How Does Deep Network Visibility Elevate Your Vulnerability Management?

Every month, thousands of new vulnerabilities flood security feeds, yet many organizations still depend on quarterly scans and static inventories. That means critical flaws on shadow-IT devices or lateral-movement paths go unnoticed until it's too late. Meanwhile, your team wastes precious cycles chasing low-risk issues while genuine exploits spread unchecked. It doesn't have to be this way. By combining continuous network monitoring with an intelligence-driven, risk-based approach, you can focus efforts on the vulnerabilities that attackers actually target—shrinking exposure windows and closing gaps in real time. Fidelis Elevate's XDR platform delivers the deep visibility, threat context, and automated prioritization needed to turn vulnerability management into a proactive, data-driven cycle.

How Does Unified Detection and Analysis Accelerate Your Vulnerability Program?

When you can't see east–west traffic—or miss devices that appear and disappear—you're blind to large swaths of your network. Attackers love these blind spots, using them to probe for weaknesses and pivot laterally before any alarm sounds.

By tapping directly into your network fabric and inspecting every packet, you gain a live inventory of all connected assets and immediate insight into anomalous behavior. For example, if a newly joined IoT camera begins sending large data streams to an unknown IP, that traffic jump-starts an investigation instead of slipping past a monthly scan. Lets see how it done:

1. Real-Time Asset Discovery

Shadow IT and temporary VMs often escape scheduled scans for days. Imagine a contractor's laptop connecting overnight to critical databases—without real-time discovery, you won't know until logs are manually reviewed.

- **Questions to Consider:**
  - How quickly does your current process detect new devices on the network?
  - Are there any segments (guest Wi-Fi, test labs) that your scanners skip?
  - What automated alerts could you set when an unknown asset first appears?

Fidelis unifies network flows with endpoint telemetry, auto-profiling every device as it appears. That continuous mapping ensures your vulnerability assessments always cover the current attack surface.

Making the Shift to Detection and Response with Deep Visibility

- Rich Metadata from NTA and EDR
- Deception Defense
- Greater Visibility, Deeper Insight

Download the Whitepaper Now!

2.Contextual Prioritization at the Network Edge

Patching every high-CVSS flaw on a test server clogs your queue and distracts from real threats. When you see a specific exploit attempt—say, repeated SMB-brute forcing against an unpatched file share—you can push that patch to the top of your list.

- **Questions to Consider:**
  - Which exploit attempts would you want to automatically elevate in your remediation queue?
  - How do you currently combine CVSS scores with observed threat activity?
  - What thresholds (failed logins, unusual data transfers) indicate an active attack?

Fidelis Elevate enriches CVE data with live threat indicators and asset criticality. In practice, this means exploit traffic detected by NDR instantly elevates the associated vulnerability's urgency, so your team fixes the most dangerous flaws first.

3.Bridging Scanner and Sensor Data

Juggling separate vulnerability scan exports and IDS alerts makes it impossible to spot active exploits tied to your open CVEs.

- **Questions to Consider:**
  - How do you currently link network alerts to specific vulnerabilities?
  - What tools or scripts could automate that mapping?
  - Which roles need visibility into both scan results and live detections?

Fidelis Elevate correlates scanner results with network detections in one console. If a packet-level signature flags an attempted SQL-injection on a database known to have CVE-YYYY-ZZZZ, that item jumps to the top of your remediation dashboard—no manual cross-referencing required.

What Role Does Network Traffic Analysis Play in Risk-Based Prioritization?

Attackers often hide their probes and exploits inside encrypted tunnels or mimic normal traffic patterns, making it impossible to know which vulnerabilities they're targeting unless you inspect traffic at the packet level. Network traffic analysis shines a light on those hidden activities—decrypting streams where policy allows, parsing hundreds of metadata attributes, and applying behavioral models to spot deviations that signal an exploit in progress. This live context is the bridge from "we have a CVE here" to "we're under attack on CVE-1234 right now."

1. Decrypting and Inspecting Encrypted Streams

Encrypted payloads can conceal both malware and exploit code, effectively blinding most vulnerability scanners. By decrypting SSL/TLS sessions (or analyzing metadata where decryption isn't feasible), network analysis reveals hidden threats—whether it's a PowerShell command embedded in a PDF or an unusual file transfer to an unknown IP.

- **Fidelis Elevate in Action:**
  Fidelis Elevate integrates with your decryption infrastructure and applies deep-packet inspection across all decrypted traffic. The moment a suspicious payload emerges, it's flagged, tied back to the host's vulnerability profile, and elevated in your remediation queue.

2. Spotting Novel Attack Patterns

Zero-day exploits leave no signatures, but they do produce abnormal behaviors—strange protocol sequences, unexpected data volumes, or out-of-pattern connections.
Imagine seeing a printer suddenly initiate large outbound connections on port 8443; that anomaly may indicate an attacker pivoting through an overlooked device.
Network analysis baselines your normal traffic and applies ML-driven anomaly detection to catch these subtle signs.

- **Fidelis Elevate in Action:**
  Fidelis Elevate's behavioral analytics engine continuously learns your environment's

“normal” and fires high-confidence alerts when deviations occur. Each anomaly is immediately cross-referenced with the device’s known CVEs, so you see not just “something odd happened,” but “this oddity targets CVE-YYYY-ZZZZ.”

3. Correlating Alerts with Vulnerability Data

Without correlation, IDS alerts and vulnerability scan reports live in separate silos—forcing manual lookups that slow your response. For instance, if your IDS flags an SQL-injection attempt on a database and your scan shows CVE-YYYY-AAAA applies, you instantly know that patch moves to the top of the queue.

Network traffic analysis arms you with real-time mappings of alerts to known CVEs, showing exactly which vulnerabilities are under active probing.

- **Fidelis Elevate in Action:**
  Elevate enriches every network detection with CVE identifiers and asset criticality. An exploit signature on an unpatched database server automatically surfaces as a top remediation ticket—no Excel gymnastics required.

Don’t let threats go unnoticed. See how Fidelis Elevate® helps you:

- Identify and neutralize threats faster
- Gain full visibility across your attack surface
- Automate security operations for efficiency

Download Datasheet

How Does Continuous Monitoring Transform Remediation Workflows?

Batch-driven patch cycles leave unacceptable windows for attackers to strike. Continuous network monitoring changes the game by delivering up-to-the-second visibility into both vulnerability scans and live exploit attempts. That real-time feed powers an automated, closed-loop remediation process—detect, prioritize, patch, verify—so your team moves at the speed of threat.

1. Instant, High-Fidelity Alerts

By inspecting traffic live, you catch exploit attempts the moment they happen—whether it's a SQL-injection probe or a brute-force login. This precision eliminates days of low-priority noise and directs attention to the vulnerabilities being targeted right now.

- **What to Do:**
  - Define high-value asset groups (databases, public APIs, domain controllers).
  - Tune alert thresholds to suppress benign deviations.
  - Map alerts to your CVE inventory so each notification includes vulnerability context.

2.Automated Patch Orchestration

Real-time detection is only half the battle—you need to remediate instantly. Continuous monitoring can trigger patch workflows the moment a high-risk vulnerability is exploited, bypassing manual handoffs.

- **What to Do:**
  - Integrate Fidelis Elevate with your patch-management platform (e.g., WSUS, SCCM, Jamf).
  - Define rollback procedures and validation checks for different asset types.
  - Establish SLAs for emergency vs scheduled patch deployments.

3.Verification and Audit-Ready Reporting

Remediation isn’t complete until you confirm exploit traffic has stopped and patches applied correctly. Continuous traffic analysis lets you verify success in real time—and generate compliance reports on the spot.

- **What to Do:**
  - Confirm no repeat exploit signatures on remediated hosts.
  - Verify patch installation via endpoint inventory.
  - Generate compliance documentation showing time-stamped detection, remediation, and verification events.

Fidelis Elevate offers a strong solution for defending against cyber threats, combining machine learning for threat detection, detailed monitoring, and automatic responses to safeguard against new threats. Features such as Deep Session Inspection®, support for cloud-based systems are present. For businesses looking for a defense strategy that adapts to changing threats, Fidelis Elevate is a perfect option.

By providing layered security and complete network protection, Fidelis Elevate helps organizations prevent complex cyberattacks while maintaining regulatory compliance.