Evolver Integrated Solution Paper (EISP)

Evolver SPECTRA

AI-Powered Self-Learning SOC

Detect the unknown. Cut the noise.

Customer Cyber Challenge — Use Case

Federal programs must accelerate reliable cyber-attack detection and response while lowering Security Operations Center (SOC) costs and security analyst fatigue across enterprise, cloud, edge, and air-gapped environments.

Rule/signature stacks flood security analysts with low-value alerts, miss emerging Tactics, Techniques, & Procedures (TTPs), and demand continual tuning—diverting teams from investigations and driving longer dwell time and higher Mean-Time-To-Detection (MTTD) and Mean-Time-To-Response (MTTR), especially in contested or disconnected operations.

Solution Overview

The New Evolver SPECTRA Solution — Self-supervised Platform for Enterprise Cyber Threat Recognition & Analysis solution combines a self-supervised AI overlay (powered by MixMode AI) with 24×7 SOC operations and Evolver's Innovation Center (EIC).

SPECTRA ingests live telemetry across NetFlow/IPFIX, DNS/proxy, authentication, EDR/host, and cloud audit logs, then normalizes and enriches that data to learn environment-specific behavior without labels, signatures, or static rules. As an AI-driven cybersecurity platform, SPECTRA autonomously detects unknown and emerging attacks, delivering AI-driven anomaly detection that can function as an NDR, NTA, SIEM and/or UEBA. Built for hyperautomation and simplicity, SPECTRA surfaces statistically meaningful deviations with timeline stitching and analyst-ready context, driving predictive detections that save SOC teams time, reduce false positives, and accelerate investigation and containment.

Evolver Integrated Solution – Unique Features

- SPECTRA is a self-learning dynamic tool designed to surface meaningful anomalies and reduce false positives
- Runs as a source-agnostic overlay integrating with common SIEM/EDR/ticketing APIs
- Uses an edge-capable architecture on standard x86 (GPUs optional for heavy local training or extreme throughput).
- Security Analysts are augmented with timeline stitching, contextual enrichment, prioritized evidence, and explainability, and automation progresses safely from advisory to enforced SOAR playbooks with rollback and full audit trails.

Operational Controls: Connectors follow least-privilege access (LPA) with scoped, vaulted credentials for any elevated access; potential Personally Identifiable Information (PII) is protected by role-based access, hashing/tokenization, and deterministic tokenization for cross-dataset correlation without exposing raw values.

The platform captures Risk Management Framework (RMF)-aligned evidence with provenance and OSCAL mapping suitable for Authorization to Operate (ATO) packages, maintains model lineage with a documented retraining cadence, and is routinely validated via purple-team exercises and MITRE ATT&CK-mapped cyber threat hunts.

As a managed service, SPECTRA provide

- Level 1–Level 3 SOC support
- Detection engineering and content QA
- Cyber threat hunt sprints SOAR playbook development
- Outcome Dashboards
- Integration with SIEM, EDR, and identity, ticketing to orchestrate containment without rip-and-replace

Expected Customer Benefits

- Programs gain a higher signal-to-noise ratio, reducing MTTD & MTTR up to 70% and fewer non-actionable alerts
- Dashboards track detection fidelity, response throughput, case aging/closure quality, and ATT&CK-mapped coverage
- Lower SOC costs by 30%+

How It Works

We deploy lightweight collectors/taps and validate parsers, telemetry quality, and canonical asset mapping; baseline learning starts immediately. A typical cadence:

Day 0-3
- Deploy collectors/taps
- Validate parsers
- Telemetry quality & asset mapping; baseline learning begins

Day 4-7
Analyst review and contextual tuning
- Asset
- Role
- Mission Priority

Day 8-30
Cyber threat hunt sprints mapped to MITRE ATT&CK; advisory SOAR actions

Post-Day 30
Transition vetted play-books to enforced actions with rollback controls

For air-gapped sites, inference and containment run locally with scheduled, policy-controlled synchronization (batched or manual transfer) to headquarters when connectivity permits.

Evolver Integrated Technology Solutions (EITS)

A portfolio of market-leading solutions for cybersecurity that accelerate federal missions delivered as modular capabilities that agencies can adopt quickly, integrate easily, and scale confidently. The EITS portfolio provides a cohesive suite of mission-ready technology accelerators designed to help federal programs improve speed, reduce operational burden, and increase measurable cybersecurity outcomes. Each solution can be deployed independently or combined to optimize customer operations.

SPECTRA
SOC Support

An advanced AI-powered toolkit that enhances SOC results through high-fidelity detections, enriched telemetry, and governed automation to reduce analyst fatigue and operational cost

30-60 Day Pilot:
Bounded COI pilot with defined telemetry/parser tests, model governance, & SOAR runbooks; progress from advisory to enforced automation.

SHIELD
Post-Quantum Cryptography

A transparent and portable solution for Post-Quantum Cryptography (PQC) enterprise network security, enabling agencies to safeguard critical tunnels with zero disruption and full auditability.

30-60 Day Pilot:
Pilot one or two critical tunnels; success = zero data-plane disruption, rotation SLOs met, policy/audit logs verified, and eMASS/CSAM artifacts updated; then phase rollout.

CLEAR
Procurement

An expedited, non-intrusive, independent cybersecurity supply-chain risk assessment that accelerates vendor cyber risk assessments, improves visibility, and supports continuous risk monitoring at scale.

30-60 Day Pilot:
Pilot a supplier wave (25–50) to validate coverage, turnaround, closure KPIs; scale with continuous monitoring.

GUARDIAN
Vulnerability Management

An integrated cyber risk- based vulnerability management solution tailored for U.S. Federal government programs to address fragmented and slow vulnerability management processes.

30-60 Day Pilot:
The pilot delivers a rapid, measurable advancement of an agency's vulnerability management maturity by unifying fragmented scanner outputs, normalizing exposure data, applying mission-aligned prioritization, and automating remediation workflows.

Procurement Options: *Existing Evolver GSA or agency services contracts *Public-sector channels/marketplaces (e.g., AWS Marketplace for CLEAR) *On-Prem/GovCloud deployment for SPECTRA/SHIELD per system boundary. 30–60-Day Pilots available.

Why Evolver

Who We Are

Our cyber teams work as partners focused on practical outcomes while leveraging AI and advanced data analytics tools to perform the work better, faster, and more cost-effectively, so authorization keeps pace with the speed of delivery.

Evolver delivers:

- End-to-end defensive cyber operations programs
- SOC operations
- Security engineering and architecture
- Cyber threat intelligence
- Penetration testing
- Cyber vulnerability scanning & analysis
- Cyber forensics analysis
- Cyber threat hunting
- AI/ML capabilities
- Full cyber governance, risk, & compliance (GRC) services
- Cyber-Supply Chain Risk Management (C-SCRM)

Gregory A. Garrett | Chief Operating Officer
Gregory.Garrett@evolverinc.com - 571.991.7768 - www.evolverinc.com