

---

# CLAROTY PLATFORM: WINDFARMS CYBERSECURITY



## Foreword

An attacker that seeks to disrupt the sound operation of windfarms would attempt to manipulate the OT protocol that is used to control and monitor the operational values on the wind turbine's controller.

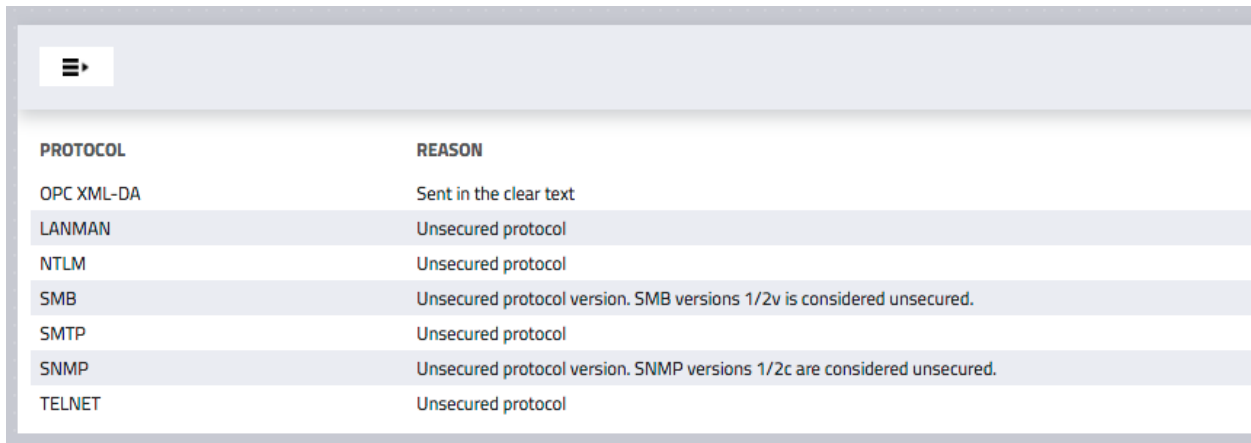
This traffic – typically implemented in DNP3, Modbus, OPC-DA, etc. – usually takes place in the portion of the OT network that is outsourced to external contractors that manage it remotely through satellite or 3G links. As a result, the windfarm's owner has limited to no visibility into what may become a systemic risk to its operational network.

In this paper, we show how the Claroty platform, would thwart an attacker's attempts to launch a cyberattack on a windfarm OT network using the OPC-XML-DA protocol.

### Proactive Steps

Wind turbine features extensively use the OPC-XML-DA protocol for controller\HMI data acquisition communications. The lack of inherent security measures makes this protocol a significant attack surface for threat actors to target.

The first priority when assessing a windfarm network’s cybersecurity resilience, is to check whether OPC-XML-DA is in use. Claroty Continuous Threat Detection gathers all the network traffic, and can easily provide the required data:



PROTOCOL	REASON
OPC XML-DA	Sent in the clear text
LANMAN	Unsecured protocol
NTLM	Unsecured protocol
SMB	Unsecured protocol version. SMB versions 1/2v is considered unsecured.
SMTP	Unsecured protocol
SNMP	Unsecured protocol version. SNMP versions 1/2c are considered unsecured.
TELNET	Unsecured protocol

Figure 1: OPC-XML-DA traffic

### Detection of Attackers in the Network

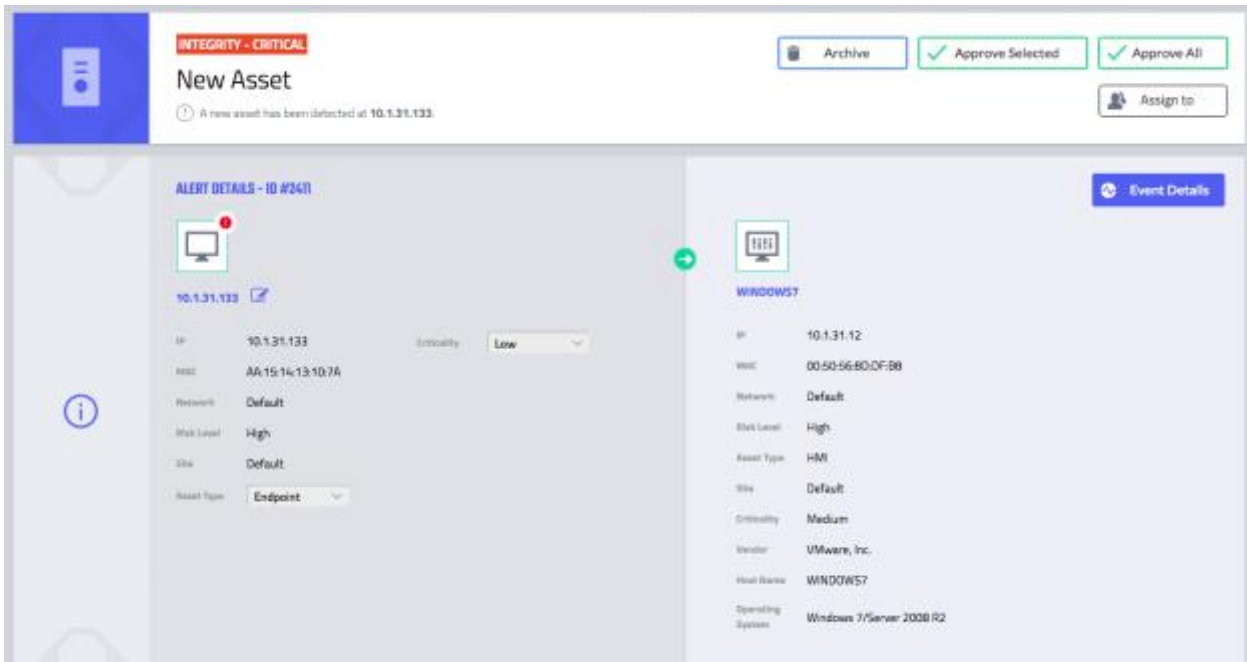
Targeted attacks on OT networks typically comprise several steps – initial asset compromise, discovery of critical assets and causing disruptions to a running process. The following section illustrates Claroty Continuous Threat Detection’s capabilities in detecting attackers in the network across these three stages.

## Initial Compromise: Malicious Asset in the Wind Turbine Network

**Description:** a common initial step in cyberattacks is either compromising an existing machine in the network, or introducing a new machine, controlled by the attacker.

**Wind Turbine Implementation:** the attacker must connect its asset to the wind turbine network's switch in order to use it as a stepping stone for further compromise.

**Clarity Platform:** Continuous Threat Detection generates an immediate alert upon the discovery of any new asset in the network.



The screenshot displays the 'New Asset' alert interface in the Clarity Platform. At the top, a red banner indicates 'INTEGRITY - CRITICAL'. Below this, the title 'New Asset' is shown, followed by a notification: 'A new asset has been detected at 10.1.31.133'. Action buttons include 'Archive', 'Approve Selected', 'Approve All', and 'Assign to'. The main content area is split into two panels. The left panel, titled 'ALERT DETAILS - ID #2471', shows details for the detected asset: IP 10.1.31.133, MAC AA:15:14:13:10:7A, Network Default, Risk Level High, Site Default, and Asset Type Endpoint. The right panel, titled 'WINDOWS7', shows details for a related asset: IP 10.1.31.12, MAC 00:50:56:8D:0F:88, Network Default, Risk Level High, Asset Type HMI, Site Default, Criticality Medium, Vendor VMware, Inc., Host Name WINDOWS7, and Operating System Windows 7/Server 2008 R2. An 'Event Details' button is located in the top right of the right panel.

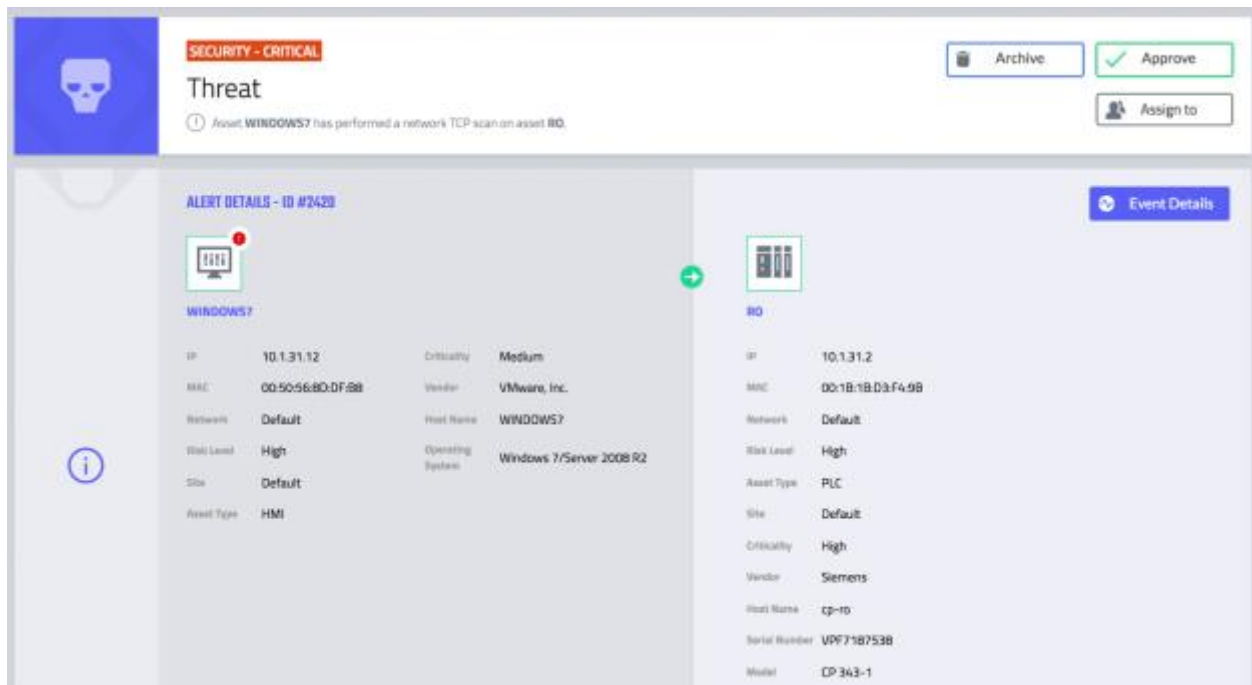
Figure 2: New Asset alert -Main Screen

## Network Discovery: Scanning for OPC Servers Inside Wind Turbines Network

**Description:** following initial foothold, the typical next step is to scan the network to discover valuable assets.

**Wind Turbine Implementation:** in this case the valuable assets would be OPC servers the attacker would use to change values in the turbine's controllers.

**Clarity Platform:** Continuous Threat Detection generates an immediate alert upon any network scanning.



**Threat**  
SECURITY - CRITICAL  
Asset: WINDOWS7 has performed a network TCP scan on asset BO

Alert Details - ID #2420

Property	Value	Property	Value
IP	10.1.31.12	Criticality	Medium
MAC	00:50:56:80:DF:98	Vendor	VMware, Inc.
Network	Default	Host Name	WINDOWS7
Risk Level	High	Operating System	Windows 7/Server 2008 R2
Site	Default		
Asset Type	HMI		

Property	Value
IP	10.1.31.2
MAC	00:1B:1B:D3:F4:9B
Network	Default
Risk Level	High
Asset Type	PLC
Site	Default
Criticality	High
Vendor	Siemens
Host Name	cp-rp
Serial Number	VDF718753B
Model	CP 343-1

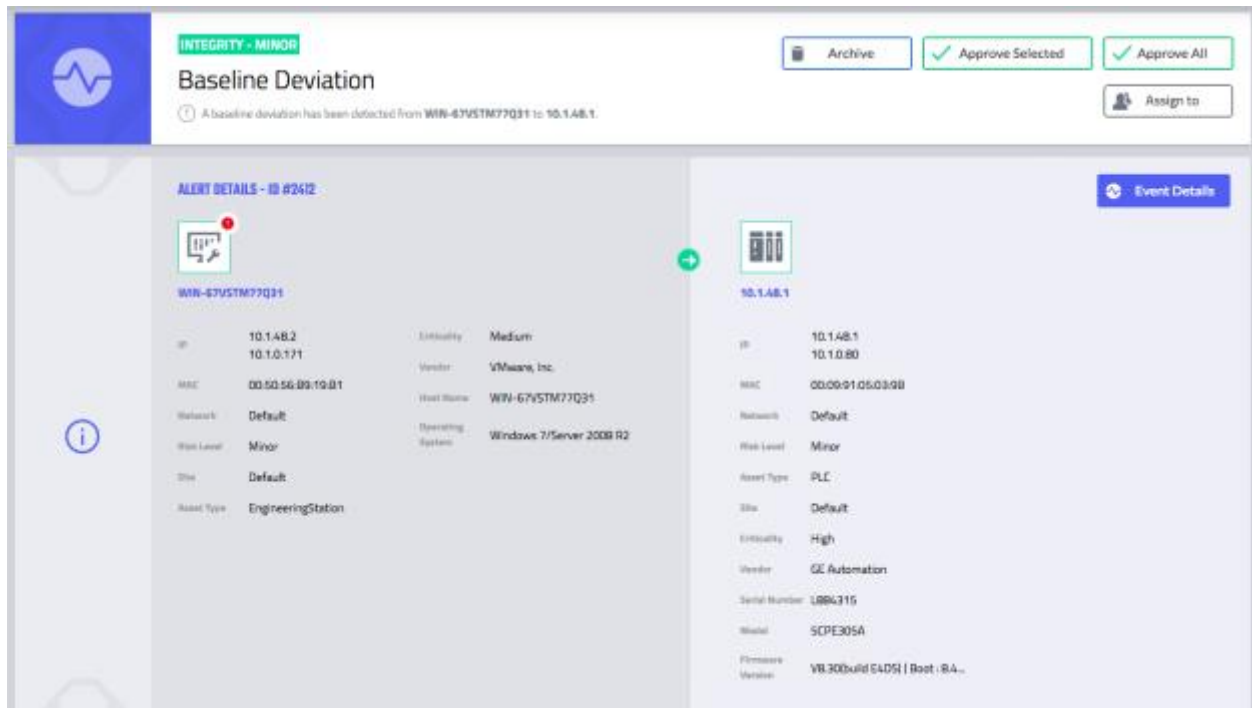
Figure 3: Network TCP Scan alert – main screen

### Malicious Action (Option 1): OPC messages on the Network

**Description:** once an attacker established a firm presence in the network, the attacker can proceed in issuing malicious commands to achieve their targets.

**Wind Turbine Implementation:** typically, attackers would maliciously use OPC messages to change values in the turbine's controller. Such changes would generate anomalous traffic in comparison with the network standard behavior.

**Clarity Platform:** Continuous Threat Detection generates an immediate alert upon any deviation from an asset's baseline behavior.



**INTEGRITY - MINOR**  
**Baseline Deviation**  
A baseline deviation has been detected from WIN-67V5TM77Q31 to 10.148.1

Archive Approve Selected Approve All Assign to

**ALERT DETAILS - ID #2612** Event Details

WIN-67V5TM77Q31		10.148.1	
IP	10.148.2 10.1.0.171	IP	10.148.1 10.1.0.80
MAC	00:50:56:09:19:01	MAC	00:09:01:05:03:98
Network	Default	Network	Default
Risk Level	Minor	Risk Level	Minor
Site	Default	Asset Type	PLC
Asset Type	EngineeringStation	Site	Default
Entity	Medium	Entity	High
Vendor	VMware, Inc.	Vendor	GE Automation
Host Name	WIN-67V5TM77Q31	Serial Number	1886716
Operating System	Windows 7/Server 2008 R2	Model	SCPE305A
		Firmware Version	VR300build64DS1   Boot : 84...

Figure 4: Baseline Deviation alert - main screen

**BASILINE DETAILS FOR ALERT**

Protocol: Select Protocol... Communication Type: Select Communication Type... Access Type: Select Access Type... Frequency: Select Frequency... Baseline name: Baseline name

Clear all filters

**RESULTS (8/8)**

Baseline Name	Transmission	Frequen...	Source	Destination	Last Seen	Communication Type	Access T...
<input type="checkbox"/> OPC-DA : Write tag Wind_speed	OPC-DA	Not timed	10.148.2	10.148.1	08-11, 10:10	Other	Execute
<input type="checkbox"/> OPC-DA : Read tag Wind_speed	OPC-DA	Not timed	10.148.2	10.148.1	08-11, 10:10	Other	Execute
<input type="checkbox"/> OPC-DA : Write tag Break_status	OPC-DA	Not timed	10.148.2	10.148.1	08-11, 10:10	Other	Execute
<input type="checkbox"/> OPC-DA : Read tag Break_status	OPC-DA	Not timed	10.148.2	10.148.1	08-11, 10:10	Other	Execute
<input type="checkbox"/> OPC-DA : Write tag Power	OPC-DA	Not timed	10.148.2	10.148.1	08-11, 10:10	Other	Execute
<input type="checkbox"/> OPC-DA : Read tag Power	OPC-DA	Not timed	10.148.2	10.148.1	08-11, 10:10	Other	Execute

Page 1 of 1

Figure 5: Baseline Deviation alert - anomalous OPC traffic (1)

### Malicious Action (Option 2): Man-in-the-Middle (MITM)

**Description:** MITM attack involves an attacker machine that intercepts communication between two nodes in the network, providing them with false data. MITM features additional masking to the attacker's actions making them difficult to discover

**Wind Turbine Implementation:** placing the attacker's machine between the HMI and the turbine's controller sending both destructive 'Write' commands to the controller, and false 'Read' responses to the HMI in order to prevent discovery.

**Clarity Platform:** Continuous Threat Detection generates an immediate alert upon initiation of MITM communication.

**SECURITY - CRITICAL**

## Threat

A Man-In-The-Middle attack detected between **Chemical\_plant** and **10.1.30.4**

Archive Approve Assign to

**ALERT DETAILS - ID #2410**

10.1.0.31 [win\_virtual] → Chemical... 10.1.30.4

IP	10.1.0.31	Criticality	Low
MAC	00:50:56:B9:C4:7B		
Network	Default		
Risk Level	High		
Site	Default		
Asset Type	Endpoint		

Figure 6: MITM alert (this MITM uses ARP poisoning) – main screen

**Event Details**

RESULTS (20/43) Search

ID	DESCRIPTION	TYPE	TIMESTAMP
97288	New asset have been detected for 005056b9c47b	NewAsset	Today, 09:52
97289	ARP : Response for ipv4 address 10.1.0.41 with mac address 00:50:56:b9:c4:7b	BaselineDeviation	Today, 09:52
97290	ARP : Response for ipv4 address 10.1.0.40 with mac address 00:50:56:b9:c4:7b	BaselineDeviation	Today, 09:52
97291	New asset have been detected for 10.1.0.31	NewAsset	Today, 09:52
97292	MAC Conflict have been detected between 10.1.0.31 and 005056b9c47b	AssetConflict	Today, 09:52
97293	ARP : Request for ipv4 address 10.1.0.40	BaselineDeviation	Today, 09:52
97294	ARP : Response for ipv4 address 10.1.0.41 with mac address 00:00:bcc7:8f:06	BaselineDeviation	Today, 09:52
97295	ARP : Request for ipv4 address 10.1.0.41	BaselineDeviation	Today, 09:52
97296	ARP : Response for ipv4 address 10.1.0.40 with mac address 00:1d9cc0:04:9d	BaselineDeviation	Today, 09:52
97297	ARP : Response for ipv4 address 10.1.0.40 with mac address 00:1d9cc0:04:9d	BaselineDeviation	Today, 09:52
97298	OPC-DA : Write tag Wind_speed	BaselineDeviation	Today, 09:52
97299	OPC-DA : Write tag Break_tatus	BaselineDeviation	Today, 09:52

Page 1 of 3

Figure 7: MITM alert (this MITM uses ARP poisoning) – events timeline