



PhantomPlant

Deploy a Fake Industrial Network Before Attackers Find the Real One.

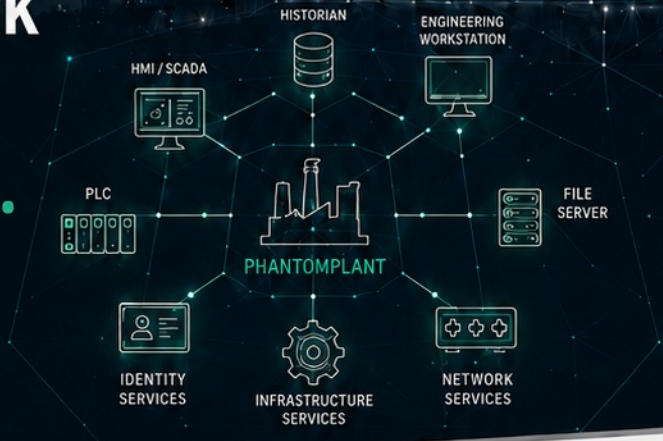
Not a simple honeypot.
A complete OT/IT deception environment.

PhantomPlant simulates a believable industrial and enterprise network segment made of multiple coordinated decoy devices - including PLCs, SCADA/HMI systems, historians, engineering workstations, file servers, and infrastructure services.

Instead of exposing one obvious trap, PhantomPlant creates a realistic fake plant with up to 10 decoy devices, each presenting its own services, protocols, hostnames, and behavior. Every scan, login attempt, protocol probe, and suspicious interaction is captured as a security event.



Every fake device becomes a sensor.
Every interaction becomes intelligence.



Deception overview
Live telemetry, attacker paths, and decoy asset health.

ASSETS 22 ↑ 2% vs. 7d Deception assets	INTERACTIONS 61,925 ↑ 18% vs. 7d Total interactions and events	CRITICAL EVENTS 0 Medium, PRIORITY, EOOOS, EOC...	CREDENTIALS 0 High, Admin, User, Kerberos
--	--	--	--

Assets surface

PLC-UNET-01 192.168.200.11 SMB: 192.168.200.11	PLC-FANIEL-02 192.168.200.12 SubNet: 192.168.200.12	PLC-COM001-03 192.168.200.13 Allen-Bradley	PLC-RTU-04 192.168.200.14 Modbus TCP
HMI-01 192.168.200.15 WinCC / WinGUI	ENG-WS-01 192.168.200.16 Engineering WS	SCADA/HMI 192.168.200.17 Ignition / Perspective	HISTORIAN-01 192.168.200.18 OPC UA, SQL, File store
ASSET-09 192.168.200.20 Linux	ASSET-10 192.168.200.20 File Server		

Live event timeline (Last 24 hours)

- 10s ago dcerpc.bind 192.168.200.41 from 192.168.100.14
- 1m ago login.failed 192.168.200.12 user: engineer
- 3m ago s7comm.read 192.168.200.11 from 192.168.100.27
- 5m ago modbus.func 03 192.168.200.14 from 192.168.100.55
- 8m ago smb.session 192.168.200.60 from 192.168.100.91
- 11m ago opcua.browse 192.168.200.51 from 192.168.100.74

OPC UA

```
NodeSet: XML      opc.tcp://192.168.200.51:4840/NodeSet.xml
S7U: Historian    192.168.200.51:1433
Pings [avg]      20 ms
```

MOST INTERACTIVE

HISTORIAN-01
192.168.200.51 - Historian live

OPC UA: 60% S7: 25% SMB: 10% Modbus: 5%

RISKS Medium	EVENTS 61,925	RISK Critical
------------------------	-------------------------	-------------------------



1

Up to 10 coordinated decoy devices



2

PLC, SCADA/HMI, historian, engineering workstation, file server, identity and infrastructure profiles

OT + IT protocol deception

Central dashboard and event visibility

Container-ready deployment for lab, edge or production-adjacent networks



PhantomPlant

Realistic Decoys, Real Services

A complete deception plant built from functional OT & IT emulations.

PhantomPlant doesn't simply open fake ports or act as a passive sensor. It deploys functional OT and IT service emulations inside a believable industrial network, allowing attackers to interact as if it were real—while capturing every action as a security event.

Deception overview
Live identities, attacker paths, and decoy asset health.

- ACTIVE DECOYS: 22 (13 assets, 22 exposed services)
- EVENTS TODAY: 61,925 (0 high-confidence attack sources)
- CRITICAL WRITES: 0 (Modbus, PROFNET, PROFIBUS writes)
- CREDENTIALS: 0 (login, token, basic, Kerberos)

Assets surface

PLC-INLET-01 PLC Modbus/PPN 192.168.200.32	PLC-PUMP-02 PLC Modbus/PPN 192.168.200.34	PLC-DOING-03 PLC Modbus/DP 192.168.200.34	PLC-FILTER-04 PLC Modbus/PPN/DP 192.168.200.35
PLC-OT-EDGE-05 Firewall SMB/HTTPS 192.168.200.36	ENG-CLIENT-01 Workstation SMB/HTTP 192.168.200.37	SCADA-SRV-01 SCADA Server NTP/PPN/OPC UA 192.168.200.38	HISTORIAN-01 Historian OPC UA/SMB 192.168.200.39
ASSET-09 Server TCP 192.168.200.40	ASSET-10 Server TCP 192.168.200.41	OPC UA OPC UA 192.168.200.39:6460	NodeSet XML OPC UA XML 192.168.200.39:8080/servlet.xml
SQL Historian SQL Server 192.168.200.38:1433			

Live event timeline (Live API stream)

- dns query client.smartthings.com -> 192.168.200.41 (192.168.200.174 to INFRA-SERVICES-01 - DNS Server) 05:48
- dns query client.smartthings.com -> 192.168.200.41 (192.168.200.174 to INFRA-SERVICES-01 - DNS Server) 05:48
- dns query ods.samsungcloudsolution.com -> 192.168.200.41 (192.168.200.174 to INFRA-SERVICES-01 - DNS Server) 05:48
- dns query odconnect-shard-eu02-ewest1.samsungotc... (192.168.200.174 to INFRA-SERVICES-01 - DNS Server) 05:48
- dns query client.smartthings.com -> 192.168.200.41 (192.168.200.174 to INFRA-SERVICES-01 - DNS Server) 05:48
- dns query client.smartthings.com -> 192.168.200.41 (192.168.200.174 to INFRA-SERVICES-01 - DNS Server) 05:48
- dns query evls.samsungcloud.com -> 192.168.200.41 (192.168.200.174 to INFRA-SERVICES-01 - DNS Server) 05:48
- dns query evls.samsungcloud.com -> 192.168.200.41 (192.168.200.174 to INFRA-SERVICES-01 - DNS Server) 05:48

1 FUNCTIONAL OT PROTOCOL EMULATION

OPC UA
OPC UA Server

OPC XML
NodeSet XML

Modbus/TCP
Modbus Server

Functional service emulations—not simple banners.

Connect

Read

Subscribe

Write

Browse

PhantomPlant supports realistic protocol interactions and commands, so attackers can connect, query, subscribe, browse, and write—just like on a real system.

2 REALISTIC FILE SERVER LURES



PhantomPlant includes a ready-made fake file system with **2,500 files** across realistic OT and business folder structures.

```

\\FILE-SERVER
├── Engineering
├── Operations
├── Maintenance
├── Documents
├── Reports
└── 2,500 Files
    
```

Detect suspicious browsing, backup hunting, document enumeration, and access to fake business or OT files.

3 WORKING INFRASTRUCTURE SERVICES

Core IT services operate normally as part of the deception environment—making the fake network more complete and believable while providing rich network data.

DNS
DNS Server
Resolves queries and provides realistic responses.

DHCP
DHCP Server
Leases addresses and options like a real DHCP service.

NTP
NTP Server
Provides accurate time to devices and clients.

4 REALISTIC DECOY ASSET PROFILES

PhantomPlant deploys a full ecosystem of believable assets that work together like a real plant network.

PLC Decoys
Functional PLC emulations with real protocols.

SCADA / HMI Decoys
Realistic HMIs and SCADA servers for operator interaction.

Historian Decoys
OPC UA & SQL historian services with live data.

Engineering Workstations
Engineering clients with tools, projects, and configurations.

File Server Decoys
SMB shares with realistic folders and documents.

Identity Services
AD, LDAP, and authentication services.

Infrastructure Services
DNS, DHCP, NTP, Syslog, and more core services.

Remote Access Endpoints
RDP, SSH, and VPN endpoints for lateral movement.

Not fake ports. Functional service emulations.

What It Detects

- 🔍 Network scanning
- 🔍 Modbus reads and write commands
- 🔍 Service enumeration
- 🔍 SMB share access
- 🔍 Unauthorized login attempts
- 🔍 File and backup enumeration
- 🔍 OPC UA / OPC XML interaction
- 🔍 DNS / DHCP / NTP interaction



From Deception Events to Actionable Alerts

Central event collection, local visibility, and flexible alert delivery.

1 DEPLOY DECEPTION WHERE VISIBILITY IS MISSING



Prebuilt container images



Static IP network layouts



ARM64 or ARM64 hardware



Small edge devices or lab servers

Place PhantomPlant close to OT labs, industrial DMZs, production-adjacent networks, remote sites, or validation zones — anywhere visibility is weak and attackers may probe.

2 CENTRAL EVENT API / EVENT FLOW



Every interaction with a decoy generates a structured security event including source IP, target asset, protocol, event type, timestamp, severity, and interaction details.

3 DASHBOARD & EVENT VISIBILITY

PhantomPlant

- ACTIVE DECOYS: 22 (10 assets, 22 exposed services)
- EVENTS TODAY: 61,925 (0 high-confidence attack sources)
- CRITICAL WRITES: 0 (Modbus, PROFINET, PROFIBUS writes)
- CREDENTIALS: 0 (login, token, basic, Kerberos)

Recent critical events

- CRITICAL: **opc ua write ControlLoop01.PhValue = 8 success** (HISTORIAN-01 - OPC UA - 27/06/2026, 11:14:32)

Top attack sources

- 192.168.200.41
- 192.168.200.35
- 10.0.5.12

Event Detail: Critical

opc ua write ControlLoop01.PhValue = 8 success
HISTORIAN-01 - OPC UA - 27/06/2026, 11:14:32

Summary
opc ua write ControlLoop01.PhValue = 8 success

RISK SCORE 100 / 100	FINGERPRINT opcua-client[HISTORIAN-01]OPC UA[opc ua write controlloop01.phvalue = 8 success	Target asset HISTORIAN-01 Historian - OPC UA/SQL 192.168.200.39 Historian live
SOURCE IP opcua-client 192.168.200.39	SOURCE COMPUTER SRC-opcua-client HISTORIAN-01	
SOURCE MAC 02:50:5D:9F:c1:ca	ASSET HISTORIAN-01	
ASSET IP 192.168.200.39	PROTOCOL OPC UA	
PORT unknown	ZONE WAN	

Attack story / source timeline

- opc ua write ControlLoop01.PhValue = 8 success (HISTORIAN-01 - OPC UA - 11:14:32) **100**

Raw event JSON [Copy JSON](#)

Assets at risk

- HISTORIAN-01: High
- PLC-PUMP-02: Medium
- ENG-CLIENT-01: Low

4 ALERTING & INTEGRATION



Email alerts
Instant notifications



SNMP traps
Send events to NMS systems



Webhooks
Real-time integrations with tools



Microsoft Teams notifications
Stay in the flow



API / SOC / SIEM integration
Automate and correlate

Important events should not stay hidden inside a dashboard. Route them to your security teams and workflows automatically.

5 LOCAL VISIBILITY / CONTROLLED ENVIRONMENTS



PhantomPlant doesn't require external cloud connectivity to operate. Events can be collected, stored, and visualized locally—making it ideal for isolated OT networks, secure labs, industrial DMZs, and restricted environments.

What Security Teams Can See

- Source IP address
- Target decoy device
- Protocol or service used
- Event type and severity
- Timestamp and repeated activity
- Asset-level interaction history



Decoys generate the signal. The Event API collects it. Alerts deliver it. The dashboard makes it visible.

