JODOR Technologies

TLP:CLEAR

JODOR TECHNOLOGIES · MANAGED DECEPTION 2026

From Managed Detection to Managed Deception

Know your attacker first. JODOR deception turns attacks on your name into intelligence about your own attackers, with nothing to install.

BRIEFING ID JTI-2026-DTI-01



MANAGED DECEPTION

Key findings

What JODOR deception revealed about attackers, and what that means for your defences.

The evidence: In 56 days, JODOR sensors and deception systems in Saudi Arabia recorded 450,908 requests from 22,924 addresses; 2,207 showed hostile intent.

KEY FINDINGS

50% — **Public lists miss half of the attackers.**
1,102 of the 2,207 attackers were on no public blocklist.

88% — **Local attackers were mostly unlisted.**
194 of the 220 attackers hosted in Saudi Arabia were on no list.

84% — **Attackers strike within seconds.**
146 of 173 attackers used a known exploit within 10 seconds of arriving.

76% — **Attacker addresses change quickly.**
1,687 of the 2,207 attackers were seen on one day only, then moved on.

82% — **AI agents can do the watching.**
In JODOR's test, AI agents settled 5,073 of 6,168 alerts without a person.

WHAT TO DO

1. **Watch who targets you, not everyone.**
2. **Load your own attacker list into your defences.**
3. **Start with a free 30-day pilot.**

Sources: JODOR sensors and deception systems in Saudi Arabia (JODOR analysis; raw data not published) · JODOR AI analysis and rules data (JODOR analysis)

THE PROBLEM

Attacks now outrun manual defence

JODOR sensors and industry research show how little time defenders now have.

84%

Of 173 attackers who used a known exploit, 146 used it within 10 seconds of arriving.

27 s

The fastest attacker in one public study spread through a network 27 seconds after breaking in.

28%

A typical security operations centre (SOC) leaves 28% of its alerts uninvestigated, a 2026 survey found.

JODOR assessment: people alone almost certainly cannot respond within 10 seconds, so defenders need warning before the attack arrives.

Sources: JODOR sensors and deception systems in Saudi Arabia (JODOR analysis; raw data not published) · CrowdStrike 2026 Global Threat Report, press release (24 Feb 2026) · Prophet Security, State of AI in the SOC 2026 (3 Aug 2026)

THE PROBLEM

Public lists miss half

A blocklist is a public list of known bad addresses. JODOR tested how much those lists catch.

50%

Of the 2,207 attackers, 1,102 were on no public blocklist.

76%

Of the attackers, 1,687 were seen on one day only, so lists go stale fast.

88%

Of the 220 attackers hosted in Saudi Arabia, 194 were on no list.

JODOR assessment: a list built from everyone's attackers will very likely miss the ones aiming at you. You need intelligence about your own attackers.

Sources: JODOR sensors and deception systems in Saudi Arabia (JODOR analysis; raw data not published)

THE SERVICE

Let the attacker introduce himself

Deception means fake systems that look easy to break into. No genuine user has a reason to visit them.

1

Anyone who touches a deception system is almost certainly an attacker, so every touch is a clear signal.

2

Deception that carries your name attracts the attackers who are looking for you.

3

Each touch reveals the attacker's address, tools and intentions before a real system is hit.

JODOR assessment: deception gives a clean signal: it turns the attacker's first move into your early warning.

Sources: JODOR sensors and deception systems in Saudi Arabia (JODOR analysis; raw data not published)

THE SERVICE

Deception in your name

JODOR operates the whole service in five steps. You install nothing.

01

Profile

JODOR learns who targets your sector and services, in a one-hour workshop.

02

Design

JODOR builds deception systems with your name and look, hosted in Saudi Arabia, with your written approval.

03

Bait

Each deception system carries fake weaknesses and fake passwords. Nothing real is ever placed in it.

04

Watch

AI agents watch every touch around the clock, with a JODOR analyst in the loop.

05

Deliver

You receive your own attacker list, priority alerts, detection rules and reports.

JODOR assessment: the service watches JODOR's deception systems, not your network, so there is nothing to connect and nothing to install.

Sources: JODOR sensors and deception systems in Saudi Arabia (JODOR analysis; raw data not published) · JODOR AI analysis and rules data (JODOR analysis)

THE SERVICE

Four steps judge each attacker

Every event moves up a step only when the step below cannot settle it.

STEP 4

Human in the loop

A JODOR security analyst reviews everything the agents escalate.

Human

STEP 3

Analyst agent

A large expert AI model (117 billion parameters) investigates what the first look could not settle.

18 s

STEP 2

First-look agent

A fast AI model reads the event and settles the clear cases.

1.2 s

STEP 1

Rule agent

It settles an attacker already proven by a security control or blocklist. It needs no AI model.

No model

WHY FOUR STEPS

Proven attackers never wait for an AI model.

Unclear cases get an expert look.

A person reviews what the agents cannot settle.

Sources: JODOR AI analysis and rules data (JODOR analysis) · JODOR response data (JODOR analysis)

THE EVIDENCE

The agents were tested live

In a 15-day test on a live JODOR-operated platform, every alert was counted once.



Step 1 · Rule agent	2,506	41%
Step 2 · First-look agent	1,305	21%
Step 3 · Analyst agent	1,262	20%
Step 4 · Human in the loop	967	16%
Still open when the 15 days ended	128	2%

6,168 alerts were settled in 15 days. A person was needed for only 1 in 6.

JODOR assessment: the same agents now watch your deception systems, so a person reviews only what needs a person.

Sources: JODOR AI analysis and rules data (JODOR analysis) · JODOR response data (JODOR analysis)

THE EVIDENCE

Fresh intelligence in minutes

How long the agents took from an attacker's first request to a confirmed block in JODOR's test.

5 min

When the firewall had already denied every request, the rule agent confirmed and blocked the attacker within about 5 minutes.

20 min

Across all 1,759 blocks that could be timed, the typical time to confirm and block was 20 minutes.

15 s

The fastest confirmation came 15 seconds after the attacker's first request.

JODOR assessment: an attacker confirmed on your deception system can reach your attacker list within minutes. The first request may have been harmless, so real times are shorter.

Sources: JODOR response data (JODOR analysis)

THE EVIDENCE

What your list would have shown

Examples of what JODOR deception recorded. A subscriber receives this about its own attackers.

261

Attackers hunted for passwords and keys, typically 0.75 seconds after arriving.

173

Attackers used a published attack on a known software flaw, mostly flaws that already have fixes.

152

Requests came from one visitor posing as a search engine's robot, sweeping secret files. No blocklist knew it.

JODOR assessment: each of these attackers would join your attacker list and your monthly report.

Sources: JODOR sensors and deception systems in Saudi Arabia (JODOR analysis; raw data not published)

THE SERVICE

Intelligence you can use at once

Four things reach you from the first week of the service.

Your own attacker list

Addresses, fingerprints and other signs that your firewall or SOC can load automatically.

Priority alerts

If someone tries a fake password that exists only in your deception systems, you know at once that you are targeted.

Detection rules

Rules written from what attackers actually did, ready for your own security tools.

Monthly report

Who targeted you, how, from where, and what to do next, with a quarterly briefing.

JODOR assessment: the intelligence is about the attackers who chose you, so it is relevant from the first day.

Sources: JODOR AI analysis and rules data (JODOR analysis)

THE SERVICE

Nothing to install

The service operates entirely on JODOR infrastructure in Saudi Arabia.

You do	You do not
Sign the subscription and authorise JODOR to use your name on deception systems.	Install any software or agent.
Approve the deception names and domains once.	Give JODOR access to your networks, systems or logs.
Choose where the list and reports arrive.	Change anything in your environment for JODOR.
Decide what to block, and block it yourself.	Hand any decision inside your environment to JODOR.

JODOR assessment: JODOR delivers intelligence; your team stays in control of every action inside your environment.

Sources: JODOR AI analysis and rules data (JODOR analysis)

THE EVIDENCE

Safety checks keep the list clean

A good attacker list must not include your friends. JODOR measured how often its blocks were wrong.

1,906

Blocks were applied in JODOR's 15-day test.

102

Of those blocks, about 5%, were later undone.

87

Of the undone blocks were caught automatically by safety checks.

15

Were corrected after escalation to the human in the loop.

JODOR assessment: most mistakes involved administrators, delivery networks and real search engines. Your attacker list starts with your list of trusted addresses.

Sources: JODOR response data (JODOR analysis)

HOW TO START

Three ways to subscribe

Each package includes deception in your name, the four-step review and a monthly report.

	Essentials	Professional	Enterprise
Deception systems in your name	Up to 3	Up to 8	Up to 20
Threat profile	Sector profile	Custom workshop	Custom, updated quarterly
Attacker list	Daily file	Live list and API	Live list, API and your own threat lists matched
Priority alerts	Email	Email and portal	Email, portal and phone
Detection rules	—	Monthly	Monthly and on request
Reports	Monthly	Monthly and quarterly briefing	Monthly, quarterly board briefing, annual review

JODOR assessment: prices are shared after a short call, because they depend on the number of deception systems and the reports you need.

Sources: JODOR planning assumption (to be confirmed)

HOW TO START

Start with one step

Two ways to begin, and how JODOR supports you after that.

01

JODOR deception

Deception in your name catches your attackers on first contact.

02

AI agents and an analyst

Rule, first-look and analyst agents, with a person in the loop, turn every touch into intelligence.

03

Professional services

JODOR experts help you harden systems, clean up secrets and act on the list.

START WITH ONE STEP

45 min A threat briefing on what now attacks organisations like yours.

30 days A free pilot with deception in your name that ends in a board-ready report.

Not ready yet? Forward this report to the head of your security operations.

Sources: JODOR sensors and deception systems in Saudi Arabia (JODOR analysis; raw data not published) · JODOR AI analysis and rules data (JODOR analysis)

JODOR Technologies

TLP:CLEAR

JODOR TECHNOLOGIES · MANAGED DECEPTION 2026

From managed detection to managed deception

WEB	jodr.sa
EMAIL	info@jodr.sa
LINKEDIN	linkedin.com/company/jodr-technologies
OFFICE	Riyadh, Kingdom of Saudi Arabia

Book a 45-minute briefing or a free 30-day pilot at info@jodr.sa.

Scan to email info@jodr.sa