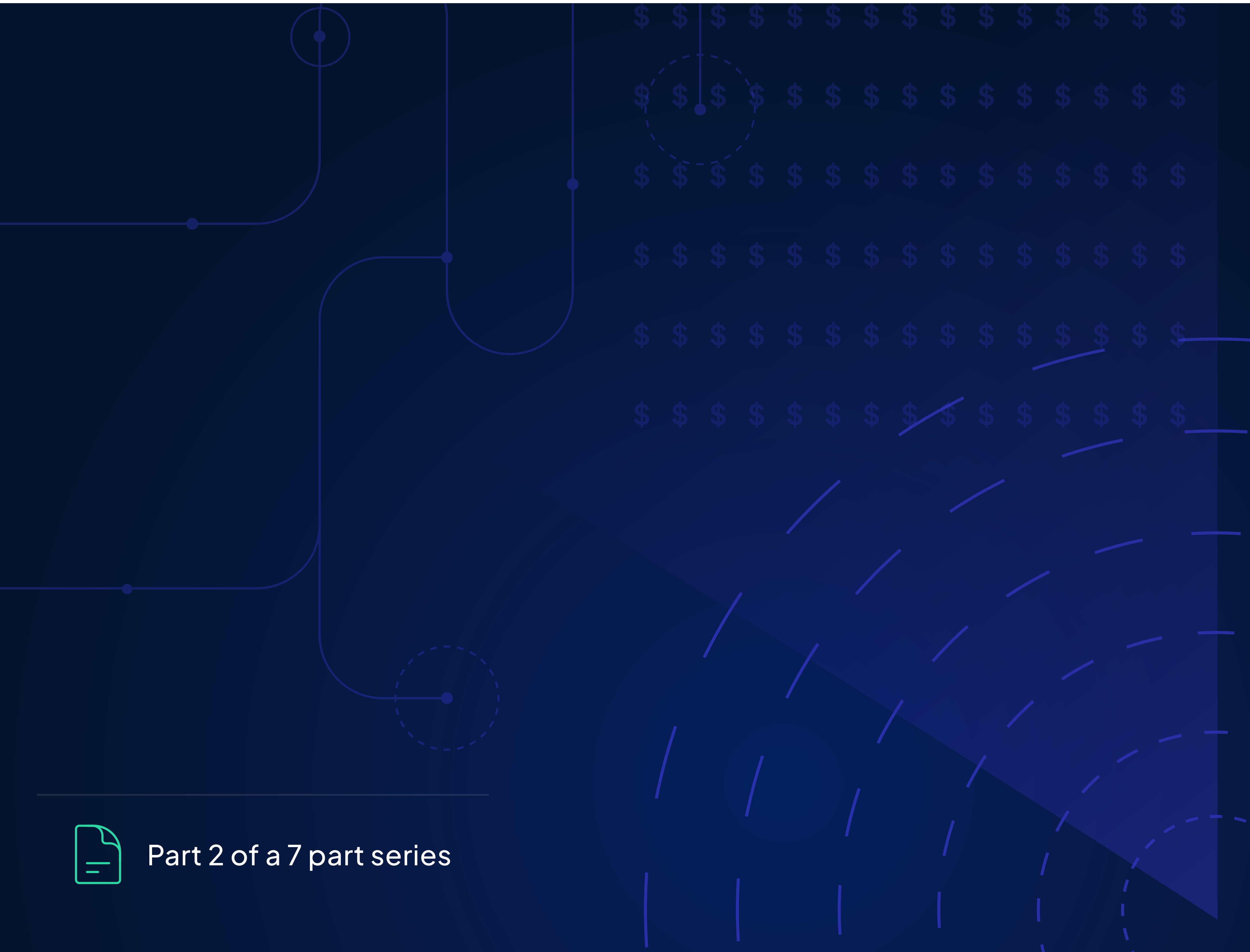
digital hands®

# The $4.88 Million Vector:

How Managed Detection and Response (MDR)
Mitigates Phishing Attacks.



Part 2 of a 7 part series

# Table of Contents

As security tools have improved and defenses have been hardened over time, malicious actors have homed in on an easier mark — the human factor. People are an ideal target because scammers know they can count on human traits like curiosity, carelessness, or fear of missing out to drive risky behaviors. This tactic also works because it exploits the trust people have in known parties such as brands.

That's why phishing has been a prevalent threat for years, serving as the initial vector in attacks ranging from business email compromise (BEC) and fraud to malware and ransomware. According to the U.S. Cybersecurity & Infrastructure Security Agency, 90% of successful cyberattacks begin with someone clicking a malicious email link.

# Why every CISO and SOC should care about phishing

As security tools have improved and defenses have been hardened over time, malicious actors have homed in on an easier mark — the human factor. People are an ideal target because scammers know they can count on human traits like curiosity, carelessness, or fear of missing out to drive risky behaviors. This tactic also works because it exploits the trust people have in known parties such as brands.

That's why phishing has been a prevalent threat for years, serving as the initial vector in attacks ranging from business email compromise (BEC) and fraud to malware and ransomware. According to the U.S. Cybersecurity & Infrastructure Security Agency, 90% of successful cyberattacks begin with someone clicking a malicious email link.

## The implications of this high-volume, high-impact threat are huge:

- ✓ 71% of surveyed organizations experienced at least one successful phishing attack in the past year.
- ✓ There are more than 1 million unique domain names associated with phishing.
- ✓ It takes a person under 60 seconds (median) to fall for a phishing email — just 21 seconds to click on a link after opening the email and 28 seconds to enter data on a phishing site.
- ✓ BEC attacks, also known as CEO fraud, are rampant — with 156,000 BEC attacks observed daily by Microsoft alone.

### The consequences of phishing attacks for organizations are many, including:

| 32% | 32% | 29% | 27% | 27% | 25% |
|---|---|---|---|---|---|
| Loss of data or intellectual property<br>(reported by 32% of surveyed organizations) | Ransomware infection | Breach of customer data | Credential or account compromise | Reputational damage | Widespread network outage and downtime |
| ↗ | ↗ | ↗ | ↗ | ↗ | ↗ |

For the SOC, phishing attacks are becoming much more difficult to detect. For instance, 76% of phishing sites now use HTTPS protocols to appear legit, according to Verizon's 2024 Data Breach Investigations Report.

Worse yet, Generative AI is making it even easier to craft legitimate-looking messages. Threat actors are taking full advantage of this technology — security researchers noted a 4,151% increase in the number of malicious emails sent in the first year and a half alone since the launch of ChatGPT.

# How a phishing attack may unfold

Attackers have a wide arsenal of tools for perpetrating phishing attacks, including spoofed links, man-in-the-middle techniques, content injection (fake login pages), and quishing (QR phishing).

This is just one example of what a successful phishing attack may look like:

**STEP 1**

## The Bait

The attackers impersonate a trusted source, such as an IT admin, with an urgent or innocuous-looking message. *(For example, an email with a subject line that reads, "Urgent: Password Expiration Notice.")*

**STEP 2**

## The Hook

The target clicks the malicious link, which leads to a spoofed website displaying a fake login page that looks legit. The target enters login credentials, which are automatically harvested by the phishers.

**STEP 3**

## The Exploitation

With access to the victim's account unlocked, attackers use a variety of methods to gain further access into the company and carry out the objectives, whether to perpetrate a BEC scam, deploy malware or ransomware, exfiltrate data, or impersonate a user.

# Here’s how a BEC attack unfolded in the real world:

**STEP 1**

The co-founder of Australian-based hedge fund Levitas Capital clicks on a malicious link masquerading as a legit-looking Zoom meeting invite.

**STEP 2**

The attacker gets full access to his email and uses it to learn how the firm operates and how to mimic email interactions.

**STEP 3**

Five days later, the bad actor impersonates the victim, sending the fund administrator a request to deposit payment for a $1.2 million invoice to the scammers bank account. **Within the next 10 days, the scammer uses this tactic to withdraw more than $8 million in total.**

**Although Levitas recovered some of the funds, the company’s reputation was shattered — it lost a critical investor, forcing it to shut down.**

# How to combat phishing with managed detection and response services

With the pivot to human-centric attacks, threat actors are more commonly using phishing to compromise user accounts — especially cloud services — rather than endpoints. Regardless of the tactics, AI-driven defenses that can understand the environment intelligently and adapt the response are especially critical when proactively mitigating phishing that slipped past your technology defenses like email security. MDR can help contain a phishing attack to limit its impact, spread, and severity — for instance, preventing data leakage or lateral movement.

**Here's what the MDR phishing incident playbook may look like, using a combination of automated tools and human experts:**

## 1. Detection

The MDR's detection technology collects and integrates telemetry to detect indicators of compromise, such as:

- Abnormal login attempts from new locations
- Suspicious email attachments or links
- Network traffic to known phishing domains
- Email forwarding activity to external domains
- New phone numbers being added to MFA
- Password or MFA resets
- Spam email sent internally

## 2. Automated containment

If the customer's email security tool didn't quarantine the suspicious email and it reached the user, the MDR platform automates actions such as disabling the user account when indicators of compromise are detected. The automated rules are based on criteria such as user role and function and the customer's risk tolerance levels.

## 3. Investigation

MDR analysts investigate flagged events to confirm phishing attempts. For instance, they will identify whether bad actors used stolen credentials to access an employee account and recommend response actions.

## 4. Action

Based on how the solution is customized to the customer's needs, the MDR SOC either advises the in-house security team to reset passwords or resets them on the customer's behalf.

# Benefits of MDR beyond phishing defense

Digital Hands' Real-World MDR offers much more than defense against the threat of phishing.

## Your MDR partner can augment your in-house SOC or security team, enabling them to:

- ✓ See more — faster — to protect your environment holistically.
- ✓ Get higher-fidelity alerts and integrated, enriched telemetry.
- ✓ Improve operational efficiency while allowing you to automate your workflows based on your risk appetite.
- ✓ Increase response time with automated containment and expert-led investigations, reducing the window of opportunity for the adversary.

Buyer's Guide

## Not sure where to start?

Get your MDR Buyer's Guide to understand key evaluation criteria and the 8 must-ask questions before you buy.

Download Now

How to Choose the Best Managed Detection and Response (MDR) Partner.

A Buyer's Guide for CISOs

digital hands