COFENSE MANAGED PHISHING DETECTION AND RESPONSE
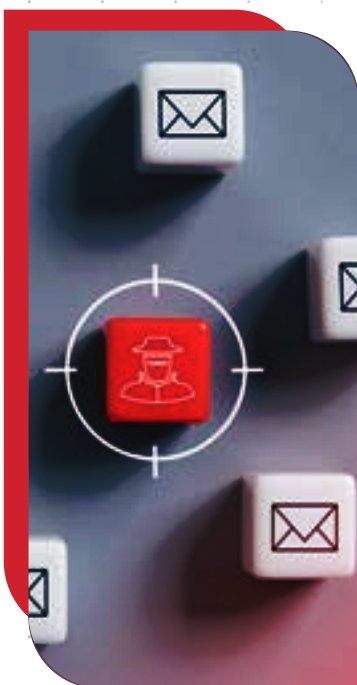
PHISHME **COFENSE**

Cofense Managed Phishing Detection and Response (MPDR) is a fully managed service designed for security teams that lack the time, headcount, or in-house expertise to keep up with today's fast-moving phishing threats.

Your Problem.

For many organizations, building and maintaining an effective phishing defense program is a complex and resource-intensive task. Limited time, expertise, and resources often hinder the ability to install, configure, deploy, and maintain a comprehensive solution. Email analysis is a critical component of threat management, but it can be highly time-intensive, requiring substantial resources and dedicated teams to handle the sheer volume of potential threats effectively. This not only places a strain on the security operations team but also diverts skilled employees from focusing on higher-level security priorities. Without a streamlined and managed approach, organizations struggle to balance operational efficiency with robust phishing mitigation.

Our Solution.

Cofense MPDR is a fully managed service that combines expert-supervised AI with dedicated phishing analysts to detect, investigate, and remediate advanced threats that evade traditional perimeter defense solutions. By owning triage and response end-to-end, Cofense accelerates MTTD and MTTR, reduces analyst workload, and delivers high-fidelity detection with actionable threat insights—all without adding operational complexity.

WHY CHOOSE COFENSE?

Faster Threat Resolution

Cofense's threat analysts take full ownership of phishing triage and response—reviewing user-reported messages, identifying malicious content, and assisting with threat insight and containment.

High-Fidelity Alerts. Less Noise.

MPDR eliminates alert fatigue by filtering out spam and false positives. Every alert your team receives has already been reviewed and validated—allowing you to focus on response, not investigation.

Real-World Threat Visibility and Actionable Intelligence

Gain visibility into emerging attack patterns informed by real phishing attempts across industries and sectors. MPDR delivers timely, actionable intelligence rooted in user behavior—so your team can prioritize the risks that matter most.

PHISHME
COFENSE

WHY CHOOSE COFENSE?

Scalable, Cost-Effective Expertise

MPDR functions as a force multiplier for your SOC—expanding your team's capabilities without adding headcount or 24x7 staffing costs. Whether you're scaling globally or just trying to keep up with daily volume, MPDR scales with your needs.

Immediate Alerting

You are notified immediately after a malicious email has been identified by a PDC analyst. You'll receive a detailed escalation report that provides threat context and all first- and second-stage IOCs are made available via API, further enhancing a rapid response.

Transparent, Monthly Reporting

Regular reports provide detailed insights into identified threats, response times, and valuable trend data, empowering you to make informed decisions on how to allocate your defensive resources.

Scan the QR code or visit **cofense.com** to learn how to catch more phish with Cofense.

EXCLUSIVE FEATURES OF COFENSE MPDR

A SOC Built for Phishing

Cofense's Phishing Defense Center (PDC) is staffed by analysts who specialize exclusively in phishing — triaging millions of real threats annually across highly targeted organizations.

Expert-Supervised AI with Real-World Insights

Our models are trained on phishing-specific patterns, attacker behavior, and a continuously updated stream of human-reported threat data. That intelligence, reviewed and refined by experts, drives a 99.998% detection accuracy and surfaces real threats faster.

Faster Containment, Measurable Results

With a 60-minute average service level objective and an average time to detect and respond of just 18 minutes, MPDR dramatically reduces dwell time and speeds remediation without overloading your team.

Rapid Auto-Quarantine

Response times far outpace legacy tools.

Cofense is the only cybersecurity company leveraging expert-supervised AI for phishing detection and response—delivering human-vetted intelligence and real-world training to help enterprises stay ahead of modern threats. Built to augment existing email defenses, Cofense identifies attacks that bypass perimeter filters, remediates them in minutes, and continuously strengthens the human layer through simulations modeled on active phishing campaigns. Informed by insights from over 35 million trained users, Cofense enables faster containment of threats and measurable reductions in risk. Organizations like Visa, Siemens, and Blue Cross Blue Shield rely on Cofense to reduce exposure, meet regulatory demands, and build lasting resilience against the most persistent cyber threat: phishing.

SMARTER PHISHING DEFENSE. STRONGER HUMAN SECURITY. COFENSE.COM