XYBERTEQ INNOVATIONS

Xyberteq Innovations

Company Brief

Xyberteq Innovations is a Malaysian Cybersecurity and AI technology company specializing in unified security operations, cyber resilience, and sovereign AI models designed for regulated and high-security environments.

- Established 2025
- Kuala Lumpur

Xyberteq Innovations Sdn Bhd (Formerly known as Peranti Technologies Sdn Bhd)
Company No: 201701035190 (1249361-M)

Address: No 14, Persiaran Damansara Endah, Damansara Heights, 50490 Kuala Lumpur, Malaysia
Tel: +603 2083 0133

Xyberteq Innovations

Certifications & Licenses

- SSM Registered
- Nacsa Cybersecurity License
  - Pentest
  - SOC
- ISO 27001
- *ISO 9001*
- *SOC II Type II*
- GDPR Compliant

In Progress

- *PDPA*
- *ISO 42001*
- *CREST*

Sentient Spire QCS Platform

Executive & Board Brief

An AI-powered SOC subscription that reduces cybersecurity risk, restores executive visibility, and lowers security operating cost — without exporting your data.

Cybersecurity is now a resilience issue

Boards need clear answers—fast.

The question is no longer “Do we have tools?”
It’s “Can we see risk early, act fast, and prove control?”

- Reduce the likelihood and impact of cyber incidents
- Maintain operational continuity during crises
- Demonstrate governance and control with evidence
- Simplify the operating model and reduce cost

Why leaders replace traditional SOC Vendors

Activity is not assurance. Tools are not outcomes.

Slow clarity in a fast crisis

Alerts arrive but understanding and action lag—when minutes matter.

High cost with unclear impact

Multiple vendors and overlapping tools dilute accountability and inflate spend.

Weak assurance for boards

Reporting is technical and fragmented—hard to translate into governance evidence.

QCS replaces fragmentation with a single operating picture, a single accountability layer, and a single source of truth for assurance.

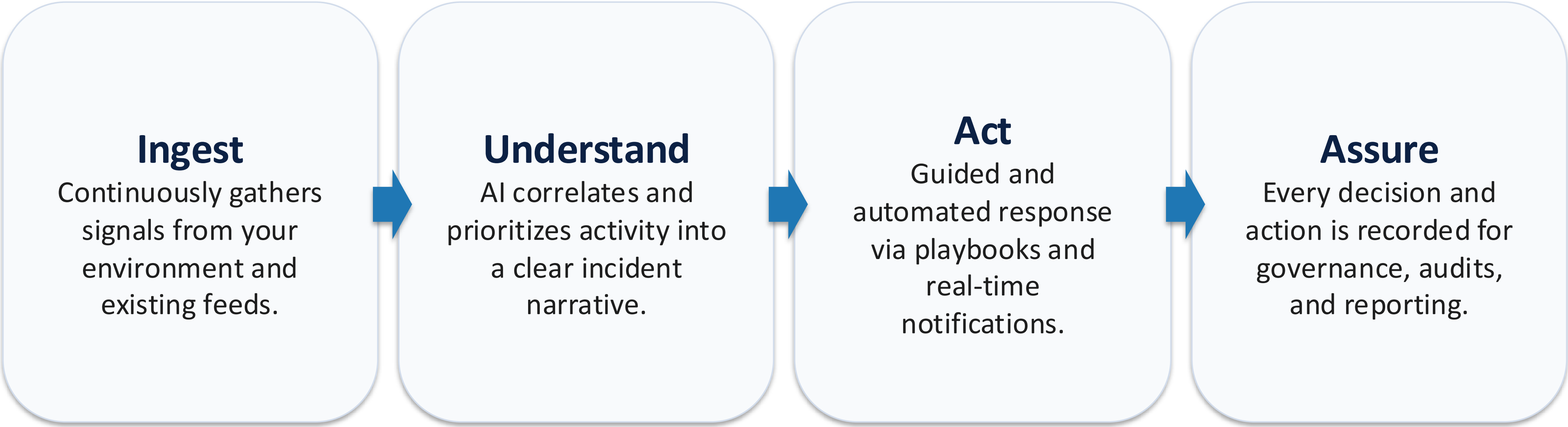
What Sentient Spire QCS is

A unified AI-driven security operations layer.

- Continuously ingests security signals across your business
- Converts noise into clear, prioritized incidents
- Guides and automates response with explainable recommendations and playbooks
- Produces board-ready assurance—incident narratives, actions taken, and evidence trails
- Keeps sensitive data inside your environment via proprietary (patent-pending) AI models

How it works

Ingest → Understand → Act → Assure



Ingest
Continuously gathers signals from your environment and existing feeds.

Understand
AI correlates and prioritizes activity into a clear incident narrative.

Act
Guided and automated response via playbooks and real-time notifications.

Assure
Every decision and action is recorded for governance, audits, and reporting.

AI-led operations that save time

From alerts to containment—without the manual “glue work”.

What the AI does automatically

- Auto-ingests signals from your existing security stack and environments
- Detects and correlates related activity into one coherent incident
- Explains what matters and why—so decisions are faster and more confident
- Recommends and executes response through approved playbooks

What you gain

- Faster understanding and containment when minutes matter
- Fewer false positives and fewer escalations
- More consistent outcomes under pressure
- Less dependence on vendor analysts to interpret events

Agentic AI Advisor

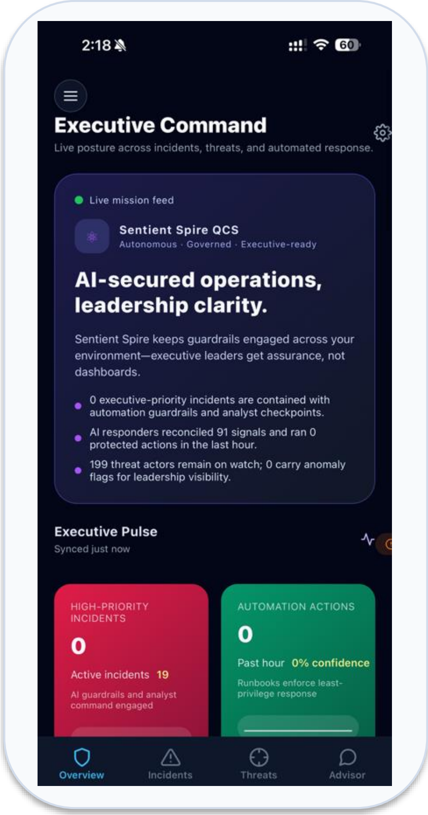
Ask. Decide. Act—with governance and traceability.

A secure, role-aware chatbot that helps mitigate incidents and provides executive-grade advisory—limited to the AI models and data inside your environment.

- “Are we under attack right now?” → concise executive answer with the supporting incident narrative
- “What’s the likely business impact and what should we do next?” → prioritized recommendations
- “What changed in our risk this week?” → leadership-ready summary
- “Show me what we can prove to auditors.” → evidence-based assurance views
- Initiate or assist with pre-approved response steps (playbooks) while keeping leadership informed

Executive visibility—anywhere

Mobile app extends the dashboard for boards and C-suite.



2:18

Executive Command

Live posture across incidents, threats, and automated response.

Live mission feed

Sentient Spire QCS
Autonomous · Governed · Executive-ready

AI-secured operations, leadership clarity.

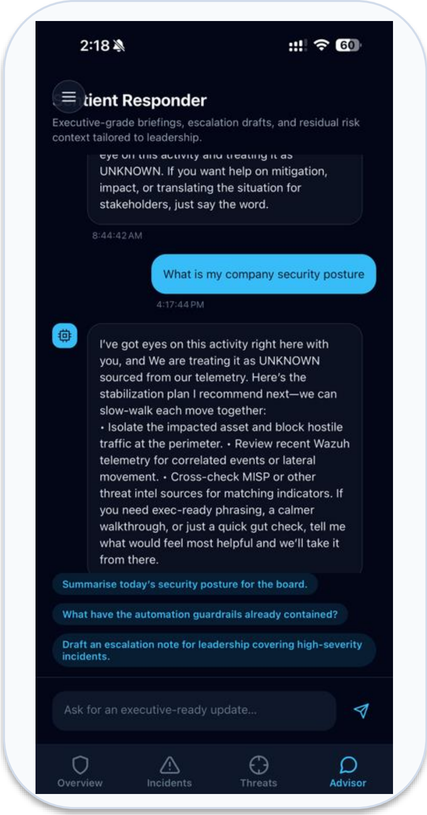
Sentient Spire keeps guardrails engaged across your environment—executive leaders get assurance, not dashboards.

- 0 executive-priority incidents are contained with automation guardrails and analyst checkpoints.
- AI responders reconciled 91 signals and ran 0 protected actions in the last hour.
- 199 threat actors remain on watch; 0 carry anomaly flags for leadership visibility.

Executive Pulse
Synced just now

HIGH-PRIORITY INCIDENTS
0
Active incidents 19
AI guardrails and analyst command engaged

AUTOMATION ACTIONS
0
Past hour 0% confidence
Runbooks enforce least-privilege response



2:18

tient Responder

Executive-grade briefings, escalation drafts, and residual risk context tailored to leadership.

eye on this activity and treating it as UNKNOWN. If you want help on mitigation, impact, or translating the situation for stakeholders, just say the word.

8:44:42 AM

What is my company security posture

4:17:44 PM

I've got eyes on this activity right here with you, and We are treating it as UNKNOWN sourced from our telemetry. Here's the stabilization plan I recommend next—we can slow-walk each move together:
• Isolate the impacted asset and block hostile traffic at the perimeter. • Review recent Wazuh telemetry for correlated events or lateral movement. • Cross-check MISP or other threat intel sources for matching indicators. If you need exec-ready phrasing, a calmer walkthrough, or just a quick gut check, tell me what would feel most helpful and we'll take it from there.

Summarise today's security posture for the board.

What have the automation guardrails already contained?

Draft an escalation note for leadership covering high-severity incidents.

Ask for an executive-ready update...

- Real-time risk posture and notable exposure changes
- Incident notifications and executive summaries on the move
- Clear view of what actions are underway and progressing
- Board-ready snapshots without waiting for weekly reporting

Data sovereignty and control

Security telemetry stays where you control it.

- Proprietary (patent-pending) AI models operate within your environment
- No need to export sensitive security data for analysis
- Supports data residency expectations and regulated-industry governance
- Reduces third-party exposure while retaining full operational insight

Your questions, incident context, and operational data remain inside the system—answers are limited to what your environment provides.

Lower budgets through consolidation

Automation + vendor simplification—without reducing protection.

What you can retire or reduce

- SOC/MDR retainers and bolt-on services
- Overlapping point tools for detection, triage, and reporting
- Integration and maintenance overhead across vendors
- Manual analyst effort spent interpreting noise

What you standardize

- One operating picture across the organization
- One subscription aligned to coverage and outcomes
- Consistent response through approved playbooks
- Clear assurance evidence for board and audit

What leadership gets

Clear value by stakeholder

- Chairman & Board: clarity on risk, fewer unknowns, defensible oversight backed by evidence
- CEO / MD: improved resilience, reduced incident impact, simpler accountability
- CFO: fewer vendors, lower run-rate, reduced hidden costs, predictable subscription spend
- CISO & Security leadership: faster triage, consistent response, stronger assurance reporting
- Risk & Compliance: audit-ready trails, policy evidence, exportable summaries

Q&A

Thank you

Contact us @ info.sec@xyberteq.com
https://xyberteq.com