NIGHTWING

CYBER VULNERABILITY ASSESSMENT (CVA)

CVA

EVERY SPACE MISSION DEPENDS ON UNSEEN RELIABILITY. NIGHTWING ENSURES IT.

Cyber risk in space and missile defense is persistent, asymmetric, and accelerating. Nightwing proactively identifies hidden vulnerabilities so space architectures work when it matters.

OVERVIEW

Nightwing's CVA for Space provides proactive security and mitigates vulnerabilities using advanced tactics, techniques, and procedures (TTPs). Unlike traditional penetration testing, our approach uncovers critical vulnerabilities in both custom and third-party code for terrestrial, launch, and orbital systems, preventing exploitation before attackers can act. The offense always has an asymmetric advantage – NW capabilities can change the equation

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 Iranian Islamic Revolutionary Guard Corps (IRGC)-affiliated "Cyber Av3ngers" targeted Unitronics PLCs, forcing a Pennsylvania water facility to operate manually. And 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, flaws unknown to the vendor and for which there is no defense. Nation-state actors have the expertise and resources to find and exploit these flaws, often bypassing conventional defenses.

KEY CAPABILITIES

- **Comprehensive Attack Surface Analysis:** Emphasizes false-positive reduction to identify real vulnerabilities accurately for systems across launch, satellite, and ground control architectures.
- **Customized Trust Models & Attack Vectors:** Prioritizes attack vectors for focused vulnerability research.
- **Zero-Day Vulnerability Research:** Leverages nation-state-level vulnerability research 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 before deployment.

Our most innovative technologies only matter when they work in highly contested environments. To protect mission-critical space and missile defense systems, it's essential to conduct proactive cyber vulnerability assessments and identify threats before they can be exploited.

CVA

HOW IT WORKS

CONSULTATION | THREAT ASSESSMENT | ADVANCED TESTING | REASSESSMENT

Initial Consultation

- Decompose the target architecture into manageable systems for analysis and perform initial risk analysis.
- Outcome: A tailored assessment plan and initial risk report.

Top-Level Threat Assessment

- Evaluate the top-level security posture of each system identified during consultation.
- Outcome: A System Threat Assessment Report detailing findings and risks.

In-Depth Threat Assessment

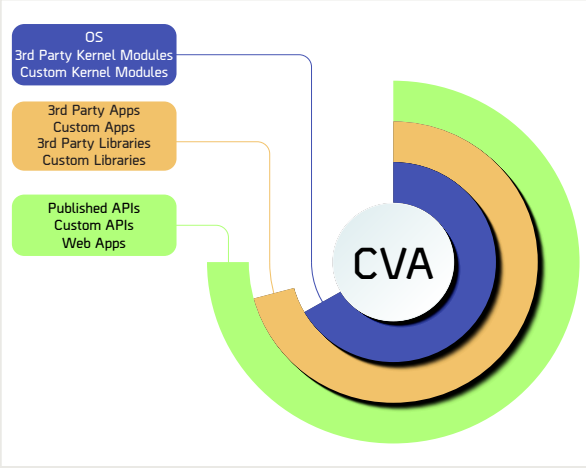
- Perform advanced testing to uncover deeper vulnerabilities in proprietary applications and system components.
- Outcome: Updated System Threat Assessment Report with detailed findings and remediation guidance.

Reassessment

- Validate prior fixes and ensure resilience against emerging threats.
- Outcome: A refreshed assessment report and recommendations for ongoing security improvements.

THE NIGHTWING CVA SOLUTION

Nightwing's CVA service finds and mitigates vulnerabilities in space and missile defense architectures 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 assessments.



As an industry leader in vulnerability research, Nightwing has discovered over 1,000 zero-day vulnerabilities across a range of systems, including critical space assets. 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 far beyond the competition's 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 mitigating 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.

As space becomes increasingly congested and contested, only a full-spectrum cyber approach can ensure the services that we depend on daily. **If your architecture hasn't been tested against unknown threats, it's already exposed.**

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

NIGHTWING