# SEPI

#### Mitigating Cyber Physical Systems Risks

May 24



Questions our OT 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?

? Are all my assets listed?

Sepio provides a complete asset inventory of whatever is connected – internal components HW BOM, USB peripherals, wired and wireless Ethernet connected devices.

Easily integrated with CMDB solutions (e.g., ServiceNow).



? Where are my assets located?

Sepio provides asset location information based on their specific network switch, USB port location or slot within the endpoint. ? Are there any vulnerable assets that put us at risk?

Sepio's embedded, regularly updated, known-to-bevulnerable OSINT database provides an instant indication when an asset that might compromise the organization is connected. ? Are my assets verified and can I trust them?

Sepio's Zero Trust Hardware Access approach, where we validate the true identity of hardware assets before they can be trusted and granted access to the enterprise's resources, provides protection against spoofing or tapping devices. ? Where are my regulatory compliance gaps?

Sepio's granular ruleset-based policies ensure that regulatory compliance gaps are easily detected and reported.



"Nearly three-quarters (73%) admit that they only have strong awareness of less than 80% of all assets"

Seeing half of the picture is not enough!





SEPIO

# **CPS Visibility Challenges**



Active scanning → Potential impact on system responsiveness and availability.



Passive probing  $\rightarrow$  Poor visibility (50%-80%) due to encrypted traffic.



Dormant assets→ Become "invisible" – MAC'less

# **Current Mean-Time-To-Value Challenges**

# Extensive use of human resources



Complexity due to additional sensors



Cumbersome network configuration



# **CPS Security challenges**

# OBUILDING a complete asset inventory



Enforcing granular security controls



Fulfilling regulatory compliance



Avoiding performance degradation

SEPIC

# Friend or Foe?









Ę





#### 00-1c-06-00-bc-37

#### 00-1c-06-00-bc-37



# **Same Ports**



Target:	ools <u>P</u> rofile <u>H</u> e	-r	V Profile:	Intense scan	~	Scan	Cancel
Comma	nmap -T4 -A	-v 192.168.10.46					
Hosts	Services	Nmap Output Ports / H	osts Topology H	ost Details Scans			
OS ◀ H	ost 🔺	nmap -T4 -A -v 192.168.1	0.46			<	Details
		Initiating Parallel Completed Parallel Initiating SVN Stee Scanning 192.168.10 Discovered open por Discovered open por Discovered open por Discovered open por Discovered open por	0:15 :15, 0.00s ela 0:15 0:15 0:15 0:15 0:15 0:05 ela :15, 0.00s ela 0:15 0:15 0.00s ela 10:15 DNS resolution DNS resolution DNS resolution DNS resolution DNS resolution 0:46 [1000 port: 443/tcp on 19 t 631/tcp on 19 t 515/tcp on 11 th Scan at 10: :	0.25s elapsed (1 total ho n of 1 host. at 10:15 of 1 host. at 10:15, 0.07 15 5] 22.168.10.46 22.168.10.46 492.168.10.46	's elapsed		



👁 Zenmap	- 0	×
Sc <u>an T</u> ools <u>P</u> rofile <u>H</u> e Target: 192.168.10.46	Profile: Intense scan 🗸 Scan	Cancel
Command: nmap -T4 -A	-v 192.168.10.46	
Hosts Services	Nmap Output Ports / Hosts Topology Host Details Scans	
OS • Host	<pre>nmap -T4-A -v 192168.10.46</pre>	SEPI©

# **Same Traffic**



Traffic Log - Network Threat Protection Logs											
File Edit View Filter	Action He	e e									
Date and	Action	Severity	Direction	Protocol	Source Nost	Source HAC	Source Port	Destination Nost	Destination NAC	Destination Port	Applic .
22/11/2013 8:07	Allowed	5	Incoming	009	192.140.0.55	7C-05-07-91-D	5353	224.0.0.251	01-00-5g-00+0	5353	
O22/11/2015 8:07	Allowed	5	Incoming	TCP	192.148.0.111	A0-83-CC-48-C	52514	216.2.40.149	00-09-07-09-0	50	D:\Pro
22/11/2013 8:08	Allowed	5	Incoming	907	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	00-50-54-86-7	58498	192.160.0.117	00-00-29-99-9	443	D:\Pro
22/11/2013 8:08	Allowed.	5	Incoming	009	192.148.0.56	00-07-12-19-5	137	192.160.0.127	fr-fr-fr-fr-r	137	C:\Win
22/11/2013 8:08	Allowed	5	Incoming	009	192.140.0.63	00-07-75-70-0	137	192.168.0.127	11-11-11-11-11-1	137	C:\Win
22/11/2013 0:08	Allowed	5	Incoming	105	192.168.0.111	A0-83-00-48-0	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-48-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	192.160.0.110	00-0C-29-2E-4	8014	C:\Win
22/11/2013 8:08	Allowed	5	Incoming	TCP	192.148.0.111	A0-83-CC-48-C	52517	214.2.40.149	00-09-07-09-0	50	D:\Pro
Dzz/11/2013 8:08	Allowed	5	Inconstr	TCP	192.148.0.111	30-83-00-48-0	\$2515	214.2.42.149	00-09-07-09-0	29	Dr\Pro
22/11/2013 8:08	Allowed	5	Incoming	900	192.148.0.51	84-85-27-17-B	50144	239.235.255.250	01-00-5E-TF-F	1900	
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
22/11/2013 8:06	Allowed	5	Incoming	009	192.148.0.57	00-23-18-C3-F	60248	224.0.0.252	01-00-55-00-0	\$355	C:\Win
D22/11/2013 8:08	Allowed	5	Incoming	19	192.168.0.55	70-03-07-91-0	HA.	224.0.0.22	01-00-55-00-0	ITA .	
D22/11/2013 8:08	Allowed	5	Incoming	100	192.148.0.55	70-08-07-91-0	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-48-C	52519	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	52820	216.2.40.149	00-09-07-09-0	#0	D:\Pro
22/11/2013 8:08	Allowed	5	Incoming	TCP	192.168.0.111	A0-83-CC-48-C	\$2821	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-48-C	52522	216.2.48.149	00-09-07-09-0	=0	D:\Pro
B22/11/2013 8:08	Allowed.	5	Outgoing	ICP	192.148.0.117	00-00-29-99-9	42303	192.160.0.110	00-0C-29-2E-4	8016	C:\Win
22/11/2013 8:06	Allowed	5	Incoming	ICP	192.148.0.111	A0-83-CC-48-C	52824	216.2.48.149	00-09-08-09-0	50	D:\Pro
ezz/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	8016	C:\Win
22/11/2013 8:09	Allowed	5	Incoming	TCP	192.148.0.111	A0-83-CC-4E-C	32825	216.2.48.149	00-09-07-09-0	80	D:\Pro
D22/11/2013 8:09	Allowed	5	Incoming	ICP	192.148.0.111	A0-83-CC-48-C	52826	214.2.48.149	00-09-07-09-0	80	D:\Pro
D22/11/2015 8:09	Allowed	\$	Incoming	17	192.148.0.64	E0-69-95-FA-3	16A.	224.0.0.22	01-00-58-00-0	NA	
22/11/2013 8:09	Allowed	5	Incoming	907	182.168.0.64	E0-69-95-FA-3	52124	224.0.0.252	01-00-55-00-0	5355	C:\Win
D22/11/2013 8:09	Allowed	5	Incoming	UDP	192.148.0.64	E0-69-95-FA-3	137	192.160.0.127	TT-TT-TT-TT-T	137	C:\Win v
C.											>

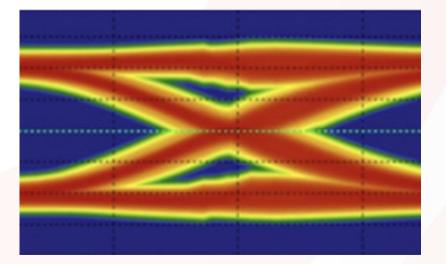


					Traffic Log - I	Network Threat Prot	ection Logs				
File Edit View Filter Ad	tion Help										
Date and A	ction	Severity	Direction	Protocol	Source Nost	Source HAC	Source Port	Destination Nost	Destination NAC	Destination Port	Applic /
22/11/2013 8:07 A	llowed	5	Incoming	009	192.140.0.55	7C-05-07-91-D	5353	224.0.0.251	01-00-55-00+0	5353	
22/11/2018 8:07 A	llowed	5	Incoming	TCP	192.148.0.111	A0-83-CC-48-C	52514	216.2.40.149	00-09-07-09-0	80	D:\Pro
22/11/2013 8:08 A	liowed	5	Incoming	907	192.168.0.55	70-08-07-91-0	1900	239.255.255.250	01-00-58-78-8	1900	
22/11/2013 8:08 A	llowed	5	Incoming	TCP	192.148.0.70	00-50-54-86-7	58498	192.140.0.117	00-00-29-99-9	463	D:\Pro
22/11/2013 8:08 A	llowed.	5	Incoming	UDP	192.148.0.56	00-07-52-59-5	137	192.160.0.127	FT-FT-FT-FT-T	137	C:\Win
022/11/2013 8:08 A	llowed	5	Incoming	009	192.140.0.63	00-07-75-70-0	137	192.168.0.127	tt-tt-tt-tt-t	137	C:\Win
022/11/2013 0:08 A	lined	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 A	llowed	5	Incoming	TCP	192.148.0.111	A0-83-CC-48-C	52816	216.2.48.149	00-09-07-09-0	80	D:\Pro
🔁 22/11/2013 8:08 A	liowed	5	Outgoing	ICP	192.148.0.117	00-00-29-99-9	62301	192.140.0.110	00-0C-29-2E-4	8016	C:\Win
022/11/2013 8:08 A	llowed	5	Incoming	TCP	192.148.0.111	A0-83-CC-4E-C	52517	214.2.48.149	00-09-07-09-0	=0	D:\Pro
D22/11/2013 0:08 K	Iloied		Inconstg	TCP	192.148.0.111	\$0-83-CC-4E-C	\$2515	214.2.48.149	00-09-07-09-0	20	Dr\Pro
22/11/2013 B:00 A	llowed	5	Incoming	900	192.148.0.51	84-85-27-17-B	50144	239.235.255.250	01-00-58-78-8	1900	
22/11/2013 8:08 A	llowed.	.5	Incoming	UDP	192.148.0.57	00-23-18-C3-F	137	192.148.0.127	TT-TT-TT-TT-T	137	C:\Win
22/11/2013 8:06 A	llowed	5	Incoming	009	192.148.0.57	00-23-18-C3-F	60248	224.0.0.252	01-00-58-00-0	\$355	C:\Win
22/11/2013 8:08 A	liowed	5	Incoming	12	192.168.0.55	70-03-07-91-0	NA.	224.0.0.22	01-00-56-00-0	15A	
22/11/2013 8:08 A:	llowed	5	Incoming	1056	192.148.0.55	70-05-07-91-0	51452	224.0.0.252	01-00-58-00-0	\$355	C:\Win
322/11/2013 8:08 A	lloved	5	Incoming	TCP	192.148.0.111	A0-83-CC-48-C	52519	216.2.48.149	00-09-07-09-0	80	D:\Pro
022/11/2013 8:08 A	llowed	5	Incoming	TCP	192.148.0.111	A0-83-CC-48-C	52820	216.2.40.149	00-09-07-09-0	20	D:\Pro
022/11/2013 8:08 A	limed	5	Incoming	TCP	192.168.0.111	A0-83-CC-48-C	\$2821	216.2.48.149	00-09-07-09-0	80	D:\Pro
22/11/2013 8:08 A	llowed	5	Incoming	TCP	192.148.0.111	A0-83-CC-48-C	52822	216.2.48.149	00-09-07-09-0	80	D:\Pro
€22/11/2013 8:08 A	llowed.	5	Outgoing	ICP	192.148.0.117	00-00-29-99-9	42303	192.168.0.310	00-00-29-28-4	8016	C:\Win
22/11/2013 8:06 A	llowed	5	Incoming	109	192.148.0.111	A0-83-CC-48-C	52824	216.2.42.149	00-09-07-09-0	50	D:\Pro
🔁 22/11/2013 8:09 A	liowed	5	Outgoing	TCP	192.168.0.117	00-00-29-99-9	42304	192.148.0.110	00-00-29-28-4	8016	C:\Win
22/11/2013 8:09 A	liowed	5	Incoming	TCP	192.148.0.111	A0-83-CC-4E-C	32825	216.2.48.149	00-09-07-09-0	80	D:\Pro
22/11/2013 8:09 A	lioved.	5	Incoming	ICP	192.148.0.111	A0-83-CC-48-C	82826	214.2.48.149	00-09-07-09-0	80	D:\Pro
022/11/2013 8:09 A	llowed	\$	Incoming	19	192.148.0.64	E0-69-95-FA-3	NR.	224.0.0.22	01-00-5g-00-0	NA	
022/11/2013 8:09 A	liowed	5	Incoming	909	182.168.0.64	E0-69-95-FA-3	52124	224.0.0.252	01-00-55-00-0	\$355	C:\Win
22/11/2013 8:09 A	llowed	5	Incoming	UDP	192.148.0.64	E0-69-95-FA-3	137	192.140.0.127	TT-TT-TT-TT-T	137	C:\Win v
0											

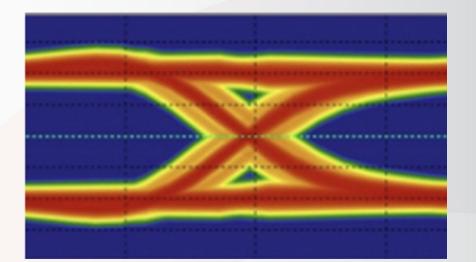
## **Different Asset DNA!**



Ļ







# Sepio's unique approach



# Harnessing new data source

getting to the true source of asset risk without traffic monitoring

O Create an Asset DNA

O Risk assessment

O Asset mapping





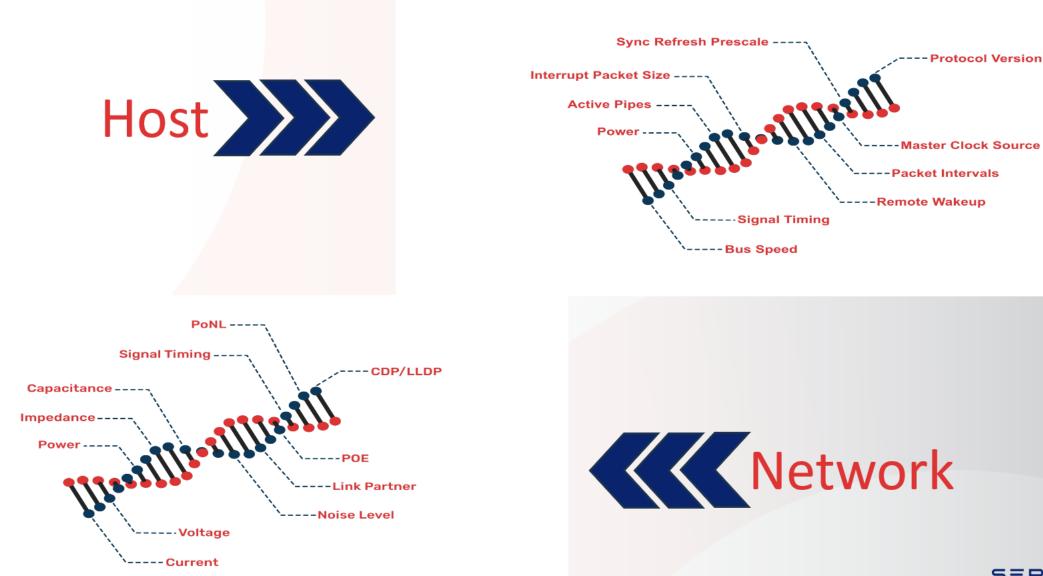
#### How do we do it?

# Asset DNA



#### Introducing Asset DNA

Ę



SEPIO

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 probing Image: Second state Image: Second

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 (IT/IoT/OT).

Establish trust validate assets, enforce regulatory compliance with a single low TCO solution.

# Sepio's proven value for CPS





Sepio has an innovative and robust solution that identifies a type of threats that were difficult to identify otherwise 55

R&D Engineer Leading Global Energy and Utilities Provider

- Complete OT/IT/IoT asset visibility
- OT asset protection
- Maintaining operational continuity
- Easier risk management compliance
- Mitigate known threats



# 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**

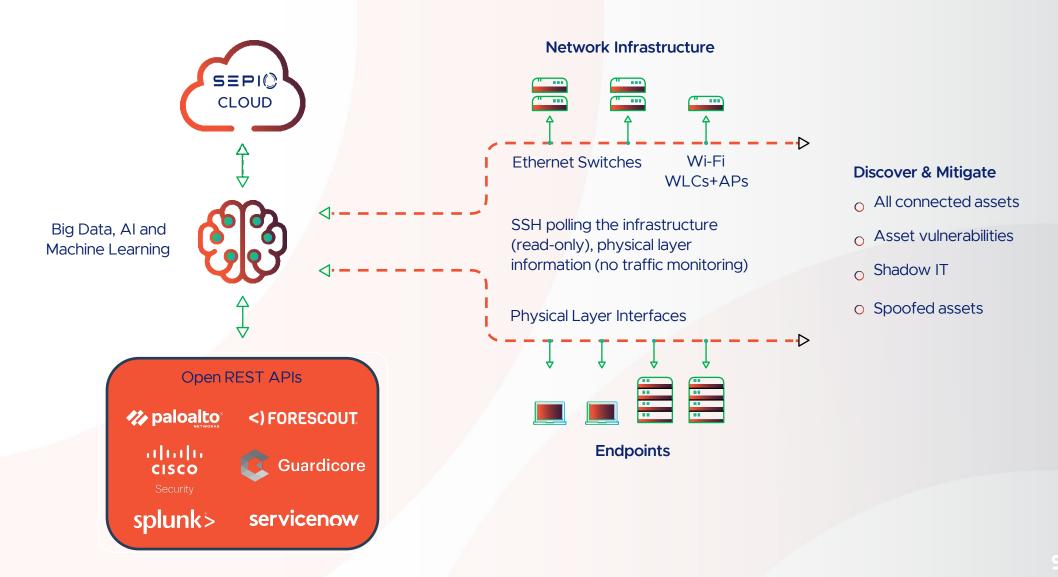
- Reduce complexity with a consolidated source of asset visibility across all environments
- Reduce hardware clutter
- Ensure operational efficiency of assets

#### CAASM

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

# **Architecture and Deployment aspects**







Sepio agent deployment options

Fixed agent (including VDI support)

Session based

Dissolvable agent



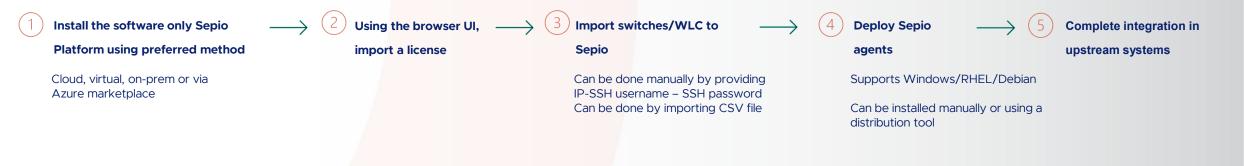
#### Typical Customer Journey

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



#### Deployment process



000

()

a)
b)
a)
b)
a)
b)
a)
b)
b)
b)
b)
b)
c)
<

	o	0	
ත් 38,470 Assets Total	1,534 () New Hosts	103 103 Reveal 103 Reveal 103 Reveal 103 Reveal 103 Reveal 104 Rev	Recent Visible Risks Assets (201) Hests (103) Netwo
			Leonardo (CDC ACM, HID) Arduino SA
Assets Risk	Assets Distribution	Sort By: Asset Count +	ord Integrated Camera P <sup>N</sup> Chicony Electronics Co., Ltd
	🗖 Host	Ausc      High Bilk	C VFS5011 Fingerprint Reader Validity Sensors, Inc.
C C	۹ IP Phone	1.3/ (10)	Big Integrated Camera Dic Chicory Electronics Co., Ltd
High Medium	loT - Others	6	VFS5011 Fingerprint Reader     Validity Sensors, Inc.
303 023	Access Point	243 12	VFSS011 Fingerprint Reader     Validity Sensors, Inc.
	Others		VFS5011 Fingerprint Reader     Validity Sensors, Inc.
	Printer	1066     10     1     1     1     1	VF55011 Fingerprint Reader     Validity Sensors, Inc.
0	Camera  Router	( 6 • 08 11	VFSS011 Fingerprint Reader     Validity Sensors. Inc.
Low 37,214	ToT - Healthcare	0 185 (1	VFSS011 Fingerprint Reader     Validity Sensors, Inc.
	[] IoT - Building Management	1 273 0	no Integrated Camera
	B <sup>r0</sup> Composite Device	1 20	ge Integrated Camera Chicory Electronics Co. Ltd

Network	Infrastructure								Q .
Cat2910-2 (19	92.168.100.21)			7 9 T	13 15 77 19 21 23	25			
✓ Risk Indicator	rs (1)	6							
No Risk Indicators		2							
<ul> <li>General Detail</li> </ul>	lis	100		~					
Status Type	Connected Switch	Detect	ed Devices					×	
Group Location Scan Priority Active Ports	Network Inhastructure Default Manual Only 2	()	Port Fa0/2 Switch Cat2	<b>4</b> 910-2			Ø Accep	t Risk Ø Block Port	Risk
Total Ports Vendor First Seen	26 Claco 2023-01-36 18:24:42		MAC		Asset	Vendor	Туре	Risk 🗸	
Last Seen Last Updated	2023-01-15 14:45:58 2023-01-15 14:45:58	8	B8:27:EB:83:CB:/	D	Raspberry Pi	Raspberry Pi Foundation	Rospberry Pi	۲	
		5550	E8:BA:70:08:50:4	0	Communication - C3750G Switch	Cisco Systems	Network Switch	۲	
<ul> <li>Asset Details</li> </ul>		0000	F8:7A:41:4D:D1:4	,	Communication - C9200 Switch	Cisco Systems	Network Switch	۲	
Policy Domain Model	Default TLV		40:46:28:55:00:0	0	Communication - C2960X Switch	Cisco Systems	Network Switch	۲	
Host MAC Address	192.68300.21 04:07:48:EB:50:00		04:E8:40:8F:10:0	7	Communication - C2960L Switch	Cisco Systems	Network Switch	۲	
Software Boot Info	12.2(50)SES C2960-HBOOT-M 12.2(44)SES #1		64:51:06:41:A2:A1	í.	PC	HP Inc.	Host	٢	
Version ID Image	V20 C2960-LANBASEK9-M		54:E1:AD:08:FF:4	1	PC	Lenovo Group Ltd.	Host	(6)	
Serial Number	FCQ1544X1M4 12.215015E5		04:2A:E2:D3:1A:8	D	sepio-2960-x (192.168.100.29)	Clico	Network Switch	(1)	
CPU Environment Transport	(PowerPC405) processor (revision T0) with 65536K bytes SSH		00:5F:86:A6:50:8	0	sepio-2960x-v3 (192.168.100.26)	Cisco	Network Switch	(4)	
		0	C 3	Fa0/13		0 Detected Devices		_	
			C 14	Fa0/14		0 Detected Devices			
			C 15	Fa0/IS		0 Detected Devices			
			<b>I</b> 16	Fa0/16		0 Detected Devices			
			Ξ π	Fa0/17		0 Detected Devices			
			C 18	FaQ/18		0 Detected Devices			

### Sepio's Asset Risk Management solution

Ę

္ခ်င္ရွိ <u>9369</u> 0	<b>1</b> 465 (7)	<b>6510</b> 26	0 📮 87180	439	Recent Visible Risks
Assets Total	New Hosts	Hosts New	Network Total	New	Assets (188) Hosts (8) Network (2
					Camera Hikvision Digital Technology Co. Ltd.
Online America Dist.	Annata Distribution			Sort By: High Risk 👻	Hikvision Digital Technology Co. Ltd.
Online Assets Risk	Assets Distribution			Gore by. High Kore	Communication - Switches Extreme Networks
	Network Switch	29	523		
<b>C</b> .	🖨 Printer	96			Communication - C3750X Switch Cisco Systems
High		4			
	🛄 Host	2		6510	Communication - C9200 Switch Cisco Systems
38	Random MAC address	59			
	Kandoni MAC address	1			CAC Card Reader Realtek Semiconductor Corp.
	Attack Tool	(  1    1			
Medium	🚔 Access Point	22			RTLB188EUS 802.11n Wireless Network Adapter Realtek Semiconductor Corp.
	E Access Point	1			RTL8153 Gioabit Ethernet Adapter
1306	💷 Keyboard	• 9 0			RTL8153 Gigabit Ethernet Adapter Realtek Semiconductor Corp.
	Smartphone	• 10			Keyboard K120 Logitech, Inc.
	Smartphone	0			Logitech, Inc.
Low	Storage	<b>  </b> 4 ( 0			Luxvisions Innotech Limited
	<ul> <li>EM600000000</li> </ul>	10			Luxvisions milotech Limited
92384	🙏 USB Hub	0			Pub Terminus Technology Inc.
	(+) IoT - Healthcare	1			

SEPIO



See what you've been missing

