InprOTech

Smart security for your industry

INPROTECH GUARDIAN

Alerts Playbook

Date: 04/2023

Reference Doc: IN-Registro de alertas

Versión: 2.5

*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 or 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.*

INDICE

Contenido

1 Introduction

InprOTech Guardian is an industrial network cyber-surveillance service whose threat detection capabilities are based on three strategies:

- The use of heuristics (static rules for detecting possible compromise scenarios).
- The use of Machine learning (AI) algorithms to detect behavioral deviations from a pre-trained pattern specific to a particular industrial network (the client's).
- The implementation of an IDS (Snort), with the detection signatures of Cisco Talos, one of the main cyber-intelligence providers in the market, including Microsoft zero-day vulnerabilities.

Through the above, Guardian is able to identify thousands of attack scenarios, compromise or anomaly of the systems and services present in the industrial network, in order to mitigate their eventual impact.

In this document, the alerts generated by InprOTech Guardian, description, probable causes, consequences and recommended actions are indicated at a high level, so that the customer can take the best course of action with as much information as possible.

2 Static alerts

2.1 New device

Alarm:	**Priority:**
“New device”	Critical

Description:

New MAC address located in the organization's network.

Probable causes:

A new, previously unregistered "MAC" address has been detected for a device connected to the organization's network.

Impact:

Possibility of intrusion into the organization's network.

Recommended actions:

Locate the device who has the "MAC" triggering the alarm, verify its identity and legitimacy, and carry out the appropriate treatment of such equipment or connection.
Its location can be tracked on the network map of the "InprOTech Guardian" application.

1. If the new "MAC" address is considered legitimate and you do not want the warning to appear again in future connections, the alarm must be set as silenced. Likewise, if the device is considered to belong to the organization's network, it must be marked as authorized.

2. If the new "MAC" address is accepted but the notifications are to be maintained in future connections, the alarm must be configured as resolved.

Link to external information sources:

InprOTech Guardian User Manual.

2.2 New IP

Alarm:	**Priority:**
“New IP”	Warning
Description:	
New IP address located in the organization's network.	
Probable Causes:	
A new, previously unregistered "IP" address has been detected in a device connected to the organization's network.	
Impact:	
Possibility of intrusion into the organization's network.	
Solution:	
Identify the equipment that has the "IP" triggering the alert, verify its identity and legitimacy, and carry out the appropriate treatment of that equipment or connection. Its location can be tracked on the network map of the "InprOTech Guardian" application. 1. If the new "IP" address is considered legitimate and you do not want the warning to appear again in future connections, the alarm must be set as silenced. Likewise, if the device is considered belonging to the organization's network, it must be marked as authorized. 2. If the new "IP" address is accepted but the notifications are to be maintained in future connections, the alarm must be configured as resolved.	
Link to external information sources:	
InprOTech Guardian User Manual.	

2.3 New Connection

Alarm:	**Priority:**
“New Connection”	Warning
Description:	
Communication through a unusual device port.	
Probable Causes:	
A communication has been established in the device, making use of one of its previously unused ports.	
Impact:	
Possibility of illegitimate access to the device interface and intrusion into the organization's network.	
Solution:	
Identify the equipment that has received communication through a port different from those previously used. Verify the legitimacy of the other device and perform the appropriate treatment of such equipment or connection. Its location can be tracked using the network map of the "InprOTech Guardian" application. 1. In case of considering acceptable the use of the new port triggering the alarm and not wanting the warning to appear again in future connections to that port, the alarm must be managed as silenced. 2. In case of considering acceptable the use of the new port triggering the alarm, but willing to keep the notifications in future connections to that port, the alarm must be managed as resolved.	
Link to external information sources:	
InprOTech Guardian User Manual.	

2.4 Network port anomaly

Alarm:	**Priority:**
“Network port anomaly”	Warning

Description:

Different communications protocol compared to the first one registered, on a given port of the device.

Probable Causes:

Guardian has detected a communication using a different protocol than the first one registered on one of the device ports.

Impact:

Possibility of unwanted access to the device interface and intrusion into the organization's network.

Solution:

Identify the device that has undergone a change of communication protocol in one of its ports, verify its identity and legitimacy, and perform the appropriate treatment of such equipment or connection.
Its location can be tracked on the network map of the “InprOTech Guardian” application.

1. In case of considering acceptable the change of protocol in the port whose device triggers the alarm, and not wanting the warning to appear again in future protocol changes in that port, the alarm must be set as silenced.

2. In case of acceptance of the change of communication protocol in the port, object of the alarm, but you want to keep the notifications in future protocol changes in that port, the alarm must be managed as resolved.

Link to external information sources:

InprOTech Guardian User Manual.

2.5 New Public IP

Alarm:	**Priority:**
“New public IP”	Warning

Description:

Public IP address located on the organization's network.

Probable Causes:

A public "IP" address connected to one organization's device network, has been detected.

Impact:

Possibility of intrusion into the organization's network.

Solution:

Locate the equipment that has the connection with a public "IP" triggering the alarm, verify its identity and legitimacy, and carry out the treatment considered appropriate for that equipment or connection.
Its location can be tracked on the network map of the "InprOTech Guardian" application.

1. In case of considering the public "IP" address as legitimate and not wanting the warning to appear again in future connections, the alarm must be managed as silenced.

2. In the case of acceptance of the public IP address, but wanting to keep the notifications in future connections, the alarm should be set as resolved.

Link to external information sources:

InprOTech Guardian User Manual.

2.6 Connection with IT port

<table>
<tr><td><b>Alarm:</b></td><td><b>Priority:</b></td></tr>
<tr><td>“Connection with IT port”</td><td>Critical</td></tr>
<tr><td colspan="2"><b>Description:</b></td></tr>
<tr><td colspan="2">IT port communication in OT network</td></tr>
<tr><td colspan="2"><b>Probable Causes:</b></td></tr>
<tr><td colspan="2">A communication has been established from a device port usually dedicated to IT services within a network.</td></tr>
<tr><td colspan="2"><b>Impact:</b></td></tr>
<tr><td colspan="2">Possibility of intrusion into the organization's OT network.</td></tr>
<tr><td colspan="2"><b>Solution:</b></td></tr>
<tr><td colspan="2">Identify the device with a declared communications port in the IT network and which is establishing communication within the organization's OT environment. Verify its identity and legitimacy, and perform the appropriate treatment of such equipment.
Its location can be tracked on the network map of the InprOTech Guardian application.

1. In case of accepting the communication of the device with communications port declared as IT with equipment of the organization's OT network, and not wanting the warning to appear again in future communications, the alarm must be managed as silenced.

2. In the case of accepting the communication, but wanting to keep track of the notifications in future communications, the alarm must be set as resolved.</td></tr>
<tr><td colspan="2"><b>Link to external information sources:</b></td></tr>
<tr><td colspan="2">InprOTech Guardian User Manual.</td></tr>
</table>

2.7 Possible fingerprinting

Alarm:	**Priority:**
“Possible fingerprinting”	Warning

Description:

Device searching for open communication ports in the organization.

Probable Causes:

Guardian has detected that the IP address of a device, external or internal, is trying to establish communication with different "IPs" of computers in the organization in search of open ports.

Impact:

Possibility of unwanted access to the devices interface and intrusion into the organization's network.

Solution:

Identify the equipment that has the IP triggering the alarm, verify its identity and carry out the appropriate treatment of that equipment.
Its location can be tracked on the network map of the InprOTech Guardian application.

1. If it is a legitimate device and you do not want the warning to appear again in future connection attempts, the alarm must be managed as silenced.

2. If legitimate but wanting to keep the notifications on future connection attempts, you should manage the alarm as resolved.

Link to external information sources:

InprOTech Guardian User Manual.

2.8 Possible ARP spoofing

Alarm:	**Priority:**
“Possible ARP spoofing”	Warning

Description:

Device with new association between "IP" and "MAC" addresses.

Probable Causes:

Guardian has detected that the MAC address of one of the devices does not correspond to the previously registered IP address. Therefore, the device has experienced an IP address change.

Impact:

Possibility of intrusion into the organization's network.

Solution:

Identify the equipment that has undergone a change of "IP" address with respect to its "MAC" address.
Its location can be tracked on the network map of the InprOTech Guardian application.

1. If the new "IP" address in the device is considered correct, and not wanting the warning to appear again in future communications, the alarm must be managed as silenced. Likewise, if you want to assign this new "IP" address to the "MAC" address of the device, it must be replaced in the device settings.

2. In the case of accepting the new "IP" address on the device but you want to keep the notifications in future similar communications, the alarm must be set as resolved.

Link to external information sources:

InprOTech Guardian User Manual.

2.9 Inactivity alert

Alarm:	**Priority:**
“Inactivity alert”	Emergency
Description:	
The alert management module does not receive data from the traffic LCP (Log Collection Platform).	
Probable Causes:	
Eventual failure in one or more points of the communication between the LCP and the alert manager. Another reason could be a configuration error by the event timeout manager. The physical disconnection of the cable connected to the mirror port of the factory switch, where the traffic ingestion takes place, should also be considered.	
Impact:	
Potential loss of data; Guardian stops monitoring traffic, which implies risk.	
Solution:	
Physical check of the equipment to rule out connection problems. If everything is OK, it demands escalation to InprOtech for internal review from admin interface.	
Link to external information sources:	
InprOTech Guardian User Manual.	

3 IA/ML alarms

Alarm:	**Priority:**

Anomaly detected in {netflow/raw} traffic	*"{critical|alert}" depending on internal parameters (threshold and severity_delta)*
Description:	
Anomaly detected using the {algorithm} model, scoring: {score}.	
Probable Causes:	
Guardian system's AI engine has detected an anomaly in network traffic due to a deviation from normal behaviour patterns previously learnt during training.	
Impact:	
Possibility of intrusion into the organization's OT network or anomalous communication of any of its elements, since a deviation is detected with respect to the baseline behavior that the algorithm had learned during its training.	
Solution:	
Internal review of the anomaly to determine the real extension of the incident.	
Link to external information sources:	
InprOTech Guardian User Manual.	

4 IDS alarms

<table>
<tr><td><b>Alarm:</b></td><td><b>Priority:</b></td></tr>
<tr><td><i>{Snort IDS alert message field}</i></td><td><i>"{emergency|alert|error}" depending on the priority of the IDS alert.</i></td></tr>
<tr><td colspan="2"><b>Description:</b></td></tr>
<tr><td colspan="2"><i>{Snort IDS alert message field}</i></td></tr>
<tr><td colspan="2"><b>Probable Causes:</b></td></tr>
<tr><td colspan="2">Review additional associated information in the Snort database, using the link provided in the corresponding Alert Value field.</td></tr>
<tr><td colspan="2"><b>Impact:</b></td></tr>
<tr><td colspan="2">Analyze additional associated information in the Snort database, using the link provided in the Alert Value field.</td></tr>
<tr><td colspan="2"><b>Solution:</b></td></tr>
<tr><td colspan="2">Follow advice from Snort database or related sources, using the link provided in the Alert Value field.</td></tr>
<tr><td colspan="2"><b>Link to external information sources:</b></td></tr>
<tr><td colspan="2">InprOTech Guardian user manual, and Snort database (https://www.snort.org/rule_docs/).</td></tr>
</table>

5 Alerts proactive testing

The following instructs how to perform proactive tests to generate alerts in order to verify that threat detection strategies are performing as expected.

o When connecting a device with a new MAC to the network, the NEW DEVICE alert should be generated.

o Having a device, new or existing, raise a previously unregistered IP, would raise the NEW IP alert.

o When making a connection against a device on a port not used in the past, the NEW CONNECTION alert would appear.

o When making a connection against a device on a previously used port but a different protocol (e.g., http on https port or the reverse), we would have the NETWORK PORT ANOMALY alert.

o If a connection is made against a public IP from a device, the NEW PUBLIC IP alert would be triggered.

o If communications are seen within the OT network on ports usually labeled as IT (e.g. http. The comprehensive current standard list is: 20, 21, 22, 23, 23, 25, 80, 443, 143, 445), the CONNECTION WITH IT PORT alert will be generated.

o If a fingerprinting is done via TCP SYN against a device for example with NMAP and you exceed the thresholds (by default more than 3 in 5 minutes), the alert of POSSIBLE FINGERPRINTING will be triggered.

o If a MAC-IP association is changed, a POSSIBLE ARP SPOOFING alert will be generated, with a default timeout period of 1h.

o If there is a significant change in network behavior with respect to the usual, one or more alerts will be given for RAW/NETFLOW TRAFFIC ANOMALY. Forcing it, would perhaps be as easy as inserting a device into the network and setting it to download an ISO of an operating system, for example, or fingerprinting via TCP SYN against a device with NMAP, or changing MAC-IP associations.

o Regarding IDS signatures, you could try any of the list, which can be found here: https://www.snort.org/downloads#rules

* It is understood that each alert is given for a specific network context (IPs, MACs, port, protocol), and then there is a silent period defined in the configuration, so that when we are in that scenario, the alert is not generated.