SECURE THE ASSETS NEUTRALIZE THE THREATS

CASE STUDY

U.S. Air Force - Defensive Applications and Network Support (DANS) Contract

Technica™

USAF DEFENSIVE APPLICATIONS AND NETWORK SUPPORT (DANS)

The Air Force Life Cycle Management Center, Defensive Cyberspace Operations Branch (AFLCMC/HNCD) envisioned a capability to identify, characterize, and mitigate cyberspace threats impacting critical operational capabilities within USAF and DoD networks. The Defensive Applications and Network Support (DANS) contract resulted from the combination of three disparate contracts: Maintenance System Support (MSS), Defensive Cyber System Engineering (DCSE), and Defensive Cyber Information Assurance and Network Support (DCIANS).
DANS was tasked to engineer, build, develop, field, and sustain the Cyberspace Vulnerability Assessment/Hunter (CVA/H) Weapon System.

THE CHALLENGE

Development, integration, and sustainment teams supporting the weapon system were not integrated and were slow to deliver new capabilities to CPTs and MDTs. The system was operating under an interim authority to operate (ATO) and training and support services were hindered by unclear delineation of responsibility and accountability among multiple support contracts.

TECHNICA SOLUTION

Three previously independent contracts were merged into the Defensive Applications and Network Support (DANS) contract, and DANS was tasked with engineering, building, developing, fielding, and sustaining the Cyberspace Vulnerability Assessment/ Hunter (CVA/H) Weapon System. Within this unified work structure, Technica instituted DevSecOps practices and improvements to integration and service management processes.

SECURE THE ASSET, NEUTRALIZE THE THREAT

Technica's CVA/Hunter DANS program comprises over 150 matrixed team members operating across seven cross-functional areas; development, systems integration, testing, training, engineering, and architecture hubs, integrated with 24/7/365 service desk operations and on-site support. The program is complemented by information assurance teams staff focused on implementing and supporting complex network and computer monitoring and data analysis needs.

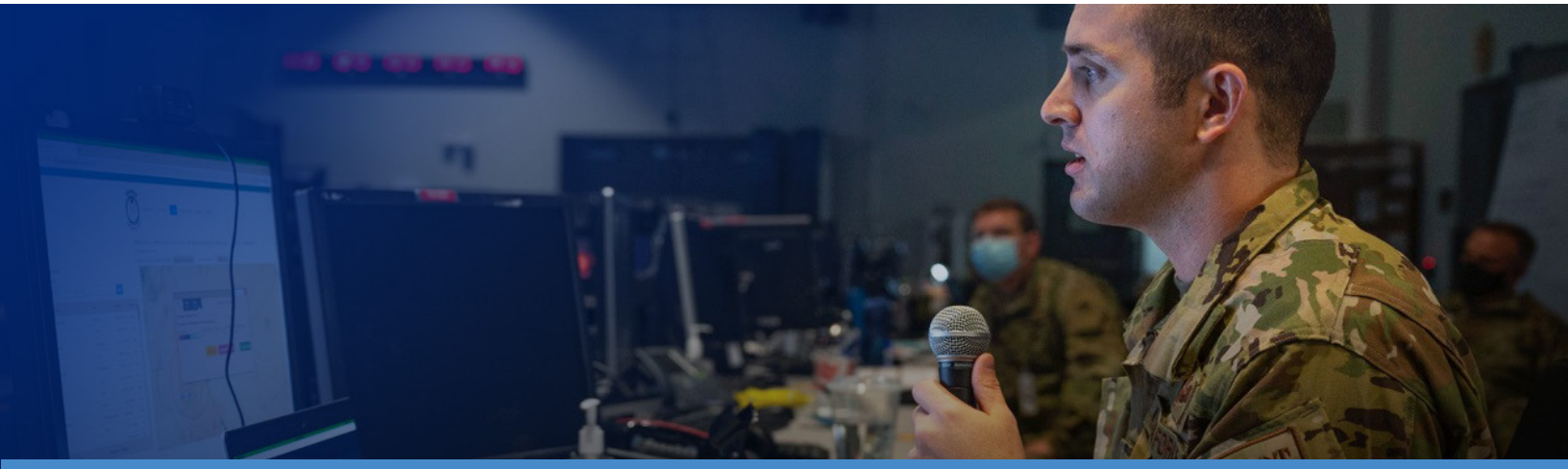
CONTRACT MISSION

The DANS mission is to provide the Air Force Cyber Command and Combatant Commanders with mobile precision protection capabilities to identify, pursue and mitigate cyberspace threats in DoD and USAF networks.
The mission is enabled by the CVA-H weapon system. CVA-H is supported by Technica through a DevSecOps paradigm that provides:

- Facilitation of threat hunting
- Support for forensic analysis
- Survey of the cyber terrain: wired, wireless and analog networks
- Identification of Advanced Persistent Threats (APTs)
- Assistance in the development of remediation plans
- Verification that threats have been neutralized or eliminated

CVA-H instances are configured in accordance with mission specifications and requirements from Cyber Protection Teams (CPTs) and Mission Defence Teams (MDTs) and are delivered for their use in three variants:

- Garrison Interceptor Platform (GIP)
- Deployable Interceptor Platform (DIP)
- Mobile Interceptor Platform (MIP)



IMPROVED SYSTEMS INTEGRATION CAPABILITIES AND PROCESSES

Technica's Systems Integration Lab (SIL) provides infrastructure and tools to manage the planning, development, testing, and deployment processes for the CVA/H weapon system. The lab is co-located with the CVA/H development teams to facilitate communication and collaboration, improving the overall quality and speed of delivery.

The SIL team and facilities provide:

- Automated processes throughout the CI/CD pipeline that streamline development and testing of simultaneous virtual environments and weapon system configurations going from manually run hashing algorithms after testing to a total of 7 hours.
- Automation of builds for mission kits and ability to image several hard drives simultaneously. This reduced the time to image a DIP/MIP from 1.5 days to 3 hours and building a hard drive from 3 days to 8 hours.
- Improved reliability and reduced rework speed delivery of certified software releases. Code defects detected by external user acceptance testing has been reduced by 90%.

IMPLEMENTATION OF SAFE AGILE DEVSECOPS

Technica focused on implementing DevSecOps practices to eliminate the confusion and conflict between teams that were slowing delivery and introducing vulnerabilities into the final products. Previously there was a cultural divide between focusing on features and functionality vs mitigating cyber risk. A successful cultural shift to accept the new paradigm with shared goals, metrics, and targets has transformed the way product, development, operations, and security teams work together, with collaboration throughout the software delivery lifecycle. The adoption of continuous integration/delivery models has integrated the development, testing, and deployment cycles to deliver new features faster and with fewer bugs and security flaws.

Occurs from the CVA/H platform within a DevSecOps paradigm:

- Survey of the cyber terrain
- Wired Ethernet Networks
- Wi-Fi Networks
- Analog Telephone Networks
- Supports forensic analysis efforts
- Facilitation of Threat Hunting
- Enables the identification of Advanced Persistent Threats
- Assistance in the development of remediation plans
- Verification that threats have been removed or neutralized

During the first year, the DANS program:

- Established a new central facility housing many government PMO members as well as development, integration, and support teams
- Recruited new leadership
- Merged new talent with the legacy team to infuse new thinking with valued system experience
- Transformed a Waterfall culture to a DevSecOps culture
- Implemented Continuous Integration/Continuous Delivery (CI/CD) pipeline
- Created cross-functional teams that removed silos between operators, developers, testers, and security personnel
- Met NIST 800-53 compliance hurdles
- Obtained 2 Year ATO – the first in program history by understanding and following the processes and requirements to navigate to success
- Delivered three complete software releases in the first nine months: 10x faster than the previous program

FUNCTIONAL PROGRAM OVERVIEW

CORE SERVICES
- Virtual Infrastructure
- Core Services (AD, DNS, DHCP, WDS, WSUS, DPS, ACAS, NMS, SQL/DR)
- Network Infrastructure
- Firewall

SYSTEMS INTEGRATION
- Integration Testing
- Virtual MIP/DIP/GIP Kits
- Contractor Testing
- Physical MIP/DIP/GIP Kits
- Breaking Point
- Small Form Factor (SFF)
- Hardware Integration

DEVELOPMENT
- CI/CD Pipeline (GitLabs)
- Peer Review
- Unit Testing
- Endgame
- Static Code Analysis (SonarQube)
- Virtual MIP/DIP/GIP Kits

ENGINEERING & ARCHITECTURE
- Virtual Environment
- Virtual MIP/DIP/GIP

TESTING RANGE
- Breaking Point
- Verodin (Malware Simulator)
- Physical MIP/DIP/GIP
- Virtual Bases
- Security Onion
- Support Development Testing (DT)

TRAINING RANGE
- Type-1 Training
- VTE
- Physical DIP Kit

SERVICE DESK
- Virtual DIP Kit
- Physical DIP Kit

OPEN-SOURCE SOFTWARE & COMMERCIAL TOOLS

- Zeke
- Moloch
- Suricata
- Kubernetes
- Gitlab Runner
- Elastic
- Wireshark
- VMware

These achievements enabled Technica to deliver three complete software releases to the PMO within the first nine months. Contrasted with the previous program's record of three years for one release, Technica increased the delivery speed by a factor of ten, shortening the time from idea to production.

SERVICE MANAGEMENT SOLUTION IMPLEMENTATION

Technica's wholistic implementation of IT Service Management processes has reduced third-tier support. The development team is now required for less than 5% of all trouble tickets. Using ServiceNow modules, common trouble tickets are transformed into Knowledge Articles that promote shared learning and faster time to resolution. In addition, Technica's service desk is trained in installing the kits, and this hands-on knowledge is a key enabler for problem resolution. Technica performs Level 1 service management for all DCO weapon systems (AF Cyber Defense, Cyber Defense Analysis, ELICSAR).

IMPROVED TEST AND TRAINING FUNCTIONS

CVA/H operators drive new requirements for the weapon system. Our testing team is integrated with both the operators and developers, and understands not only what to test, but why a given feature is being added or modified at the request of the operator. This agile organizational structure along with our CI/CD pipeline allows us to test early and often and has reduced software defects by 90% during this contract. Testing in the CI/CD pipeline is being increasingly automated, and a systems integration tester is being added to each team.

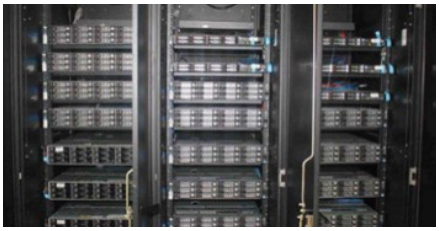
The DANS training organization keeps product owners and operators abreast of the latest advancements with the CVA/H weapon system. This team provides product owners with an understanding of what is changing, and why. For operators, training focuses on new features and installation and configuration of the systems on various hardware kits. Training includes technical documentation, video-based explanations, and classroom instruction regarding the latest advancements of the CVA/H weapon.

Mobile Interceptor Platform (MIP)

Mobile kit enables an operator to execute DCO missions; configure sensors and analyze the data collected.

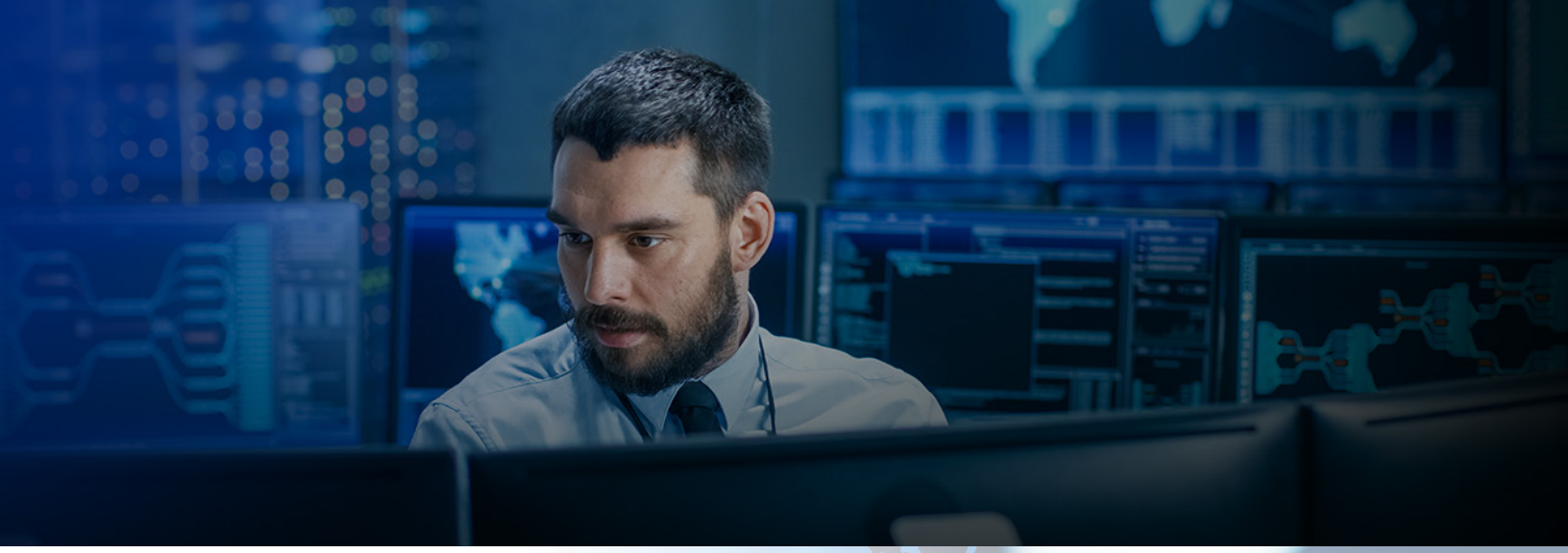
Deployable Interceptor Platform (DIP)

Portable kit that collects, detects, and responds to incidents and threats.



Garrison Interceptor Platform (GIP)

Stationary C2 platform that includes tactical display, storage area network, virtual machine hosting, and incident management.



RESULTS

Technica has proven to be a valued partner to the USAF CVA/H PMO. Through consolidation of functions, reorganization of support teams, and implementation of industry best practices for software development, integration, deployment, and support, we have:

- **Improved Speed and Quality of Delivery.**
  New capabilities are fielded faster, with simultaneous improvements to product quality and the organization's security posture.
- **Improved Effectiveness of End Users.**
  Improved documentation and training provide operators with the tools to incorporate new functionality into mission planning and execution.
- **Better, Faster Support.**
  Visibility into program support requirements and decreased time to problem resolution maintain uptime for CPTs and MDTs to achieve mission objectives.

NEXT GENERATION DCO

While Technica is dedicated to excellence in supporting today's defensive cyber weapon systems, Technica's Research and Development team, Technica Labs, is focused on innovations that will inform the development of next-generation cyber threat hunting weapons platforms featuring:

- Explainable AI for Cyber Threat Hunting
  - Graph Neural Networks for Cyber Threat Hunting
  - Natural Language Processing (NLP) for Cyber Log Analysis
- Next Generation Deployable Threat Hunting Kits (GPU/DPU)
- Edge Analytics in D/DL environment
- AIOPs for Cyber Operations (includes intelligent data path for analytics)

Technica is a leader in applying innovative technologies and processes to the most difficult technology challenges. We bring over 30 years of system engineering, innovation, and program delivery expertise to address today's daunting Cyber Warfare threats. With groundbreaking R&D, Technica's senior scientists and engineers are always finding new, innovative ways to solve complex problems and overcome today's Cyber Warfare challenges by leveraging deep experience in Systems Architecture & Integration, DevSecOps, IT Service Management, AIOps, Machine Learning, and Artificial Intelligence.

WE LISTEN. WE APPLY. WE SOLVE.


Technica™
technicacorp.com
Technica TM is a trademark of Technica Corporation.