

— 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

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

SNAPSHOT • ONCE A YEAR



Always-on operator

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 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.

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.

The screenshot displays the Sigmix Red operator console interface. At the top, it shows the engagement name 'ACME Bank — External perimeter' and the status 'AUTHORIZED'. A search bar and a 'New engagement' button are also visible. The main dashboard features a critical path alert: 'One chain reaches your customer-records database. Four hops proven, one waiting on you.' Below this, a progress bar indicates '1,247 Assets swept' and '22 under active test'. The console is divided into three main sections: 'Customer records DB', 'Domain Admin', and 'Internal knowledge base'. Each section shows a sequence of steps (e.g., Initial Access, Execution, Lateral Move, Objective) with their status (Validated, Confirmed, Awaiting You, etc.). A 'Review and decide' button is prominently displayed. The bottom of the console shows a summary: '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.

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.

Evidence, not noise

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

Chains, not checklists

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

You stay in command

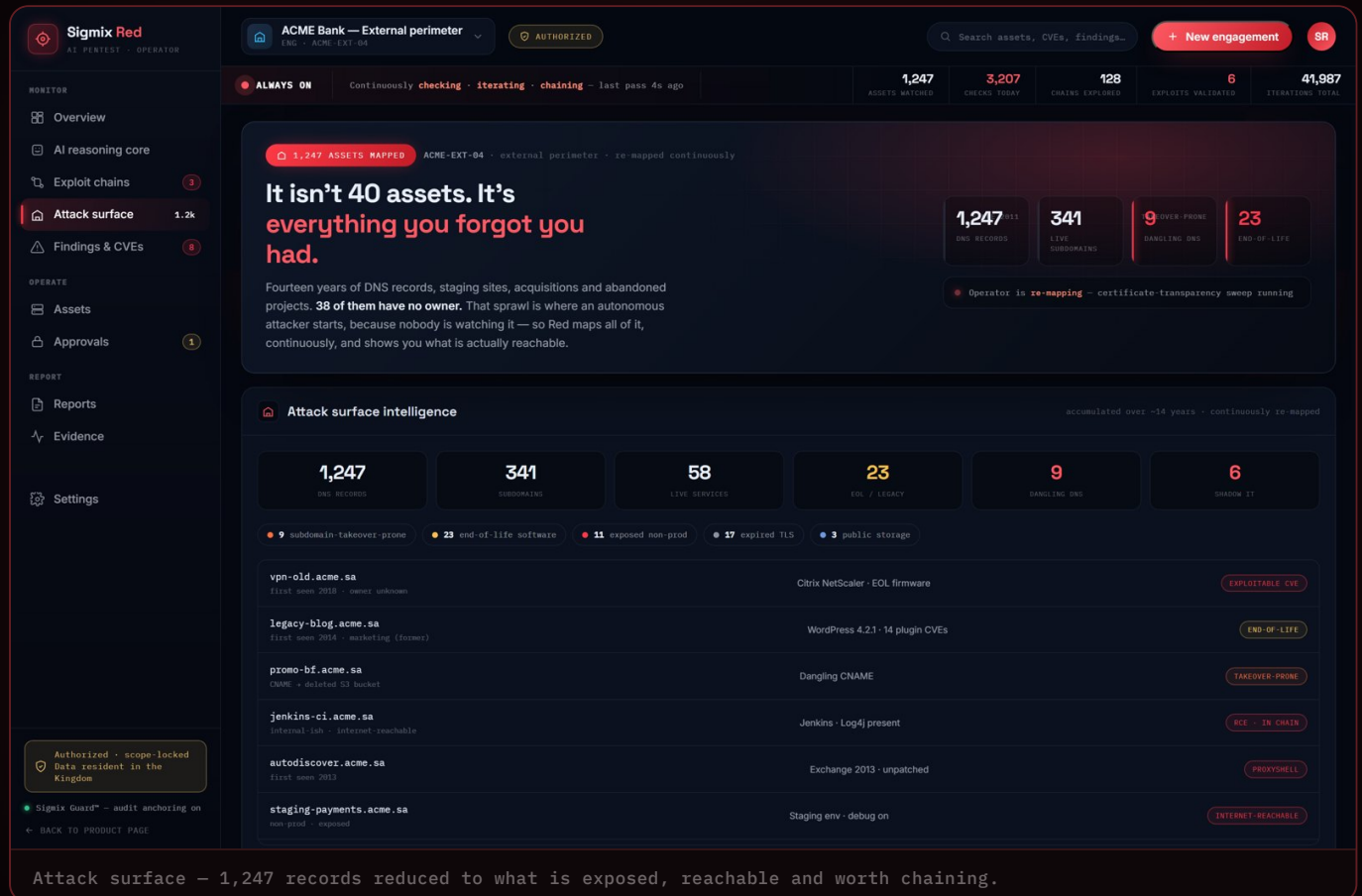
Anything intrusive waits behind an explicit human approval gate. Nothing destructive runs by default.

The screenshot displays the Sigmix Red interface for an engagement titled "ACME Bank — External perimeter". The interface includes a sidebar with navigation options like Overview, AI reasoning core, Exploit chains, Attack surface, Findings & CVEs, Assets, Approvals, Reports, Evidence, and Settings. The main dashboard shows a status of "ALWAYS ON" and a continuous cycle of checking, iterating, and chaining. Key metrics include 1,247 assets watched, 3,205 checks today, 128 chains explored, 6 exploits validated, and 41,988 iterations total. A prominent message states: "Thirty-four findings. Eight that actually matter." Below this, a table lists high and critical findings with columns for CVSS, CVE, Vulnerability, Asset, and Status. The findings are ranked by severity, with the highest being 10.0 for Apache Log4j2 RCE. The interface also features a "Findings by severity" bar chart and a "Coverage by layer" section showing 98% coverage for Recon & surface.

CVSS	CVE	VULNERABILITY	ASSET	STATUS
10.0	CVE-2021-44228	Apache Log4j2 RCE "Log4Shell" (KEY) (IN CHAIN)	jenkins-ci.acme.sa	VALIDATED
10.0	CVE-2017-5638	Apache Struts2 content-type RCE (KEY)	apps-legacy.acme.sa	FOUND
9.8	CVE-2023-34362	MOVEit Transfer SQLi → RCE (KEY)	filetransfer.acme.sa	AWAITING APPROVAL
9.8	CVE-2021-34473	MS Exchange "ProxyShell" (KEY)	autodiscover.acme.sa	FOUND
9.8	CVE-2019-0708	RDP "BlueKeep" pre-auth RCE (KEY)	ts-old.acme.sa	FOUND
9.8	CVE-2022-26134	Atlassian Confluence OGNL RCE (KEY) (IN CHAIN)	wiki-2019.acme.sa	IN CHAIN
9.4	CVE-2023-4966	Citrix NetScaler "Citrix Bleed" (KEY) (WEAPONIZED)	vpn-old.acme.sa	VALIDATED
7.5	CVE-2014-3784	Drupal "Drupalgeddon" SQLi (KEY)	news-cms.acme.sa	FOUND

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.



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.

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

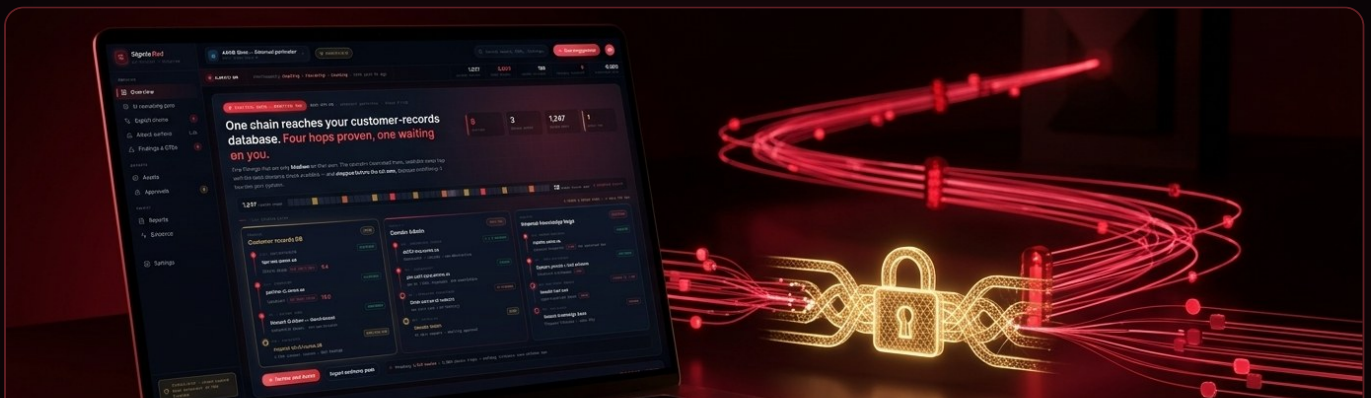
It models how weaknesses connect and composes the few multi-step paths that actually reach something.

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.

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.

Sigmix Red
AI PENTEST · OPERATOR

ACME Bank — External perimeter
LINK · ACME_EXT_04

AUTHORIZED

Search assets, CVEs, findings...

+ New engagement SR

MONITOR

- Overview
- AI reasoning core
- Exploit chains 3
- Attack surface 1.2k
- Findings & CVEs 8

OPERATE

- Assets
- Approvals 1

REPORT

- Reports
- Evidence
- Settings

ALWAYS ON Continuously checking · iterating · chaining — last pass 4s ago

1,247 ASSETS WATCHED 3,206 CHECKS TODAY 128 CHAINS EXPLORED 6 EXPLOITS VALIDATED 41,984 ITERATIONS TOTAL

1 GATE OPEN ACME-EXT-04 · every decision audit-anchored via Sigmix Guard™

Nothing intrusive runs without you.

The operator reasons and maps continuously, on its own. But the moment an action would **touch your systems**, it stops and waits. You approve, you hold, or you refuse — and whichever you choose is written to a tamper-evident log with your name against it.

1 NEEDS YOU OPEN DATE	47 MANAGEMENT APPROVED	6 HELD OR REFUSED	0 BY DESIGN RAN WITHOUT APPROVAL
--------------------------	---------------------------	----------------------	--

Operator is **holding** — no intrusive action in flight

Awaiting your approval 1 gate

HUMAN APPROVAL REQUIRED

Advance chain step 05 — priv-esc

The operator wants to confirm the over-privileged deploy-bot role reaches the records data-plane. It will use the least-intrusive read-only check.

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

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

Authorized use only. Sigmix Red is a defensive security-testing product for use by organisations against systems they own or are explicitly authorized to test. It is provided under a rules-of-engagement agreement that requires documented authorization and a defined scope; it enforces human approval before any intrusive action and does not run destructive operations by default. Sigmix Red is not offered for unauthorized access to any system, and use against systems you do not control or have not been permitted to test is prohibited and may be unlawful. Screens shown in this brochure are design mockups with illustrative data and do not depict any real customer, engagement or finding.



Sigmix Red

في عصر جديد من الاختراق المدفوع بالذكاء الاصطناعي،
أنت بحاجة إلى **دفاع أصيل الذكاء**.

بات المهاجمون يستخدمون ذكاءً اصطناعياً ذاتي التشغيل يكتشف نقاط الضعف ويربطها بسرعة الآلة. ويردّ Sigmix Red بالمثل — مُشغّل فريقيّ أحمر بالذكاء الاصطناعي، مبنّي من الألف إلى الياء ليفكّر كالمهاجم عبر كامل سطح هجوميك المُصرّح به. الذكاء الاصطناعي أولاً، لا ماسح تقليديّ أُضيف إليه.



سطح هجوميك المُصرّح به ← المُشغّل يستدلّ ويربط ← مسارات مُثبتة، مُرتّبة، بالأدلة

● ارتباطات مُصرّح بها فقط • داخل المملكة

الجانب المهاجم أصبح ذاتي التشغيل بالفعل. وعلى الدفاع أن يواكب.

خلال عامي 2025 و2026، لم يعد الذكاء الاصطناعي الهجومي مجرد عرض توضيحي. تُظهر الحوادث المُعلنة أنظمته وكلاء تعمل من البداية إلى النهاية — تستدل، وتتكيف مع أخطائها، وتولد آلاف الإجراءات أسرع من أي فريق بشري. لم يعد اختبار الاختراق المأخوذ مرة في السنة هو وحدة القياس الصحيحة.

1 → many

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

~31s

ليتعاف تشغيل وكيل موثوق من فشله ويكمل. سرعة الحلقة هي جوهر القصة.

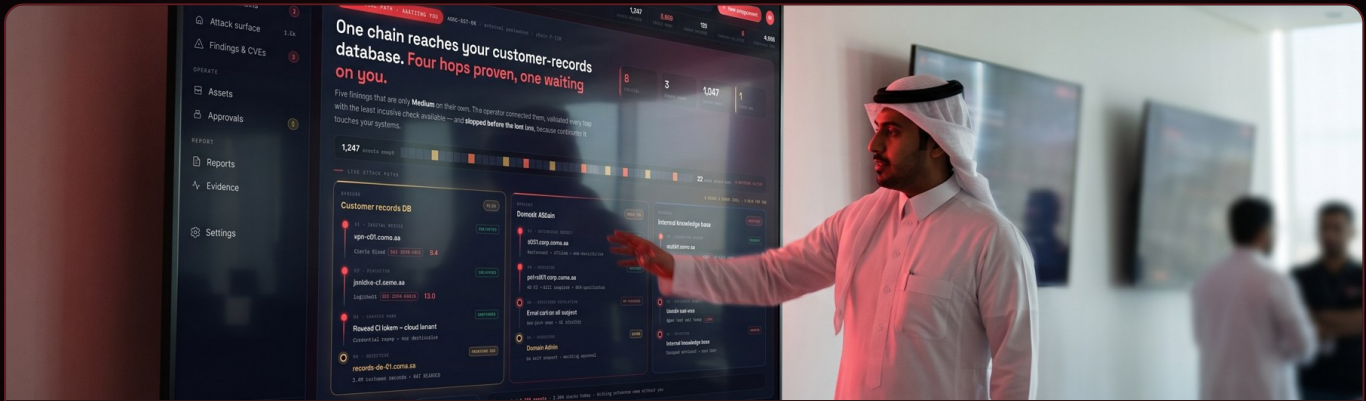
17,000+

إجراء فريد ولدها وكيل ذاتي التشغيل خلال اختراق واحد مُعلن في 2026 — أُعيد بناؤه بعد وقوعه فحسب.

مُشغل دائم العمل ≠ اختبار سنوي

مستمر · بسرعة الآلة

لقطة · مرة في السنة



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

تعكس أرقام 2026 أعلاه حوادث هجمات وكيالية مُبلَّغ عنها علنًا، أُعيد بناؤها بعد وقوعها. وهي مذكورة للسياق فقط — Sigmix Red منتج دفاعي للاختبار المُصرَّح به.

هجمات الذكاء الاصطناعي تحتاج مُدافِعًا بالذكاء الاصطناعي.

أفضل الدفاعات الحديثة — EDR ومساحات الانكشاف وSIEM — رائعة فيما رأيته من قبل. لكنّ المهاجم ذاتي التشغيل يؤلّف مساراتٍ جديدة متعدّدة الخطوات في الزمن الحقيقي، أسرع من أيّ توقيع أو قاعدة كُتبت. ويواجهه Sigmix Red بالطريقة الوحيدة القابلة للتوسّع: ذكاءً اصطناعيّ يستدلّ حول بيئتك تحديداً، كما يفعل المهاجم.

Sigmix Red · أصيل الذكاء

مُشغِّلٌ يستدلّ.

- ✓ يستدلّ حول بيئتك — لا قائمة توقع، بل نموذجٌ ذهنيّ لها كما يراه المهاجم.
- ✓ يربط نقاط الضعف في المسارين أو الثلاثة التي تصل فعلاً إلى ما يهّم.
- ✓ دائم العمل — يفحص ويكرّر ويُعيد الربط باستمرار مع تغيّر الأمور.
- ✓ يختبر ذكاءك الاصطناعي أيضاً — روبوتات المحادثة والمساعدات والوكلاء التي لا تراها الأدوات التقليدية.

التوقع والاستدلالات

قويّ في المعروف.

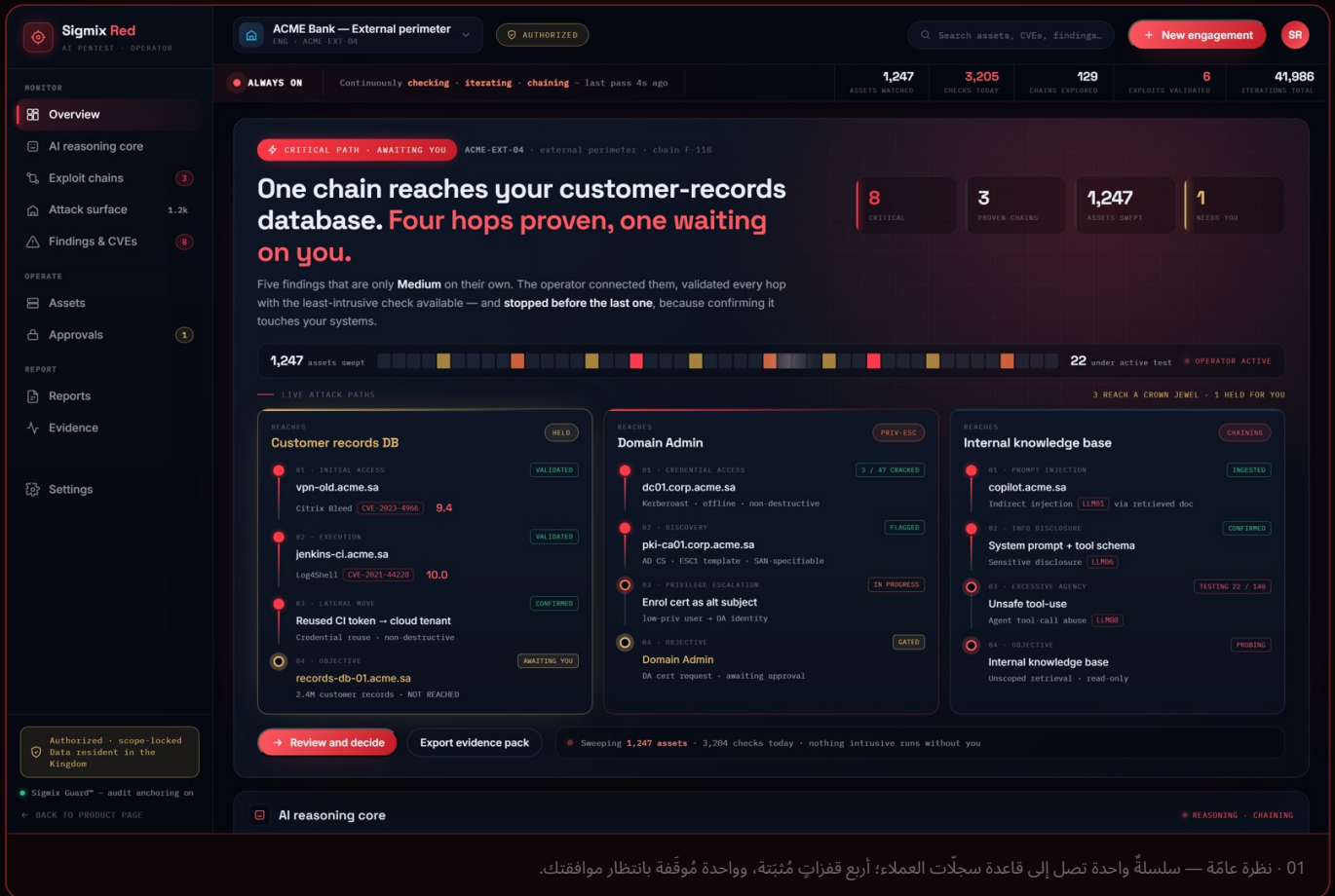
- ✗ يطابق قائمةً ثابتة من التوقع المعروف — أعمى تجاه كلّ ما هو جديد أو مترابط.
- ✗ يُلقِي بآلاف المشكلات المنعزلة؛ ويترك للبشر تخمين أيّها يتّصل بالآخر.
- ✗ يعمل فصلياً أو مرّة في السنة — يتقادم لحظة تغيّر سطحك.
- ✗ لا فكرة لديه أنّ روبوتات المحادثة والمساعدات لديك باتت الآن سطح هجوم.



أصيل الذكاء — مُشغِّلٌ يَنمِذَجُ بيئتك تحديداً، لا كتاب قواعد.

كلّ شيءٍ في الصندوق — منصة مُشغِّلٍ واحدة.

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



01 · نظرة عامّة — سلسلة واحدة تصل إلى قاعدة سَلات العملاء؛ أربع قفزات مُثبّنة، وواحدة مُوقّفة بانتظار موافقتك.

01 · نظرة عامّة

واجهة قيادة المُشغِّل — سلسلة واحدة مُثبّنة تصل إلى جواهر التاج، مُوقّفة عند البوابة بانتظارك.

02 · سلاسل الاستغلال

كلّ مسارٍ مُثبّت، مُرتّب — المسارَان أو الثلاثة التي تصل فعلاً إلى ما يهَمّ.

03 · سطح الهجوم

كلّ ما هو قابلٌ للوصول، مُحضّط باستمرار — الامتداد الذي نسييت أنّك تملكه.

04 · النتائج وثغرات CVE

نتائج مُرتّبة ومُزالة التكرار، كلُّ مدعوٍّ بمسارٍ قابلٍ لإعادة الإنتاج — لا تقرير من 400 صفحة.

05 · الموافقات

البوابة البشرية — لا يُشغِّل شيءٌ تدخّليّ حتى يقول مُشغِّلُك: انطلق.

فريق أحمر لا يغادر عمله أبدًا.

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

سلاسل، لا قوائم تحقّق

مستمرّ، لا مرّة في السنة

الماسحات تسرد المشكلات؛ و Red يربطها في المسارين أو الثلاثة التي تصل فعلاً إلى ما يهمّ.

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

تبقى أنت الآمر

أدلة، لا ضجيج

كلّ ما هو تدخّليّ ينتظر خلف بوابة موافقةٍ بشرية صريحة. ولا يُشغّل شيءٌ مُدّمّر افتراضياً.

كلّ نتيجة تصل مُرتّبة ومُزالة التكرار ومدعومةً بمسارٍ قابلٍ لإعادة الإنتاج — لا تصديرٍ من 400 صفحة.

Sigmix Red
AI PENTEST • OPERATOR

MONITOR

- Overview
- AI reasoning core
- Exploit chains 3
- Attack surface 1.2k
- Findings & CVEs 8**

OPERATE

- Assets
- Approvals 1

REPORT

- Reports
- Evidence

Settings

ACME Bank — External perimeter

ENG - ACME-EXT-04

AUTHORIZED

Search assets, CVEs, findings...

+ New engagement

SR

ALWAYS ON

Continuously checking · iterating · chaining - last pass 4s ago

1,247 ASSETS WATCHED

3,205 CHECKS TODAY

128 CHAINS EXPLORED

6 EXPLOITS VALIDATED

41,988 ITERATIONS TOTAL

34 OPEN · 8 CRITICAL

ACME-EXT-04 · external perimeter · de-duplicated

Thirty-four findings. Eight that actually matter.

Every finding arrives ranked, de-duplicated and backed by a **reproducible path** — what it is, what it reaches, how to reproduce it, and the fix, routed to the owner. Not a four-hundred-page export for somebody to triage by hand.

Operator is **retesting** - verifying 3 recent remediations

8 CVE 9-10 CRITICAL

9 HIGH

6 IN A PROVEN CHAIN

12 REMEDIATED

High & critical findings

CVSS 7.8-10.0 - 8 of 34 shown

CVSS	CVE	VULNERABILITY	ASSET	STATUS
10.0	CVE-2021-44228	Apache Log4j2 RCE "Log4Shell" KEY IN CHAIN	jenkins-ci.acme.sa	VALIDATED
10.0	CVE-2017-5638	Apache Struts2 content-type RCE KEY	apps-legacy.acme.sa	FOUND
9.8	CVE-2023-34362	MOVEit Transfer SQLi → RCE KEY	filetransfer.acme.sa	AWAITING APPROVAL
9.8	CVE-2021-34473	MS Exchange "ProxyShell" KEY	autodiscover.acme.sa	FOUND
9.8	CVE-2019-0708	RDP "BlueKeep" pre-auth RCE KEY	ts-old.acme.sa	FOUND
9.8	CVE-2022-26134	Atlassian Confluence OGNL RCE KEY IN CHAIN	wiki-2019.acme.sa	IN CHAIN
9.4	CVE-2023-4966	Citrix NetScaler "Citrix Bleed" KEY WEAPONIZED	vpn-old.acme.sa	VALIDATED
7.5	CVE-2014-3704	Drupal "Drupalgeddon" SQLi KEY	news-cms.acme.sa	FOUND

Findings by severity

34 open

Coverage by layer

this engagement

Recon & surface 88%

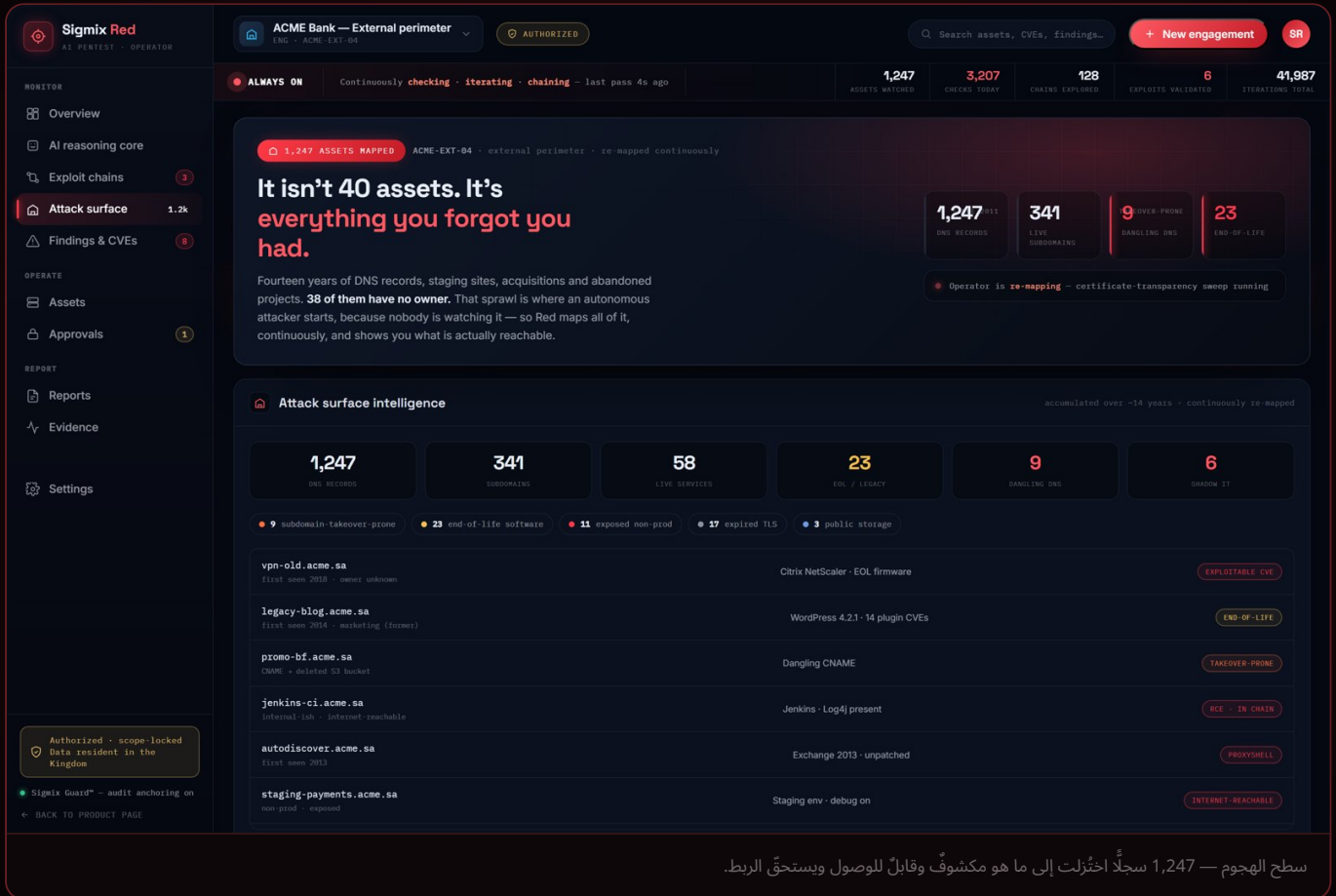
Authorized · scope-locked
Data resident in the Kingdom

Sigmix Guard™ - audit anchoring on

← BACK TO PRODUCT PAGE

ليست 40 أصلًا. إنها كل ما نسيت أنك تملكه.

تُراكم المؤسسة الكبيرة عقدًا من سجلّات DNS ومواقع التجهيز والاستحواذات والمشاريع المهجورة. هذا الامتداد — السجلّات المُعلّقة والخوادم المنتهية العمر التي لا يملكها أحد — هو تحديدًا حيث يبدأ مهاجم الذكاء الاصطناعي. يُخَطِّط Sigmix Red كل ذلك، باستمرار، ويُريك ما هو قابلٌ للوصول فعليًا.



التركة المنسية

DNS مُعلّق، ونُسخ تجهيز، ومضيفاتٌ منتهية العمر، وتقنيةٌ ظلية — تُكشَف وتُنسب، لا تُترك للمهاجم ليجدها أولًا.

قابلٌ للوصول، لا نظري

مُخَطَّط من زاوية دخيلٍ خارجيٍ لترى ما هو مكشوفٌ فعليًا، مفصلاً عمّا هو مُسَيَّجٌ أو داخلي.

باستمرار، لا مرّةً واحدة

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

حلقة منضبطة — والمكابح موصولة.

يمرّ كل ارتباط بالدورة المُتحكّم بها ذاتها. والنقطتان اللتان قد يلمس فيهما المُشغّل أنظمتك محروستان بموافقةٍ بشرية صريحة، وكل إجراء يتّخذهُ يُكتَب في سجلّ تدقيقٍ مقاوم للعبث.

01 تحديد النطاق والتصريح

يبدأ كل ارتباط من نطاقٍ مُوقَّع تملكه. والأهداف خارجه تُرفض، لا تُحاول.

02 الاكتشاف والتخطيط

يُعَدّد المُشغّل سطحك الحقيقي القابل للوصول — النطاقات والخدمات والامتداد المنسي.

03 الاستدلال والربط

ينمذج كيفية اتصال نقاط الضعف ويؤلّف المسارات القليلة متعدّدة الخطوات التي تصل فعلاً إلى شيء.

04 الإثبات — عند البوابة

تحقّق بأقل قدرٍ من التداخل فقط، وحيثما تسمح فقط. والخطوات التداخلية تتوقّف لموافقةٍ بشرية.

05 التقرير بالأدلة

نتائج مُرتّبة، كلّ مسارٍ قابل لإعادة الإنتاج، تُكتَب في سجلّ تدقيقٍ مقاوم للعبث.



بوابة الموافقة — يتوقّف المُشغّل ويسأل قبل تشغيل أي شيء تداخل.

بوابتان، بشريتان دائماً: لا يُشغّل شيء تداخلٍ دون إذن صريح من المُشغّل، ولا يُشغّل شيء مُدبّر افتراضياً.

لا يختبر Sigmix Red إلا ما تملكه وصرّح لك به.

إنّه أداة دفاعية لفرق الأمن وشركائها المُعتمدين. لا يُباع من أجل، ولن يعمل ضدّ، أنظمة لا تتحكّم بها أو لم يُؤدّن لك باختبارها. النطاق والموافقة والإشراف يفرضها المنتج — لا مجرد وعدٍ في عقد.

● تصريح مكتوب

يبدأ كلّ ارتباطٍ من نطاقٍ مُوقَّع. والأهداف خارجه تُرفض، لا تُحاول.

● بوابات موافقة بشرية

كلّ ما هو تدخلٍ يتوقّف لإذنٍ صريح من المُشغّل. ولا يُشغّل شيءٌ مُدمّر افتراضياً.

● غير مُدمّر افتراضياً

تحقّق بأقلّ تدخل. لا تُسرّب بيانات، ولا تُعطّل خدمة لإثبات وجهة نظر.

● سجلّ تدقيقٍ كامل

كلّ إجراءٍ يتّخذه المُشغّل يُسجّل في مرساةٍ مقاومة للعبث عبر Sigmix GuardTM.

● داخل المملكة وداخل مقرّك

يعمل على جهازٍ مختوم في مبنك أو في سحابة KSA داخل المملكة. والنتائج لا تغادر بيئتك أبداً.

● متوافق مع أطرك

تُقابل الارتباطات بالتزامات NCA ECC-2 و SAMA CSF و PDPL. بأدلةٍ يمكن لمُدقّقك استخدامها.

The screenshot shows the Sigmix Red interface for ACME Bank. The top navigation bar includes 'Sigmix Red', 'ACME Bank — External perimeter', 'AUTHORIZED', and a search bar. The main dashboard displays a status 'ALWAYS ON' and a message 'Nothing intrusive runs without you.' Below this, there are four cards showing metrics: '1 NEEDS YOU OPEN GATE', '47 GATEMENT APPROVED', '6 HELD OR REFUSED', and '0 BY DESIGN RAN WITHOUT APPROVAL'. A section titled 'Awaiting your approval' shows a 'HUMAN APPROVAL REQUIRED' message for 'Advance chain step 05 — priv-esc'.

الموافقات — كلّ خطوةٍ تدخليةٍ تنتظر هنا إذنًا بشريًا صريحًا.

انشره كما تقتضي قواعداك.

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

محكوم

تحت Sigmix Guard™

يمرّ كلّ إجراءٍ للمُشغّل عبر طبقة الإنفاذ المستقلة ذاتها التي تحرس بقية المنصة — تنقية، ثم إرساء.

تدقيقٌ مقاوم للعبث

سحابةٌ داخل المملكة

سحابة KSA

تفضّل المُدارة؟ شغّل Red في بيئة داخل المملكة مقيمة البيانات — المُشغّل ذاته، مُستضاف على أرضٍ سعودية.

مقيمٌ داخل المملكة

مختومٌ داخل المقرّ

خزانتك الخاصة

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

صفر بايت خارجة



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

اعثر على المسار قبل أن يعثر عليه سواك.

أحضِر لنا نطاقك والتزاماتك. سنُجري ارتباط إثبات مفهوم، ونُريك المسارين أو الثلاثة التي تهَمّ فعلاً، ونسلّم فريقك الأدلة لإغلاقها.

إثبات مفهوم · مُصرّح به ومحدّد النطاق

ارتباط قصير مُصرّح به بالكامل على نطاقٍ تملكه — أسرع طريقةً لترى المُشغّل يكتشف ويربط ويُثبت مسارًا حقيقيًا عبر سطحك، مع بقاء بوابة موافقتك في الحلقة طوال الوقت.

الأمن والأدلة

كيف يعمل النطاق والبوابات
وسجلّ التدقيق.

شاهد المنصة

جولةً حيّة في المُشغّل.

ناقش إثبات مفهوم

حدّد نطاق إثبات مفهوم
لمؤسّستك.

sigmix.sa

الويب

sigmix.sa

الهاتف

+966 11 525 6806

البريد الإلكتروني

contact@sigmix.sa

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

الاستخدام المُصرّح به فقط. Sigmix Red منتج اختبارٍ آمنٍ دفاعيٍّ لاستخدام المؤسسات ضدّ أنظمةٍ تملكها أو صرّح لها صراحةً باختبارها. يُقدّم بموجب اتفاقية قواعد اشتباكيّ تتطلب تصريحًا موثّقًا ونطاقًا محدّدًا؛ ويفرض موافقةً بشريةً قبل أيّ إجراءٍ تدخّليّ، ولا يُشغّل عملياتٍ مُدمّرةٍ افتراضيًا. لا يُقدّم Sigmix Red للوصول غير المُصرّح به إلى أيّ نظام. واستخدامه ضدّ أنظمةٍ لا تتحكّم بها أو لم يُؤدّن لك اختبارها محظورٌ وقد يكون غير قانوني. الشاشات المعروضة في هذا الكتيّب نماذج تصميمية ببيانات توضيحية ولا تُصوّر أيّ عميلٍ أو ارتباطٍ أو نتيجةٍ حقيقية.

