CAPABILITIES STATEMENT

COMPANY

- NAICS CODES: 511210 (Primary), 541512
- 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

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

INTRODUCTION:

XSOC Corp ("XC") was founded on the notion that the only real way to ensure computer systems and data are protected from external 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.

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 when protecting files, hard drives, email, text/instant messages, and networks. There are very few, if any, 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.

XC is led by a highly experienced executive team with multidisciplined cybersecurity and cryptography experts focused on: High-Velocity/ Quantum-Safe encryption, Ultra-secure/Out-of-Band Symmetric Key Exchange, and Encrypted/ High-Speed File and Communication Transmission.

CAPABILITIES STATEMENT

CORE COMPETENCIES:

High Strength Encryption
- Symmetric/ Asymmetric
- NIST Suite B
- 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 Guidance
- SOC
- CMMC
- Pen Test

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

CORE COMPETENCIES:

XC 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.

XC products on 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, OT/IT, 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

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

PRODUCTS

XSOC ™ Cryptosystem – Hybrid Symmetric Encryption Engine

Description:

Purpose-built, customizable encryption engine designed to provide Quantum-Safe information security for any data stored or data sent, shared, transferred, migrated, or streamed- regardless of size or format, and 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 (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)
- Integrated into "constrained" internet-connected devices (e.g., IoT/ IIoT/ IIoBT/ sensors) where the efficiency of the encryption engine, or being "lightweight", is a primary decision factor

Competitive Differentiators:

- Post-Quantum strength (key starts at 512-bit), number of available keys, and "randomization" modes
- Ability to be software or hardware-integrated without affecting performance or throughput
- Ability to customize or "tune" the encryption engine based on the use-case or user requirements

XSOC Value Proposition:

By incorporating the XSOC encryption engine into an organizations 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 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, incl. resource-constrained IoT/ Mobile)	**YES**	NO	YES
▷ **LATENCY** (Processing time required from start to finish)	**Lowest**	Highest	Middle
▷ **AGILITY/ FLEXIBILITY** (Ability to be customized or "tuned" to fit the use case)	**YES**	NO	NO
▷ **BRUTE FORCE ATTACK RESISTANCE (TODAY)** (Against current "Classical" computing systems)	**Excellent** XSOC key lengths start at 512-bit	Good	Good
▷ **BRUTE FORCE ATTACK RESISTANCE (TOMMOROW)** (Against upcoming "Quantum Computing" systems)	**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

PRODUCTS

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 excels in Speed, Reliability, and Efficiency while offering the Highest Level of Security. EBP exemplifies the difference between "innovation" and "incremental enhancement"

EBP Value Proposition:

By incorporating the EBP protocol into an organizations 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 Deplpyment	**Simple**	Difficult	Avg	Difficult
▪ Ease of Administration	**Simple**	Difficult	Avg	Avg
▷ OVERALL TCO ($)	**Low**	High	Low	Avg

PRODUCTS

SOCKET – Cryptographic Key Exchange (for LAN, Closed, Air-Gapped Networks)

Description:

Purpose-built, protocol used to exchange/ distribute/ facilitate 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 networks.

Optimal Uses:

- When needing to securing 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 Critical Infrastructure/OT/SCADA environments where key exchange efficiency and speed have precluded the use of existing key exchange methods
- When the Public Key Infrastructure (PKI) + certificate process would not be viable, not adequately secure, or would likely need to be replaced in 3-5yrs (which is the projected timeframe when sufficiently powerful Quantum Computer would be able to break PKI's asymmetric encryption)
- 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, would not meet the organizations data security requirements

Competitive Differentiators:

- 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 protocol into an organizations 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

PRODUCTS

WAN-SOCKET - Cryptographic Key Exchange (for WAN, Fully-Open Networks)

Description:

Purpose-built, highly optimized data transmission and communications process used to send, share transfer, or migrate small to very large data packets (e.g., file data, audio, video, multimedia, big data) across WAN or Fully Open and globally connected networks, via on-premise or cloud storage repositories, leveraging Distributed Hash Tables.

Optimal Uses:

- Ideal for securing data transmissions from smart phones, mobile, IoT devices and websites
- For application 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 process into an organizations business processes and leveraging its increased SPEED, EFFICIENCY 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.