



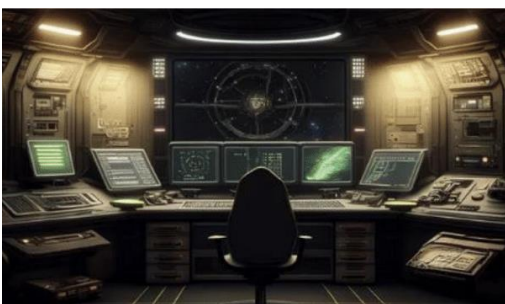
SECUREXPERTS



SXi CyberWatch Solutions™

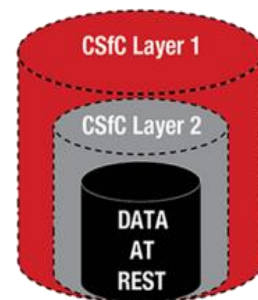
Maintaining and optimizing Cybersecurity via NSA Approved Commercial Solutions for Classified (CSfC) Inspired technologies

The SXi CyberWatch™ solutions is built using an integration of open-source framework, commercial applications, and custom developed tools that leverages open-source technologies with commercially available software as well as tools and capabilities uniquely written to achieve US and international compliance requirements defined by the US Department of Defense (DoD), National Institute of Standards and Technology (NIST), and the National Security Agency (NSA).



- Intrusion Detection**
- Log Analysis**
- File Integrity Monitoring**
- Vulnerability Detection**
- Configuration Assessment**
- Incident Response**
- Regulatory Compliance**
- Cloud Security**
- Black Pearl SXi™ Secure EUD**

SECUREXPERTS



SecureXperts, Incorporated, "SXi", founded in 2001 by a team of industry experts in cybersecurity, is recognized as an industry leader in the evaluation of cyber security posture for cyber-physical systems used in critical infrastructure protection such as the energy and power grid industrial control systems, healthcare, Military, law enforcement and financial sectors to name a few.

The NSA now allows classified information to be transmitted on wired and wireless connections, even over public and partner networks by using two sets of encryption technologies (such as Cisco and Aruba VPNs), one layered inside the other. The NSA has also approved combinations of solutions that include a layer of VPN combined with encryption provided by Wi-Fi, TLS or MACsec, following specific guidelines. Our de-centralized solution, SXi CyberWatch™ is a threat prevention, detection, and response platform capable of protecting systems whether on-premises, virtualized, cloud based, or hybrid computing environments.

Our US based personnel have security clearances up to and including Top Secret. We work vigilantly to protect you and our nation's most critical assets 24/7/365.

Your Mission is our Focus.



SXi CyberWatch™

SXi CyberWatch™ is rigorously tested to safeguard against unauthorized intrusions using penetration and meets regulatory requirements to include NIST 800-53 as well as proposed Department of Defense mandates for Safeguarding Controlled and Unclassified Defense Information.

Log-Analysis – Our Mother of Pearl (MOP) server component uses a signature-based approach to intrusion detection, using its regular expression engine to analyze collected log data using the system agents and look for indicators of compromise.

Intrusion Protection – CyberWatch system agents scan the monitored systems looking for malware, rootkits and suspicious anomalies. They can detect hidden files, cloaked processes or unregistered network listeners, as well as inconsistencies in system call responses.

Vulnerability Detection - Hardware and software agents collect software inventory data and send this information to the server, where it is correlated with *continuously* updated CVE (Common Vulnerability and Exposure) databases, to identify security flaws, exploitable weaknesses and vulnerable software.

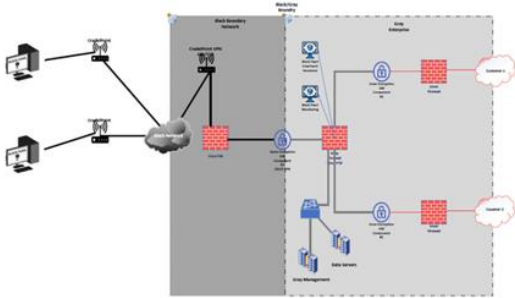
Configuration Assessment- We monitor system and application configuration settings to ensure they are compliant with your security policies, standards and/or hardening guides. Agents perform periodic scans to detect applications that are known to be vulnerable, unpatched, or insecurely configured.

Incident Response- We provide out-of-the-box active responses to perform various countermeasures to address active threats, such as blocking access to a system from the threat source when certain criteria are met. In addition, we can remotely run commands or system queries (Using SXi CyberSafe Access Product), to identify indicators of compromise (IOCs) and perform live forensics or incident response tasks.

Regulatory Compliance – We configure custom tools needed to follow industry standards (i.e. HIPAA, SOX, PCI-DSS, GDPR, NIST, FedRAMP, and DoD and US Federal Standards (FISMA).

Cloud Security- We manage Cloud Infrastructure security at an API level, using integration modules that can pull security data from well known cloud providers. We provide a rich set of rules to assess the configuration of your cloud environment, easily spotting exploitable weaknesses within your environment.

Black Pearl SXi™ Secure EUD- We developed the next generation solution of an out-of-the box solution meeting NIST 800-171 requirements for Safeguarding Controlled and Unclassified Information (“CUI”). This standard is currently mandated by all Defense Industrial Base Contractors to protect federal contract information and controlled information.



NASA Kennedy Space Center
Building M6-306 Room 1120
Kennedy Space Center FL 32899
888-804-4674

www.securexperts.com

