XENEX
Agentic SOC-as-a Service

THE AGENTIC SOC PLAYBOOK

Enterprise-level Agentic SOC. Built for the middle market.

A practical guide for business leaders on how AI intelligence, millisecond detection, and autonomous response are redefining security for SMB and middle market organizations.

40ms
AI-powered threat detection

10s
Autonomous response initiated

10.8M
Events processed per hour

THE CYBERSECURITY CRISIS

01

SMBs are the most targeted, least resourced businesses in cyber.

Mid-market businesses hold exactly the kind of data attackers want — customer PII, financials, intellectual property — but rarely have a dedicated security operations team watching the perimeter around the clock. The math of traditional security doesn't work at this scale.

$4.88M

Average cost of a data breach in 2024 — up 10% year over year (IBM).

267 days

Average breach lifecycle: 194 days to identify, 73 more to contain (IBM).

$2.22M saved

Organizations using AI & automation cut breach costs and detect threats 98 days faster (IBM).

43%

Of all cyberattacks target small and mid-sized businesses (Accenture).

70–90%

Of SOC alerts are false positives, burning analyst time daily (IBM, Verizon).

4.8M

More cybersecurity professionals needed globally than exist today (ISC2).

Why you're the target, not the exception

You carry the same compliance obligations as much larger organizations — HIPAA, PCI, FERPA, CMMC, NIST — but meet them with roughly a tenth of the staff. That makes you the soft entry point into a larger supply chain.

WHY TRADITIONAL SOC MODELS ARE BROKEN

02

More tools haven't meant more protection.

Most organizations juggle a patchwork of vendors, alerts, and promises that still leave them exposed. Each additional tool adds another stream of alerts — and another layer of noise, not clarity.

69% vs 57%

Alert-fatigue rate for teams running 10+ security tools, vs. teams running under 5 (Orca Security).

1 at a time

The bottleneck in a traditional SOC isn't technology — it's human triage, working the queue one alert at a time.

Three tools, three blind spots

SIEM alone

Is just log collection. It tells you what happened — not what to do about it.

EDR alone

Sees only endpoints — blind to network, cloud, and identity activity happening around it.

MDR

Adds human eyes to the process — but those humans are still working through the same slow queue.

The fix isn't another tool.

It's a different operating model — one where correlation and response don't wait in a human queue. See Chapter 3.

WHAT IS AGENTIC SOC?

03

Not a copilot. A digital analyst.

A copilot assists a human — it needs constant prompting. Agentic AI acts autonomously to complete entire workflows, from alert interpretation to containment, emulating the process a skilled analyst would follow, without waiting in a queue.

Copilot

- Assists a human, one prompt at a time
- Speeds up individual tasks
- Still depends on a person to drive every step
- Doesn't remove the triage bottleneck

Agentic AI

- Acts autonomously across the full workflow
- Runs a hypothesis engine across every domain at once
- Involves a human only for high-value decisions
- Removes the bottleneck instead of speeding it up

29 min

Average adversary breakout time in 2026 — as fast as 27 seconds in the fastest observed case (CrowdStrike 2026 Global Threat Report).

When attackers move at machine speed, a defense model built around human triage queues isn't just inefficient — it's structurally outmatched. That's the case for an agentic model: detecting anomalies in milliseconds and initiating response in seconds, because there's no queue to wait behind.

INSIDE XENEX AGENTIC SOC-AS-A-SERVICE

04

Speed, with a human backstop.

"Confidence through clarity. Protection through partnership." XeneX doesn't just monitor — we act before you have to. While competitors push every alert to your IT team, our world-class team validates every AI-reported incident so you only see what's actionable.

AI Detects

Anomaly identified across endpoint, network, cloud, and identity signals.

Autonomous Containment

Isolate endpoint, disable account, or block IP — automatically.

Human Validation

Our analysts review, investigate, and correlate every AI-reported incident.

You Get Answers

One validated incident, with context, impact, and remediation already underway.

700+ connectors

Across cloud (Azure, AWS, M365), on-prem, and hybrid environments — feeding a single pane of glass.

Zero breaches

In over a decade of client history — with weekly summaries, monthly executive reviews, and a 1-hour SLA on critical incidents.

06

BUILT FOR MIDDLE MARKET REALITY

Sized for organizations with 200–10,000 employees.

Rated 10/10 on TrustRadius for Mid-Size Companies and 5.0/5 on G2 — because the platform is designed for your reality, not scaled down from an enterprise product.

Focus on core competency

You're a school, clinic, manufacturer, or law firm — not a security firm. We become your cybersecurity extension.

No hiring or retaining

A true 24/7 SOC needs 8–12 analysts — $1M+ in salary alone. We deliver full-stack protection at predictable cost.

True 24/7/365 protection

Attackers don't work 9-to-5. Our SOC never sleeps — continuous monitoring, not just business hours.

No in-house SME needed

Your IT generalists manage helpdesk to infrastructure. We provide decades of hands-on cybersecurity expertise on demand.

Insurance & compliance ready

Meet cyber insurance prerequisites and regulatory needs — HIPAA, PCI, FERPA, CMMC, NIST — with documentation ready to go.

07

PLATFORM VS. SERVICE · WHAT YOU GET

Buy the outcome, not another tool to manage.

The rest of the market sells you a platform and expects you to run it — buy tools, hire staff, integrate, tune, and hope. XeneX flips that: we deliver the entire outcome as one managed service.

> "XeneX delivers what every CIO hopes for — a true turnkey partner."
>
> **Alan Shamma, CIO · Paige**

> "Owns their technology end to end... the cleanest architecture we've seen."
>
> **Kirby Winters, Managing Partner · TechCXO**

> "XeneX gives schools enterprise-grade protection they can actually afford."
>
> **Marc Netka, Chairman · STS Education**

Comprehensive cybersecurity, simplified

- 24/7 monitoring with AI-driven detection (40ms) and autonomous response (10s)
- Unified dashboard with full network and endpoint visibility
- Vulnerability scanning, asset discovery, intrusion detection, log retention
- 700+ integrations — works with the tools you have today
- Phishing training, browser isolation, and biometric MFA available
- Weekly summaries, monthly executive reviews, MITRE ATT&CK mapping
- Scalable across cloud, on-prem, or hybrid environments
- Built to meet cyber insurance and compliance requirements

READY WHEN YOU ARE

Ready for cybersecurity you can finally trust?

We offer a proof-of-value engagement so you can experience the XeneX platform in your own environment before committing to anything. Most clients are fully configured within four hours.

VISIT

xenexsoc.com

EMAIL

sales@xenexSOC.com

ASK ABOUT

The Webinar Bundle

XENEX
Agentic SOC-as-a Service

Unshakeable. Accountable. Always On.