NIGHTWING

CYBER VULNERABILITY ASSESSMENT (CVA)

STAY AHEAD OF EVOLVING CYBER THREATS

Cyber threats are evolving, with nation-state actors increasingly exploiting zero-day vulnerabilities — unknown flaws that remain undetected until exploited. These vulnerabilities pose significant risks to mission-critical systems.

OVERVIEW

Nightwing's CVA services proactively identify and mitigate these hidden vulnerabilities using advanced tactics, techniques, and procedures (TTPs). Unlike traditional penetration testing, our approach uncovers critical vulnerabilities in both custom and third-party code, preventing exploitation before attackers can act.

NEED FOR CYBER VULNERABILITY ASSESSMENTS

In February 2022, Russian-linked hackers exploited a misconfigured VPN to deploy Acid Rain malware on Viasat's KA-SAT network, disrupting thousands of modems. In November 2023, the IRGC-affiliated "Cyber Av3ngers" targeted Unitronics PLCs, forcing a Pennsylvania water facility to operate manually. These incidents, along with the Volt Typhoon campaign—linked to China and targeting U.S. critical infrastructure since mid-2023—highlight the growing frequency and sophistication of cyber threats, especially from nation-state actors.

Many of these attacks exploit zero-day vulnerabilities. Unlike known vulnerabilities, zero-days are undetectable until exploited, leaving systems highly vulnerable. Nation-state actors have the expertise to find and exploit these flaws, often bypassing conventional defenses like automated scanners or red team efforts.

To protect mission-critical systems, it's essential to prioritize proactive cyber vulnerability assessments focused on identifying and mitigating these unknown, hard-to-detect threats before they can be exploited.

KEY CAPABILITIES

- **Comprehensive Attack Surface Analysis:** Emphasizes false-positive reduction to identify real vulnerabilities accurately.
- **Customized Trust Models & Attack Vectors:** Prioritizes attack vectors for focused vulnerability research.
- **Zero-Day Vulnerability Research:** Leverages nation-state-level VR expertise to uncover hidden flaws & develop proof-of-concept exploits for real-world simulations.
- **Iterative System Reassessment:** Continuously tests systems based on new threats and mitigations.
- **Actionable Remediation Recommendations:** Provides practical strategies to address vulnerabilities and strengthen defenses.

CVA

HOW IT WORKS

PHASE 1

System Security Consultation & Environment Setup

- Assess system architecture, dependencies, and security posture.
- Configure a realistic test environment (physical, virtual, or hybrid).
- Define safe testing parameters for development and production systems.

PHASE 2

Top-Level Threat Assessment

- Identify OS vulnerabilities, misconfigurations, and access control risks.
- Perform CVE analysis and evaluate firewall/network security.
- Establish a threat profile and document findings.

PHASE 3

In-Depth Threat Assessment

- Conduct advanced vulnerability research on key system components.
- Use static/dynamic analysis, reverse engineering, and fuzz testing.
- Re-test mitigations and continuously update findings.

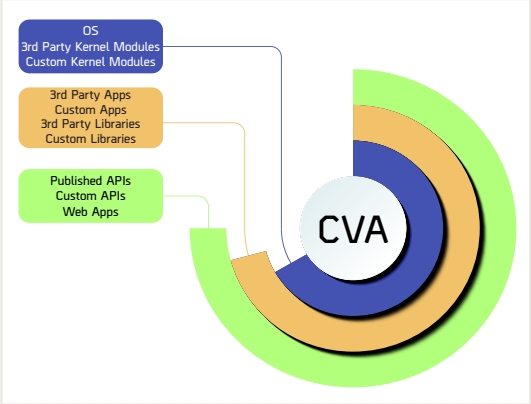
PHASE 4

Component Reassessment

- Reassess select components for new vulnerabilities or regressions.
- Validate prior fixes and detect security gaps from updates.
- Maintain long-term resilience through ongoing analysis.

THE NIGHTWING CVA SOLUTION

Nightwing's CVA services identify and mitigate zero-day vulnerabilities by applying advanced adversarial TTPs to prevent exploitation before attackers can act. Unlike traditional penetration testing or red teaming, which focus higher in the tech stack (e.g., APIs, Web Apps), Nightwing's CVA leverages nation-state-level vulnerability research expertise to uncover critical flaws across all layers, including custom applications and kernel modules—areas often overlooked by conventional security assessments.



As an industry leader in vulnerability research, Nightwing has discovered and identified over 1,000 zero-day vulnerabilities across a range of systems. Our proprietary static and dynamic analysis tools, combined with the expertise of our elite vulnerability researchers, reverse engineers, and systems internals specialists, enable us to go beyond surface-level scanning. We apply advanced techniques like reverse engineering and custom fuzz testing to expose deeply embedded vulnerabilities that automated tools and traditional assessments fail to detect.

Identifying vulnerabilities is only part of the solution. We take an active role in helping customers mitigate risk by providing direct remediation guidance, validation testing, and full-component reassessments. Our process ensures that fixes are both effective and secure, while continuously adapting to emerging threats—delivering a persistent, proactive approach to system resilience.

Contact
Nightwing
1220 N Hwy A1A, Suite 123
Indialantic, FL 32903
cyber-Resiliency@nightwing.com

nightwing.com

NIGHTWING