#### FSI ITAM & Security Challenges Innovative Hardware Asset Risk Management

Presented By

## SEPI©



Ó

#### Questions our FSI customers ask themselves -

- Are all my assets listed?
- Where are my assets located?
- Are there any vulnerable assets that put us at risk?
  - Are my assets verified, and can I trust them?
    - Where are my regulatory compliance gaps?



### Hardware assets pose major security concerns



Visibility and validation of **all Hardware Assets** including:

- O Peripheral devices
- (MAC-less devices)
- Hardware BOM



2

Hardware Zero Trust Control access to the enterprise through granular policy enforcement & hardware identity validation



3

Rogue Device Mitigation (RDM) of spoofed, manipulated devices, and hidden implants





#### Detection of Hardware Manipulation within the supply chain



## Hardware attack tools are gaining popularity

- O Every physical asset is an exposure
- Uncontrolled assets are an entry point for malware/ransomware payloads
- Uncontrolled assets are an exit door for sensitive data leakage
- Uncontrolled asset provide a permanent foothold for threat actors in the organization: MiTM, Data manipulation etc.













#### Demonstrated value to IT operation

- Existing CMDB, CMMS and NAC performance boost ~~~~
  - Visibility across inventory, shadow and rogue assets

(0)

Reduced hardware clutter and better budget spending



Uninterrupted streamlined operations





## **Attack study**



### ATM use case: FiXS The new ATM malware in LATAM



Sepio detects the disguised keyboard & blocks it at connection. Stops the execution before it starts.



### USB use case: Bypassing biometric security measures



Palm vein scanner connected over USB



Beaglebone low-cost board running USB Proxy MiTM.





High privilege user endpoint



### Network use case: MiTM transparent attack



First entry point



## Peripheral asset attacks

Way In



0x8A,0xC6,0x22,... http://URL... cmd /c netsh wlan show profiles "+NetName+"...



Depending on attacker's "style" and prior knowledge of the target, they will either:

- O Use HID emulation for binary payload
- "Send" the target PC to a pre-known/prepared web URL  $\bigcirc$ to download the payload
- Act as a Network Interface and inject the payload into the  $\bigcirc$ PC
- Use USB Proxy MiTM attacks  $\bigcirc$

#### Way Out



- Use an integrated Wi-Fi to remotely extract  $\bigcirc$
- Connect to the internet and exfiltrate the data  $\bigcirc$ 
  - "invisibly" such as adding comments on youtube
- Use continuous and invisible remote shell into  $\bigcirc$ corporate PCs







Exfiltrate the data directly to the attack tool



## Network asset – MiTM & 802.1xbypassing

- Unmanaged switch & uncontrolled (MiTM) hardware  $\bigcirc$ are completely invisible to NAC and IDS/IPS
- Any device that is connected poses a risk- $\bigcirc$ 
  - Spoof to be a legitimate device and send traffic into the network
  - Intercept/manipulate traffic between a legitimate asset and the network
  - Invisibly infect/attack a legitimate asset without being flagged
  - Create as invisible and continuous foothold in the infrastructure







#### Unmanaged switch



## Avoiding existing technologies blind spots



## Friend or Foe?







## **Same MAC**



#### MAC:00D085045802





#### MAC:00D085045802



## **Same Ports**

Ē



Sc <u>a</u> n <u>T</u> ools <u>P</u> rofile <u>H</u> el			
arget: 192.168.10.46	V Profile: Intense scan	<ul> <li>✓ Scan</li> </ul>	Cancel
ommand: nmap -T4 -A -	v 192.168.10.46		
Hosts Services	Nmap Output Ports / Hosts Topology Host Details Scans		
S 4 Host 🔺	nmap -T4 -A -v 192.168.10.46	~ =	Details
	<pre>Initiating NSE at 10:15 Completed NSE at 10:15, 0.00s elapsed Initiating ARP Ping Scan at 10:15 Scanning 192.168.10.46 [1 port] Completed ARP Ping Scan at 10:15, 0.25s elapsed (1 total hosts) Initiating Parallel DNS resolution of 1 host. at 10:15 Completed Parallel DNS resolution of 1 host. at 10:15, 0.07s elaps Initiating SYN Stealth Scan at 10:15 Scanning 192.168.10.46 [1000 ports] Discovered open port 443/tcp on 192.168.10.46 Discovered open port 631/tcp on 192.168.10.46 Discovered open port 515/tcp on 192.168.10.46 Completed SYN Stealth Scan at 10:15, 1.76s elapsed (1000 total por Initiating Service scan at 10:15</pre>	sed rts)	



Versee		
117		2
100	1	
1940		
100	1	1

		<u> 27 - 12</u>		$\mathbf{\vee}$
				$\wedge$
file	Intense scan	~	Scan	Cancel
inc.	interise sean		Con	concer
Ho	ost Details Scans			
			=	Detaile
			=	Derails
map:	org ) at 2023-04-18 10:15 Jerusal	em Dayligh	t Time	
anni	ng.			
elap	sed			
-1				
elap	sed			
elap	sed			
:15				
]				
15, tion	0.25s elapsed (1 total hosts)			
ion	of 1 host. at 10:15, 0.07s elapse	d		
10:	15			
orts	3			
n 19	2.168.10.46			
192	.168.10.46			
on 1	92.168.10.46			
n 19	2.168.10.46			
10:1	5, 1.76s elapsed (1000 total port	s)		
15				



## **Same Traffic**



0					Traffic Log -	Network Threat Prot	ection Logs				12
File Edit View Filter	Action He	þ									
Date and	Action	Severity	Direction	Protocol	Source Nost	Source MAC	Source Port	Destination Nost	Destination NAC	Destination Port	Applic A
22/11/2013 8:07	Allowed	5	Incoming	TOP	192.140.0.55	7C-05-07-91-D	5353	224.0.0.251	01-00-58-00+0	\$353	
22/11/2018 8:07	Allowed	5	Incoming	TCP	192.148.0.111	A0-83-CC-4E-C	52614	216.2.40.149	00-09-08-09-0	80	D:\Pro
22/11/2013 8:08	Allowed	5	Incoming	105	192.168.0.55	70-08-07-91-0	1900	239.255.255.250	01-00-58-78-6	1900	
22/11/2013 8:08	Allowed	5	Incoming	TCP	192.148.0.70	00-50-56-86-7	58498	192.148.0.117	00-00-29-99-9	443	D:\Pro
22/11/2013 8:08	Allowed.	5	Incoming	009	192.148.0.56	00-07-FE-F9-5	137	192.140.0.127	11-11-11-11-11-1	137	C:\Win
22/11/2015 8:08	Allowed	5	Incoming	909	192.148.0.63	00-07-76-70-0	137	192.148.0.127	tt-tt-tt-tt-tt-t	137	C:\Win
22/11/2013 8:08	Allowed	5	Incoming	105	192.168.0.111	A0-83-CC-48-C	32015	216.2.40.149	00-09-07-09-0	80	D:\Pro
22/11/2013 8:08	Allowed	5	Incoming	TCP	192.148.0.111	A0-83-CC-4E-C	52816	216.2.48.149	00-09-07-09-0	80	D:\Pro
22/11/2013 8:08	Allowed	5	Outgoing	ICP	192.148.0.117	00-00-29-99-9	62301	192.168.0.110	00-0C-29-2E-4	8016	C:\Win
O22/11/2015 8:08	Allowed	5	Incoming	TCP	192.148.0.111	A0-83-CC-4E-C	52617	214.2.48.149	00-09-08-09-0	80	D:\Pro
222/11/2015 8:08	Allowed		Incoming	TCP	193.148.0.111	30-83-CC-4E-C	52515	214.2.48.149	00-09-07-09-0	20	Dr\Pre
22/11/2013 8:08	Allowed	5	Incoming	000	192.168.0.51	84-85-27-17-B	50144	239.235.255.250	01-00-58-78-8	1900	1000
22/11/2013 8:08	Allowed	5	Incoming	UDP	192.148.0.57	00-23-18-C3-F	137	192.168.0.127	TT-TT-TT-TT-T	137	C:\Win
22/11/2010 8:06	Allowed	5	Incoming	009	192.168.0.57	00-23-18-C3-F	60248	224.0.0.252	01-00-58-00-0	\$355	C:\Win
22/11/2013 8:08	Allowed	5	Incoming	19	192.168.0.55	7C-03-07-91-D	NA	224.0.0.22	01-00-58-00-0	834	
22/11/2013 8:08	Allowed	5	Incoming	909	192.148.0.55	70-05-07-91-0	51452	224.0.0.252	01-00-58-00-0	\$355	C:\Win
22/11/2013 8:08	Allowed	5	Incoming	TCP	192.148.0.111	A0-83-CC-4E-C	52519	216.2.48.149	00-09-07-09-0	80	D:\Pro
22/11/2015 8:08	Allowed	5	Incoming	TCP	192.148.0.111	A0-83-CC-4E-C	52820	216.2.40.149	00-09-07-09-0	80	D:\Pro
22/11/2013 8:08	Allowed	5	Incoming	TCP	192.148.0.111	A0-83-CC-48-C	52021	216.2.48.149	00-09-07-09-0	80	D:\Pro
22/11/2013 8:08	Allowed	5	Incoming	TCP	192.148.0.111	A0-83-CC-4E-C	52822	216.2.48.149	00-09-07-09-0	80	D:\Pro
£22/11/2013 8:08	Allowed	5	Outgoing	ICP	192.148.0.117	00-00-29-99-9	42303	192.165.0.110	00-0C-29-2E-4	8016	C:\Win
22/11/2013 8:06	Allowed	5	Incoming	109	192.148.0.111	A0-83-CC-4E-C	52824	216.2.48.149	00-09-08-09-0	50	D:\Pro
€22/11/2013 8:09	Allowed	5	Outgoing	TCP	192.168.0.117	00-00-29-99-9	42304	192.148.0.110	00-00-29-28-4	8014	C:\Win
22/11/2013 8:09	Allowed	5	Incoming	TCP	192.148.0.111	A0-83-CC-4E-C	52525	216.2.48.149	00-09-05-09-0	80	D:\Pro
22/11/2013 8:09	Allowed	5	Incoming	ICP	192.148.0.111	A0-83-CC-48-C	52026	216.2.48.149	00-09-07-09-0	80	D:\Pro
O22/11/2015 8:09	Allowed	5	Incoming	17	192.148.0.64	E0-69-95-FA-3	NR.	224.0.0.22	01-00-58-00-0	NA	
22/11/2013 8:09	Allowed	5	Incoming	909	182.168.0.64	E0-69-95-FA-3	52124	224.0.0.252	01-00-58-00-0	5355	C:\Win
22/11/2013 B:09	Allowed	5	Incoming	TOP	192.148.2.64	E0-69-93-FA-3	137	192.148.0.127	TT-TT-TT-TT-T	137	C:\Winv
			and the second second		Constanting of the second second						

V					tranic Log - I	NC.
File Edit View Filte	Action He	φ				
Date and	Action	Severity	Direction	Protocol	Source Nost	T
22/11/2013 8:07.	Allowed	5	Incoming	009	192.148.0.55	
O22/11/2015 8:07.	Allowed	5	Incoming	TCP	192.148.0.111	
22/11/2013 8:08.	Allowed	5	Incoming	105	192.168.0.55	
22/11/2013 8:08.	Allowed	5	Incoming	TCP	192.148.0.70	
O22/11/2013 8:08.	Allowed.	5	Incoming	009	192.148.0.56	
O22/11/2015 8:08.	Allowed	5	Incoming	009	192.168.0.63	
22/11/2013 8:08.	Allowed	5	Incoming	105	192.168.0.111	
22/11/2013 8:08.	Allowed	5	Incoming	TCP	192.148.0.111	
22/11/2013 8:08.	Allowed	5	Outgoing	ICP	192.148.0.117	
22/11/2013 8:08.	Allowed	5	Incoming	TCP	192.148.0.111	
Oza/11/2013 8:08.	Allowed	1	Inconing	322	183.148.0.111	
22/11/2013 8:08.	Allowed	5	Incoming	900	192.148.0.51	
O22/11/2013 8:08.	Allowed.	5	Incoming	UDP	192.148.0.57	
22/11/2013 8:06.	Allowed	5	Incoming	009	192.148.0.57	
22/11/2013 8:08.	Allowed	5	Incoming	19	192.168.0.55	
O22/11/2013 8:08.	Allowed	5	Incoming	909	192.148.0.55	
O22/11/2013 8:08.	Allowed	5	Incoming	ICP	192.148.0.111	
O22/11/2013 8:08.	Allowed	5	Incoming	TCP	192.148.0.111	
22/11/2013 8:08.	Allowed	5	Incoming	TCP	192.148.0.111	
22/11/2013 8:08.	Allowed	5	Incoming	TCP	192.148.0.111	
€22/11/2013 8:08.	Allowed.	5	Outgoing.	ICP	192.148.0.117	
22/11/2013 8:08.	Allowed	5	Incoming	ICP	192.148.0.111	
€22/11/2013 8:09.	Allowed	5	Outgoing	TCP	192.168.0.117	
O22/11/2013 8:09.	Allowed	5	Incoming	TCP	192.148.0.111	

192.148.0.111

192.148.0.64

192.168.0.64

192.148.0.64

Incoming TCP

Incoming IP

Incoming UCP

Incoming UDP

\$22/11/2013 8:09... Allowed 5

022/11/2013 8:09... Allowed 5

O22/11/2013 8:09... Allowed 5

O22/11/2013 8:09... Allowed 5



#### Traffic Log - Network Threat Protection Logs

83

ource MAC	Source Port	Destination Nost	Destination NAC	Destination Port	Applic A
C-05-07-91-D	5353	224.0.0.251	01-00-58-00+0	\$353	
0-83-00-48-0	52614	216.2.40.149	00-09-08-09-0	80	D:\Pro
C-08-07-91-D	1900	239.255.255.250	01-00-58-78-8	1900	
0-50-56-56-7	58498	192.148.0.117	00-00-29-99-9	443	D:\Pro
0-07-18-19-5	137	192.148.0.127	rr-rr-rr-rr-r	137	C:\Win
0-07-76-70-0	137	192.168.0.127	11-11-11-11-11-1	137	C:\Win
0-83-00-48-0	32015	216.2.40.149	00-09-07-09-0	80	D:\Pro
0-83-CC-48-C	52816	216.2.48.149	00-09-07-09-0	80	D:\Pro
0-00-29-99-9	62301	192.168.0.110	00-00-29-28-4	8016	C:\Win
0-83-CC-4E-C	52617	214.2.48.149	00-09-07-09-0	80	D:\Pro
0-83-00-48-0	52515	214.2.42.149	00-09-07-09-0	20	Dr\Pre
4-85-27-17-B	50144	239.255.255.250	01-00-58-78-8	1900	1000
0-23-18-03-1	137	192.148.0.127	TT-TT-TT-TT-T	137	C:\Win
0-23-18-C3-F	60248	224.0.0.252	01-00-58-00-0	\$355	C:\Win
C-05-07-91-D	NA	224.0.0.22	01-00-58-00-0	15A	
C-08-07-91-D	51452	224.0.0.252	01-00-58-00-0	\$355	C:\Win
0-83-CC-48-C	52519	216.2.48.149	00-09-07-09-0	80	D:\Pro
0-83-00-46-0	52820	216.2.40.149	00-09-08-09-0	80	D:\Pro
0-83-00-48-0	52021	216.2.48.149	00-09-07-09-0	80	D:\Pro
0-83-00-48-C	52522	216.2.48.149	00-09-05-09-0	80	D:\Pro
0-00-29-99-9	42303	192.168.0.110	00-0C-29-2E-4	8016	C:\Win
0-83-00-46-0	52824	216.2.40.149	00-09-08-08-0	50	D:\Pro
0-00-29-99-9	42304	192.148.0.110	00-00-29-28-4	8016	C:\Win
0-83-CC-48-C	52525	216.2.48.149	00-09-05-09-0	80	D:\Pro
0-83-CC-48-C	52826	216.2.48.149	00-09-07-09-0	80	D:\Pro
0-69-95-FA-3	NR.	224.0.0.22	01-00-58-00-0	NA	
0-69-95-72-3	52124	224.0.0.252	01-00-58-00-0	5355	C:\Win
0-69-93-FA-3	137	192.148.0.127	rr-rr-rr-r	137	C:\Win v
					,



## **Different Asset DNA!**









## Sepio's unique approach



## Harnessing new data source

getting to the true source of asset risk without traffic monitoring

Create an Asset DNA
 Dick accordent

O Risk assessment

O Asset mapping



## How do we do it?

# Asset DNA





#### Introducing Asset DNA





Ē







Asset DNA provides a single source of truth, focusing on EXISTENCE – rather than ACTIVITY.

With our patented technology, we now harness a new data source – physical layer to accurately identify and classify your assets.



# Passive network probingis an IT/OT nightmare

Sepio's trafficless solution avoids cumbersome deployments and privacy issues, vertical, type and protocol indifferent, at any scale, without effecting the network performance.





Sepio's enhanced visibility provides unmatched rogue device mitigation, while supporting USB entitlement at scale.







Embrace Sepio's Zero Trust Hardware Access (ZTHA) to augment your ZTNA initiatives across all your assets (|T/|OT/OT).Establish trust validate assets, enforce regulatory

compliance with a single low TCO solution.



## Sepio's proven value for FSI







## Finance **Business Benefits**

Sepio sheds light on items I couldn't identify and now I can make better decisions; I can contextualize what a device is where I wouldn't have had visibility otherwise. 55

Director of Network Architecture and Engineering, **Tier 1 Financial Institution** 

- Complete asset visibility

- Support regulatory compliance
- Budget and resource planning

Mitigate rogue devices and supply chain risks.

Close NAC gaps and fortify micro segmentation

Apply assets usage policy entitlement, at scale.



## Who benefits from our data?

#### SIEM/SOAR

- Instant alerts when unwanted or rogue devices are connected, eliminating unnecessary noise
- Contextual information, i.e. asset location, expedites response time to prevent crises
- Publicly recognized asset vulnerability module (OSINT and proprietary) for an immediate mitigation

#### **Security team**

- Understand what needs attention with actionable data
- Enforce organization policies and establish trust at the asset level
- Greater ROI by radically improving the efficacy of existing tools

#### **ITAM & CMDB**

- asset visibility across all environments
- Reduce hardware clutter
- Ensure operational efficiency of assets

#### CAASM

- Augment existing data sources
- Validate security controls
- Remediate issues

Reduce complexity with a consolidated source of



## **Architecture and Deployment aspects**





#### **Discover & Mitigate**

- O All connected assets
- O Asset vulnerabilities
- O Shadow IT
- Spoofed assets



### Sepio agent deployment options

Fixed agent (including VDI support)

- **Session based**
- Dissolvable agent



### Typical Customer Journey

Workshop with extended team

Identify key use cases – endpoint or network PoV – installs in hours; standard duration up to 2 weeks

Develop deployment and integration plan

Present business case for approval

SEPIC

## Deployment process

(1)	Install the software only Sepio	$\longrightarrow$ 2 Using the browser UI,	$\longrightarrow$ 3 Import switches/WLC to $\longrightarrow$	4 De
	Platform using preferred method	impo <mark>rt a license</mark>	Sepio	age
	Cloud, virtual, on-prem or via Azure marketplace		Can be done manually by providing IP-SSH username – SSH password	Sup
	·		Can be done by importing CSV file	Car dist
				-
			0.0 Notwork Infrastructure	

ූ <mark>ර</mark> ් 38,470	0 1,534	103	103	© 	988	0 482	Recent Visible Risks Assets (201) Hosts (103) Network (482)	
Assets Total	New Host	s Hosts	New	Network	Total	New	Leonardo (CDC ACM, HID) Arduino SA	
Assets Risk	Assets Distribution					Sort By: Asset Count 👻	ojo Integrated Camera P <sup>iii</sup> Chicony Electronics Co., Ltd	
	Host	Asset High Risk		18,762			VF55011 Fingerprint Reader Validity Sensors, Inc.	
0.0	lP Phone	37   13	6,885				big Integrated Camera B <sup>ig</sup> Chicony Electronics Co., Ltd	
High Medium	💮 IoT - Others	2,898 6					VF55011 Fingerprint Reader     Validity Sensors, Inc.	
	Access Point     Network Switch	16					VFS5011 Fingerprint Reader Validity Sensors, Inc.	
	⑦ Others	1,555					VFS5011 Fingerprint Reader     Validity Sensors. Inc.	
	Printer	<ul> <li>1.056</li> <li>1</li> <li>845</li> </ul>					VFS5011 Fingerprint Reader     Validity Sensors, Inc.	
()	Router	[6 ● 508 [1					VFS5011 Fingerprint Reader Validity Sensors, Inc.	
37,214	ToT - Healthcare	• 583 1					VFS5011 Fingerprint Reader     Validity Sensors, Inc.	
	이 IoT - Building Managemer g <sup>rd</sup> Composite Device	1 273					pre Integrated Camera B <sup>10</sup> Chicony Electronics Co., Ltd	
	1 USB Hub	I 109					VFS5011 Fingerprint Reader	

Recover	innuscruceure									
Cat2910-2 (19	(2.168.100.21)	-	200	م م م			n n n n n n n n n n n n n n n n n n n			
<ul> <li>Risk Indicator</li> </ul>	s (1)									
No Risk Indicators	Actions	2	2)(5							
<ul> <li>General Detail</li> </ul>	6	100	_							
Status	Connected	Detecte	ed De	evices					×	
Group	Network Infrastructure Default	-								Risk
Location Scan Priority	Manual Only	۲	Sw	vitch Cat2910	2			O Accep	ot Risk Ø Block Port	
Active Ports Total Ports	2									
Vendor	Cisco		MAC			Asset	Vendor	Туре	Risk ¥	
Last Seen	2023-01-15 14:45:58	86	B8:27	EB:83:CB:AD		Raspberry Pi	Raspberry Pi Foundation	Raspberry Pi	()	
Last Updated	2023-01-15 14:45:58	(000)	E8:BA	70:0B:50:40		Communication - C3750C Switch	Cisco Systems	Network Switch		
<ul> <li>Asset Details</li> </ul>								in the second second		
Policy	Default	(22.2.2)	F8:7A	541540:01:647		Communication - C9200 Switch	Cisco Systems	Network Switch		
Pomain Model	112		40:A6	:E8:55:00:C0		Communication - C2960X Switch	Cisco Systems	Network Switch		
Host MAC Address	192.168.100.21 D4:D7:48:EB:5C:00	0000	04:EB	3:40:8F:1D:07		Communication - C2960L Switch	Cisco Systems	Network Switch	۲	
Software Boot Info	12.2(50)SE5 C2960-HBOOT-M12.2(44)SE5 fc1		64:51:	06:41:A2:AB		PC	HP Inc.	Host	(6)	
Version ID	V10 C2060-LANBASEK9-M		54:E1:	AD:08:FF:41		PC	Lenovo Group Ltd.	Host	(8)	
Serial Number	FCQ1544X0M4	0000	04:2A	E2:D3:1A:80		sepio-2960-x (192.168.100.29)	Cisco	Network Switch		
CPU Environment	(PowerPC405) processor (revision T0) with 65536K bytes									
Transport	SSH	0000	00:51	:86:A6:50:80		Septo-2960k-v3 (192.168.100.26)	CISCO	NELWORK SWITCH		
				13	Fa0/13		0 Detected Devices			
				14	Fa0/14		0 Detected Devices			
				15	Fa0/15		0 Detected Devices			
			8	36	Fa0/06		0 Detected Devices			
					r-ofer					
			-		Court.		o Detected Devices			
			10	18	Fa0/18		0 Detected Devices			

#### eploy Sepio



Complete integration in

upstream systems

#### gents

pports Windows/RHEL/Debian

n be installed manually or using a stribution tool

## Sepio's Asset Risk Management solution

Ţ

$\bigcirc$	Visibility Overview					
Visibility Assets Visibility	<b>ුරු 93690</b> Assets Total	465 New Hosts	6510 26 Hosts New	(1)       Image: Ward of the second seco	© 439 <sub>New</sub>	Recent Visible Risks Assets (188) Hosts (8) Camera
Control Center	Online Assets Risk	Assets Distribution		523	Sort By: High Risk 👻	Hikvision Digital Technology Co. Ltd.     Gommunication - Switches     Extreme Networks
¥= Logs 랴 Settings	High	Printer	29 96 4			Communication - C3750X Switch Cisco Systems
	38	Host	59		6510	Communication - C9200 Switch Cisco Systems
	<i>.</i>	E Attack Tool	[1 [1 [1			CAC Card Reader Realtek Semiconductor Corp.
	Medium	🚔 Access Point	22			RTL8188EUS 802.11n Wireless Network Realtek Semiconductor Corp.
	1306	E Keyboard	• 9 • 0			Realtek Semiconductor Corp.      Keyboard K120     Looitech. Inc.
	Low	Storage	0   4   0			Integrated Camera Luxvisions Innotech Limited
	92384	JUSB Hub	• 10 •			Je Hub Terminus Technology Inc.
		(+) IOT - Healthcare	0			• Hub



#### Additional video resources

https://www.youtube.com/watch?v=vDTtbfXDwbc

https://www.youtube.com/watch?v=pLHliLh3njg&list=PLlhAGMBWwGmdl t7aRfTc0C07N\_1kA49p4&index=15

https://www.youtube.com/watch?v=GBqYnalOXBU&list=PLIhAGMBWwG mdlt7aRfTcOC07N 1kA49p4&index=20



## SEPI©

#### See what you've been missing.



Ó