PHISHCLOUD
Protect The Click. Defend The Core.

PhishCloud Operational Technology Incident Response Services

PhishCloud Incident Response Services help industrial organizations triage security events, declare and classify incidents, contain threats safely, restore operations, and close the loop with after-action improvement across IT and OT environments.

SERVICES

- OT-Aware Incident Triage
- Safety-First Containment
- Purdue-Zone-Aware Response
- Operations-Integrated Incident Command
- After-Action Continuous Improvement

The Problem

Most industrial organizations have an incident response plan. Few have a true incident response capability.

Organizations commonly struggle with:

- IR plans that have never been tested under realistic conditions.
- IT-centric playbooks that fail when incidents touch OT.
- No incident commander available when an event fires.
- Containment decisions made without process-safety review.
- Emergency onboarding during an active incident.
- Detection gaps that remain open after the incident ends.
- Regulatory reporting clocks that are missed or poorly coordinated.
- Lessons learned that never become better playbooks, detections, or response actions.

The consequence is predictable. Incidents take longer than they should, cost more than they should, create unnecessary operational risk, and often repeat because the response loop was never closed.

The Solution: PhishCloud OT Incident Response Services

PhishCloud Incident Response Services provide a retainer-backed response capability for converged IT and OT environments. The service begins the moment a detection event is referred for review and continues through triage, incident declaration, containment, eradication, recovery, stakeholder coordination, and after-action reporting.

PhishCloud separates Incident Response from Digital Forensics on purpose. Incident Response restores operations and removes the threat. Digital Forensics preserves evidence and produces defensible findings. The two services coordinate when needed, but they are delivered as separate disciplines with separate objectives and success criteria.

PhishCloud Incident Response Services support:

- Active security events requiring triage.
- Declared incidents across IT and OT environments.
- Ransomware, BEC, insider, third-party, denial-of-service, data exfiltration, and OT disruption scenarios.
- Safety-aware containment decisions.
- Executive, operational, regulatory, and technical communications.
- Hand-off to Digital Forensics when deeper investigation is required.
- After-action improvement tied to detection engineering, threat hunting, and playbook maturity.

The result is faster response, safer containment, clearer decision authority, stronger regulatory readiness, and a response capability that improves after every incident.

Strategy Components

A structured incident response approach built for converged IT and industrial environments.

- Incident response plan development
- Sector and scenario-specific playbooks
- RACI and incident command structure
- Executive, operational, technical, and regulatory communication templates
- Tabletop exercise program
- Retainer onboarding and environment familiarization
- Detection event validation and incident classification
- Purdue Level scoping and asset impact analysis
- Safety-first containment planning
- Eradication, recovery, and watch-period support
- After-action reporting, continuous improvement backlog

Why Customers Trust PhishCloud?

Incident Response and Digital Forensics as Separate Disciplines. PhishCloud does not blur response and forensics into a generic DFIR motion. Incident Response restores operations. Digital Forensics produces defensible findings. Separating the two protects both outcomes.

Safety-First OT Containment. Containment actions are reviewed against operational state and process safety before execution. PhishCloud avoids actions that could destabilize production or turn a cyber incident into a safety event.

Purdue-Zone-Aware Response. PhishCloud response actions are designed around the affected Purdue Level. A historian, HMI, engineering workstation, jump host, firewall, and PLC do not carry the same operational risk.

Operations-Integrated Incident Command. PhishCloud's incident commander works alongside the client's operations lead, plant manager, and safety officer. Cyber recommends. Operations owns process-impact decisions.

Playbook-Driven Response. Retained clients receive pre-built, reviewed, and exercised playbooks before an incident occurs. Response is rehearsed, not improvised.

Regulatory Clock Awareness. PhishCloud tracks applicable reporting obligations, including CISA CIRCIA, TSA directives, NERC CIP, NIS2, SEC disclosure, cyber insurance, and contractual requirements.

Closed Loop with Detection Engineering. Every incident produces detection gaps, TTPs, indicators, and improvement items that feed directly into the detection engineering backlog.

OT Incident Response Key Deliverables

Typical outputs from the engagement:

Incident Response Readiness

- Incident Response Plan.
- Playbook library.
- RACI and incident command structure.
- Communication templates.
- Tabletop exercise program.
- Retainer onboarding package.
- Annual program review.

Triage and Classification

- Detection event validation.
- Incident severity classification.
- Affected asset and account scoping.
- Purdue Level impact assessment.
- Incident declaration record.
- Initial evidence preservation package.

Containment

- Containment action plan.
- Safety and operational risk review.
- Purdue-zone-specific containment recommendations.
- Identity, access, segmentation, and firewall control actions.
- Action log with timestamp, author, asset, action, and rationale.

Eradication and Recovery

- Malware removal and vector closure support.
- Credential rotation and access revocation guidance.
- Configuration repair and hardening recommendations.
- Recovery validation.
- Watch-period monitoring recommendations.
- Formal hand-back to operations.

Communications and Coordination

- Incident commander support.
- Executive, technical, and operations update cadence.
- Regulatory reporting clock tracking.
- Third-party coordination support.
- Warm hand-off to Digital Forensics when needed.

OT Incident Response Key Benefits

How this helps teams immediately:

- Responds faster because the team, plan, and environment are known before the incident.
- Protects process safety and reduces operational risk during containment and recovery.
- Restores operations quickly through structured incident command and documented recovery procedures.
- Provides clear executive visibility into what happened, what is happening, and what decisions are required.
- Supports regulatory, insurance, and stakeholder confidence with a defensible response process.
- Continuously improves security posture by turning incident lessons into stronger detections, playbooks, and reduced repeat incidents.

PHISHCLOUD
Protect The Click. Defend The Core.

www.phishcloud.com
sales@phishcloud.com
14400 NE Bel Red Road
Unit 209
Bellevue, WA 98007