

Bezpečnosť IoT/IoMT/OT

9.Jun, Hotel Tatra, Bratislava

Lubos Chovan
Channel System Engineer

lchovan@paloaltonetworks.com

Exstítujúce riešenie nefungujú

Japanese government plans to hack into citizens' IoT devices



Even DSLR cameras are vulnerable to ransomware

engadget

DEF CON 2019: Researchers Demo Hacking Google Home for RCE

threatpost

IOT SECURITY. SORRY, NO CAVALRY IS COMING

ENGINEERING.COM

The Washington Post
How a fish tank helped hack a casino

MICROSOFT CATCHES RUSSIAN STATE HACKERS USING IOT DEVICES TO BREACH NETWORKS

Unpatched Flaws in IoT Smart Deadbolt Open Homes to Danger

threatpost

techradar

Fancy Bear hackers used IoT devices to hack corporate networks

How crooks can cover up crimes by hacking IoT cameras to show fake footage



IoT Security - Vertical support



Enterprise



Healthcare



Industrial

- In 2021, there were more than **10 Billion active IoT** devices
- By 2025, there will be **152,200 IoT devices** connecting to the internet per minute
- **1.3 Billion** IoMT devices by 2030
- **18 Billion** IoT devices will be connected by 2030

Enterprise IoT Devices

Security Issues

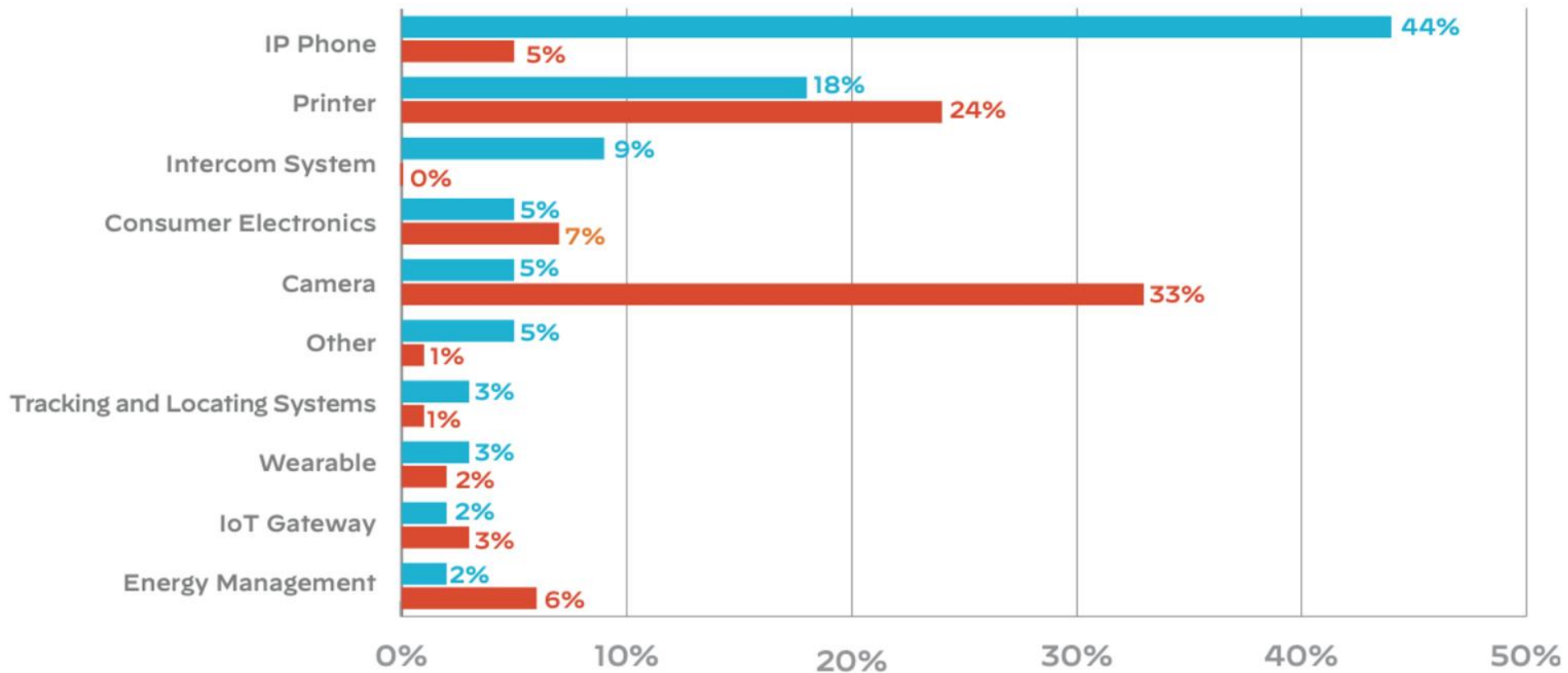


Figure 1: IP phones have only 5% of all security issues

Unit 42 IoT Threat Report: Most High Risk Devices?



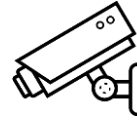
Medical Imaging
Systems

51%



Patient Monitoring
Systems

26%



Security
Cameras

33%



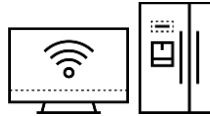
Printers

24%



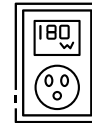
Medical Devices
Gateways

9%



Consumer
Electronics

7%



Energy Management
Devices

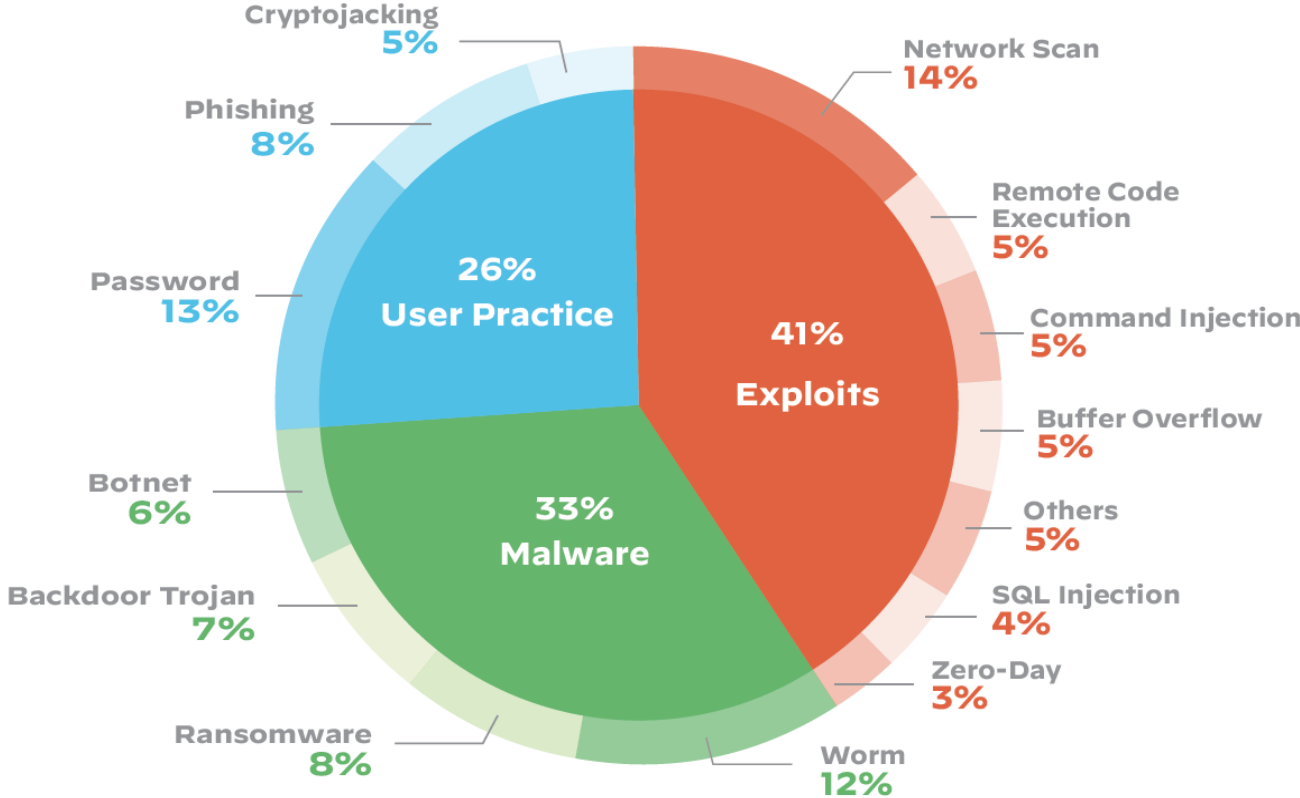
6%



IP
Phones

5%

Unit 42 IoT Threat Report: Top Threats for IoT Devices



Unit 42 IoT Threat Report: Highly Vulnerable Medical Devices



of all IoT device traffic is unencrypted

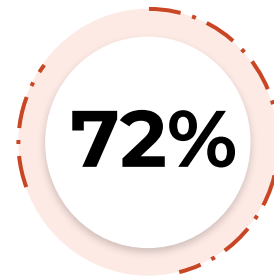


of all IoT devices are vulnerable to medium or high severity attacks

“83% of Imaging Systems Powered by End-of-Life OS”

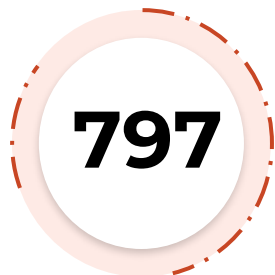


of infusion pumps have unpatched vulnerabilities



of HDOs have a mix of IT and IoMT devices in the same VLANs

Industrial Control Systems vulnerabilities in 2022



Vulnerabilities
published in 2H 2021



Increase from 637
in H1 2021

“63% of the vulnerabilities disclosed may be exploited remotely”

Palo Alto Networks approach

IoT Security Features & Capabilities



1. Understand IoT Assets

- Identify 90+% of devices **within 48 hours**
- ML accurately classifies devices with **50+ attributes**
- **Continual detection** of new and never before seen devices



2. Assess IoT Risk

- Passive **discovery of vulnerabilities** and integration with databases
- **Continuous risk assessment** and scoring to prioritize response
- **Vendor advisory** for security patching



3. Apply Risk Reduction Policies

- **Risk-based policy recommendations** to enforce only trusted behaviour of devices and groups
- Reduce attack surface with **context-aware segmentation**
- **Automated enforcement** with Device-ID



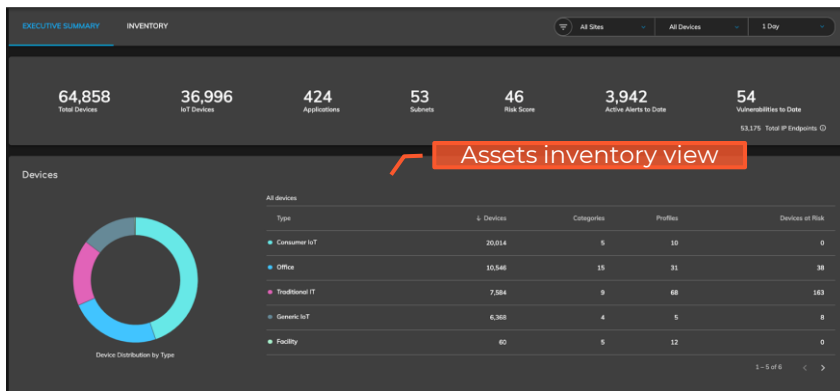
4. Prevent Known Threats

- **Protection from exploits, C2, spyware** and other known threats
- Enhance detail of all alerts with **IOT device context**



5. Detect & Respond to Unknown Threats

- Anomalous activity and **zero-day detection**
- **Stop unknown** file and web-based threats
- Detailed **incident context** for response



Rich device context

Status	Risk	Device Name	Profile	Vendor	Model	OS	IP Address	MAC Address	VLAN	VLAN	Last	Conf.	Conf.	Asset	Subnet
100	100	10.27.16.11.1019	Raspber...	Raspber...		Windows	192.168.1.101	68:27:eb:31:10:59		IoT-3_RP	Jan 26, 20	High	99		192.168.1.0/24
100	100	10.21.23.22	Dell Co...	Dell	Latitude	Windows	10.21.23.22	00:1b:17:00:01:92		Primary	Jan 26, 20	High	99		10.21.0.0/24
100	100	black-pa01	Raspber...	Raspber...		Windows	192.168.1.193	68:27:eb:59:ca:88			Jan 26, 20	High	99		192.168.1.0/24
100	100	black-pa01	Raspber...	Raspber...		Windows	192.168.1.191	68:27:eb:59:7a:69			Jan 26, 20	High	99		192.168.1.0/24
100	100	black-pa01	Raspber...	Raspber...		Windows	192.168.1.197	68:27:eb:59:7a:69			Jan 26, 20	High	99		192.168.1.0/24
76	10.21.28.200		Dell Co...	Dell	Latitude	Window...	10.21.28.200	00:1b:17:22:01:92		Primary	Jan 26, 20	High	99		10.21.0.0/24
76	10.35.38.79		Johnson	Johnson		Windows	10.33.38.79	61:ca:11:12:11:29		Primary	Jan 26, 20	High	99		10.0.0.0/8
73	sc004803.entropysec...		Microsof...	Microsof...		Windows	10.113.60.177	61:5b:71:22:a1:22		Primary	Jan 26, 20	High	99		10.0.0.0/8
73	00:1b:17:00:01:92		Palo AL...	Palo AL...	PA-3200	PAN-OS	10.21.29.58	00:1b:17:00:37:33		Primary	Jan 26, 20	High	99		10.21.0.0/24
70	black-pa01		Raspber...	Raspber...		Windows	192.168.1.195	68:27:eb:58:91:42			Jan 26, 20	High	99		192.168.1.0/24
70	black-pa01		Raspber...	Raspber...		Windows	192.168.1.196	68:27:eb:58:b1:21			Jan 26, 20	High	99		192.168.1.0/24
66	78:32:c1:64:6a:8b		Macintos...	Apple Inc.		MacOS	10.54.101.35	78:32:c1:64:6a:8b	922	Primary	Jan 26, 20	High	99		10.0.0.0/8
66	NP080CC46		HP Com...	Hewlett ...		Embedd...	10.33.110.2	6c:3a:61:06:0c:6e		Primary	Jan 26, 20	High	99		10.0.0.0/8
66	5CWN60C7543		PC Win...	Intel Cor...		Windows	10.54.101.173	00:18:eb:c3:33:64	922	Primary	Jan 26, 20	High	99		10.0.0.0/8

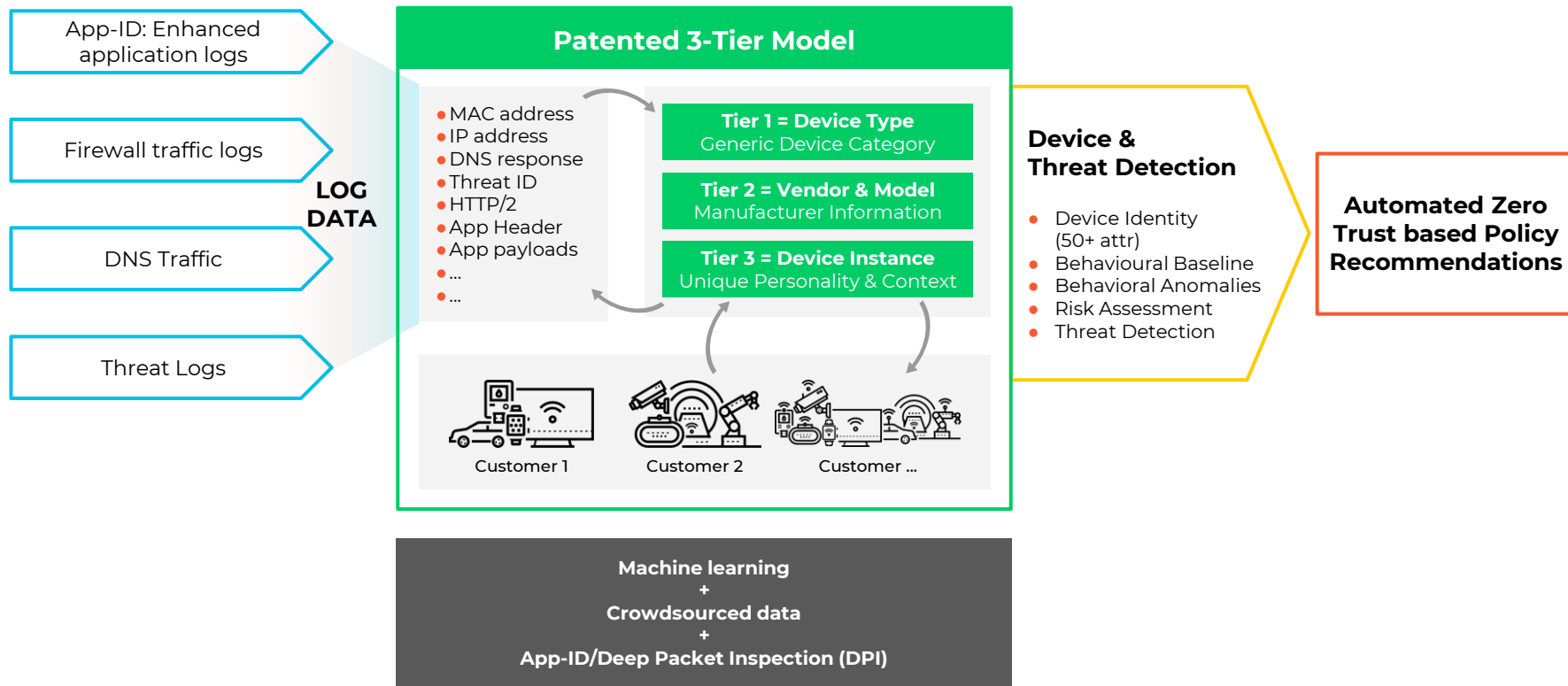


1. Understand IoT Assets

Identify devices quickly and accurately using the unique combination of machine learning and App-ID technology

- Discover any IoT, OT or IT device on your network with 90+% found within first 48 hours
- Identifies new, never-seen-before devices and gain deep insights from 50+ attributes
- Continuous monitoring ensures no device is missed regardless of when they connect

IoT Security Machine Learning: Personality & Context





2. Assess IoT Risk

Real-time monitoring and risk scoring allows security teams to prioritize efforts based on individual or groups of devices

- Automatically assess risk based on vendor advisories, vulnerability information, anomalous device behavior, Unit 42 and other intel
- Scores and tracks risk changes over time for compliance and retrospective analysis
- Customize risk levels to match existing risk frameworks

Comprehensive Risk Framework and Assessment



Threats

Exploits | Malware

- Abnormal connections between IoTs
- Malicious files on devices
- Connections to risky website
- Abnormal traffic between devices
- Personal device connecting to a large no. of devices
-



Vulnerability

CVEs

- Default passwords
- End of Life OS/Apps/Devices
- Obsolete protocols
- Cloud/network connections
- CVE tracking
-



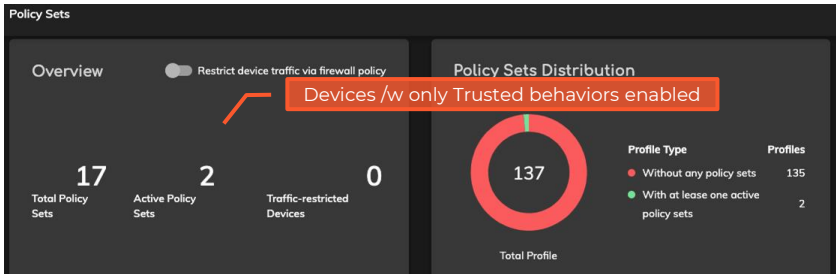
Context

Static | Dynamic

- Misconfiguration
- Unusual software
- Patch-level
- Apps-Name/version
- Internal/ external connection type and frequency
- Unexpected amount of data transmission
- Device behavior anomalies
- Manufacturer specifications
-

Device Risk

Leverages ML, Crowdsourced Telemetry, Unit 42 Threat Research



Profiles > GE UltraSound Machine > Create New Policy Set

1 Settings 2 Select Internal Destinations 3 Select External Destinations 4 Review

Internal Destinations (32) Applications (18)

Select which network behaviors with internal destinations you want to allow. Group policies by Application Source Profile Behavior

Enable device behaviors confidently

dicom (2) Usage High ✓ Application Allowed

No.	Source Profile	Application	Destinatio...	# of IP Addr...	# of Selecte...	Usage
1	GE UltraSound Ma...	dicom	Dell Computer	1	-	High
2	GE UltraSound Ma...	dicom	-	4	-	High

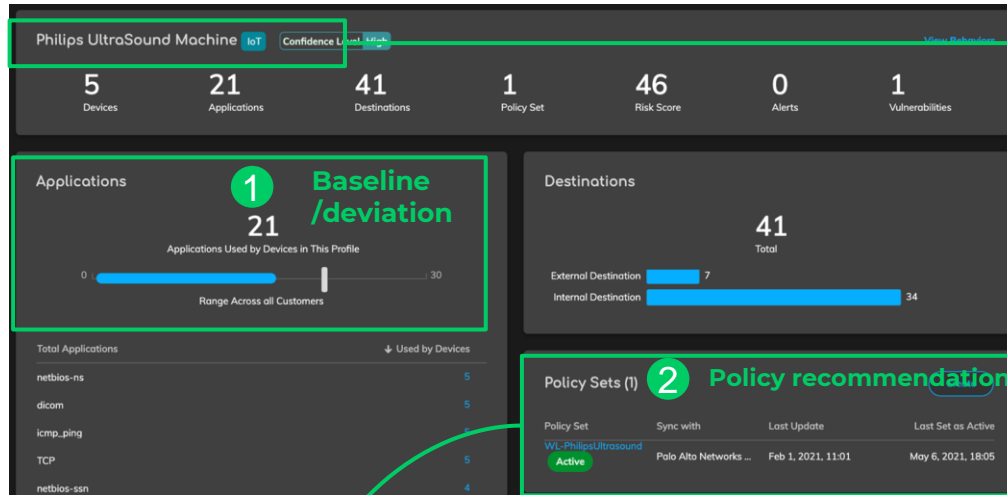
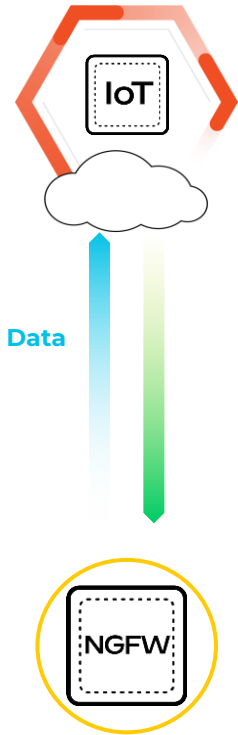


3. Apply Risk Reduction Policies

Consistent profiling of device activity is accurately converted into risk-based policy recommendations, allowing security teams to confidently allow only trusted behavior

- Gain context for segmenting IoT, OT and IT devices to reduce your attack surface
- Eliminate pain-staking policy creation for Zero-trust with recommended policies
- Enforce policies natively or via an integration in just a few clicks
- Monitors behavior and applies updates automatically with the new Device-ID construct

Built-in Zero Trust Policy Enforcement and Threat Prevention



The screenshot shows the PA-VM interface with the 'POLICIES' tab selected. A search for 'ultrasound' has been performed, resulting in the following table:

NAME	TAGS	TYPE	Source				Destination				APPLICATION	SERVICE
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION		
35 WL-PhilipsUltrasound	IoTSecurityReco...	universal	any	any	any	PhilipsUltras...	zone-internal	any	any	dicom	appli	
87 intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	
88 interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	

Device Objects

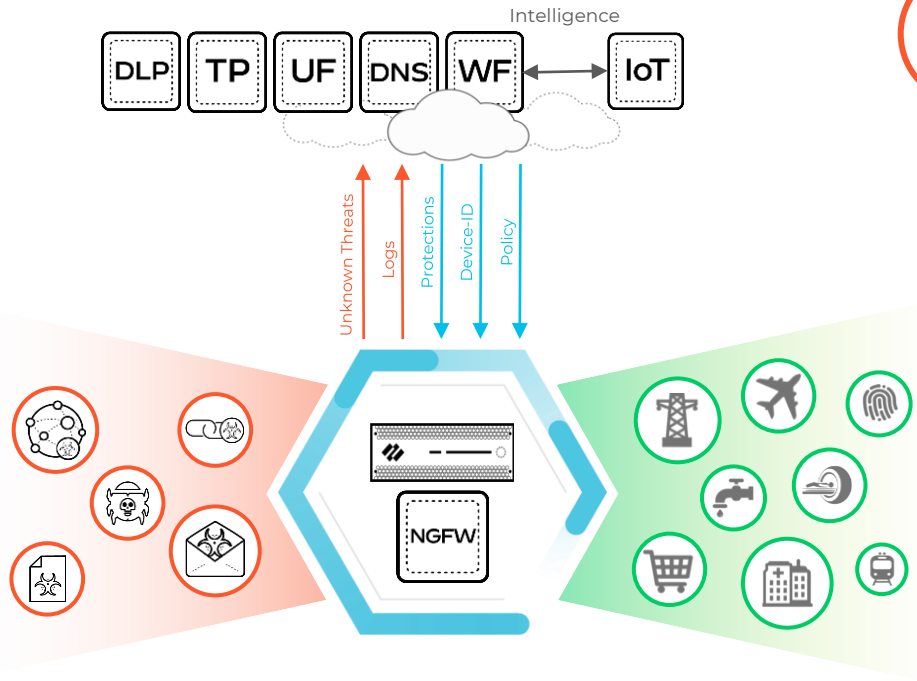
The screenshot shows the PA-5280 dashboard with the 'Virtual System' set to 'vsys1'. The left-hand navigation menu is expanded to show the 'Devices' section. The 'Devices' section is highlighted in blue and contains a search bar and a list of device objects:

- Addresses
- Address Groups
- Regions
- Dynamic User Groups
- Applications
- Application Groups
- Application Filters
- Services
- Service Groups
- Tags
- Devices**
 - GlobalProtect
 - HIP Objects
 - HIP Profiles
 - External Dynamic Lists
 - Custom Objects
 - Data Patterns
 - Spyware
 - Vulnerability
 - URL Category
 - Security Profiles

The 'Device Object' configuration form is shown with the following fields:

- Name:** Automation Pi
- Description:** Pi devices used for lab automation
- Shared
- Category:** Embedded System
- Profile:** Raspberry Pi Dev
- Model:** None
- OS:** Debian GNU/Lin
- Osfamily:** Linux
- Vendor:** Raspberry Pi Four

At the bottom of the form, there are three buttons: a 'Browse' button with a magnifying glass icon, a blue 'OK' button, and a 'Cancel' button.



4. Prevent Known Threats

Our leading Security Services stop all threats targeting IoT, IoMT and IT devices.

- Block known targeted IoT malware, spyware and exploits
- Provide safe web access for IoT device and stop bad URLs or malicious websites
- Prevent the use of DNS for C2
- Stop the loss of confidential and customer data
- Eliminate the burden of detection alerts that can be prevented

Policies > Alert

Detect Threats & Anomalies

Mirai remote code execution attempt

Severity: High | Status: New | Assign: Assign

Client: 134.209.69.7

Protocol: TCP

IP: 10.21.39.250

Category: Personal Computer

Site: Mountain View

Alert Events: Alert Detected (09:14, May 07, 2022)

Workflow: Assign, Resolve, Other, Add Notes, Download, Restrict Traffic, Vulnerability Scan, ServiceNow, SIEM, Quarantine via Cisco ISE, Release via Cisco ISE

Mirai is a malware that targets IoT or vulnerable devices with default or weak credentials. A suspicious connection from a remote host to this device has been detected. Zingbus detected that remote host successfully connected to this device and sent HTTP POST message with suspicious scripts and commands. These commands include initiating new connections to Mirai botnet C&C servers, and modifying local firewall rules such as IP table configurations. If these suspicious scripts and commands are successfully executed, the infected IoT or vulnerable device will become a remotely controlled bot that can be used to launch largescale attacks such as Distributed Denial of Service (DDoS) attacks. Subsequently, the attacker will gain the full control of the device.

A deviation from the normal baseline was detected.

Device profile	Personal Computer
Device category	PC-Windows
remote URL	134.209.69.7
remote URL classification	Mirai infected site
Mirai botnet C&C inside payload	206.189.118.55
local server port	5555/TCP
remote IP count	1
internal connection	false
inbound connection	true
time period (seconds)	3600

Device Details

Detect anomalous behaviour

ESTABLISHED CONNECTIONS

X-Ray DR6000

Geo-location

IP/Ports

Applications

Chart Type: Detail View

1 Day

Applications: TCP, modbus, dcom, netbios-ns, netbios-dgm, ftp

Workstation Ibm-90-Fb-a6-19-0E-B5-To-Ftp

Workstation Ibm-90-Fb-a6-19-0E-B5-To-Ftp



5. Detect & Respond to Unknown Threats

Use existing processes to respond to risks and threats unique to your environment.

- Block unknown file and web-based threats
- Detect and analyze anomalous activity, factoring in vendor and other data
- Use detailed device context to help analysis of any alert
- Use customizable playbooks to orchestrate response

Priklady


More than 65 categories



Physical Security

Devices 7

Profiles 5


Risk Score 38 



CT Scanner

Devices 4

Profiles 1

Risk Score 10 



Industrial Network Equipment

Devices 2

Profiles 2

Risk Score 26 

**Enterprise
IoT**

**Healthcare
IoMT**

Industrial

Special categories for Medical Devices



UltraSound Machine

Devices **14** Profiles **4**

Risk Score **69**



DICOM-Viewer

Devices **5** Profiles **2**

Risk Score **63**



MRI Machine

Devices **3** Profiles **1**

Risk Score **62**



CT Scanner

Devices **4** Profiles **1**

Risk Score **46**



X-Ray Machine

Devices **22** Profiles **8**

Risk Score **39**



VNA Server

Devices **2** Profiles **1**

Risk Score **38**



Printer

Devices **472** Profiles **10**

Risk Score **37**



PACS System

Devices **1** Profiles **1**

Risk Score **36**

Dashboard

Devices

Profiles

Alerts

Risks

Policy Sets


Applications

Network

00:50:f9:01:93:ee 




Risk Score 36 



Category Physical Security
 Profile Tyco Security Products
 Confidence Level High
 Confidence Score 99 
 Last Activity 22:06 March 01, 2021

IDENTITY


Vendor	Tyco International PLC	MAC Address	00:50:f9:01:93:ee
Model	CCURE 9000	IP Address	10.118.85.238
Serial Number	809541993	VLAN	400
OS Group	Windows	Subnet	10.0.0.0/8

Connected Switch	core1-dfw2.vmware.com 
Switch IP	10.118.80.10 
Switch Port	Po1 


Site	test
International Access	No

Risk Score 66 



Category Personal Computer
Profile PC-Windows
Confidence Level High
Confidence Score 99 
Last Activity 10:06 February 19, 2021
Internet Access Last Activity: 19:42 May 22, 2019

IDENTITY

Vendor	Dell	MAC Address	d4:81:d7:27:6d:33
Serial Number	414161267	IP Address	10.118.85.116
OS Group	Windows	VLAN	400
OS Version	Windows 10	Subnet	10.0.0.0/8
OS / Firmware Version	10	DHCP	Yes
OS Support	Yes	Connected Switch	core1-dfw2.vmware.com 
Site	test		
International Access	No		



SECURITY

Risk Score 66 
Endpoint Protection 
SMB Version V2|3

First Seen 05:23 August 14, 2020
Last Activity 10:06 February 19, 2021

! Mirai.Gen Command And Control Traffic

Severity **Critical**

Status **New**

Assignee [Assign](#)

Traffic Restricted **No**

b8:27:eb:31:10:59

Client Attacker

IP: 192.168.100.108
 Category: Embedded Systems
 Site: SJC



Port: 57722
 Protocol: unknown-tcp

185.130.215.13

Server Victim Internet

Country:RU

This signature detects Mirai.Gen Command and Control Traffic.

A deviation from the normal baseline was detected.

device profile	Raspberry Pi Device
client port	57842
threat ID	13974
threat category	spyware
threat type	spyware
number of occurrences	1
alert source	Firewall
firewall name	uk2-gcp
firewall action	Terminated the session and sent a TCP reset to both sides of the connection
firewall inbound interface	ethernet
firewall outbound interface	ethernet



Manufacturer default username and password in http login

Severity **High**

Status **New**

Assignee [Assign](#)

Traffic Restricted **No**

[New Alert Detail Page](#)

Action

10.118.80.200

Client



Protocol: http

[Hikvision-Camera](#)

Server

IP: 192.168.1.17

Category: Camera

Site: SJC

Confidence Level: High

A http login attempt was detected with a default username and password pair. The use of a default username and password pair set by a device manufacturer may be a security risk.

A deviation from the normal baseline was detected.

IoT category	Camera
IoT profile	Hikvision Camera
application	http
internal connection	true
inbound connection	true
time period (seconds)	300
default logins (username, password)	(superuser , superuser)
default login count	1
number of established sessions	1
total payload bytes	1119



Zabudnute defaultne prihlasovacie udaje

Alert Events

- Released via Cisco ISE pxGrid - test
by Dawar Hamid
04:21, August 02, 2021
- Quarantined via Cisco ISE pxGrid - test
by Dawar Hamid
04:20, August 02, 2021
- Test Note
Note entered by Eugene Vong
16:56, June 13, 2021
- Alert Detected
05:00, November 08, 2021

Crypto mining activity detected

! Cryptomining Activity Detected

Cryptocurrency is a digital currency that uses encryption techniques and blockchain technology to secure and verify transactions, and cryptomining is a way to earn cryptocurrency by leveraging mining ... [More](#)

Impact on Risk Score	■ ■
Alert Type	Miner
IoT category	Personal Computer
IoT profile	PC-Windows
application	http, TCP
remote mining servers	46.4.119.208 78.46.49.212 94.130.9.194 94.130.64.225 136.243.88.145 136.243.94.27 136.243.102.157 176.9.147.178 185.143.223.188
remote port	80, 45700
mining protocol	Stratum
mining software version	XMRig/2.6.0-beta1
outbound connection	true
external connection	true
time period (seconds)	3600
number of established sessions	106
total payload bytes	48548

More Insights ▼

+ Action ▼

Alert Events

- 19:46, March 15, 2021
- 09:32, March 03, 2021
- 09:32, March 03, 2021
- 21:09, February 28, 2021
- **Alert Detected**
06:00, April 08, 2021

Industrial devices



Category Robotic Arm
 Profile FANUC Robotic Arm
 Confidence Level High
 Confidence Score 99
 Last Activity 11:30 June 06, 2022
 Internet Access No
 Filtered IT device data No

Category Industrial Network
 Equipment
 Profile MOXA Network Device
 Confidence Level High
 Confidence Score 99
 Last Activity 13:06 November 07, 2021
 Internet Access Last Activity: 12:20
 November 12, 2020

Category Automatic Guided Vehicle
 Profile JBT AGV
 Confidence Level High
 Confidence Score 99
 Last Activity 12:30 June 06, 2022
 Internet Access No
 Filtered IT device data No

Filter Query

Entity = "device" Time Range = "week" Device Type = "All IoT" x [device] Endpoint Protection IN ("Not protected", "Outdated") x [device] OS = "Windows" x

x

Add more filters or press "Enter" to search



Robotic0CBN



Risk Score 26



Category	Robotic Arm
Profile	FANUC Robotic Arm
Confidence Level	High
Confidence Score	99
Last Activity	11:30 June 06, 2022
Internet Access	No
Filtered IT device data	No


IDENTITY

Vendor	FANUC America
Model	M-10
Serial Number	961848000
OS Group	Linux
OS Version	Linux
MAC Address	22:21:5c:62:4e:46
IP Address	192.168.10.63
VLAN	100
Subnet	unknown


Site	SJC
------	-----

Risk Score 26 




Category	Automatic Guided Vehicle
Profile	JBT AGV
Confidence Level	High
Confidence Score	99 
Last Activity	12:30 June 06, 2022
Internet Access	No
Filtered IT device data	No

IDENTITY

Vendor	JBT Corp.
Model	Forkover
Serial Number	961848085
OS Group	Linux
OS Version	Linux
MAC Address	01:21:5c:62:4e:46
IP Address	192.168.10.163
VLAN	100 
Subnet	unknown


Site SJC

SEE20060013SA 





Risk Score 41 






Category Industrial Automation
Profile Advantech Device
Confidence Level High
Confidence Score 99 
Last Activity 13:06 November 07, 2021
Internet Access Last Activity: 22:34 November 17, 2020

IDENTITY

Vendor	Advantech	MAC Address	74:fe:48:44:9a:ae
OS Group	Windows	IP Address	10.23.72.184
OS Version	Windows XP	VLAN	110 
OS / Firmware Version	XP	Subnet	unknown
OS Support	No 		
Tags	Cisco ISE > In Scope		
Site	SJC		
Countries			



SECURITY

Risk Score	41 
Baseline Modeling	 
SMB Version	V1
First Seen	05:08 May 27, 2021
Last Activity	13:06 November 07, 2021

DEVICES IP ENDPOINTS

Filter Query Domain: D industrial equipment

Devices [See All 78 Devices](#)

	00:90:e8:44:3c:b4	00:90:e8:44:3c:b4	MOXA Network Device	10.23.22.43	Explore Topology
	00:80:82:87:75:db	00:80:82:87:75:db	PEP Modular Computer	10.23.72.59	Explore Topology

Device Types

All devices

EXECUTIVE SUMMARY INVENTORY

Filter Query All Sites

Inventory Search: ciscd

Devices [See All 14 Devices](#)

	00:08:e3:ff:fd:90	00:08:e3:ff:fd:90	Cisco Systems Device	10.62.0.5	Explore Topology
	00:08:e3:ff:ff:20	00:08:e3:ff:ff:20	Cisco Systems Device	10.118.85.252	Explore Topology

42,229

Total Devices

27,361

IoT Devices

4 Critical Risk Devices

388

Applications

67

Subnets

18

Risk Score

20,136

Active Alerts to Date


98

Vulnerabilities to Date

47,580 Total IP Endpoints

Querying and searching

Show me devices vulnerable running End-of-life Windows

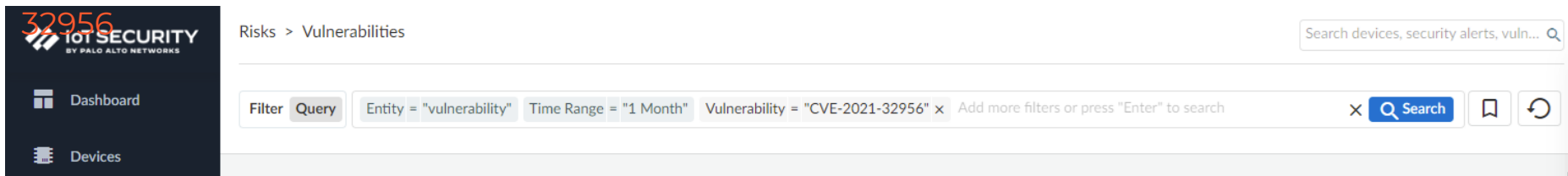


The screenshot shows the IoT Security interface with the following elements:

- Header:** Risks > Vulnerabilities
- Search Bar:** Search devices, security alerts, vuln... Q
- Filter Query:** Entity = "vulnerability" Time Range = "1 Month" Vulnerability = "End-of-life Windows OS" x Add more filters or press "Enter" to search
- Buttons:** Search, Bookmark, Refresh

Show me devices vulnerable to CVE-2021-

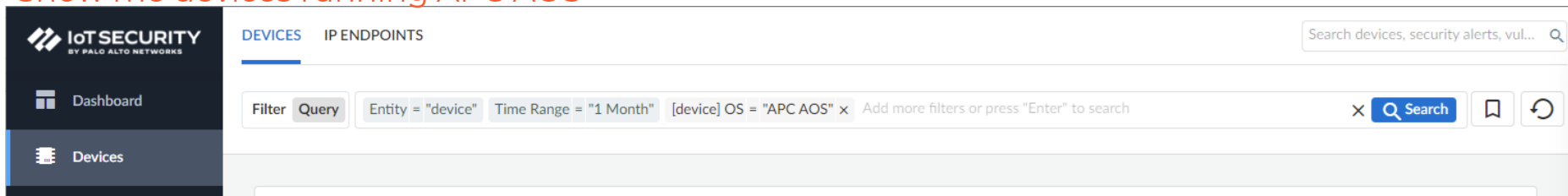
32956



The screenshot shows the IoT Security interface with the following elements:

- Header:** Risks > Vulnerabilities
- Search Bar:** Search devices, security alerts, vuln... Q
- Filter Query:** Entity = "vulnerability" Time Range = "1 Month" Vulnerability = "CVE-2021-32956" x Add more filters or press "Enter" to search
- Buttons:** Search, Bookmark, Refresh

Show me devices running APC AOS



The screenshot shows the IoT Security interface with the following elements:

- Header:** DEVICES IP ENDPOINTS
- Search Bar:** Search devices, security alerts, vul... Q
- Filter Query:** Entity = "device" Time Range = "1 Month" [device] OS = "APC AOS" x Add more filters or press "Enter" to search
- Buttons:** Search, Bookmark, Refresh

Health care devices



SJSIVUS1



Risk Score 42



Category UltraSound Machine

Profile Volcano UltraSound Machine

Confidence Level High

Confidence Score 98

Last Activity 13:06 March 25, 2021

IDENTITY


Vendor	Philips/Volcano
OS Group	Windows
OS Version	Windows XP
OS / Firmware Version	XP
OS Support	No
AE Title	SJSIVUS1
MAC Address	0c:c4:7a:02:91:e2
IP Address	10.163.23.72
VLAN	110
Subnet	10.0.0.0/8
International Access	No

MAC Address is not device



X-Ray Machine 

Risk Score 42 




Category X-Ray Machine
Profile DICOM-Imager-X-Ray
Confidence Level High
Confidence Score 98 
Last Activity 08:06 April 08, 2021
Internet Access Last Activity: 13:25 November 17, 2020

IDENTITY



Vendor	Intel Corporation	MAC Address	00:16:6f:ea:ce:32
Serial Number	23000CF3	IP Address	10.44.176.25
OS Group	Windows	VLAN	110 
OS Version	Windows 7	Subnet	10.0.0.0/8
OS / Firmware Version	7	DHCP	Yes
OS Support	No 		
AE Title	SAC_CANON_DRTAB		
Tags	Radiology		
International Access	No		
Countries			

Risk Score 42 



Category MRI Machine
Profile Siemens MRI Machine
Confidence Level High
Confidence Score 96 
Last Activity 23:06 April 07, 2021
Internet Access Last Activity: 22:44 November 17, 2020

IDENTITY



Vendor	Siemens AG	MAC Address	c8:d3:ff:ba:4c:00
Model	Aera	IP Address	10.160.214.200
Serial Number	141521	VLAN	110 
OS Group	Windows	Subnet	10.0.0.0/8
OS Version	Windows 7	DHCP	Yes
OS / Firmware Version	7		
OS Support	No 		
AE Title	ZR1FNWK4		
Tags	Radiology		

International Access Yes
Countries



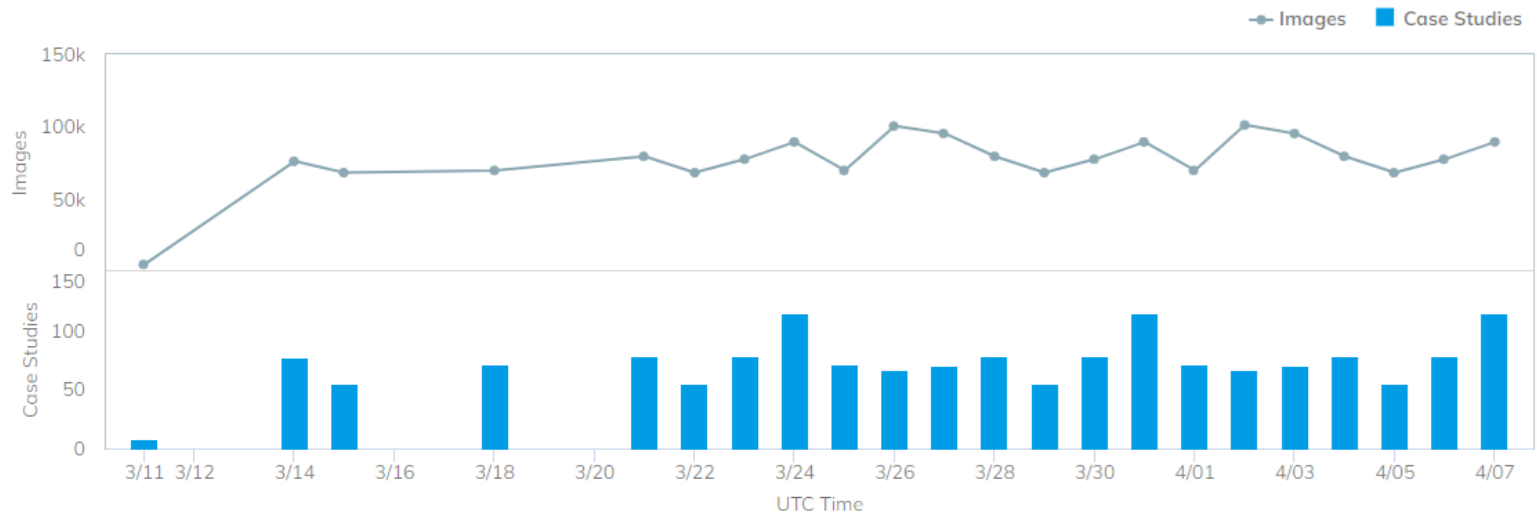
Current Behaviors 

SECURITY

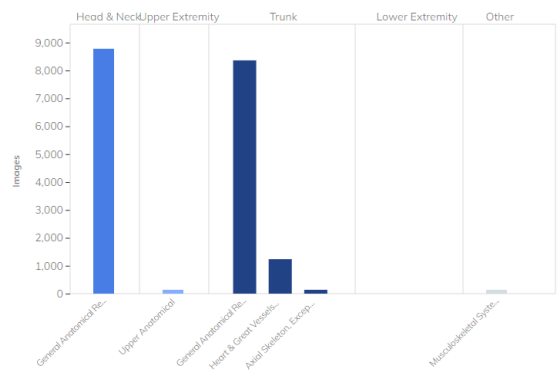
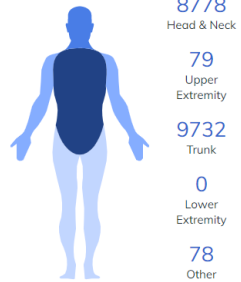
Risk Score 42 
Baseline Modeling 
First Seen 00:16 November 18, 2020
Last Activity 23:06 April 07, 2021

1,695,254
Total Images Scanned

1,583
Total Case Studies



Imaging Scan Analysis



**OT / ICS / SCADA
protocols support**

Granular Control over ICS Protocol

MODBUS

modbus
└ modbus-base
└ modbus-write-multiple-coils
└ modbus-write-file-record
└ modbus-read-write-register
└ modbus-write-single-coil
└ modbus-write-single-register
└ modbus-write-multiple-registers
└ modbus-read-input-registers
└ modbus-encapsulated-transport
└ modbus-read-coils
└ modbus-read-discrete-inputs
└ modbus-mask-write-register
└ modbus-read-fifo-queue
└ modbus-read-file-record
└ modbus-read-holding-registers

DNP3

dnp3
└ dnp3-base
└ dnp3-write
└ dnp3-read
└ dnp3-operate
└ dnp3-direct-operate
└ dnp3-confirm
└ dnp3-record-current-time
└ dnp3-open-file
└ dnp3-close-file
└ dnp3-delete-file
└ dnp3-get-file-information
└ dnp3-authenticate-file
└ dnp3-abort-file
└ dnp3-freeze-at-time
└ dnp3-freeze-at-time-no-resp
└ dnp3-cold-restart
└ dnp3-warm-restart
└ dnp3-initialize-data
└ dnp3-initialize-application
└ dnp3-select
└ dnp3-direct-operate-no-resp
└ dnp3-freeze
└ dnp3-freeze-no-resp
└ dnp3-freeze-clear-no-resp
└ dnp3-start-application
└ dnp3-stop-application
└ dnp3-save-configuration
└ dnp3-enable-unsolicited
└ dnp3-disable-unsolicited
└ dnp3-assign-class
└ dnp3-delay-measurement
└ dnp3-freeze-clear

ICCP

iccp
└ iccp-base
└ iccp-read
└ iccp-define-named-type
└ iccp-define-named-variable
└ iccp-define-named-variable-list
└ iccp-define-scattered-access
└ iccp-define- semaphore
└ iccp-delete-named-type
└ iccp-delete-named-variable-list
└ iccp-delete- semaphore
└ iccp-delete-variable-access
└ iccp-download-segment
└ iccp-get-named-type-attr
└ iccp-get-named-var-list-attr
└ iccp-get-name-list
└ iccp-get-scattered-access-attr
└ iccp-get-variable-access-attr
└ iccp-identity
└ iccp-initiate-download-seq
└ iccp-initiate-upload-seq
└ iccp-input
└ iccp-output
└ iccp-relinquish-control
└ iccp-rename
└ iccp-report-pool-sem-status
└ iccp-report- semaphore-status
└ iccp-status
└ iccp-take-control
└ iccp-terminate-download-seq
└ iccp-write

BACnet

bacnet
└ bacnet-base
└ bacnet-ack-alarm
└ bacnet-confirmed-cov-notify
└ bacnet-confirmed-event-notify
└ bacnet-get-alarm-summary
└ bacnet-get-enrollment-summary
└ bacnet-subscribe-cov
└ bacnet-atomic-read-file
└ bacnet-atomic-write-file
└ bacnet-add-list-element
└ bacnet-remove-list-element
└ bacnet-create-object
└ bacnet-delete-object
└ bacnet-read-property
└ bacnet-read-prop-conditional
└ bacnet-read-prop-multiple
└ bacnet-write-property
└ bacnet-write-prop-multiple
└ bacnet-device-comm-control
└ bacnet-confirmed-private-xfer
└ bacnet-confirmed-text-message
└ bacnet-reinitialize-device
└ bacnet-vt-open
└ bacnet-vt-close
└ bacnet-vt-data
└ bacnet-authenticate
└ bacnet-request-key
└ bacnet-read-range
└ bacnet-life-safety-operation
└ bacnet-subscribe-cov-property
└ bacnet-get-event-information

S7

siemens-s7
└ siemens-s7-base
└ siemens-s7-read
└ siemens-s7-stop
└ siemens-s7-start
└ siemens-s7-setup-communication
└ siemens-s7-check-password-set
└ siemens-s7-status-controller

IEC "104"

iec-60870-5-104
└ iec-60870-5-104-base
└ 104asdu-process-monitor
└ 104asdu-process-control
└ 104asdu-system-monitor
└ 104asdu-system-control
└ 104asdu-param-control
└ 104apci-supervisory
└ 104apci-unnumbered
└ 104asdu-file-transfer

ICS App-IDs with Function-Level Variants

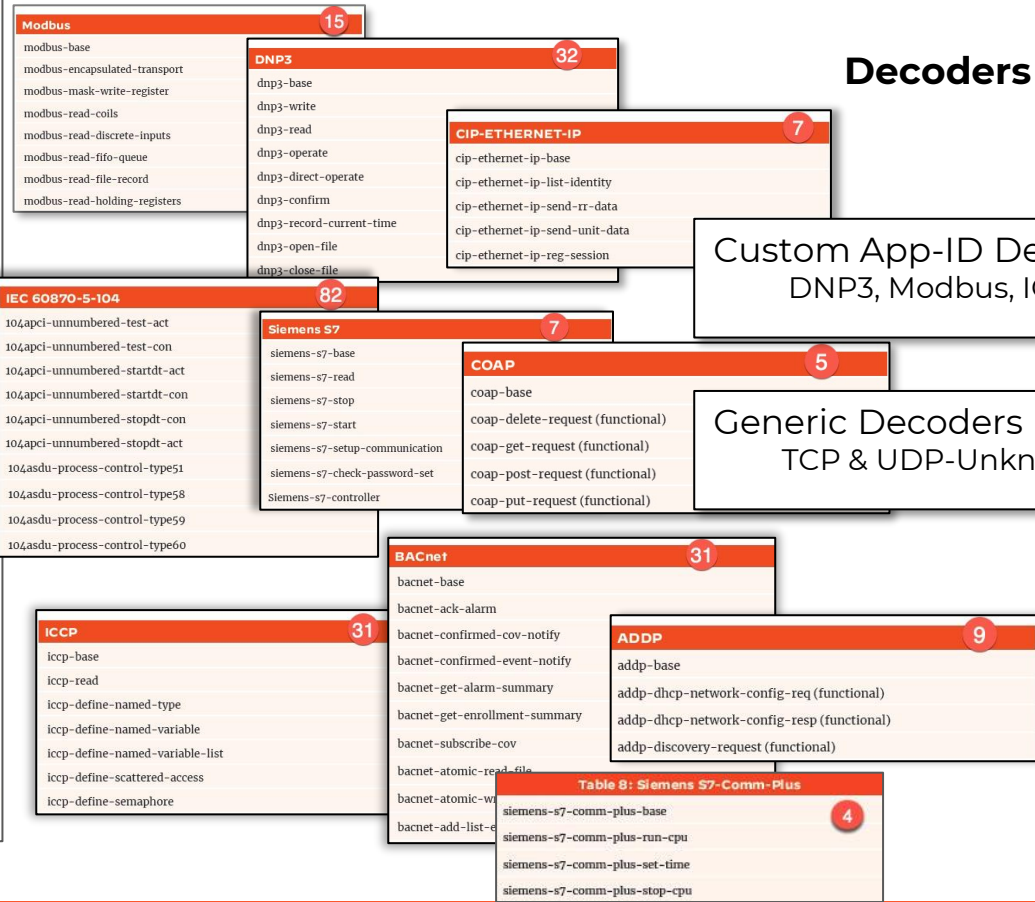
Decoders

Custom App-ID Decoders
DNP3, Modbus, ICCP

Generic Decoders
TCP & UDP-Unknown

Table 1: Base ICS App-IDs	
104 APCI	IEC 60870-5-104
ABB Network Manager	Irig-106
ABB-rp570	Modbus
ADDP	MQTT
BACnet	MTConnect
CC-Link	Net-c-x to protocols list
CIP EtherNet IP	OPC-DA*
COAP	OPC UA
Cygnnet SCADA	OSisoft PI Systems
DLMS / COSEM / IEC 62056	R-goose
DNP3	Rockwell FactoryTalk
Elcom 90	RTCM (GPS/IP)
Emerson-delta-v	RTPS
ETHER-S-I/O (esio)	Schneider OASyS
Fanuc-focas	Schneider Wonderware Suitelink
Fisher-ROC	Schweitzer Engineering SEL Fast Messaging
Foundation Fieldbus	Siemens S7-Comm-Plus
GE EGD	Siemens FactoryLink
GE-Historian	Siemens Profinet IO
GE iFIX	Siemens-P2
Honeywell Matrikon OPC Tunneller	Siemens S7
ICCP (IEC 60870-6 / TASE.2)	Synchrophasor (IEEE C37.118)

* OPC-DA is also referred to as "OPC Classic"



ICS-Specific IPS Signatures

Product-Specific



Risky Protocol Commands

Iconics Genesis SCADA CSService Integer Overflow Vulnerability

SCADA ICCP Unauthorized MMS Write Request Attempt

ID	CVE	Threat Name	Category
31673		SCADA ICCP Unauthorized MMS Write Request Attempt	info-leak
31676		SCADA ICCP COTP Disconnect Protocol Error	info-leak
31651		SCADA Modbus Server Information Fetch Attempt	info-leak
34678		GenBroker SCADA CSService Buffer Overflow Vulnerability	overflow
31677		SCADA ICCP Invalid OSI SSEL Refuse PDU	info-leak
34694		Iconics Genesis SCADA CSService Integer Overflow Vulnerability	overflow
34675		Siemens Tecnomatix FactoryLink SCADA VRN Server Multiple Buffer Overflow Vulnerability	overflow
31660		SCADA DNP3 Stop Application Attempt	info-leak
34706		Siemens Tecnomatix FactoryLink SCADA VRN Server Multiple Buffer Overflow Vulnerability	overflow
36944	CVE-2013-0699	Galil RIO 47100 PLC Denial of Service Vulnerability	info-leak
31678		SCADA ICCP Invalid OSI PSEL ACSE Abort Message	info-leak
31662		SCADA DNP3 Broadcast Request Attempt	info-leak
34695		Iconics Genesis SCADA CSService Integer Overflow Vulnerability	overflow
31674		SCADA DNP3 Warm Restart Attempt	info-leak
34676		Siemens Tecnomatix FactoryLink SCADA VRN Server Multiple Buffer Overflow Vulnerability	overflow
36925	CVE-2011-1564	IEC-104 Interrogation Command Type-identification Unknown Found	info-leak
55034		IEC-104 Interrogation Command Information Object Address Unknown Found	info-leak
34696		RealFlex RealWin Buffer Overflow Vulnerability	code-execut.
36983	CVE-2014-0779	Iconics Genesis SCADA CSService Integer Overflow Vulnerability	overflow
31670		Schneider Electric ClearSCADA OPF File Parsing Denial of Service Vulnerability	dos
		SCADA ICCP COTP Connection Request from Unauthorized Client	info-leak
		SCADA Modbus TCP server Communications Power Company Attempt	info-leak

Modbus Server Information Fetch Attempt

DNP3 Stop Application Attempt

Galil RIO 47100 PLC

Galil RIO 47100 PLC Denial of Service Vulnerability

Siemens Tecnomatix FactoryLink

IEC-104 Interrogation Command Type-identification Unknown Found

Schneider Electric ClearSCADA

Honeywell OPOS Suite

ICS-Specific IPS Signatures

Anti-Spyware



Antivirus

Threat Name	Category	Severity
Flame.Gen Command And Control Traffic	botnet	critical
Flame.Gen DNS Request Traffic	botnet	critical

Threat Name	Category	Severity
Stuxnet.Gen Command and Control Traffic	net-worm	critical

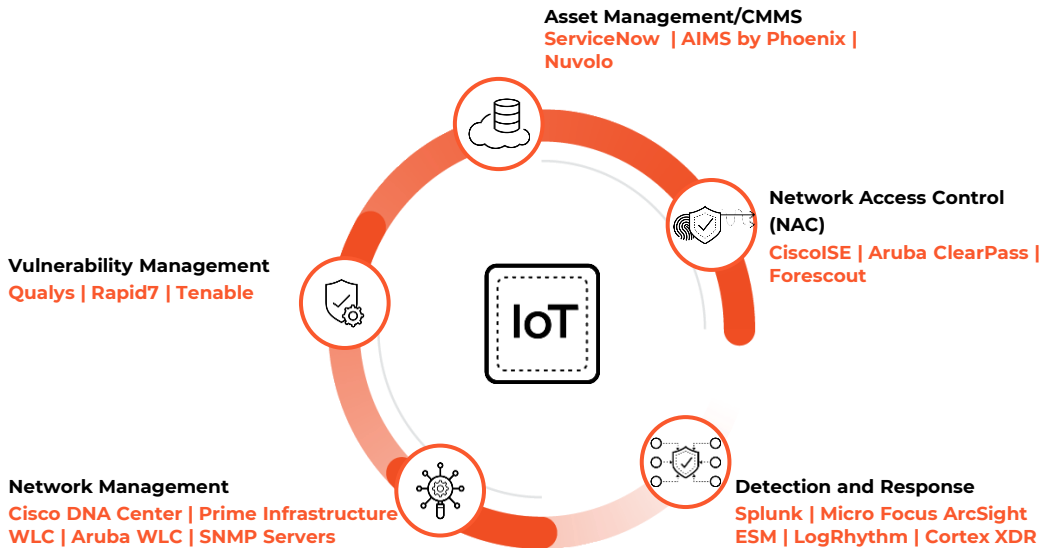
Threat Name	Category
Havex.Gen Command And Control Traffic	backdoor
Havex.Gen Command And Control Traffic	backdoor
Havex.Gen Command And Control Traffic	backdoor

Threat ID	Threat Name
3080347	Virus/Win32.WGeneric.agthtu
98468110	Trojan/Win32.karagany.jsf

Integration

Integrated Workflows

With Built-in Integrations, Unlocking the Power of Existing IT and Security Solutions



CMMS= Computerized maintenance management system
WLC= Wireless LAN Controller



Built-In Integrations

Avoid resource intensive programming with playbook-driven automation



Automate Existing Workflows

Seamlessly integrate into existing IT and security workflows



Enable New Use Cases

Locate IoT Devices, automate onboarding, microsegmentation and retirement and more



Extensive Ecosystem

Upgrade to Cortex XSOAR to enable use cases for over 700+ integrations

Deployment

Consistent Security For Industrial Deployments



Water Utilities



Electric Transmission & Distribution



Oil & Gas

PA-220R



Manufacturing



Transportation



Power Generation



Extended operating range for temperature



Certified for industrial use in harsh environments



Fan-less design, no moving parts for higher reliability



Prevention of known and unknown threats, including ICS-specific threats



Range of ICS / SCADA App-IDs supported with PAN-OS



High availability and dual DC power supplies for redundancy

Ďakujem za pozornosť