## Meet the Team

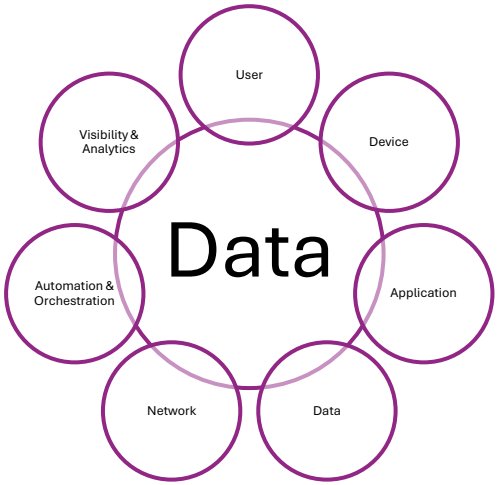
Offensive Team: Simulates attacker Tactics, Techniques, and Procedures (TTPs) to test specific defenses.

Defensive Team: Evaluates defensive posture of system and System Defenders through technical and non-technical evaluation.

System Defenders: Monitor system security tools, detects threats, and execute defensive actions.

White Team: Neutral control group that manages the evaluation, sets the rules of engagement, and ensures the assessment objectives are met.

The "Purple" Team: The fusion of Offensive and Defensive teams, collaborating to achieve a unified defensive goal.




## Cybersecurity Assessment Request Process

Requests can be submitted at any time. Preferably, the assessment date should be at least 120 days in the future to ensure sufficient time for planning and securing contract support. If the request is within 120 days, requests will be evaluated based on availability and priority. If exact dates are unknown, an anticipated month/quarter/FY can be provided.

346 CTES / Plans:
DSN: (312) 945-3130
Comm: (210) 925-3130
E-mail: 346ctes.plans_all@us.af.mil

https://go.mil/epot42hm4d (.mil only)
Select 'Test Request'

# Zero Trust Cybersecurity Assessment

**Collaborate | Defend | Secure**

# 346th Cyberspace Test and Evaluation Squadron

Joint Base San Antonio-Lackland, Texas

A virtual copy is available via QR code →

## What is a Zero Trust Cybersecurity Assessment?

A Zero Trust Cybersecurity Assessment is a collaborative cybersecurity evaluation designed to test, measure, and improve Zero Trust security controls.

## Key Benefits of a Zero Trust Cybersecurity Assessment

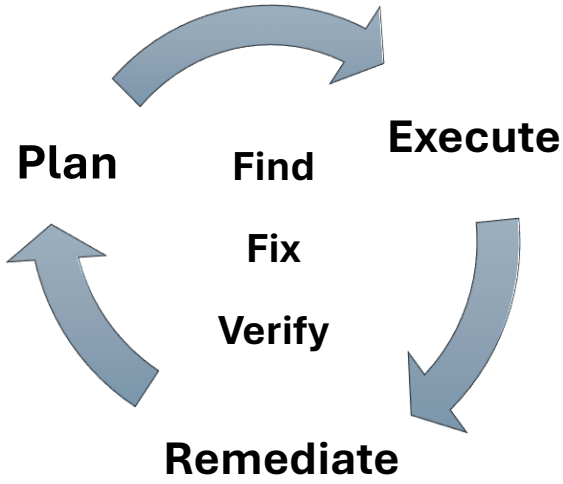
- ✓ Enhanced Security Posture: Directly validate and harden Zero Trust architectures.
- ✓ Improved System Defender Skills: Provide defensive teams with hands-on experience detecting real-world attack techniques.
- ✓ Rapid Remediation: Move from vulnerability discovery to a validated fix in hours, not weeks.
- ✓ Data-Driven Validation Replace assumptions about security with measurable proof of defensive capabilities.
- ✓ Increased ROI: Maximize the effectiveness of security tools and personnel through continuous tuning and improvement.

## Beyond Adversary vs. Defender: The Power of Collaboration

In a traditional security test, Offensive and Defensive Teams operate separately to see who "wins". The most critical vulnerabilities in the system architecture are identified. Ultimately when it comes to security, there is no winner if problems are only detected. Organizations need *solutions*.

A Zero Trust Cybersecurity Assessment transforms the dynamic from a competition into a live-fire, collaborative engagement.

Fusing offensive and defensive capabilities into a single, cohesive unit, the "Purple" Team, working together in real-time accelerates the pace toward achieving a secure architecture.




## Our Collaborative Approach

Plan & Prepare: Identify critical assets and define specific test scenarios based on known adversary tactics.

Execute & Collaborate: Offensive Team simulates an attack while the Defensive Team works with the System Defenders to detect and respond. All teams are in constant communication to analyze outcomes.

Remediate & Re-test: Detect issues and assist in remediation. Teams work together to implement solutions and immediately re-run tests to validate the fix, providing evidence of secure posturing.