

# User Manual InprOTech Guardian

Date: 07/2025 Doc Reference: IN-User Manual InprOTech Guardian

Version: 0.17

This document has been generated by **InprOTech** for the exclusive use of the **CLIENT** and its content is confidential. This document may not be disclosed to third parties, nor used for purposes other than those for which it was provided, without the prior written permission of **InprOTech**. In the case of delivery under a contract, its use and dissemination shall be limited to what is expressly authorized in the contract. **InprOTech** cannot be held responsible for any errors or omissions in the edition of the document.



# **INDEX**

1	Intro	oduction	6
2	First	steps	7
	2.1	Web console access	7
	2.2	Device list organization	8
	2.3	Rules configuration	.11
	2.4	Settings	.12
	2.5	Reports configuration	.12
	2.6	Continuous dashboard (optional)	.13
	2.7	Alerts exportation (optional)	.13
	2.8	Active device scanner (optional)	.13
	2.9	Analysis of Wireless devices (optional)	.13
	2.10	Licences	.13
	2.11	Access control and roles	.14
	2.12	Customized Fields	.15
3	Quic	k Guide	16
	3.1	Menu	.16
	3.2	Main Dashboard	.17
	3.3	Network Map	.18
	3.4	Device List	.19
	3.5	Alerts panel	.20
	3.6	Communications List	.21
	3.7	Reports	.21
	3.8	Parameter settings window	.24
	3.8.1	User profile	.24
	3.8.2	Security	.25
	3.8.3	Alerts notification	.26
	3.9	Settings	.27
	3.10	Help	.28
4	Appl	ication management	28
	4.1	Main Dashboard	.28
	4.1.1	Actives summary	.29
	4.1.2	Quick links	.29
	4.1.3	Network traffic graph	.30
	4.1.4	Alerts graph	.31
	4.1.5	Last reports	.31





4.2	Network map and device list	
4.2	2.1 Network map	
4.2	2.2 Device list	
4.3	Alerts panel	43
4.3	3.1 Public IP	45
4.4	Vulnerability analysis	
4.4	1.1 Vulnerabilities Panel	
4.4	P.2 Device statistics	52
4.4	4.3 Global statistics	52
4.5	Communications	52
4.6	Reports	53
4.7	Other settings	53
5 AN	INEX I: Devices and alerts classification	56
5.1	Devices classification	56
5.1	.1 According to State	56
5.2	Alerts classification	56
5.2	2.1 According to State	56
5.2	2.2 According to Severity	56
6 AN	INEX II: Asset Icons and Purdue Level	57
7 AN	INEX III: Alert icons	59
7 AN	INEX III: Alert icons	59
7 AN 1 Int	INEX III: Alert icons	
7 AN 1 Int 2 Fir	INEX III: Alert icons troduction rst steps	59 6 7
<ul> <li>7 AN</li> <li>1 Int</li> <li>2 Fir</li> <li>2.1</li> </ul>	INEX III: Alert icons troduction rst steps Web console access	59 6 7 7
<ul> <li>7 AN</li> <li>1 Int</li> <li>2 Fir</li> <li>2.1</li> <li>2.2</li> </ul>	INEX III: Alert icons troduction rst steps Web console access Device list organization	59 
<ul> <li>7 AN</li> <li>1 Int</li> <li>2 Fin</li> <li>2.1</li> <li>2.2</li> <li>2.3</li> </ul>	INEX III: Alert icons troduction rst steps Web console access Device list organization Rules configuration	
<ul> <li>7 AN</li> <li>1 Int</li> <li>2 Fir</li> <li>2.1</li> <li>2.2</li> <li>2.3</li> <li>2.4</li> </ul>	INEX III: Alert icons troduction rst steps Web console access Device list organization Rules configuration Settings	
<ul> <li>7 AN</li> <li>1 Int</li> <li>2 Fin</li> <li>2.1</li> <li>2.2</li> <li>2.3</li> <li>2.4</li> <li>2.5</li> </ul>	INEX III: Alert icons troduction rst steps Web console access Device list organization Rules configuration Settings Reports configuration	
<ul> <li>7 AN</li> <li>1 Int</li> <li>2 Fin</li> <li>2.1</li> <li>2.2</li> <li>2.3</li> <li>2.4</li> <li>2.5</li> <li>2.6</li> </ul>	INEX III: Alert icons troduction rst steps Web console access Device list organization Rules configuration Settings Reports configuration Continuous dashboard (optional)	
<ul> <li>7 AN</li> <li>1 Int</li> <li>2 Fin</li> <li>2.1</li> <li>2.2</li> <li>2.3</li> <li>2.4</li> <li>2.5</li> <li>2.6</li> <li>2.7</li> </ul>	INEX III: Alert icons troduction rst steps	
<ul> <li>7 AN</li> <li>1 Int</li> <li>2 Fin</li> <li>2.1</li> <li>2.2</li> <li>2.3</li> <li>2.4</li> <li>2.5</li> <li>2.6</li> <li>2.7</li> <li>2.8</li> </ul>	INEX III: Alert icons troduction rst steps	<b>59 6 7 7 8 11 12 12 13 13 13</b>
<ul> <li>7 AN</li> <li>1 Int</li> <li>2.1</li> <li>2.2</li> <li>2.3</li> <li>2.4</li> <li>2.5</li> <li>2.6</li> <li>2.7</li> <li>2.8</li> <li>2.9</li> </ul>	INEX III: Alert icons troduction rst steps Web console access Device list organization Rules configuration Settings Reports configuration Continuous dashboard (optional) Alerts exportation (optional) Active device scanner (optional) Analysis of Wireless devices (optional)	<b>59 6 7 .</b> 7 <b>.</b> 8 <b>.</b> 11 <b>.</b> 12 <b>.</b> 12 <b>.</b> 13 <b>.</b> 13 <b>.</b> 13 <b>.</b> 13 <b>.</b> 13
<ul> <li>7 AN</li> <li>1 Int</li> <li>2 Fir</li> <li>2.1</li> <li>2.2</li> <li>2.3</li> <li>2.4</li> <li>2.5</li> <li>2.6</li> <li>2.7</li> <li>2.8</li> <li>2.9</li> <li>2.10</li> </ul>	INEX III: Alert icons troduction rst steps	<b>59 6 7 7 8 11 12 12 13 13 13 13 13 13 13 13</b>
<ul> <li>7 AN</li> <li>1 Int</li> <li>2 Fin</li> <li>2.1</li> <li>2.2</li> <li>2.3</li> <li>2.4</li> <li>2.5</li> <li>2.6</li> <li>2.7</li> <li>2.8</li> <li>2.9</li> <li>2.10</li> <li>2.11</li> </ul>	INEX III: Alert icons troduction rst steps	<b>59 6 7 .</b> 7 <b>.</b> 8 <b>.</b> 11 <b>.</b> 12 <b>.</b> 13 <b>.</b>
<ul> <li>7 AN</li> <li>1 Int</li> <li>2 Fir</li> <li>2.1</li> <li>2.2</li> <li>2.3</li> <li>2.4</li> <li>2.5</li> <li>2.6</li> <li>2.7</li> <li>2.8</li> <li>2.9</li> <li>2.10</li> <li>2.11</li> <li>2.12</li> </ul>	INEX III: Alert icons troduction rst steps	<b>59 6 7 7 8 11 12 12 13 13 13 13 13 13 13 14 15</b>
<ul> <li>7 AN</li> <li>1 Int</li> <li>2 Fin</li> <li>2.1</li> <li>2.2</li> <li>2.3</li> <li>2.4</li> <li>2.5</li> <li>2.6</li> <li>2.7</li> <li>2.8</li> <li>2.9</li> <li>2.10</li> <li>2.11</li> <li>2.12</li> <li>3 Que</li> </ul>	INEX III: Alert icons troduction rst steps	<b>59 6 7 .</b> 7 <b>.</b> 8 <b>.</b> 11 <b>.</b> 12 <b>.</b> 12 <b>.</b> 13 <b>.</b> 13 <b>.</b> 13 <b>.</b> 13 <b>.</b> 13 <b>.</b> 14 <b>.</b> 15 <b>.</b> 16





	3.2	Main Dashboard	.17
	3.3	Network Map	18
	3.4	Device List	19
	3.5	Alerts panel	20
	3.6	Communications List	21
	3.7	Reports	21
	3.8	Parameter settings window	24
	3.8.1	User profile	24
	3.8.2	Security	25
	3.8.3	Alerts notification	26
	3.9	Settings	.27
	3.10	Help	28
4	Appl	ication management	28
	4.1	Main Dashboard	.28
	4.1.1	Actives summary	.29
	4.1.2	Quick links	29
	4.1.3	Network traffic graph	30
	4.1.4	Alerts graph	31
	4.1.5	Last reports	31
	4.2	Network map and device list	32
	4.2.1	Network map	.32
	4.2.2	Device list	.34
	4.3	Alerts panel	.43
	4.3.1	Public IP	.45
	4.4	Vulnerability analysis	.49
	4.4.1	Vulnerabilities Panel	.49
	4.4.2	Device statistics	.52
	4.4.3	Global statistics	.52
	4.5	Communications	.52
	4.6	Reports	.53
	4.7	Other settings	.53
5	ANN	EX I: Devices and alerts classification	56
	5.1	Devices classification	56
	5.1.1	According to State	56
	5.2	Alerts classification	56
	5.2.1	According to State	56
	5.2.2	According to Severity	.56



6	ANNEX II: Asset Icons and Purdue Level	57
7	ANNEX III: Alert icons	59





María Berdiales St. 20 4<sup>th</sup> floor 36203 Vigo, Spain. Tel: (+34) 886113106





# **1** Introduction

InprOTech Guardian is an asset discovery and anomaly monitoring and detection tool capable of identifying cybersecurity threats in industrial environments. It analyses network traffic, identifies assets on the network, generates comprehensive reports, and raises alerts using static rules, IDS signatures and artificial intelligence to mitigate threats in the industrial network.

The InprOTech Guardian interface is highly interactive, easy to understand and manageable. In addition, it is available in both English and Spanish.

This interface is developed using the Angular framework following best practices and security methodologies to ensure secure information navigation.

Through the InprOTech Guardian application the user will have a complete view and knowledge of the following aspects:

- **Continuous Dashboard:** self-refreshing dashboard to monitor the main aspects of assets, threats and 24x7 reporting in an operations centre.
- **Asset summary**: Visualization of the number of devices connected to the network, classified according to the **<u>PURDUE</u>** model.
- Quick access: To alerts, vulnerabilities, algorithms, and active rules.
- Network traffic graph: Graph of the traffic generated, both sent and received, in the last 24 hours and compared to the same period 7 days before.
- Alerts graph: Graph of the alerts received in the last 7 days, differentiated by colour according to their severity level and the trend they follow over time.
- Network mapping: Visualization of all network devices, how they are connected and how the organization's network is structured. It will also visualize all those devices connected and that have not been considered legitimate.
- Device manager: List of assets, wired or wireless, for identification and management. Including the identification and labelling of devices, or the inclusion of devices in the blacklist according to their criticality level Additionally, the user can define customizable fields to classify and filter the network devices, with a virtual inventory of the created fields that can be organized, filtered, and exported.
- Alert manager: List of events and alerts in the organization's OT network, classified according to their level of severity. They are color-coded and detailed with dynamic information. They will be classified according to their status (resolved and silenced), and are generated based on heuristics, IDS signatures and artificial intelligence/machine learning.
- **Integration with third party systems (SIEM)**: Guardian provides the ability to send the generated active alerts to a third-party system such as a SIEM (Security Information and Event Management), for ingest and correlation with other log sources. To do so, it makes use of the rsyslog protocol.
- Vulnerability manager: Possibility to perform vulnerability scans upon customer request and only to selected devices (under development).
- Public IP reputation: Connections to public IP addresses will be analyzed to check the reputation of that address. In case it is determined that it is an IP listed as malicious, the corresponding alert will be conveniently highlighted in the panel.
- Blocking bad traffic: In case of connections to public IP addresses considered malicious, it is possible to establish strategies to communicate with the system's







firewall and include that address in a list of filtered IPs. Among these strategies we have an informative mode, where we only report the situation, a manual mode, where the user themself blocks or unblocks the connections, and an automatic mode, where the communication with the firewall is done without human intervention (manual and automatic policies under development).

- **Communications list**: List with all the communications that have been made between OT devices in the organization's network, and information about them.
- **Report generation**: Compilation of information about the network, devices, indicators, etc., for future analysis and verification at both technical and business level.

It is important to note that in addition to the use of the application itself, the service involves a series of preparations for onboarding, which include adequate data collection, deployment, installation, and fine-tuning of the solution to get the most out of it, based on actions such as those indicated in the following section.

# 2 First steps

### 2.1 Web console access

First, access the browser and enter the address <u>http://[IP]:9000</u>, where IP is the address assigned to the management interface.

<b>TinprOTech</b>	Login Uterrome Possord Hocost Journal	
	Log in	

InprOTech Guardian Log in screen

At any time, you can select the language of your choice in the world map icon (English or Spanish).

The user must authenticate by entering the username and password assigned to him/her. In case of having the second authentication factor activated, he/she must additionally enter the single-use token received via email in his/her user email account of the service.

The user can be:





- **Admin Inprotech**: Will have access to all the information presented by the application and will be able to make the configurations he/she deems appropriate for algorithms, factory Ids, production modes, etc.

- **Factory Admin**: Access like the previous case, except for the specific configuration part mentioned above.

- **Guardian Operator**: Exclusive reading permissions user. He/she will have access to download manuals, reports and export search results and certain lists (Devices, Alerts, Vulnerabilities, Communications, Traffic Analysis, etc.).

In case the user has forgotten or blocked his/her password, he/she will have the option to recover it by clicking on the "I forgot my password" option.



Password recovery screen

When entering the e-mail address, if valid, a link will be sent to the e-mail address to reset the access password by means of a one-time use token.

\*This functionality, as well as others necessary for Guardian software updates or remote access, require connectivity between the system and certain InprOTech or internet services, so the list of rules to be applied in the firewall will be provided.

## 2.2 **Device list organization**

The list of devices must be organized by declaring the name of each device, as well as its <u>PURDUE</u> level and its status (See Annex I). By means of this declaration, the user will find it easier to identify each device in the different windows of the application, and thus be able to carry out operations on each device with greater agility, as well as to extract more value from the service.







 $\bigoplus$ on the left side of the The user must go to the list of devices by clicking on the icon screen and selecting the "Device list" tab.

٢	Guar	dian					0 ****		
ง	Ne	twork Map	List of devices	List of wireless					
€	D	evice <b>p</b>	banel (i) 587 (	f 810 Devices				۵ 🖌	+ Create device
2	All	ır ID	General search	Туре	6	Rol Purdue lev	el IP address	MAC address	Show virtual MAC Yes 🔿 No 🖲
Q	Pinne Yes	d devices	Critical devices Ves No All	Authorized devices  Yes No All	۲				
2		STATUS	NAME	ТУРЕ	PURDUE	MAC ADDRESS	IP ADDRESSES	SCORING	OPTIONS
נ	63	•00		нм		-	-		D to #
3		•00				10100-00-00-00-00	-		8
		•00				\$10.00 (\$1.00) (\$1.00)	-		8 6 8
		•00	100,000,000	HM		10100-0010-0010-0	-		8 5 8
		•00	Santana, MI	Other		10100-00-001-01-01	-		🗎 🕤 🛱
		•00				-	-		
		000				BORD 0010000	-		

Device list screen

B To be able to modify a device, we will have to click on the button and the next tab will open.

AME	SITE ID	UDP SCAN
tellen for		And includes the Manhood Streamer, which its
AC	SENSOR IDs	And the owner wanted the same
ALC: 1 10 10 10 10 10	sonda_vc	700.0010
	ROL	ICP SCAN
NAME AND ADDRESS A	Not applicable SCORING	All restores and the second second second
And and Annual Contract Contractor	MEDIUM	Second in
	SCORING DATE	And the second second second second
A/06/2024 13:13:20	05/05/2024 15:25:00 STATUS	ARE TO US OF A RECEIPTING
/PE	UNAUTHORIZED UNPINNED	
ther	UNCRITICAL	
URDUE LEVEL	LAST SCAN	
	24/05/2024 11:01:40	
ENDOR	SCAN STATUS	
termine it is a second se	SCANNING	

Device details pop-up

Then click on the button down to modify the selected device.

Name		
Device type	Purdue Level	
	Level 2	9
Pinned*	Critical*	Authorized*
Yes 🔿 No 🖲	Yes 🔿 No 🖲	Yes 🔍 No 🤇

Edit devices screen.

And manually fill in the device name, **<u>PURDUE</u>** level to which the device belongs and select its status indicating whether the device is fixed, critical and/or authorized (see definitions in Annex I).







To make massive changes in a more agile way, this configuration can be made directly in the list of assets by clicking on the padlock icon and accepting in the confirmation pop-up.

Once this has been done, the "Save" button is clicked to make the changes effective in the system.





María Berdiales St. 20 4<sup>th</sup> floor 36203 Vigo, Spain. Tel: (+34) 886113106 page 10



www.inprosec.com info



## 2.3 Rules configuration

The Guardian system performs threat detection based on multiple behavioural criteria, such as:

- Threats based on predefined parameterizable rules
- Threats based on IDS signatures
- Threats based on AI/ML algorithms
- Honeypot threats

The user must configure which rules he wants to be operational for the analysis of his organization's network, as well as the time ranges to bypass each of the alarms if he deems it appropriate. This would be done in mutual agreement with InprOTech in the onboarding; in principle, the user will only see the rules and thresholds but will not be able to edit them.

The time range to bypass a rule means that we can set a threshold or time in which the established rules will not generate an alert in an identical scenario, and thus avoid unnecessary warnings and alerts of which we are already aware.

Additionally, other parameters can be configured. These will be detailed later. To configure these time ranges, click on the left menu button on the screen and click on Threat Detection > General > Rule-based threats, VIEW STATUS.

C	Guardian	Admin Last access 03/07/2025 2228.40	[→ <u>Log Out</u>
ណ	Settings		
⊕ ∧	PROFILE	General <b>status</b>	
6	THREAT DETECTION	Status of detection mechanisms $^{(j)}$	
유 []	NETWORK  Traffic Blocking  ADVANCED	Rule based threats	
ŝ	段 General 볼 Preferences	SHOW STATUS SHOW STATUS	

#### Status screen detection mechanism

R	ules engine ① GRutes			<b>B</b>
	NAME	STATUS	THRESHOLDS	OPTIONS
۲	New device	Production	15 (j)	Z
۲	New connection	Production	15 🕠	Z
۲	Network port anomaly	Production	15 (j)	Z
۲	New public IP	Production	15 🕠	Z
۲	Possible fingerprinting	Production	5-3-3 (j)	L
۲	Possible ARP spoofing	Production	1 (j)	2

Rules engine screen



María Berdiales St. 20 4<sup>th</sup> floor 36203 Vigo, Spain. Tel: (+34) 886113106





In the threshold's column, we can quickly see the thresholds configured for each rule.

THRESHOLDS	OPTIONS
15 (1)	L
15 (1)	L
15 (1)	R
15 (1)	R
5-3-3 (i)	L
1 (1)	L



In the actions column we can edit these parameters.

15	
Statue	
Detecting	
Required fields	
	Save

Rules edit screen.

In addition, this section will include, once available, the configuration of the messaging associated with notifications of alerts that you wish to receive, and reports.

### 2.4 Settings

Basic settings for user profile data, security settings, and alert notification preferences can be found in the Settings section of the Quick Guide. It is recommended to review and adapt them to the environment needs.

### 2.5 **Reports configuration**

Now, reports are generated automatically on a weekly basis.







# 2.6 Continuous dashboard (optional)

If you are interested in being able to permanently consult the status of Guardian and the main associated indicators (unauthorized devices, network traffic, alerts, etc.), you can have the main Guardian dashboard on a monitor in your operations room with auto-refresh every 5 minutes.

To do so, contact your Guardian Support and request the creation of a Monitoring user.

# 2.7 Alerts exportation (optional)

If the customer wishes, he can contact his Guardian Support to enable the automatic sending of the generated alerts to a syslog server of a SIEM or similar, for their ingestion and correlation\* with other log sources.

The only thing you need to provide is the IP and port to which you want the messages to be sent.

\* For this purpose, it is important to note that all dates returned by the web application are shown in UTC time.

# 2.8 Active device scanner (optional)

Guardian Support can be contacted to enable the active device query engine to obtain additional properties of the nodes (firmware version, open ports and services running on them, among others).

See the Devices Scanner Section within Application Management for more details.

# 2.9 Analysis of Wireless devices (optional)

If traffic collectors have the appropriate hardware for it, Guardian Support can be contacted to enable scanning of Wireless devices in the vicinity.

Refer to the Wireless Device List section within Application Management for more details.

### 2.10 Licences

This will allow to provide the Guardian Service on a temporary basis only, so that it can be provided for testing purposes limiting the usage time window.

If you see the message **"License error. Contact support."**, means that the license files are missing or the license has expired.









# 2.11 Access control and roles

This feature allows control of user access and actions performed in the system. The implementation of this system provides an additional layer of security and privacy in the handling of information and system resources.

This role and access control system has the following features:

- **Predefined roles and permissions:** different predefined roles and permissions can be established in the system, which will be granted to determine their levels of access and control in the system.
- **Assignment of permissions to users and groups:** the system allows assigning permissions to users and groups according to their roles and responsibilities in the organisation.
- **User group management:** users' groups should be established to allow the assignment of permissions to multiple users at the same time, which will facilitate the management of permissions.
- **Resources access control:** the system will allow control of access to different Guardian resources by assigning specific permissions.

The roles to be implemented will be as follows:

- **INPROTECH:** Full access is granted to configuration, service operations, logs, etc., including the ability to transition between training and production environments, and modify AI algorithm sets as needed.







- **ADMIN:** Factory's privileged user mode, changes can be made to the visible data on the frontend, such as device data, and alerts can be marked as resolved or muted.
- **OPERATOR:** standard factory user mode, permissions are more restricted. Users can only view data and download reports or CSVs.

## 2.12 Customized Fields

If the user believes any new fields can be added to the device list to allow for their better categorization, they can define them on a key-value format using a ".csv" file.

Just add a new file from the **b**utton on the device panel, including the devices we want in the rows along with the new customizable fields in any of the formats explained in section 4.2.2.1.

The user can check the loaded fields from the device panel by either clicking on the link

'Show fields' on the devices with any fields configured or on 🗈 'Device Details' and then continuing by clicking the 'Customized fields' button.

Device **Details** 

This action will open a new modal that allows the user to view them.

Customized Fields	<b>〈</b> Go to details
Operario: "RS" Label: "01-U"	
Close	







# 3 Quick Guide

# 3.1 **Menu**

K	Guardian
ណ៍	Dashboard
$\oplus$	Network
	Alerts
<b>@</b>	Vulnerabilities
몲	Communications
Ľ	Reports
තු	Settings
i	Help

Access window detail

- 1: Home: Main Dashboard
- 2: Network: Network map and device list
- 3: Alerts: Alerts list
- 4: Vulnerabilities: List of vulnerabilities
- 5: Traffic Sessions: List of inter-device communications
- 6: Reports: List of automatic reports
- 7: Settings: Parameters setting window
- 8: Help documentation







# 3.2 Main Dashboard

K	Guardian		•	Admin_2 ast access: 08/10/2024 16:15:00		[→ <u>Log Out</u>
ធ	Welcome Admin_2			0	Unauthorized de	evices 737
	Hardware assets summary 🕕	VIEW ALL	Network traffic 🚯	Last update 9 oct 2024	110:38 C VI	EW DETAIL
	Purdue Level unassigned	*	10 MB	TX	RX • TX -7d	• RX -7d
٩	• • •		5 MB			
器	10 PLC 32 HMI 514 NI 31 Other		0 MB <b>10:00 12:00 14:00 16:00 18</b>	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	04:00 06:00	08:00 10:00
ß		*	Alerts (i)	Last update 9 oct 2	2024 10:38 C <sup>#</sup>	VIEW ALL
廢	Shortcuts					
	7 Active Algorithms +99 Activ showLust showLust	s []	0			
			Latest reports 🔅		[	VIEW ALL
	6 Active Rules 64 Active Vulnero	abilities	24/09/2024 02:58:00	report_UnauthorizedDevices	_20240924T0058.cs	i¥.
i	SHOW LIST SHOW LIST		24/09/2024 02:58:00 24/09/2024 02:58:00	report_Alerts_20240924T00	58.csv 10058.csv	

Main dashboard view

#### Top bar:

Type of session and date of previous access

Change application language.

Log out from logged in session.

Unauthorized devices counter.

#### Top left widget:

Number of assets in the organization sorted by <u>Purdue</u> model.

#### Top right widget:

Graphical representation of network traffic sent and received in bits/sec the last 24 hours, and comparison with respect to the same magnitude just 7 days earlier.

#### Lower left widget:

Shortcuts to listings

Active vulnerabilities (under construction)

#### Bottom right widgets:

Graphical representation of number of alerts according to their severity.

Access to list of generated reports







## 3.3 Network Map

The network map presents two topology views: classic network, or by <u>PURDUE</u> levels.

In th	e first case:									
T	Guardian					2	Admin_4 Last access: 03/10/		÷	[→ <u>log Out</u>
ធ	Network Map	List of devices	List of wireless							
•	Network	map 🖲 💷	ated: 09/10/2024 10:41						76	Q Show
	Sensor ID	9/10/2024	■ 10:41 Ø	Network topology Standard	Protocol	IP ac	ldress	Port	Show virtual Yes 🔿 No 🤅	MACs
6										
율							2			T
C				1						
(\$)										
				1						
				?						(+) (-) -'+'
i										~ ~ 11

Network map window in classic view.

At the top, there is a tab to select the network map view, the date of the last update of the graphical representation of the topology, as well as a button to make the filters entered effective.

The next row shows the possible filters to view the devices of interest on the screen.

Below, we already have the map and topology of the organization's network devices.

Note that:

- By hovering with the mouse, you can see the properties of a node or a link.

- By clicking on them, you can go to the detail view and edit device properties, or to the filtered communications section for that link source, respectively.

In the <u>PURDUE</u> view of the topology, the communications compliance is analysed based on the ISA/IEC 62443 standard. The warnings are classified as **high severity** (communications type, indicating the existence of communications between nonadjacent levels), **medium severity** (PURDUE level assignment to device types that seem questionable) or **low severity** (no level assignment and/or recommendation of manual review for certain device types).







3	Guardian	Admin_4 Last access: 03/10/2024 12:38:20	[→ <u>Log Out</u>
ភ	Network Map List of devices List of wireless		
•	Network map (1) Updated: 09/10/2024 10:41	<b>7</b>	Show
	Sensor ID         Datetime         Network topology           All	Protocol         IP address         Port         Show virtual MAC           Image: Constraint of the state of t	S
<b>(</b>			(i) X
器	Nivel 2	Warnings Level 2	~
C Ø		Warning severity HIGH (with level unassigned)  C powce for the public level 2 is communicating with  In PURDUE level unassigned. Usually communications are only allowed between adjacent levels	^
	Nivel 1	Warnings Level 1	~
		Warning severity LOW	~
	and a set of a set of a set of a	Warnings Level unassigned	^
i	Nivel 0	Warning severity LOW	~

Network map in PURDUE view.

Note that in the graphical version (left side of the window):

- Only communications between distinct levels are shown, not those between devices of the same level.

- It is indicated with triangular icons under the image of the device, if it is affected by any regulatory compliance warning. The colours are red, orange and teal, and represent high, medium, and low severity warnings, respectively.

- The devices can be clicked to filter the warnings on the right-hand side that apply to the node in question. If the filter is unchecked, all the detected devices are displayed, in descending order of levels and severity.

The rest of the filtering capabilities are the same as in the classic view, and on the right side of the window, as mentioned above, the global warnings or those associated with a selected device are listed.

### 3.4 Device List

K	Guar	dian					Admin_4 Last access:		⊕ Log Out
ធ	Ne	twork Map	List of devices	ist of wireless					
۲	D	evice	panel (1) 359 of 69	5 Devices				۵ 🖗	+ Create device
	All	or ID	General search	Туре	6	Rol Purdue le	evel IP address	MAC address	Show virtual MACs Yes No 💿
٩	Pinne Yes (	d devices	Critical devices	Authorized devices Yes No All	۲				
**	8	STATUS	NAME	ТҮРЕ	PURDUE LEVEL	MAC ADDRESS	IP ADDRESSES	SCORING	OPTIONS
Ľ		•00						LOW	8
ŝ	2	•••				101103-0017-001-001		+1 LOW	
		•00				10100-0010-00-001		LOW	
		•00	ingrames.	Other	2	10.00171-00171-008		MEDIUM	
		•00	(regression)	Other	2	10.00.00.00.00		MEDIUM	
	2	•00				101000-00-00-00		MEDIUM	
	18	••0	Street, Million, providence.	Server	2	1010101-1010-00F		+515 MEDIUM	8 🗢 🗊
	<	••••				ARRANGE.		1014	فاتات

Device list window







In the tab to select the view of the list of devices registered in the network, the number of devices with the current filter applied versus the total number of devices in the database is displayed next to the panel title. On the right side, the button panel for deleting previously applied filters, exporting the list of devices in CSV format, and manually registering a device in the application.

The next row includes the possible filters applicable to keep the devices of interest.

The list of assets itself with information about them, and buttons to perform certain actions (view details, edit them, delete them, or access alerts, communications or vulnerabilities present, the latter pending development). It is possible to sort the devices alphabetically directly or inversely by clicking on any of the columns.

The third tab contains the inventory of wireless devices detected in the vicinity of the traffic collectors (if compatible hardware is available and the functionality is enabled by Guardian support staff).

) G	Guar	dian					Admin_4 Last access: 03/10/202	24 12:38:20	N [→ <u>Log</u>
	Ale	erts Panel							
		erts <b>pc</b>	anel 🕚 117566 of 1175	566 Alerts				76	+ Create alert
	Senso	r ID	General search	IP address	MAC address	Start datetim	• •	End datetime	•: O
	Severi	ty	Category	Show resolved Yes No All	Show silenced Yes No All	•			
		SEVERITY	NAME	SOURCE MAC	DESTINATION MAC	SOURCE IP	DESTINATION IP	DATE	OPTIONS
	-	EMERGENCY	Possible ARP spoofing	-	***	-	SCHOOL SECTION.	09/10/2024 13:08	
	-	EMERGENCY	Possible ARP spoofing	second and		-	-	09/10/2024 13:07	
	-	EMERGENCY	Possible ARP spoofing	41708031044	*****	-	-	09/10/2024 13:07	
	-	WARNING	New connection	more thank	****	-	-	09/10/2024 13:07	
	-	WARNING	New public IP	motoriante (		-	-	09/10/2024 13:07	
	-	EMERGENCY	Possible ARP spoofing	-	-	-	-	09/10/2024 13:05	
	-	EMERGENCY	Possible ARP spoofing	-		-	-	09/10/2024 13:04	
		DIEDODION	Possible APP spoofing	-	-	-		09/10/2024 13:02	

# 3.5 Alerts panel.

Alerts list explanatory window.

Next to the section title, the number of alerts in the organization's network (filtered vs. total) is displayed. On the right side, there is a button panel for deleting the set filters, exporting the list of alerts in CSV format, or manually creating an alert in the application.

The next row includes the possible filters to view the alerts of interest on the screen. Note that the general search field is of type CONTAINS and allows to perform searches on the internal notes field of the alert, visible in Details.

Finally, we have the list of alerts with associated information and buttons to perform actions on them (status updates\*, access to detail and addition of notes).

As you can see in the image, if a device has a name assigned to it, next to the MAC we can see an exclamation mark which, if we place the cursor over it, will show us the name assigned to that MAC address.

\*To check the status change options, see definitions in Annex I.







## 3.6 **Communications List**

Communications, understood as a grouping of connections between MAC, IP, and source port, and the same at the destination. Unbundled if there is a change of protocol.

3	Guard	ian <sup>OTech</sup>				admin Last access: 07/10/2024 10:43:06		<u>Out</u>
ធ	Com	munications						
•	Cor	mmunication	s panel () 22 of 22	Connections			▼ ●	
	Sensor ID	IP addres	s MAC address	Port	Protocol			
٩		SOURCE MAC	DESTINATION MAC	SOURCE IP	DESTINATION	P DESTINATION PORT	PROTOCOL	
		-	-	and the second	-	53	UDP	
ß	00	-	-	-	And the Party of t	137	TCP	
~	88	1010/1010/001011	101110-0010-00	-	10000	137	UDP	
\$	56	Margin Street and Col.	Manufacture and	sources.	and the second	137	UDP	
	88	Magnetic Street, St.	101712-0110	STOCKED.	Statute of	53	UDP	
	00	Bear Statements	Man manufacture of	10000	All Street of St	53	UDP	
	80	Bear 10, 81, 10, 11	B107102-0100	10000	and the second	5353	UDP	
	80	Bear Statements	Reprint and the second	Real Property lies	10000	53	UDP	
	88	-	10.40 - 00.000 P 11.0	and the second	ADD DO	5353	GRE	
i							•	٠

#### Communications list window.

In this section, the number of devices with the current filter applied is shown next to the title, compared to the total number of devices in the database. On the right side, the buttons to remove the set filters and to export the list of connections in CSV format, respectively.

In the next row, there are the possible filters to view the connections of interest on the screen.

Finally, the list of connections with information about them. It is possible to sort the communications alphabetically, either directly or inversely, by clicking on any of the columns.

### 3.7 Reports

This section will allow downloading reports of several types, automatically generated by the system. As of today, Guardian generates weekly reports on Monday mornings, with downloadable files in CSV format, with the following information:

- Unauthorized connected devices:
  - o Name: Name of the device
  - MAC of the device
  - Vendor: Manufacturer
  - o Role: Role
  - o Discovery date: Date of discovery
  - o Ips





- Purdue level
- Fixed (Y/N)
- Critical (Y/N)
- Device type
- Score and score timestamp.
- Scan status and last scan.
- o Vulnerability risk number
- o Vulnerability risk label
- **OS**
- Blocked (Allowed/Not allowed).
- $\circ \quad \text{Customized field} \quad$

- Last detected alerts:

- o ID
- o Title
- Category
- Severity
- Silenced
- Resolved
- o Value
- Source IP
- Source ID
- Destination IP
- Destination ID
- o Protocol
- Creation date
- Location (City / Continent / Country / Latitude /Longitude...)
- o Hostname
- o IP
- Source device (name / type)
- Destiny device (name / type)
- o Creator
- MAC-IP associations:
  - o MAC
  - Associated IP
  - Vendor: Manufacturer
  - Public IP: Whether it is public or not.
  - Discovery date: Date and time of discovery
- Public Ips (External IPs connected):
  - IP (source/destination)
  - MAC (source/destination)
  - Discovery date
- Risk Score Report (scoring)
  - o Name
  - o MAC
  - o Manufacturer
  - Individual score

María Berdiales St. 20 4<sup>th</sup> floor 36203 Vigo, Spain. Tel: (+34) 886113106





- Date of scoring
- Overall factory score
- Overall cloud score
- Wireless devices
  - o IP
    - o MAC
    - Connection type
    - Authorized (Y/N)
    - Device type
    - o Channel
    - Signal power
    - o AP Mode
  - Frequency Band
- Vulnerabilities
  - o MAC
  - o IP
  - o CVE
  - o Status
  - Source
  - Discovery Date
  - o Last Seen
  - o Port
  - o CPE
  - Criticity
  - Description
  - Timestamp published.
  - o CWE
  - o URL

If the device has the label Name reported, it will replace the MAC field in the alert's reports. On the other hand, in manual downloads of user searches from the alerts panel or the device list, the "Latest reports" section will display both fields independently.

The user will be able to download the latest generated reports from the main Dashboard shortcut.









#### Latest reports on main Dashboard

Additionally, Guardian has its own section dedicated to Reports, where you can use the search engine to filter and download the report of interest:

K	Guardi	an Tech	Adr	nin_2 access: 04/10/2024 10:46:40	[→ <u>Log Out</u>
ធ	Report	S			
$\oplus$	Rep	orts panel (1) 7 of 7 Reports			76
	Туре	Start datetime           Image: Constraint of the start datetime           Image: Constraint of the start datetime	End datetime		
Q		FILE TYPE	CREATION DATE	FORMAT	OPTIONS
몲	Ľ	Unauthorized devices	24/09/2024 02:58	CSV	<u>الله</u>
ß	C	Alerts	24/09/2024 02:58	CSV	Ł
សា	C	MACs & IPs	24/09/2024 02:58	CSV	Ł
~	Ľ	Scoring	24/09/2024 02:58	CSV	<u>ځ</u>
	C	Public IPs	24/09/2024 02:58	CSV	±
	ß	Wireless devices	24/09/2024 02:58	CSV	<u>ا</u>
	Ľ	Vulnerabilities	24/09/2024 02:58	CSV	<u>ا</u>
i					

Report list view.

Next to the title, the total reports generated are shown, and to the right the filter reset button.

In the next row, we have the different search filters.

Finally, there is the grid with the reports available CSV format for downloading.

### 3.8 Parameter settings window

In this section we can adjust our profile or the service, modify some parameters related to threat detection, or different configurations of alerts, threats, and user management.

The most relevant aspects at user level are summarized below.

### 3.8.1 User profile

This section displays basic information such as username, associated email, date and time of last and current connection, language preference (EN/ES), and contact telephone number. The last two are editable by the user.

The user can reach it from "Settings" on the left side Menu.







K	Guardian			Admin_4 Last access: 05	9/10/2024 13:41:40	¢	[→ <u>Log Out</u>
ය ⊕	Settings	Profile <b>data</b>					
ک اٹ	User THREAT DETECTION C General ADVANCED C General	User Admin_4 Email	Language EN Current login	Ø	Phone number		
<mark>ت</mark> ه	▲ Preferences	Session token lifetime (minutes)	10/10/2024	15:10	9/10/2024	13:41	
						Save	
i							

#### User profile view

#### 3.8.2 Security

In Advanced > Preferences, in the 'Security & MFA' section, we can indicate whether we want to activate the second authentication factor as an additional (recommended) security mechanism to prevent identity theft. In this case, after identification with username and password, we will be invited to enter a single-use token that we will have received (initially by email).

K	Guardian			Admin_4 Last access: 09/	10/2024 13:41:40		[→ Log Out
ធ	Settings						
⊕ ∧	PROFILE	User <b>preferences</b>					
٩	THREAT DETECTION	Security & MFA					
器	ADVANCED	Enable Yes No ()	Method				
ß	ter Breferences				_		_
សា						Save	
~							
		Alerts notifications					
		Enable	Method	Minimal	severity		
		Yes 🔿 No 🖲	Email	Notice			
		Verbose info	Periodicity	Static ru	les		
		Verbose	Instant	Ves 🔿	No		
		IDS	IA/ML				
		Yes No	Yes No				
							_

Security & MFA view

Remember that as access control method, a role-based mechanism has been implemented, by means of which there are groups of permissions associated to three user levels:

- InprOTech Administrator
- Plant Administrator
- Plant operator





The assignment of roles to users cannot be managed directly by your organization but is defined with InprOTech at the time of deployment of the solution. Contact us for further information.

### 3.8.3 Alerts notification

In case it is considered appropriate, initiative-taking alerts can be configured to generate alerts in the system. The alerts and warnings are generated based on the detection of anomalies according to the different strategies implemented in Guardian (heuristics, IA/ML, IDS, Honeypot, manuals...).

This allows Guardian to warn of potential incidents, instead of having to periodically go to the web interface to check if events have been generated.

The user will therefore be able to:

- Decide if he/she wants to receive security alert notifications.
- If so, from what severity threshold they will be sent to the user.
- What type of alerts (heuristics, IA/ML, IDS, Honeypot, all...)
- In what format

Alerts notifications

- Individual: one notification per alert
- Grouped: a daily notification with the summary of all alerts, selectable from Monday to Friday or from Monday to Sunday.

- If individual, whether summary or verbose format is desired.

Enable	Method	Minimal severity	
Yes 🔿 No 🖲	Email	Notice	$\bigtriangledown$
Verbose info	Periodicity	Static rules	
Verbose	Instant	✓ Yes ● No ○	
IDS	IA/ML	Honeypot	
Yes 🖲 No 🔿	Yes 🖲 No 🔵	Yes 🔿 No 🖲	

Alerts notification view

For the time being, notifications will be sent via email to the user's account.

Important:

- Alert notification must be enabled in the backend to allow the user to enable proactive sending.

- In case that with the established conditions too many alerts are generated per time unit, the functionality will be auto-disabled for security (previously informing via email to the user about this circumstance), so that other more demanding notification sending conditions (of lower volume of events) can be selected.

A couple of examples of alert notifications with different formats are shown below:







Soporte Guardian Para $ \begin{array}{c c}  & & \\  & &$
A new alert has been generated in the severity level system: emergency
Creation date: 28/07/2023 20:34:42 +0000 Type: STATIC Name: Possible ARP spoofing Src MAC Dst MAC: Src IP: Dst IP: Value:
Access the alert for its management in Guardian.
Once managed, if applicable, proceed to silence or resolve it to avoid unnecessary noise. For more information, consult the alerts playbook or the user manual in the reference documentation.
Remember that you can modify your preferences for receiving notifications, their level of severity, format and periodicity, from the user settings.
InprOTech Guardian Support Team https://inprotech.es/
Summarized individual alert notification example.

Daily summary of al	orte fe	om Nombro I	Tabrica													
Daily summary of an	erts in	omnombrei	abrica													
Soporte Guardia	n											Responder	(f) Responder a todos	-> Reenviar	<b>1</b> 36	-
Para														mi. 26	6/07/2023 1	074
																1
On 26/07/2023 15:13:50 +00	00, 50 ne	ew alerts have bee	n generated in the	system in the last 24	hours.											
Summary:																
										-						
Creation date	туре	Name	Src MAC	Dst MAC	Src IP	Src Type	Dst IP	Dst Type Probe	Protocol	Description	Value	1				
19/10/2018 06:44:55 +0000	STATIC	New IP	2010/10/2010	an Principalities	15,081.00		175.06.0.02	sonda1	6	New IP discovered	119-14-130					
19/10/2018 06:44:56 +0000	STATIC	New connection	Statistics and state	echtlechtlich in	171.161.00		170.162.12	sonda1	6	New connection discovered	1462					
19/10/2018 06:44:56 +0000	STATIC	New IP	1048-010-0-0010	ec/1016/01/10124	111.081.00		101010-04	sonda1	6	New IP discovered	170,053,40	1				
19/10/2018 06:44:56 +0000	STATIC	New connection	search index	41.75.56.0° (0.04	10.000.000		375.96.3.46	sondal	6	New connection discovered	1940	1				
19/10/2018 06:44:56 +0000	STATIC	New IP	104070-0404	et. Notes in the lat	170.06.048		170.06110	sonda1	1	New IP discovered	175,000,040	1				
19/10/2018 06:44:56 +0000	STATIC	New connection	property and in a	#1763#1010#10	111-10-1-00		11009-040	sondal	1	New connection discovered	NA					
19/10/2018 06:44:56 +0000	STATIC	New IP	Real Property lies	ex. Philes. 27-35, 14	210.061-00		170.083.03	sonda1	6	New IP discovered	100,084130	i i				
19/10/2018 06:44:56 +0000	STATIC	New connection	NUMBER OF CONTRACTS	100 million (1990) (19900) (19900) (1990) (1990) (1990) (1990) (1990) (1990) (1	111.04(1.00)		275.58.5.10	sondal	6	New connection discovered	1958	i				
19/10/2018 06:44:56 +0000	STATIC	New IP	No.45-Tel: Suiteria	an Malani I da un	170.080.085		170.064-08	sonda1	6	New IP discovered	070.064.02	1				
19/10/2018 06:44:56 +0000	STATIC	New connection	1040 for carding	and the local different little set	175,183.60		15440.00	sondal	6	New connection discovered	199					
19/10/2018 06:44:55 +0000	STATIC	New IP	NUMBER OF TAXABLE	ec. Writes 27 Mills Sal	110,080,000		170.060.11	sondat	6	New IP discovered	170.063.01	í.				
19/10/2018 06:44:56 +0000	STATIC	New connection	periorita bellete	and the part of the	279-384-30		175.56.5.55	sondal	6	New connection discovered	200	6				
19/10/2018 06:44:56 +0000	STATIC	New device	*******	*****				sondal	17	New device discovered	*****	1				
19/10/2018 06:44:56 +0000	STATIC	New IP	and the second	0.0.044.0	175,080,05	İ	810.00	sondal	17	New IP discovered	170.083-00	1				
19/10/2018 06:44:56 +0000	STATIC	New IP	******	******	101.08.0.04	1	4554	sondal	17	New IP discovered	6205					
19/10/2018 06:44:56 +0000	STATIC	New connection	******	-	175.08140		40.00	sondal	17	New connection discovered	392	1				
19/10/2018 06:44:56 +0000	STATIC	New IP	mentionethers.	a. This is the last	10 MR 24 M 24 14		175.084.00	sondal	б	New IP discovered	170.237/00/08					
19/10/2018 06:44:55 +0000	STATIC	New connection	Manager Street, Square, 199	in have still be	170.008.00.00		170.164.18	sonda1	6	New connection discovered	1912	6				
19/10/2018 06:44:56 +0000	STATIC	New public IP	NAME OF GROOM	and international states of	ALC: NO WORK		Philbrid	sondal	6	Connection with public IP (source IP:	ATTAXABLE !!	1				
19/10/2018 06:44:55 +0000	STATIC	New connection	NAME OF COMPARISON.	The second second	NOR 221 44.00		110,084.02	sondat	6	New connection discovered	28					
19/10/2018 06:44:56 +0000	STATIC	New device	10000-00-0010-00-00	and The loss Of the loss				sondal	6	New device discovered	10-00-70-04-Fb/Fi					
19/10/2018 06:44:56 +0000	STATIC	New IP	post-to-united.	and the local division of the	State over the set		100,084.00	sondal	6	New IP discovered	100.007.02.14	í l				
19/10/2018 06:44:56 +0000	STATIC	New device	Country in case of	the research the part			-	sondal	6	New device discovered	PR 10.00.00 Mail					
19/10/2018 06:44:56 +0000	STATIC	New IP	an	No. No. inc. (17-18). (a)	1000-2019 20.34	1	170.084.07	sondal	6	New IP discovered	178.017.01.08	( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( )				
19/10/2018 06:44:55 +0000	STATIC	New device	10.0310-01.0410-01	International Contents				sonda1	6	New device discovered	10102/02/02/02	6				
19/10/2018 06:44:55 +0000	STATIC	New IP	NAME OF TAXABLE	and the latter of the latter	10.000		171.16.3.10	sondat	6	New IP discovered	171.051.00					
19/10/2018 06:44:55 +0000	STATIC	New device	10.00.0.0.0.00.0	-				sonda1	6	New device discovered	au Philes 27 (Sector	6				
10/10/2010 00-04-05 40000	STATIC	Advent 10	second division division.	1		1		readat	1 .	New it discovered	100.00.00	i .				

Grouped daily alert notification example.

### 3.9 Settings

In this section we can adjust our profile or authorized employee profile, adjust some parameters related to threat detection or different configurations of alerts, threats, and user management.

Under development, subject to change.







# 3.10 Help

Section that enables the download of the latest version of the InprOTech Guardian user manual. Leads to the InprOTech website, where the relevant documentation is posted.

To access it, click on the Menu icon *i* in the bottom left corner.



Dashboard principal

Access to the documentation is in the lower left corner. For any technical issue, please contact <u>customer.support@inprosec.com</u>.

# 4 Application management

## 4.1 Main Dashboard

K	Guardian		▲ admin Acceso anterior: 08/10/2024 14:59:32 ⊕	<u>Salir</u>
ធ	Bienvenido <b>admin</b>		Dispositivos no autorizados (	2
$\oplus$	Resumen de activos h	ardware 🔅 🛛 VER TODO	Tráfico de red (i) Utimo actualización 10 act 2024 15:27 C VER DETALLE	
	Nivel Purdue 2		2000 MB	7d
<b>@</b>			1000 MB	
器	1 SCADA 2 PC		0 MB 21:00 23:00 01:00 03:00 07:00 09:00 11:00 13:00 15:00 19:00 19:00	
ß		•	Alertas (1) Última actualización 10 oct 2024 15:27 C VER TODO	
ති	Accesos rápidos		15 Notice Warning Alert Emergen	icy
	5 Algoritmos activos	30 Alertas	10 5 0 4 octubre 5 octubre 6 octubre 7 octubre 8 octubre 9 octubre 10 octubre	
	VERUSIADO	VERUSTADO	Últimos reportes ①	٦.
	6 Reglas	58 Vulnerabilidades	30/09/2024 0I-26-28 report_UnauthorizedDevices_2024092812326.csv	
	VER LISTADO	VER LISTADO	30/09/2024 01:26:28 report_Alerts_2024092912326.csv	
i			30/09/2024 0h26:28 report_Scoring_2024092912326.csv	

Dashboard principal







### 4.1.1 Actives summary



Asset summary

The user can visualize the number of devices connected to the network, differentiated by type (PLCs, RTU, Switch, Router, Robot, PC, SCADA, DCS, HMI, Firewall, frequency inverter, Controller cards, sensors, V.A. Cameras, tablets, Phones, Honeypots, other equipment), and classified according to the Purdue model as indicated in Annex II (provided that it has been reported as indicated in section 4.4).

### 4.1.2 Quick links



Quick links

### 4.1.2.1 Active Algorithms

By clicking on the "VIEW LIST" link, the user will be able to view the list of artificial intelligence algorithms that are active for threat detection within the organization's network (this section will be discussed later in this manual).







Amenazas basadas en IA/ML

estión de algoritmos IA/ML I Sonda Búsqueda general				
ALGORITMO	ESTADO		ACCIONES	
🕸 👘 anagram	Inactivo	Entrenar		
©	Inactivo	Entrenar		
W news-op_ext-iforest	Detectando	Entrenar		Parar
Process-Mining	Detectando	Entrenar		Parar
isolation-forest	Detectando	Entrenar		Parar
autoencoder	Inactivo	Entrenar		
UEBA-LSTM	Preparado	Entrenar	Detector	

Algorithm list

#### 4.1.2.2 Active Alerts

By clicking on the "VIEW LIST" link, the user will be able to view a list of the total active alerts.

#### 4.1.2.3 Active Rules

By clicking on the "VIEW LIST" link, the user will be able to view a list of the fixed rules that are active for threat detection within the organization's network (this section will be discussed later in this manual).

R	ules engine () GRules			ß
	NAME	STATUS	THRESHOLDS	OPTIONS
۲	New device	Production	15 🚯	
۲	New connection	Production	15 (j)	2
۲	Network port anomaly	Production	15 👔	2
۲	New public IP	Production	15 (j)	2
۲	Possible fingerprinting	Production	5-3-3 (1)	Z
	Possible ARP spoofing	Production	1 (i)	2

#### List of active rules

#### 4.1.2.4 Active Vulnerabilities

By clicking on the "VIEW LIST" link, the user can view a list of the total active vulnerabilities that are not managed. Pending development.

#### 4.1.3 Network traffic graph.











The user can graphically display the traffic generated (in bit/s, or multiple of that unit) in the last 24 hours, both sent (orange) and received (green). It will also have an automatic refresh in that time interval and a button for a manual refresh by the operator. The circled dots on each of the bars will indicate the traffic that occurred 7 days before, as a comparison.

By clicking on the "VIEW DETAIL" button, the user will see on the screen the network sessions window of the InprOTech Guardian application (Section that will be discussed later in this manual).

### 4.1.4 Alerts graph.



The user will have a graphic representation of the number of alerts differentiated according to their severity level (See Annex I) and colours, per day of the last five days, and the trend they have followed. It will also have an automatic refresh at that time interval and a button for a manual refresh by the operator.

If the user places the cursor over the graphic bar of one of the days, the exact number of alerts and emergencies captured so far can be displayed.

By clicking on the "VIEW ALL" button, the user will see on the screen the alerts window of the InprOTech Guardian application (Section that will be discussed later in this manual).

### 4.1.5 Last reports

#### WAIT NEW REPORTS

C	Guard	lian r <sup>oTech</sup>	admin Last access: 09	/10/2024 14:59:32	[→ Log Out
ធ	Repo	orts			
•	Re	ports panel (i) 7 of 7 Reports			76
	Туре	Start datetime End	datetime		
<b>@</b>		FILE TYPE	CREATION DATE	FORMAT	OPTIONS
器	C	Dispositivos no autorizados	30/09/2024 01:26	CSV	<u>الله</u>
ß	C	Alertas	30/09/2024 01:26	CSV	<u>الله</u>
ស្រ	C	Scoring	30/09/2024 01:26	CSV	٤
~	C	IPs públicas	30/09/2024 01:26	CSV	٤
	C	MACs & IPs	30/09/2024 01:26	CSV	đ.
	C	Dispositivos inalámbricos	30/09/2024 01:26	CSV	<u>الله</u>
	C	Vulnerabilidades	30/09/2024 01:26	CSV	٤
i					







#### Last available reports

By clicking on the "VIEW ALL" button, the user can view a list of the latest reports generated automatically or at the customer's request.

Currently, the reports generated on a weekly basis are:

- List of last alerts detected.
- List of unauthorized devices connected to the network.
- MAC-IP relationship seen on the network.
- Network scoring scores.
- Report of technical service indicators (KPIs)

### 4.2 Network map and device list.

### 4.2.1 Network map

To access the network map, the user must click on the icon on the left side of the screen and select the "Network Map" tab.



Network map

In the network map tab, the user will be able to visualize all the devices connected to the network in real time, as well as the communication links between them. Each device will be referenced with a representative image and a series of properties such as its MAC address or name in case it has been informed manually. The network map will show the implemented topology.

The icons represented will correspond to those described in Annex II.

Unauthorized devices will be displayed on the network map shaded with a red background. Fixed and critical devices will also have their corresponding halo (see Annex I for definitions).









#### Unauthorized device

If we place the cursor over a device, we will get a pop-up window where we will see the basic information of the device.



Device basic information

If we click on the device, the window with all the device information will be displayed.

If we place the cursor over one of the links, we will see a pop-up window with the basic information of that communication.



Link basic information.

If we click on the link, the window with all the connection information will be displayed.

The network map can be simplified to display only the devices of interest by using the different filters and accepting the filtering by clicking on the "Consult" button.

Network Map	List of devices			
Network	map (i) Updated: 31/05/2023 12:26			C Create
Sensor ID All	Datetime Network topol 31/5/2023 12:26 Standard	ogy Protocol IP address	Port Show virtual MACs	

Available filters in network map

Filters can be applied according to:

- Date and time: Time frame to be displayed per screen.
- Network topology: Sampling model of the organization's network per screen.
- Protocol: Sampling by screen of only connections using the selected protocol.







- IP Address: Sampling only of device and connections with the selected IP.
- Port: Sampling by screen of connections to the selected port.

- Viewing or not of virtual MACs (multicast/broadcast), automatically calculated by the system.

### 4.2.2 **Device list**

To access the list of devices, the user must click on the icon on the left side of the screen and select the "Device list" tab.

T	Guar	dian					admin Last access		59:32	
ລ	Ne	twork Map	List of devices	List of wireless						
€	De	evice <b>p</b>	anel 🕕 13 of 1	3 Devices				8	۵ 🖻	+ Create device
2	Senso	r ID	General search	Туре		Rol Purdue level	IP address	MAC add	ess	Show virtual MACs Yes O No 💿
)	Pinner Yes (	d devices ) No () All (	Critical devices	Authorized devices  Yes No All	Ð					
ъ		STATUS	NAME	TYPE	PURDUE	MAC ADDRESS	IP ADDRESSES		SCORING	OPTIONS
j	5		100.00	PLC	1	-	anonii		HIGH	
3			812-04	PLC	1	BOUTOD BOUTS	And the Party of Concession of		MEDIUM	
	899 B		14.0	PC	2	10110-0110-00-000	1000	+3	HIGH	
	2		Prop. Product	Robot	0	-	anone.		HIGH	
		•00	Converse Hill	VA Camera	1	-	10000		LOW	
		000	beau inst	Sensor		10101010-0010-001	And a lot of the lot o			
		•00	Annales III	Controller Card	0	-	-		HIGH	
	-					to the second second				

Device list

A list of all the devices present in the organization will be displayed along with their information in a more expanded form:

- STATUS
  - The first of the circles will indicate whether the device is authorized (green colour) or unauthorized (red colour).
  - The second of the circles will indicate whether the device is critical (orange colour with fill) or non-critical (orange colour without fill).
  - The third circle indicates whether the device is fixed (grey colour with fill) or not fixed (grey colour without fill).
- NAME: Name assigned to each device.
- TYPE: Differentiation of the type of device (PLC, RTU, SCADA, Honeypot, etc.).
- PURDUE LEVEL: Classification level according to the Purdue model.
- MAC: Assigned MAC address of the device.
- IP ADDRESSES: Assigned IP address of the device.
- SCORING: device importance/risk (low, medium, or high).
- VULN RISK: highest criticality level for all the device's vulnerabilities.
- VENDOR: device manufacturer, identified by the first three fields of its MAC address.
- FIRMWARE: integrated firmware device.
- CUSTOMIZED FIELDS: In addition to the existing fields, users can create their custom fields in key-value format. Each customizable field will appear in the





device list as a new virtual column, allowing the user to catalogue, organize, and filter the devices. These customizable fields will also appear in the reports. The columns created as customizable fields will be part of a virtual inventory. The user can apply filters to this inventory as desired. This field inventory is also exportable.

**ACTIONS:** 

Button to view device information in detail.

Device Details		🖉 Edit
NAME  MAC  Fs  Mathematical Statematical Sta	STE ID SCHOOR IDS sondq_vc ROL Not applicable SCORNO DATE DG/05/2024 IS25:00 STATUS CORNOR DATE DG/05/2024 IS25:00 LAT SCAN 24/05/2024 IS101:40 SCANTATUS SCANTATUS	UDP SCAN
Edit Device	<i>Device details</i> tton to modify de <sup>.</sup>	vice parameters.
Name Device type Pinned* Yes O No © * Required fields	Critical* Yes O No ®	C Authorized* Yes  No C
Cancel	24	Save
	Dice parameters	

<sup>(2)</sup>: Button to perform other actions on the device, such as access with pre-filtered view to the list of alerts, vulnerabilities (under development), as well as node deletion.

There is the possibility of filtering so that the screen displays only the devices in which we are interested.

Device	panel i 13 of 13 Device	es				76 🗠 🔤	+ Create device
Sensor ID All Pinned devices Yes No Al	General search Free text Critical devices Au I Yes No All Ye	thorized devices	Rol	Purdue level	IP address	MAC address	Show virtual MACs Yes No 💿
			Device	filterina			

vevice fiitering







The user can perform this filtering according to:

- Probe ID, to filter by zone of the industrial network and/or headquarters.
- Device name
- Device Type (PLC, RTU, SCADA, Honeypot, FIREWALL, etc.)
- Device Role (Transmitter, Receiver, or both)
- Purdue level, according to Annex II
- Device IP address
- Device MAC address
- View of broadcast reserved virtual MACs (Y/N).
- Fixed devices (Y/N), see Annex I.
- Critical devices (Y/N), see Annex I.
- Authorized devices (Y/N), see Annex I.

The user can also perform a general search using a text string.

+ Create device

Pressing the button will reset the filtering values and Guardian will display the complete list with all devices again.

By means of the button our product will perform a CSV file export of the list of devices with their information.

It is possible to manually add a new device to the organization's network and list by

clicking on the button

The following pop-up window will appear:

MAG		
The field is required		
Name		
Device type		
The field is required		
Purdue Level		
The field is required		
Pinned*	Critical*	Authorized*
Yes No C The field is required	Yes No No The field is required	Yes No C The field is required

Available fields to create a device.

The requested information about the device to be added must be entered manually and to make the creation effective, click on the "Save" button.

#### 4.2.2.1 Import CSV

The system allows mass import/editing of devices, to avoid unnecessary alerts during initial onboarding or major changes in the industrial network.

In the network section and the "Device List" tab, you will see the following icon: <sup>(1)</sup> . Clicking on this icon will open the following pop-up window.







From this window, you can select or drag a file with ".csv" extension containing the data of the devices you wish to add or modify, in the format indicated below.

EVICE IMPORT					
	Dro	ıg and drop f	iles h	nere	
		or			
		Select a file	۵		
Cancel					✔ Confirm

Import CSV pop-up.

For the CSV file to be valid, it must comply with the following characteristics:

- A maximum of 250 records.

- Header with the following columns (we can name the columns as we wish):

- o MAC
- Device name
- Authorised (Y/N)
- Critical (Y/N)
- Fixed (Y/N)
- Device type (from the allowed list: virtual, plc, rtu, switch, router, robot, pc, scada, hmi, firewall, adjustable\_frequency\_drive, controller\_card, sensor, va\_camera, tablet, voip\_phone, server, code\_bar\_scanner, other)
- PURDUE level (0 to 4, as explained in Annex II)
- Customized fields.
- The field delimiter shall be ";".
- It shall not contain empty fields.
- It may contain new device records, or existing devices in the database to which you want to change one or more of the attributes mentioned in the previous point. One row per device is required, in the format indicated.
- The new records will simply have all the CSV fields covered with the desired information.
- The existing records that we want to modify, will contain the literal \*CURRENT\* in all those fields that must remain fixed. In the fields to be updated, we will simply put the latest information based on what has been previously established.
- The ones we want to modify must have \*CURRENT\* in some of their properties; this allows us to distinguish these records from the new ones.
- The mac field cannot contain the literal \*CURRENT\* since it univocally identifies the device.





- New records may also contain the literal \*CURRENT\* in some of their fields; this means leaving those fields with default values. In the case of Boolean data, it will be false, and text fields, such as name, Purdue, and device type, will remain as NULL, and the user can modify it through the web interface.
- There are two posible ways to define a set of customized fields, respecting their key-value structure:
  - .json format: {"key1": "value1", "key2": "value2"}
  - Bars: key1 | value1 | key2 | value2

You could delete previously defined customizable fields by overwriting the data with a new CSV document. This document should contain the literal \*DELETE\* in place of those fields, like the use of the literal "CURRENT."

• It is crucial to write literals between asterisks.

**Notice:** Please consult Support if you have any doubts, as improper use of this functionality can significantly impact the integrity of the node information.

Once the file has been selected, click on "Confirm", as this is a high impact operation (it allows both adding and modifying device properties):

Do you really wa	nt to import new devices?
It is recommended to bac	k up your devices before importing
(E)	import.csv
Cancel	✓ Confirm

If the ".csv" file we have sent does not contain any device, the following error message will be displayed.



If there are errors in the data within the ".csv" file, a message will be displayed with details of the errors found, along with the line number where each error is found.









If no errors are detected, it shall be possible to verify that the devices have been correctly added to the database.

### 4.2.2.2 Air Watcher (Wireless devices list)

In the network section, there third tab allows access to the list of Wireless devices registered in the network.

At the top, the total number of devices in the database can be seen and, if with a filter applied, how many match that filter in relation to the total.

On the right side, there is a button panel to delete the previously applied filters and export the list of devices in CSV format.

The information provided by this section will be the following, for all those devices with Wi-Fi or Bluetooth capability detected in the vicinity of the collectors:

- **Authorized**: determines whether the device has been authorized by an administrator (green) or not (red).
- **Name**: it corresponds to the name of the device.
- **Connection Type**: could be Wi-Fi or Bluetooth.
- Device Type: values can vary for Bluetooth devices. For Wi-Fi devices, it can take values such as "Access Point" or "Smartphone or Laptop," in addition to "Unknown."
- **Source MAC**: source MAC address of the packet. Identifies the device itself in the captured communication.
- **Destination MAC**: destination MAC address of the packet. Identifies the receiving device of the packet.
- **Activity**: reflects the state of the device or the type of activity it has performed:
  - Searching for networks: the device has the Wi-Fi antenna on and is searching for access points.
  - Connection attempt: the device has tried connecting to an access point.
  - Access point active: the device is functioning as an Access point.
  - Transmitting data: the device is sending information to an access point.
  - Device visible: this only applies to Bluetooth devices; the device has Bluetooth on and is visible to other devices.
- **Wireless ID**: name or identifier of the Wi-Fi network (could be empty if, for example, the connection is Bluetooth).
- **First Seen**: format dd/mm/yyyy hh:mm.
- Last Seen: format dd/mm/yyyy hh:mm.







K	Guardian						• ****		[→ <u>Log_Out</u>
ធ	Network Map	List of devices	List of wireless						
•	Wireless	panel 🤅 2	77 of 277 Wireless devices						6
 (€)	Sensor ID All Author	Name	Wireless MAC	Wireless ID	Connection type	Activity	Start datetime	End da	tetime
器	AUTHORIZED		▼ CONNECT		DEVICE TYPE ¥	SOURCE MAC ¥	DESTINATION MAC		OPTIONS <b>^</b>
Ľ			w	i-Fi	Access Point	*****	-	Punto de acceso activo	
<b>\$</b>			w	i-Fi	Access Point	*****	******	Punto de acceso activo	
	•		w	i-Fi	Access Point	40.000 All (\$10.000)	*****	Punto de acceso activo	
	•		w	i-Fi	Access Point	410000	******	Punto de acceso activo	
	•		w	i-Fi	Access Point	0.000000000	and the second	Punto de acceso activo	
			w	i-Fi	Access Point	40.000.000.000.000	and the second second	Punto de acceso activo	
			w	i-Fi	Access Point	0.0000000000	and the second second	Punto de acceso activo	
	•		w	i-Fi	Access Point	and the first of	and the second second	Punto de acceso activo	
			w	i-Fi	Access Point	101001-0010	and the second second	Punto de acceso activo	
i					· · · · · · · · · · · · · · · · · · ·			Provide all according to the second	

Wireless device list

Below are the possible filters that can be applied to keep the devices we are interested in:

Pane	l de <b>inalámbricos</b>	(i) 13	34 of 134 Dispositivo:	s inalámbria	os					76	•
IDs Sonda Todos	Nombre	MAC Wir	reless ID	Wireless	Tipo de conexión	$\odot$	Actividad	Fec	nha y hora de Inicio	Fecha y hora de fin	
:	Dispositivos autorizados Sí () No () Todos ()										

Wireless list filters

Remember that it is possible to sort the devices alphabetically either directly or inversely by clicking on any of the columns.

Finally, the actual list of assets contains information details about them, as well as buttons to perform certain further actions (view more details or delete).

				ast access: 16/12/202	4 15:53:20	
	f devices List o	Wireless Details	Ledit	•		
Wireless pan	el (j) 277 of 277	NAME Not available	SENSOR IDs			•
All		CONNECTION TYPE WI-FI	WIRELESS ID Xiaomi			
	• IIA (	DEVICE TYPE Access Point	AUTHORIZED			
NAME ¥	CONNECTION TYPE Wi-Fi	ACTIVITY Access point active	FIRST SEEN 12/12/2024 11:58:49	ACTIVITY V	WIRELESS ID ¥	
	Wi-Fi	SOURCE MAC	LAST SEEN 16/12/2024 14:50:16	nsmitting data	Wildcard	
	Wi-Fi Wi-Fi	DESTINATION MAC		nsmitting data	Wildcard	
	Wi-Fi	CHANNEL 1		nsmitting data	Wildcard	
	Wi-Fi Wi-Fi	SITE ID 2		hing for networks	Wildcard	
	Wi-Fi	_		nsmitting data	Wildcard	
4	Wi-Fi	Close		ning for networks	Wildcard	

Wireless devices details

We will also be able to see some additional fields in this new modal window:





![](_page_40_Picture_1.jpeg)

- Channel: transmission channel identifier.
- Site ID: represents the factory.
- Sensor IDs: identifies the sensor.
- Wireless ID: device unique identifier.

If we click on the *letter* button, we can rename the device and determine whether it is authorized or not.

					10:43:06	[→ <u>Log Out</u>
	Wireless	pa				-
	Sensor ID All		it Wireless	✓ Go to details	datetime	: ©
		Marma				
					LAST SEEN	
	tooth	Author spe Yes 🖲	zed*		04/10/2024 00:20	
	tooth	unk			03/10/2024 23:35	
		* Requi	red fields			
		Co	ncel	Save		
i	4		_			P.

#### 4.2.2.3 Smart View (Device scan)

This capability allows an active scan of the devices in the OT network, to identify some additional properties of each node by means of a light fingerprinting: device version, firmware, open ports, and services running on the machine itself.

For this purpose, the nmap tool will be used, and the ports on the TCP and UDP network protocols will be scanned. This information will be recorded in the system database and can be extracted as additional attributes of each device, which will be refreshed by a periodic pooling.

3	Guar	dian					admin Last access	09/10/2024 14:59:32	
5	Ne	itwork Map	List of devices	List of wireless					
Ð	De	evice <b>p</b>	anel 🛈 13 of 1	3 Devices				8 4 🖶	+ Create device
2	Senso All Pinner Yes	d devices	General search Free text Critical devices	Authorized devices Ves No All (		Rol Purdue lev	Vel IP address	MAC address	Show virtual MACs Yes No O
ŧ,		STATUS	NAME	ТҮРЕ	PURDUE	MAC ADDRESS	IP ADDRESSES	SCORING	OPTIONS
	51		10.0	PLC	1	-	anosii	HIGH	6 0
	<b>S</b>		10.00	PLC	1	Bear 10, 80, 80, 10	And a second	MEDIUM	•
	8.9P		100.00	PC	2	10110-0110-00-000	1000	+3 HIGH	
	2		Rear Protection	Robot	0	-	and the second	HIGH	8 5 8
		•00	Carrana (15	VA Camera	1	10.000	*****	LOW	
		000	Server Cross	Sensor		10111111111111111	And a second		D 🗢 🗊
		•00	Reader III	Controller Card	0	-	1000	HIGH	1
	-								فاعاص

![](_page_40_Picture_12.jpeg)

![](_page_40_Picture_13.jpeg)

![](_page_40_Picture_15.jpeg)

![](_page_41_Picture_1.jpeg)

As can be seen, once the scanner has been run, information associated with the firmware of some of the devices is showed in the list.

The rest of the scanner information can be viewed by clicking on the icon on the right

In the pop-up will appear all the information of the device in question, and two sections called 'TCP Scan' and 'UDP Scan.' There all the open ports found for a given device will be displayed, as well as the date of the last scan and if it has finished correctly or if there has been some kind of error.

MAC SENSOR IDS sonda_vc TCP SCAN IPS ROL Not applicable SCORING MEDIUM SCORING DATE 06/05/2024 15:25:00 STATUS TYPE Other UNENTROL	Manual States allow a
AAC SENSOR IDS sonda_vc TCP SCAN Ps ROL SCORING MEDIUM AST CONNECTION 04/06/2024 13:13:20 YPE Other UNENINED UNFINNED	
AST CONNECTION PPE YPE Sther SOUND STATUS UNPINNED UNPINNED SOUND STATUS UNPINNED UNPINNED UNPINNED UNPINNED	a see a second
Ps RoL Not applicable SCORING MEDIUM AST CONNECTION 04/06/2024 13:13:20 YPE UNAUTHORIZED UNPINNED WRENCE	
AST CONNECTION 04/06/2024 13:13:20 YPE Dther CONNECTION 05/05/2024 15:25:00 UNPINNED UNPINNED UNPINNED	count the state of the
AST CONNECTION O4/06/2024 13:13:20 YPE Dther SCORING DATE 06/05/2024 15:25:00 UNPINNED UNPINNED UNPINNED	to other same differences of these
SCORING DATE           LAST CONNECTION         06/05/2024 15:25:00           004/06/2024 13:13:20         STATUS           TYPE         UNAUTHORIZED         UNPINNED           Other         UNCRITICAL	a monoral distance i m
AST CONNECTION 00/05/2024 15:25:00 04/06/2024 13:13:20 STATUS VPE UNAUTHORIZED UNPINNED Other UNCRITICAL	Contraction of Contraction of Contraction
STATUS     STATUS       type     UNAUTHORIZED       Other     UNCRITICAL	COLUMN TRAVEL OF TAXABLE
Other UNCRITICAL	
PURDUE LEVEL LAST SCAN	
2 24/05/2024 11:01:40	
VENDOR SCAN STATUS	
AAEON Technology Inc. (SCANNING)	

Device details

DISCLAIMER: Given the active nature of this operation, although no operational impact has been observed, it cannot be completely ruled out. It is therefore up to the customer to decide whether to activate this functionality (for which InprOTech support should be consulted). If you would like to activate it in your instance but leave some subset of devices excluded from the list of nodes to be analysed, just tag them with the 'Critical' property enabled in the device inventory (individually or through a mass update).

Additionally, honeypot devices labelled as such are also exempt due to their behaviours as decoys with vulnerable ports. This helps prevent the excessive generation of false positives.

![](_page_41_Picture_9.jpeg)

![](_page_41_Picture_12.jpeg)

![](_page_42_Picture_1.jpeg)

# 4.3 Alerts panel.

To access the list of alerts, the user must click on the following icon on the left side of the screen.

S	Guar	dian					admin Last access: 09/10/202	24 14:59:32	⊖ [→ <u>Log Out</u>
ធ	Ale	erts Panel							
•	AI	erts po	anel i 37 of 37 Alerts					6	+ Create alert
~	Senso	r ID	General search	IP address	MAC address	Start dateti	me	End datetime	
45	All		Free text_				• ·: Ø		<ul> <li> •</li> </ul>
6	Severi	tγ	Category	Show resolved	Show silenced				
				Yes No All 🖲	Yes No All 🖲				
22		SEVERITY	NAME	SOURCE MAC	DESTINATION MAC	SOURCE IP	DESTINATION IP	DATE	OPTIONS
ß	-	WARNING	New public IP			-	-	04/10/2024 00:29	
ණ	-	WARNING	Anomalía en tráfico net	4(I)		-	101000	04/10/2024 00:00	
	-	ALERT	Conexión con puerto IT		a (i)		-	03/10/2024 23:19	
	2	WARNING	PROTOCOL-ICMP Echo R		-		And shades	03/10/2024 22:12	
	-	WARNING	New public IP	$[(\alpha,\beta),(\alpha,$	()	100000	10000	03/10/2024 21:23	
	S.	WARNING	PROTOCOL-ICMP PING		-		1.0.00	03/10/2024 21:17	
	-	EMERGENCY	Posible ARP spoofing		()	*****	-	03/10/2024 20:29	
i	-	NOTICE	Nueva conexión		****	STATUS .	and the second	03/10/2024 20:24	

#### Alerts list.

A list will be shown with all the alerts present in the organization and information about them.

- Severity: Classification of the alert according to the impact it could have on the organization.

- Name: Defined name of the alert.
- Source MAC: MAC of the alert generating device.
- Destination MAC: MAC of the device to which the action was directed.
- Source IP: IP of the device generating the alert.
- Destination IP: IP of the device to which the action was directed.
- Date: Date and time of alert appearance.
- Actions (see annex I for definitions):

Example: If we place the cursor over it, we will be able to know the name of the device assigned to that MAC address.

Eutton to change the alert status to muted or unmuted (see section 6.2 in Annex I).

Sutton to change the alert status (solved or not solved), according to the logic indicated in Annex I.

<sup>(2)</sup>: Button to perform further actions on the alert, such as viewing the details or adding notes.

![](_page_42_Picture_19.jpeg)

![](_page_42_Picture_21.jpeg)

![](_page_43_Picture_1.jpeg)

NAME	DATE	SOURCE NAME	NOTE UPDATE
Network port anomaly	26/07/2023 10:34:45	received contractive	Not available
CATEGORY	SOURCE MAC	DESTINATION NAME	NOTE CREATOR
STATIC	COMPANY OF THE OWNER.	ADD TREAST - Service T - Art?	Not available
PROTOCOL	DESTINATION MAC	(80101-880)	
ARP	DESTINATION MAD	MALLIE	
		https://0	
SEVERITY	SOURCE IP	indpoil [ 0	
ALERT	100.000	DESCRIPTION	
STATIS	DESTINATION IP	Network port anomaly 0:	
ACTIVA	DESTINATION IP	expected protocol -> ICMP; found	
		-> 2054	
SITE ID	SOURCE TYPE		
1	Not applicable	NOTE	
		Not available	
SENSORID	DESTINATION TYPE		
and the face	Not applicable		

Alert details

It is possible to filter the display to show only the alarms of interest.

Alerts panel 3 37091 of 37091	Alerts						😽 🔒 🕂 Create alert
Sensor ID         General search           All         Free text           Show resolved         Show stlenced           Yes         No         All (*)	MAC address	IP address	Start datetime	End datetime	Severity	Category	G

Available alert filters

This filtering can be done according to:

- Probe ID, to filter by zone of the industrial network and/or headquarters.

- General search: Search by entering a text containing the alarm (including in your notes).

- IP address of the device
- MAC address of the device
- Date and time of start of alert search
- Date and time of alert search end date and time
- Severity, according to Annex I
- Alarms resolved or not resolved, according to Annex I
- Alarms silenced or not silenced, according to annex I

Pressing the button will reset the filtering values and the complete list with all the alarms will be displayed again.

By means of the button a CSV file export of the list of alarms with their information will be made.

It is possible to manually create a specific alarm in the organization's network by clicking on the button + Create alert.

The following pop-up window will appear:

![](_page_43_Picture_21.jpeg)

![](_page_43_Picture_23.jpeg)

![](_page_44_Picture_1.jpeg)

Title*	Protocol
The field is required	
Source IP	Description*
	The field is required
Destination IP	Severity*
	The field is required
Source MAC	Date
Destination MAC	Value
* Required fields	

Alert creation

The requested information about the new alarm created must be entered manually and to make the creation effective, click on the "Save" button.

### 4.3.1 **Public IP**

This alert is connected to a cyber-intelligence service that allows us to obtain more information about the communication endpoint outside the trusted network, to try to determine whether it may be malicious.

To access the details of the alert, click on the gear icon, which can be seen on the righthand side of the panel. Then, by clicking on "View details", you can access this information:

NAME	DATE	SOURCE NAME	NOTE CREATOR
New public IP	06/09/2023 12:12:46	INCUSION - MAG, CARREL-LAN	Not available
CATEGORY	SOURCE MAC	0070880180	
STATIC	8000707070480	DESTINATION NAME	
PROTOCOL	DESTINATION MAC	Not applicable	
TCP	1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	VALUE	
SEVEDITY	SOURCEIR	20.00170.000	
WARNING	SOURCEN	DESCRIPTION	
		Connection with public IP	
ACTIVA	DESTINATION IP	(destination IP: )	
SITE ID	SOURCE TYPE	NOTE	
1	Not applicable	Not available	
SENSOR ID	DESTINATION TYPE	NOTE UPDATE	
extituitee	Not applicable	Not available	

Screen with alert details.

![](_page_44_Picture_10.jpeg)

![](_page_44_Picture_12.jpeg)

![](_page_45_Picture_1.jpeg)

At the top of this tab, there is a button called 'Public IP Data'. Clicking this button will take you to additional information about the IP, which may include details such as home city, region, time zone, continent, country name, public IP address, coordinates, organisation, and postcode.

Public IP <b>Details</b>	C Go to details
Country name Spain	IP 18.67.240.48
City Madrid	Geo location 40.4165,-3.7026
Region Madrid	Organization AS16509 Amazon.com, Inc.
Timezone Europe/Madrid	Postal 28004
Continent Europe	
Hostname server-	
18-67-240-48.mad56.r.cloudfront.net	
Close	

Public IP details

### 4.3.2 **Ip Reputation and Blocking Policy**

When the system detects a *New public IP* connection alert, Guardian connects to a series of public listings where activities considered abusive (spamming, hacking, etc) are reported. The alert is enriched with this information, visible in the public IP details, and in case it detects that the public address involved has a bad reputation, it changes the severity, the description, and marks it in red.

3	Guar	dian proTech					admin Last access: 11	/06/2025 08:46:40	(→ <u>Log Out</u>
ស	Ale	erts							
•	Al	erts <b>pan</b>	<b>e</b> (i) 42 of 42 Alerts					<b>™</b>	+ Create alert
	Sensor		General search Free text	IP address MAC	address Start datet	ime /yyyy 🖬: @	End datetime dd/mm/yyyy	Severity	Ū
٩	Catego	ory D	Show resolved Show silen						
器									
		SEVERITY V	NAME V	SOURCE MAC V	DESTINATION MAC V	SOURCE IP V	DESTINATION IP V	DATE V	OPTIONS
6		WARNING	New public IP	242 2012	CICALISE IN ()	<b>E-2</b> C	01014-6036	09/06/2025 09:09	۲
<b>®</b>	-	WARNING	New public IP	222202	CECSESEE :	1.5.41	BERING	09/06/2025 09:09	× < 0
	-@-	EMERGENCY	New public IP	00 BUBDELFESS	SEGREBORIDE CO	(DVLS/98)	(PACK)	09/06/2025 09:09	æ 🔦 💿
	-@-	EMERGENCY	Posible ARP spoofing	007112965 ()	ECITO SE DOCES 🔹	E3-24	CHOH-S	08/06/2025 09:09	æ 🔦 🐵
	-	ALERT	Nuevo dispositivo	i i i i i i i i i i i i i i i i i i i	ECITE VEDERALE ()			08/06/2025 09:09	æ 🔦 🙁
	-	NOTICE	Nueva conexión	CTIERS (			DE 05-75	08/06/2025 09:09	& <b>4</b> Ø

![](_page_45_Picture_8.jpeg)

![](_page_45_Picture_11.jpeg)

![](_page_46_Picture_1.jpeg)

Alert <b>det</b>	ails		Public IP data
AME ew public IP	DATE 09/06/2025 09:09:53	SOURCE NAME Not applicable	NOTE Not available
	SOURCE MAC	DESTINATION NAME Not applicable	NOTE UPDATE Not available
ROTOCOL CP	DESTINATION MAC		NOTE CREATOR Not available
WERGENCY MERGENCY ATUS CTIVE re ID NSOR ID Inda	SOURCE IP CONTRACTOR DESTINATION IP CONTRACTOR SOURCE TYPE Not applicable DESTINATION TYPE Not applicable	Connection with public IP (destination IP: "2:2006% 55). This IP has been listed as abusive and/or malicious. We recommend to block traffic to and from this IP.	
Cc	Public IP <b>Det</b> o <sup>Japan</sup>	Geo location	tails
	ty saka igion saka mezone	Organization INSERVICE UNDER INSERVICE Company Inservice Postal S12+0010	
As Co As Ho	sia/lokyo ontinent sia ostname	Reputation Bad IP Reputation source abuseipdb	
-			

The Reputation Check can be enabled and disabled in the configuration menu, Network/Blocking section. This option affects incoming alerts, i.e., enabling reputation will not retroactively affect those public IP alerts that came in while reputation was disabled.

![](_page_46_Picture_4.jpeg)

![](_page_46_Picture_7.jpeg)

![](_page_47_Picture_1.jpeg)

K	Guardian			admin Last access: 11/06/2025 08:46:40		[→ <u>Log Out</u>
ធ	Settings					
•	PROFILE	Traffic <b>blocking</b>				
6	<b>THREAT DETECTION</b> ல General	Import Whitelist file	Export Whitelist file			
86 (%)	NETWORK					
\$	ADVANCED @ General	Reputation check and Blo	cking policy			
	▲ Preferences	Reputation check Enable O Disable 💿	Blocking policy Automatic Automatic			
			Manual		Save	
			off			

When the system receives a public IP alert considered malicious, Guardian will respond applying one of the three available Blocking Policies:

-**Informative**, where the user is informed and recommended to review and block traffic from/to that address.

**-Manual or semi-unattended**, where a button is enabled to block/unblock the malicious IP by sending the firewall an instruction to include that address in a filter.

-Automatic, where Guardian sends this instruction to the firewall without human intervention.

The Blocking Policy can also be disabled. In this case, all information regarding the IP reputation in the alerts will be disabled, as well as the blocking rules (via sending command to the firewall to lift the address blocking rule). This information is not deleted, and will be reapplied if the Blocking Policy is re-selected to an active value. A drop-down selector for the Blocking Policy can be found in the same menu. Public IP alerts that reach the system while the Blocking Policy is disabled are not retroactively changed when the Blocking Policy is re-enabled.

Automatic and semi-automatic options are currently under development

### 4.3.3 IP whitelist

The user can provide a list of always-allowed IP addresses, or also address ranges in CIDR format (whitelist). These addresses will never have their reputation calculated even if the check is enabled when a related alert is received. This will only be reflected in the public IP data menu in their reputation field as *whitelist*.

The upload file must be in *csv* format, with only one column per row, which must contain either an IP address (192.168.0.1) or a CIDR range (192.168.1.0/24). The loading is performed atomically: a single misformatted or invalid data invalidates the entire operation. Possible redundancies in the list of addresses and ranges (repeated IPs, IPs contained in CIDR ranges, overlapping CIDR ranges) are not treated as errors.

The import will be performed in the blocking options, through the screen displayed after pressing the button under the "*Import Whitelist file*" option, which will present the following pop-up window where you can either drag the file to the green box, or find it in the users's filetree.

![](_page_47_Picture_15.jpeg)

![](_page_48_Picture_1.jpeg)

	Drag and drop files he	re
	or	
	Select a file	
Cancel		✓ Confirm
WHITELIST IM	PORT	
Check the user mo	nual for format restrictions and limi	tations of this functionality
Do yo It is recommer	bu really want to import ne Inded to back up your white Mulist.csv	w whitelist? list before importing

Next imports will completely replace the previous whitelist. Thus, if you do not want to implement any whitelist, simply load an empty file.

Uploading a new whitelist has an effect on the public IP alerts already in the database:

- those alerts with IPs that have the reputation already processed before, and that are included in the new whitelist, are returned to the original state with the status *'reputation: Wlisted'*.

- Those alerts with IPs within the previous whitelist, but which are outside the new whitelist, have their reputation calculated and the alert description modified accordingly.

The loaded whitelist can be downloaded for examination by clicking on the button **report**, which will download a csv file with the saved data.

### 4.4 Vulnerability analysis

### 4.4.1 Vulnerabilities Panel

To access the vulnerabilities panel, the user must click on the icon it that appears on the left side of the screen and select the "Vulnerabilities Panel" tab.

![](_page_48_Picture_11.jpeg)

![](_page_48_Picture_14.jpeg)

![](_page_49_Picture_1.jpeg)

3	Guard	lian wOTech						Admin_2 Last access: 0	07/10/2024 11:13:20	<b>⊕</b> ∎	[→ <u>Log C</u>	Dut
ធ	List	of vulnerabilities	Device statistics	Global stat	istics							
•	Vu	Inerabilitie	s Panel 🗉	64 of 64 Vulner	abilities						76 🗠 📾	
		dress CVE	Sta	tus (	Begin date		: ©	te	ð: Ø			
6		MAC	ST	ATUS	CVE		PORT		CPE		OPTIONS -	
暴		10.000.0000	Ac	tive	CVE-2024-6387		22	0	cpe:/a:openbsd:opens	:h:8	5 <b>4</b> 8	
		10.0000.0000	Ac	tive	CVE-2024-6387		443				5 4 8	
6		10.0000.0000	Ac	tive	CVE-2024-6387		23		cpe:/o:linux:linux_ker	nel	5 3 8	
ŝ		10.000	Ac	tive	CVE-2024-6387		80				5 9 9	
		10.000	Ac	tive	CVE-2023-51767		23		cpe:/o:linux:linux_ker	nel	5 9 0	
		10.000	Ac	tive	CVE-2023-51767		22	0	cpe:/a:openbsd:opens	:h:8	5 3 8	
		11-12-10-10-14-14	Ac	tive	CVE-2023-51767		80				5	
		11-12-18-18-19-19	Ac	tive	CVE-2023-51767		443				5	
		10.000	Ac	tive	CVE-2023-51385	i i	80				5	
i	4								1		· · · · · · ·	1

#### View of the Vulnerabilities Panel

In the vulnerabilities panel tab, the user can view a list of all the vulnerabilities present in the network. These are found in the services detected after the open ports discovered by Smart View and checked against the NIST vulnerability database, the National Vulnerability Database (NVD).

The information displayed in each row is as follows:

- MAC Address: the MAC address of the device where the vulnerability has been detected.
- Status: indicates whether the vulnerability is active, resolved, silenced, or a false positive.
- CVE: "Common Vulnerabilities and Exposures." Identifier according to the vulnerability classification glossary.
- Port: port f the device
- CPE: "Common Platform Enumeration." Identifier of the product or system affected by the vulnerability in question.
- Source: system or device that found the vulnerability.
- Criticity: score from 0 to 10, assigned based on the criticality level of the vulnerability.
- CWE: "Common Weakness Enumeration." Identifier of the common weakness associated to the vulnerability found.
- Discovered date: Date when the vulnerability has been found.
- Published Date: the documentation date when the vulnerability with the referenced CVE was reported in the NVD vulnerability database.
- "Last seen": timestamp when the vulnerability was seen for the last time.
- Options (Actions):
  - Go To: allows viewing the alerts generated by this vulnerability or the devices on which it is present.
  - Change status (active, resolved, silenced, or false positive.).
  - Other actions: allows to view the details of a vulnerability and add a note.

![](_page_49_Picture_23.jpeg)

![](_page_50_Picture_1.jpeg)

Guardian			Admin_2	2024 103:20	Generation Contraction
List of vulnerabilities	Show Vulnerabil	ity			
<b> </b> Vulnerabilities	SITE ID 2	CRITICITY High (8.1)	DATE DISCOVERED 24/09/2024 16:30:41		<b>6 0</b>
MAC Address CVE	MAC	CWE Not applicable	DATE PUBLISHED 01/07/2024 15:15:06	: (0)	
CRITICITY High (8.1)	CVE CVE-2024-6387	STATUS Active	DATE LAST SEEN 24/09/2024 16:30:41	24/09/2024 16:30	
<ul> <li>High (8.1)</li> <li>High (8.1)</li> </ul>	PORT 22	NOTE Not available		24/09/2024 16:30 24/09/2024 16:30	
👩 High (8.1)	CPE cpe:/a:openbsd:openssh:8.8	NOTE CREATOR Not available		24/09/2024 16:30	
<ul> <li>High (7)</li> <li>High (7)</li> </ul>	SOURCE in-house scanner	NOTE UPDATE Not available		24/09/2024 18:30 24/09/2024 18:30	
😁 High (7)				24/09/2024 16:30	
<ul> <li>High (7)</li> <li>Medium (6.5)</li> </ul>	Close			24/09/2024 16:30 24/09/2024 16:30	

Details of a vulnerability.

Next to the header, we can see the number of vulnerabilities displayed, along with the total count.

Vulnerabilit	ies <b>Panel</b> (	i 64 of 64 Vulnerabilitie	es			76 🗗	•
MAC Address C	VE	Status	Begin date	© End date	D: 0		

Number of de vulnerabilities and filters.

In the upper screenshot, we can also see that it is possible to apply filters, so the display only shows the desired vulnerabilities. This filtering is done by:

- MAC Address
- CVE
- Status
- Start Date and Time
- End Date and Time

By pressing the button , the filter values will be reset, and the complete list with all vulnerabilities will be displayed again.

Using the button, you can import a file with a ".csv" extension containing the vulnerabilities you want to add. They must contain the following fields, keeping the dates in the format YYYY-MM-DDTHH:MM:SS.000GMT+XX:XX:

- Vendor ID
- MAC Address
- CVE
- Port
- CPE (Optional)
- Source
- Criticity
- CWE (Optional)
- Status
- URL
- Note (Optional)
- Creator Note (Optional)

![](_page_50_Picture_27.jpeg)

![](_page_50_Picture_29.jpeg)

![](_page_51_Picture_1.jpeg)

- Timestamp Discovered
- Timestamp Published
- Timestamp Last Seen

On the other hand, using the button, it is possible to export a CSV file containing the list of devices and their information.

### 4.4.2 **Device statistics**

Offers the vulnerabilities found in the network, sorted by the available devices.

### 4.4.3 Global statistics

Offers global statistics of the network given its vulnerabilities.

# 4.5 **Communications**

To access the communications list, the user must click on the icon 📅 that appears on the left side of the screen.

K	Guard	lian <sup>roTech</sup>				admin Last access: 09/10/2024 14:59:32	<b>a</b> 🖗	Log Out
ធ	Com	munications						
۲	Co	mmunicatio	ns <b>panel</b> () 22 of 22	Connections			8	
⊿	Sensor I	D IP addr	MAC address	Port	Protocol			
٩		SOURCE MAC	DESTINATION MAC	SOURCE IP	DESTINATION I	DESTINATION PORT	PROTOCOL	*
	88	Married Works	-	-	-	53	UDP	
ß	80	-	-	-	and the second s	137	TCP	
6		-	No. of Concession, edited	Southern Street	Station of Concession, Name	137	UDP	
\$	56	800710300114	\$1000000000000000000000000000000000000	Shinks.	Same and	137	UDP	
	56	Mag	No. of Concession, Name	-	Silicity of	53	UDP	
	88	1000/1100/0000110	Man Constants	And so the second	Statutes of	53	UDP	
	80	No. 11 100100-011	1012-102-00-00 M	STATUTE OF	Statistics.	5353	UDP	
	58	Accesses 1	Manufacture and American	And a second	Statute of	53	UDP	
	50	-	10.00 (0.000 P ())	same.	Sciences of	5353	GRE	
i								*

#### Communications list.

A list of all the communications that have been made between the OT devices of the organization's network, and information about them, will be displayed.

A communication is understood as the grouping of connections between MAC, IP, and source port, and the same for the destination. It is considered a new communication if there is a change of protocol.

 Communications panel
 Is of 3008 Connectors

 Sensor D
 IP address
 MAC address
 Port

 All
 O
 283
 56
 30184
 O

Available communications filters

![](_page_51_Picture_20.jpeg)

8 0

![](_page_52_Picture_1.jpeg)

# 4.6 **Reports**

To access the list of reports, the user must click on the icon 🗅 that appears on the left side of the screen.

K	Guar	dian prOTech	admin Last access: 09	9/10/2024 14:59:32	[→ <u>Log Out</u>
ធ	Re	ports			
$\oplus$	Re	ports panel (i) 7 of 7 Reports			
	Туре	Start datetime         E           Image: Constraint of the start date image: Co	nd datetime		
0		FILE TYPE	CREATION DATE	FORMAT	OPTIONS
**	ß	Dispositivos no autorizados	30/09/2024 01:26	CSV	<u>الله</u>
Ľ	ß	Alertas	30/09/2024 01:26	CSV	<u>الله</u>
សា	Ľ	Scoring	30/09/2024 01:26	CSV	Ŀ
~	C	IPs públicas	30/09/2024 01:26	CSV	٤
	C	MACs & IPs	30/09/2024 01:26	CSV	<u>الله</u>
	Ľ	Dispositivos inalámbricos	30/09/2024 01:26	CSV	<u>الله</u>
	Ľ	Vulnerabilidades	30/09/2024 01:26	CSV	٤.
i					

Last available reports

A list of the reports generated both manually and automatically with a certain periodicity, available for downloading, will be displayed on the screen.

# 4.7 **Other settings**

In configuration, different parameters of the Service can be customised.

In the user profile, there is all the information associated with the identity with which the system is accessed. Some of the fields can be edited, such as the language, the telephone number, and the duration of the session token in minutes:

K	Guardian			Admin_4 Last access: 09	/10/2024 13:41:40		[→ <u>Log Out</u>
ធ	Settings						
₩	PROFILE	Profile data					
٩	THREAT DETECTION (항 General	User Admin_4	Language EN	Ø	Phone number		
유 []	영 General 삶 Preferences	Email	Current login 10/10/2024	15:10	Last login 9/10/2024	13:41	
ø		Session token lifetime (minutes) 720					
						Save	
i							

Profile data screen.

![](_page_52_Picture_12.jpeg)

![](_page_52_Picture_14.jpeg)

![](_page_53_Picture_1.jpeg)

In Threat Detection, the overall status of the different anomaly detection strategies is initially presented in traffic light mode (red, Orange, green):

<b>X</b>	Guardian	admin Lost occess: 09/10/2024 1459:32 ⊕	<u>Log Out</u>
ណ៍	Settings		
⊕ ▲ ●	PROFILE User THREAT DETECTION General ADVANCED Si General	General status Status of detection mechanisms  Rule Rule Hand	
t t i	♣ Preferences	based threats     based threats     based threats       SHOW STATUS     SHOW STATUS	
i			

Algorithm setting screen.

Rule-based threats

- Red: all rules are in training mode, inactive or not covered by their status field.
- Orange: some of the rules have production status, but not all of them.
- Green: all rules are in production mode.
- Grey: no rules exist.

#### AI/ML based threats

- Red: all rules are in training mode, inactive or not covered by their status field.
- Orange: some of the algorithms are in production mode, but not all of them.
- Green: all the algorithms are in production mode.
- Grey: No algorithms exist

Signature-based threats

- Red: all elements have a training value, inactive or some not covered in their status field.
- Orange: some of the elements have a value other than active, but not all of them.
- Green: all elements have a status equal to active and the signature\_timestamp field is less than seven days old.
- Grey: no elements exist.

![](_page_53_Picture_20.jpeg)

![](_page_53_Picture_23.jpeg)

![](_page_54_Picture_1.jpeg)

![](_page_54_Picture_2.jpeg)

![](_page_54_Picture_3.jpeg)

María Berdiales St. 20 4th floor 36203 Vigo, Spain. Tel: (+34) 886113106 page 55

![](_page_54_Picture_6.jpeg)

www.inprosec.com info

![](_page_55_Picture_1.jpeg)

# **5** ANNEX I: Devices and alerts classification.

## 5.1 **Devices classification**

### 5.1.1 According to State

- **Authorized/Unauthorized**: Authorized devices are those that the customer has explicitly recognized as legitimate.
- **Critical/Non-critical**: The Guardian system will not actively interact with those devices marked as critical. E.g. old devices, unmanned for maintenance, no spare parts, etc.
- **Fixed/Not fixed**: Fixed devices will appear in the Guardian application even if they have not established any communication in the organization's network. E.g. devices temporarily isolated from the network for maintenance.

### 5.2 Alerts classification

### 5.2.1 According to State

- **Resolved/Unresolved**: Alarms marked as resolved are those that have been dealt with, but you want to maintain the occurrence of the alarm in future identical situations (same typology, MACs, IPs, and ports involved). Those not resolved are pending management.

- **Silenced/Unsilenced**: Alarms declared as silenced will not occur again in the same network context\*. E.g. a device communicating with a public IP known and controlled by the organization, and you do not want alarms to be generated for this situation.

\* It is worth mentioning that silenced alarms, although not displayed to the user, are still stored in a database for later consultation by InprOTech staff at the customer's request, if necessary.

### 5.2.2 According to Severity

The severity levels of the application in terms of alert generation are taken from RFC 5424, although they are not equivalent since the severity of the events has been catalogued based on the experience of our technicians.

From greater to lesser severity, alerts are classified as follows:

- Emergency
- Alert
- Critical
- Error
- Warning
- Warning
- Informational
- Debug

![](_page_55_Picture_26.jpeg)

![](_page_56_Picture_1.jpeg)

# 6 ANNEX II: Asset Icons and Purdue Level

The Purdue model defines the following levels for existing devices:

Level 0: Field devices, such as sensors or actuators.

Level 1: Basic controllers, PLCs, I/O devices, and the first layer of security.

Level 2: Monitoring, supervision, and representation devices (SCADA and HMI systems, interfaces, or historical data servers).

Level 3: Operations and systems management devices, such as database servers and MES. Real-time planning and production control.

Level 4: Enterprise management devices, such as ERP, CRM, or SCM systems.

Certain devices may change their Purdue level depending on their function and location.

Icon	Description	PURDUE Level
	РС	2
	SCADA	2
	DCS	2
	Virtual	2
	HMI	2
	TABLET	2
	VOIP PHONE	2
	SERVER	2

![](_page_56_Picture_11.jpeg)

![](_page_56_Picture_13.jpeg)

![](_page_57_Picture_1.jpeg)

	HANDSET	2
	RTU	1
	VS-CAM	1
7	BARCODE READER	1
••	PLC	1
3	ROBOT	0
	FREQUENCY VARIATOR	0
	CONTROLLER CARD	0
	SENSOR	0
	AFD	0
	SWITCH	Various
	ROUTER	Various
	FIREWALL	Various
	OTHER	Various
働	HONEYPOT	Various

Table 1: Representative Icons of Devices

![](_page_57_Picture_6.jpeg)

![](_page_58_Picture_1.jpeg)

# 7 ANNEX III: Alert icons.

Icon	Description	
	Manual alert	
	Machine Learning alert	
	Static rule alert	
	IDS alert	
	Alerta de Honeypot	

![](_page_58_Picture_4.jpeg)

María Berdiales St. 20 4<sup>th</sup> floor 36203 Vigo, Spain. Tel: (+34) 886113106

![](_page_58_Picture_7.jpeg)