

WELCOME TO THE FUTURE OF CYBER SECURITY

How to make SCADA protocols policies in the Application Control Blade

Shlomi Feldman SCADA/ICS Sales 05/11/17

How to make policies for SCADA protocols which support DPI:

(Modbus, DNP3, IEC 60870-5104, CIP)

- 1. Open the Smart Dashboard.
- 2. Click on the Application & URL Filtering tab.
- 3. On the left menu click on Applications/Sites.
- 4. Click to open the dropdown menu and pick SCADA Application



5. In the SCADA Application window, give a name to the application you want to create and pick the protocol you want to monitor from the protocol list. In the Unit field pick a specific or a range of PLCs unit IDs or pick any unit to monitor all the PLCs in the network. In the Function field pick any function to monitor all the protocol functions or choose the option Standard function to pick the protocol specific function. Under this option you can point all addresses or specific address or addresses range. In the value field you can pick specific values range for a specific PLC address.

SCADA Application		×		
General Properties	General Properties			
-	Name:	Black 👻		
	Comment:			
	Primary Category: 🚫 SCADA Protocols	•		
	Protocol: Modbus	-		
	Unit			
	Any Unit			
	Specified Unit ID 0 → - 0 →			
	Function			
	Any Function			
	Address Bange 0 - 0			
	Value			
	Any Value			
	○ Specified Value 0 ▲ ✓ -			
	Allow out of range values			
		DK Cancel		

- 6. Click OK to close the window and click save.
- 7. On the left menu click on Policy.
- 8. Click on one of the options to add a new policy



9. In the Applications/Sites field click on the + icon. In the search field write the name of the SCADA application you just added.

Applications/Site	s Action	Track	Install On	Time
🧓 Any Recog	🗄 🗖 Block	nol 🖴	⊡ All	Anv
	Q 🚫 Cat	egories 😜 Applications/Sites 🔇	Custom 👼 Widgets	🔀 Any R 👻 🗙
Pulse	Available (7,885)			
Pulse1	PB #hashtags	PB #hashtags		Risk: 🚺 Very Low
Modbus_Pump_	650 Plus	Primary Category: Twitte	er Clients	
Modbus_Auto Modbus_Water Modbus_Water Modbus_Water	1000keyboards 1000memories 100 1001 100bao 010 Okey Domino hakkarim.net 115	Hashtags are a community- to your tweets. They're like hashtag simply by prefixing a	driven convention for adding addition tags on Flickr, only added inline to yo a word with a hash symbol: #hashtag	al context and metadata ur post. You create a . Supported from: R75.
Any Recognized	Selected	•		
	Any Recognized	*		
		🚽 📎 Additional Categori	es: Share links Very Low Risk	Twitter Clients
	New		OF	Cancel

10. Choose the application checkbox. Please note you have the possibility to choose multiple applications. Click OK and note that the application was attached to the Policy.

pulse	Categories	Applications/Sites Subscript Custom 💀 Widgets	😸 Any R 👻 🗙
Available (6)			Risk: II Unknown
🔄 🌄 Da <mark>pulse</mark>	A		
🔽 🚼 Pulse		Primary Category: SCADA Protocols	
Pulse1			
Pulseway			
Yahoo! Pulse			
🔜 🔝 kiwi <mark>pulse</mark>			
	-		
Selected (1)			
Pulse			
00			
		Additional Categorian	
	~		
New			OK Cancel

11. Right click the action field and choose your required action for this application.



12. To conclude click save and install the policy.

How to make policies for SCADA protocols which don't support DPI:

1. Click on one of the options to add a new policy



2. In the Applications/Sites field click on the "+" icon. In the search field write the name of the SCADA Protocol you would like to use.

Applications/Sites	s Action	Track		Install On	Time
any Recog	🗄 🗖 Block	🖻 Loa		🕀 All	Anv
	Q 🚫 Cat	egories	📮 Applications/Sites	Custom 👼 Widgets	😿 Any R 👻 🗶
Pulse	Available (7.885)				
Pulse1	PB #hashtags		PB #hashtags		Risk: 1 Very Low
Modbus Pump	600 050 Plus	E	Primary Category: Twitte	r Clients	
Modbus_Auto Modbus_Water Modbus_Water Modbus_Water Modbus_all	 1000keyboards 1000memories 1001 100bao 101 Okey Domino hakkarim.net 115 	Ţ	Hashtags are a community-d to your tweets. They're like to hashtag simply by prefixing a	Iriven convention for adding additiona ags on Flickr, only added inline to you word with a hash symbol: #hashtag.	al context and metadata ir post. You create a Supported from: R75.
Log Any Recognized	Selected	*	S Additional Categoria	se • Share links Venz I ow Risk	Twitter Clients
	New	T			Cancel

3. Pick one or multiple of the protocol functions you would like to monitor. Click OK and note that the application was attached to the Policy.



4. Right click the action field and choose your required action for this application.



5. To conclude click save and install the policy.