NDAY Security, an NVIDIA Inception member, enhances exploitability products with CrowdFense vulnerability intelligence

NVIDIA Inception Program's NDAY Security Enhances Exploitability Products with CrowdFense Vulnerability Intelligence

MIAMI, FL, UNITED STATES, March 10, 2026 /EINPresswire.com/ -- NDAY Security (“NDAY”), the AI-powered offensive security company and NVIDIA Inception Program member behind the AttackN continuous exploitability platform, today announced a strategic partnership with Crowdfense, the world-leading vulnerability research hub and acquisition platform. Under the agreement, Crowdfense’s curated N-Day Vulnerability Feed, delivering weaponized exploits and deep technical analysis for high-risk, actively exploited vulnerabilities, will be integrated directly into NDAY’s proprietary platform and its autonomous penetration testing agent, AttackBench.

The partnership enhances NDAY’s proprietary continuous exploitability platform and Agent with elite, real-world vetted vulnerability intelligence from Crowdfense’s research team, the same caliber of exploit intelligence leveraged by Advanced Persistent Threat (APT) groups and nation-state operators. For the first time, defenders gain access to the same weaponized insight adversaries use to breach enterprises, giving security teams the ability to validate their defenses before attackers strike.

Crowdfense Intelligence Meets NDAY’s Continuous Exploitability Engine

Security teams face a critical challenge: while threat intelligence reveals what adversaries are exploiting, traditional testing cycles are too slow to validate defenses against rapidly evolving threats. Point-in-time assessments leave organizations blind to newly disclosed vulnerabilities for weeks or months, and attackers know it.

NDAY's continuous exploitability platform and Agent was built to eliminate that gap. Now, with direct integration of Crowdfense's curated feed of root cause analyses and fully weaponized exploits covering vulnerabilities from leading vendors including Microsoft, Google, Adobe, Fortinet, Ivanti, and Juniper, many of which are listed in the CISA Known Exploited Vulnerabilities (KEV) catalog, the platform gains an unmatched offensive intelligence layer.

This enables NDAY and Crowdfense customers to:

• Automatically simulate active threat campaigns using real-world exploits, not theoretical proof-of-concepts
• Prioritize patching based on demonstrated exploitability rather than CVSS scores alone
• Validate detection and response capabilities against weaponized exploits at machine speed
• Accelerate high-confidence vulnerability triage across the entire attack surface
• Assess true operational risk within a controlled, compliant, and governance-led framework

How It Works: From Disclosure to Validated Defense in Minutes

NDAY's continuous exploitability platform, now enhanced with Crowdfense intelligence, turns vulnerability disclosure into validated defense at machine speed. Here's what that looks like in practice:

Example: A critical vulnerability affecting a major enterprise platform is publicly disclosed. Within hours, NDAY's platform identifies the vulnerability across a customer's environment through DiscoverN. AttackBench, NDAY's autonomous AI agent, then leverages Crowdfense's proprietary N-Day data feed to safely execute the real-world exploit within NDAY's controlled testing environment. The exploit is never exposed to the open internet, never shared publicly, and never leaves the secure platform.

Within minutes, the customer receives a validated, non-public assessment confirming whether their systems are truly exploitable, not based on a CVSS score or a theoretical proof-of-concept, but on the actual weaponized exploit that APT groups are using in the wild.
Both Crowdfense and NDAY maintain strict safeguards throughout this process. Crowdfense's proprietary exploit data remains protected within NDAY's controlled infrastructure, ensuring responsible handling of sensitive offensive intelligence. The result: customers receive unique, non-public findings that no scanner, no CVSS feed, and no traditional pen test can replicate, the ground truth of whether an attacker could breach their environment today.
Redefining Penetration Testing and Vulnerability Management

Traditional penetration testing delivers a point-in-time snapshot that is outdated the moment it's complete. Conventional vulnerability management tools generate thousands of alerts ranked by CVSS scores, with no proof of actual exploitability. NDAY's platform and Agent, now add an optional layer powered by Crowdfense intelligence, fundamentally changes both disciplines:
• Penetration testing becomes continuous, autonomous, and fueled by the same weaponized

exploits APT groups deploy, not recycled public proof-of-concepts
• Vulnerability management shifts from theoretical severity scoring to validated exploitability, enabling security teams to prioritize the vulnerabilities that attackers can actually use today
• Organizations move from reactive patching cycles to proactive, intelligence-driven defense, closing the gap between disclosure and validated remediation

What the Leaders Are Saying

“Crowdfense has built the industry’s most comprehensive pipeline of high-impact vulnerability intelligence. By integrating our N-Day Feed into NDAY’s proprietary continuous exploitability platform and AttackBench agent, we’re transforming static intelligence into dynamic, continuous security validation. NDAY’s customers can now test their resilience against the same exploits APTs are weaponizing in the wild, automatically and at scale.”

— Paolo Stagno, Director of Research, Crowdfense

“Criminal and geopolitical threat actors are using artificial intelligence to exploit business vulnerabilities faster across all industries. NDAY’s technology, combined with advanced exploits at CrowdFense, enables security teams to test their defences more quickly and effectively than manual methods allow.

— Kory Daniels, Chief Security and Trust Officer, LevelBlue

Availability

Crowdfense N-Day Feed integration within NDAY’s continuous exploitability platform will be available to select customers beginning Q2 2026. Organizations interested in early access can contact NDAY Security or Crowdfense directly.

About Crowdfense

Crowdfense is the world-leading vulnerability research hub and acquisition platform for high-quality zero-day exploits and advanced vulnerability research. Through its Exploit Acquisition Program and Vulnerability Research Hub (VRH), Crowdfense connects independent researchers with vetted institutional clients, delivering strategic cyber capabilities with the highest bounties in the industry. The N-Day Vulnerability Feed provides real-time exploits and technical analysis for high-risk vulnerabilities actively abused in the wild.

www.crowdfense.com

About NDAY Security

NDAY Security provides continuous exploitability platforms designed to identify critical

vulnerabilities in seconds. NDAY is an NVIDIA Inception Program member and is available through Carahsoft, SHI, Spry Methods, among others for federal, DoD, state, local, and education procurement.
www.ndaysecurity.com

PR
NDAY Security, Inc.
inbound@ndaysecurity.com
Visit us on social media:
LinkedIn
