SoftServe

AI-Powered Detection Engineering

Eliminate SOC Overload with SoftServe's Deep Internal Expertise.

$10.5T

Annual cost of cybercrime by 2025

Alert Overload: 10,000+ daily alerts make it difficult to identify real threats for already overworked security teams.

2,200+

Daily global cyberattacks

Limited Security Resources: Shortage of 3.4M cybersecurity professionals hinders scaling security operations.

70%

Organizations reporting phishing-related breaches

Increasing Attack Sophistication: AI-powered phishing, ransomware-as-a-service, and supply-chain attacks.

SOFTSERVE'S AI-ENABLED SOC SERVICES

01

AI-DRIVEN ENTERPRISE CSOC

Accurate threat identification, false positives reduction, expanded attack-type coverage, reduced analyst time.

02

24/7 CSOC-AS-A-SERVICE

Continuous environment monitoring with assessment and improvement planning for 24/7 threat detection and response.

03

SECURE SDLC SERVICES

Identify and fix security issues in your applications at early development stages, before they reach production.

04

VULNERABILITY MANAGEMENT

Find vulnerabilities and security gaps; deliver a structured remediation roadmap for a strengthened security posture.

05

SECURITY AWARENESS

Improve organizational resilience through phishing simulations and training that minimize human-error risk.

06

ESDLC / CONFIGURATION MANAGEMENT

Embed secure-by-design practices across the product lifecycle; Configuration Management ensures controlled change.

OUTCOMES

30 min	Threat detection and MTTR
40%	Lower false-positive rate
95%+	Coverage across infrastructure and apps
30-50%	Fewer vulnerabilities during dev lifecycle
20-50%	Log volume optimization
+20-40%	Improvements to Tier 3 efficiency

ENGAGEMENT TIMELINE

SCOPING

2–3 Weeks

Scoping and discovery to define security objectives and engagement boundaries.

→

SOW PREPARATION

1 Week

Statement of Work preparation aligning deliverables, timelines, and success criteria.

→

EXECUTING

Ongoing

Ongoing execution with continuous monitoring, reporting, and optimization.

CONTACT OUR TEAM TO GET STARTED

"Modern security operations must improve detection, response, and vulnerability management without expanding security teams".

Michael Kropyva — AVP, Infosec, SoftServe
mkrop@softserveinc.com