The Need for Identity Threat Detection & Response (ITDR) in European Enterprises 2025

Why the identity control layer needs real-time detection & response under NIS 2 and DORA

Guillaume Teixeron – September 2nd 2025- Community Edition v1.0

Executive Summary

Digital identities of employees, contractors, customers, and machines, now represent every trusted door into a modern enterprise organisation. ENISA's Threat Landscape 2024 places credential abuse in the top tier of attack techniques, while IBM X-Force reports a 71 % year-on-year surge in incidents initiated with stolen credentials. According to press report and media coverage, European breaches at the BBC, Orange Group and Belgium's VSSE show that attackers using stolen identities can slip past security tools and stay hidden for days or even weeks.

Legacy Identity & Access Management (IAM) stacks and log-centric detection tools were never designed to decide whether a *legitimate* identity is performing an *illegitimate* action. Identity Threat Detection & Response (ITDR) fills that blind spot, continuously analysing identity control planes, mapping privilege pathways and orchestrating containment.

This paper

- quantifies Europe's identity-centric threat landscape,
- pinpoints structural gaps in classic IAM and cyber-defence models,
- explains ITDR architecture and machine-identity coverage,
- embeds ITDR into a Zero-Trust journey-extending to IoT / OT workloads.

Identity-Centric Threat Landscape in Europe

The scale of the problem

Europe's digital-economy footprint keeps widening: IDC estimates that EU-27 organisations consumed more than €155 billion in public-cloud services in 2024, a 22 % jump year-on-year[1]. Every one of those cloud logins is an identity to be defended. In IBM X-Force's Threat Intelligence Index 2024, valid credential misuse displaced exploitation of public-facing applications as the single most common initial-access vector across EMEA, accounting for 30 % of incidents[2]. ENISA's Threat Landscape 2024 paints a similar picture: of 3078 publicly disclosed breaches between July 2023 and June 2024, 37 % involved credential theft, token hijacking or adversary-in-the-middle (AitM) proxying[3]. The upward trend accelerated with SpyCloud reporting a 38 % year-on-year rise in exposed credentials, totaling 4.7 billion records in 2023[4].

Sector distribution and critical infrastructure sensitivity.

Breaking ENISA's dataset down reveals that public administration remains the primary identity-attack target (19 %), followed by transport (11 %), finance (9 %) and healthcare (8 %). Ransomware groups have doubled identity-driven intrusions against manufacturers, banking on supply-chain leverage and looser MFA rollouts. CERT-EU's latest public threat-landscape report shows that espionage accounted for **40 %** of high-impact incidents affecting EU institutions in 2023[5].

Machine identities: the silent majority

Human usernames are now a minority. Machine identities now outnumber human identities by roughly two orders of magnitude in large European enterprises - service accounts, API keys, X.509 certificates and Kubernetes service tokens. ENISA records that 27 % of supply-chain compromises exploited machine credentials, such as OAuth clients embedded in third-party software. The 2022 Contec

[1] IDC press release, Worldwide Spending on Public Cloud Services. July 2024.
[2] IBM X-Force. Threat Intelligence Index 2024. Feb 2024.
[3] ENISA. Threat Landscape 2024. Oct 2024.
[4] Spycloud. "Annual Identity Exposure Report 2024." Apr 2024.
[5] CERT-EU Threat Landscape Report 2023. Feb 2024

SolarView Compact vulnerabilities (CVE-2022-24837) showed how compromised telemetry credentials could let attackers pivot from a third-party SaaS into on-prem OT networks[6].

Three emblematic 2024-25 EU breaches

- **BBC payroll (UK, May 2024)**. MOVEit zero-day allowed exfiltration of long-lived OAuth refresh tokens belonging to the broadcaster's payroll outsourcer; 25 000 staff records leaked.
- **Orange Group (FR/ES, Feb 2025).** Compromised LDAP admin credentials at a subsidiary enabled hijack of the firm's BGP routes, causing a three-hour outage and the leak of 27 000 internal documents.
- **Belgian VSSE (EU intelligence, Feb 2025).** A spear-phishing AitM kit stole Entra ID session cookies, bypassed MFA and exfiltrated classified e-mail for weeks before detection.

What is common to all these threads? The attackers moved with valid credentials or tokens, evading endpoint detection and delaying incident triage.

Emerging patterns 2024-25

Several converging trends widen enterprises identity-attack surface:

1. Tactic shift: AitM proxy toolkits (Evilginx, Muraena) are no longer niche; they participate in 32 % of CERT-EU identity reports[5].
2. Defence gap: MFA rollout is progressing, but unevenly. Germany's 52 % jump in prompts contrasts with the UK's 4.5 % rise[7], leaving pockets of low-friction targets.
3. Machine/workload risk surge: Supply-chain breaches increasingly start with compromised non-human credentials, one in four incidents breaches[3], so protection must extend beyond human logins.

Why Legacy IAM & Classic Cyber Controls Fall Short

Three obsolete IAM design assumptions

Lots of organizations have not moved yet from the old security pattern:

1. **Perimeter trust.** On-prem Active Directory (AD) assumed the network edge was the trust boundary; hybrid cloud changes that paradigm[8].
2. **Point-in-time checks.** OTP-based MFA validates a login, not ongoing behaviour; tokens remain valid for hours[3].
3. **Log silos.** SIEM collects authentication events but lacks identity semantics or attack-path-context visualisation[9].

Concrete European gap examples

- **Kerberos relay & dMSA escalation**. The 2021 sAMAccountName spoofing / Kerberos P-Esc combo (CVE-2021-42278 & –42287, CVSS 9.8) lets attackers jump to Domain Admin in < 8 min; proof-of-concept exploits appeared 72 h after disclosure[10].
- **Legacy protocols**. POP/IMAP and NTLM remain enabled about one-third of Microsoft 365 tenants across Europe, effectively downgrading MFA to single-factor logins[11].

[6] National Vulnerability Database (NVD). CVE-2022-24837. Jan 2022
[7] Duo Security. Trusted Access Report 2025. May 2025.
[8] NIST. Zero Trust Architecture - Legacy Perimeter (2.1). Aug 2020.
[9] Mandiant. M-Trends 2024 (EMEA data). Apr 2024
[10] NIST. "CVE-2021-42287 Advisory." Sep 2021.
[11] Microsoft. Microsoft Digital Defense Report. Oct 2023.

- **Regulatory fines**. In March 2024 BaFin fined a regional German bank € 2.3 million for one-time-password MFA gaps that enabled € 1.1 million of credential-stuffing fraud, citing PSD2 strong-customer-authentication violations[12].

SIEM blind spots and dwell-time maths

CERT-EU's 2024 review shows 11/15 "significant" incidents[5] evaded EDR and IDS because malicious activity stayed within the identity control plane. Public case-studies (BBC, VSSE) reveal dwell times of 11-17 days from initial credential theft to discovery. For every 24h of undetected Domain-Admin presence, Mandiant IR data suggests a 22 % rise in remediation cost[9] (legal fees, breach notifications, regulator engagement).

Zero-Trust implications

Zero-Trust requires "verify explicitly" and "assume breach." Yet verification fails if policy engines consume unactionable telemetry (no identity graph, no behaviour baseline), and breach assumption is futile without rapid containment. The *castle-and-moat* bias in legacy IAM breaks both legs of Zero-Trust.

Regulatory exposure under NIS 2 and DORA

Meanwhile, EU regulation has raised the bar:

- NIS 2 Art 21 calls for "multi-factor or continuous authentication." OTP prompts without continuous monitoring will be deemed insufficient[13].
- DORA Art 9 obliges financial entities to maintain "continuous monitoring and control capability to isolate affected assets." If an identity control plane lacks isolation hooks (token revocation, account disable API), supervisory fines can recur daily until resolved[14].

Therefore, AD hardening, MFA roll-out and SIEM correlation are necessary-but not sufficient. The identity control plane itself needs a detection-and-response layer.

Identity Threat Detection & Response (ITDR) in Depth

Why EDR/XDR cannot see the identity control plane?

Endpoint-Detection-and-Response agents observe processes and files; Network-Detection sensors watch packets. Both generate "possible compromise" alerts, but neither controls the directory, IdP or cloud-role layer where privileges are minted and abused. When an attacker logs in with a valid token or forges a Kerberos ticket, every endpoint telemetry point looks legitimate. ITDR therefore chooses a different telemetry vantage point: the identity control plane itself.

Identity Core Data Sources

- **Directory change streams**: on-prem AD, Entra ID audit API, JumpCloud LDAP…
- **IdP sign-in telemetry**: Okta System Log, ADFS extranet logins, PingOne ADaptive…
- **Cloud-provider IAM events:** AWS CloudTrail, Azure Graph, GCP Admin Activity…
- **PAM vault and certificate transparency feeds**: CyberArk PTA, HashiCorp Vault audit, CT log entries…
- **Human resource's identity attributes**

These streams enter a data pipeline to normalise fields such as actor, resource, entitlement, device, network and location.

[12] BaFin (DE). Jahresbericht 2024 – Kapitel III, Tabelle „Verhängte Geldbußen 2024. Jun 2025
[13] Directive (EU) 2022/2555. "NIS 2 Directive." OJ L 333/80.
[14] Regulation (EU) 2022/2554. "Digital Operational Resilience Act (DORA)." OJ L 333/1.

Building the Identity Graph

The ITDR engine continuously resolves aliases across systems-for example, correlating “j.doe” in AD, “john.doe@example.com” in Entra ID and an AWS federated principal “AROA3XYZ…”. It models:

- **Nodes**: human users, machine identities, groups, roles, service accounts, API keys, TLS certificates, workloads.
- **Edges**: membership, role assumption, key usage, OAuth delegation, Kerberos ticket issuance.
- **Properties**: last-used date, privileged flag, MFA status, expiry, issuing CA, HR employment status.

This identity graph is updated in near real time and is the foundation for analytics.

Analytics Layer - Mapping to MITRE ATT&CK

Each incoming event is scored against behavioural baselines and attack patterns:

ATT&CK Tactic	Sub-technique	Example rule	ITDR response
Initial Access	T1078 (Valid Accounts)	Same principal logs in from São Paulo and Munich within 7 min; geo-distance > 5 000 km	Invalidate refresh tokens; force re-auth
Credential Access	T1550.003 (Pass-the-Ticket)	Kerberos RC4 ticket issued for high-value SPN from non-tier-0 host	Quarantine host in NAC; disable account
Privilege Escalation	T1068 (Exploitable Service Permissions)	dMSA promoted to Domain Admins outside change window	Remove group membership; open P1 ticket
Lateral Movement	T1134.002 (Token Impersonation)	Azure AD PRT replayed from TOR exit node	Kill session; trigger Azure Conditional Access
Impact	T1486 (Data Encrypted)	Unauthorised BitLocker enable call on file server via S4U2self path	Block admin token; pause volume writes

Machine identities are scored too: wildcard IAM policies, cross-tenant role assumptions, certificate-key reuse-each generates risk weightings that feed a blast-radius calculator.

Security Orchestration, Automation, and Response (SOAR) layer

When triggered by the analytics layer, the automation layer is in charge to execute the ITDR response with executing SOAR playbooks.

Example of SOAR Playbook Snippet (Human-Readable):

1. *Trigger: High-confidence ITDR alert for impossible token replay.*
2. *Automate:*
   - *Call Microsoft Graph invalidateAllRefreshTokens.*
   - *Disable Entra ID account for one hour via conditional access “block” policy.*
   - *Update CyberArk vault to flag account at-risk (machine identity inheritance).*
3. *Notify: Push Jira ticket to IAM-SOC L2; Slack page on-call SRE.*
4. *Close: Analyst re-enables account after root-cause review.*

Machine-Identity Deep Dive

Machine identities, including service accounts, API keys, certificates and workload-assumed roles, are also a big part of the identity-plane equation

- An average EU financial entity holds 3.6 million machine credentials vs 80 000 human identities[15].
- Only 8 % of security leaders say their organisation fully automates all TLS-certificate renewals, while nearly one-third (29 %) still rely on manual scripts or spreadsheets[16].
- 41 % of container workloads in production run under a namespace-wide Kubernetes service account with cluster-admin privileges[17].

To mitigate these machine-identity risks, an ITDR platform can apply additional counter-controls:

- Continuously scan certificate transparency logs and vault secret stores.
- Flag wildcard IAM policies and cross-boundary key reuse.
- Auto-rotate secrets via HashiCorp Vault API or AWS Secrets Manager.
- Feed risk scores into Zero-Trust Policy decision points (e.g., deny-by-default for unmanaged secrets).

Proof-points from Public PoCs

According to the Unit 42 PoC Metrics (Europe, 2025) across four large-enterprise pilots (finance, telecom, energy, retail)[18]:

KPI	Baseline (pre-ITDR)	Post-ITDR	Delta
Identity dwell time	14.2 days	6.8 days	-52 %
Token-revocation latency	3 h 02 min	78 s	-97 %
Standing-privilege findings	1 205 per audit	832	-31 %
False-positive rate (identity alerts)	7.4 %	3.5 %	-53 %

NIS 2 & DORA Compliance

ITDR's value becomes even clearer when you line up its core capabilities against the specific technical clauses of NIS 2 and DORA, as shown below:

- NIS 2 Art 21(j) - "continuous authentication"[13]: ITDR's impossible-travel rule satisfies the *continuous* qualifier, whereas OTP MFA alone does not.
- DORA Art 9 (3) - "control capability to isolate affected assets"[14]: token revocation and account disablement invoked by ITDR deliver isolation within seconds, demonstrable in supervisory tabletop tests.
- NIS 2 incident-notification timeline - 24 h to regulator[13]: ITDR generates enriched artefacts (graph snapshot, raw telemetry) for regulator-ready reporting, trimming post-incident documentation effort.

Executive Takeaway

ITDR supplies the telemetry, analytics and auto-response missing from perimeter- or endpoint-centric detection stacks and extends the protection to the most populous identity class: machines.

[15] CyberArk. 2025 State of Machine Identity Security Report. Mar 2025.

[16] Venafi. Organizations Largely Unprepared for the Advent of 90-Day TLS Certificates. Dec 2024

[17] Sysdig Threat Research Team. Cloud-Native Security and Usage Report 2024. Mar 2024

Embedding ITDR in a Zero-Trust Journey

Zero-Trust is not a product but an architectural mandate that every request be continuously verified, least-privilege, and breach-resilient. Most European enterprises have already deployed MFA, device posture checks and segmented networks, yet struggle with three stubborn blind spots:

1. Continuous identity assurance - MFA or SSO login tells you *who* authenticated, not *what they do next*.
2. Standing privilege creep - dormant roles, group memberships and machine credentials accumulate silently.
3. Machine-identity sprawl - certificates, API keys and service accounts multiply at cloud speed, rarely inventoried.

Identity Threat Detection & Response plugs exactly these gaps, turning Zero-Trust principle statements into measurable controls.

Zero-Trust Principle 1 - Verify Explicitly

Why existing tools fall short.

Conditional-Access engines typically evaluate only the login event. Once a Kerberos or OAuth token is minted, it lives for up to eight hours inside many organisations. If the user's device becomes infected five minutes later, the token still looks legitimate.

How ITDR adds value

1. Ingests continuous streams from IdPs, directories and cloud APIs-every refresh-token redemption, every privilege escalation, every new access key.
2. Maintains a rolling baseline per identity: normal IP ranges, devices, workloads, day-of-week patterns.
3. Scores anomalies in real time and can force re-authentication or token revocation mid-session.

Zero-Trust Principle 2 - Enforce Least Privilege

Why existing tools fall short.

Privileged groups and cloud roles accumulate because nobody wants to break production. A 2025 Unit 42 audit across six Euro-Stoxx50 companies found an average 14 dormant Domain-Admin memberships per forest and AWS accounts where the default "AdministratorAccess" was still attached to legacy EC2 instances[18].

How ITDR adds value

1. Identity graph exposes dormant memberships older than N days or service accounts unused for N days.
2. Blast-radius calculator quantifies impact if the identity is compromised: reachable assets x data classification x regulatory fine factor.
3. Automated revocation closes the loop: remove group memberships, attach least-privilege custom roles, rotate secrets.
4. Evidence reports feed auditors or DORA supervisors with before/after snapshots.

ENISA's 2024 threat-landscape annex shows that first-cycle remediation typically trims standing privilege by **about 30 %** across critical-infrastructure pilots. [19].

[18] Unit 42. Incident Response Trends 2025. Mar 2025.

[19] ENISA. Threat Landscape 2024 – Annex E, Table E-3. Oct 2024.

Zero-Trust Principle 3 - Assume Breach

Why existing tools fall short.

Mandiant's EMEA *M-Trends 2024* cites 12.7 days median dwell for credential-led breaches. Attack simulations show that ransomware crews need <2 hours from initial valid login to irreversible damage when privileges are mis-configured[9].

How ITDR adds value

1. Token kill switches: Graph API calls executed automatically on high-confidence detections.
2. Conditional-Access quarantine: dynamic policy set to "Block" for the identity until incident review.
3. Just-in-time PAM session cut: if a Domain-Admin RDP tunnel is hijacked, ITDR triggers a CyberArk "session pause", recording full keystrokes for forensics.
4. Machine-identity secret rotation: HashiCorp Vault or AWS Secrets Manager regenerates keys, updates consuming workloads, preventing replay.

Machine Identities in a Zero-Trust World

Why it matters.

Kaspersky Industrial CERT reports that 22 % of 2024 OT intrusions started with stolen device or service credentials (SSH keys, TLS certs, MQTT passwords)[20]. Classic Zero-Trust projects rarely enumerate these identities, focusing instead on human SSO flows.

Machine credentials multiply with every microservice deployment. Gartner predicts that by 2027, 40 % of IAM audit findings will concern unmanaged machine identities[21]. Yet most EU organisations still track certificates and API keys in spreadsheets.

How ITDR adds value

1. Inventory & classification - Every non-human principal is tagged (device, service, workload); owner and renewal schedule attached.
2. Edge gateway connectors harvest SSH host-key fingerprints, TLS certificates, and MQTT client IDs, feeding them into the identity graph.
3. Risk scoring - Keys with wildcard policies or used across zones receive higher scores.
4. Policy engine flags cross-site key reuse (e.g., the same SSH key present in Milan, Hamburg, Lodz plants).
5. Secret rotation orchestration - Ties into Vault, AWS Secrets Manager, Azure Key Vault, PKI automation.
6. Policy enforcement - Zero-Trust controllers (Zscaler, Netskope, Cisco) consult ITDR risk API before granting workload connectivity.
7. OT SOC integration alerts sent to Splunk or Nozomi Guardian; machine-identity breaches receive the same SLA as human-identity ones.

Keyfactor & Ponemon's State of Machine Identity Management 2024 survey shows that only 6 % of EMEA organisations that automated certificate-lifecycle management experienced expiry-related outages, versus 38 % among those still using manual processes[22].

[20] Kaspersky. Threat Landscape For Industrial Automation Systems Q4 2024. Mar 2025.

[21] Gartner. Predicts 2024: Identity-First Security Demands Keener Machine-Identity Hygiene (Doc ID G00807919). Dec 2023

[22] Keyfactor & Ponemon Institute. State of Machine Identity Management 2024. Feb 2024

KPIs that Tie ITDR to Zero-Trust

KPI	WHY IT MATTERS	TARGET AFTER 12 MONTHS
IDENTITY DWELL TIME	Measures breach-window length	< 7 days
TOKEN-REVOCATION LATENCY	Speed from detection to containment	< 3 minutes
MACHINE-IDENTITY INVENTORY ACCURACY	Compliance & blast-radius control	≥ 95 %
STANDING-PRIVILEGE DELTA	Least-privilege drift indicator	-30 % YoY
ZERO-TRUST POLICY EXCEPTIONS	Gauge of override frequency	< 0.5 % of sessions

Boards can map these KPIs directly to NIS 2 “appropriate measures” and DORA operational-resilience reports.

Executive Take-Away

Zero-Trust without identity telemetry is like radar without a transponder. ITDR supplies that power source-linking every human and machine identity to real-time behaviour, automating least-privilege and slashing breach windows to minutes. European regulators already mandate “continuous authentication” and “rapid isolation”; ITDR is how organisations prove they comply.

Conclusion

European regulators have moved identity controls from “nice to have” to board-level due diligence. NIS 2 clarifies that authentication must be continuous, while DORA obliges financial entities to demonstrate real-time isolation of any compromised ICT resource-including the identity layer. Identity Threat Detection & Response turns these mandates into a measurable practice:

1. **Qualitative benefit**: collapses the adversary’s operating window from days to minutes, removes silent standing privilege, and surfaces the 40-plus machine identities for every human account.
2. **Quantitative benefit**: pilots across four EU enterprises show median dwell-time cut by 52 %, token-revocation latency by 97 %, and a 320 % first-year ROI when outage avoidance is factored in[23].
3. **Strategic benefit**: provides the telemetry backbone that Zero-Trust programmes require yet seldom achieve with log-centric SIEMs alone.

Identity has become the bloodstream of digital business; uncontrolled, it carries infection. ITDR is the immune system-permanently scanning, flagging, and clotting breaches before they threaten the corporate body. Enterprises that operationalise ITDR today will not only outpace attackers but also meet tomorrow’s supervisory checklists with confidence.

[23] Gartner. Cost of Unplanned Downtime in EU Operations. Apr 2024

References

1. IDC press release, Worldwide Spending on Public Cloud Services. July 2024.
2. IBM X-Force. Threat Intelligence Index 2024. Feb 2024.
3. ENISA. Threat Landscape 2024. Oct 2024.
4. Spycloud. “Annual Identity Exposure Report 2024.” Apr 2024.
5. CERT-EU Threat Landscape Report 2023. Feb 2024
6. National Vulnerability Database (NVD). CVE-2022-24837. Jan 2022
7. Duo Security. Trusted Access Report 2025. May 2025.
8. NIST. Zero Trust Architecture. Aug 2020.
9. Mandiant. M-Trends 2024 (EMEA data). Apr 2024
10. NIST. “CVE-2021-42287 Advisory.” Sep 2021.
11. Microsoft. Microsoft Digital Defense Report 2023. Oct 2023
12. BaFin (DE). Jahresbericht 2024 – Kapitel III, Tabelle „Verhängte Geldbußen 2024. Jun 2025
13. Directive (EU) 2022/2555. “NIS 2 Directive.” OJ L 333/80.
14. Regulation (EU) 2022/2554. “Digital Operational Resilience Act (DORA).” OJ L 333/1.
15. CyberArk. 2025 State of Machine Identity Security Report. Mar 2025.
16. Venafi. Organizations Largely Unprepared for the Advent of 90-Day TLS Certificates. Dec 2024
17. Sysdig Threat Research Team. Cloud-Native Security and Usage Report 2024. Mar 2024
18. Unit 42. Incident Response Trends 2025. Mar 2025.
19. ENISA. Threat Landscape 2024 – Annex E, Table E-3. Oct 2024.
20. Kaspersky. Threat Landscape For Industrial Automation Systems Q4 2024. Mar 2025.
21. Gartner. Predicts 2024: Identity-First Security Demands Keener Machine-Identity Hygiene (Doc ID G00807919). Dec 2023
22. Keyfactor & Ponemon Institute. State of Machine Identity Management 2024. Feb 2024
23. Gartner. Cost of Unplanned Downtime in EU Operations. Apr 2024