PANOP

PANOP RESEARCH

State of Security 2026

A global view of the threat landscape at the midpoint of 2026: where attacks now start, what artificial intelligence has changed on both sides of the line, and which regulatory deadlines land before December.

EDITION JULY 2026

PANOP RESEARCH · PANOP.IO

PANOP

PANOP RESEARCH

State of Security 2026

A global view of the threat landscape at the midpoint of 2026: where attacks now start, what artificial intelligence has changed on both sides of the line, how exposure differs by region, and which regulatory deadlines land before December.

THE YEAR IN NUMBERS

$4.99M

Global average cost of a data breach, a record, up 12%

IBM / Ponemon, 2026

1 in 4

Malicious breaches that were AI-enabled, up 56%

IBM / Ponemon, 2026

48%

Confirmed breaches involving a third party, up 60%

Verizon DBIR, 2026

31%

Initial access from vulnerability exploitation

Verizon DBIR, 2026

94%

Leaders naming AI the top driver of change

WEF, 2026

69%

Ransomware victims that did not pay

Verizon DBIR, 2026

77%

Share of recorded EU incidents that were DDoS

ENISA, 2025

73%

Personally affected by cyber-enabled fraud in 2025

WEF, 2026

THREE SHIFTS BEHIND THE NUMBERS

The entry point moved from stolen credentials to unpatched exposure. The perimeter moved outward into the supply chain, which now features in nearly half of confirmed breaches. And AI risk acquired a measurable price for the first time: AI-enabled breaches cost roughly a million dollars more than the average, while defenders who have deployed AI save close to two million.

Panop SA · Crissier · August 2026 · panop.io | Compiled from public primary sources. Full citations on page 8.

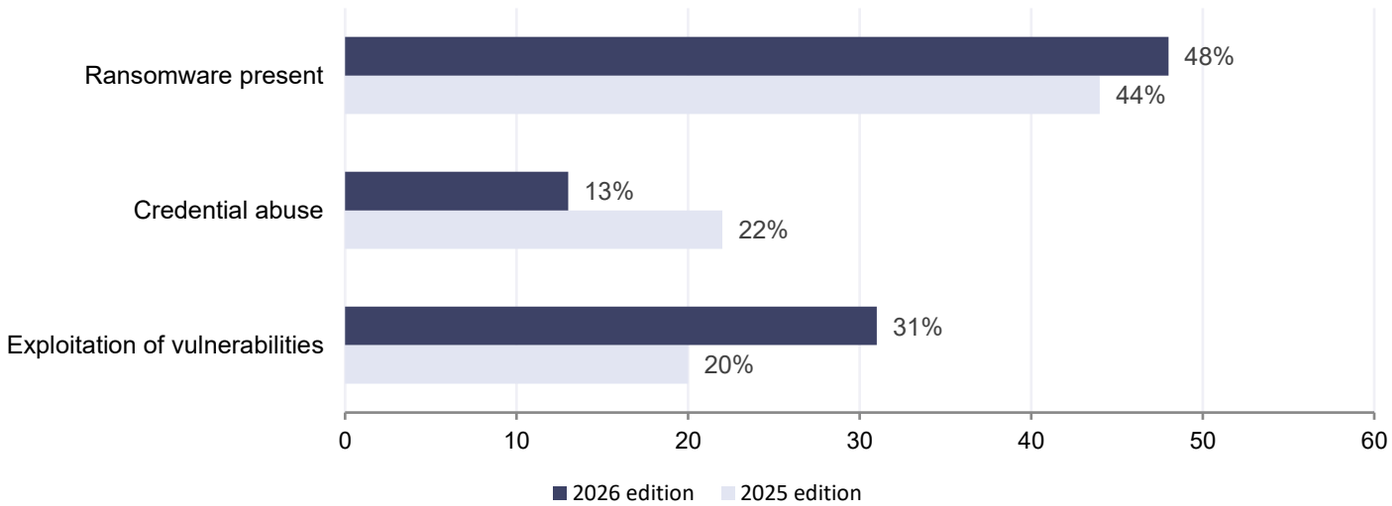
Sources *IBM Security / Ponemon Institute, Cost of a Data Breach Report 2026. Verizon, 2026 Data Breach Investigations Report. ENISA, Threat Landscape 2025. World Economic Forum with Accenture, Global Cybersecurity Outlook 2026.*

PANOP

02 · HOW ATTACKS BEGIN, AND HOW THEY PAY

The front door changed, and so did the economics

Two structural movements define the year. Exploitation displaced stolen credentials as the primary entry route, and ransomware became more frequent but less profitable per victim.



Verizon 2026 DBIR. Exploitation rose 55% year on year and overtook credential abuse as the leading initial access vector for the first time.

69%

of ransomware victims did not pay

Median paid $139,875

down from $150,000

RANSOMWARE: MORE OFTEN, LESS PROFITABLY

69% of victims did not pay and the median payment fell to $139,875 from $150,000. Better backups and rehearsed recovery are working, so operators have shifted to volume: ENISA counted 82 distinct ransomware variants deployed against EU organisations in a single reporting year, with Akira the most frequently observed. Verizon confirmed 7,152 SMB breaches in the 2026 dataset.

The practical reading. Vulnerability management has become a capacity problem rather than a diligence problem, so the answer is exposure reduction and segmentation rather than faster patching alone. Meanwhile the value of a tested restore is now quantifiable: two thirds of victims used one instead of paying.

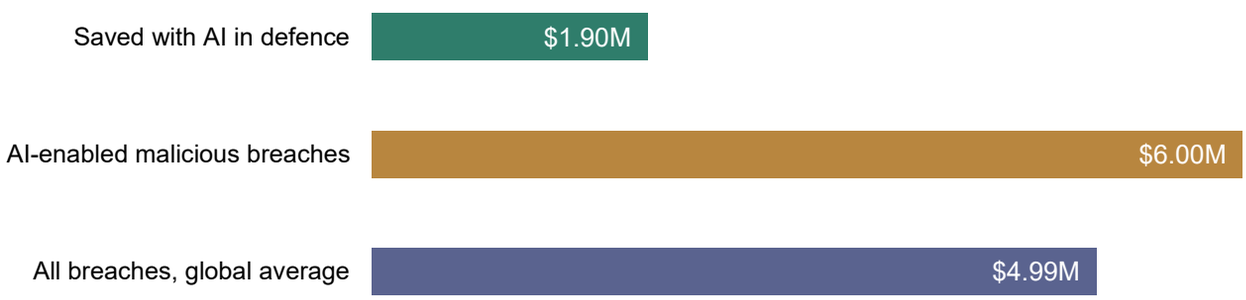
Sources *Verizon, 2026 Data Breach Investigations Report. ENISA, Threat Landscape 2025, 1 October 2025.*

PANOP

03 · WHAT AI HAS INTRODUCED

The first-year AI risk had a price tag

Until 2026 the AI threat conversation ran on anecdote. This year it has arrived in the breach datasets, with a measurable frequency, a measurable cost premium, and a documented case of an intrusion run largely by the model itself.



IBM Security and Ponemon Institute, Cost of a Data Breach Report 2026. Chart redrawn by Panop from published figures. 1 in 4 malicious breaches were AI-enabled, up 56% year on year, and 1 in 4 organisations still use no AI or automation in security operations.

DEEPFAKE IMPERSONATION

IBM records deepfake impersonation and AI-enabled malware as the two most common forms of AI-enabled attack in the period. In the WEF survey, 73% of respondents said they or someone in their network had been personally affected by cyber-enabled fraud during 2025, and CEOs now rank fraud above ransomware.

INDUSTRIALISED SOCIAL ENGINEERING

ENISA assessed that by early 2025, AI-supported phishing represented more than 80% of observed social engineering activity worldwide. The marginal cost of a personalised campaign has collapsed.

AUTONOMOUS OPERATIONS

In November 2025 Anthropic reported disrupting the first documented AI-orchestrated cyber espionage campaign, attributed to a state-sponsored group it designated GTG-1002. Around 30 organisations were targeted, and Anthropic assessed that the model executed 80% to 90% of the tactical work.

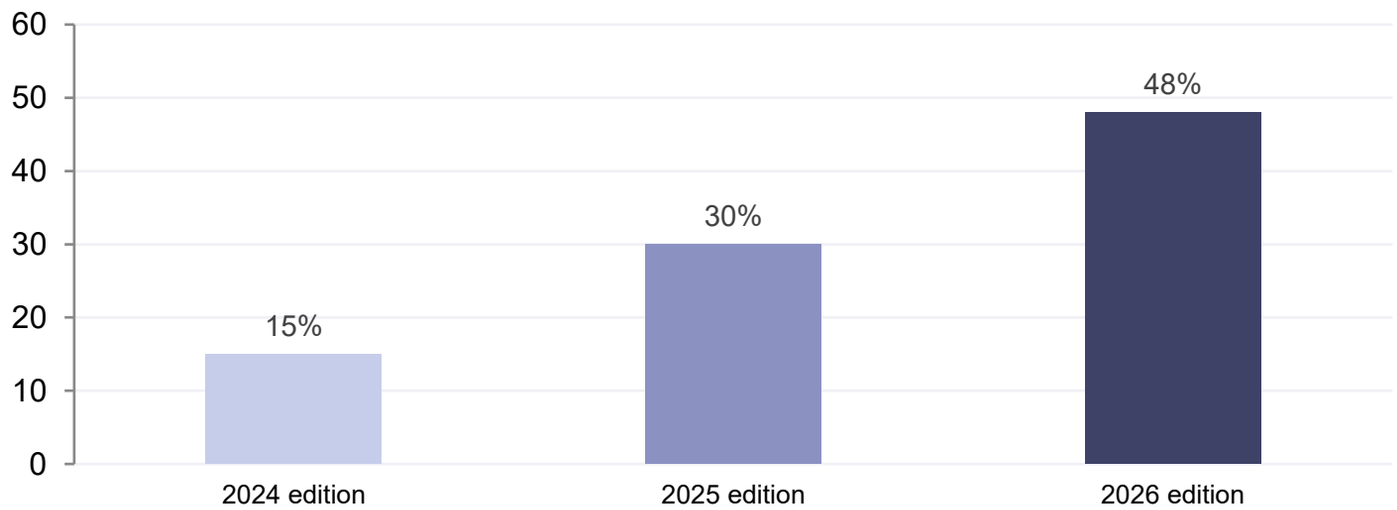
What changed is tempo, not technique. The tactics in an AI-run intrusion are familiar. What is new is that reconnaissance, exploitation and lateral movement proceed at machine speed and in parallel across many targets, compressing the window between exposure and impact. Shadow AI accounts for 43% of AI-related incidents, and mean time to identify and contain rose this year after five years of improvement.

Sources *IBM / Ponemon, Cost of a Data Breach Report 2026. ENISA, Threat Landscape 2025. WEF, Global Cybersecurity Outlook 2026. Anthropic, Disrupting the first reported AI-orchestrated cyber espionage campaign, November 2025.*

04 · THIRD-PARTY AND CONCENTRATION RISK

Half of all breaches now arrive through somebody else

The fastest-moving number in this year's data is not ransomware or AI. It is the share of breaches involving a third party, which has grown from roughly a third to nearly half in two annual editions.



Verizon DBIR, successive annual editions. Third-party involvement rose 60% year on year.

Vendor identity hygiene is the mechanism

Only 23% of third-party organisations fully remediated missing or improperly secured MFA on cloud accounts.

Eight months is not a response timeline

That is the median time for third parties to resolve half of weak password and permission findings: a structural exposure window inside environments that already hold your data.

One supplier, many operators

A ransomware attack on a shared check-in and boarding platform disrupted several major European airports in September 2025. ENISA identifies supply chain compromise and the abuse of digital dependencies as a defining theme of the year.

CONCENTRATION MAKES IT SYSTEMIC

When many organisations in a sector depend on the same handful of platforms, an incident stops being a firm-level event and becomes a sector one. That logic put a critical third-party provider regime into DORA and supply chain risk management into Article 21 of NIS2. For most organisations the gap is not policy but evidence: few programmes can show on demand which vendors hold which access, when it was last reviewed, and what would still function if a supplier stopped answering tomorrow.

Sources *Verizon, 2026 Data Breach Investigations Report. ENISA, Threat Landscape 2025. Regulation (EU) 2022/2554 (DORA); Directive (EU) 2022/2555 (NIS2).*

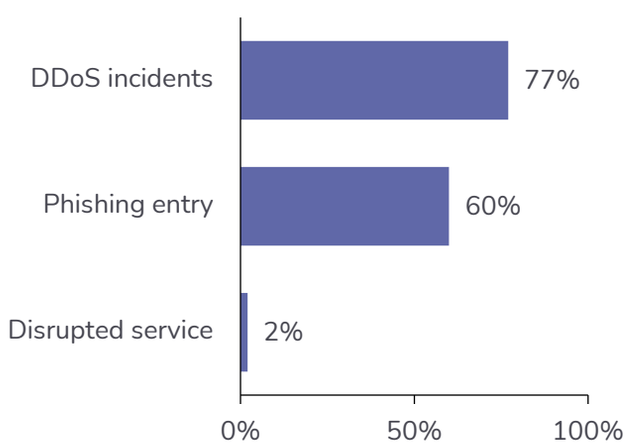
05 · INCIDENTS, INTRUSIONS AND BREACHES

High volume, narrow impact

Counting incidents and counting damage give different answers. Across the EU, ENISA curated 4,875 incidents in twelve months, most of them noisy denial-of-service campaigns with no operational effect. Switzerland now sees the same split in its own mandatory reporting: the disruptive minority is intrusion, credential theft and ransomware.

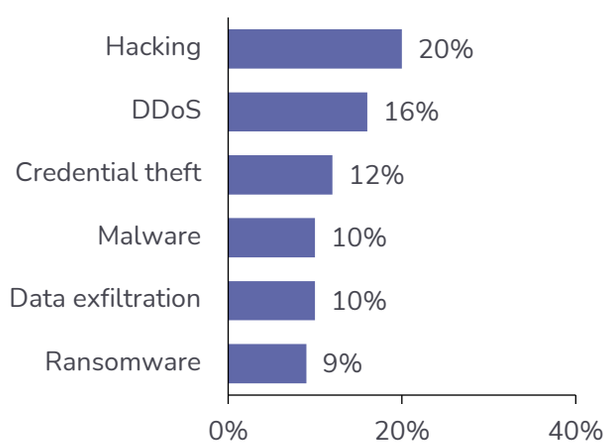
THE EUROPEAN PICTURE

EU incidents: volume against impact



THE SWISS PICTURE

Swiss reports by attack type, H2 2025



EUROPEAN UNION · ENISA ETL 2025

4,875 incidents curated, July 2024 to June 2025
Hacktivism drove 79% of them, almost all DDoS
Only 2% of those caused any service disruption
Ransomware remains the most impactful threat
Public administration absorbed 38% of incidents

SWITZERLAND · NCSC 2025 REPORTS

64,733 voluntary reports processed, up 2,000 on 2024
222 mandatory reports from critical infrastructure
Ransomware reports 104, up from 92 in 2024
2.35 million malware infections flagged, double 2024
Ransomware now routinely paired with data theft

What this means: volume is dominated by attacks that do not stop operations, so incident counts are a poor proxy for risk. The cases that breach data and halt services are a small share of the total, and they arrive through phishing, exposed vulnerabilities and stolen credentials, which is where control investment belongs.

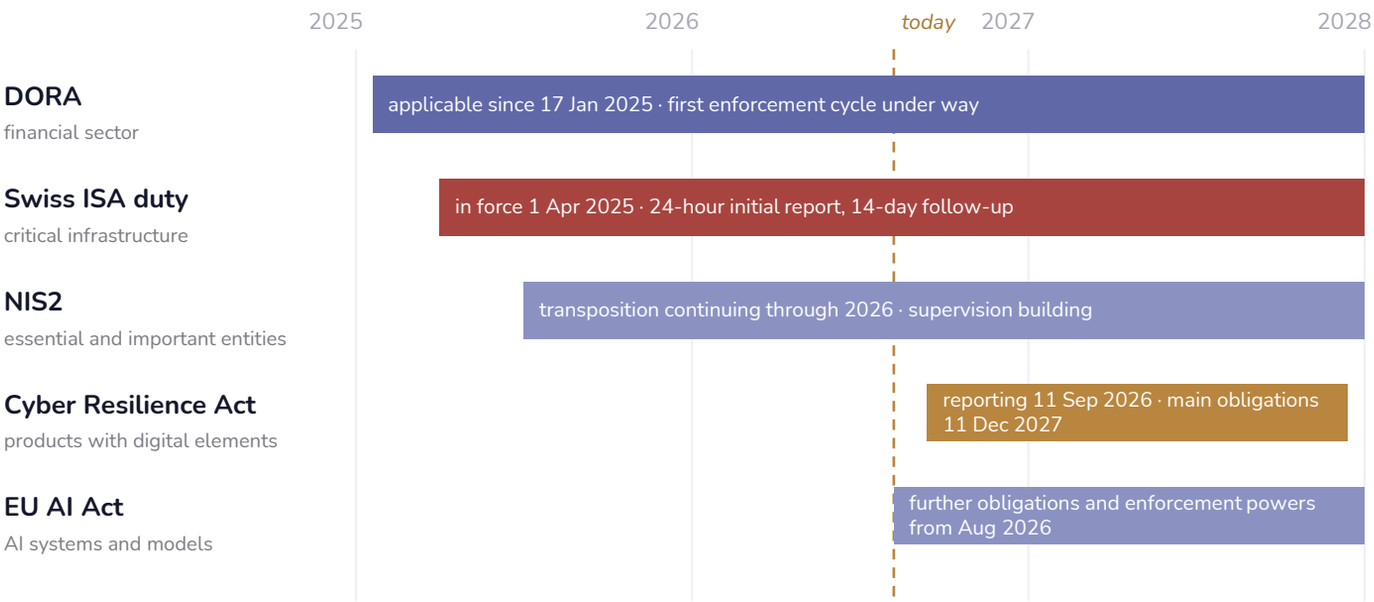
Sources *ENISA, Threat Landscape 2025 (October 2025, v1.2 January 2026): 4,875 incidents, 1 July 2024 to 30 June 2025. Swiss NCSC, Annual Report 2025 (16 February 2026) and Semi-Annual Report 2025/2 (30 March 2026). Figures cited with attribution; EU material reused under Decision 2011/833/EU.*

PANOP

06 · WHAT LANDS, AND WHEN

2026 is the year the rules start collecting

Four European instruments and one Swiss obligation move from transposition to enforcement inside eighteen months. The overlap is the difficulty: the same incident can trigger separate notifications to separate authorities on separate clocks.



CRA reporting of actively exploited vulnerabilities and severe incidents begins 11 September 2026 via the ENISA Single Reporting Platform, and applies to products already on the market.

THE SWISS OVERLAP IS THE SHARPEST

A single incident at a supervised financial institution that is also a critical infrastructure operator can trigger three separate notifications: to the NCSC under the Information Security Act, to FINMA under the Financial Market Supervision Act, and to the FDPIC if personal data was involved. Satisfying one does not satisfy the others, and the clocks differ.

Swiss organisations without an EU establishment are not directly bound by NIS2, DORA or the CRA, but reach them through EU customers, subsidiaries and contractual flow-down.

WHAT SUPERVISORS ACTUALLY ASK FOR

Across all five instruments the recurring demands are the same four artefacts: a current register of ICT dependencies, a documented and tested exit or continuity path for critical suppliers, incident classification criteria agreed before an incident rather than improvised during one, and evidence that the management body has substantively reviewed the risk position.

Build those once and each additional regime costs documentation rather than design.

Further change is already signalled: proposals presented in January 2026 under the Cybersecurity Act 2.0 label would adjust NIS2, revise certification frameworks and alter ENISA's role in incident reporting.

Sources *Regulation (EU) 2022/2554 (DORA); Directive (EU) 2022/2555 (NIS2); Regulation (EU) 2024/2847 (CRA); Regulation (EU) 2024/1689 (AI Act); Swiss Information Security Act art. 74a et seq. Descriptive only, not legal advice.*

PANOP

07 · WHAT FOLLOWS FROM THE DATA

Five priorities for the next twelve months

Every high-value control in this year's data is one that shortens the distance between exposure and evidence: what is reachable, who holds access, what your models send outward, and whether recovery has been tested rather than documented.

01

Exposure Management

Exploitation is the top entry route, at 31% of initial access. Patching cannot keep pace, so rank exposures by reachability and business criticality, and fix those first.

02

Vendor access, on evidence

Half of breaches involve a third party. Know which vendor holds which access, when it was last reviewed, and prove MFA is enforced rather than accepting an attestation.

03

Govern the AI you run

Shadow AI is 43% of AI-related incidents. One egress gateway, an inventory of agents and their tool permissions, and classification applied to prompts and retrieval context.

04

Verify identity out of band

Deepfake impersonation is now a leading AI-enabled attack type. Payment and access changes need confirmation on a channel the caller cannot choose.

05

Rehearse recovery

Sixty-nine percent of victims did not pay because restoring worked. A tested restore is the single best measured return in this year's data.

THE COMMON THREAD

The organisations that absorbed 2025 well were not the ones that avoided being hit. They were the ones that could see what was reachable, who held access, what their models were sending outward, and whether recovery had been tested rather than merely documented.

Sources *Priorities derived by Panop from the datasets cited throughout this report. Figures as published by IBM / Ponemon, Verizon, ENISA and the World Economic Forum.*

PANOP

08 · SOURCES, METHODOLOGY AND REUSE

Every figure traces to a public primary source

Panop has redrawn all charts from published numerical findings. No third-party graphics, figures or layouts are reproduced.

Source	Publication and date	Reuse position
ENISA	Threat Landscape 2025, 1 October 2025 (4,875 incidents, Jul 2024 to Jun 2025)	EU agency publication, open licence with attribution
Swiss NCSC / BACS	Annual Report 2025, 16 February 2026	Swiss federal publication, reuse with source citation
European Commission	DORA, NIS2, CRA and AI Act legal texts, via EUR-Lex	Official texts, reuse permitted with attribution
IBM Security / Ponemon	Cost of a Data Breach Report 2026, 29 July 2026 (602 organisations)	Freely published, cite findings with attribution
Verizon Business	2026 Data Breach Investigations Report (22,000+ confirmed breaches, 145 countries)	Freely published, cite findings with attribution
World Economic Forum	Global Cybersecurity Outlook 2026, 12 January 2026, with Accenture (804 respondents)	Cite findings with attribution, do not reproduce figures
Anthropic	Disrupting the first reported AI-orchestrated cyber espionage campaign, November 2025	Public threat report, cite with attribution

METHOD AND RIGHTS

Every figure in this report comes from a publicly available primary publication, cited on the page where it appears. Statistics are factual findings and are attributed to their publisher. Where a publisher applies a non-commercial or no-derivatives licence to its own document, that restriction applies to reproducing their material, not to citing their findings with attribution.

Prepared by Panop SA, Crissier, August 2026. Figures reflect the most recent editions available at the date of publication. This report is provided for information and does not constitute legal advice.

panop.io · support@panop.io · +41 21 539 15 07