NVIDIA Inception Member NDAY Security Breaks Cybersecurity Cost Barriers with Fixed-Cost AI Vulnerability Exploit Engine

Nvidia Inception startup Nday launches Valadin, an automated fixed-cost exploit validation engine designed to cut unpredictable cybersecurity testing costs.

AI Penetration Testing

MIAMI, FL, UNITED STATES, July 29, 2026 /EINPresswire.com/ -- NDAY Security today announced the launch of VALADIN, a fixed-cost CVE validation platform built to help security teams determine which vulnerability scanner findings represent real, exploitable risk. Designed for enterprise environments, VALADIN ingests findings from third-party vulnerability scanners, applies controlled offensive-security validation, and returns evidence-backed verdicts that help organizations prioritize remediation with greater confidence.

Security teams are under constant pressure to reduce risk while managing increasingly large volumes of vulnerability data. Traditional scanners are essential for identifying potential weaknesses, but they often produce long lists of findings that still require human interpretation. Severity scores, signatures, and detection logic can indicate that a vulnerability may exist, yet they do not always prove that exploitation is possible in the customer's specific environment.

VALADIN addresses that gap by validating exploitability rather than relying solely on scanner output. The platform converts third-party findings into clear outcomes, including Exploitable, Not Exploitable, Inconclusive, and Not Testable. Each result can include supporting evidence, testing details, timestamps, and audit history, giving security teams a defensible record of what was tested and why a particular verdict was reached.

“Security teams do not need another dashboard that tells them what might be wrong,” said Mark Whitehead, CEO of NDAY Security. “They need to know what an attacker can actually use. VALADIN was built to take the output organizations already have, validate it safely and consistently, and turn vulnerability noise into actionable knowledge. The goal is simple: stop guessing and start knowing.”

VALADIN supports common third-party vulnerability data formats, including Nessus XML, Burp XML, OpenVAS or Greenbone XML, and compatible CSV exports. After a report is uploaded, the platform parses and normalizes the findings, allows authorized users to review targets, and then runs validation based on the approved level of intrusiveness.

Customers can select validation settings aligned to their environment and risk tolerance. Safe validation is designed for minimum-impact proof, Standard validation permits active but reversible exploitation to confirm impact, and Aggressive validation allows broader permitted testing where appropriate. Destructive activities such as denial of service, data destruction, exfiltration, or lateral movement are not included in standard validation workflows.

The platform is designed to combine automation with operational control. VALADIN supports multi-user access, programmatic access through APIs, MCP, and tokens, configurable parallel validations, and automatic retries for inconclusive results. These capabilities allow enterprises, managed security service providers, and security teams to integrate validation into existing vulnerability management, ticketing, reporting, and remediation processes.

A central results dashboard provides a summarized view of validation posture across active reports. Security teams can filter findings by verdict, severity, host, port, vulnerability, or report, and then drill into supporting evidence. Evidence can include the validation summary, method used, confidence level, technical output, and downloadable files.

VALADIN also maintains a full audit trail across approvals, validations, reports, evidence access, configuration changes, and system events. This gives organizations a documented history of how findings were handled and supports internal governance, risk, compliance, and third-party assurance requirements.

The launch reflects NDAY Security’s broader focus on exploitability across infrastructure, applications, APIs, cloud environments, and AI systems. Rather than requiring customers to replace their existing scanners, VALADIN adds an independent validation layer to the security investments they already use.

VALADIN can be used as a standalone validation capability or incorporated into broader managed security and assessment programs. Organizations can evaluate individual applications, subsidiaries, business units, or large portions of the attack surface while maintaining centralized visibility. Partners and MSSPs can also use the platform to deliver consistent validation services across multiple customers, helping standardize evidence, reduce operational variability, and

support repeatable reporting without removing the experienced testers who provide judgment, context, and consultative guidance.

“Different organizations require different approaches to enterprise security,” Whitehead added. “ATTACKN is built for companies ready to move beyond the limitations of traditional vulnerability management, while VALADIN works alongside existing scanners, exposure platforms, and security operations to validate findings, improve prioritization, and minimize disruption.”

Predictable pricing is a central part of the platform’s positioning. Manual validation is currently purchased through consulting projects, individual penetration tests, or variable cost AI models that can be difficult to forecast at scale. VALADIN is designed to provide fixed-cost CVE validation, enabling organizations to build repeatable validation programs without unpredictable per-finding fees.

The platform also applies OSCP-level AI penetration testing techniques to help reproduce and validate reported weaknesses under authorized conditions. By pairing automated offensive-security methods with customer-defined controls, evidence capture, and auditability, VALADIN is intended to provide a scalable bridge between vulnerability detection and penetration testing.

For enterprise security leaders, the result is a more focused remediation process. Confirmed exploitable findings can be escalated quickly, while unvalidated or non-exploitable findings can be handled with appropriate context. This helps security teams use limited time more effectively, communicate risk more clearly to executives and business owners, and demonstrate measurable progress against real attack paths.

VALADIN is available for enterprise customers and partners seeking API-first integration, scalable validation, predictable fixed-cost pricing, and third-party de-risking. NDAY Security will provide demonstrations and scoping discussions for organizations evaluating how validation can fit into their existing vulnerability management and continuous threat exposure management programs.

NDAY Security is a member of the NVIDIA Inception Program, which supports companies advancing AI and accelerated computing technologies. VALADIN is powered by NDAY Security’s offensive-security expertise and is designed to work alongside experienced penetration testers, security teams, and existing enterprise platforms.

To request a demonstration or learn more about VALADIN, visit ndaysecurity.com/contact.

About NDAY Security

NDAY Security develops AI-driven offensive-security platforms and services that help organizations identify, validate, and reduce cyber risk. Its capabilities span vulnerability and exposure management, penetration testing, AI-assisted offensive security, third-party validation,

and continuous security testing. NDAY Security focuses on helping customers move beyond theoretical risk by identifying what is reachable, exploitable, and meaningful to the business.

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