DARKTRACE

ANNUAL THREAT REPORT 2026: KEY TAKEAWAYS

The cyber threat environment in 2025 was defined by acceleration, convergence, and complexity. Adversaries are no longer relying solely on traditional exploits; they are weaponizing AI to automate attacks, evade detection, and scale operations at unprecedented speed. This evolution marks a shift from opportunistic campaigns to highly adaptive, intelligence-driven intrusions.

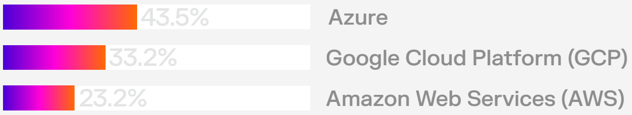
01 IDENTITY IS THE NEW PERIMETER

~70% of incidents in the Americas originated from Software-as-a-Service (SaaS)/Microsoft 365 compromise or phishing, making credential abuse the single most effective initial access vector.

58% of incidents in Europe from cloud account and email compromise, exceeding network-based compromise (42%).

02 CLOUD & SAAS AMPLIFY SYSTEMIC RISK

■ **honeypot malware samples targeted:**

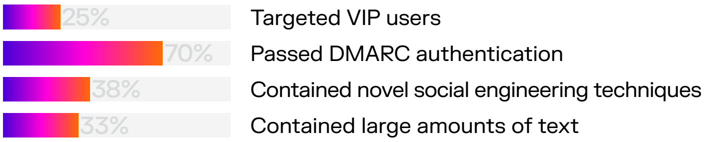


2 Minutes time **to exploitation of React2Shell (CVE-2025-55182) after deployment of Darktrace's honeypot**

DOWNLOAD THE FULL REPORT ↗

03 EMAIL REMAINS THE MOST RELIABLE ATTACK CHANNEL

32+ million **high-confidence phishing emails detected by Darktrace / EMAIL™ globally**



1.2 million **used QR codes**

04 RANSOMWARE IS A PROFESSIONALIZED ECOSYSTEM

Top 5 strains: Akira, Qilin, RansomHub, Lynx, INC

Top 5 sectors globally impacted sectors: Manufacturing; Information & Communication; Construction; Healthcare; and Wholesale & Retail.

~ 50% of Akira and Qilin cases **included compromised administrative or service credentials were used for initial access or lateral movement**

05 CRITICAL INFRASTRUCTURE IS A STRATEGIC TARGET

Stage 1 Industrial Control System attack observed that originated from a compromised SaaS account within a European renewable energy organization. **Nation-state activity** observed across telecom, energy, healthcare, and finance

06 VULNERABILITY EXPLOITATION IS OUTPACING DISCLOSURE AND PATCHING

- +20.6% YoY increase in Common Vulnerabilities and Exposures (CVEs) disclosed
- 18 days before disclosure Darktrace identified model alerts related to CVE exploitation of Trimble Cityworks
- 6 days before disclosure of SAP NetWeaver (CVE-2025-31324) Darktrace detected anomalous behavior, including observing suspicious patterns indicative of exploitation attempts against Enterprise Resource Planning (ERP) systems.