JODOR Technologies

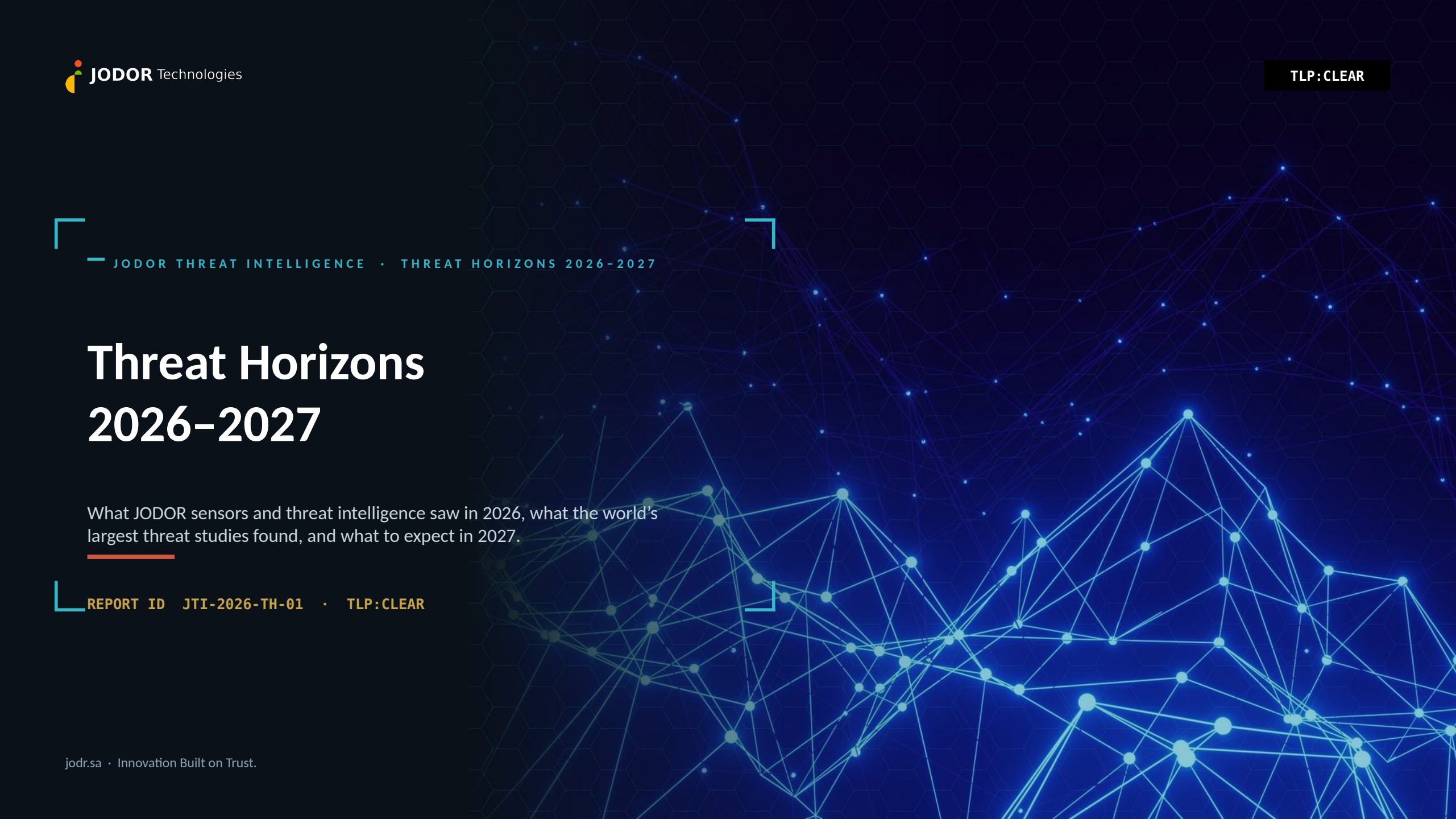
TLP:CLEAR

JODOR THREAT INTELLIGENCE · THREAT HORIZONS 2026–2027

Threat Horizons 2026–2027

What JODOR sensors and threat intelligence saw in 2026, what the world's largest threat studies found, and what to expect in 2027.

REPORT ID JTI-2026-TH-01 · TLP:CLEAR



THREAT HORIZONS

Key findings

Five signals from 2026 that shape the defence plan for 2027.

The evidence: JODOR combined 56 days of its own sensor and deception data in Saudi Arabia with the main global and regional threat studies of 2026.

KEY FINDINGS

27 s — **Attacks now move at machine speed.**
The fastest breakout in CrowdStrike's data was 27 seconds; 84% of JODOR's exploit attackers struck within 10 s.

32% — **Old flaws are still the main way in.**
Exploits were the top first step in 32% of Mandiant's 2025 intrusions, for the sixth year running.

48% — **Ransomware is in nearly half of all breaches.**
Verizon found ransomware in 48% of breaches, and a third party in about half.

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

SAR 27M — **A breach in the Kingdom is costly.**
IBM put the average Saudi breach at SAR 27 million, found after 226 days.

WHAT TO DO

1. **Act on the first request, not the first report.**
2. **Patch internet-facing systems in days, not months.**
3. **Build intelligence about your own attackers.**

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) · Mandiant M-Trends 2026 (23 Mar 2026) · Verizon 2026 Data Breach Investigations Report, as reported by GovInfoSecurity (19 May 2026) · IBM Cost of a Data Breach 2026, Saudi Arabia findings (Aug 2026)

2026 IN REVIEW

Attacks moved to machine speed

Three measurements of how little time defenders had in 2026.

27 s

The fastest attacker in CrowdStrike's 2025 data spread through a network 27 seconds after breaking in. The average eCrime breakout was 29 minutes.

22 s

Mandiant found that the hand-off from the first intruder to a second criminal group took a median 22 seconds, down from over 8 hours in 2022.

10 s

On JODOR sensors, 146 of 173 attackers who used a known exploit did so within 10 seconds of arriving.

JODOR assessment: defence that waits for a person to read an alert will almost certainly arrive after the attacker.

Sources: CrowdStrike 2026 Global Threat Report, press release (24 Feb 2026) · Mandiant M-Trends 2026 (23 Mar 2026) · JODOR sensors and deception systems in Saudi Arabia (JODOR analysis; raw data not published)

2026 IN REVIEW

Old flaws are still the main way in

How attackers got their first foothold in 2025, according to the two largest incident studies.

32%

Exploits were the most common first step in Mandiant's intrusions, for the sixth year in a row.

1 in 3

Verizon: one in three breaches began with a software flaw, overtaking stolen passwords for the first time in the report's 19-year history.

43 days

Verizon: the median time to patch rose to 43 days, from 32 days a year earlier.

26%

Verizon: only 26% of CISA known-exploited flaws were fully fixed across the 13,000 organisations it polled.

JODOR assessment: attackers reuse what works, and patching is getting slower, not faster.

Sources: Mandiant M-Trends 2026 (23 Mar 2026) · Verizon 2026 Data Breach Investigations Report, as reported by GovInfoSecurity (19 May 2026) · Verizon 2026 DBIR, as reported by Help Net Security (20 May 2026)

2026 IN REVIEW

Exploitation now starts before the patch

Attackers increasingly use a flaw before defenders can fix it.

−7 days

Mandiant estimates the mean time to exploit fell to −7 days: exploitation now routinely comes before the patch.

42%

CrowdStrike found that 42% of exploited flaws were used before they were publicly disclosed.

VPNs

Mandiant tracked groups that target VPNs and routers on purpose, because these devices rarely carry endpoint detection tools.

JODOR assessment: patching alone can no longer close the gap; you also need to see who is probing you before the fix exists.

Sources: Mandiant M-Trends 2026 (23 Mar 2026) · CrowdStrike 2026 Global Threat Report, press release (24 Feb 2026)

2026 IN REVIEW

Ransomware and partners drive the breaches

What Verizon found in more than 22,000 confirmed breaches.

48%

of breaches involved ransomware, up from 44% the year before.

~50%

of breaches involved a third party, after a 60% rise in a single year.

69%

of ransomware victims did not pay, and payments kept falling.

JODOR assessment: your exposure now includes your suppliers' weakest system, not only your own.

Sources: Verizon 2026 Data Breach Investigations Report, as reported by GovInfoSecurity (19 May 2026) · Verizon 2026 DBIR, as reported by Help Net Security (20 May 2026)

2026 IN REVIEW

Identity and people remain the target

How attackers use accounts and conversations rather than malware.

73%

Microsoft: 73.3% of initial access attempts used user execution, valid accounts, social engineering or phishing.

63%

Microsoft: 63% of the intrusions it saw involved data theft.

11%

Mandiant: voice phishing rose to 11% of intrusions, the second most common way in.

18%

IBM: phishing, including voice and SMS, was the top attack vector in Middle East breaches.

JODOR assessment: a convincing call or message now opens more doors than malware does.

Sources: Microsoft Digital Defense Report 2026, Microsoft Source Asia (13 Oct 2026) · Mandiant M-Trends 2026 (23 Mar 2026) · IBM Cost of a Data Breach 2026, Middle East findings (3 Aug 2026)

2026 IN REVIEW

AI joined the attacker's toolkit

What the largest threat teams saw attackers do with AI.

+89%

CrowdStrike: activity by AI-enabled adversaries rose 89% in one year.

LLM

Google: malware such as PROMPTSTEAL queried a large language model during live operations, a first for Google.

Iran

Google: the Iranian state group TEMP.Zagros (MuddyWater) used an AI model to help build custom malware.

Not yet

Mandiant: 2025 was not the year breaches were the direct result of AI; most still stem from human and systemic failures.

JODOR assessment: AI makes attackers faster and cheaper today; it will very likely take over more steps of the attack in 2027.

Sources: Google Threat Intelligence Group, AI threat tracker (5 Nov 2025) · CrowdStrike 2026 Global Threat Report, press release (24 Feb 2026) · Mandiant M-Trends 2026 (23 Mar 2026)

2026 IN REVIEW

The Middle East saw a ransomware surge

Two regional studies of the Middle East between 2025 and 2026.

20×

CloudSEK: ransomware-related threat intelligence feeds about the region rose from 17 in April 2025 to a peak of 357 in June 2026.

12%

Positive Technologies: Saudi Arabia drew 12% of attacks in the region, the second most targeted country.

44%

Positive Technologies: 44% of successful attacks in the region led to a data leak.

25%

Positive Technologies: government was the most attacked sector at 25%, then industry at 15%.

JODOR assessment: hacktivism was the largest threat by volume, but ransomware kept rising even after hacktivist activity fell sharply in April 2026.

Sources: CloudSEK, Middle East Cyber Threat Landscape 2025-2026, as reported by Arabian Reseller (16 Sep 2026) · Positive Technologies, Current cyberthreats in the Middle East (Q2 2025 to Q1 2026)

2026 IN REVIEW

What a breach costs in the Kingdom

IBM's 2026 study of breaches between March 2025 and February 2026.

SAR 27M

The average cost of a breach in Saudi Arabia.

285 days

Saudi organisations took 226 days to find a breach and 59 more to contain it.

SAR 38M

Financial services had the highest average breach cost in the Kingdom.

SAR 8.9M

Breaches cost about SAR 8.9 million less where AI and automation were used widely (SAR 23.15M vs 32.08M).

JODOR assessment: speed is now a cost line: every day an attacker stays hidden adds to the bill.

Sources: IBM Cost of a Data Breach 2026, Saudi Arabia findings (Aug 2026) · IBM Cost of a Data Breach 2026, Middle East findings (3 Aug 2026)

2026 IN REVIEW

What JODOR sensors saw in 2026

JODOR sensors and deception systems in Saudi Arabia, 29 Aug – 23 Oct 2026.

2,207

attackers from 84 countries, out of 450,908 requests from 22,924 addresses.

50%

of attackers were on none of 34 public blocklists.

88%

of attackers hosted in Saudi Arabia were on no list (194 of 220).

76%

of attackers were seen on one day only, then moved on.

0.75 s

was the typical time before an attacker asked for passwords or keys.

0

attackers matched a known state-linked group; no match is not proof of absence.

JODOR assessment: most attackers were automated and opportunistic, and half were new to every public list.

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

2026 IN REVIEW

What worked in defence

Results from JODOR's 15-day live test of AI agents with a human in the loop.

82%

of 6,168 alerts were settled by AI agents without a person.

41%

were settled by rules alone, because a security control had already proven the attack.

20 min

was the typical time from an attacker's first request to a block.

5%

of blocks were later undone; safety checks reversed most of them automatically.

JODOR assessment: machines with clear rules and a person in the loop matched the attacker's speed without losing control.

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

THE 2027 HORIZON

Horizon 1: AI runs more of the attack

What we expect to change in 2027, and why.

JODOR outlook for 2027: AI agents will very likely carry out more steps of an attack on their own, from scanning to writing the first exploit.

THE EVIDENCE

Activity by AI-enabled adversaries rose 89% in 2025. Malware already asks AI models for commands mid-attack. On JODOR sensors, 84% of exploit attackers struck within 10 seconds.

WHAT IT MEANS

The window between first contact and damage will keep shrinking. Alerts that wait in a queue will be read after the event.

WHAT TO DO

Let rules act alone on proven attacks. Send unclear cases to fast AI analysis. Keep a person for decisions that cannot be undone.

Sources: CrowdStrike 2026 Global Threat Report, press release (24 Feb 2026) · Google Threat Intelligence Group, AI threat tracker (5 Nov 2025) · Mandiant M-Trends 2026 (23 Mar 2026) · JODOR sensors and deception systems in Saudi Arabia (JODOR analysis; raw data not published)

THE 2027 HORIZON

Horizon 2: the patch arrives too late

What we expect to change in 2027, and why.

JODOR outlook for 2027: Exploitation before a fix exists will almost certainly become routine, especially on VPNs, firewalls and other edge devices.

THE EVIDENCE

Mandiant's mean time to exploit fell to −7 days. 42% were used before disclosure. Patching slowed to a median of 43 days.

WHAT IT MEANS

Patching stays essential but can no longer be the only control. Edge devices are the blind spot because they rarely run detection tools.

WHAT TO DO

List every internet-facing system. Patch edge devices first. Watch who probes you, so you see a new exploit before it reaches a real system.

Sources: Mandiant M-Trends 2026 (23 Mar 2026) · CrowdStrike 2026 Global Threat Report, press release (24 Feb 2026) · Verizon 2026 DBIR, as reported by Help Net Security (20 May 2026)

THE 2027 HORIZON

Horizon 3: people and partners as the way in

What we expect to change in 2027, and why.

JODOR outlook for 2027: Voice phishing, stolen sessions and supplier compromise will likely open more doors in 2027 than malware does.

THE EVIDENCE

73.3% of initial access attempts used people or accounts. Voice phishing reached 11% of intrusions. About half of breaches involved a third party.

WHAT IT MEANS

Attackers will sound like your colleagues and arrive through your suppliers. Passwords alone will not stop them.

WHAT TO DO

Use phishing-resistant multi-factor sign-in. Verify payment and access requests by a second channel. Review supplier access every quarter.

Sources: Microsoft Digital Defense Report 2026, Microsoft Source Asia (13 Oct 2026) · Mandiant M-Trends 2026 (23 Mar 2026) · Verizon 2026 Data Breach Investigations Report, as reported by GovInfoSecurity (19 May 2026) · IBM Cost of a Data Breach 2026, Middle East findings (3 Aug 2026)

THE 2027 HORIZON

Horizon 4: regional pressure rises

What we expect to change in 2027, and why.

JODOR outlook for 2027: Ransomware against Gulf organisations will likely keep rising, with hacktivist waves that follow regional events.

THE EVIDENCE

Regional ransomware intelligence feeds rose more than 20 times. Saudi Arabia drew 12% of regional attacks. 88% of Saudi-hosted attackers on JODOR sensors were on no list.

WHAT IT MEANS

Local attackers are the least visible. A defence built on global lists will very likely miss the ones closest to you.

WHAT TO DO

Collect intelligence about your own attackers. Rehearse ransomware recovery. Keep tested, offline backups.

Sources: CloudSEK, Middle East Cyber Threat Landscape 2025-2026, as reported by Arabian Reseller (16 Sep 2026) · Positive Technologies, Current cyberthreats in the Middle East (Q2 2025 to Q1 2026) · JODOR sensors and deception systems in Saudi Arabia (JODOR analysis; raw data not published)

THE 2027 HORIZON

Horizon 5: the quantum clock is running

What we expect to change in 2027, and why.

JODOR outlook for 2027: Data stolen today may be decrypted later. Planning the move to post-quantum cryptography will likely become a board topic in 2027.

THE EVIDENCE

NIST's final transition plan (Oct 2026) deprecates today's common public-key algorithms (RSA and elliptic curve) after 2030 and disallows them after 2035.

WHAT IT MEANS

Records with a long life, such as identities, contracts and health or financial data, are already at risk from "collect now, decrypt later".

WHAT TO DO

Build an inventory of where cryptography is used. Ask suppliers for their post-quantum plans. Start with long-life data.

Sources: NIST IR 8547, Transition to Post-Quantum Cryptography Standards (final, 27 Oct 2026)

WHAT TO DO

Five actions for 2027

Each action answers one of the horizons in this report.

#	Action	Answers
1	Let proven attacks be blocked in seconds by rules, and send unclear alerts to fast AI analysis with a person in the loop.	Horizon 1
2	Patch internet-facing and edge devices first, and watch who probes them before a fix exists.	Horizon 2
3	Move to phishing-resistant sign-in and verify sensitive requests by a second channel.	Horizon 3
4	Build intelligence about your own attackers, not only public lists, and rehearse ransomware recovery.	Horizon 4
5	Start a cryptography inventory and a post-quantum plan for long-life data.	Horizon 5

JODOR assessment: each action starts with knowing what you have and who is targeting it.

Sources: JODOR sensors and deception systems in Saudi Arabia (JODOR analysis; raw data not published) · Mandiant M-Trends 2026 (23 Mar 2026) · Verizon 2026 Data Breach Investigations Report, as reported by GovInfoSecurity (19 May 2026)

HOW JODOR HELPS

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 THREAT INTELLIGENCE · THREAT HORIZONS 2026–2027

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