How Can NDR Help You Detect Exploitation—and Fix Vulnerabilities Faster?

Many organizations struggle to address network security vulnerabilities in time. By the time vulnerabilities are discovered, attackers may already be exploiting them across your infrastructure, especially in areas where visibility is limited.

That delay leaves you scrambling patches get applied too late, remediation workflows are disjointed, and attackers can move laterally or exfiltrate data before containment begins. Without real-time insight into exploitation-in-progress, remediation efforts feel reactive, slow, and incomplete.

Network Detection and Response (NDR) changes the game. By continuously analyzing network traffic, correlating threat intelligence, and surfacing exploitation behavior as it unfolds, NDR dramatically accelerates your vulnerability remediation process—helping you detect, prioritize, and neutralize threats before they become breaches.

Why NDR supercharges vulnerability remediation

1. You get real-time visibility into exploitation in progress

Most vulnerability remediation processes rely on scanning and patching—but remediation only matters if attacks aren't already moving through those gaps. NDR fills that blind spot by analyzing all network traffic—north-south and east-west—and surfacing anomalies tied to exploitation behaviors like C2, lateral movement, or suspicious file transfers. When you see attack steps happening live, you can jump into containment immediately.

2. You reduce dwell time and speed up the response

Traditional remediation can lag—patches get scheduled, tickets circulate, and delays rack up. NDR reduces dwell time by integrating detection with response workflows. Analysts get immediate alerts when exploitation shows up, with context to drive action. That means remediation steps—patching, network isolation—can begin as soon as a threat is detected.

4 Keys to Automating Threat Detection, Threat Hunting and Response

- Maturing Advanced Threat Defense
- 4 Must-Do's for Advanced Threat Defense
- Automating Detection and Response

Download the Whitepaper Now!

3. You prioritize high-risk vulnerabilities based on actual exploitation

Not all vulnerabilities are equally dangerous at any given time. NDR helps you focus on those under active attack. As anomalies—like unexpected outbound connections or data exfiltration—surface, you can map them back to underlying vulnerabilities. That lets you prioritize remediation based on real-time threat presence, not just severity scores.

4. You deliver contextual analysis and threat intelligence alongside alerts

NDR platforms integrate threat intelligence feeds and metadata enrichment, giving you not just

“something is wrong” but “this behavior ties to known attack techniques or indicators.” That enriches your remediation process—by revealing exploited techniques, likely threat actors, and the specific parts of your infrastructure under attack.

5. You build better triage and remediation workflows

With NDR reducing false positives via behavioral analytics and ML, you avoid wasting time on noise. Alerts are prioritized, enriched with context, and can be integrated into automated containment or remediation sequences in SIEM, SOAR, or patch management tools—so that engineers and defenders act faster and smarter.

How you can integrate NDR into your vulnerability remediation process

1. Configure your network to support visibility—and NDR

Position NDR sensors—whether TAPs or span ports—so that all critical segments are monitored. Ensure coverage across on-prem, cloud, and hybrid networks. By ingesting raw traffic and metadata, NDR captures the full spectrum of activity needed to detect intrusion in motion.

2. Define workflows triggered by exploitation signals

Set up detection rules for behaviors linked to vulnerability exploitation—like unusual SMB traffic, C2 beaconing, or privilege escalation patterns. When these triggers fire, integrate them into your incident response and vulnerability ticketing workflows—say, by creating remediation tasks or activating automated patch/prevention rules.

3. Close the loop with risk-based vulnerability management

Use real-time exploitation detection to feed into your vulnerability management dashboards. This helps you assign higher risk scores to vulnerabilities actively being exploited, enabling more tactical patching. Over time, this feedback loop improves your prioritization and strategic patch planning.

4. Support threat hunting and retrospective analysis

After initial detection or remediation, NDR retains traffic metadata and allows querying of past sessions. That means you can hunt for evidence or validation—“***Was this vulnerability exploited before?***”—and debrief incident response to improve detection and prevention for next time.

How Fidelis NDR helps you accelerate vulnerability and threat remediation

1. Deep Session Inspection and full visibility across all network segments

FIDELIS NDR (part of Fidelis Elevate) uses Deep Session Inspection™ to reconstruct entire sessions—including encrypted traffic—and applies cyber terrain mapping to ensure full visibility. That means even when attackers are exploiting vulnerabilities within encrypted tunnels or local subnets, Elevate captures the activity in context.

2. Post-breach detection up to 9× faster

The platform's active threat detection capabilities—leveraging behavioral anomaly detection, sandboxing, and threat intelligence—enable you to detect exploitation in progress much faster than traditional tools. Customers have seen post-breach detection accelerate nearly nine-fold, enabling faster remediation.

3. Unified detection, enrichment, and response within a single interface

As part of Elevate XDR, Fidelis NDR integrates detection, sandboxing, DLP, threat intelligence, deception, and response orchestration. Alerts come enriched with context (asset risk, technique, historical behavior) and can trigger response workflows directly—letting you go from detection of exploitation to remediation without hopping between tools.

4. Terrain-based defense that highlights probable attack paths

Fidelis Network's cyber terrain mapping shines a light on your attack surface—showing not just vulnerabilities, but likely paths of exploitation. That insight guides focused on areas under active threat, enables you to patch or isolate strategically to disrupt attacker movements.

Conclusion

NDR fundamentally transforms the vulnerability remediation process. Instead of remediate-first, respond-later, you detect exploit behaviors as they unfold, enrich alerts with context, and feed remediation workflows with actionable insight—all in real time. With platforms like Fidelis Network providing deep visibility, faster detection, and unified response, you close the loop between vulnerability, threat, and remediation—saving time, reducing risk, and staying ahead of attackers.

Our Customers Detect Post-Breach Attacks over 9x Faster.

See why security teams trust Fidelis to:

- Cut threat detection time by 9x
- Simplify security operations
- Provide unmatched visibility and control

Book a Demo Now!