CAPABILITY STATEMENT · V1.0 · MMXXVI

SPARTYN

CYBER OPERATIONS CENTER

NST // 038°N 077°W

Operator-led, AI-accelerated cyber operations. One integrated command surface across every mission phase.

SPARTYN unifies offensive testing, threat intelligence, wireless operations, compliance orchestration, exercise, and continuous exposure management into a single deployable platform — engineered for teams that measure outcomes in minutes, not quarters.

01 WHAT SPARTYN IS

A UNIFIED CYBER OPERATIONS ECOSYSTEM

Deployed on-premise as a Nightshade-managed NUC with dedicated GPU, SPARTYN runs every module locally — no cloud dependency and no inbound exposure. All seven systems report through a single command surface. Built by operators, for operators.

01 · DOCTRINE

OPERATOR-LED

Human decision authority at every stage. The AI proposes; the operator commits.

02 · CADENCE

AI-ACCELERATED

On-device GPU inference. Attack paths surfaced in minutes, not fatigue-driven hours.

03 · POSTURE

ON-DEVICE

Local NUC + GPU per site. No cloud dependency. No inbound firewall exposure.

04 · SIGNAL

CONTINUOUS

Persistent visibility across the fleet. Findings mapped to MITRE ATT&CK, always current.

CONT · P. 02 →

NODE.LAX-04 · STATE · OK · LAT 32ms · UPTIME 99.98%

THE PLATFORM →

02 THE PLATFORM

Seven interlocking systems.
One command surface.

Each SPARTYN module operates independently and reports into the same operator console, connecting offensive operations, intelligence, wireless, compliance, exercise, exposure, and command telemetry into a unified operational view.

A · SYS.01
ARES
OFFENSIVE SECURITY

Operator-driven, AI-assisted red-team operations and continuous adversary emulation across the client estate.

B · SYS.02
ATHENA
THREAT INTELLIGENCE

Curated adversary techniques, campaigns, and IOCs — kept current and piped into every active module.

Γ · SYS.03
ARGUS
WIRELESS OPERATIONS

Automated wireless reconnaissance, rogue detection, and RF-perimeter validation across 2.4 / 5 / 6 GHz.

Δ · SYS.04
THEMIS
COMPLIANCE · ORCHESTRATION

Framework-aware control mapping, evidence collection, and orchestration across CMMC, NIST, and ISO regimes.

E · SYS.05
AGOGE
EXERCISE · SIMULATION

Adaptive tabletop and live-fire cyber exercises. Scenarios mutate as the team responds — no static scripts.

Z · SYS.06
AEGIS
CONTINUOUS THREAT EXPOSURE

Continuous validation of exposure surface — attack-path scoring, control-drift, and blast-radius modeling.

H · SYS.07
COMMAND
OPERATIONS INTERFACE

Live NOC-style oversight — availability, utilization, incidents, SLA, and audit — for every deployed node.

DIFF · 01
OPERATOR AUTHORITY
Every consequential action requires a human commit. AI accelerates decisions — it does not replace them.

DIFF · 02
LOCAL BY DESIGN
Each site runs an NST-managed NUC with dedicated GPU. Zero inbound exposure via Tailscale mesh.

DIFF · 03
TECHNIQUE-MAPPED
Findings mapped to MITRE ATT&CK and Red Canary APT — outcomes framed in adversary language, not CVSS noise.

MISSION FIT · REPRESENTATIVE
WHERE SPARTYN OPERATES
- Defense & intelligence primes
- Critical-infrastructure operators
- Global financial services
- Federal & state agencies
- Healthcare & life sciences
- Managed detection & response

ENGAGE · SECURE CHANNEL
Request a Briefing

NIGHTSHADE-TECHNOLOGIES.COM
OPS@NIGHTSHADE-TECHNOLOGIES.COM
+1 · 202 · 555 · 0184