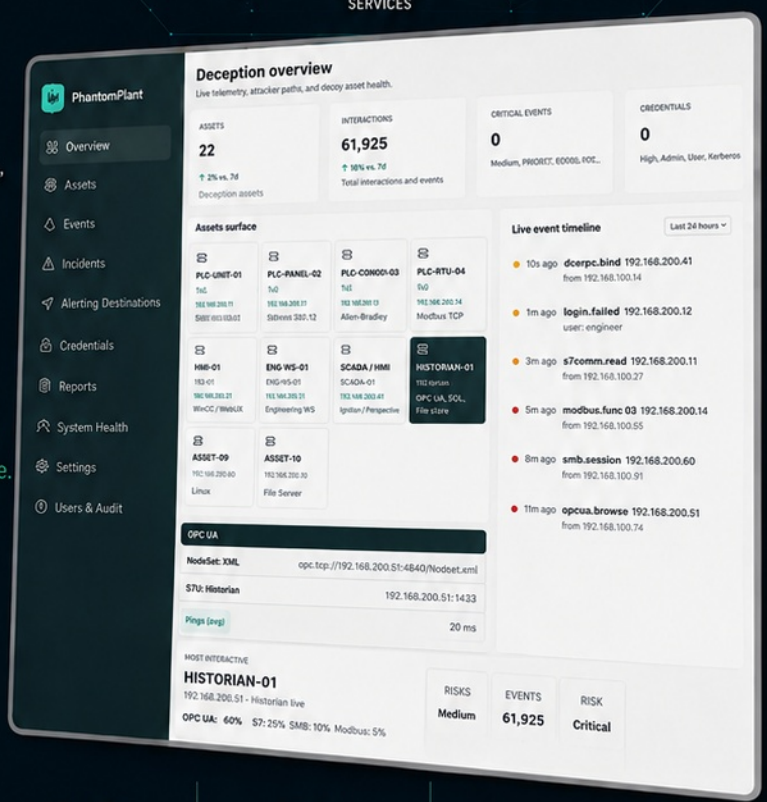
PhantomPlant

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.

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

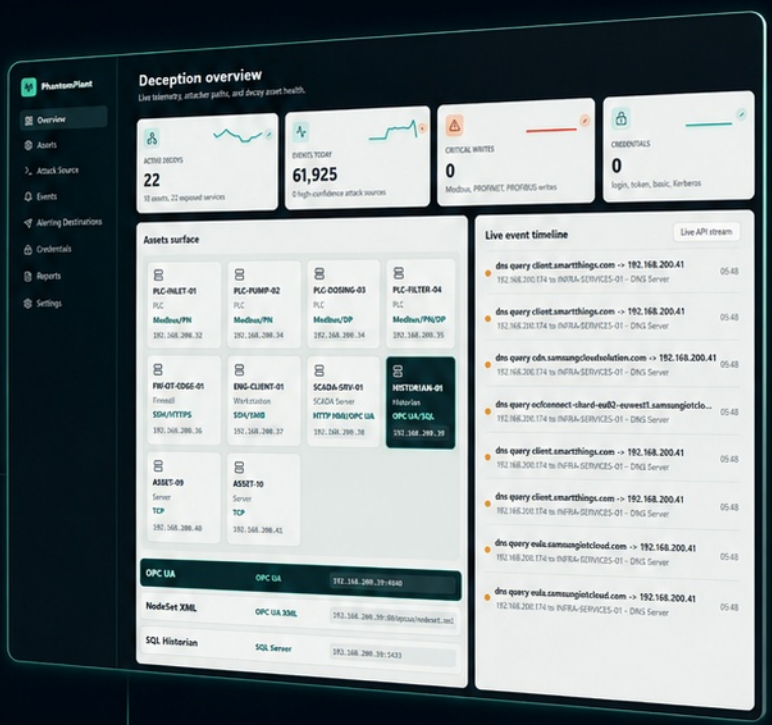
SMALL FOOTPRINT. HIGH SIGNAL. OT-AWARE DECEPTION.

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.



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

SMALL FOOTPRINT. HIGH SIGNAL. OT-AWARE DECEPTION.

PhantomPlant

From Deception Events to Actionable Alerts

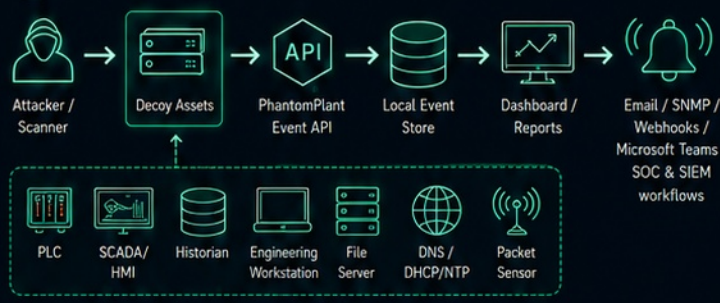
Central event collection, local visibility, and flexible alert delivery.

1 DEPLOY DECEPTION WHERE VISIBILITY IS MISSING

- Prebuilt container images
- Static IP network layouts
- ARM64 or ARM64 hardware
- Small edge devices or lab servers

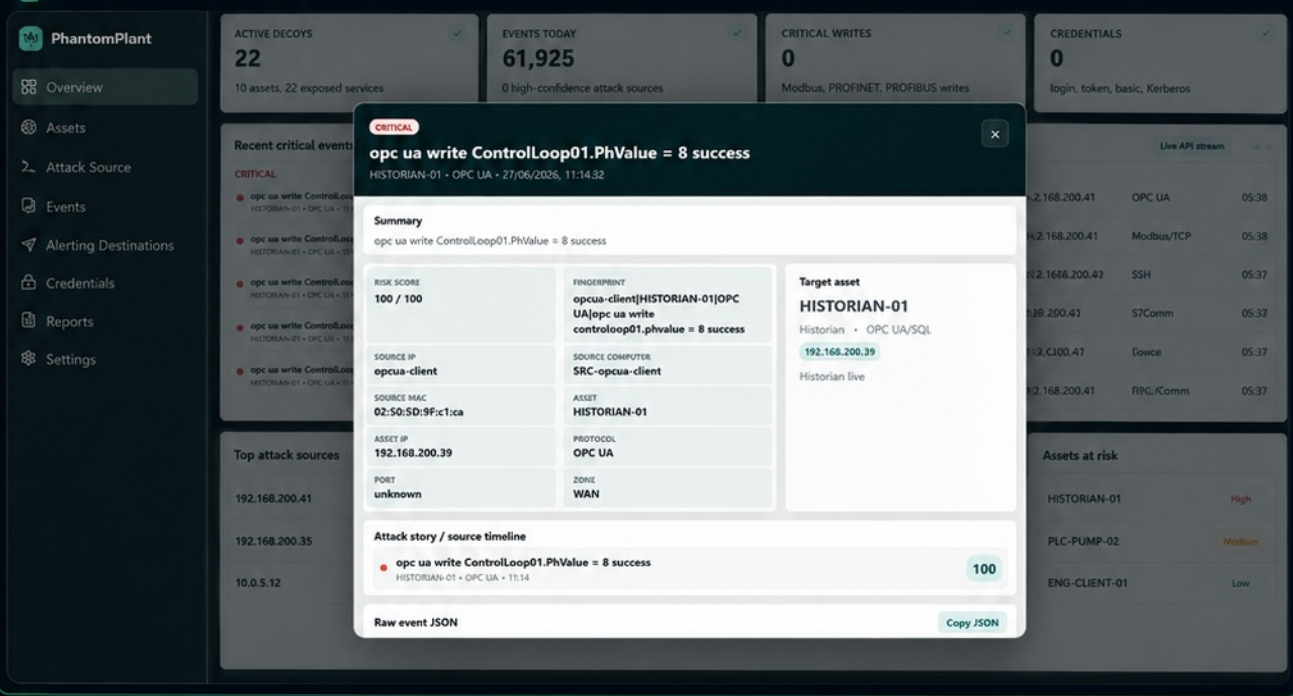
Place PhantomPlant close to OT labs, industrial DMZs, production-adjacent networks, remote sites, or validation zones — anywhere visibility is weak and attackers may probe.

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



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.