CAPABILITIES STATEMENT

COMPANY

- NAICS CODES: 541512 (Primary), 511210, 518210, 541511, 541690, 541990
- DUNS: 117936878
- CAGE CODE: 8ZXJ8

MARKET EXPERTISE

- Corporate Enterprise
- IoT / IIoT Security
- Secure Communications
- Ad hoc Networks
- Government Departments & Agencies
- Critical Infrastructure, Industrial OT/IT, SCADA
- Healthcare
- Financial & Accounting
- Gaming & Entertainment

CORE TECHNOLOGY / PRODUCTS

- XSOC ™ Cryptosystem Symmetric Encryption Engine
- EBP ™ - Encrypted Broadcast Protocol
- SOCKET - Cryptographic Key Exchange (Local/ Open)
- WAN-SOCKET - Cryptographic Key Distribution (Global P2P)

INTRODUCTION:

XSOC CORP was founded on the notion that the only real way to ensure computer systems and data are protected from today's threats is through the continual and methodical use of better cybersecurity tools that include: strong encryption, vastly more efficient and secure methods for exchanging keys, and advanced user authentication factors.

Improvements in these three areas have proven to have the greatest impact in reducing cybersecurity risk, strengthening organizational cyber resilience, and mitigating data loss in the event of a breach or malware/ransomware attack.

Even the world's most advanced and complex networks share a common weakness when it comes down to the limitations imposed by the most commonly cybersecurity tools used to protect files, multimedia streams, hard drives, email, text/ communications, as well as IT and OT network traffic.

There are very few, if any, cybersecurity tools that allow IT/ InfoSec professionals to perform in-place or bump-in-the-wire upgrades to their core cryptography (encryption engines or secure workflows) seamlessly and without undue complexity.

XSOC CORP is led by a highly experienced executive team with multi-disciplined cybersecurity and cryptography expertise, focused on: high-velocity/Quantum-Safe encryption, advanced symmetric key exchange and distribution platforms, and encrypted data transmission and communication protocols.

CAPABILITIES STATEMENT

CORE COMPETENCIES:

High Strength Encryption
- Symmetric/ Asymmetric
- CNSA Cryptography
- Next-Gen Ciphers
- 512bit+ PQ Cryptography
- Advanced Key Mgmt

Software Development Services
- HTTP/HTTPS
- Web Integration
- File/Text/Email Security
- Hybrid Cloud
- DB Encryption

Hardware Integration/ Engineering
- Embedded Encryption
- Purpose-built devices
- Asymmetric Encryption Alternatives

Cybersecurity Consulting
- Cybersecurity Architecture & Integration Guidance
- SOC
- CMMC
- Pen Test

Cybersecurity Training & Education Consulting
- Course Development
- CISSP/ Skills Assessment
- Field Demos
- Lab - Test Environment
- Best Practices

CORE COMPETENCIES:

XSOC CORP products address the vulnerabilities present in most all of today's applications and computers systems that are not currently using Quantum-Safe encryption or cryptographic protocols to address the immediate threats posed by today's hackers, and those in the future that will have access to Quantum Computing resources.

XSOC CORP products are uniquely capable of addressing the current cybersecurity challenges posed by:

Public Key Infrastructure (PKI) and its use of (Quantum-vulnerable) asymmetric encryption

- Critical Infrastructure/ ICS/ SCADA environments where the convergence of OT & IT networks and the deployment of IIoT sensors make these previously "air-gapped" networks vulnerable
- Data whose value or retention period would exceed 3-5yrs and would require the use of Quantum-Safe encryption to guard against Data Harvesting attacks or data breaches
- SSL/TLS "encrypted transports" being unduly relied upon (over data encryption) to protect data from Man-in-The-Middle and other attacks attempting to intercept data "in-motion"
- Ineffective or poorly utilized user authentication factors that leave data or encryption keys vulnerable to insider and outsider threats

XSOC CORP products are available as SDK toolsets/ API protocols, user-installable plugs and extensions, or as-a-service offerings that can be licensed for large enterprise/ industrial/ government use that enable wide-spread adoption and deployment. By utilizing XSOC CORP products, data residing on-premise, in cloud archives, or even DR/BC facilities can be truly protected – offering consumers measurable and monetizable reductions in cyber risk and associated costs, while increasing productivity.

PRODUCT

XSOC™ Cryptosystem – Symmetric Encryption Engine

Description:

Purpose-built, optimizable encryption engine designed to provide Quantum-Safe information security using FIPS 140-2 Certified functionality, for any data stored or transmitted regardless of size or format, and can be integrated into new or existing cybersecurity applications or workflows.

Optimal Uses:

- When the low-speed/ high-latency of existing (legacy) encryption make it prohibitive to deploy
- Where the value or retention period of the data being stored or transmitted is expecting be longer than 3-5years (the timeframe when powerful Quantum Computers could be used to decrypt data)
- Integrated into “constrained” internet connected devices (e.g., IoT/ IIoT/ IoBT/ sensors) where the efficiency of the encryption engine, or being “lightweight”, is a primary decision factor
- Live video streaming/ conferencing without relying on Network Time Protocol (NTP) for syncing

Competitive Differentiators:

- FIPS 140-2 Certified, with (100) Quantum-Safe waveform encryption settings (starting 512-bit)
- Extremely fast performing, can be software or hardware-integrated without affecting performance
- Optimizable, flexible and combinable modes allow highest speed/lowest latency or max strength

XSOC Value Proposition:

By incorporating the XSOC encryption engine into an organization’s business processes and leveraging its increased SPEED, EFFICIENCY, and SECURITY (compared with legacy encryption) it delivers measurable and monetizable reductions in application/ device resource utilization, network latency, corporate cyber-risk, and IT maintenance while increasing cyberattack resistance, cyber resilience and productivity.

Encryption Efficiency & Attack-Resistance Metrics	XSOC™ Cryptosystem Encryption Engine	AES Block Cipher	ChaCha Stream Cipher
▷ STRENGTH (Length of symmetric key, expressed in "bits")	100 Available Key Lengths From 512-bit to 51,200-bit	3 Choices 128, 192, 256-bit	2 Choices 128, 256-bit
▷ LIGHTWEIGHT/ SOFTWARE-EFFICIENT (Ability to be deployed on variety of platforms, including resource-constrained IoT/ Mobile)	YES	NO	YES
▷ LATENCY (Processing time required from start to finish)	Lowest	Highest	Middle
▷ AGILITY/ FLEXIBILITY (Ability to be customized/tailored to use case)	YES	NO	NO
▷ BRUTE FORCE ATTACK RESISTANCE (Against today's "Classical Computers")	Excellent XSOC key lengths start at 512-bit	Good	Good
▷ BRUTE FORCE ATTACK RESISTANCE (Against upcoming "Quantum Computers")	Excellent XSOC key lengths are "Quantum-Safe" today	Below Avg Max 256-bit keys not "Quantum Safe"	Below Avg Max 256-bit keys not "Quantum Safe"
▷ DATA HARVESTING ATTACK (Against upcoming "Quantum Computers")	Excellent XSOC key lengths are "Quantum-Safe" today	Below Avg Max 256-bit keys not "Quantum Safe"	Below Avg Max 256-bit keys not "Quantum Safe"
▷ SIDE CHANNEL ATTACK RESISTANCE (Attacks based on information gained from the implementation of a computer system, rather than weaknesses in the encryption algorithm itself, to learn the encryption key)	Very Good Hybrid design is inherently resistant to Block-cipher only and Stream-cipher only attacks	Average	Average

PROTOCOL

EBP ™ – Encrypted Broadcast Protocol

Description:

Purpose-built, highly optimized data transmission and communications protocol used to send, share transfer, migrate or stream small to very large data packets (e.g., file data, audio, video, multimedia, big data) across internal or external networks, via on-premise or cloud storage repositories.

Optimal Uses:

- When transmission Speed, Reliability and Security are all EQUALLY important
- Where the value or retention period of the data being transmitted is expecting be longer than 3-5years (which is the projected timeframe when sufficiently powerful Quantum Computers could be used to decrypt data that was encrypted using today's legacy encryption algorithms)
- Where the threat of a viable Man-in-The Middle attack is present (where attackers will attempt to intercept data in-motion and either use, store, sell, or ransom the stolen data)
- Where a company's cybersecurity policy requires that certain types of data (e.g., big data, PII, corporate IP) be sent using E2E encryption methods and not solely reliant SSL/TLS to ensure security

Competitive Differentiators:

- Most vendors' high-speed data transmission products utilize general-purpose protocols that prioritize Speed or Reliability but fail to address Security
- Select vendors' high-speed data transmission products utilize specialized protocols that deliver "better" Speed and Reliability with minor improvements in Efficiency or Security
- The EBP protocol leverages "Proactive Flow Control" to intelligently monitor and adjust throughput on-the-fly to provide the highest-possible transmission speeds while ensuring complete reliability.

EBP Value Proposition:

By incorporating the EBP protocol into an organization's business processes and leveraging its increased SPEED, EFFICIENCY, RELIABILITY & SECURITY (compared with general-purpose or even select specialized data transmission protocols) it delivers measurable and monetizable reductions in carrier costs, network latency, corporate cyber-risk, and IT maintenance while increasing productivity.

Data Transmission Protocol Efficiency & Utilization Metrics	EBP ™ Protocol	FASP Protocol	UDP Protocol	TCP Protocol
▷ SPEED	Highest	High	High	Low
▷ RELIABILITY	Highest	High	Low	High
▷ EFFICIENCY	Highest	High	Avg	Avg
▷ DATA SECURITY	Highest	Avg	None	None
▷ END-TO-END ENCRYPTION	Yes	Yes	No	No
▪ Quantum-Safe Encryption	Yes	No	No	No
▷ UTILIZATION COMPLEXITY	Simple	Extensive	Simple	Simple
▪ Ease of Deployment	Simple	Difficult	Avg	Difficult
▪ Ease of Administration	Simple	Difficult	Avg	Avg
▷ OVERALL TCO ($)	Low	High	Low	Avg

SOCKET

PLATFORM

SOCKET – Symmetric Key Exchange Platform for Closed, Semi-Open, or WAN

Description:

Purpose-built platform for exchanging/ distributing/ facilitating the movement of encryption keys generated by symmetric encryption engines or algorithms, between senders and receivers, over closed/air-gapped, ad hoc, or local wired/ wireless, or open networks.

Optimal Uses:

- When needing to secure signal communications across wireless/ ad hoc/ tactical networks
- When ease of setup, deployment speed, or enhanced security are priorities
- Closed/air-gapped networks such as those found in Critical Infrastructure/OT/SCADA environments where key exchange efficiency and speed have precluded the use of existing key exchange methods
- When the use of digital certificates managed by the Public Key Infrastructure process would not be viable or would not provide long-term security (as they would likely need to be replaced in 3-5yrs at which time a sufficiently powerful Quantum Computer may become available and be used to break the asymmetric encryption used throughout the PKI process)
- When hardware/device-based Quantum Key Distribution (QKD) would not be ideal or viable, not work within the prescribed distance limitations, be too costly to deploy, or would not meet an organizations data security requirements
- When combined with XSOC CORP's EBP (Protocol), the resulting platform would create the world's most secure (symmetrically encrypted) VPN offering significant data security and integrity assurances over existing standard VPNs that rely on (Quantum-vulnerable) asymmetric encryption algorithms and SSL/TLS "encrypted transports" to protect data from Man-in-The-Middle and other attacks attempting to intercept data "in-motion"

Competitive Differentiators:

- Received UL 2900-1 Cybersecurity Assurance Program Certification
- Can be integrated as an in-place or "bump-in-the-wire" upgrade to existing hardware/ workflows
- Accommodates the use of both (legacy), or newer Quantum-Safe symmetric encryption keys
- Does not require a long complex installation, costly hardware, or a fibre optic network to use

SOCKET Value Proposition:

By incorporating the SOCKET platform into an organization's business processes and leveraging its increased SPEED, EFFICIENCY, and SECURITY (in comparison to other key distribution methods) it delivers measurable and monetizable reductions in application/ device resource utilization, network latency, corporate cyber-risk while increasing cyberattack resistance and productivity.

WAN-SOCKET

PLATFORM

WAN-SOCKET - Global P2P Symmetric Key Distribution Platform for WAN

Description:

Purpose-built platform for exchanging/ distributing/ facilitating the movement of encryption keys generated by symmetric encryption engines or algorithms, between senders and receivers, over WAN or Fully-Open globally connected networks by leveraging the scalability, performance and redundancy of Distributed Hash Tables.

Optimal Uses:

- Ideal for securing P2P data transmissions from smart phones, mobile, IoT devices and websites
- For applications requiring fully secure end-to-end encryption as well high-speed and efficiency
- Significantly increased security for public cloud and virtual private networks (VPNs)
- When needing to mitigate and protect against potential DDoS and MiTM attacks (as distributed networks have no single points of failure)

Competitive Differentiators:

- Distributed Hash Table technology that allows for maximum reliability and uptime when exchanging encryption keys
- More efficient and more secure in comparison to legacy software and newer hardware-based methods or processes for exchanging symmetric key material worldwide
- More versatile than Signal's double-ratchet technology for providing true end-to-end encryption options for devices and apps

WAN-SOCKET Value Proposition:

By incorporating the WAN-SOCKET platform into an organization's business processes and leveraging its increased SPEED, EFFICIENCY, RELIABILITY and SECURITY (in comparison to other globally-applicable key distribution methods) it delivers measurable and monetizable reductions in application/ device resource utilization, network latency, corporate cyber-risk while increasing cyberattack resistance and productivity.