NOZOMI NETWORKS

Alerts and Incidents
Reference Guide

2026-09-02

Legal notices

Information about the Nozomi Networks copyright and use of third-party software in the Nozomi Networks product suite.

Copyright

Third Party Software

Nozomi Networks uses third-party software, the usage of which is governed by the applicable license agreements from each of the software vendors. Additional details about used third-party software can be found at https://security.nozominetworks.com/licenses.

Contents

Chapter 1. Alerts

A description of alerts in the Nozomi Networks software.

Type ID
The strict identifier for an alert type. Use this field to setup integrations.

Name
A friendly name identifier.

Security profile
The default security profile the alert type belongs to.

Risk
The default base risk the alert shows. For specific instances, this value is weighted by other factors (the learning state of the involved nodes and their reputation) and it will result in a different number.

Details
General information about the alert event, and what has caused it.

Product Versions
The minimum product versions required to generate the Alert.

Trace
Whether a trace is produced or not.

Note:
Traces are always based on buffered data and, depending on the overall network traffic throughput, the buffer might not contain all of the packets responsible for the alert itself. Only the last packet responsible for triggering the alert is always present as the trace is generated.

Built-in checks

Built-in checks are based on specific signatures or hard-coded logics with reference to: known ICS threats (by signatures provided by Threat Intelligence), known malicious operations, system weaknesses, or protocol-compliant operations that can impact the network/ICS functionality. They might also leverage the Learning process to be more accurate.

SIGN:BOOT-SECURITY-ERROR

Boot security error

Type ID
SIGN:BOOT-SECURITY-ERROR

Security profile
Alerts of this type are visible in the following security profiles:

- PARANOID

Risk
The base risk for this alert is 7.

Cause
Some software or hardware subject to secure boot.

Solution
Revise the secure boot components and make sure everything is configured correctly to enable for a successful boot.

Product versions
Arc 1.14

Trace
Alerts of this type do not generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:CLEARTEXT-PASSWORD

Cleartext password

Type ID
SIGN:CLEARTEXT-PASSWORD

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 7.

Cause
A cleartext password has been issued or requested.

Solution
Update to secure communication or assess the risks of having this data exposed on the network.

Product versions
Guardian 19.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `PROTOCOL`

SIGN:CONFIGURATION-CHANGE

Configuration change

Type ID
SIGN:CONFIGURATION-CHANGE

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 6.

Cause
A changed configuration has been uploaded to the OT device. This can be a legitimate operation during maintenance and upgrade of the software or an unauthorized tentative to disrupt the normal behavior of the system.

Solution
Verify the device configuration and status.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `DESTINATION_NODE_ID`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:CPE:CHANGE

CPE change

Type ID
SIGN:CPE:CHANGE

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 0.

Cause
An installed software change has been detected. The change relates to the vulnerabilities list, possibly changing it.

Solution
Verify the device configuration and status, and the reason behind the software change.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:DEV-STATE-CHANGE

Device state change

Type ID
SIGN:DEV-STATE-CHANGE

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 7.

Cause
A command that can alter the device state has been detected. Examples are a request of reset of processor's memory, and technology-specific cases.

Solution
Verify the device configuration and status, and the reason behind the command.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Property `state_before`
- Property `state_after`

SIGN:DUALUSE-DETECTED

DUALUSE detection

Type ID
SIGN:DUALUSE-DETECTED

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 5.

Cause
A file transfer was identified as a known dual-use tool (e.g., nmap, PsExec). These tools serve legitimate administrative purposes but are also commonly abused by attackers, so their use should be verified.

Solution
Confirm whether the tool's use is authorized and expected on this network. If not, treat the source as potentially compromised and investigate or block it.

Product versions
Guardian 23.3.0

Trace
Alerts of this type do not generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`

SIGN:DUALUSE-DOMAIN

DUALUSE domain

Type ID
SIGN:DUALUSE-DOMAIN

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 4.

Cause
A DNS query was made for a domain associated with a known dual-use tool. These tools serve legitimate administrative purposes but are also commonly abused by attackers.

Solution
Verify that this usage is authorized and expected. If not, validate the health of the involved nodes, as they may be compromised.

Product versions
Guardian 24.0.0

Trace
Alerts of this type do not generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`

SIGN:DUALUSE-IP

DUALUSE IP

Type ID
SIGN:DUALUSE-IP

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 4.

Cause
A node communicated with an IP address associated with a known dual-use tool. These tools serve legitimate administrative purposes but are also commonly abused by attackers.

Solution
Verify that this communication is authorized and expected. If not, validate the health of the involved nodes, as they may be compromised.

Product versions
Guardian 24.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`

SIGN:DUALUSE-URL

DUALUSE URL

Type ID
SIGN:DUALUSE-URL

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 5.

Cause
A request was made to a URL associated with a known dual-use tool. These tools serve legitimate administrative purposes but are also commonly abused by attackers.

Solution
Verify that this usage is authorized and expected. If not, validate the health of the involved nodes, as they may be compromised.

Product versions
Guardian 24.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`

SIGN:FIRMWARE-TRANSFER

Firmware transfer

Type ID
SIGN:FIRMWARE-TRANSFER

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 6.

Cause
A firmware has been transferred to the device. This can be a legitimate operation during maintenance or an unauthorized attempt to change the behaviour of the device.

Solution
Verify the device configuration and status, and the possible presence of malicious actors.

Product versions
Guardian 19.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `PROTOCOL`

SIGN:FIRMWARE:CHANGE

Firmware change

Type ID
SIGN:FIRMWARE:CHANGE

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 6.

Cause
A changed firmware has been uploaded to the OT device. This can be a legitimate operation during maintenance and upgrade of the software or an unauthorized tentative to disrupt the normal behavior of the system.

Solution
Verify the device configuration and status, and the possible presence of malicious actors.

Product versions
Arc 1.12

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:INFORMATION-GATHERING

Information gathering

Type ID
SIGN:INFORMATION-GATHERING

Security profile
Alerts of this type are visible in the following security profiles:

- PARANOID

Risk
The base risk for this alert is 6.

Cause
Sensitive information has been transferred between an OT Device (e.g. an IED) and a workstation / local SCADA. This can be a legitimate troubleshooting operation or an unauthorized attempt to extract some device information.

Solution
Investigate on the actor that has initiated the transfer and on the transferred information.

Product versions
Guardian 24.1.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `PROTOCOL`

SIGN:LOGIN

Login to Device

Type ID
SIGN:LOGIN

Security profile
Alerts of this type are visible in the following security profiles:

- PARANOID

Risk
The base risk for this alert is 4.

Cause
A successful login to the device has been detected.

Solution
Verify whether the login was performed by authorized personnel, or credentials were stolen and should be updated.

Product versions
Arc 1.13

Trace
Alerts of this type do not generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:MALICIOUS-DOMAIN

Malicious domain

Type ID
SIGN:MALICIOUS-DOMAIN

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 8.

Cause
A DNS query towards a malicious domain has been detected.

Solution
Investigate on why this domain has been contacted and consider to ban it from your network.

Product versions
Guardian 19.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`

SIGN:MALICIOUS-HID

Malicious USB device

Type ID
SIGN:MALICIOUS-HID

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 10.

Cause
Suspicious behaviour detected in a device announcing itself as Human Interface Device (HID). It may be compromised, including malicious software running on it and performing dangerous actions targeting the main system it is connected to.

Solution
Disconnect the Human Interface Device (HID) and inspect it carefully, it might have an miniature embedded chip inside. Find the root cause of the unexpected behavior.

Product versions
Arc 1.0

Trace
Alerts of this type do not generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:MALICIOUS-IP

Bad ip reputation

Type ID
SIGN:MALICIOUS-IP

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 8.

Cause
A node with a bad reputation IP has been found.

Solution
Investigate on why this IP has been contacted and consider to ban it from your network.

Product versions
Guardian 19.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`

SIGN:MALICIOUS-URL

Malicious URL

Type ID
SIGN:MALICIOUS-URL

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 7.

Cause
A request towards a malicious URL has been detected.

Solution
Investigate on why this URL has been contacted and consider to ban it from your network.

Product versions
Guardian 19.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`

SIGN:MALWARE-DETECTED

Malware detection

Type ID
SIGN:MALWARE-DETECTED

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 9.

Cause
A potentially malicious payload has been transferred.

Solution
Investigate on the malware source and infected device, and consider to remove the file.

Product versions
Guardian 18.0.0

Trace
Alerts of this type do not generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`

SIGN:MITM

MITM attack

Type ID
SIGN:MITM

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 10.

Cause
A potential MITM attack has been detected. The attacker is ARP-poisoning the victims. The attacker node could alter the communication between its victims.

Solution
Investigate on the network configuration and the possible presence of malicious actors.

Product versions
Guardian 20.0.5

Trace
Alerts of this type do not generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Property `bad_actor`

SIGN:OT_DEVICE-REBOOT

OT device reboot request

Type ID
SIGN:OT_DEVICE-REBOOT

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 6.

Cause
An OT device program has been requested to reboot (e.g. by the engineering workstation). This may be something due to Engineering operations, for instance the maintenance of the program itself or a system updates. However, it may indicate suspicious activity from an attacker trying to manipulate the device execution.

Solution
Investigate on the network configuration and the possible presence of malicious actors.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:OT_DEVICE-START

OT device start request

Type ID
SIGN:OT_DEVICE-START

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 6.

Cause
An OT device program has been requested to start (e.g. by the engineering workstation). This may be something due to Engineering operations, for instance the maintenance of the program itself or a system updates. However, it may indicate suspicious activity from an attacker trying to manipulate the device execution.

Solution
Investigate on the network configuration and the possible presence of malicious actors.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `DESTINATION_NODE_ID`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:OT_DEVICE-STOP

OT device stop request

Type ID
SIGN:OT_DEVICE-STOP

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 9.

Cause
An OT device program has been requested to stop (e.g. by the engineering workstation). This may be something due to Engineering operations, for instance the maintenance of the program itself or a system updates. However, it may indicate suspicious activity from an attacker trying to manipulate the device execution.

Solution
Investigate on the network configuration and the possible presence of malicious actors.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `DESTINATION_NODE_ID`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:OUTBOUND-CONNECTIONS

High rate of outbound connections

Type ID
SIGN:OUTBOUND-CONNECTIONS

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 9.

Cause
A host has shown a sudden increase of outbound connections. This could be due to the presence of a malware.

Solution
Investigate on the reason behind such connections to the outside on the device, and consider to update the network configuration to prevent them.

Product versions
Guardian 21.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`

SIGN:PACKET-RULE

Packet rule match

Type ID
SIGN:PACKET-RULE

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 9.

Cause
A packet has matched a Packet rule.

Solution
Verify the device configuration and status, and the possible presence of malicious actors.

Product versions
Threat Intelligence

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`

SIGN:PASSWORD:WEAK

Weak password

Type ID
SIGN:PASSWORD:WEAK

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 5.

Cause
A weak password, possibly default, has been used to access a resource.

Solution
Consider to update your passwords.

Product versions
Guardian 18.5.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `PROTOCOL`

SIGN:PROGRAM:CHANGE

Program change

Type ID
SIGN:PROGRAM:CHANGE

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 6.

Cause
A changed program has been uploaded to the OT device. This can be a legitimate operation during maintenance and upgrade of the software or an unauthorized tentative to disrupt the normal behavior of the system.

Solution
Verify the device configuration and status, and the possible presence of malicious actors.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`

SIGN:PROGRAM:TRANSFER

Program transfer

Type ID
SIGN:PROGRAM:TRANSFER

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 6.

Cause
A program has been transferred between an OT Device (e.g. an IED) and a workstation / local SCADA. This can be a legitimate operation during maintenance and upgrade of the software or an unauthorized attempt to read the program logic.

Solution
Investigate on the entity that has initiated the transfer and on the program content.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:PUA-DETECTED

PUA detection

Type ID
SIGN:PUA-DETECTED

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 5.

Cause
A potentially unwanted application (PUA) payload was transferred. PUAs, such as adware or software bundled with third-party installers, are not outright malicious but serve no legitimate business purpose and are considered suspicious.

Solution
Investigate the source of the payload and the receiving device, and consider removing the application.

Product versions
Guardian 20.0.6

Trace
Alerts of this type do not generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`

SIGN:PUA-DOMAIN

PUA domain

Type ID
SIGN:PUA-DOMAIN

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 4.

Cause
A DNS query was made for a domain associated with a potentially unwanted application (PUA). PUAs, such as adware or bundled software, are not outright malicious but serve no legitimate business purpose.

Solution
Investigate the involved nodes and consider removing the associated application.

Product versions
Guardian 24.0.0

Trace
Alerts of this type do not generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`

SIGN:PUA-IP

PUA IP

Type ID
SIGN:PUA-IP

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 4.

Cause
A node communicated with an IP address associated with a potentially unwanted application (PUA). PUAs, such as adware or bundled software, are not outright malicious but serve no legitimate business purpose.

Solution
Investigate the involved nodes and consider removing the associated application.

Product versions
Guardian 24.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`

SIGN:PUA-URL

PUA URL

Type ID
SIGN:PUA-URL

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 5.

Cause
A request was made to a URL associated with a potentially unwanted application (PUA). PUAs, such as adware or bundled software, are not outright malicious but serve no legitimate business purpose.

Solution
Investigate the involved nodes and consider removing the associated application.

Product versions
Guardian 24.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`

SIGN:SD-CARD

SD card operation

Type ID
SIGN:SD-CARD

Security profile
Alerts of this type are visible in the following security profiles:

- PARANOID

Risk
The base risk for this alert is 6.

Cause
This is most likely a human-driven event.

Solution
SD cards might be a physical infiltration vector carrying files with malicious behaviour. Check the device nature and its content.

Product versions
Arc 1.14

Trace
Alerts of this type do not generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:SIGMA-RULE

Sigma rule match

Type ID
SIGN:SIGMA-RULE

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 9.

Cause
Rule-dependent. A suspicious local event has been detected on a machine.

Solution
Rule-dependent. Verify the device configuration and status, and the possible presence of malicious processes.

Product versions
Arc 1.0, Threat Intelligence

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`

SIGN:SUSP-TIME

Suspicious time value

Type ID
SIGN:SUSP-TIME

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 7.

Cause
A suspicious time has been observed in the network. There could be a malfunctioning device or a packet injection.

Solution
Verify the device configuration and status.

Product versions
Guardian 20.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Property `time_server`

SIGN:USB-DEVICE

New USB device connected

Type ID
SIGN:USB-DEVICE

Security profile
Alerts of this type are visible in the following security profiles:

- PARANOID

Risk
The base risk for this alert is 6.

Cause
This is most likely a human driven event.

Solution
USB devices might be a physical infiltration vector carrying files with malicious behaviour. Check the device nature and its content.

Product versions
Arc 1.0

Trace
Alerts of this type do not generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `SOURCE_MAC`
- Property `usb_device_identifier`

SIGN:USB-FILE-TRANSFER

USB file transfer

Type ID
SIGN:USB-FILE-TRANSFER

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 6.

Cause
A user or operator has connected a USB device and transferred data, or a script might have initiated the operation.

Solution
Verify whether the operation is permitted.

Product versions
Arc 1.9

Trace
Alerts of this type do not generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:WEAK-ENCRYPTION

Weak encryption

Type ID
SIGN:WEAK-ENCRYPTION

Security profile
Alerts of this type are visible in the following security profiles:

- PARANOID

Risk
The base risk for this alert is 6.

Cause
The communication has been encrypted using an obsolete cryptographic protocol, weak cipher suites or invalid certificates.

Solution
Update to more secure algorithms or assess the risks of using this technology on the network.

Product versions
Guardian 19.0.5

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `DESTINATION_NODE_ID`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:WIFI:CONNECTION-ATTEMPT

Repeated Connection Attempt

Type ID
SIGN:WIFI:CONNECTION-ATTEMPT

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 3.

Cause
The device failed to connect to the Wi-Fi network. This is most often due to an incorrect or outdated password, but can also result from a mismatch in security or authentication mode (such as WPA2, WPA3, or 802.1X), rejection by RADIUS or MAC filtering, or—less commonly—radio frequency (RF) instability.

Solution
Check the Wi-Fi password, security mode, and authentication settings on both the device and access point. Review logs for authentication errors or filtering issues. If the problem persists, analyze the connection process in detail.

Product versions
Guardian Air 1.0.15

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:WIFI:DEAUTH:ATTEMPT

Deauth Attack Attempt

Type ID
SIGN:WIFI:DEAUTH:ATTEMPT

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 5.

Cause
The 802.11 family of standards (also known as WiFi) includes a way for Access Points to disconnect clients through specific packets. However, this management functionality allows attackers to disrupt WiFi networks easily.

Solution
More recent 802.11 Access Points and devices support the 802.11w extension, which makes client deauthentication and disassociation available only from real Access Points governing those clients. Check with your Access Point configuration if such extension is available, and enable it.

Product versions
Guardian Air 1.0.1

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:WIFI:DEAUTH:SUCCESS

Deauth Attack

Type ID
SIGN:WIFI:DEAUTH:SUCCESS

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 10.

Cause
The 802.11 family of standards (also known as WiFi) includes a way for Access Points to disconnect clients through specific packets. However, this management functionality allows attackers to disrupt WiFi networks easily.

Solution
More recent 802.11 Access Points and devices support the 802.11w extension, which makes client deauthentication and disassociation available only from real Access Points governing those clients. Check with your Access Point configuration if such extension is available, and enable it.

Product versions
Guardian Air 1.0.1

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:WIFI:ESPNOW-ATTACK

ESP-NOW attack

Type ID
SIGN:WIFI:ESPNOW-ATTACK

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 5.

Cause
A replay attack using ESP-NOW protocol has been detected. An attacker is resending previously captured ESP-NOW frames to disrupt or manipulate wireless device communication.

Solution
ESP-NOW protocol does not implement proper protections against replay attacks. An attacker can inject a huge amount of ESP-NOW frames to saturate the receivers cache and replay older frames.

Product versions
Guardian Air 1.0.1

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:WIFI:LORA-ANOMALY

Lora Anomaly

Type ID
SIGN:WIFI:LORA-ANOMALY

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 5.

Cause
Anomalous LoRaWAN protocol activity detected that may indicate potential security threats, protocol violations, or interference in Low Power Wide Area Network communications.

Solution
Verify the legitimacy of LoRaWAN device operations and ensure network integrity. If issues persist, restart the affected device or re-register it through the network management application, then re-execute the Join procedure between the End-Node and Gateway. Additionally, investigate the possibility of replay attacks or device spoofing, while implementing ongoing monitoring for any unauthorized LoRaWAN devices in the network.

Product versions
Guardian Air 1.0.1

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:WIFI:REGION-MISMATCH

Region mismatch on Japan country

Type ID
SIGN:WIFI:REGION-MISMATCH

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 3.

Cause
A packet is using Japan's country code (JP) in a non-Japanese region. This configuration incorrectly enables WiFi channel 14, which is legally restricted to Japan only and violates regulatory compliance elsewhere.

Solution
Reconfigure the device with the correct regional country code through its administration interface or firmware update to ensure regulatory compliance and prevent potential legal issues or network disruptions.

Product versions
Guardian Air 1.0.16

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:WIFI:SSID-XSS-INJECTION

SSID XSS injection attempt

Type ID
SIGN:WIFI:SSID-XSS-INJECTION

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 5.

Cause
An attacker may be aware that a wireless-enabled device is flawed by an XSS vulnerability in its web interface, and they are trying to leverage this issue to get execution of arbitrary HTML/JavaScript code. If successful, in the worst case, this can lead to full device compromise and network penetration.

Solution
Typically, exploiting these vulnerabilities requires user interaction. For example, the vulnerable web application must be accessed through a web browser. Advise your personnel to avoid browsing web applications related to wireless devices until the rogue SSID has been taken down.

Product versions
Guardian Air 1.0.1

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Property `malicious_ssid`

SIGN:WIRELESS:BLE-MALFORMED-CONNECTION

Bluetooth Malformed Connection Request

Type ID
SIGN:WIRELESS:BLE-MALFORMED-CONNECTION

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 5.

Cause
In 2020, a collection of 18 vulnerabilities, called SweynTooth, was discovered. These vulnerabilities are reported to expose flaws in specific BLE (Bluetooth Low Energy) devices, allowing an attacker to trigger deadlocks, crashes, buffer overflows, or the complete bypass of security.

Solution
Keep the device as up-to-date as possible: many of the affected manufacturers have already released firmware updates.

Product versions
Guardian Air 1.0.1

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:WIRELESS:INJECTION

Suspected wireless packet injection

Type ID
SIGN:WIRELESS:INJECTION

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 5.

Cause
A wireless packet that looks to have been injected by an attacker has been captured.

Solution
Check the surroundings of the involved assets and its wireless network.

Product versions
Guardian Air 1.0.1

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Property `attack_key`

SIGN:WIRELESS:ODID-VIOLATION-RULES

OpenDrone ID packet violating rules

Type ID
SIGN:WIRELESS:ODID-VIOLATION-RULES

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 5.

Cause
Anomalous Open Drone ID (ODID) telemetry data detected that may indicate potential security threats or protocol violations in drone communications.

Solution
Verify the legitimacy of drone operations in the airspace. Investigate potential packet injection attacks or spoofing attempts. Consider implementing additional authentication mechanisms for drone telemetry.

Product versions
Guardian Air 1.0.1

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

Custom checks

These are checks set in place by the user. Typically the nature of an event related to a custom check cannot generally be referred to a problem per se, if not contextualized to the specific network and installation.

ASRT:FAILED

Assertion failed

Type ID
ASRT:FAILED

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 0.

Cause
An assertion has failed.

Solution
Assertion dependent. Check out the elements making the assertion to fail.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

GENERIC:EVENT

Generic Event

Type ID
GENERIC:EVENT

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 0.

Cause
A generic event has been generated by the SDK.

Solution
Event dependent. More details are available in the description of the event.

Product versions
Guardian 20.0.5

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `PROTOCOL`

NET:INACTIVE-PROTOCOL

Inactive protocol

Type ID
NET:INACTIVE-PROTOCOL

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 3.

Cause
The link has been inactive for longer than the set threshold.

Solution
Investigate whether that is the expected behavior or something prevents the link from working.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `PROTOCOL`

NET:LINK-RECONNECTION

Link reconnection

Type ID
NET:LINK-RECONNECTION

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 3.

Cause
The link configured to be persistent has experienced a complete TCP reconnection.

Solution
Investigate whether the reconnection is legitimate.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `PROTOCOL`

NET:TCP-SYN

TCP SYN

Type ID
NET:TCP-SYN

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 3.

Cause
A connection attempt (TCP SYN) has been detected on a link.

Solution
Investigate on the entity that has attempted to connect.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

PROC:CRITICAL-STATE-OFF

Critical state off

Type ID
PROC:CRITICAL-STATE-OFF

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 1.

Cause
The system has recovered from a user-defined critical process state.

Solution
Investigate such critical state.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

PROC:CRITICAL-STATE-ON

Critical state on

Type ID
PROC:CRITICAL-STATE-ON

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 9.

Cause
The system has entered in a user-defined critical process state.

Solution
Investigate on the values and whether the process is at risk.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

PROC:INVALID-VARIABLE-QUALITY

Invalid variable quality

Type ID
PROC:INVALID-VARIABLE-QUALITY

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 3.

Cause
A variable has showed a quality bit set for longer than the set threshold.

Solution
Investigate on the protocol implementation and the process status.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

PROC:NOT-ALLOWED-INVALID-VARIABLE

Not allowed variable quality

Type ID
PROC:NOT-ALLOWED-INVALID-VARIABLE

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 3.

Cause
A variable has shown one or more specific quality bits the user set as not allowed.

Solution
Investigate on the protocol implementation and the process status.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

PROC:STALE-VARIABLE

Stale variable

Type ID
PROC:STALE-VARIABLE

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 3.

Cause
A variable has not been read/written for longer than the set threshold.

Solution
Investigate on the protocol implementation and the link and process status.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

Protocol validations

An undesired protocol behavior has been detected. This can refer to a wrong single message, to a correct single message not supposed to be transmitted or transmitted at the wrong time (state machines violation) or to a malicious message sequence. Protocol specific error messages indicating misconfigurations also trigger alerts that fall into this category.

NET:RST-FROM-PRODUCER

Link RST request by Producer

Type ID
NET:RST-FROM-PRODUCER

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 3.

Cause
The link has been dropped because of a TCP RST sent by the producer.

Solution
Verify that the device is working properly, no misconfigurations are in place and that network does not suffer excessive latency.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `DESTINATION_NODE_ID`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

PROC:SYNC-ASKED-AGAIN

Producer sync request by Consumer

Type ID
PROC:SYNC-ASKED-AGAIN

Security profile
Alerts of this type are visible in the following security profiles:

- PARANOID

Risk
The base risk for this alert is 3.

Cause
A new sync (e.g. General Interrogation in iec101 and iec104) command has been issued, while in some links it is sent only once per started connection. It may be due to a specific sync request of an operator, a cyclic sync, or to someone trying to discover the process global state.

Solution
Investigate on the protocol implementation and possible presence of malicious actors.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `PROTOCOL`

PROC:WRONG-TIME

Process time issue

Type ID
PROC:WRONG-TIME

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 3.

Cause
The time stamp specified in process data is not aligned with current time. There could be a time sync issue with the source device, a malfunctioning or a packet injection.

Solution
Verify the device configuration and status.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:ARP-FLOOD

ARP flood

Type ID
SIGN:ARP-FLOOD

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 7.

Cause
One or more hosts have sent a great amount of ARP packets

Solution
Verify the device configuration and status, and the possible presence of malicious actors.

Product versions
Guardian 24.2.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:ARP:DUP

Duplicated IP

Type ID
SIGN:ARP:DUP

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 5.

Cause
ARP messages have shown a duplicated IP address in the network. It may be a misconfiguration of one of the devices, or a tentative of a MITM attack.

Solution
Investigate on the network configuration and the possible presence of malicious actors.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:DDOS

DDOS attack

Type ID
SIGN:DDOS

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 5.

Cause
A suspicious Distributed Denial of Service has been detected on the network.

Solution
Verify that all the devices in the network are allowed and behaving correctly.

Product versions
Guardian 19.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `DESTINATION_NODE_ID`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:DHCP-OPERATION

DHCP operation

Type ID
SIGN:DHCP-OPERATION

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 4.

Cause
A suspicious DHCP operation has been detected. This is related to the presence of new Mac addresses served by DHCP server, and to DHCP wrong replies.

Solution
Investigate on the network configuration and the possible presence of malicious actors.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Property `dhcp_server`

SIGN:ILLEGAL-PARAMETERS

Illegal parameters request

Type ID
SIGN:ILLEGAL-PARAMETERS

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 7.

Cause
A request with illegal parameters (e.g. outside from a legal range) has been issued. This may mean that a malfunctioning software is trying to perform an operation without success or that a malicious attacker is trying to understand the functionalities of the device.

Solution
Verify the device configuration and status, and the possible presence of malicious actors.

Product versions
Guardian 19.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:INVALID-IP

Invalid IP

Type ID
SIGN:INVALID-IP

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 7.

Cause
A packet with an IP reserved for special purposes (e.g. loopback addresses) has been detected. Packets with such addresses can be related to misconfigurations or spoofing/denial of service attacks.

Solution
Investigate on the network configuration and the possible presence of malicious actors.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`

SIGN:MAC-FLOOD

Flood of MAC addresses

Type ID
SIGN:MAC-FLOOD

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 7.

Cause
A high number of new MAC addresses has appeared in a short time. This can be a flooding technique.

Solution
Investigate on the network configuration and the possible presence of malicious actors.

Product versions
Guardian 20.0.1

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:MALFORMED-TRAFFIC

Malformed traffic

Type ID
SIGN:MALFORMED-TRAFFIC

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 7.

Cause
A L7 malformed packet has been detected. A maliciously malformed packet can target known issues in devices or software versions, and thus should be considered carefully as a source of a possible attack.

Solution
Investigate on the protocol implementation and the possible presence of malicious actors.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:MALICIOUS-PROTOCOL

Malicious protocol

Type ID
SIGN:MALICIOUS-PROTOCOL

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 6.

Cause
An attempted communication by a protocol known to be related to threats has been detected.

Solution
Verify the device configuration and status, and the possible presence of malicious actors.

Product versions
Guardian 19.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`

SIGN:MULTIPLE-ACCESS-DENIED

Multiple Access Denied events

Type ID
SIGN:MULTIPLE-ACCESS-DENIED

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 8.

Cause
A host has repeatedly been denied access to a resource.

Solution
Verify whether the calling device is supposed to access those resources and tune the authorization permissions accordingly.

Product versions
Guardian 19.0.5

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `DESTINATION_NODE_ID`
- Attribute `PROTOCOL`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:MULTIPLE-OT_DEVICE-RESERVATIONS

Multiple OT device reservations

Type ID
SIGN:MULTIPLE-OT_DEVICE-RESERVATIONS

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 8.

Cause
A host has repeatedly tried to reserve the usage of an OT device causing a potential denial-of-service.

Solution
Verify the device configuration and status, and the possible presence of malicious actors.

Product versions
Guardian 19.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:MULTIPLE-UNSUCCESSFUL-LOGINS

Multiple unsuccessful logins

Type ID
SIGN:MULTIPLE-UNSUCCESSFUL-LOGINS

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 8.

Cause
A host has repeatedly tried to login to a service without success. It can be either an user or a script, and due to a malicious entity, or a wrong configuration.

Solution
Verify whether the calling device is supposed to access the target device and tune the authentication credentials accordingly.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:NET-MALFORMED

Malformed Network/Transport layer

Type ID
SIGN:NET-MALFORMED

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 7.

Cause
A packet containing a semantically invalid sequence below the application layer has been observed.

Solution
Investigate on the protocol implementation, and the possible presence of malicious actors.

Product versions
Guardian 20.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:NETWORK-SCAN

Network Scan

Type ID
SIGN:NETWORK-SCAN

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 7.

Cause
An attempt to reach many target hosts or ports in a target network (vertical or horizontal scan) has been detected.

Solution
Investigate whether it is an expected behavior or a malicious scan activity is undergoing.

Product versions
Guardian 19.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:PROC:MISSING-VAR

Missing variable request

Type ID
SIGN:PROC:MISSING-VAR

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 6.

Cause
An attempt to access an unexisting variable has been made. This may be due to a misconfiguration or a tentative to discover valid variables inside a producer. Example: COT 47 in iec104.

Solution
Verify the device configuration and status, and the possible presence of malicious actors.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `PROTOCOL`
- Property `variable`

SIGN:PROC:UNKNOWN-RTU

Missing or unknown device

Type ID
SIGN:PROC:UNKNOWN-RTU

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 6.

Cause
An attempt to access an unexisting virtual RTU (controller's logical portion) has been made. This may be due to a misconfiguration or a tentative to discover valid virtual producer RTU. Example: COT 46 in iec104.

Solution
Verify the device configuration and status, and the possible presence of malicious actors.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `PROTOCOL`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`

SIGN:PROTOCOL-ERROR

Protocol error

Type ID
SIGN:PROTOCOL-ERROR

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 7.

Cause
A generic protocol error occurred, this usually relates to a wrong field, option or other general violation of the protocol.

Solution
Investigate on the protocol implementation, and the possible presence of malicious actors.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:PROTOCOL-FLOOD

Protocol-based flood

Type ID
SIGN:PROTOCOL-FLOOD

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 7.

Cause
One or more hosts have sent a suspiciously high amount of packets with the same application layer (e.g., ping requests) to a single, target host.

Solution
Verify the device configuration and status, and the possible presence of malicious actors.

Product versions
Guardian 19.0.4

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `PROTOCOL`

SIGN:PROTOCOL-INJECTION

Protocol packet injection

Type ID
SIGN:PROTOCOL-INJECTION

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 6.

Cause
A correct protocol packet in the wrong context has been detected: this may be caused by an injection, network retransmissions, or a non compliant protocol implementation, and may cause equipment to operate improperly. Example: a correct GOOSE message sent with a wrong stNum/sqNum.

Solution
Investigate on the protocol implementation, the presence of retransmissions due to network configurations, and the possible presence of malicious actors.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `DESTINATION_NODE_ID`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:TCP-FLOOD

TCP flood

Type ID
SIGN:TCP-FLOOD

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 7.

Cause
One or more hosts have sent a great amount of anomalous TCP packets or TCP FIN packets to a single, target host.

Solution
Verify the device configuration and status, and the possible presence of malicious actors.

Product versions
Guardian 19.0.4

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `DESTINATION_NODE_ID`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:UDP-FLOOD

UDP flood

Type ID
SIGN:UDP-FLOOD

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 7.

Cause
One or more hosts have sent a great amount of UDP packets to a single target host.

Solution
Verify the device configuration and status, and the possible presence of malicious actors.

Product versions
Guardian 20.0.7.1

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `DESTINATION_NODE_ID`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`

SIGN:UNSUPPORTED-FUNC

Unsupported function request

Type ID
SIGN:UNSUPPORTED-FUNC

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 7.

Cause
An unsupported function (e.g. not defined in the specification) has been used on the OT device. This may be a malfunctioning software trying to perform an operation without success or a malicious attacker trying to understand the device functionalities. Example: COT 44 in iec104.

Solution
Verify the device configuration and status, and the possible presence of malicious actors.

Product versions
Guardian 19.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Property `function_code`

Learned behavior (virtual image)

Virtual image represents a set of information by which Guardian represents the monitored network. This includes for example node properties, links, protocols, function codes, variables, variable values. Such information is collected via learning, smart polling, or external contents, such as Asset Intelligence. Alerts in this group represent deviations from expected behaviors, according to the learned or fed information. When an alert of this category is raised, if the related event is not considered a malicious attack or an anomaly, it can be learned.

SIGN:WIRELESS:CELLULAR-ROGUE

Rogue Cell Tower Detected

Type ID
SIGN:WIRELESS:CELLULAR-ROGUE

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 7.

Cause
Rogue Cell Towers are false base stations that hijack nearby mobile device connections, performing active or passive attacks against devices. They trick the mobile device into thinking it is connected to an authorized cell tower, leaving it vulnerable to man-in-the-middle attacks and increasing threats to privacy. In this way, an attacker can collect private information about you indirectly through metadata, as well as tracing users' location and capturing the content of messages or calls.

Solution
To date, the detection of Rogue Cell Towers can't be done by the mobile device's operating system. Usually, the attacker is not very far from the targeted devices: if possible, start an investigation to find suspicious antennas. Also, if supported, it is advisable to use your mobile device's full 5G connection, less vulnerable than 3G (UMTS) and 4G (LTE) connections.

Product versions
Guardian Air 1.0.1

Trace
Alerts of this type are expected to generate traces.

Deduplication key

- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Property `cell_context`

VI:CONF-MISMATCH

Configuration Mismatch

Type ID
VI:CONF-MISMATCH

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 7.

Cause
A parameter describing a configuration version that was previously imported from a project has been observed having a different value in the traffic.

Solution
Validate the event and learn it if legitimate, or treat it as anomaly.

Product versions
Guardian 20.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `DESCRIPTION`

VI:GLOBAL:NEW-FUNC-CODE

New global function code

Type ID
VI:GLOBAL:NEW-FUNC-CODE

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 5.

Cause
A previously unknown protocol Function Code for has appeared in the network.

Solution
Validate the event and learn it if legitimate, or treat it as anomaly.

Product versions
Guardian 19.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `DESCRIPTION`

VI:GLOBAL:NEW-MAC-VENDOR

New global MAC vendor

Type ID
VI:GLOBAL:NEW-MAC-VENDOR

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 5.

Cause
A previously unknown MAC vendor has appeared in the network.

Solution
Validate the event and learn it if legitimate, or treat it as anomaly.

Product versions
Guardian 19.0.4

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `SOURCE_MAC`

VI:GLOBAL:NEW-VAR-PRODUCER

New global variable producer

Type ID
VI:GLOBAL:NEW-VAR-PRODUCER

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 5.

Cause
A node has started sending variables. It can be a new command, a new object, or a tentative of enumerating existing variables from a malicious attacker.

Solution
Validate the event and learn it if legitimate, or treat it as anomaly.

Product versions
Guardian 21.3.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `PROTOCOL`
- Property `var_key`

VI:KB:UNKNOWN-FUNC-CODE

Unknown asset function code

Type ID
VI:KB:UNKNOWN-FUNC-CODE

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 5.

Cause
The node has communicated using a function code that is not known for this kind of Asset. This detection is possible by knowing the specific Asset's profile.

Solution
Validate the event and learn it if legitimate, or treat it as anomaly.

Product versions
Asset Intelligence

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `DESCRIPTION`

VI:KB:UNKNOWN-PROTOCOL

Unknown asset's protocol

Type ID
VI:KB:UNKNOWN-PROTOCOL

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 5.

Cause
The node has communicated using a protocol that is not known for this kind of Asset. This detection is possible by knowing the specific Asset's profile.

Solution
Validate the event and learn it if legitimate, or treat it as anomaly.

Product versions
Asset Intelligence

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `DESCRIPTION`

VI:NEW-ARP

New ARP

Type ID
VI:NEW-ARP

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 4.

Cause
A new MAC Address has started requesting ARP information.

Solution
Validate the event and learn it if legitimate, or treat it as anomaly.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `SOURCE_MAC`
- Attribute `SOURCE_IP`

VI:NEW-FUNC-CODE

New function code

Type ID
VI:NEW-FUNC-CODE

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 6.

Cause
A known protocol between two nodes has started using a new function code (i.e. message type). For example, if a client A normally uses a function code 'read' when talking to server B, this alert is raised if client A begins to use a function code 'write'.

Solution
Validate the event and learn it if legitimate, or treat it as anomaly.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `DESCRIPTION`

VI:NEW-LINK

New link

Type ID
VI:NEW-LINK

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 4.

Cause
Two nodes have started communicating with each other with a new protocol.

Solution
Validate the event and learn it if legitimate, or treat it as anomaly.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `PROTOCOL`

VI:NEW-LINK-CONFIRMED

New confirmed link

Type ID
VI:NEW-LINK-CONFIRMED

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 5.

Cause
Two nodes have started communicating with each other with a new, confirmed protocol.

Solution
Validate the event and learn it if legitimate, or treat it as anomaly.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `PROTOCOL`

VI:NEW-LINK-GROUP

New link group

Type ID
VI:NEW-LINK-GROUP

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 5.

Cause
Two nodes have started communicating with each other.

Solution
Validate the event and learn it if legitimate, or treat it as anomaly.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`

VI:NEW-MAC

New MAC address

Type ID
VI:NEW-MAC

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 6.

Cause
A new MAC Address has appeared in the network.

Solution
Validate the event and learn it if legitimate, or treat it as anomaly.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `DESCRIPTION`

VI:NEW-NET-DEV

New network device

Type ID
VI:NEW-NET-DEV

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 3.

Cause
A new network device (switch or router) has appeared on the network.

Solution
Validate the event and learn it if legitimate, or treat it as anomaly.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`

VI:NEW-NODE

New node

Type ID
VI:NEW-NODE

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 5.

Cause
A new node has appeared on the network.

Solution
Validate the event and learn it if legitimate, or treat it as anomaly.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`

VI:NEW-NODE:DUALUSE-IP

DUALUSE IP (new node)

Type ID
VI:NEW-NODE:DUALUSE-IP

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 4.

Cause
A node was observed communicating, for the first time, with an IP address associated with a known dual-use tool. These tools serve legitimate administrative purposes but are also commonly abused by attackers.

Solution
Verify that this communication is legitimate and expected, then approve it as normal behavior; otherwise, treat it as anomalous and investigate.

Product versions
Guardian 24.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`

VI:NEW-NODE:MALICIOUS-IP

Bad IP reputation (new node)

Type ID
VI:NEW-NODE:MALICIOUS-IP

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 5.

Cause
A node with a bad reputation IP has been detected. It is suggested to validate the health status of communicating nodes, as they may be infected by some malware.

Solution
Validate the event and learn it if legitimate, or treat it as anomaly.

Product versions
Guardian 20.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`

VI:NEW-NODE:PUA-IP

PUA IP (new node)

Type ID
VI:NEW-NODE:PUA-IP

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 4.

Cause
A node was observed communicating with an IP address associated with a potentially unwanted application (PUA). PUAs, such as adware or bundled software, are not outright malicious but serve no legitimate business purpose.

Solution
Verify that the applications installed on the involved asset are legitimate and expected; otherwise, remove them.

Product versions
Guardian 24.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`

VI:NEW-NODE:TARGET

New target node

Type ID
VI:NEW-NODE:TARGET

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 4.

Cause
A new target node has appeared on the network. This node is not yet confirmed to exist as it still has not sent back any data.

Solution
Validate the event and learn it if legitimate, or treat it as anomaly.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `DESTINATION_MAC`

VI:PROC:NEW-VALUE

New OT variable value

Type ID
VI:PROC:NEW-VALUE

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 6.

Cause
A variable has been set to a value never seen before.

Solution
Validate the event and learn it if legitimate, or treat it as anomaly.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `DESCRIPTION`

VI:PROC:NEW-VAR

New OT variable

Type ID
VI:PROC:NEW-VAR

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 6.

Cause
A new variable has been sent, or accessed by a client. It can be a new command, a new object, or a tentative of enumerating existing variables from a malicious attacker.

Solution
Validate the event and learn it if legitimate, or treat it as anomaly.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `DESCRIPTION`

VI:PROC:PROTOCOL-FLOW-ANOMALY

Protocol flow anomaly

Type ID
VI:PROC:PROTOCOL-FLOW-ANOMALY

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 8.

Cause
A message aimed at reading/writing one or multiple variables which is sent cyclically, has changed its transmission interval time. Example: a iec104 command breaking its normal transmission cycle.

Solution
Validate the event and learn it if legitimate, or treat it as anomaly.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `SOURCE_NODE_ID`
- Attribute `DESTINATION_NODE_ID`
- Attribute `SOURCE_MAC`
- Attribute `DESTINATION_MAC`
- Attribute `DESCRIPTION`

VI:PROC:VARIABLE-FLOW-ANOMALY

Variable flow anomaly

Type ID
VI:PROC:VARIABLE-FLOW-ANOMALY

Security profile
Alerts of this type are visible in the following security profiles:

- HIGH
- PARANOID

Risk
The base risk for this alert is 6.

Cause
A variable which is sent cyclically has changed its transmission interval time.

Solution
Validate the event and learn it if legitimate, or treat it as anomaly.

Product versions
Guardian 18.0.0

Trace
Alerts of this type are expected to generate traces.

Deduplication key
- Attribute `TYPE_ID`
- Attribute `PROTOCOL`
- Property `var_key`

VI:WIRELESS:GEOFENCE

Geofencing event

Type ID
VI:WIRELESS:GEOFENCE

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 7.

Cause
A geofencing event involving an asset was detected.

Solution
Review the asset's geofencing event and verify if the activity is expected or authorized.

Product versions
Guardian Air 1.0.18

Trace
Alerts of this type do not generate traces.

Deduplication key
- Attribute `SOURCE_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Property `geofence_area_id`
- Property `geofence_event`

VI:WIRELESS:PROTECTED_NETWORK

Protected network event

Type ID
VI:WIRELESS:PROTECTED_NETWORK

Security profile
Alerts of this type are visible in the following security profiles:

- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 7.

Cause
A protected network event involving an asset was detected.

Solution
Review the asset's access rights for this wireless network. Update the list of permitted assets if the change is authorized, or investigate unauthorized activity.

Product versions
Guardian Air 1.0.20

Trace
Alerts of this type do not generate traces.

Deduplication key
- Attribute `SOURCE_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Property `wireless_network_id`

VI:WIRELESS:ROGUE-AP

Rogue Access Point

Type ID
VI:WIRELESS:ROGUE-AP

Security profile
Alerts of this type are visible in the following security profiles:

- LOW
- MEDIUM
- HIGH
- PARANOID

Risk
The base risk for this alert is 8.

Cause
A new Access Point has been detected with a known SSID. However, the vendor of the newly discovered Access Point differs from the existing ones.

Solution
Check if the discovered Access Point is a legit network equipment.

Product versions
Guardian Air 1.0.2

Trace
Alerts of this type do not generate traces.

Deduplication key
- Attribute `SOURCE_MAC`
- Attribute `TYPE_ID`
- Attribute `TRIGGER_ID`
- Property `uncommon_vendor`

Chapter 2. Incidents

Incidents are a set of alerts that are related to each other. You can use them to streamline alerts analysis. The user interface (UI) lets you group alerts into incidents. You can toggle the view between Alerts or Incidents.

Built-in checks

Built-in checks are based on specific signatures or hard-coded logics with reference to: known ICS threats (by signatures provided by Threat Intelligence), known malicious operations, system weaknesses, or protocol-compliant operations that can impact the network/ICS functionality. They might also leverage the Learning process to be more accurate.

INCIDENT:BRUTE-FORCE-ATTACK

Brute-force Attack

Type ID
INCIDENT:BRUTE-FORCE-ATTACK

Cause
Several failed login attempts to a node, using a specific protocol, are detected.

Solution
Investigate on the host attempting the login attempts.

INCIDENT:ENG-OPERATIONS

Engineering Operations

Type ID
INCIDENT:ENG-OPERATIONS

Cause
Various operations to modify the configuration, the program, or the status of a device have been detected.

Solution
Validate the engineering operations.

INCIDENT:FORCE-COMMAND

Force Command

Type ID
INCIDENT:FORCE-COMMAND

Cause
A command to manually force a variable value has been detected.

Solution
Investigate on the entity that has initiated the forcing.

INCIDENT:FUNCTION-CODE-SCAN

Function Code Scan

Type ID
INCIDENT:FUNCTION-CODE-SCAN

Cause
A node has performed several actions that are not supported by the target devices.

Solution
Investigate the source and destination devices configuration.

INCIDENT:ILLEGAL-PARAMETER-SCAN

Illegal Parameter Scan

Type ID
INCIDENT:ILLEGAL-PARAMETER-SCAN

Cause
A node has performed a scan of the parameters available on a device.

Solution
Investigate the source authenticity.

INCIDENT:MALICIOUS-FILE

Malicious File

Type ID
INCIDENT:MALICIOUS-FILE

Cause
A compressed archive with some malware inside has been transferred.

Solution
Investigate on the malware source and infected device, and consider to remove the file.

INCIDENT:SUSPICIOUS-ACTIVITY

Suspicious Activity

Type ID
INCIDENT:SUSPICIOUS-ACTIVITY

Cause
Suspicious activity that can be potentially related to known malware has been detected over two nodes.

Solution
Investigate on the malware source and infected device.

INCIDENT:WEAK-PASSWORDS

Weak Passwords

Type ID
INCIDENT:WEAK-PASSWORDS

Cause
Several weak passwords have been detected on this communication.

Solution
Consider to update to secure communication or evaluate the risks of having this data exposed on the network.

Protocol validations

An undesired protocol behavior has been detected. This can refer to a wrong single message, to a correct single message not supposed to be transmitted or transmitted at the wrong time (state machines violation) or to a malicious message sequence. Protocol specific error messages indicating misconfigurations also trigger alerts that fall into this category.

INCIDENT:ANOMALOUS-PACKETS

Anomalous Packets

Type ID
INCIDENT:ANOMALOUS-PACKETS

Cause
Malformed packets have been detected during the deep packet inspection.

Solution
Investigate on the protocol implementation, and the possible presence of malicious actors.

Learned behavior (virtual image)

Virtual image represents a set of information by which Guardian represents the monitored network. This includes for example node properties, links, protocols, function codes, variables, variable values. Such information is collected via learning, smart polling, or external contents, such as Asset Intelligence. When an incident of this category is raised, if the related event is not considered a malicious attack or an anomaly, it can be learned.

INCIDENT:INTERNET-NAVIGATION

Internet Navigation

Type ID
INCIDENT:INTERNET-NAVIGATION

Cause
A node has started surfing the Web.

Solution
Investigate the network and firewall configuration, and the reason why the endpoint shows this behavior, to validate this is a legitimate action.

INCIDENT:VARIABLES-FLOW-ANOMALY

Variables Flow Anomaly

Type ID
INCIDENT:VARIABLES-FLOW-ANOMALY

Cause
An updated time interval on a variable that used to be written or read with a regular interval has been detected.

Solution
Validate the set of events and learn them if legitimate, or treat them as anomalies.

INCIDENT:VARIABLES-FLOW-ANOMALY:CONSUMER

Variables Flow Anomaly on Consumer

Type ID
INCIDENT:VARIABLES-FLOW-ANOMALY:CONSUMER

Cause
A consumer which used to write or read a variable with a regular interval has been detected to have changed its update interval.

Solution
Validate the set of events and learn them if legitimate, or treat them as anomalies.

INCIDENT:VARIABLES-FLOW-ANOMALY:PRODUCER

Variables Flow Anomaly on Producer

Type ID
INCIDENT:VARIABLES-FLOW-ANOMALY:PRODUCER

Cause
A Producer which used to write or read a variable with a regular interval has been detected to have changed its update interval.

Solution
Validate the set of events and learn them if legitimate, or treat them as anomalies.

INCIDENT:VARIABLES-NEW-VALUES

New Values on Producer

Type ID
INCIDENT:VARIABLES-NEW-VALUES

Cause
New variable values have been detected in a device.

Solution
Validate the set of events and learn them if legitimate, or treat them as anomalies.

INCIDENT:VARIABLES-NEW-VARS

New Variables on Producer

Type ID
INCIDENT:VARIABLES-NEW-VARS

Cause
New variables have been detected in the system.

Solution
Validate the set of events and learn them if legitimate, or treat them as anomalies.

INCIDENT:VARIABLES-NEW-VARS:CONSUMER

New variables request from consumer

Type ID
INCIDENT:VARIABLES-NEW-VARS:CONSUMER

Cause
A new variable has been detected in a Consumer device.

Solution
Validate the set of events and learn them if legitimate, or treat them as anomalies.

INCIDENT:VARIABLES-NEW-VARS:PRODUCER

New variables transmission from producer

Type ID
INCIDENT:VARIABLES-NEW-VARS:PRODUCER

Cause
A new variable has been detected in a Producer device.

Solution
Validate the set of events and learn them if legitimate, or treat them as anomalies.

INCIDENT:VARIABLES-SCAN

Variable Scan

Type ID
INCIDENT:VARIABLES-SCAN

Cause
A node in the network has started scanning not existing variables.

Solution
Investigate whether this is a malicious operation or the devices configuration should be updated.

Hybrid threat detection

The Hybrid Category is assigned when alerts belonging to different categories as defined in the Alerts Dictionary are grouped within such one incident. The other categories are as defined in the Alerts Dictionary.

INCIDENT:NEW-COMMUNICATIONS

New Communications

Type ID
INCIDENT:NEW-COMMUNICATIONS

Cause
A node has started to communicate with a new protocol.

Solution
Investigate whether such communication is legitimate.

INCIDENT:NEW-NODE

New Node

Type ID
INCIDENT:NEW-NODE

Cause
A new node has started to send packets in the network.

Solution
Validate the set of events and learn them if legitimate, or treat them as anomalies.

INCIDENT:PORT-SCAN

Network Scan

Type ID
INCIDENT:PORT-SCAN

Cause
A node has executed a series of scans in the network.

Solution
Investigate whether it is an expected behavior or a malicious scan activity is undergoing.