SEPIO

Mitigating Cyber Physical Systems Risks in Healthcare

Jan 25

Questions our healthcare customers ask themselves-

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

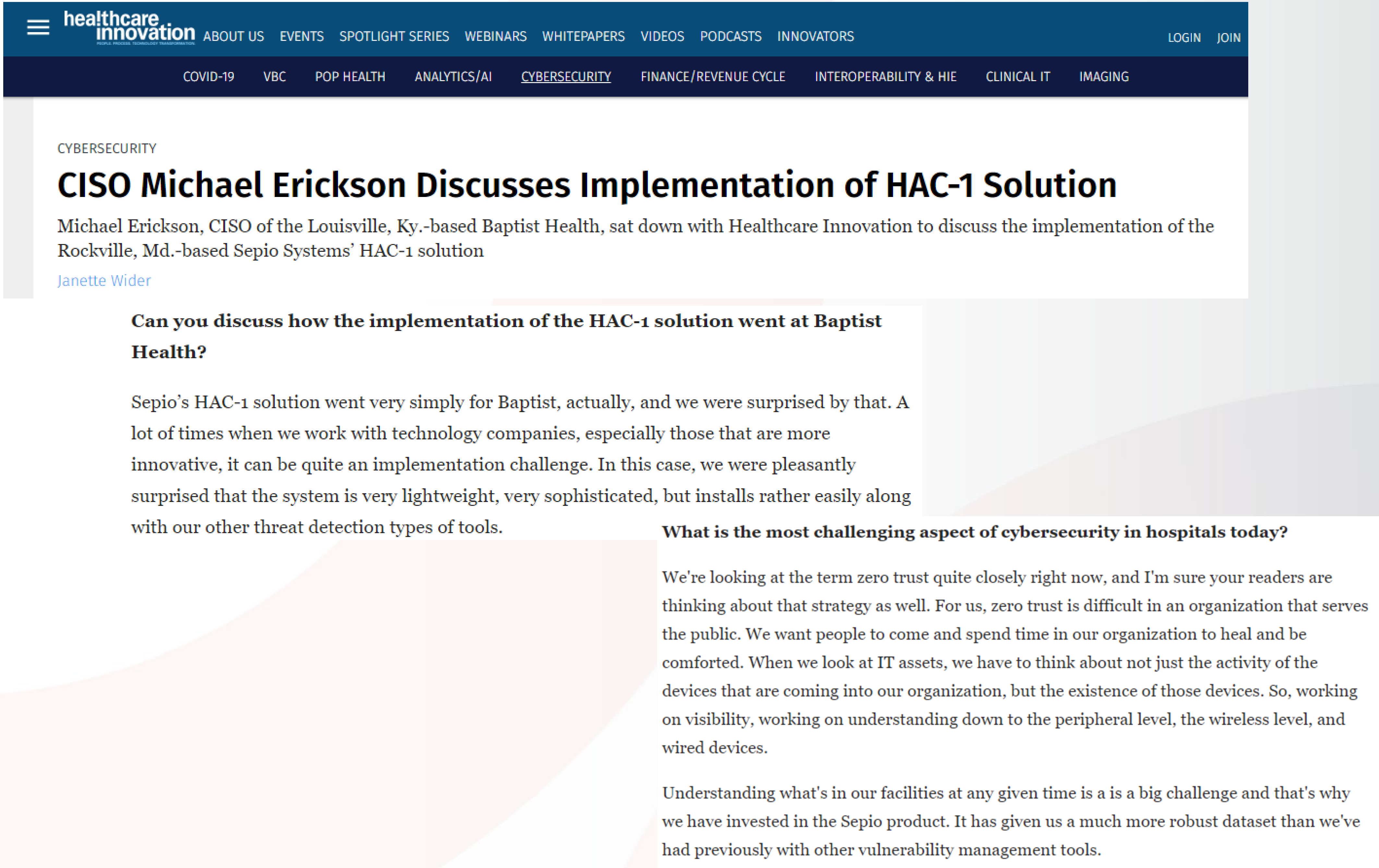
SEPIO

Case study

BAPTIST HEALTH

Baptist deployment highlights

- More than 27,500 hosts and 544 network switches
- More than 635K connected assets
- Mix of new and legacy networking infrastructure
- Periodic reporting
- Attack surface reduction



CYBERSECURITY

CISO Michael Erickson Discusses Implementation of HAC-1 Solution

Michael Erickson, CISO of the Louisville, Ky.-based Baptist Health, sat down with Healthcare Innovation to discuss the implementation of the Rockville, Md.-based Sepio Systems' HAC-1 solution

Janette Wider

Can you discuss how the implementation of the HAC-1 solution went at Baptist Health?

Sepio's HAC-1 solution went very simply for Baptist, actually, and we were surprised by that. A lot of times when we work with technology companies, especially those that are more innovative, it can be quite an implementation challenge. In this case, we were pleasantly surprised that the system is very lightweight, very sophisticated, but installs rather easily along with our other threat detection types of tools.

What is the most challenging aspect of cybersecurity in hospitals today?

We're looking at the term zero trust quite closely right now, and I'm sure your readers are thinking about that strategy as well. For us, zero trust is difficult in an organization that serves the public. We want people to come and spend time in our organization to heal and be comforted. When we look at IT assets, we have to think about not just the activity of the devices that are coming into our organization, but the existence of those devices. So, working on visibility, working on understanding down to the peripheral level, the wireless level, and wired devices.

Understanding what's in our facilities at any given time is a is a big challenge and that's why we have invested in the Sepio product. It has given us a much more robust dataset than we've had previously with other vulnerability management tools.

“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!

Source: ESG ,April 2023

CPS Visibility Challenges

Active scanning → Potential impact on system responsiveness and availability.

Passive probing → Poor visibility (50%-80%) due to encrypted traffic.

Dormant assets→ Become “invisible” – MAC’less

SEPIO

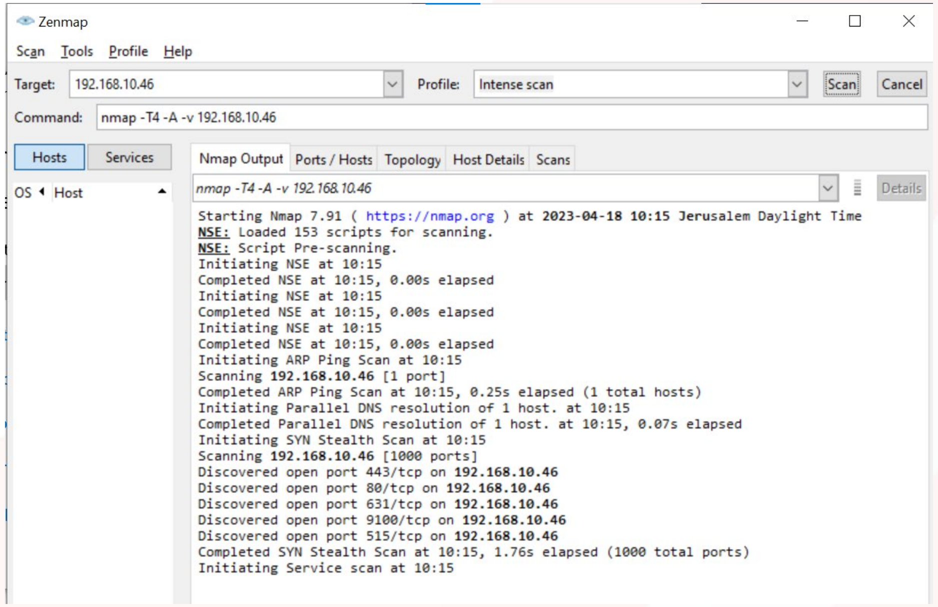
Friend or Foe?

Same MAC

MAC:00D085045802

MAC:00D085045802

Same Ports



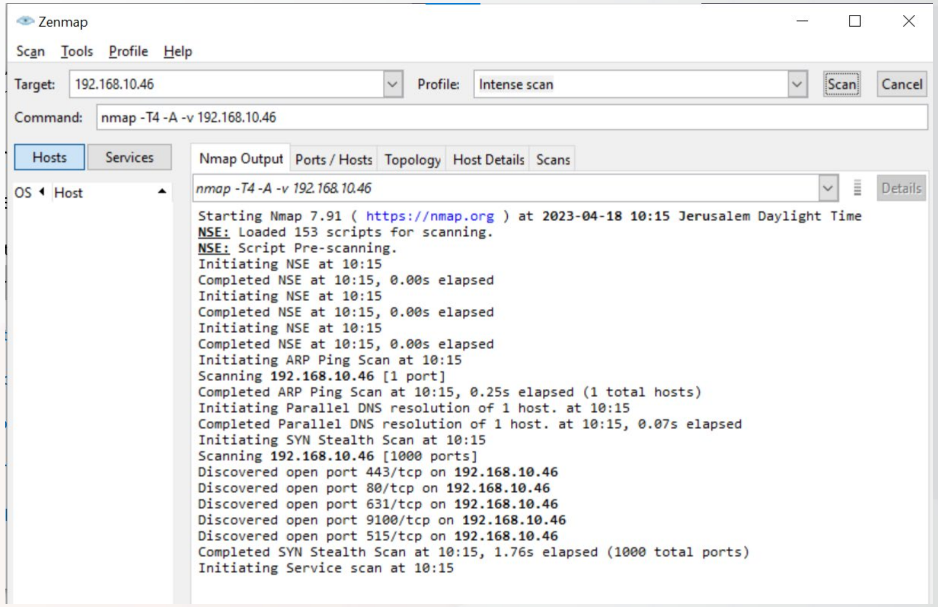
Target: 192.168.10.46

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.10.46

```
nmap -T4 -A -v 192.168.10.46

Starting Nmap 7.91 ( https://nmap.org ) at 2023-04-18 10:15 Jerusalem Daylight Time
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:15
Completed NSE at 10:15, 0.00s elapsed
Initiating NSE at 10:15
Completed NSE at 10:15, 0.00s elapsed
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 elapsed
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 80/tcp on 192.168.10.46
Discovered open port 631/tcp on 192.168.10.46
Discovered open port 9100/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 ports)
Initiating Service scan at 10:15
```



Target: 192.168.10.46

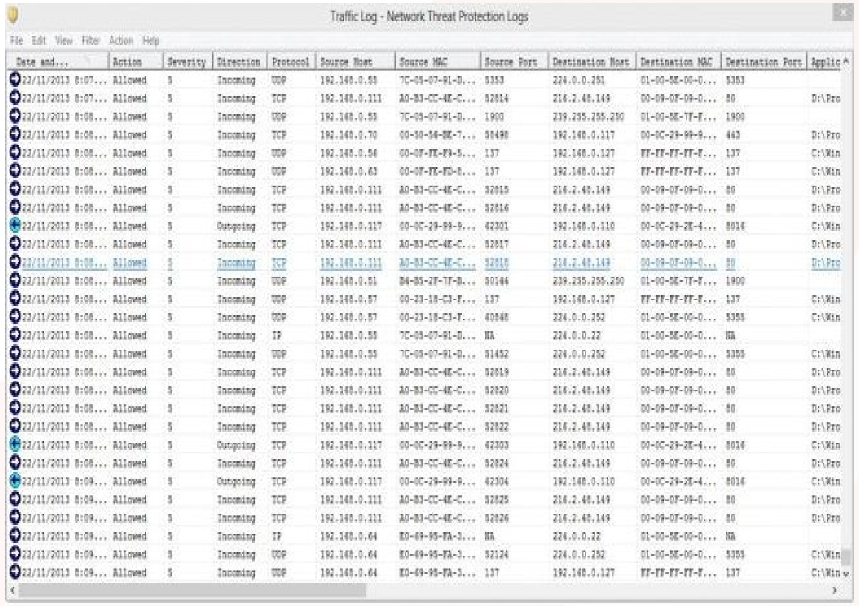
Profile: Intense scan

Command: nmap -T4 -A -v 192.168.10.46

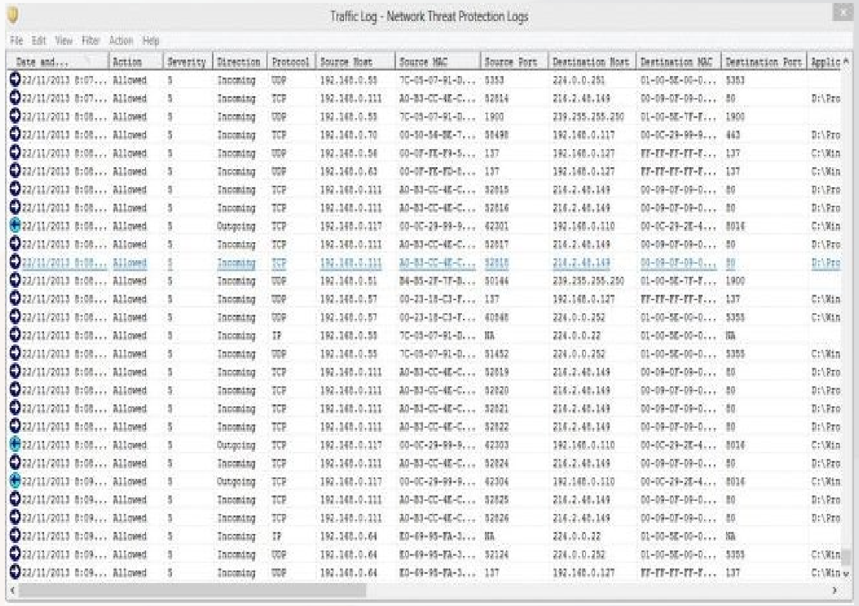
```
nmap -T4 -A -v 192.168.10.46

Starting Nmap 7.91 ( https://nmap.org ) at 2023-04-18 10:15 Jerusalem Daylight Time
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:15
Completed NSE at 10:15, 0.00s elapsed
Initiating NSE at 10:15
Completed NSE at 10:15, 0.00s elapsed
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 elapsed
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 80/tcp on 192.168.10.46
Discovered open port 631/tcp on 192.168.10.46
Discovered open port 9100/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 ports)
Initiating Service scan at 10:15
```

Same Traffic

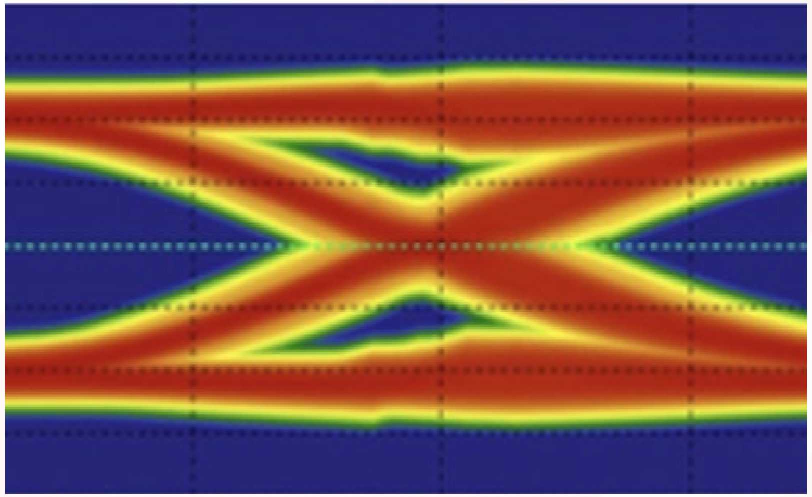

Traffic Log - Network Threat Protection Logs
File Edit View Filter Action Help

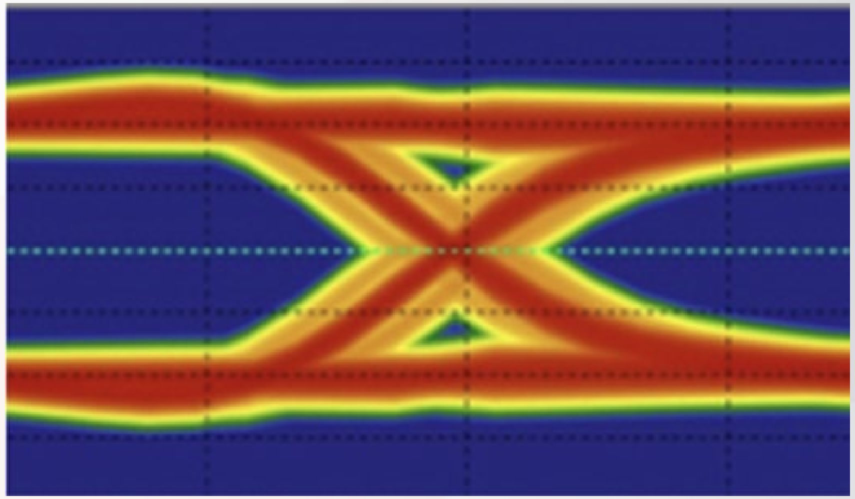
Date and...	Action	Severity	Direction	Protocol	Source Host	Source MAC	Source Port	Destination Host	Destination MAC	Destination Port	Applic
22/11/2013 8:07...	Allowed	5	Incoming	UDP	192.168.0.53	7C-05-07-91-D...	5353	224.0.0.251	01-00-5E-00-0...	5353	
22/11/2013 8:07...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52814	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.53	7C-05-07-91-D...	1900	239.255.255.250	01-00-5E-7F-F...	1900	
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.70	00-50-56-BE-7...	58498	192.168.0.117	00-0C-29-99-9...	443	D:\Pro
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.56	00-0F-FE-F9-5...	137	192.168.0.127	FF-FF-FF-FF-F...	137	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.63	00-0F-FE-FD-8...	137	192.168.0.127	FF-FF-FF-FF-F...	137	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52815	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52816	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:08...	Allowed	5	Outgoing	TCP	192.168.0.117	00-0C-29-99-9...	42301	192.168.0.110	00-0C-29-2E-4...	8016	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52817	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52818	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.51	B4-B5-2F-7F-B...	50144	239.255.255.250	01-00-5E-7F-F...	1900	
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.57	00-23-18-C3-F...	137	192.168.0.127	FF-FF-FF-FF-F...	137	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.57	00-23-18-C3-F...	40848	224.0.0.252	01-00-5E-00-0...	5355	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	IP	192.168.0.58	7C-05-07-91-D...	NA	224.0.0.22	01-00-5E-00-0...	NA	
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.53	7C-05-07-91-D...	51452	224.0.0.252	01-00-5E-00-0...	5355	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52819	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52820	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52821	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52822	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:08...	Allowed	5	Outgoing	TCP	192.168.0.117	00-0C-29-99-9...	42303	192.168.0.110	00-0C-29-2E-4...	8016	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52824	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:09...	Allowed	5	Outgoing	TCP	192.168.0.117	00-0C-29-99-9...	42304	192.168.0.110	00-0C-29-2E-4...	8016	C:\Win
22/11/2013 8:09...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52825	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:09...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52826	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:09...	Allowed	5	Incoming	IP	192.168.0.64	E0-69-95-FA-3...	NA	224.0.0.22	01-00-5E-00-0...	NA	
22/11/2013 8:09...	Allowed	5	Incoming	UDP	192.168.0.64	E0-69-95-FA-3...	52124	224.0.0.252	01-00-5E-00-0...	5355	C:\Win
22/11/2013 8:09...	Allowed	5	Incoming	UDP	192.168.0.64	E0-69-95-FA-3...	137	192.168.0.127	FF-FF-FF-FF-F...	137	C:\Win


Traffic Log - Network Threat Protection Logs
File Edit View Filter Action Help

Date and...	Action	Severity	Direction	Protocol	Source Host	Source MAC	Source Port	Destination Host	Destination MAC	Destination Port	Applic
22/11/2013 8:07...	Allowed	5	Incoming	UDP	192.168.0.53	7C-05-07-91-D...	5353	224.0.0.251	01-00-5E-00-0...	5353	
22/11/2013 8:07...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52814	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.53	7C-05-07-91-D...	1900	239.255.255.250	01-00-5E-7F-F...	1900	
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.70	00-50-56-BE-7...	58498	192.168.0.117	00-0C-29-99-9...	443	D:\Pro
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.56	00-0F-FE-F9-5...	137	192.168.0.127	FF-FF-FF-FF-F...	137	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.63	00-0F-FE-FD-8...	137	192.168.0.127	FF-FF-FF-FF-F...	137	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52815	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52816	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:08...	Allowed	5	Outgoing	TCP	192.168.0.117	00-0C-29-99-9...	42301	192.168.0.110	00-0C-29-2E-4...	8016	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52817	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52818	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.51	B4-B5-2F-7F-B...	50144	239.255.255.250	01-00-5E-7F-F...	1900	
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.57	00-23-18-C3-F...	137	192.168.0.127	FF-FF-FF-FF-F...	137	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.57	00-23-18-C3-F...	40848	224.0.0.252	01-00-5E-00-0...	5355	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	IP	192.168.0.58	7C-05-07-91-D...	NA	224.0.0.22	01-00-5E-00-0...	NA	
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.53	7C-05-07-91-D...	51452	224.0.0.252	01-00-5E-00-0...	5355	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52819	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52820	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52821	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52822	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:08...	Allowed	5	Outgoing	TCP	192.168.0.117	00-0C-29-99-9...	42303	192.168.0.110	00-0C-29-2E-4...	8016	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52824	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:09...	Allowed	5	Outgoing	TCP	192.168.0.117	00-0C-29-99-9...	42304	192.168.0.110	00-0C-29-2E-4...	8016	C:\Win
22/11/2013 8:09...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52825	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:09...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52826	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:09...	Allowed	5	Incoming	IP	192.168.0.64	E0-69-95-FA-3...	NA	224.0.0.22	01-00-5E-00-0...	NA	
22/11/2013 8:09...	Allowed	5	Incoming	UDP	192.168.0.64	E0-69-95-FA-3...	52124	224.0.0.252	01-00-5E-00-0...	5355	C:\Win
22/11/2013 8:09...	Allowed	5	Incoming	UDP	192.168.0.64	E0-69-95-FA-3...	137	192.168.0.127	FF-FF-FF-FF-F...	137	C:\Win

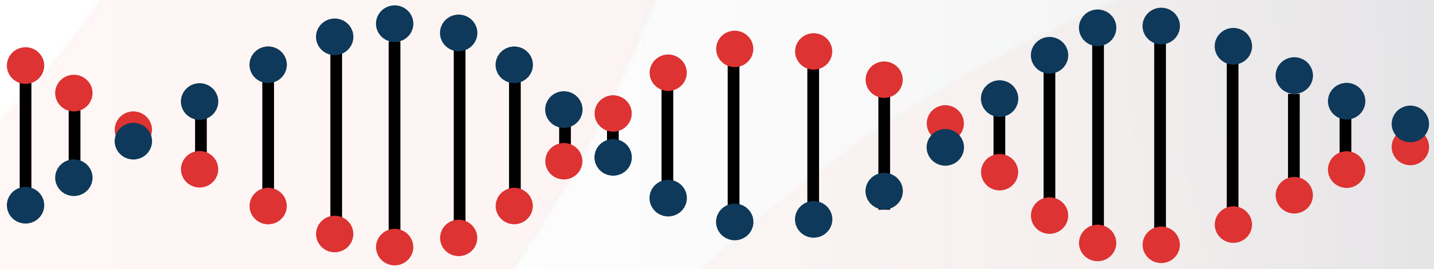
Different Asset DNA !





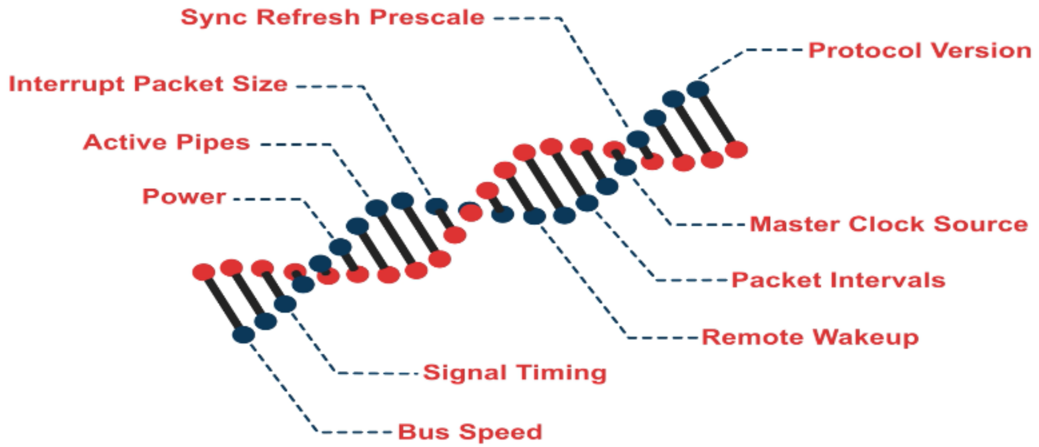
How do we do it?

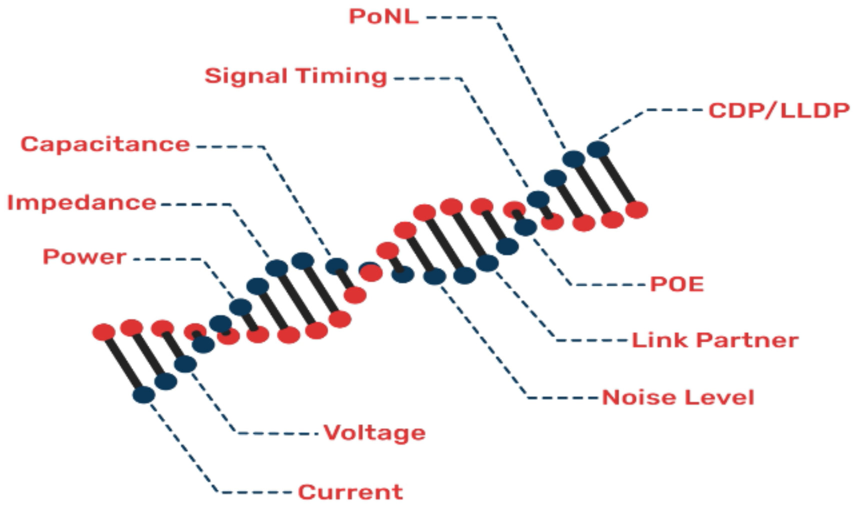
Asset DNA



Introducing Asset DNA

Host





Network

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

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

SEPIO

Healthcare Business Benefits

> *We're bringing a new set of information to our asset inventories and it's helping us plan the lifecycle of assets*

Michael Erickson, CISO,
Baptist Health

- Complete asset inventory
- Ensure operational efficiency of medical assets
- Maintain delivery of healthcare services
- Uphold patient safety
- Budget and resource planning
- Support regulatory compliance (HIPAA, GDPR)
- Prevent breaches

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

ITAM & CMDB

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

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

CAASM

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

SEPIO

See what you’ve been missing