AI PENETRATION TESTING

Sigmix Red

In a new era of AI-driven hacking, you need AI-native defense.

Attackers now wield autonomous AI that finds and chains weaknesses at machine speed. Sigmix Red answers in kind — an AI red-team operator **built from the ground up** to think like an attacker across your entire authorized surface. AI-first, not a legacy scanner with AI bolted on.

Your authorized surface → the AI operator reasons & chains → proven paths, ranked, with evidence

AUTHORIZED ENGAGEMENTS ONLY · IN-KINGDOM

NCA ECC-2 ALIGNED · IN-KINGDOM & ON-PREM · HUMAN-IN-THE-LOOP

WHY NOW

The attack side already went autonomous. The defense has to keep pace.

Through 2025 and 2026, offensive AI stopped being a demo. Publicly disclosed incidents show agent systems running end-to-end — reasoning, adapting to errors, and generating thousands of actions faster than any human team could review. An annual pen test taken once a year is no longer the right unit of measurement.

17,000+

individual actions an autonomous agent generated across one disclosed 2026 intrusion — reconstructed only after the fact.

~31s

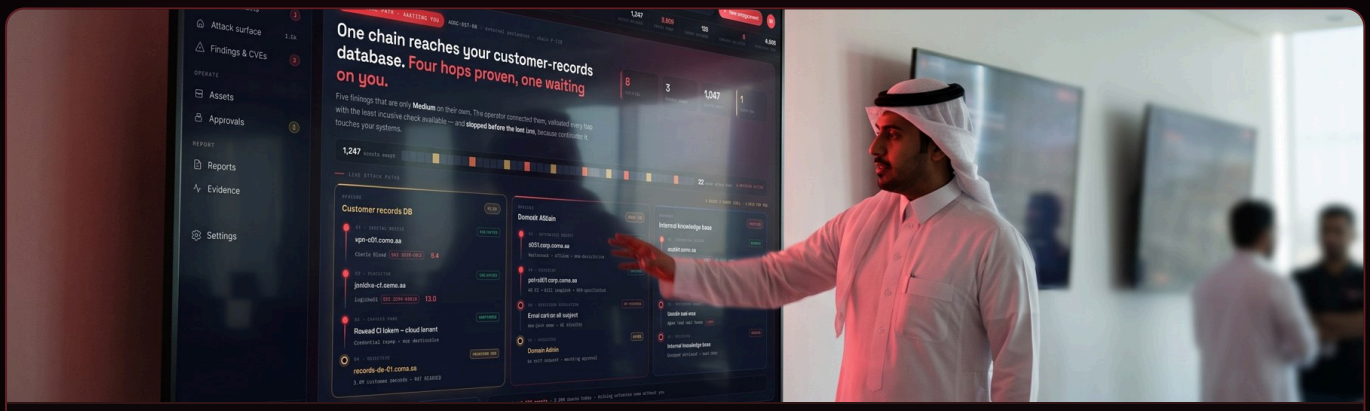
for a documented agentic operation to recover from its own failure and keep going. The speed of the loop is the story.

1 → many

agentic tooling lowers the skill and cost barrier: one operator can now drive activity across many organisations at once.

Annual pen test ≠ **Always-on operator**

SNAPSHOT · ONCE A YEAR — CONTINUOUS · MACHINE-SPEED



A modern security operations centre — the tempo the defenders now have to match.

> The 2026 figures above reflect publicly reported agentic-attack incidents, reconstructed after the fact. They are cited only as context — Sigmix Red is a defensive, authorized-testing product.

AI-FIRST, BY DESIGN

AI attacks need an AI defender.

The best modern defences — EDR, exposure scanners, SIEM — are superb at what they have seen before. But an autonomous attacker composes novel, multi-step paths in real time, faster than any signature or rule was written for. Sigmix Red meets it the only way that scales: an AI that reasons about your specific environment, the way the attacker's does.

SIGNATURES & HEURISTICS

Strong at the known.

- ✕ Matches a fixed list of known signatures — blind to anything novel or chained.
- ✕ Dumps thousands of isolated issues; a human has to guess which ones connect.
- ✕ Runs quarterly or once a year — stale the moment your surface changes.
- ✕ Has no idea your own chatbots and copilots are now an attack surface.

SIGMIX RED · AI-NATIVE

An operator that reasons.

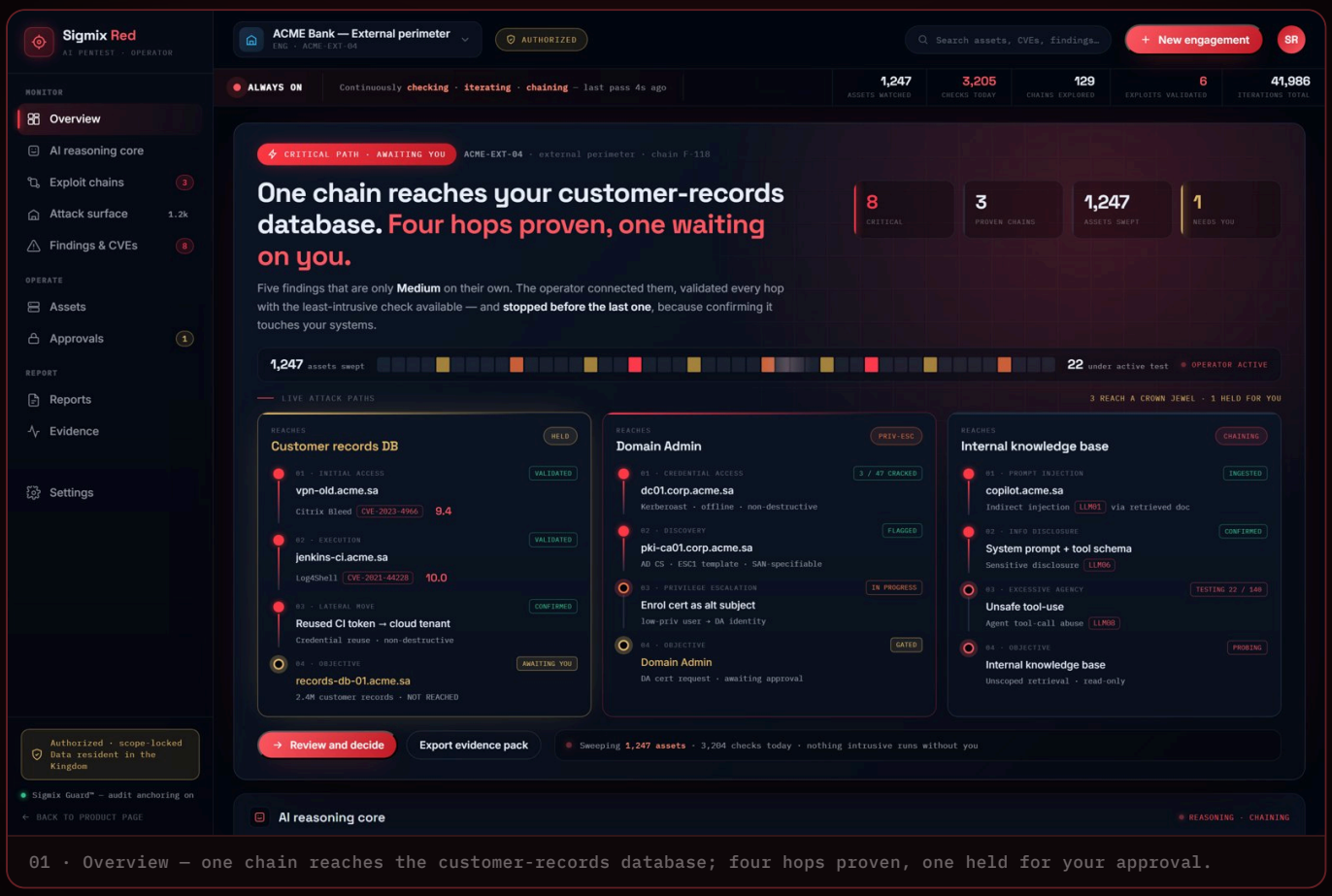
- ✓ **Reasons about your environment** — not a signature list, an attacker's mental model of it.
- ✓ **Chains weaknesses** into the two or three paths that actually reach something that matters.
- ✓ **Always on** — continuously checking, iterating and re-chaining as things change.
- ✓ **Red-teams your AI too** — the chatbots, copilots and agents legacy tools can't even see.

AI-native — an operator that models your specific environment, not a rulebook.

INSIDE THE CONSOLE

Everything in the box — one operator console.

Five live views your team works from: the operator overview, proven exploit chains, the discovered attack surface, ranked findings, and the human approval gate. One place to run an engagement end to end.



01 · Overview — one chain reaches the customer-records database; four hops proven, one held for your approval.

01 · Overview

The operator's command view — one proven chain to your crown jewels, held at the gate for you.

02 · Exploit chains

Every proven path, ranked — the two or three that actually reach something that matters.

03 · Attack surface

Everything reachable, mapped continuously — the sprawl you forgot you had.

04 · Findings & CVEs

Ranked, de-duplicated findings, each backed by a reproducible path — not a 400-page export.

05 · Approvals

The human gate — nothing intrusive runs until your operator says go.

WHAT IT IS

A red team that never clocks off.

Point Sigmix Red at a scope you own and are authorized to test. It behaves like a patient, tireless operator: enumerating your surface, reasoning about how pieces connect, and — only where you allow it — safely confirming that a path is real. Then it writes it up in plain language.

Continuous, not once a year

It re-tests every time your surface changes, so drift is caught in days rather than at the next audit.

Chains, not checklists

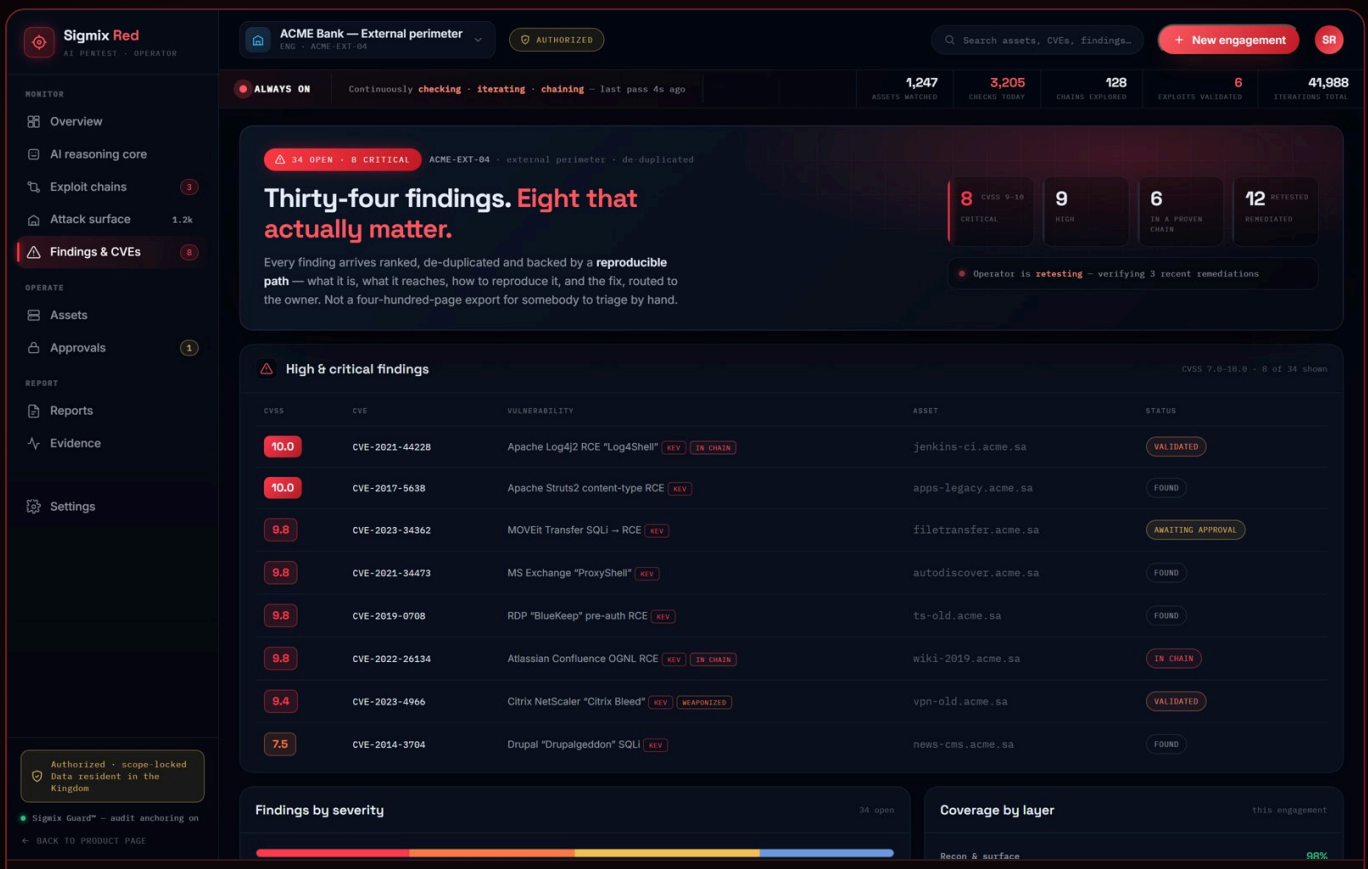
Scanners list issues; Red connects them into the two or three paths that actually reach something that matters.

Evidence, not noise

Every finding arrives ranked, de-duplicated, and backed by a reproducible path — not a 400-page export.

You stay in command

Anything intrusive waits behind an explicit human approval gate. Nothing destructive runs by default.

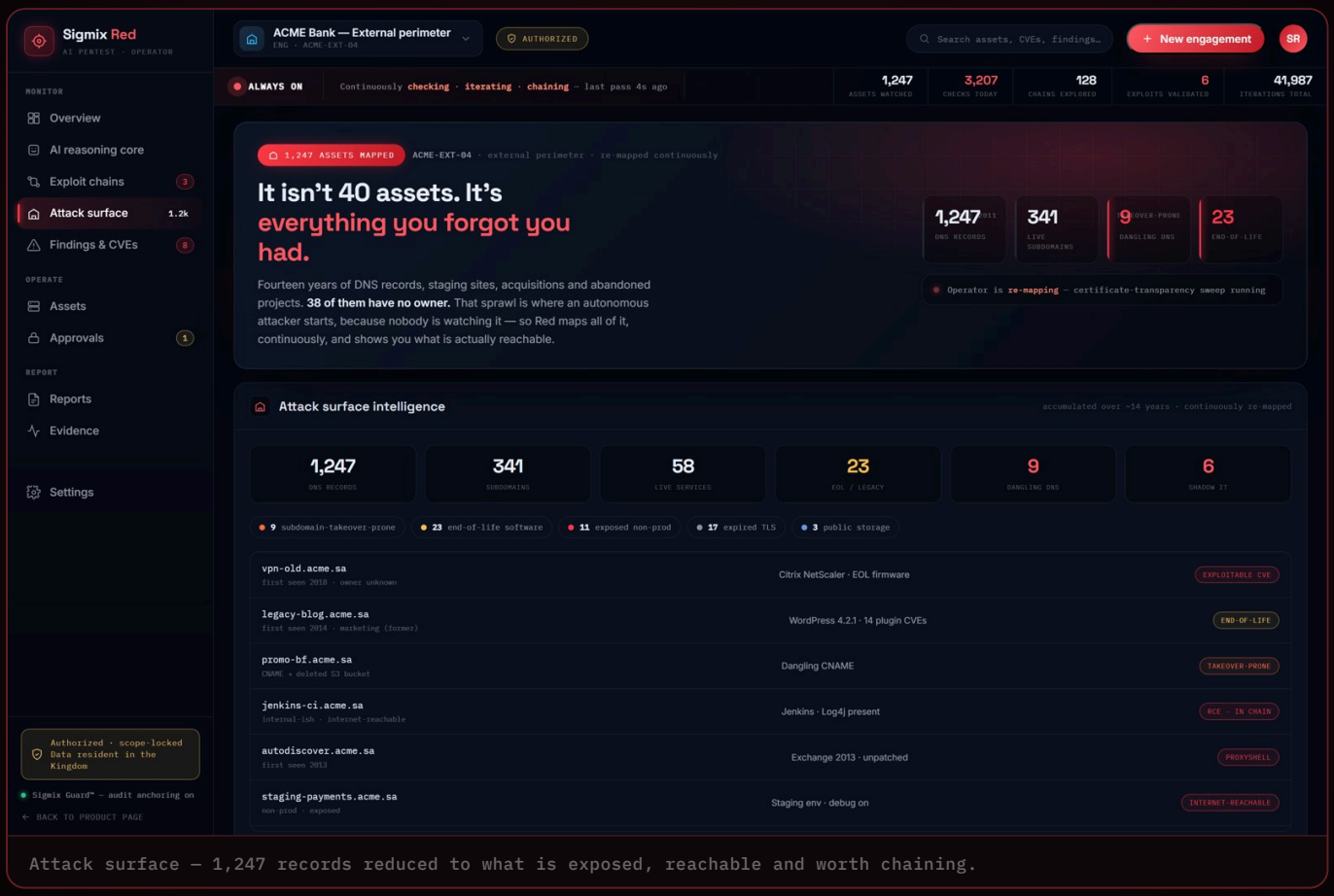


Findings & CVEs — thirty-four findings, ranked and de-duplicated, each backed by a reproducible path.

YOUR REAL ATTACK SURFACE

It’s not 40 assets. It’s everything you forgot you had.

A big organisation accumulates a decade of DNS records, staging sites, acquisitions and abandoned projects. That sprawl — the dangling records, the end-of-life servers nobody owns — is exactly where an AI attacker starts. Sigmix Red maps all of it, continuously, and shows you what’s actually reachable.



Attack surface — 1,247 records reduced to what is exposed, reachable and worth chaining.

The forgotten estate

Dangling DNS, staging clones, end-of-life hosts and shadow IT — surfaced and attributed, not left for the attacker to find first.

Reachable, not theoretical

Mapped from an outsider’s vantage so you see what is genuinely exposed, separated from what is fenced or internal.

Continuously, not once

Re-run as your surface changes, so a new subdomain or a forgotten record is caught in days — not at the next annual test.

HOW IT WORKS

A disciplined loop — with the brakes wired in.

Every engagement runs the same controlled cycle. The two points where the operator could touch your systems are guarded by explicit human approval, and every action it takes is written to a tamper-evident audit trail.

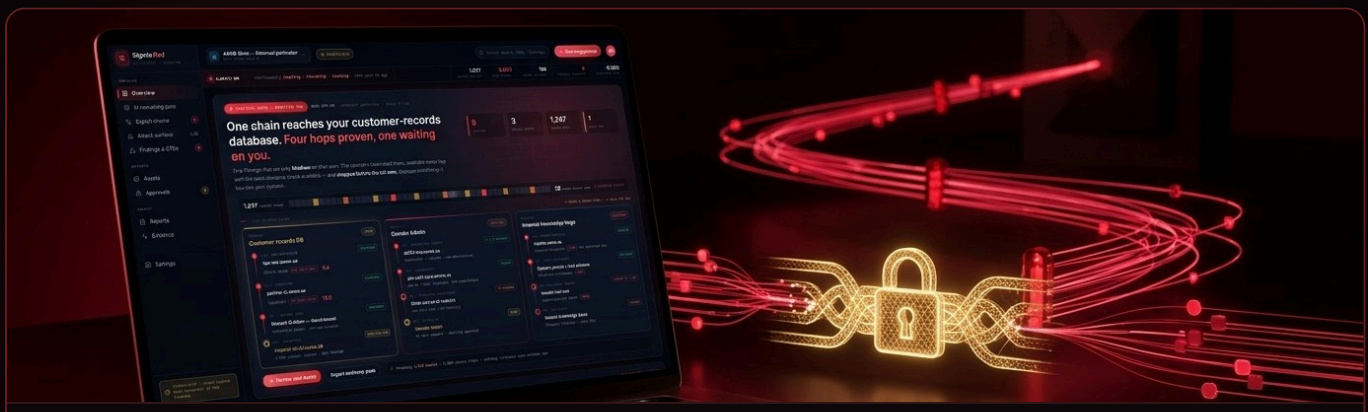
01 **Scope & authorize**
Every engagement starts from a signed scope you own. Targets outside it are refused, not attempted.

02 **Discover & map**
The operator enumerates your real, reachable surface — domains, services, the forgotten sprawl.

03 **Reason & chain**
It models how weaknesses connect and composes the few multi-step paths that actually reach something.

04 **Prove — at the gate**
Least-intrusive validation only, and only where you allow it. Intrusive steps pause for human approval.

05 **Report with evidence**
Ranked findings, each with a reproducible path, written to a tamper-evident audit trail.



The approval gate — the operator stops and asks before anything intrusive runs.

> Two gates, always human: nothing intrusive runs without an explicit operator go-ahead, and nothing destructive runs by default.

RULES OF ENGAGEMENT

Sigmix Red only ever tests what you own and have authorized.

It is a defensive tool for security teams and their approved partners. It is not sold for, and will not run against, systems you do not control or have not been permitted to test. Scope, consent and oversight are enforced by the product — not just promised in a contract.

Written authorization

Every engagement starts from a signed scope. Targets outside it are refused, not attempted.

Human approval gates

Anything intrusive pauses for an explicit operator go-ahead. Nothing destructive runs by default.

Non-destructive by default

Least-intrusive validation. No data is exfiltrated, no service is knocked over to prove a point.

Full audit trail

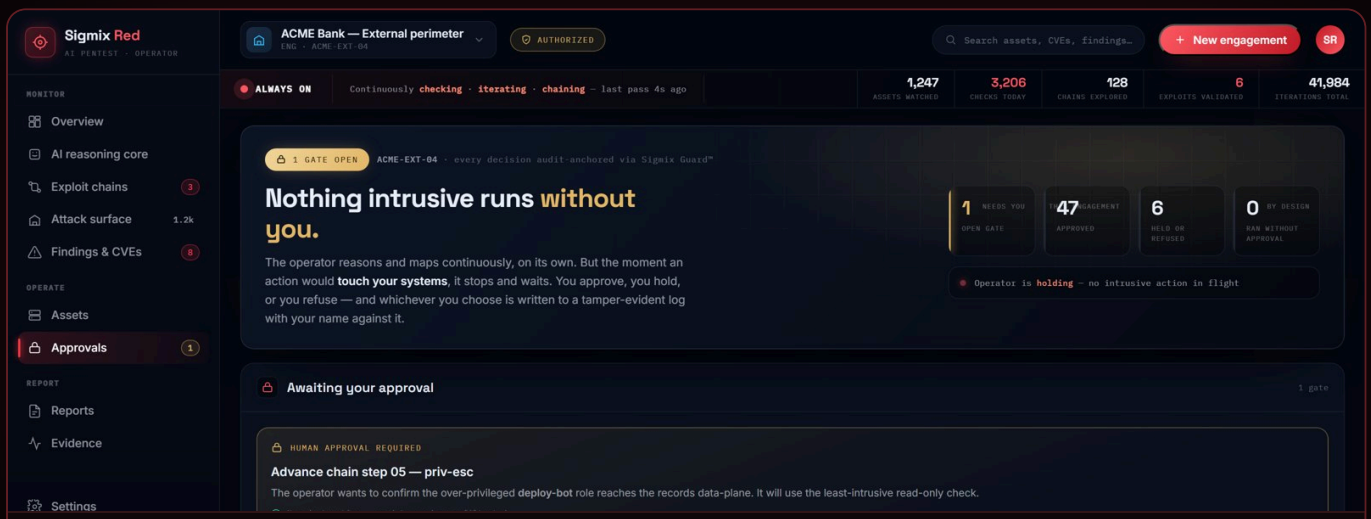
Every action the operator takes is logged to a tamper-evident anchor via Sigmix Guard™.

In-Kingdom & on-prem

Runs on a sealed appliance in your building or in-Kingdom KSA Cloud. Findings never leave your environment.

Aligned to your frameworks

Engagements map to NCA ECC-2, SAMA CSF and PDPL obligations, with evidence your auditors can use.



Approvals — every intrusive step waits here for an explicit human go-ahead.

WHERE IT RUNS

Deploy it the way your rules require.

Sigmix Red fits your security posture, not the other way around — a sealed appliance in your own building, an in-Kingdom managed cloud, or governed by Sigmix Guard™. Wherever it runs, your surface, findings and evidence stay under your control.

SEALED ON-PREM

Your own rack

Red runs on a sealed Sigmix appliance inside your data centre. Nothing about your weaknesses ever leaves the building.

`0 bytes egress`

IN-KINGDOM CLOUD

KSA Cloud

Prefer managed? Run Red in an in-Kingdom, data-resident environment — the same operator, hosted on Saudi soil.

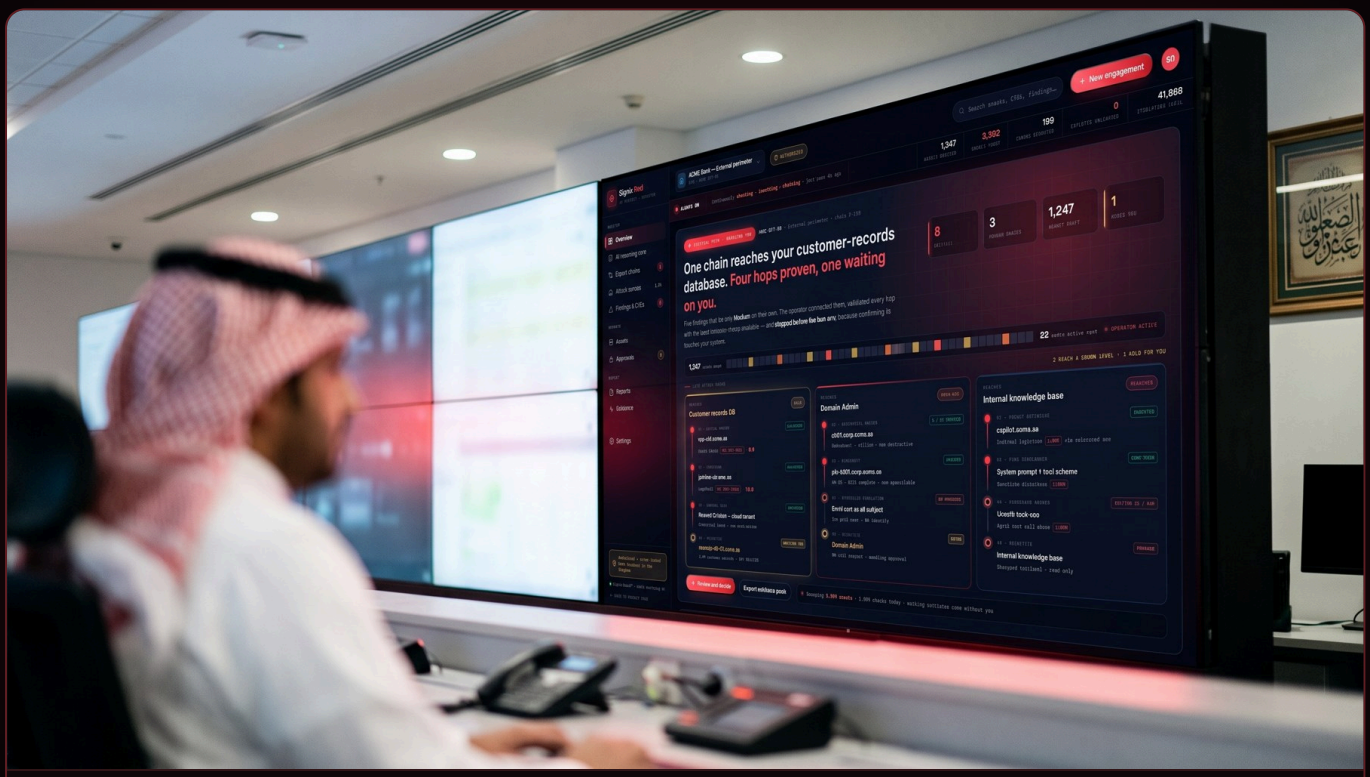
`Resident in the Kingdom`

GOVERNED

Under Sigmix Guard™

Every operator action passes the same independent enforcement layer that guards the rest of the platform — scrub, then anchor.

`Tamper-evident audit`



One operator, or a wall of them — Sigmix Red runs sealed on your own metal or in an in-Kingdom managed cloud.

GET AHEAD OF IT

Find the path before someone else does.

Bring us your scope and your obligations. We will run a proof-of-concept engagement, show you the two or three paths that actually matter, and hand your team the evidence to close them.

PROOF-OF-CONCEPT · AUTHORIZED & SCOPED

A short, fully-authorized engagement on a scope you own — the fastest way to see the operator find, chain and prove a real path through your surface, with your approval gate in the loop the entire time.

Discuss a POC
Scope a proof-of-concept for your organisation.

See the console
A walkthrough of the operator, live.

Security & evidence
How scope, gates and the audit trail work.

sigmix.sa

EMAIL
contact@sigmix.sa

TELEPHONE
+966 11 525 6806

WEB
sigmix.sa

7229 Innovation Boulevard · Al Aqeeq District · 13519 Riyadh · Kingdom of Saudi Arabia · CR 7054521799 VAT 314836510700003 MISA 24926260339

Sigmix .sa

اختبار الاختراق بالذكاء الاصطناعي

Sigmix Red

في عصرٍ جديد من الاختراق المدفوع بالذكاء الاصطناعي، أنت بحاجة إلى دفاعٍ أصيل الذكاء.

بات المهاجمون يستخدمون ذكاءً اصطناعيًا ذاتيّ التشغيل يكتشف نقاط الضعف ويربطها بسرعة الآلة. ويردّ Sigmix Red بالمثل — مُشغِّل فريقٍ أحمر بالذكاء الاصطناعي، مبنيٌّ من الألف إلى الياء ليفكّر كالمهاجم عبر كامل سطح هجومك المُصرَّح به. الذكاء الاصطناعي أولًا، لا ماسحٌ تقليديّ أُضيف إليه.

سطح هجومك المُصرَّح به ← المُشغِّل يستدلّ ويربط ← مساراتٌ مُثبَتة، مُرتَّبة، بالأدلّة

ارتباطاتٌ مُصرَّح بها فقط · داخل المملكة

متوافق مع NCA ECC-2 · داخل المملكة وداخل مقرّك · بإشراف بشري

الجانب المُهاجِم أصبح ذاتيّ التشغيل بالفعل. وعلى الدفاع أن يواكب.

خلال عامَي 2025 و2026، لم يعد الذكاء الاصطناعي الهجومي مجرّد عرضٍ توضيحي. تُظهر الحوادث المُعلَنة أنظمةَ وكلاءَ تعمل من البداية إلى النهاية — تستدلّ، وتتكيّف مع أخطائها، وتولّد آلاف الإجراءات أسرع من أيّ فريقٍ بشري. لم يعد اختبار الاختراق المأخوذ مرّةً في السنة هو وحدة القياس الصحيحة.

17,000+

إجراءٍ فرديّ ولّدها وكيلٌ ذاتيّ التشغيل خلال اختراقٍ واحد مُعلَن في 2026 — أُعيد بناؤه بعد وقوعه فحسب.

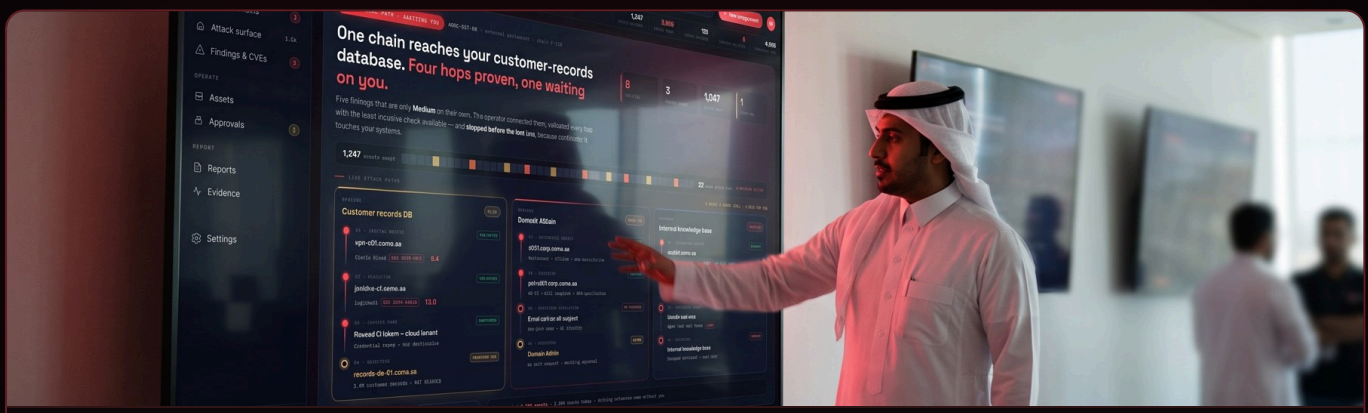
~31s

ليتعافى تشغيلٌ وكيليّ موثّق من فشله ويُكمِل. سرعة الحلقة هي جوهر القصّة.

1 → many

تخفض أدوات الوكلاء حاجز المهارة والكلفة: يستطيع مُشغِّلٌ واحد الآن دفع النشاط عبر مؤسّساتٍ كثيرة معًا.

اختبارٌ سنوي	≠	مُشغِّلٌ دائم العمل
لقطةٌ · مرّة في السنة		مستمرّ · بسرعة الآلة



مركز عمليات أمنٍ حديث — الوتيرة التي بات على المدافعين مجاراتها.

تعكس أرقام 2026 أعلاه حوادثَ هجماتٍ وكيليّة مُبلَّغ عنها علنًا، أُعيد بناؤها بعد وقوعها. وهي مذكورةٌ للسياق فقط — Sigmix Red منتجٌ دفاعيّ للاختبار المُصرَّح به.

هجمات الذكاء الاصطناعي تحتاج مُدافِعًا بالذكاء الاصطناعي.

أفضل الدفاعات الحديثة — EDR وماسحات الانكشاف وSIEM — بارعةٌ فيما رأته من قبل. لكنّ المهاجم ذاتيّ التشغيل يؤلّف مساراتٍ جديدة متعدّدة الخطوات في الزمن الحقيقي، أسرع من أيّ توقيعٍ أو قاعدة كُتبت. ويواجهه Sigmix Red بالطريقة الوحيدة القابلة للتوسّع: ذكاءٌ اصطناعيّ يستدلّ حول بيئتك تحديدًا، كما يفعل المهاجم.

التواقيع والاستدلالات

قويٌّ في المعروف.

- ✕ يطابق قائمةً ثابتة من التواقيع المعروفة — أعمى تجاه كلّ ما هو جديد أو مترابط.
- ✕ يُلقي بآلاف المشكلات المنعزلة؛ ويترك للبشر تخمين أيّها يتّصل بالآخر.
- ✕ يعمل فصليًّا أو مرّة في السنة — يتقادم لحظة تغيّر سطحك.
- ✕ لا فكرة لديه أنّ روبوتات المحادثة والمساعِدات لديك باتت الآن سطح هجوم.

Sigmix Red · أصيل الذكاء

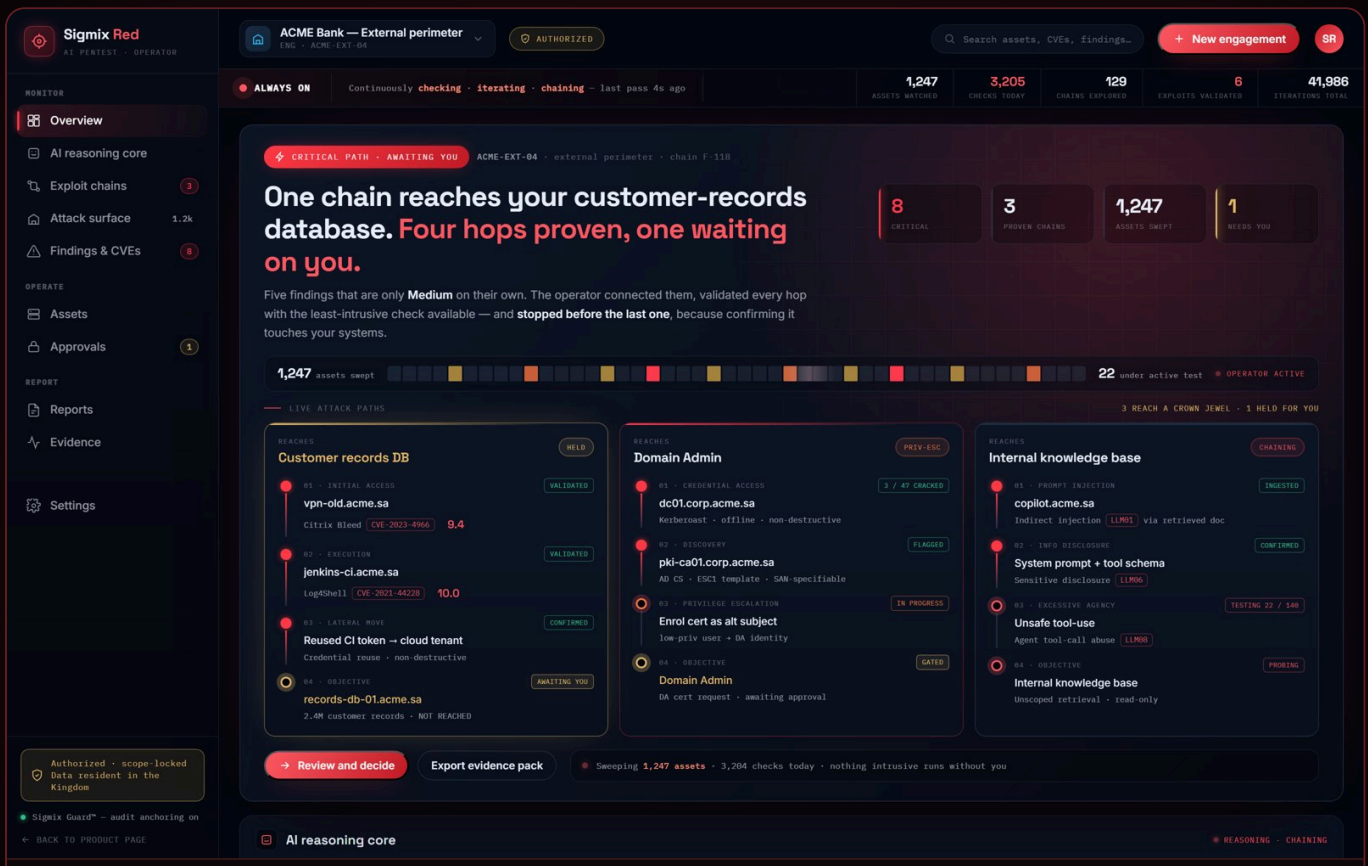
مُشغِّلٌ يستدلّ.

- ✓ **يستدلّ حول بيئتك** — لا قائمة تواقيع، بل نموذجٌ ذهنيّ لها كما يراه المهاجم.
- ✓ **يربط نقاط الضعف** في المسارَين أو الثلاثة التي تصل فعلًا إلى ما يهمّ.
- ✓ **دائم العمل** — يفحص ويكرّر ويُعيد الربط باستمرار مع تغيّر الأمور.
- ✓ **يختبر ذكاءك الاصطناعي أيضًا** — روبوتات المحادثة والمساعِدات والوكلاء التي لا تراها الأدوات التقليدية.

أصيل الذكاء — مُشغِّلٌ ينمذج بيئتك تحديدًا، لا كتاب قواعد.

كلّ شيءٍ في الصندوق — منصّةٌ مُشغِّلٍ واحدة.

خمس واجهاتٍ حيّة يعمل منها فريقك: نظرة المُشغِّل العامّة، وسلاسل الاستغلال المُثبَتة، وسطح الهجوم المُكتشَف، والنتائج المُرتَّبة، وبوابة الموافقة البشرية. مكانٌ واحد لإدارة الارتباط من أوّله إلى آخره.



01 · نظرة عامّة — سلسلةٌ واحدة تصل إلى قاعدة سجلّات العملاء؛ أربع قفزاتٍ مُثبَتة، وواحدة مُوقَفة بانتظار موافقتك.

01 · نظرة عامّة

واجهة قيادة المُشغِّل — سلسلةٌ واحدة مُثبَتة تصل إلى جواهر التاج، مُوقَفة عند البوابة بانتظارك.

02 · سلاسل الاستغلال

كلّ مسارٍ مُثبَت، مُرتَّب — المسارَان أو الثلاثة التي تصل فعلًا إلى ما يهمّ.

03 · سطح الهجوم

كلّ ما هو قابلٌ للوصول، مُخطَّطٌ باستمرار — الامتداد الذي نسيت أنّك تملكه.

04 · النتائج وثغرات CVE

نتائج مُرتَّبة ومُزالة التكرار، كلٌّ مدعومٌ بمسارٍ قابل لإعادة الإنتاج — لا تقرير من 400 صفحة.

05 · الموافقات

البوابة البشرية — لا يُشغَّل شيءٌ تدخّليّ حتى يقول مُشغِّلك: انطلق.

ما هو

فريقٌ أحمر لا يغادر عمله أبدًا.

وجّه Sigmix Red إلى نطاقٍ تملكه ومُصرَّحٌ لك باختباره. يتصرّف كمُشغِّلٍ صبورٍ لا يكلّ: يُعدّد سطحك، ويستدلّ حول كيفية اتّصال الأجزاء، و — حيثما تسمح فقط — يؤكّد بأمانٍ أنّ المسار حقيقي. ثمّ يكتبه بلغةٍ واضحة.

مستمرّ، لا مرّة في السنة

يُعيد الاختبار كلّما تغيّر سطحك، فيُلتقَط الانحراف خلال أيّامٍ لا عند التدقيق التالي.

سلاسل، لا قوائم تحقّق

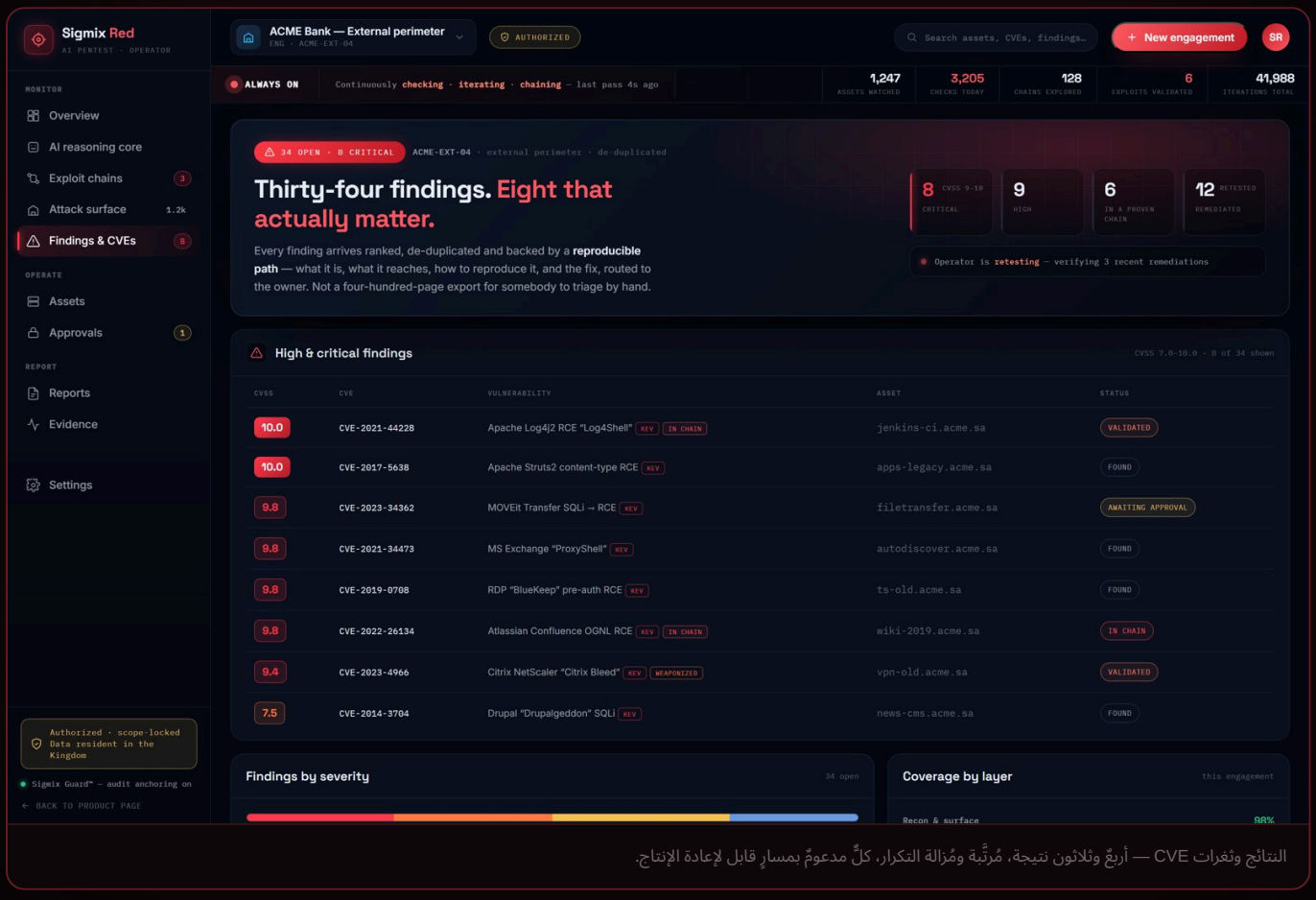
الماسحات تسرد المشكلات؛ وRed يربطها في المسارَين أو الثلاثة التي تصل فعلًا إلى ما يهمّ.

أدلّة، لا ضجيج

كلّ نتيجةٍ تصل مُرتَّبة ومُزالة التكرار ومدعومةً بمسارٍ قابل لإعادة الإنتاج — لا تصديرٌ من 400 صفحة.

تبقى أنت الآمِر

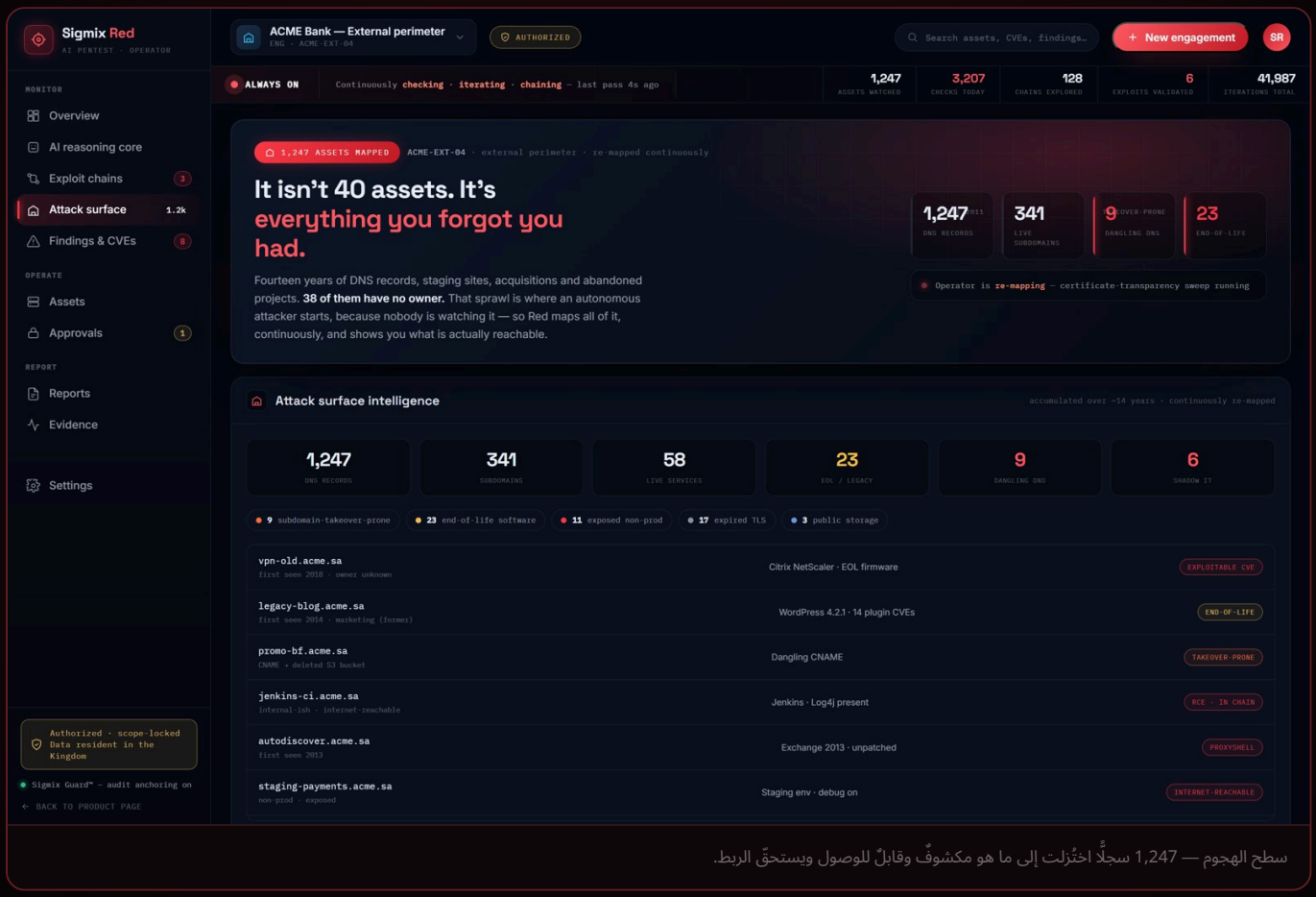
كلّ ما هو تدخّليّ ينتظر خلف بوابة موافقةٍ بشرية صريحة. ولا يُشغَّل شيءٌ مُدمِّر افتراضيًا.



النتائج وثغرات CVE — أربعٌ وثلاثون نتيجة، مُرتَّبة ومُزالة التكرار، كلٌّ مدعومٌ بمسارٍ قابل لإعادة الإنتاج.

ليست 40 أصلًا. إنّها كلّ ما نسيت أنّك تملكه.

تُراكم المؤسّسة الكبيرة عقدًا من سجلّات DNS ومواقع التجهيز والاستحواذات والمشاريع المهجورة. هذا الامتداد — السجلّات المُعلَّقة والخوادم المنتهية العمر التي لا يملكها أحد — هو تحديدًا حيث يبدأ مهاجم الذكاء الاصطناعي. يُخطّط Sigmix Red كلّ ذلك، باستمرار، ويُريك ما هو قابلٌ للوصول فعلًا.



سطح الهجوم — 1,247 سجلًّا اختُزلت إلى ما هو مكشوفٌ وقابلٌ للوصول ويستحقّ الربط.

التركة المنسيّة

DNS مُعلَّق، ونُسَخ تجهيز، ومضيفاتٌ منتهية العمر، وتقنيةٌ ظلّية — تُكشَف وتُنسَب، لا تُترَك للمهاجم ليجدها أوّلًا.

قابلٌ للوصول، لا نظريّ

مُخطَّطٌ من زاوية دخيلٍ خارجيّ لترى ما هو مكشوفٌ فعلًا، مفصولًا عمّا هو مُسيَّجٌ أو داخليّ.

باستمرار، لا مرّةً واحدة

يُعاد تشغيله مع تغيّر سطحك، فيُلتقَط نطاقٌ فرعيّ جديد أو سجلٌّ منسيّ خلال أيّام — لا عند الاختبار السنوي التالي.

كيف يعمل

حلقةٌ منضبطة — والمكابح موصولة.

يمرّ كلّ ارتباطٍ بالدورة المُتحكَّم بها ذاتها. والنقطتان اللتان قد يلمس فيهما المُشغِّل أنظمتك محروستان بموافقةٍ بشرية صريحة، وكلّ إجراءٍ يتّخذه يُكتَب في سجلّ تدقيقٍ مقاوم للعبث.

01

تحديد النطاق والتصريح

يبدأ كلّ ارتباطٍ من نطاقٍ مُوقَّع تملكه. والأهداف خارجه تُرفَض، لا تُحاوَل.

02

الاكتشاف والتخطيط

يُعدّد المُشغِّل سطحك الحقيقي القابل للوصول — النطاقات والخدمات والامتداد المنسيّ.

03

الاستدلال والربط

ينمذج كيفية اتّصال نقاط الضعف ويؤلّف المسارات القليلة متعدّدة الخطوات التي تصل فعلًا إلى شيء.

04

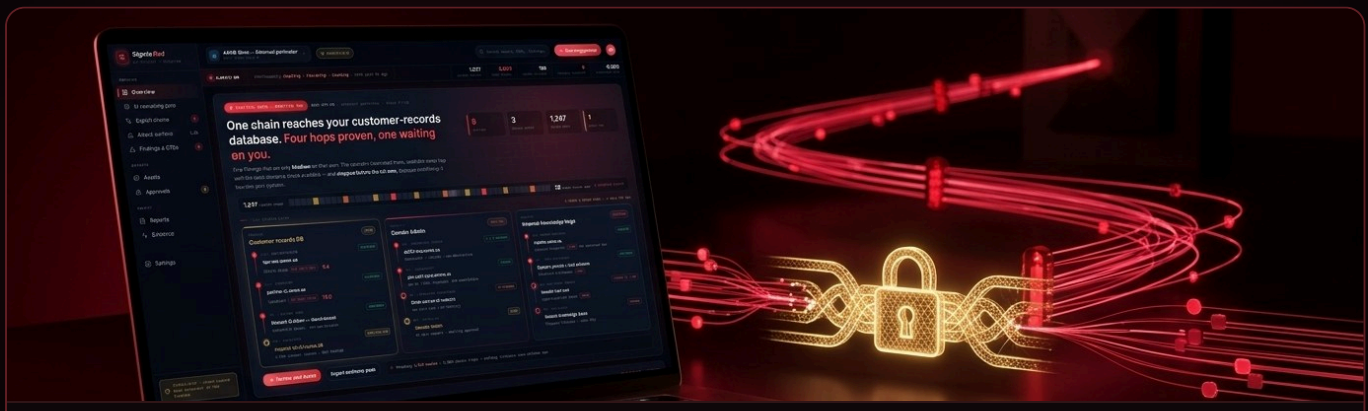
الإثبات — عند البوابة

تحقّقٌ بأقلّ قدرٍ من التدخّل فقط، وحيثما تسمح فقط. والخطوات التدخّلية تتوقّف لموافقةٍ بشرية.

05

التقرير بالأدلّة

نتائج مُرتَّبة، كلٌّ بمسارٍ قابل لإعادة الإنتاج، تُكتَب في سجلّ تدقيقٍ مقاوم للعبث.



بوابة الموافقة — يتوقّف المُشغِّل ويسأل قبل تشغيل أيّ شيءٍ تدخّليّ.

بوابتان، بشريّتان دائمًا: لا يُشغَّل شيءٌ تدخّليّ دون إذنٍ صريح من المُشغِّل، ولا يُشغَّل شيءٌ مُدمِّر افتراضيًا.

لا يختبر Sigmix Red إلّا ما تملكه وصُرِّح لك به.

إنّه أداةٌ دفاعية لفرق الأمن وشركائها المُعتمَدين. لا يُباع من أجل، ولن يعمل ضدّ، أنظمةٍ لا تتحكّم بها أو لم يُؤذَن لك باختبارها. النطاق والموافقة والإشراف يفرضها المنتَج — لا مجرّد وعدٍ في عقد.

تصريحٌ مكتوب

يبدأ كلّ ارتباطٍ من نطاقٍ مُوقَّع. والأهداف خارجه تُرفَض، لا تُحاوَل.

بوابات موافقةٍ بشرية

كلّ ما هو تدخّليّ يتوقّف لإذنٍ صريح من المُشغِّل. ولا يُشغَّل شيءٌ مُدمِّر افتراضيًا.

غير مُدمِّر افتراضيًا

تحقّقٌ بأقلّ تدخّل. لا تُسرَّب بيانات، ولا تُعطَّل خدمة لإثبات وجهة نظر.

سجلّ تدقيقٍ كامل

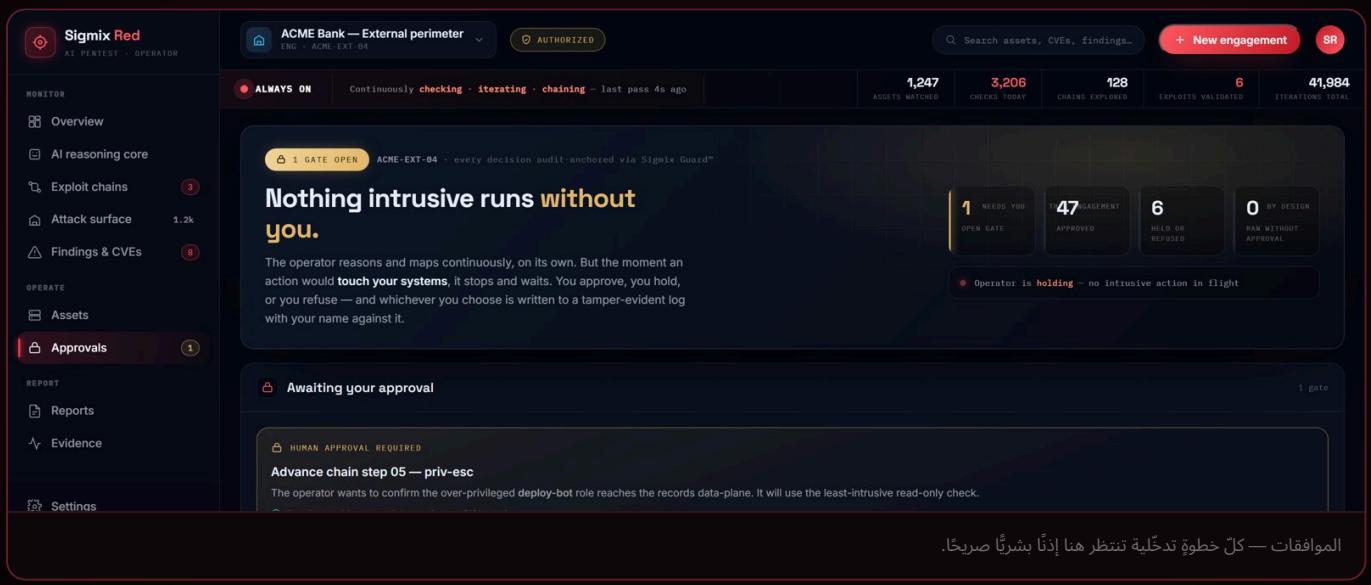
كلّ إجراءٍ يتّخذه المُشغِّل يُسجَّل في مرساةٍ مقاومة للعبث عبر Sigmix Guard™.

داخل المملكة وداخل مقرّك

يعمل على جهازٍ مختوم في مبناك أو في سحابة KSA داخل المملكة. والنتائج لا تغادر بيئتك أبدًا.

متوافق مع أُطُرك

تُقابَل الارتباطات بالتزامات NCA ECC-2 وSAMA CSF وPDPL، بأدلّةٍ يمكن لمُدقّقيك استخدامها.



الموافقات — كلّ خطوةٍ تدخّلية تنتظر هنا إذنًا بشريًّا صريحًا.

أين يعمل

انشره كما تقتضي قواعدك.

يتلاءم Sigmix Red مع وضعك الأمني، لا العكس — جهازٌ مختوم في مبناك، أو سحابةٌ مُدارة داخل المملكة، أو محكومٌ بـ Sigmix Guard™. وأينما عمل، يبقى سطحك ونتائجك وأدلّتك تحت سيطرتك.

مختومٌ داخل المقرّ

خزانتك الخاصّة

يعمل Red على جهاز Sigmix مختوم داخل مركز بياناتك. ولا يغادر المبنى أيّ شيءٍ عن نقاط ضعفك.

صفر بايت خارجة

سحابةٌ داخل المملكة

سحابة KSA

تفضّل المُدارة؟ شغّل Red في بيئةٍ داخل المملكة مقيمة البيانات — المُشغِّل ذاته، مُستضافٌ على أرضٍ سعودية.

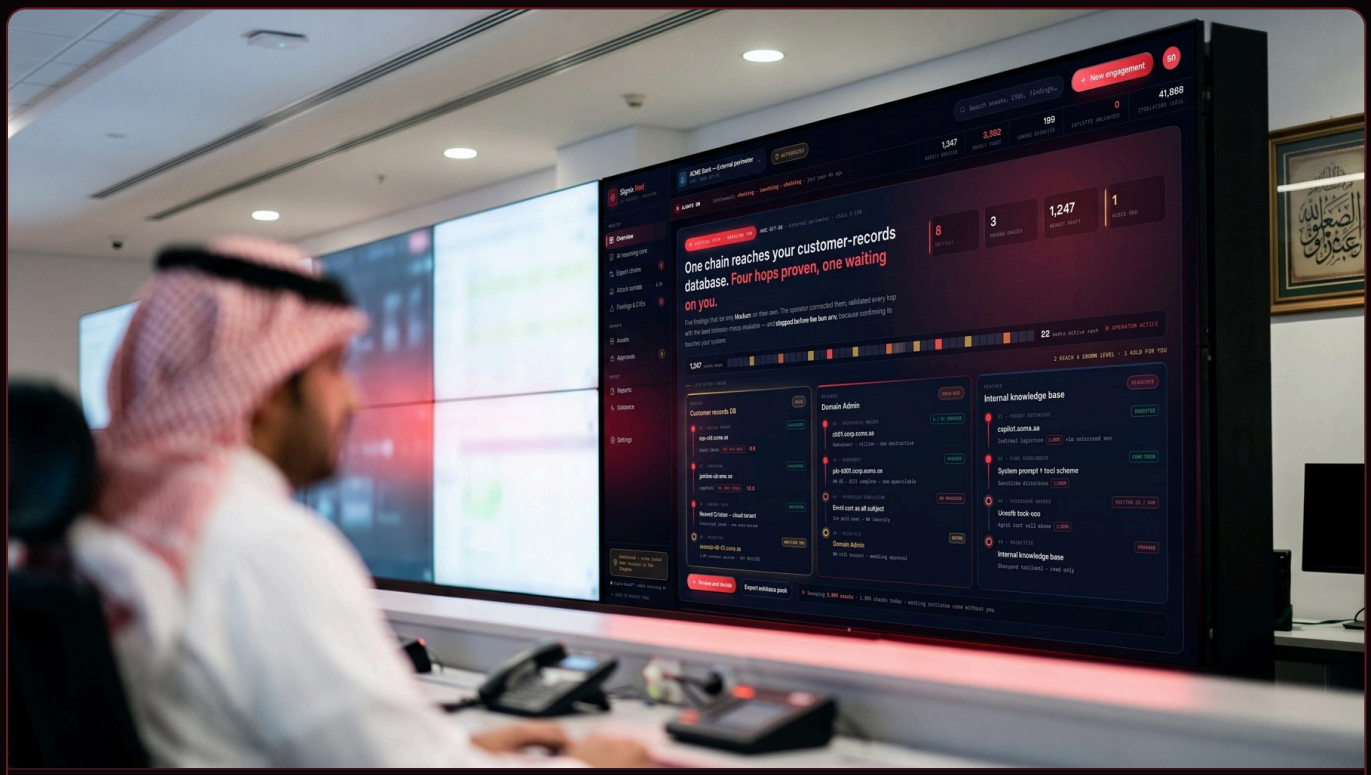
مقيمٌ داخل المملكة

محكوم

تحت Sigmix Guard™

يمرّ كلّ إجراءٍ للمُشغِّل عبر طبقة الإنفاذ المستقلّة ذاتها التي تحرس بقيّة المنصّة — تنقيةٌ، ثمّ إرساء.

تدقيقٌ مقاوم للعبث



مُشغِّلٌ واحد، أو جدارٌ منهم — يعمل Sigmix Red مختومًا على معدنك الخاصّ أو في سحابةٍ مُدارة داخل المملكة.

اسبِقهم إليها

اعثر على المسار قبل أن يعثر عليه سواك.

أحضِر لنا نطاقك والتزاماتك. سنُجري ارتباط إثبات مفهوم، ونُريك المسارَين أو الثلاثة التي تهمّ فعلًا، ونسلّم فريقك الأدلّة لإغلاقها.

إثبات مفهوم · مُصرَّحٌ به ومحدّد النطاق

ارتباطٌ قصير مُصرَّحٌ به بالكامل على نطاقٍ تملكه — أسرع طريقةٍ لترى المُشغِّل يكتشف ويربط ويُثبت مسارًا حقيقيًا عبر سطحك، مع بقاء بوابة موافقتك في الحلقة طوال الوقت.

ناقِش إثبات مفهوم

حدّد نطاق إثبات مفهومٍ لمؤسّستك.

شاهِد المنصّة

جولةٌ حيّة في المُشغِّل.

الأمن والأدلّة

كيف يعمل النطاق والبوابات وسجلّ التدقيق.

sigmix.sa

البريد الإلكتروني: contact@sigmix.sa

الهاتف: +966 11 525 6806

الويب: sigmix.sa

7229 طريق الابتكار · حي العقيق · 13519 الرياض · المملكة العربية السعودية · MISA 24926260339 VAT 314836510700003 CR 7054521799

Sigmix · sa