PhishCloud IT/OT Threat Hunting Services

PhishCloud Threat Hunting Services detect hidden threats, expose attack paths, and strengthen operational resilience before disruption

PHISHCLOUD
Protect The Click. Defend The Core.

SERVICES

- Hypothesis-Driven Hunt Methodology
- IT and OT Environment Coverage
- Passive, Non-Disruptive OT Approach
- Managed or Periodic Engagement Models
- CFC-Integrated Intelligence Loop

The Problem

Most organizations rely on automated detection to find threats. But the most dangerous adversaries don't trigger alerts. They blend in. Nation-state actors like Volt Typhoon maintained persistent access inside U.S. critical infrastructure for five years using living-off-the-land techniques that look like normal system activity. Today, 79% of intrusions are completely malware-free, meaning signature-based detection never had a chance.

For organizations with operational technology, the stakes are higher still. IT and OT security teams operate in silos. Engineers are measured on uptime. Security teams are measured on data protection. The result: no one is actively hunting across the full attack surface, the IT networks, engineering workstations, historians, PLCs, and HMIs that sophisticated adversaries use as stepping stones from enterprise to operations.

The problem isn't your tools. Tools generate alerts. Alerts aren't insight. The adversaries already inside your network are counting on that gap.

The Solution: PhishCloud OT Threat Hunting Services

Industrial organizations and enterprises don't fail because they lack tools. They fail because no one is actively searching for the threats those tools aren't built to find.

PhishCloud IT/OT Threat Hunting Services deliver human-led, AI-augmented, hypothesis-driven hunting across your entire environment: IT networks, OT systems, and the converged boundary between them. We hunt for adversaries who have already bypassed automated detection: living-off-the-land actors, credential abusers, lateral movers, and nation-state actors pre-positioning for operational disruption.

Our hunters bring deep operational awareness to every engagement. In OT environments, we use passive, non-disruptive methods: network taps, SPAN ports, and historian data with zero impact to production systems. In IT environments, we correlate behavioral deviations, authentication anomalies, and telemetry gaps that automated tools consistently miss.

PhishCloud offers two delivery models designed to fit different operational realities:

Managed Threat Hunting: Continuous, subscription-based hunt coverage as an extension of your security team: ongoing hypothesis-driven hunts, dedicated hunter capacity, regular reporting, and sustained maturity advancement.

Periodic Hunt Engagements: Structured, targeted hunting on a defined schedule or for specific threat scenarios, expert-level hunting without a long-term commitment.

Both models integrate directly with PhishCloud's Cyber Fusion Center framework, ensuring every finding enriches detection engineering, threat intelligence, and incident response, not just a report that sits in a folder.

www.phishcloud.com
sales@phishcloud.com

OT Threat Hunt Key Benefits

How this helps teams immediately:

- Find adversaries automated tools miss, including living-off-the-land actors, credential abusers, and pre-positioned nation-state threats.
- Hunt OT environments without disrupting production, uptime, or safety systems.
- Convert hunt findings into detection improvements, not reports that gather dust.
- Gain architectural intelligence revealing systemic gaps requiring strategic remediation.

Why Customers Trust PhishCloud?

Deep OT Operational Expertise: PhishCloud understands that industrial and enterprise environments are complex ecosystems, not isolated networks. Our hunters analyze activity within real operational workflows, not theoretical attack models.

IT to OT Threat Visibility: We eliminate blind spots between enterprise networks and operational systems. PhishCloud correlates activity across identity, network, endpoint, and OT telemetry to identify threats moving across domains.

Threat Led Detection: We focus on how attackers actually behave, not just what tools detect. By hunting for adversary techniques and attack paths, we identify threats before they trigger automated defenses.

Cross-Domain Intelligence Correlation: Threats rarely stay in one domain. PhishCloud correlates activity across identity, network, endpoint, cloud, and OT systems to expose attack patterns that isolated tools miss. Customers trust PhishCloud because we see the full picture, not fragments.

Executive Level Communication: Security findings only matter if leadership understands them. PhishCloud translates hunt results into operational and financial risk insights leadership can act on.

Cyber Fusion and OT MDR Integration: Our threat hunting services integrate directly into Cyber Fusion Center and OT MDR workflows, enabling continuous improvement across detection, response, and intelligence operations.

Production First Security Model: Everything we deploy is designed to strengthen security without disrupting operations. Hunting is performed using passive and intelligence-driven methods that protect uptime and safety.

OT Threat Hunter Key Deliverables

Typical outputs from each delivery model.

Managed Threat Hunting

- Continuous hypothesis-driven hunts across IT and OT environments.
- Monthly executive hunt summary with findings and risk context.
- Detection rule recommendations with MITRE ATT&CK coverage gap analysis.
- Hunt intelligence integrated into CFC detection engineering and IR playbooks.
- Dedicated hunter capacity working as an extension of your security team.

Periodic Threat Hunt Engagement

- Scoped hunt plan with defined hypotheses, target environment, and methodology.
- Full hunt execution across designated IT and/or OT systems.
- Findings report: confirmed threats, behavioral anomalies, and detection gaps.
- Detection rule and incident response playbook recommendations.
- Executive briefing with risk-adjusted findings and business impact summary.
- Post-engagement maturity assessment with recommended next step.

OT Threat Hunt Strategy Components

A structured approach built for converged IT and OT environments:

- **Hypothesis-driven methodology.** Hunts built on adversary TTPs and environmental intelligence, not just alert queues.
- **Assumption of compromise.** We hunt as if adversaries are already present, because they may be.
- **MITRE ATT&CK and ATT&CK for ICS alignment.** Structured coverage across tactics and techniques in both IT and industrial environments.
- **Behavioral analytics.** Anomaly detection across users, devices, applications, and industrial systems against established baselines.
- **IT/OT convergence awareness.** Cross-domain correlation connecting enterprise telemetry with operational network visibility.
- **CFC feedback loop.** Every hunt finding flows back to detection engineering, threat intelligence, IR playbooks, and vulnerability management.
- **Continuous maturity advancement.** Every engagement improves your program, not just your report count.

OT Threat Hunt Key Outcomes

What customers can expect to achieve:

- Reduced mean time to detect across IT and OT environments.
- Detection gaps identified and closed through hunt-driven detection engineering.
- Threat intelligence enriched with environment-specific adversary behavior.
- Incident response playbooks refined with real-world hunt findings.
- Executive visibility into quantified security posture improvement.
- A hunt program that advances in maturity with every engagement.

If you're ready to find what your automated tools are missing, in IT, in OT, or across both, PhishCloud IT/OT Threat Hunting Services are built for you.

PHISHCLOUD
Protect The Click. Defend The Core.

www.phishcloud.com
sales@phishcloud.com
9 Lake Bellevue Drive
Suite 120
Bellevue, WA 98005