

CYBERSECURITY FOR EVOLVING THREATS



Elevate Cyber Posture with the Right Mix of Intelligent Automation, Dynamic Configuration Control, and Expertise

PERATON'S MANAGEMENT OF THE DOD'S LARGEST NETWORK



Supported 675,000 users



Blocked 3.5 million spam messages per month



Prevented more than 231 million unauthorized intrusion attempts per month



Detected 26 million threats per month



Sent 90 million email messages a week



Enabled 1+ billion browser transactions a day



Managed 37,000 mobile devices

Across the cyber landscape, the Air Force faces adversaries ranging from well-funded nation states to criminal cyberattack groups to individual hackers.

Easy access to low-cost tools and basic computer skills are all it takes to inflict significant damage to Air Force operations, the nation's infrastructure and institutions, and confidence in the government's ability to counter the threats. The harm done from exploiting vulnerable information systems and processes can cause more injury and disruption than any kinetic attack.

SPECIFIC SKILLSETS

Strengthening cyber posture demands the right expertise to get the most value from the technology. Peraton's team has created methodologies around modifying, integrating, and evolving technologies so they fit mission parameters continuously. These professionals—7,500 of whom hold a TS/SCI clearance—stand out because the solutions they develop get more results than baseline technology implementations can achieve alone.

Functioning as "connective tissue" with the technologies, technical and certified professionals think like hackers but act like guardians to monitor, detect, and respond to incidents.

With a DevSecOps mindset, essential staff have skills in security, testing, identity management, architecture, flow design, agile development, quality assurance, and robotic process automation. They also drive the enterprise to enforce policies, manage platform and vendor risk, and oversee audits.

USE OF DYNAMIC TECHNOLOGY

Effective mitigation of cyberattacks requires more than traditional point solutions and perimeter security.

Cyber resiliency needs an elastic infrastructure that predicts attacks, proactively responds to threats, ensures compliance—and protects data, applications, infrastructure, and endpoints.

The sheer volume and evolving nature of cyberattacks means that enterprises must leverage the right technologies—artificial intelligence, machine learning, data analytics and cloud computing—to enable dynamic configuration that allows fast deployment of code updates to devices, even in remote regions.

PROVEN PROVIDER

As the provider of technical solutions to the Department of Defense (DOD) for more than five decades, Peraton understands how to handle ever-changing cyber challenges that require large, complex integration of complementary technologies.

Peraton has a long tenure in delivering and managing the DOD's largest network. We know how to strengthen cyber resiliency in a multi-domain environment and transform an enterprise so that the Air Force mission is achieved. From this reputation as an experienced partner, Peraton has become the provider of choice.