





Oct 2023 version 2.1 Contact awen@sapphire.net 0845 58 27001



Discover what's on your Industrial Control System network with <u>Dot</u>. Dot is a software system which performs Asset & Vulnerability Discovery on Operational Technology (OT), including ICS, SCADA and IIoT systems. Built using security-by-design and safety-critical scanning technology to support modern and legacy networks. Dot uses deep packet inspection and exclusive active scanning software to build a full picture of your network.



The first step in establishing an effective OT cyber security programme



Gather in-depth information about your OT assets



Accurate information on vulnerabilities, and informed risk scoring



Flexible and scalable to meet the constraints of your OT environment



Easy to deploy, reach 100% visibility of your OT assets



Gain a total understanding of your OT architecture

Book a demo

ASSET DISCOVERY

d	arch		Name	 Search-For Nos 	et 🛛 🕹	arch			Export option	ons Custom I	leids 🗘	Hide Device	T OR	Q Search For Vulnerabilitie
		e devices only v	Show OT Devices Only	Nerb	ny distar addiest: Tro	-====						JeneSys Door co	ntroller HMI	
sh	Showing 170 Devices More Information													
		Vendor	Device Name	MAC	IP Address		Pundue e	sportance		Last Seen		Property	Value	
				Accress			Level			Universitation		MAC Address	74e6x2e0567f	
			ES0 67 host	00:50:56:63		Awen Collective	Level 3 L	D.F		Expired. Reliad		Date Added (LTC)	2022 Mar 10 14:0	5.28
0Bes			NICI	:53:39		Main	units to			timestaing		Site	Awen Collective I	fain .
		VMware, Inc.	ESRI 6.7 host -	00.50.58.69		Awen Collective	(evel)	ew.		Expired. Related		Device Name	Jeneflys Door co	straller HM
		V008217, FK.	NC2	:59:05	94.126.10.62	Main	Unite 2	ANK.		timestano		Type	Human Hachine	interface
Y - 1		Richard Hirschmann Gmbh	EagleOne	00.80.63.57	10.128.70.14	Awen Collective	Level4	Low		Expired. Inicad		Vendor	Dellinc.	
		A Co	Trevali.	53.e9	6	Main	Lever a			timestano		Model.	None.	
205		Hewlett Packard	KSLAB-EWS	3c52.92.05	10.128.70.10	Assen Collective	Level 2	Low	2022 Mar	Expired. Reload		Location	None	
· .	9	Heward Packard	KSUARYWS	21.16	10.128.70.10	Main	Pane 1	Live	19 14:02:05	timestartp		Miscellaneous Notes	160/00	
		Dell Inc.	JeneSys Door controller HMI	75454240	10.128.70.13					Expired. Relato		Operating System	None	
		Ups m.	controller HMI	38/11	3	No.			16 14 03 23	tinestamp		Firmware Version	None	
		Dell Inc.	JeneSys HMI		10.128.70.13	Awen Collective	Unaffocated	Low	2022 Mar 10 14:03:28	Expired. Invited		Secial Number	Note	
	^H			36.0	2	Main			TO TRULLE	timestano Depired		Pundue Model Level	Level 2	
		Koyo Electronics	Koyo Click PLC		10.128.70.16	Awen Collective	Level 1	Low	2022 Mar 10 14/03/28	Ryload		Importance	LOW	
	\$	Inc. Co.,Ltd.		23:60	4	Main				timestano Expired		Host Recent VLAN Last Seen (J7C)		16:48:58:061994
	-	Red Lion Controls	Red Lion C09	00:05:e4.04 :43:09	6 10.128.73.39	Awen Collective Main	Level 2	Low	2022 Mar 19 14:03:2	7 Heload. timestamp		Las see long		
		Automation/Allen Bradley	Rockwell 1-Por EtherNet I/O Adapter Modul	00000000	6 10.128.783	Awen Collective Main	Level 1	Low	2822 Mar 10 14:03:2	timestemp				
		Pockwell Automation/Mier Bradley	Rockwell	N:54:33 a 50.ec	di: 16.128.70.3	Awen Collective Main	Level 1	Low	2022 Mar 10 14.03	28 Unestamp				
		Rockwell Automation/Alle Bradley	Pr Reckwell NLX-1100	00:01:73: 17:00	00: 10.128.70. 5	16 Aven Collectiv Main	Unallocate	d Low	2022 Ma 10 14 02					
awen		Rockovel & Automation/Alla Bradies	n- Rockwell Micro820	(4.54.3) 4584	94: 10.128.70	Assen 35 Collectiv Maio	e Level 1	Medium	2022 Mi 10 14/03	C Autorit	10	-		-



Automated in-depth metadata discovery about your assets including;

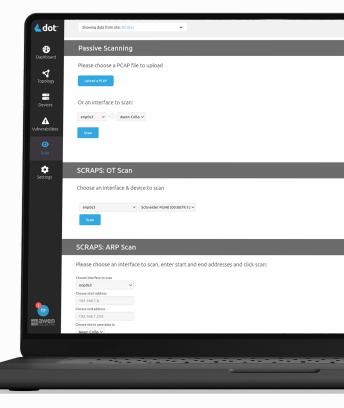
- Vendor/Manufacturer
- Model
- Type (e.g. PLC, HMI, Firewall, Switch, etc.)
- Serial Number
- Firmware Version
- MAC Address
- IP Address
- and more...

Easy to deploy. 100% visibility.



Data is discovered using passive network scanning and SCRAPS™

- Data input can be real-time or from PCAP files
- Initial discovery can be completed without any direct connectivity to your OT network, ensuring no impact to operations
- The depth of data discovered can be increased through the use of SCRAPS™ (Safety CRitical Active Protocol Scanning)
 - Targeted and validated active scanning to ensure the retrieval of valuable asset metadata without impacting the operations of a live OT environment
 - SCRAPS[™] can also be used to validate whether the data feed provided to Dot is capturing all network traffic, or if it's missing data from devices on the network



ASSET DISCOVERY

T

Easily filter and focus on the assets that matter most

- Arrange your assets by site view one or all sites at any time
- Search your assets by Name, MAC Address, IP Address, Vendor, Type, and many more criteria
- Limit your search by when traffic was last seen from a device



Export asset data

• Your data belongs to you - all asset metadata and network connectivity information stored in Dot is exportable via CSV

In depth information on assets

Se	arch	Name	✓ Search Fo	r None?	Search	Ex			
Vi	sible devices only	✓ Show OT Devices C	Dnly 📄 Fil	ter by date added:	From 📩 To 📩	1			
Sho	wing 170 Devices								
	Vendor	Device Name 🔺	MAC Address	IP Address	Site	Purdue Level	Importance	Date Added 2022 M 10 14:0	
슈	VMware, Inc.	ESXi 6.7 host - NIC1	00:50:56:63 :53:39	10.128.70.81	Awen Collective Main	Level 3	Low		
습	VMware, Inc.	ESXi 6.7 host - NIC2	00:50:56:69 :b9:88	10.128.70.82	Awen Collective Main	Level 3	Low	2022 N 10 14:0	
☆	Richard Hirschmann Gmbh & Co	EagleOne firewall	00:80:63:bf: 53:e9	10.128.70.14 6	Awen Collective Main	Level 4	Low	2022 N 10 14:0	
☆	Hewlett Packard	ICS-LAB-EWS	3c:52:82:05: 71:16	10.128.70.10	Awen Collective Main	Level 2	Low	2022 M 10 14:	
*		JeneSys Door controller HMI	74:e6:e2:e0 :9b:7f	10.128.70.13 3	Awen Collective Main	Level 2	Low	2022 / 10 14:	
☆	Dell Inc.	JeneSys HMI	74:e6:e2:e0 :9d:ff	10.128.70.13 2	Awen Collective Main	Unallocated	Low	2022 M 10 14:	
☆	Koyo Electronics Inc. Co.,Ltd.	Koyo Click PLC	00:d0:7c:12: 23:6b	10.128.70.16 4	Awen Collective Main	Level 1	Low	2022 M 10 14:	
¢	Red Lion Controls Inc.	Red Lion G09	00:05:e4:06 :43:09	10.128.70.39	Awen Collective Main	Level 2	Low	2022 M 10 14:	
¢	Rockwell Automation/Allen- Bradley	Rockwell 1-Port EtherNet I/O Adapter Module	00:00:bc:66: 20:da	10.128.70.33	Awen Collective Main	Level 1	Low	2022 / 10 14:	
¢	Rockwell Automation/Allen- Bradley	Rockwell CompactLogix 5370 L3 Controller	f4:54:33:ab: 50:ec	10.128.70.36	Awen Collective Main	Level 1	Low	2022 / 10 14:	
¢	Rockwell Automation/Allen- Bradley	Rockwell MLX-1100	00:0f:73:00: f7:00	10.128.70.16 5	Awen Collective Main	Unallocated	Low	2022 I 10 14:	
ŵ	Rockwell Automation/Allen- Bradley	Rockwell Micro820	f4:54:33:9e: a5:8a	10.128.70.35	Awen Collective Main	Level 1	Medium	2022 1	



Compatibility with many OT protocols and vendors including



Plus many IT protocols often found within OT environments including

실 do

🕕 Dashboa

> **d** Fopolo

Device Device Inerabili Scan Settings

- Siemens S5 and S7
- Ethernet/IP
- CIP
- Modbus
- Bacnet
- DNP3
- IEC 61850
- LLDP
- MQTT
- OPCUA
- Profinet
- SSDP
- Schneider Foxboro IA
- and more...

Book a demo



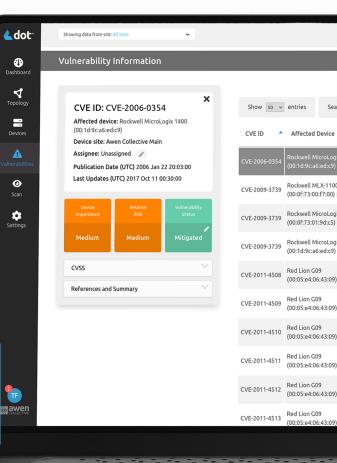
- HTTP
- ICMP
- IMAP
- POP3
- RDP
- SMB
 SMTE
- SMTPSNMP
- SSH
- and more...

See our latest protocol support list for more information

VULNERABILITY MANAGEMENT

- Accurate and verifiable vulnerability information can be discovered using your in-depth asset data
- Vulnerabilities published by vendors are identified and attributed to assets
- Vulnerabilities can be assigned to a member of your team to triage and action as appropriate
- Relative vulnerability severity scores via CVSS can be interrogated and re-calculated based on individual system knowledge
- Overall risk to your organisation is deduced based on the severity of the vulnerability and the importance of the asset (or group of assets) to your operations
- Prioritise vulnerabilities via risk to your organisation
- Links to further information and remediation advice
- Export vulnerability data via CSV
- Works in an offline environment cache vulnerability definitions for use when Dot is deployed in an offline or airgapped environment

Accurate vulnerability information and informed risk scoring



DASHBOARD

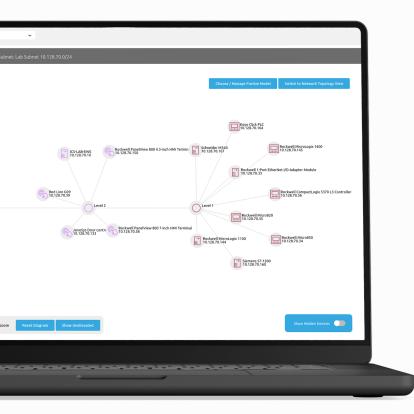
See vital statistics about your assets and vulnerabilities at a glance

PDF REPORTS

Generate PDF reports for print, directly from the dashboard.



NETWORK TOPOLOGY



- See all your assets and how they're communicating across your OT network
- Align your OT network to the Purdue Model understand how well-segregated your network currently is, and how you could improve it using the guidance of current standards

SETTINGS AND SECURITY

- Two Factor Authentication
- Granular user access controls
- User behaviour and audit logging capability

INTEGRATIONS

- SIEM/SOC centralised alerting via CEF/LEEF/Syslog
- Alerts via email
- More coming soon...

SIMPLE DEPLOYMENT

- Dot can be run in the cloud, on premise or on portable hardware
- Can be supplied as SaaS, a Virtual Machine or custom installed on hardware
- Dot has a small footprint and limited hardware requirements, ensuring costeffective deployment on affordable hardware to meet all scaling requirements

Minimum 1 core, 4GB RAM, 25GB storage; subject to bandwidth of network traffic analysed and realtime data requirements

All of this means we can design the right deployment architecture for your organisation, to get you to 100% visibility across your OT estate, no matter the complexity of your OT networks, the geographical distribution of your sites, the limited network connectivity between them, or the prevalence of legacy OT equipment.



Book a demo

WITH SUPPORT FROM





National Digital Exploitation Centre Canolfan Ecsbloetio Ddigidol Genedlaethol

Defence and Security Accelerator

Raytheon SIEMENS

GET IN TOUCH

Dot has been developed with the support of these organisations and many more. We are continuously improving our solutions capabilities, and would be more than happy to discuss your individual requirements with you. Our collaborative and consultative approach to OT cyber security will ensure 100% visibility of your assets, working around any constraints of your OT environment.

Book a demo

۲