CLAROTY
Clarity for OT Networks

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.

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

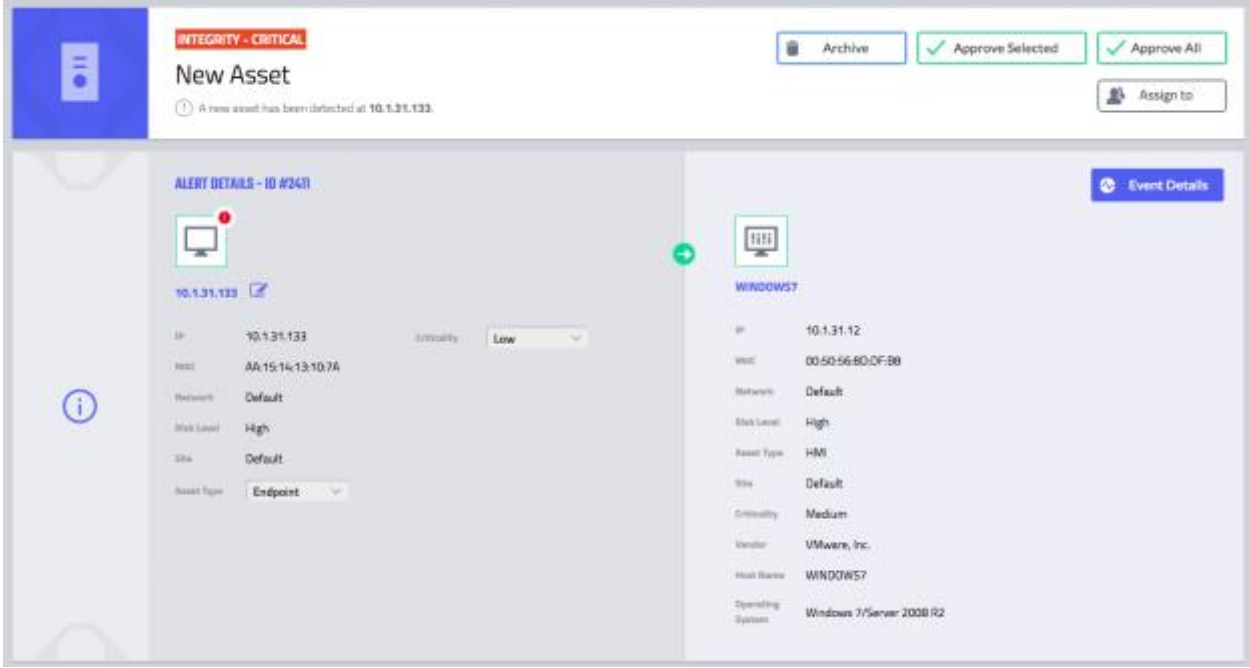

Figure 2: New Asset alert -Main Screen

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.

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

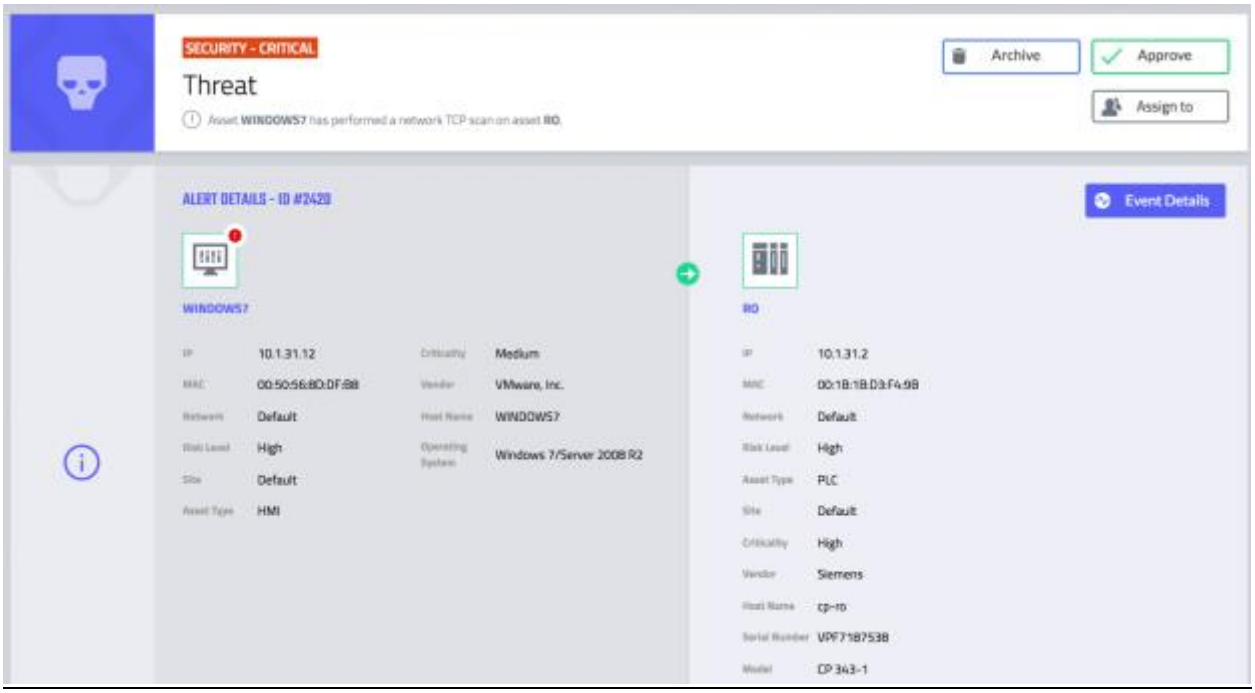

Figure 3: Network TCP Scan alert – main screen

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.

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

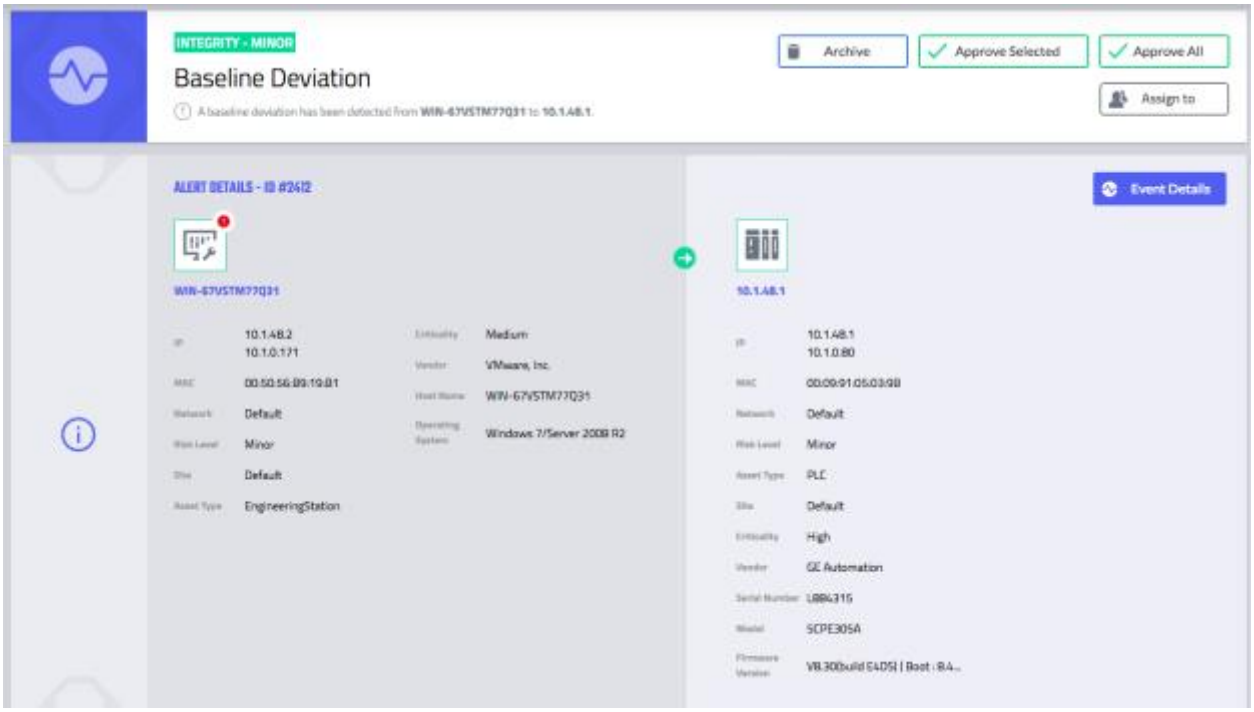

Figure 4: Baseline Deviation alert - main screen

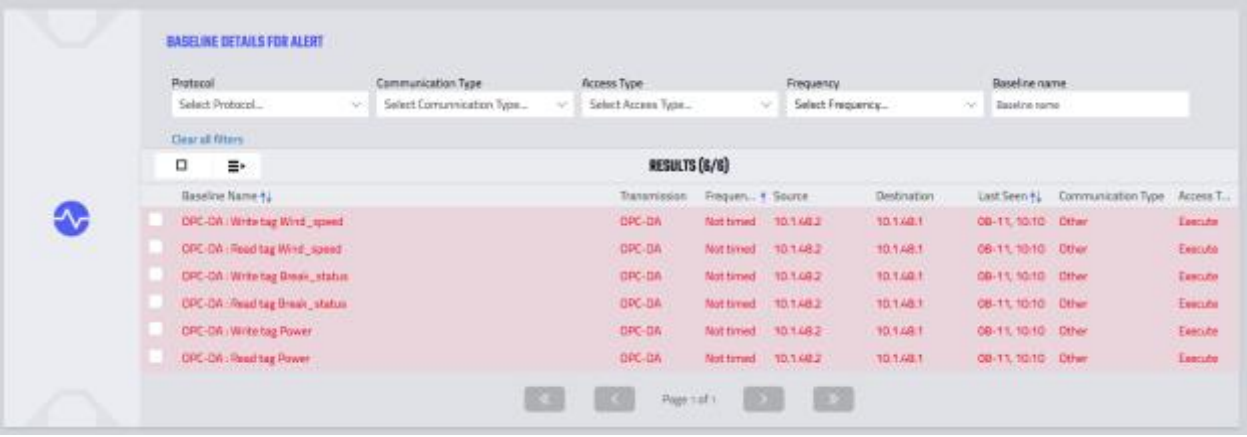

Figure 5: Baseline Deviation alert - anomalous OPC traffic (1)

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.

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

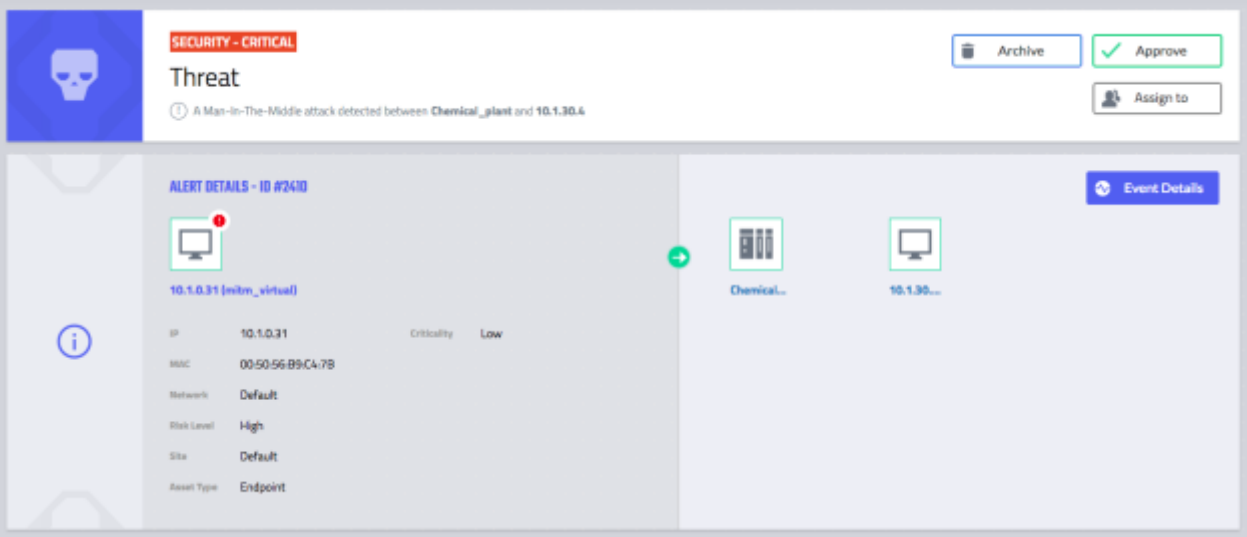

Figure 6: MITM alert (this MITM uses ARP poisoning) – main screen

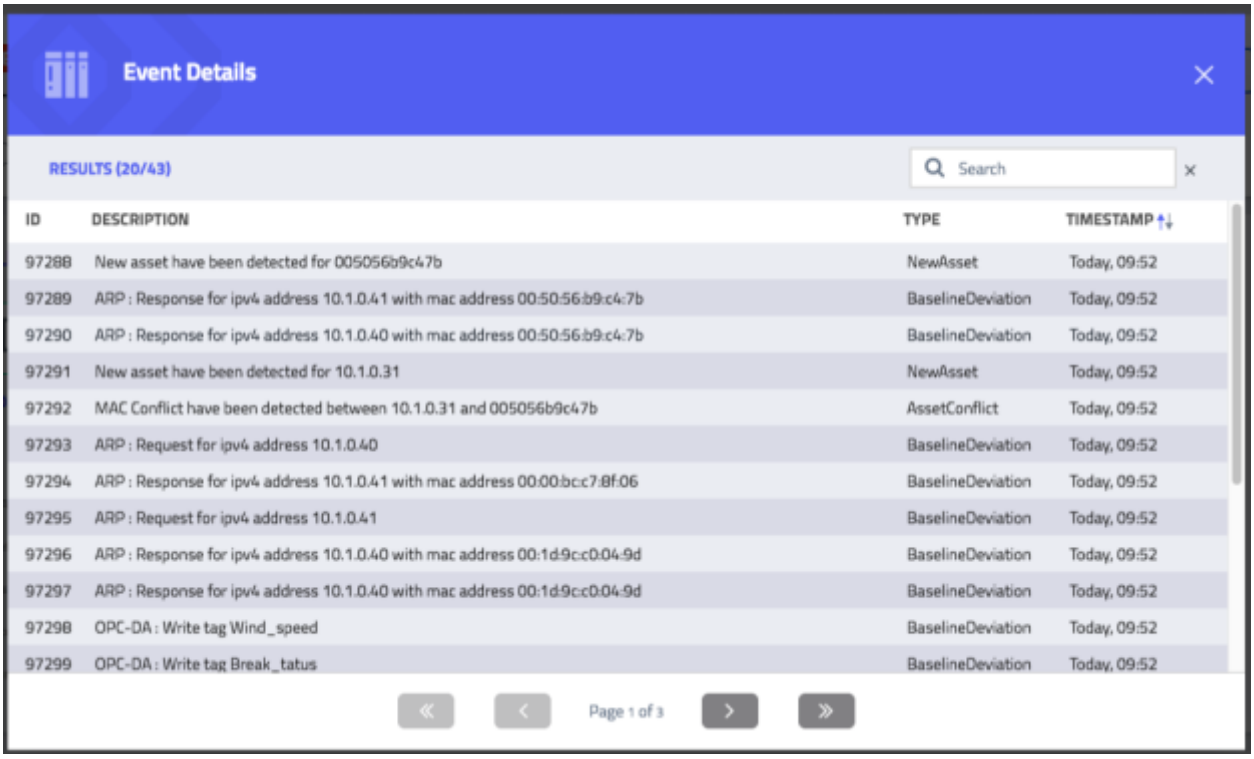

Figure 7: MITM alert (this MITM uses ARP poisoning) – events timeline