AIR FORCE CYBER DEFENSE CASE STUDY

Problem:

• The Air Force needed a new cyber defense system that is cost-effective, powerful, and efficient
• The previous 102 COS infrastructure required additional system components to perform mission tasks
• The Hanscom ITF needed system implementations to simulate field operations

Solution:

• We delivered a cost-efficient solution by connecting our strategic IT partners
• The 102nd Cyber Operations Squadron (102 COS), North Kingston Rhode Island is equipped as a dual location with new Air Force Cyber Defense System
• Successfully upgraded both the NIPRNet and SIPRNet
• Designed a roadmap for future Air Force Cyber Defense (ACD) requirements

Overview: Building a Simpler, More Powerful Cyber Defense System.

As a trusted IT partner to the United States Department of Defense, our Air Force team creates custom-built technical solutions mindful of the cost drivers that impact the branch's operations and capabilities.

The 102nd Cyber Operations Squadron (102 COS) is an Air Combat Command (ACC) unit that provides Computer Network Defense (CND) services. CND incorporates actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within Department of Defense (DoD) information systems and computer networks. The previous 102 COS equipment/infrastructure required additional system components to perform mission tasks. The Hanscom Integrated Test Facility (ITF) needed system implementations to simulate field operations.

ID Technologies' Air Force team constructed a custom Air Force Cyber Defense (ACD) system to tackle this problem. We worked with our strategic IT partners – Dell, Cisco, HPE, VMware, Palo Alto, BlueCoat, Clearcube, Microsoft, SolarWinds, FireEye, and RedHat – to build this custom solution. We fortified the 102nd Cyber Operations Squadron (102 COS) – North Kingston Rhode Island as a Dual Operations Location (AF and ANG) with the Air Force's Cyberspace Defense Weapons System (ACD WS). Both the Non-Classified Internet Protocol Router Network (NIPRNet) and the Secret Internet Protocol Router Network (SIPRNet) were successfully upgraded as a result of our solution.

Challenge: More Simulations and Tasks. Not Enough Infrastructure.

The previous 102 COS infrastructure required additional system components to perform mission tasks, and the Hanscom ITF needed system implementations to simulate field operations.

Our Approach: Strategic Partnerships and Cost-Benefit Delivery.

We worked with our IT partners – Dell, Cisco, HPE, VMware, Palo Alto, BlueCoat, Clearcube, Microsoft, SolarWinds, FireEye, and RedHat – to deliver a cost-effective solution according to Lowest Price Technically Available (LPTA).

The affordable ACD WS created by our team utilizes logically separated VPNs to provide a secure framework for performing Cyber Security Service Provider (CSSP) services to the entire Air Force on both the Non-Classified Internet Protocol Router Network (NIPRNet) and the Secret Internet Protocol Router Network (SIPRNet). There are sensors connected to various networks which send security events back to collectors located either at the 33NWS or the Integrated Management System (IMS).

These security events are correlated using location and event time to provide a global security picture to the 33NWS analysts.

The 102NWS currently performs limited CSSP services by connecting to various resources using a VPN tunnel from Quonset to Lackland Air Force Base. This connectivity, while robust and secure, added a level of network latency that slowed down the 102NWS analysts. By creating this dual operating location, the 102NWS is now able to execute all the CSSP services, previously performed by the 33NWS, using local resources. This has made the 102NWS more independent and efficient.

Solution: A Simple, Robust, and Efficient Cyber Defense System.

This effort provided a permanent modification to replicate and install the ACD baseline at the 102NWS, located at ANG Base, Quonset Rhode Island, so that the 102NWS shall be able to support full ACD operations. This expansion at the 102NWS included hardware, software, and circuits as well as full configuration management. This solution provides full ACD WS functionality and capability at the 102NWS, including fixes to current network deficiencies on the Defender, Patriot, and Cyber Response Networks (CRN).

Our cost-effective solution equipped the 102nd Cyber Operations Squadron (102 COS), North Kingston Rhode Island as a Dual Operations Location (Air Force and Air National Guard) with the Air Force's Cyberspace Defense Weapons System (ACD WS). This also includes Hanscom's Integrated Test Facility (ITF).

Result: Set-Up for Success.

We successfully upgraded both the NIPRNet and SIPRNet and designed a roadmap for future Air Force Cyber Defense (ACD) requirements.

ACD is the biggest piece in an array of automated cybersecurity weapons the Air Force runs. Because of cyberspace's increasing importance to military operations and the escalating threats to the Defense Department's networks and communications systems, DoD officially classified cyberspace as a domain of warfare in 2011. Two years later, the Air Force classified six of its cyber capabilities as weapons systems. Along with ACD, the others are:

- **Automated Remediation Asset Discovery** (ARAD) – a modification of the original Cyber Security and Control System (CSCS), which monitors network activity, filters traffic going in and out of Air Force base domains, and blocks suspicious software.
- **Air Force Intranet Control** (AFNIC) – the primary Internet interface for each base, providing

defense-in-depth, proactive defense, network standardization, and situational awareness.

- **Cyberspace Defense Analysis** (CDA) – works in concert with the other cyber weapons systems, monitors Internet and email traffic, unclassified telephone networks, radio frequency communications, cyberspace operational risk assessment, and Web risk assessment. It also provides unintentional and intentional insider threat monitoring.
- **Cyberspace Vulnerability Assessment/Hunter** (CVA/Hunter) – provides vulnerability assessments and performs penetration testing and other white hat hacker operations to identify vulnerabilities.
- **Cyber Command and Control Mission System** (C3MS) – acts as the quarterback for the other cyber weapons systems, synchronizing their operations in support of combatant commands around the world.

The Air Force's systems are primarily defensive, focusing on prevention, detection, and response, but they reflect DoD's growing emphasis on cyber weapons of all kinds–offensive as well as defensive–in an escalating environment of cyber conflict.

102nd Defender Network