Aug, 2025

INTELLIGENCE INSIGHTS EUROPE

Defend against what’s ahead by uncovering month-on-month trends and insights for Europe’s threat landscape (Jun - July)

Key Insights

- Crypto24 published a post on their DLS website with data related to Larimart S.p.A.: an Italian defense and security company, part of Leonardo Group.
- Devman 2.0 published a post on their DLS website with data related to Elis Portugal: a Portuguese branch of a French multinational provider of textile, hygiene, and facility services.
- Rhysida ransomware group published a post on their DLS website with data related to Welthungerhilfe: a German non-denominational and politically independent non-profit and non-governmental aid agency.
- Server Killers, NoName057(16), Z-ALLIANCE and Mr Hamza participated in an operation FuckEastwood targeting government websites in Germany, Italy, Belgium, Spain, Romania, Latvia and Czechia as well as website of Europol as an act of retribution for Operation Eastwood: a major, coordinated international law enforcement operation led by Europol and supported by Eurojust, targeting the pro-Russian cyber-crime and hacktivist group known as NoName057(16).

Val Shirko
Regional Business Head, Europe

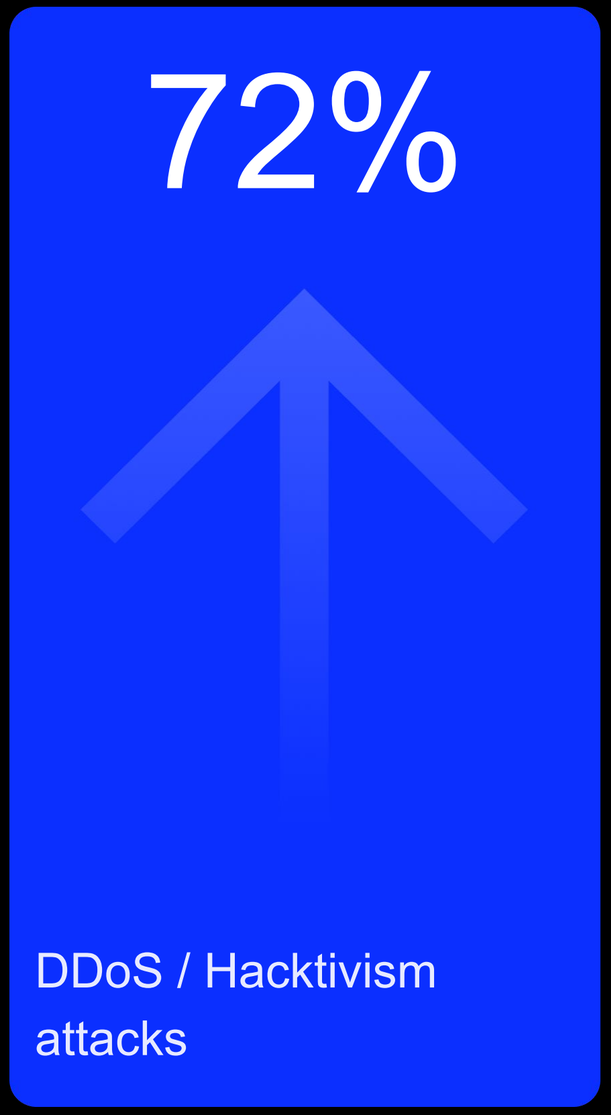
This report offers an overview of the latest threat landscape in Europe, covering key developments such as ransomware attacks, leaked credentials, data breaches, and more. It includes a month-over-month trend analysis to track evolving patterns. Additionally, the report spotlights a newly identified threat actor, campaign, emerging technique, providing actionable insights for proactive defenses.

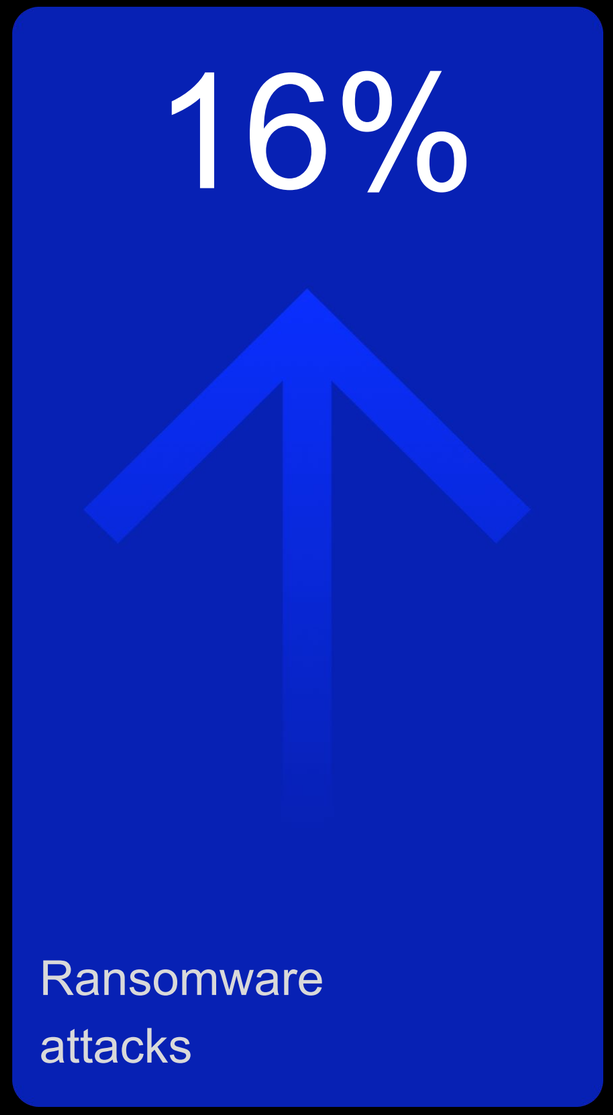
Click here to take a 1-min survey now to improve the report.

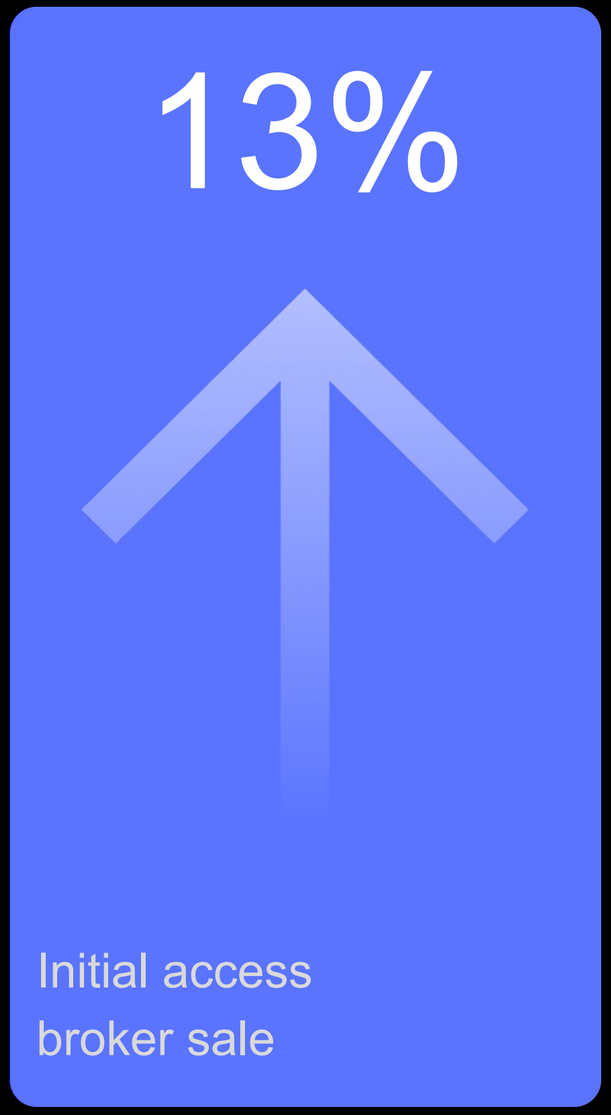
THREAT LANDSCAPE

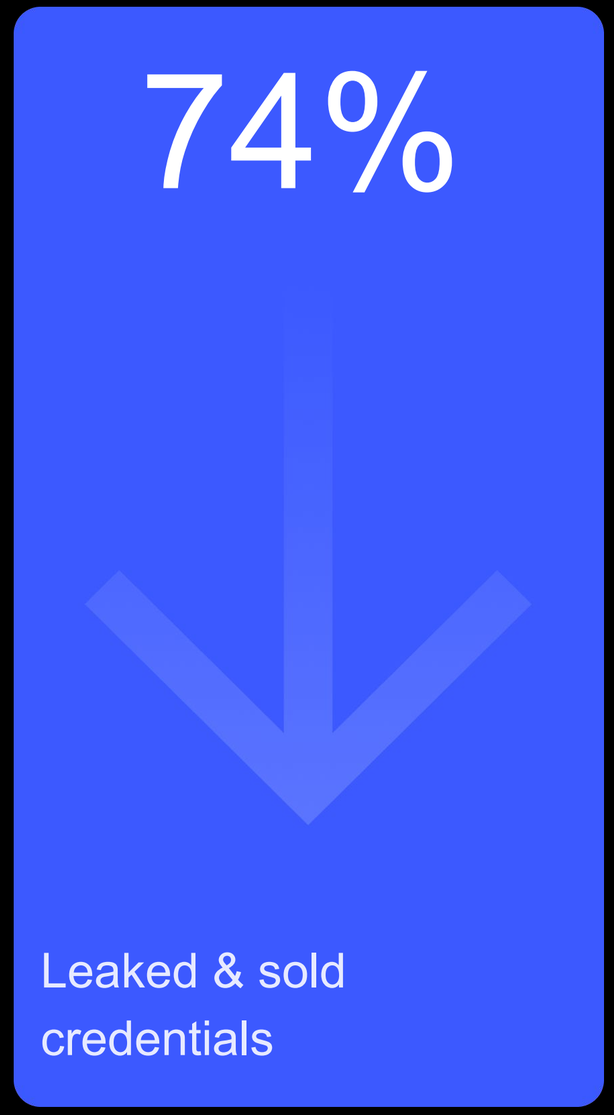
GROUP-IB

Month over Month Comparison
(June vs July)









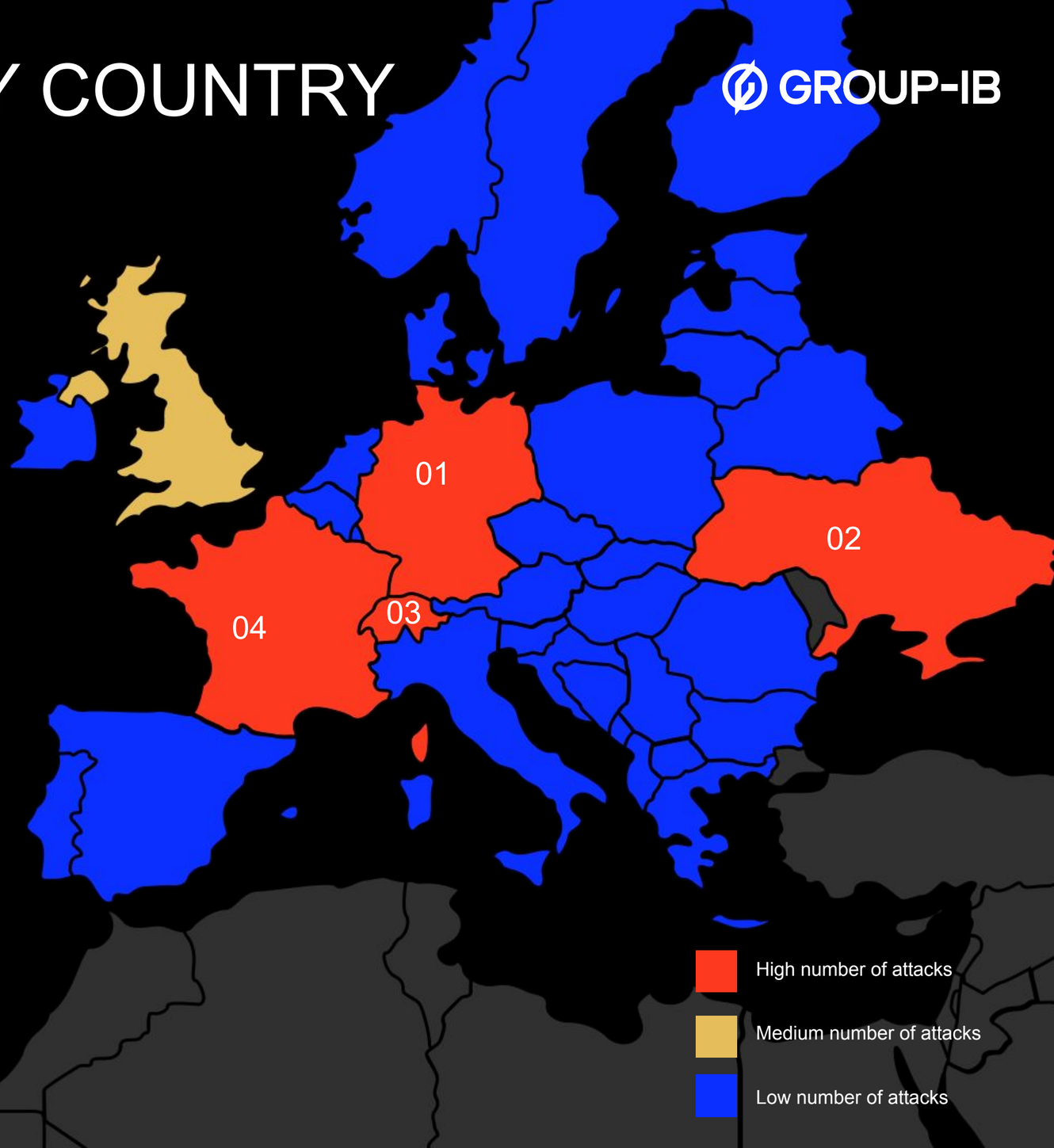
DDOS AND HACKTIVISM BY COUNTRY

Key Events

- Server Killers, NoName057(16), Z-ALLIANCE and Mr Hamza participated in an operation FuckEastwood targeting government websites in Germany, Italy, Belgium, Spain, Romania, Latvia and Czechia as well as website of Europol as an act of retribution for Operation Eastwood: a major, coordinated international law enforcement operation led by Europol and supported by Eurojust, targeting the pro-Russian cyber-crime and hacktivist group known as NoName057(16). The operation took place between July 14 and 17, 2025 across numerous countries.

Most attacked countries

Germany	Ukraine	Switzerland	France
61 attacks	58 attacks	18 attacks	14 attacks
+ 455%	+ 57%	+ 800%	+ 180%



RANSOMWARE ACTIVITIES

GROUP-IB

Key Events

- In July 2025 Group-IB experts discovered five new ransomware groups: Sinobi, Payouts King, D4RK 4RMY, RansomedVC2, BQTLock.
- Rhysida ransomware group published a post on their DLS website with data related to Welthungerhilfe - a German non-denominational and politically independent non-profit and non-governmental aid agency.
- Devman 2.0 published a post on their DLS website with data related to Elis Portugal - a Portuguese branch of a French multinational provider of textile, hygiene, and facility services, supporting healthcare, industry, and hospitality sectors.

↑ 16%

94 Ransomware incidents

Most active threat actors

Qilin

18 attacks
- 25%

Akira

14 attacks
+ 40%

Safepay

11 attacks
+ 175%

INC Blog

7 attacks
+ 75%

Cl0p

6 attacks
(June at 0)

Most targeted industries

Manufacturing

17 attacks
+ 89%

Retail

10 attacks
+ 233%

Construction

7 attacks
+ 17%

Education

5 attacks
+ 400%

Automotive

5 attacks
+ 400%

INITIAL ACCESS BROKER SALE ON DARK WEB

↑ 13%

54 Sales

GROUP-IB

Initial access to a company's system can lead to data theft, corporate espionage, or the installation of malware for various malicious purposes. This page illustrates the volume and geographic distribution of corporate infrastructure accesses currently being sold on the dark web.

Key Event

The Group-IB team analyzed a phishing campaign impersonating **Salesforce** that targeted companies in the United States, Canada, Taiwan, the Netherlands, the United Kingdom, and Germany.

Most targeted countries

LEAKED & SOLD CORPORATE CREDENTIALS

GROUP-IB

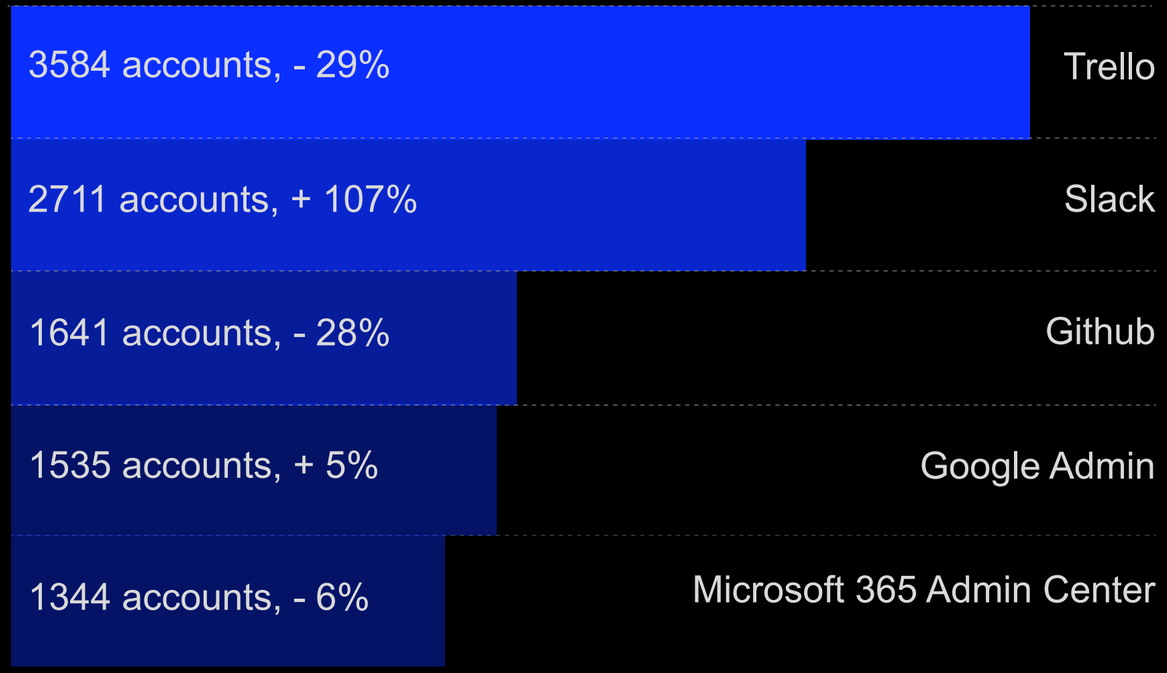
Key Events

- Most of detected compromised corporate accounts in Europe detected in July belong to users from Italy, Spain, France, Poland and the United Kingdom.

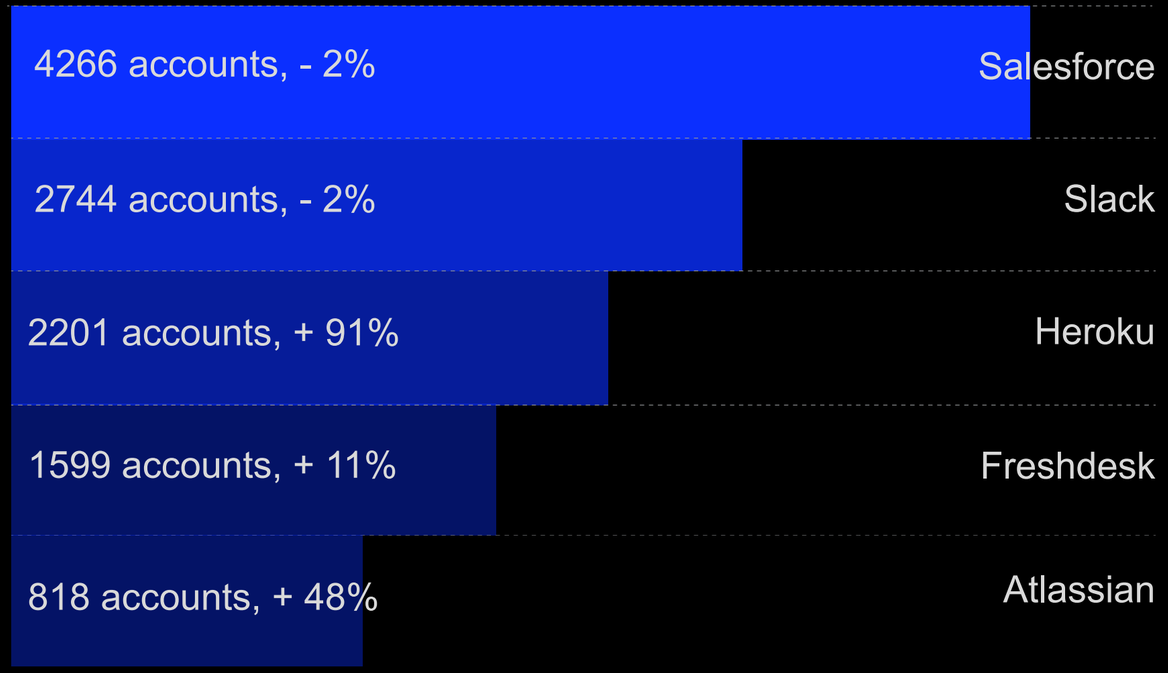
↓ 75%
Compromised account: 381,776

↑ 20%
on sale on dark web markets: 20,581

Services with the most compromised accounts



Services with the most on sale accounts



Scam Spotlight

GROUP-IB

Scam case

Fake Receipts Generators

Key Observations

- MaisonReceipts offers a fake receipt generator through a tiered subscription model, supporting over 21 well-known brands.
- Receipts are customizable and localized, with formats tailored for the US, UK, and EU.
- Other similar platforms (e.g., Receiptified.com) are emerging, suggesting a broader trend in the fake receipt generator market.

Read more in our recent blog.

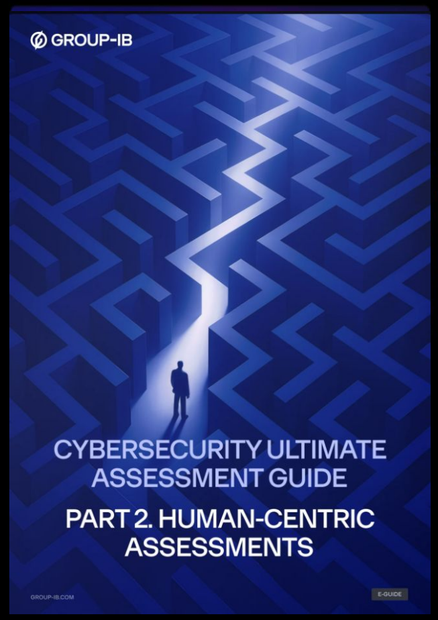
Click here to take a 1-min survey now to improve the report.

STAY SMART. STAY CONNECTED. STAY SECURED

[Talk to our team]

RECENT RESOURCES

Read now



Read Now

MEET US AT EVENTS