AIR FORCE CYBERSPACE DEFENSE

Current as of March 20, 2023

MISSION

The Air Force Cyberspace Defense (ACD) weapon system is designed to prevent, detect, respond to, and provide forensics of intrusions into unclassified and classified networks. This weapon system supports the Air Force Information Network Security Operations Center in fulfilling their responsibilities.

ACD is operated by the 33d Cyberspace Operations Squadron (COS) and 426 Network Warfare Squadron (Air Force Reserve), at Joint Base San Antonio-Lackland, Texas, as well as the 102d COS (Air National Guard) at Quonset Air National Guard Base, R.I.

BACKGROUND

ACD evolved from the Air Force Computer Emergency Response Team. The team's primary responsibility was coordination of the former Air Force Information Warfare Center technical resources to assess, analyze, and mitigate computer security incidents and vulnerabilities.

ACD was officially designated by the Chief of Staff of the Air Force in March 2013.

FEATURES

ACD provides continuous monitoring and defense of Air Force unclassified and classified networks. ACD operates in four sub-discipline areas:

1. Incident prevention: Protecting Air Force networks against new and existing malicious logic by assessing and mitigating known software and hardware vulnerabilities.

2. Incident detection: Monitoring classified/unclassified Air Force networks, identifying and researching anomalous activity to determine problems and threats to networks, and monitoring real-time alerts generated from network sensors. The system also performs in-depth, historical traffic research reported through sensors.

3. Incident response: Determining the extent of intrusions, developing courses of action required to mitigate threats, and determining and executing response actions. The operational crew interfaces with law enforcement during malicious logic related incidents.

4. Computer forensics: Conducting in-depth analysis to determine threats from identified incidents and suspicious activities, then assessing damage. Supporting the incident response process, capturing the full impact of various exploits and reverse engineering code to determine impact to the network/system.

Characteristics

Primary Function: Defensive cyberspace operations to prevent, detect and respond to network intrusions.

Crew Positions: Cyberspace Crew Commander, Network Sensor Operator, Incident Response Operator, Defensive Counter Cyber, Host Sensor Operator, Forensic Malware Analyst, Cyber Threat Emulation. All mission crews are supported by mission support personnel.

Inventory: Two

Major Command: Air Combat Command, Joint Base Langley-Eustis, Virginia

Numbered Air Force: 16th Air Force, JBSA-Lackland, Texas

AIR COMBAT COMMAND PUBLIC AFFAIRS
115 Thompson St., Ste 121
Langley AFB, Va. 23665-1987
ACCPA.operations@us.af.mil
757-764-5007