Smartronix | MISSION ASSURED®

CYBER SECURITY

Battling Today's Threats While Protecting Mission-Critical Information

Cyber Security Solutions Using Advanced Hunting Capabilities and Agile Methods to Protect Mission-Critical Information

Smartronix has been providing top-level information technology, engineering, and cyber security for DoD, U.S. Government, and commercial customers for more than 25 years, placing our team at the leading edge of offensive and defensive cyber operations. Cyber security 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), Smartronix is at the forefront of fusing cyber security into the cloud environment, assuring customers can obtain cost savings, redundancy, and scalability of a cloud environment without sacrificing security or privacy.

Capabilities

- 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

aws partner network
Premier Consulting Partner

Gold Microsoft Partner
Azure Expert MSP
Microsoft

Premier Partner
Google Cloud

Smartronix provides a wide range of cyber security solutions for:

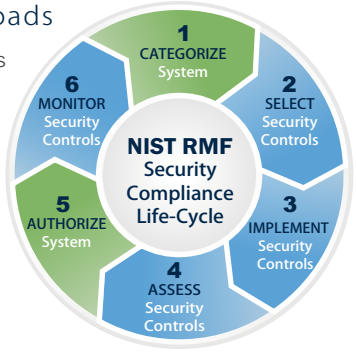
- Global enterprises with hundreds of thousands of clients
- Highly classified, closed networks
- Vehicle communication systems (air and ground)
- Health information exchange (data in transit and at rest)
- Tactical communications
- Cloud, network, software, and data information assurance validation

24x7x365 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. Smartronix leverages cyber security expertise gained across multiple, complex environments to provide 24x7x365 security operations and defense for today's most critical enterprise networks.

Compliance Solutions for NIST, RMF, and other Regulatory Workloads

Smartronix has a team of highly trained and experienced Cyber Security Specialists who are experts in implementing the Risk Management Framework (RMF) in a multitude of services, agencies, and communities. 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). The Smartronix team provides best practices from across Government and is often able to meet customer requirements with a smaller footprint and tighter schedule than required.



World-Class Penetration Testing and Advanced Cyber Hunting

Through our world-class penetration (pen) testing, Smartronix is able to 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 our 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.

A few of our Contracting Vehicles:

- GSA Alliant 2
- OASIS
- NITAAC/CIO-SP3
- NETCENTS-2 (NetOps SBC)
- SeaPort-NxG
- AAFES
- RS3
- GSA Schedule 70
- ACCENT
- DOI-FCHS

PRODUCT CAPABILITY SPOTLIGHT | CyberHunter

CyberHunter

An Advanced, Rapid Response Solution for Next-Gen Threats

CyberHunter® is a managed hunting platform purpose built by Smartronix to detect cyber intrusion attempts with full-time Analysts and Investigators dedicated to pro-actively hunting for adversary activity in your environment 24x7x365. CyberHunter hunts for signs of attack and automatically alerts when it identifies malware or malicious activity. CyberHunter monitors for subtle signs of adversary actions, including those that reside only in memory (never being written to disk and eluding traditional end point malware protections).

For more information, contact: CyberHunter@smartronix.com

PROGRAM SPOTLIGHT | Joint Strike Fighter

Smartronix supports the F-35 Joint Strike Fighter (JSF) Program Office (JPO) providing cyber security support to the JPO Special Access Program (SAP) networks. In six months, the Smartronix team installed and migrated seven enterprise networks, deploying a Nutanix hyperconverged virtualization capability, providing the JPO with a level of scalability it had not yet experienced. Through close cooperation with Air Force Office of Special Investigations (AFOSI) Authorizing Officials, Smartronix was able to obtain RMF authorization through the Joint SAP Implementation Guidance (JSIG) authorizing networks, which had been taken offline for years. Smartronix also led a consolidation effort collapsing five SAP networks into two, while delivering a first of its kind multi-level SAP network with Attribute Based Access Control (ABAC); and removing obstacles to multi-nation, multi-program cooperation at the SAP level, while still ensuring a high level of confidentiality and integrity.

PROGRAM SPOTLIGHT | NAVAIR RMF Center of Excellence (CoE)

Smartronix has extensive experience providing cyber security support and guidance. As part of the NAVAIR RMF CoE, Smartronix provides Information System Security Officers/Engineers (ISSO/E) and Validator support to the 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. Smartronix support to the RMF CoE has resulted in dozens of programs avoiding de-authorization and a higher level of cyber security rigor being applied throughout the NAVAIR portfolio. The RMF CoE team has provided support to more than 70 programs since it was established in 2019.

Smartronix 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.

Smartronix
MISSION ASSURED
DefenseSolutions@smartronix.com
301-373-6000
smartronix.com