Alerts and Incidents
Reference Guide

2024-09-09

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

Alerts

A description of alerts in the Nozomi Networks software.

Alert types

The Nozomi Networks software generates four categories of alerts. These are:

- Protocol validations
- Learned behavior
- Built-in checks
- Custom checks

Some alerts can specify the triggering condition. For example, with some specific information checks, each protocol can instantiate the **Malformed Packet Alert**.

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.

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.

Type ID	Name	Security Profile	Risk	Details	Product Versions	Trace
NET:RST-FROM-PRODUCER	Link RST request by Producer	LOW	3	The link has been dropped because of a TCP RST sent by the producer. Verify that the device is working properly, no misconfigurations are in place and that network does not suffer excessive latency.	Guardian 18.0.0	YES
PROC:SYNC-ASKED-AGAIN	Producer sync request by Consumer	PARANOID	3	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. Investigate on the protocol implementation and possible presence of malicious actors.	Guardian 18.0.0	YES
PROC:WRONG-TIME	Process time issue	HIGH	3	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. Verify the device configuration and status.	Guardian 18.0.0	YES

Type ID	Name	Security Profile	Risk	Details	Product Versions	Trace
SIGN:ARP-FLOOD	ARP flood	MEDIUM	7	One or more hosts have sent a great amount of ARP packets Verify the device configuration and status, and the possible presence of malicious actors.	Guardian 24.2.0	YES
SIGN:ARP:DUP	Duplicated IP	HIGH	5	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. Investigate on the network configuration and the possible presence of malicious actors.	Guardian 18.0.0	YES
SIGN:DDOS	DDOS attack	HIGH	5	A suspicious Distributed Denial of Service has been detected on the network. Verify that all the devices in the network are allowed and behaving correctly.	Guardian 19.0.0	YES
SIGN:DHCP-OPERATION	DHCP operation	HIGH	4	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. Investigate on the network configuration and the possible presence of malicious actors.	Guardian 18.0.0	YES

Type ID	Name	Security Profile	Risk	Details	Product Versions	Trace
SIGN:ILLEGAL-PARAMETERS	Illegal parameters request	MEDIUM	7	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. Verify the device configuration and status, and the possible presence of malicious actors.	Guardian 19.0.0	YES
SIGN:INVALID-IP	Invalid IP	HIGH	7	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. Investigate on the network configuration and the possible presence of malicious actors.	Guardian 18.0.0	YES
SIGN:MAC-FLOOD	Flood of MAC addresses	MEDIUM	7	A high number of new MAC addresses has appeared in a short time. This can be a flooding technique. Investigate on the network configuration and the possible presence of malicious actors.	Guardian 20.0.1	YES
SIGN:MALFORMED-TRAFFIC	Malformed traffic	MEDIUM	7	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. Investigate on the protocol implementation and the possible presence of malicious actors.	Guardian 18.0.0	YES

Type ID	Name	Security Profile	Risk	Details	Product Versions	Trace
SIGN:MALICIOUS-PROTOCOL	Malicious protocol	LOW	6	An attempted communication by a protocol known to be related to threats has been detected. Verify the device configuration and status, and the possible presence of malicious actors.	Guardian 19.0.0	YES
SIGN:MULTIPLE-ACCESS-DENIED	Multiple Access Denied events	MEDIUM	8	A host has repeatedly been denied access to a resource. Verify whether the calling device is supposed to access those resources and tune the authorization permissions accordingly.	Guardian 19.0.5	YES
SIGN:MULTIPLE-OT_DEVICE-RESERVATIONS	Multiple OT device reservations	HIGH	8	A host has repeatedly tried to reserve the usage of an OT device causing a potential denial-of-service. Verify the device configuration and status, and the possible presence of malicious actors.	Guardian 19.0.0	YES
SIGN:MULTIPLE-UNSUCCESSFUL-LOGINS	Multiple unsuccessful logins	MEDIUM	8	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. Verify whether the calling device is supposed to access the target device and tune the authentication credentials accordingly.	Guardian 18.0.0	YES
SIGN:NET-MALFORMED	Malformed Network/ Transport layer	MEDIUM	7	A packet containing a semantically invalid sequence below the application layer has been observed. Investigate on the protocol implementation, and the possible presence of malicious actors.	Guardian 20.0.0	YES

Type ID	Name	Security Profile	Risk	Details	Product Versions	Trace
SIGN:NETWORK-SCAN	Network Scan	MEDIUM	7	An attempt to reach many target hosts or ports in a target network (vertical or horizontal scan) has been detected. Investigate whether it is an expected behavior or a malicious scan activity is undergoing.	Guardian 19.0.0	YES
SIGN:PROC:MISSING-VAR	Missing variable request	HIGH	6	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. Verify the device configuration and status, and the possible presence of malicious actors.	Guardian 18.0.0	YES
SIGN:PROC:UNKNOWN-RTU	Missing or unknown device	MEDIUM	6	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. Verify the device configuration and status, and the possible presence of malicious actors.	Guardian 18.0.0	YES
SIGN:PROTOCOL-ERROR	Protocol error	HIGH	7	A generic protocol error occurred, this usually relates to a wrong field, option or other general violation of the protocol. Investigate on the protocol implementation, and the possible presence of malicious actors.	Guardian 18.0.0	YES

Type ID	Name	Security Profile	Risk	Details	Product Versions	Trace
SIGN:PROTOCOL-FLOOD	Protocol-based flood	MEDIUM	7	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. Verify the device configuration and status, and the possible presence of malicious actors.	Guardian 19.0.4	YES
SIGN:PROTOCOL-INJECTION	Protocol packet injection	LOW	9	A correct protocol packet injected in the wrong context has been detected: this may cause equipment to operate improperly. Example: a correct GOOSE message sent with a wrong sequence number (that, if received in the right moment, would just work instead). Investigate on the protocol implementation, and the possible presence of malicious actors.	Guardian 18.0.0	YES
SIGN:TCP-FLOOD	TCP flood	MEDIUM	7	One or more hosts have sent a great amount of anomalous TCP packets or TCP FIN packets to a single, target host. Verify the device configuration and status, and the possible presence of malicious actors.	Guardian 19.0.4	YES
SIGN:UDP-FLOOD	UDP flood	MEDIUM	7	One or more hosts have sent a great amount of UDP packets to a single target host. Verify the device configuration and status, and the possible presence of malicious actors.	Guardian 20.0.7.1	YES

Type ID	Name	Security Profile	Risk	Details	Product Versions	Trace
SIGN:UNSUPPORTED-FUNC	Unsupported function request	MEDIUM	7	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. Verify the device configuration and status, and the possible presence of malicious actors.	Guardian 19.0.0	YES

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.

Type ID	Name	Security Profile	Risk	Details	Product Versions	Trace
SIGN:WIRELESS:CELLULAR-ROGUE	Rogue Cell Tower Detected	LOW	7	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. 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.	Guardian Air 1.0.1	YES

Type ID	Name	Security Profile	Risk	Details	Product Versions	Trace
VI:CONF-MISMATCH	Configuration Mismatch	MEDIUM	7	A parameter describing a configuration version that was previously imported from a project has been observed having a different value in the traffic. Validate the event and learn it if legitimate, or treat it as anomaly.	Guardian 20.0.0	YES
VI:GLOBAL:NEW-FUNC-CODE	New global function code	MEDIUM	5	A previously unknown protocol Function Code for has appeared in the network. Validate the event and learn it if legitimate, or treat it as anomaly.	Guardian 19.0.0	YES
VI:GLOBAL:NEW-MAC-VENDOR	New global MAC vendor	MEDIUM	5	A previously unknown MAC vendor has appeared in the network. Validate the event and learn it if legitimate, or treat it as anomaly.	Guardian 19.0.4	YES
VI:GLOBAL:NEW-VAR-PRODUCER	New global variable producer	HIGH	5	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. Validate the event and learn it if legitimate, or treat it as anomaly.	Guardian 21.3.0	YES
VI:KB:UNKNOWN-FUNC-CODE	Unknown asset function code	HIGH	5	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. Validate the event and learn it if legitimate, or treat it as anomaly.	Asset Intelligence	YES

Type ID	Name	Security Profile	Risk	Details	Product Versions	Trace
VI:KB:UNKNOWN-PROTOCOL	Unknown asset's protocol	HIGH	5	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. Validate the event and learn it if legitimate, or treat it as anomaly.	Asset Intelligence	YES
VI:NEW-ARP	New ARP	HIGH	4	A new MAC Address has started requesting ARP information. Validate the event and learn it if legitimate, or treat it as anomaly.	Guardian 18.0.0	YES
VI:NEW-FUNC-CODE	New function code	HIGH	6	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'. Validate the event and learn it if legitimate, or treat it as anomaly.	Guardian 18.0.0	YES
VI:NEW-LINK	New link	HIGH	4	Two nodes have started communicating with each other with a new protocol. Validate the event and learn it if legitimate, or treat it as anomaly.	Guardian 18.0.0	YES

Type ID	Name	Security Profile	Risk	Details	Product Versions	Trace
VI:NEW-LINK-CONFIRMED	New confirmed link	HIGH	5	Two nodes have started communicating with each other with a new, confirmed protocol. Validate the event and learn it if legitimate, or treat it as anomaly.	Guardian 18.0.0	YES
VI:NEW-LINK-GROUP	New link group	HIGH	5	Two nodes have started communicating with each other. Validate the event and learn it if legitimate, or treat it as anomaly.	Guardian 18.0.0	YES
VI:NEW-MAC	New MAC address	HIGH	6	A new MAC Address has appeared in the network. Validate the event and learn it if legitimate, or treat it as anomaly.	Guardian 18.0.0	YES
VI:NEW-NET-DEV	New network device	MEDIUM	3	A new network device (switch or router) has appeared on the network. Validate the event and learn it if legitimate, or treat it as anomaly.	Guardian 18.0.0	YES
VI:NEW-NODE	New node	MEDIUM	5	A new node has appeared on the network. Validate the event and learn it if legitimate, or treat it as anomaly.	Guardian 18.0.0	YES

Type ID	Name	Security Profile	Risk	Details	Product Versions	Trace
VI:NEW-NODE:DUALUSE-IP	DUALUSE IP (new node)	MEDIUM	4	A node with a suspicious IP has been detected. It is suggested to validate the health status of communicating nodes, as they may be infected by some malware. Validate the event and learn it if legitimate, or treat it as anomaly.	Guardian 24.0.0	YES
VI:NEW-NODE:MALICIOUS-IP	Bad IP reputation (new node)	LOW	5	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. Validate the event and learn it if legitimate, or treat it as anomaly.	Guardian 20.0.0	YES
VI:NEW-NODE:PUA-IP	PUA IP (new node)	MEDIUM	4	A potentially unwanted application has contacted one of its IP address. This is normally less dangerous than a malware but may have some undesired privacy effects. Verify that the applications installed on the involved asset are correct.	Guardian 24.0.0	YES
VI:NEW-NODE:TARGET	New target node	HIGH	4	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. Validate the event and learn it if legitimate, or treat it as anomaly.	Guardian 18.0.0	YES

Type ID	Name	Security Profile	Risk	Details	Product Versions	Trace
VI:PROC:NEW-VALUE	New OT variable value	HIGH	6	A variable has been set to a value never seen before. Validate the event and learn it if legitimate, or treat it as anomaly.	Guardian 18.0.0	YES
VI:PROC:NEW-VAR	New OT variable	HIGH	6	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. Validate the event and learn it if legitimate, or treat it as anomaly.	Guardian 18.0.0	YES
VI:PROC:PROTOCOL-FLOW-ANOMALY	Protocol flow anomaly	HIGH	8	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. Validate the event and learn it if legitimate, or treat it as anomaly.	Guardian 18.0.0	YES
VI:PROC:VARIABLE-FLOW-ANOMALY	Variable flow anomaly	HIGH	6	A variable which is sent cyclically has changed its transmission interval time. Validate the event and learn it if legitimate, or treat it as anomaly.	Guardian 18.0.0	YES

Type ID	Name	Security Profile	Risk	Details	Product Versions	Trace
VI:WIRELESS:ROGUE-AP	Rogue Access Point	LOW	8	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. Check if the discovered Access Point is a legit network equipment.	Guardian Air 1.0.2	NO

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.

Type ID	Name	Security Profile	Risk	Details	Product Versions	Trace
SIGN:CLEARTEXT-PASSWORD	Cleartext password	MEDIUM	7	A cleartext password has been issued or requested. Consider to update to secure communication or evaluate the risks of having this data exposed on the network.	Guardian 19.0.0	YES
SIGN:CONFIGURATION-CHANGE	Configuration change	MEDIUM	6	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. Verify the device configuration and status.	Guardian 18.0.0	YES
SIGN:CPE:CHANGE	CPE change	LOW	0	An installed software change has been detected. The change relates to the vulnerabilities list, possibly changing it. Verify the device configuration and status, and the reason behind the software change.	Guardian 18.0.0	YES
SIGN:DEV-STATE-CHANGE	Device state change	MEDIUM	7	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. Verify the device configuration and status, and the reason behind the command.	Guardian 18.0.0	YES

Type ID	Name	Security Profile	Risk	Details	Product Versions	Trace
SIGN:DUALUSE-DETECTED	DUALUSE detection	MEDIUM	5	Suspicious transfer of Dual Use Application (DUALUSE) named. Verify the usage of the application and, if malicious, cleanup the victim, and block or cleanup also the attacker.	Guardian 23.3.0	NO
SIGN:DUALUSE-DOMAIN	DUALUSE domain	MEDIUM	4	A DNS query towards a suspicious domain has been detected. Investigate on the health status of the involved nodes.	Guardian 24.0.0	NO
SIGN:DUALUSE-IP	DUALUSE IP	MEDIUM	4	A node with a suspicious IP has been detected. Validate the health status of the communicating nodes, as they may be infected by some malware.	Guardian 24.0.0	YES
SIGN:DUALUSE-URL	DUALUSE URL	MEDIUM	5	A request towards a suspicious URL has been detected. Investigate on the health status of the involved nodes.	Guardian 24.0.0	YES
SIGN:FIRMWARE-TRANSFER	Firmware transfer	HIGH	6	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. Verify the device configuration and status, and the possible presence of malicious actors.	Guardian 19.0.0	YES

Type ID	Name	Security Profile	Risk	Details	Product Versions	Trace
SIGN:INFORMATION-GATHERING	Information gathering	PARANOID	6	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. Investigate on the actor that has initiated the transfer and on the transferred information.	Guardian 24.1.0	YES
SIGN:MALICIOUS-DOMAIN	Malicious domain	LOW	8	A DNS query towards a malicious domain has been detected. Investigate on why this domain has been contacted and consider to ban it from your network.	Guardian 19.0.0	YES
SIGN:MALICIOUS-HID	Malicious USB device	LOW	10	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. 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.	Arc 1.0	NO
SIGN:MALICIOUS-IP	Bad ip reputation	LOW	8	A node with a bad reputation IP has been found. Investigate on why this IP has been contacted and consider to ban it from your network.	Guardian 19.0.0	YES

Type ID	Name	Security Profile	Risk	Details	Product Versions	Trace
SIGN:MALICIOUS-URL	Malicious URL	LOW	7	A request towards a malicious URL has been detected. Investigate on why this URL has been contacted and consider to ban it from your network.	Guardian 19.0.0	YES
SIGN:MALWARE-DETECTED	Malware detection	LOW	9	A potentially malicious payload has been transferred. Investigate on the malware source and infected device, and consider to remove the file.	Guardian 18.0.0	NO
SIGN:MITM	MITM attack	LOW	10	A potential MITM attack has been detected. The attacker is ARP-poisoning the victims. The attacker node could alter the communication between its victims. Investigate on the network configuration and the possible presence of malicious actors.	Guardian 20.0.5	NO
SIGN:OT_DEVICE-REBOOT	OT device reboot request	HIGH	6	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. Investigate on the network configuration and the possible presence of malicious actors.	Guardian 18.0.0	YES

Type ID	Name	Security Profile	Risk	Details	Product Versions	Trace
SIGN:OT_DEVICE-START	OT device start request	HIGH	6	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. Investigate on the network configuration and the possible presence of malicious actors.	Guardian 18.0.0	YES
SIGN:OT_DEVICE-STOP	OT device stop request	HIGH	9	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. Investigate on the network configuration and the possible presence of malicious actors.	Guardian 18.0.0	YES
SIGN:OUTBOUND-CONNECTIONS	High rate of outbound connections	LOW	9	A host has shown a sudden increase of outbound connections. This could be due to the presence of a malware. Investigate on the reason behind such connections to the outside on the device, and consider to update the network configuration to prevent them.	Guardian 21.0.0	YES
SIGN:PACKET-RULE	Packet rule match	LOW	9	A packet has matched a Packet rule. Verify the device configuration and status, and the possible presence of malicious actors.	Threat Intelligence	YES

Type ID	Name	Security Profile	Risk	Details	Product Versions	Trace
SIGN:PASSWORD:WEAK	Weak password	HIGH	5	A weak password, possibly default, has been used to access a resource. Consider to update your passwords.	Guardian 18.5.0	YES
SIGN:PROGRAM:CHANGE	Program change	MEDIUM	6	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. Verify the device configuration and status, and the possible presence of malicious actors.	Guardian 18.0.0	YES
SIGN:PROGRAM:TRANSFER	Program transfer	HIGH	6	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. Investigate on the entity that has initiated the transfer and on the program content.	Guardian 18.0.0	YES
SIGN:PUA-DETECTED	PUA detection	MEDIUM	5	A potentially unwanted application payload (PUA) has been transferred. This is normally less dangerous than a malware payload. Investigate on the malware source and infected device, and consider to remove the payload.	Guardian 20.0.6	NO

Type ID	Name	Security Profile	Risk	Details	Product Versions	Trace
SIGN:PUA-DOMAIN	PUA domain	MEDIUM	4	A DNS query towards a suspicious domain has been detected. Investigate on the health status of the involved nodes.	Guardian 24.0.0	NO
SIGN:PUA-IP	PUA IP	MEDIUM	4	A node with a suspicious IP has been detected. Validate the health status of the communicating nodes, as they may be infected by some malware.	Guardian 24.0.0	YES
SIGN:PUA-URL	PUA URL	MEDIUM	5	A request towards a suspicious URL has been detected. Investigate on the health status of the involved nodes.	Guardian 24.0.0	YES
SIGN:SIGMA-RULE	Sigma rule match	LOW	9	Rule-dependent. A suspicious local event has been detected on a machine. Rule-dependent. Verify the device configuration and status, and the possible presence of malicious processes.	Arc 1.0, Threat Intelligence	YES
SIGN:SUSP-TIME	Suspicious time value	HIGH	7	A suspicious time has been observed in the network. There could be a malfunctioning device or a packet injection. Verify the device configuration and status.	Guardian 20.0.0	YES
SIGN:USB-DEVICE	New USB device plugged	PARANOID	6	This is most likely a human driven event. USB devices might be a physical infiltration vector carrying files with malicious behaviour. Check the device nature and its content.	Arc 1.0	NO

Type ID	Name	Security Profile	Risk	Details	Product Versions	Trace
SIGN:WEAK-ENCRYPTION	Weak encryption	PARANOID	6	The communication has been encrypted using an obsolete cryptographic protocol, weak cipher suites or invalid certificates. Consider to update to more secure algorithms or evaluate the risks of having this technology still used on the netowrk.	Guardian 19.0.5	YES
SIGN:WIFI:DEAUTH	Deauth Attack	LOW	7	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. 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.	Guardian Air 1.0.1	YES
SIGN:WIFI:SSID-XSS-INJECTION	SSID XSS injection attempt	LOW	5	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. 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.	Guardian Air 1.0.1	YES

Type ID	Name	Security Profile	Risk	Details	Product Versions	Trace
SIGN:WIRELESS:INJECTION	Sospected wireless packet injection	LOW	5	A wireless packet that looks to have been injected by an attacker has been captured. Check the surroundings of the involved assets and its wireless network.	Guardian Air 1.0.1	YES
SIGN:WIRELESS:SUSPICIOUS	Suspicious wireless activity	LOW	5	A wireless suspicious packet has been captured. Something does not look as it should according to the protocol or specifications. Check the involved assets and wireless network.	Guardian Air 1.0.1	YES
SIGN:WIRELESS:VIOLATION-RULES	Wireless packet violating rules	LOW	5	A wireless packet that is not complying to protocol rules has been captured on the network. Check that the involved assets have not been compromised.	Guardian Air 1.0.1	YES

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.

Type ID	Name	Security Profile	Risk	Details	Product Versions	Trace
ASRT:FAILED	Assertion failed	LOW	0	An assertion has failed. Assertion dependent. Check out the elements making the assertion to fail.	Guardian 18.0.0	YES
GENERIC:EVENT	Generic Event	LOW	0	A generic event has been generated by the SDK. Event dependent. More details are available in the description of the event.	Guardian 20.0.5	YES
NET:INACTIVE-PROTOCOL	Inactive protocol	LOW	3	The link has been inactive for longer than the set threshold. Investigate whether that is the expected behavior or something prevents the link from working.	Guardian 18.0.0	YES
NET:LINK-RECONNECTION	Link reconnection	LOW	3	The link configured to be persistent has experienced a complete TCP reconnection. Investigate whether the reconnection is legitimate.	Guardian 18.0.0	YES
NET:TCP-SYN	TCP SYN	LOW	3	A connection attempt (TCP SYN) has been detected on a link. Investigate on the entity that has attempted to connect.	Guardian 18.0.0	YES

Type ID	Name	Security Profile	Risk	Details	Product Versions	Trace
PROC:CRITICAL-STATE-OFF	Critical state off	LOW	1	The system has recovered from a user-defined critical process state. Investigate such critical state.	Guardian 18.0.0	YES
PROC:CRITICAL-STATE-ON	Critical state on	LOW	9	The system has entered in a user-defined critical process state. Investigate on the values and whether the process is at risk.	Guardian 18.0.0	YES
PROC:INVALID-VARIABLE-QUALITY	Invalid variable quality	LOW	3	A variable has showed a quality bit set for longer than the set threshold. Investigate on the protocol implementation and the process status.	Guardian 18.0.0	YES
PROC:NOT-ALLOWED-INVALID-VARIABLE	Not allowed variable quality	LOW	3	A variable has shown one or more specific quality bits the user set as not allowed. Investigate on the protocol implementation and the process status.	Guardian 18.0.0	YES
PROC:STALE-VARIABLE	Stale variable	LOW	3	A variable has not been read/written for longer than the set threshold. Investigate on the protocol implementation and the link and process status.	Guardian 18.0.0	YES

Chapter 2. Incidents

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.

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.

Type ID	Name	Details
INCIDENT:ANOMALOUS-PACKETS	Anomalous Packets	Malformed packets have been detected during the deep packet inspection. Investigate on the protocol implementation, and the possible presence of malicious actors.

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.

Type ID	Name	Details
INCIDENT:INTERNET-NAVIGATION	Internet Navigation	A node has started surfing the Web. 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	An updated time interval on a variable that used to be written or read with a regular interval has been detected. 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	A consumer which used to write or read a variable with a regular interval has been detected to have changed its update interval. Validate the set of events and learn them if legitimate, or treat them as anomalies.

Type ID	Name	Details
INCIDENT:VARIABLES-FLOW-ANOMALY:PRODUCER	Variables Flow Anomaly on Producer	A Producer which used to write or read a variable with a regular interval has been detected to have changed its update interval. Validate the set of events and learn them if legitimate, or treat them as anomalies.
INCIDENT:VARIABLES-NEW-VALUES	New Values on Producer	New variable values have been detected in a device. Validate the set of events and learn them if legitimate, or treat them as anomalies.
INCIDENT:VARIABLES-NEW-VARS	New Variables on Producer	New variables have been detected in the system. 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	A new variable has been detected in a Consumer device. 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	A new variable has been detected in a Producer device. Validate the set of events and learn them if legitimate, or treat them as anomalies.
INCIDENT:VARIABLES-SCAN	Variable Scan	A node in the network has started scanning not existing variables. Investigate whether this is a malicious operation or the devices configuration should be updated.

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.

Type ID	Name	Details
INCIDENT:BRUTE-FORCE-ATTACK	Brute-force Attack	Several failed login attempts to a node, using a specific protocol, are detected. Investigate on the host attempting the login attempts.
INCIDENT:ENG-OPERATIONS	Engineering Operations	Various operations to modify the configuration, the program, or the status of a device have been detected. Validate the engineering operations.
INCIDENT:FORCE-COMMAND	Force Command	A command to manually force a variable value has been detected. Investigate on the entity that has initiated the forcing.
INCIDENT:FUNCTION-CODE-SCAN	Function Code Scan	A node has performed several actions that are not supported by the target devices. Investigate the source and destination devices configuration.
INCIDENT:ILLEGAL-PARAMETER-SCAN	Illegal Parameter Scan	A node has performed a scan of the parameters available on a device. Investigate the source authenticity.

Type ID	Name	Details
INCIDENT:MALICIOUS-FILE	Malicious File	A compressed archive with some malware inside has been transferred. Investigate on the malware source and infected device, and consider to remove the file.
INCIDENT:SUSPICIOUS-ACTIVITY	Suspicious Activity	Suspicious activity that can be potentially related to known malware has been detected over two nodes. Investigate on the malware source and infected device.
INCIDENT:WEAK-PASSWORDS	Weak Passwords	Several weak passwords have been detected on this communication. Consider to update to secure communication or evaluate the risks of having this data exposed on the network.