ELEZAR

SOL BY ELEZAR · AUTONOMOUS THREAT OPERATIONS PLATFORM

Scale threat-led services with your existing team.

Expand managed threat hunting and CTI advisory across more customers without scaling specialist workload.

Scale existing services or launch new ones with the team you already have.

elezar.io

Threat-led services, without the traditional delivery burden.

Managed threat hunting and CTI advisory have traditionally depended on specialist expertise, customer-by-customer context and repeated manual execution.

Whether you're scaling an existing service or launching a new one, Sol changes how that work gets delivered.

THE OPPORTUNITY WITH SOL

New revenue

Launch new threat-led services or expand what you already offer.

Scale

Deliver across more customers with your existing team.

Better economics

Automate more of the specialist work required per customer.

Your service. Your customers. Powered by Sol.

Sol operates behind your service. You retain the customer relationship, service model and commercial ownership.

One operating layer across your customer base

Sol Autonomous Threat Operations Platform

STRUCTURED THREAT CONTEXT

TTPs · Victimology · Procedures · Actors · Malware · Campaign · IoCs

THREAT PROFILE

Matches threats to each customer's environment, industry, geography and technology.

AUTONOMOUS OPERATIONS

Hunt	CTI / Advisory	Detection Engineering (Soon)	Attack Simulation (Soon)	Mitigation (Soon)

YOUR CUSTOMER ENVIRONMENTS

Customer A	Customer B	Customer C
SIEM · EDR · Cloud · Apps	SIEM · EDR · Cloud · Apps	SIEM · EDR · Cloud · Apps

CLOUD-BASED · CROSS-STACK · WORKFLOW-INTEGRATED · MULTI-CUSTOMER OPERATIONS

Sol is designed to help MSSPs scale threat-led services across their customer base by standardising delivery across the tools their customers already use.

It continuously processes global threat reporting, structures each threat into actionable context, and matches it against each customer's technology, industry and geography. When a relevant threat is identified, Sol autonomously runs threat-led operations across customer environments, beginning with threat hunting and CTI advisory.

The result is more scalable services, better unit economics and stronger outcomes for your customers.

Benefits of managed threat hunting at scale.

Sol turns relevant threat intelligence into customer-specific, hypothesis-driven hunts across each customer's security stack. Fully autonomous, or with a human in the loop.

TRADITIONAL MSSP HUNTING

Analyst-heavy and manual
Significant time spent researching threats and designing hunts.

Hunts constrained by capacity
Limited number of hunts driven by the availability of specialist analysts.

Customer-by-customer execution
Repetitive work to assess relevance, build hunts and report for each customer.

Coverage varies
Dependent on analyst expertise, time and the tools they have access to.

VS

SOL-POWERED DELIVERY

Latest adversary tradecraft
Threat-led hunts based on the newest adversary activity and procedures.

Customer-specific relevance
Threat profiles ensure hunts focus on what matters to each customer's environment.

Cross-stack execution
Runs across the customer's existing stack: SIEM · EDR · Cloud · Applications and more.

Minutes to evidence
From threat report to executed hunt in minutes, not days.

10 minutes

From threat report to customer-specific hunt.

24/7

Threat processing and hunt generation continue outside analyst hours.

More customers per analyst

Expand managed hunting coverage without scaling specialist effort at the same rate.

THE OUTCOMES THAT MATTER

Know what matters
Focus on the threats relevant to each customer, not the noise.

Broader customer coverage
Operationalise more relevant adversary tradecraft across more customer environments.

Lower delivery overhead
Reduce manual research, hunt design and reporting so analysts focus on investigation and response.

Benefits of managed CTI & advisory at scale.

Sol turns global threat reporting into customer-specific intelligence and advisory across your customer base.

TRADITIONAL MSSP CTI / ADVISORY

Analyst-heavy research
Teams manually read, correlate and rewrite intelligence for customers.

Generalised outputs
The same intelligence is often distributed broadly, with limited customer context.

Periodic delivery
Advisory depends on analyst capacity and reporting cycles.

Hard to scale customer-by-customer
Every additional customer increases research, tailoring and reporting workload.

VS

ELEZAR-POWERED DELIVERY

Continuous and automated
24/7 processing of new threat reporting and relevance assessment.

Customer-specific relevance
Threat profiles determine what matters based on each customer's technology, industry, geography and priorities.

Weekly, or at your chosen cadence
Relevant advisory is prepared automatically on the cadence of your service.

Repeatable across many customers
One intelligence workflow supports tailored advisory across the customer base.

24/7

Continuous threat processing and relevance assessment.

Minutes, not days

From new threat reporting to customer-specific intelligence and advisory.

On-brand

Deliver advisories in your service branding and customer-ready format.

THE OUTCOMES THAT MATTER

More relevant advisory
Give each customer intelligence that reflects their environment, not generic threat reporting.

Lower analyst overhead
Reduce the manual research, correlation, rewriting and reporting required to run an advisory service.

Stay current
Keep customers informed as the threat landscape changes, not just at the next reporting cycle.

Sol AI for threat operations.

Investigate threats, analyse customer context, generate operational outputs and run expert security workflows from one evidence-grounded AI interface.

Evidence-grounded answers

Responses are tied to underlying intelligence, findings and customer data.

Report generation in chat

Turn intelligence and findings into hunts, advisories and other customer deliverables through natural language.

Customised, on-brand output

Tailor scope, tone, structure and technical depth while automatically applying your branding and report format.

Faster from insight to delivery

Move from question to evidence to customer-ready output in the same workflow.

Built-in expert workflows in Sol AI

Use ready-made workflows to accelerate common threat operations.

Table-top exercises	Generate threat-informed scenarios tailored to a customer's environment and risk profile.	**Outcome:** Faster preparation for customer exercises.
Red / purple team scenarios	Turn current adversary tradecraft into realistic validation scenarios.	**Outcome:** Reduce manual scenario design and validation.
Detection analytics	Analyse detection coverage and identify gaps and opportunities from threat intelligence and findings.	**Outcome:** Prioritise detection improvements that matter most.
Attack simulation signature creation	Translate adversary procedures into reusable simulation logic or signatures.	**Outcome:** Move faster from intelligence to validation at scale.

More capability for your analysts. Faster delivery for your customers.

Sol AI gives your team the context, workflows and automation to deliver more value, without adding more headcount or complexity.

Customer-specific intelligence that drives better outcomes.

From deep, customer-specific threat profiles to a continuously updated intelligence library, Sol gives your analysts the context and coverage to stay ahead.

1. Threat Profiling

SELLABLE SERVICE

A living, customer-specific view of the threats that matter most.

Customer-specific relevance

Profile threats against each customer's industry, geography, technology stack and risk context.

- Relevant adversaries, campaigns and TTPs
- Mapped to customer exposures and priorities
- Focused on what matters, not everything

Continuously maintained

Profiles evolve as new reporting and adversary activity emerges.

- 24/7 monitoring of global threat reporting
- Automatic updates and enrichment
- Always current, no manual refresh

Sellable service

Offer profiling as a standalone assessment or as part of hunting and advisory services.

- Standalone customer value
- Easy to package and price
- Strengthens your service portfolio

Faster analyst delivery

Reduce the manual work of collecting, structuring and keeping customer context current.

- Pre-structured and prioritised context
- Less time on research and curation
- More time on analysis and action

2. Threat Library

INTELLIGENCE FOUNDATION

Hundreds of hours of threat engineering, built in. Sol continuously collects, structures, maps and maintains threat intelligence so your team doesn't have to.

Continuously updated

New threat reporting processed 24/7 and added to the library.

Source-traceable

Every entry linked to original sources and supporting evidence.

Adversary Context

Adversaries, campaigns, malware, TTPs, procedures, victimology and more.

Zero overhead

No TIP infrastructure to deploy, operate or maintain.

Know what matters to each customer – and keep it current.

Better prioritisation. Faster delivery. Stronger outcomes.

ELEZAR

See Sol scale your services.

Talk to us →