The $16 Billion Nightmare:

How MDR Mitigates Zero-Day Exploits Before They Escalate

Part 6 of a 7 part series

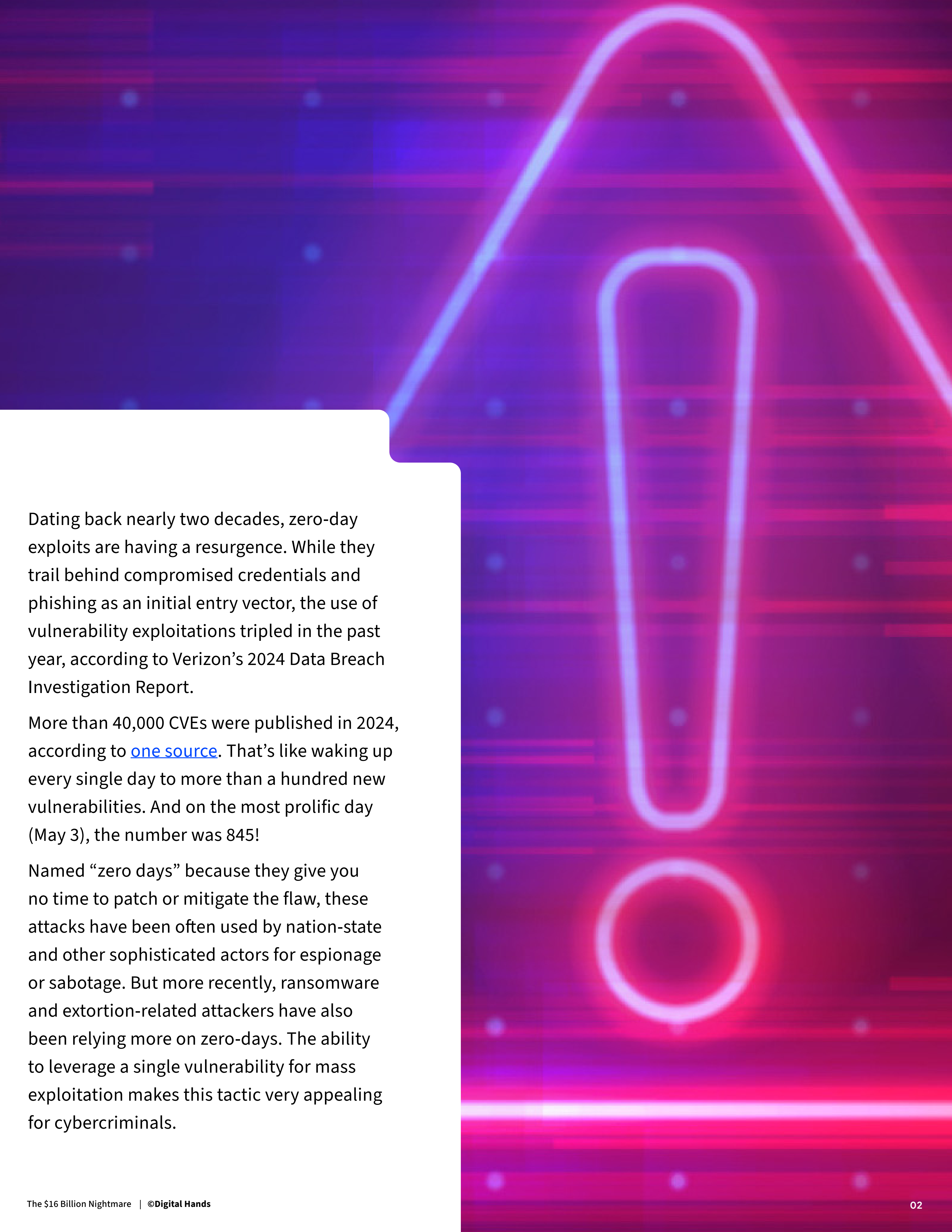
Table of Contents

Why every CISO and SOC should care about zero-days 03

How a zero-day attack may unfold 04

How to combat zero-day vulnerabilities with managed detection and response 06

Benefits of MDR beyond zero-day defense 08



Dating back nearly two decades, zero-day exploits are having a resurgence. While they trail behind compromised credentials and phishing as an initial entry vector, the use of vulnerability exploitations tripled in the past year, according to Verizon's 2024 Data Breach Investigation Report.

More than 40,000 CVEs were published in 2024, according to one source. That's like waking up every single day to more than a hundred new vulnerabilities. And on the most prolific day (May 3), the number was 845!

Named "zero days" because they give you no time to patch or mitigate the flaw, these attacks have been often used by nation-state and other sophisticated actors for espionage or sabotage. But more recently, ransomware and extortion-related attackers have also been relying more on zero-days. The ability to leverage a single vulnerability for mass exploitation makes this tactic very appealing for cybercriminals.

Why every CISO and SOC should care about zero-days

Zero-day attacks are especially damaging because the threat is immediate and the details of the exploit are sparce, as are the remediation actions. Your organization is vulnerable until the vendor issues a patch (and you take the time to apply it) — and the exploit window can be extensive.

Once they gain access inside an organization with a zero-day exploit, the adversary can execute malicious actions like exfiltrating data and escalating to advanced attacks like ransomware. Although every industry faces this threat, critical infrastructure sectors, such as manufacturing, energy, and utilities, are especially at risk due to vulnerabilities in ICS/SCADA systems.

In 2023, some security researchers observed a more than 50% increase in zero-day exploits in the wild, with the trend continuing in 2024. A potential driver behind the growth is the fact that many threat actors are now developing these exploits in-house rather than relying on shared kits.

The impact of a successful zero-day is growing (even prompting a joint advisory by several national governments in November 2024) and can be wide-reaching:

✓ The majority of the vulnerabilities that were most frequently exploited in 2023 were initially exploited as zero-days, an increase from 2022.

✓ Attacks that use zero-days take the longest to contain, an average of 69 days, giving attackers ample time for execution.

The number of victims from one campaign can be mind-boggling. Here are some of the most far-reaching examples:

- The 2023 attack on the MOVEit file-transfer platform impacted nearly 2,800 organizations and compromised the data of nearly 96 million people. Based on the estimated cost of a data breach per record at the time ($165 on average), the potential total cost to the affected organizations was just short of $16 billion.
- The 2017 WannaCry ransomware worm spread rapidly across the world, impacting more than 200,000 computers in 150 countries within 24 hours. Victims ranged from small organizations to very large ones, including FedEx and UK’s National Health Service, with total global losses estimated at $4 billion or more.
- The Heartbleed bug exploiting the ubiquitous OpenSSL cryptographic toolkit shook the internet community when it was discovered a decade ago. It impacted at least half a million websites, including heavily trafficked websites like Google, Wikipedia, and Yahoo. But the damage went far beyond web access. In one example, Heartbleed was the initial access vector in an attack on one of the largest U.S. healthcare systems, resulting in stolen data of 4.5 million patients.

How a zero-day attack may unfold

STEP 1

Discovering the vulnerability

Malicious actors use coding or a purpose-built tool to identify a previously unknown flaw in an IT resource like an application. Or they may purchase vulnerabilities from a specialized criminal underground market. Let's say they land on a memory-corruption flaw in a widely used browser, allowing them to execute malicious code.

STEP 2

Exploitation

The attackers create a malicious payload, such as malware, to exploit the vulnerability. Often times, they deploy bots or other tools to automatically scan systems affected by the vulnerability. In our scenario, they scan public-facing websites for the memory-corruption flaw to execute the arbitrary code. When an employee visits the compromised website, the malware delivers the exploit to the victim's system.

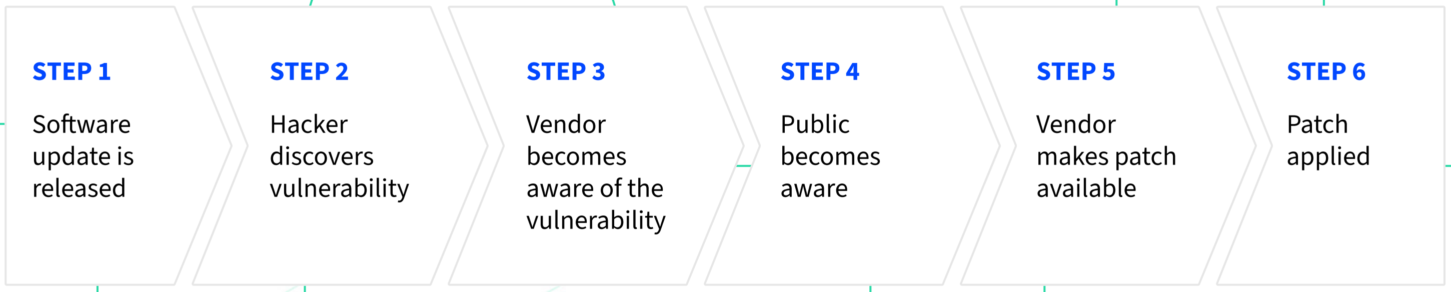
[Indented section] Attackers can also now use large language models to exploit the CVEs — feeding the publicly available CVE data into generative AI chatbots to generate new exploits nearly instantly. Which means the response window for organizations is even shorter.

STEP 3

Lateral movement and escalation

Once they have the initial access, the attackers escalate admin privileges — often by deploying more malware — and move laterally within the organization's network to carry out their objectives. In this instance, they have gained full access to the network, and they deploy ransomware to servers and endpoints across the organization.

Zero-day attack timeline



STEP 1

Software update is released

STEP 2

Hacker discovers vulnerability

STEP 3

Vendor becomes aware of the vulnerability

STEP 4

Public becomes aware

STEP 5

Vendor makes patch available

STEP 6

Patch applied

How to combat zero-day vulnerabilities with managed detection and response

Zero-days are inevitable and unavoidable as attackers are constantly on the hunt for new ways of causing as much damage as possible — and now also leveraging LLMs. But MDR can help identify anomalous behavior and contain these attacks to limit their impact, spread, and severity before patches are made available by the manufacturer. **Here's what the playbook may look like, using a combination of automated tools and human experts:**

1. Detection

The MDR's detection platform sees across multiple technologies. This breadth and depth across systems allows it to detect abnormal behaviors that single point systems may miss due to the lack of curated threat intelligence and AI capabilities. **The platform monitors communication patterns to identify anomalies such as:**

- Unauthorized privilege escalation
- Unusual traffic
- System crashes
- Memory corruption

2. Automation

The MDR's automated workflows isolate affected systems and block lateral movement, as well as quarantine files or processes that are linked to the exploit.

3. Investigation

MDR analysts analyze logs and indicators of compromise to confirm a zero-day exploit and assess the scope and impact of the attack.

4. Action

Once the software vendor releases a patch, the MDR experts guide the customer on how to prioritize vulnerability patching and remediation. The analysts collaborate with threat intelligence teams to further identify and respond to emerging exploitation. If the MDR provider manages the impacted solution, it can also help the customer implement a patch or workaround. Injecting firewall management into an MDR solution allows for additional flexibility and more robust actions because the MDR experts who are detecting and responding to the threat can directly implement the patch or workaround instead of simply letting you know about a zero-day and leaving you to fend for yourself.

Security practices you should have in place before MDR steps in

- **Defense in depth:** MDR checks this box. Nonetheless, you can't rely on a single-point solution to detect anomalous behavior, and your defenses need to go beyond one layer deep. Add as many layers as possible to identify, block, and contain attacks.
- **Principle of least privilege:** Systems and users should have the bare minimum privileges required to perform their necessary tasks. By restricting their authorizations and access to resources, you can minimize the impact if an attacker takes over the account.
- **Network segmentation:** You need the ability to shut off part of an infected network to limit access and to prevent lateral movement.

An experienced MDR partner can help you mature your security program outside of simply implementing and managing tools. An MDR provider who's a true partner will enforce best practices, ensuring you implement more rudimentary measures like the ones above to limit the impact of zero-days.

Benefits of MDR beyond zero-day defense

MDR offers much more than defense against zero-days.

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

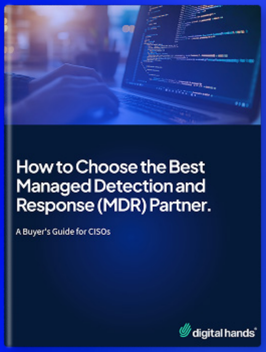
- ✓ See more — faster — to protect your environment holistically.
- ✓ Get higher-fidelity alerts and integrated, enriched telemetry.
- ✓ Improve operational efficiency while allowing you to automate your workflows based on your risk appetite.
- ✓ Decrease response time with automated containment and 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