



Cybersecurity

Protect Your Data. Empower Your Mission.

Advanced Cyber Capabilities with Agile Methods

Securing data, applications, and people is about more than just protecting critical assets. Done right, cybersecurity enables greater performance and the confidence to focus on the mission.

For more than 25 years, SMX has been providing cybersecurity for DoD, Government, and commercial clients, placing our team at the leading edge of offensive and defensive cyber operations.

Cybersecurity has been the cornerstone of our capabilities since we first began supporting one of our nation's most critical enterprise networks decades ago. While defending these large-scale networks from adversary threats, we have gained valuable insight into the challenges of defensive operations. Our cyber experts battle threats with advanced hunt capabilities and agile methods while protecting the confidentiality, integrity, and availability of mission-critical information.

Furthermore, as a Premier Partner in all three hyperscaler cloud platforms (AWS, Microsoft® Azure, Google Cloud), SMX is at the forefront of fusing cybersecurity into the cloud environment, assuring customers can obtain cost savings, redundancy, and scalability of cloud without sacrificing security or privacy.



- ✗ Managed Security Services
- ✗ Continuous Monitoring and Advanced Hunting
- ✗ Penetration Testing
- ✗ Red Team Tool Development
- ✗ Vulnerability Analysis and Remediation
- ✗ Automated Compliance and Reporting
- ✗ NIST RMF Assessment and Authorization
- ✗ Consulting and Training
- ✗ Platform RMF Certification

Continuous Security Operations and Defense of Enterprise Networks

Our 21st century national security environment faces unparalleled threats in today's world unlike anything we have experienced in the past. The cyber warfare game changes daily. Threat sources include sophisticated attacks of near-peer adversaries, the illicit efforts of organized crime to gain access to proprietary or user personal information, and the persistent insider threat. Today's security leadership must balance combating these threats with delivering mission-focused information systems to the warfighter in need. SMX leverages cybersecurity expertise gained across multiple, complex environments to provide continuous security operations and defense for today's most critical enterprise networks.

Compliance for Highly Regulated Workloads

SMX Cybersecurity Specialists are highly trained, experienced, and have the expertise to implement vital cybersecurity compliance standards across a multitude of services, agencies, and communities. The SMX team provides best practices from across DoD, government, and commercial enterprises, and is often able to meet customer requirements with a smaller footprint and tighter schedule than required. Each member of this multi-disciplinary team not only fulfills traditional Information System Security Officers/Engineers (ISSO/E) roles but also can conduct independent security assessments on behalf of agency/service Security Control Assessors (SCAs).



SMX Cloud Managed Services are FedRAMP Authorized and ISO certified for Information Security Management. Our solutions follow the NIST RMF framework for information security. SMX provides a wide range of cybersecurity solutions for:

- Global enterprises with hundreds of thousands of clients
- Highly classified, closed networks
- Vehicle communication systems (air and ground)
- Health information exchange (data in transit and at rest)
- Tactical communications
- Cloud, network, software, and data information assurance validation

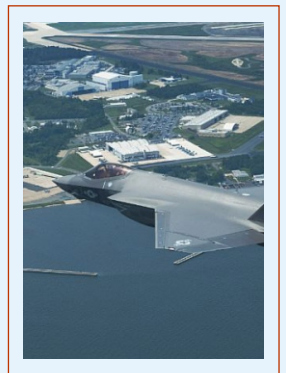
World-Class Penetration Testing and Advanced Hunting

Through our world-class penetration (pen) testing, SMX can identify weak spots in an organization's security posture, measure the compliance of their security policy, test the awareness of security issues, and determine whether (and how) the organization would be subject to security disasters. The reports generated by a pen test provide the feedback needed to prioritize the investments an organization plans to make in its security.

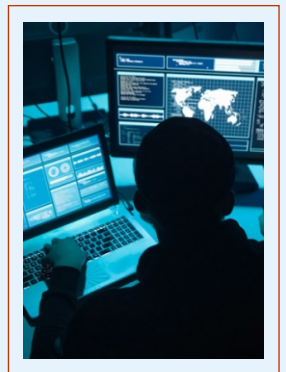
Our seasoned security professionals use a multi-tenant rapid scan capability for performing non-service impacting live system triage and compromise assessments. Our innovative detection techniques were developed based on years of defending high-value environments from the most sophisticated threat actors. We have developed an intelligent hunting platform that applies adversary behavior, machine/code learning, and proprietary, multi-faceted security analytics for the collection and triage of systems. This enables our experienced, proven hunters to provide critical 'overwatch' support for systems that give a higher level of assurance that bad actors are not attempting to operate in your environment.

Client Solution Spotlights

Joint Strike Fighter - The Department of Defense's (DoD) Joint Program Office (JPO) needed to provide government employees better access to Joint Strike Fighter (F-35) development efforts. As a result of the DoD 'Cloud First' strategy, an SMX-led team was selected to build the infrastructure, pipelines, security posture, and environment. This program established the first joint cloud environment with government control and private business partners. A viable product was delivered within just six months. Just as importantly, our solution enables them to support building multiple DevSecOps pipelines, which will sustain continuous ATO on the software that is built through them. This will include pipelines that enable flight system support by seven different government depots, along with major private companies that build and maintain the F-35, up to 40 small businesses that work on F-35 supply chain issues, and foreign nationals. This is possible because of the solid infrastructure security plan built by the SMX team for the new, modernized environment.



NAVAIR RMF Center of Excellence (CoE) - As part of the NAVAIR RMF Center of Excellence (CoE), SMX provides Information System Security Officers/Engineers (ISSO/E) and Validator support to programs at risk of losing authorization within the NAVAIR IS portfolio. This team of specialists surge to under-resourced and at-risk programs to provide full spectrum RMF support, including categorization, implementation, and assessment—more than 70 programs in total since the RMF CoE was established in 2019. Our support has resulted in dozens of programs avoiding de-authorization and a higher level of cyber security rigor being applied throughout the NAVAIR portfolio. Additionally, SMX maintains a team of skilled and experienced Navy Qualified Validators (NQVs) to support all NAVAIR clients. This cadre of validators specialize in conducting vulnerability assessment on Navy Information Systems (IS), utilizing Defense Information Service Agency (DISA) tools such as Secure Compliance Automation Protocol (SCAP), Security Technical Implementation Guides (STIGs), and the Assured Compliance Assessment Solution (ACAS) to ascertain the level of risk resident on an IS.



For more information, please contact our Digital Solutions Group: DigitalSolutions@smxtech.com

SMX harnesses the transformative power of technology to achieve mission success as a leader in digital and mission solutions, specializing in secure and advanced cloud, ISR, cyber, data analytics, engineering, space, and IT solutions. Operating in close proximity to our clients across the globe, the SMX team has a shared vision to deliver scalable and secure solutions to assure outcomes for the critical missions of our Government and commercial clients.

A few of our contracting vehicles: GSA ASTRO, GSA Alliant 2, GSA OASIS, GSA MAS IT, NITAAC CIO-SP3, SeaPort-NxG, and DIA SITE III.