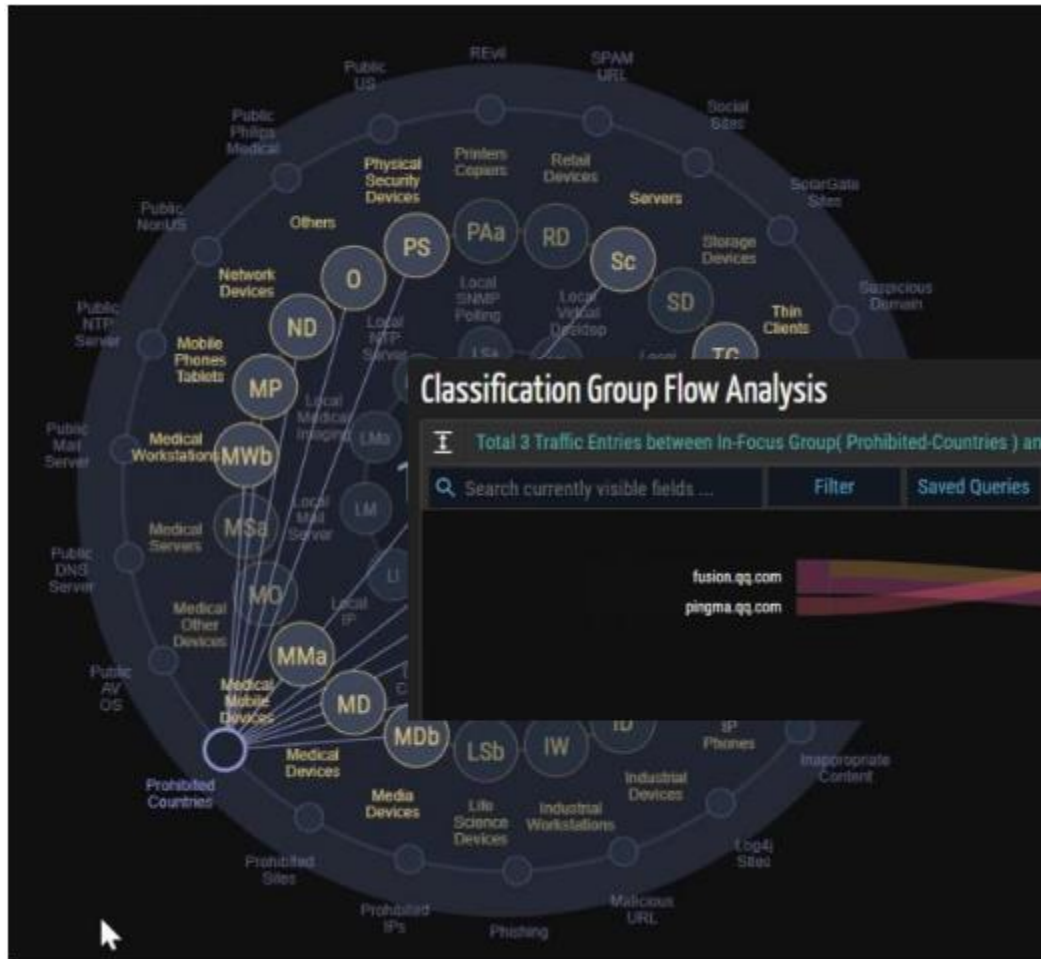
# Interfacing hubs



## Three key areas in connectivity

- Process/culture
- Governance
- Technical and management

# Who are they communicating with ?



# Thank You

Adrian Byrne CIO  
@adebyrne @UHSDigital

