YARIX
a vargroup company

H1 2024
CYBER NUMBERS

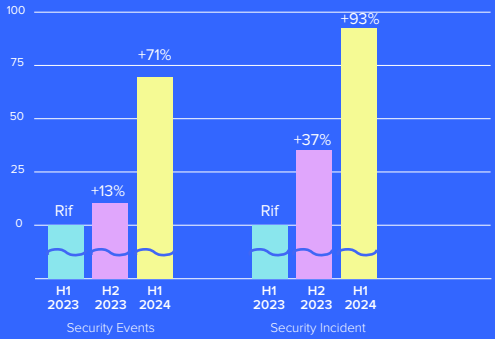
SECURITY OPERATION CENTER

Total events analysed | H1 2024

67.797
Security incidents

182.248
Security events not leading to incidents

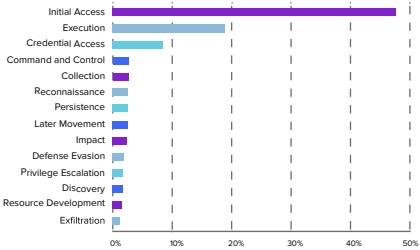
Distribution of events | H1 23 - H2 23 - H1 24



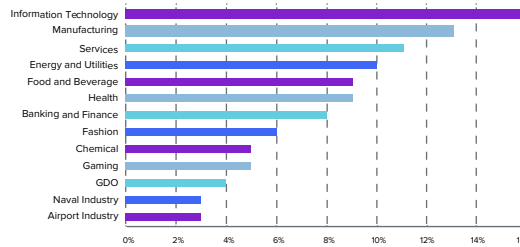
In the first half of 2024, Yarix's Security Operation Center observed a significant increase in recorded security events. Specifically, there has been a 71% growth compared to the same period last year, and 80% of the total events from last year have already been analysed. Notably, there has been a 93% rise in security incidents compared to the same period in the previous year, highlighting the increasing severity of attacks, as well as a rise in their volume.

SECURITY OPERATION CENTER

Mitre ATT&CK Tactics | H1 2024



Security events in H1 2024 subdivided by industry



The analysis of data by industry has revealed a significant increase in detections in the IT sector (from 9% to 16% of the total) and in Services (from 8% to 11%), while the Manufacturing sector remains in the top positions as in the previous year, consistently ranking as the second most affected industry. The mapping of events against MITRE Tactics highlights the clear predominance of detections in the initial phases of attacks, thanks to the SOC's ability to identify and intervene early.

INCIDENT RESPONSE

Threat Actor H1 2024:

Total Identifications	**20**
Unknown actors	**21**

Akira **QLIN** BlackBasta
MONTI **Mamba** Phobos
ALPHV/BlackBasta Medusa
Lockbit 3.0 FOG
Globeimposter2.0 **Cactus**
PHOBOS **Rhysida** Lockbit3
SURTR

INCIDENT RESPONSE

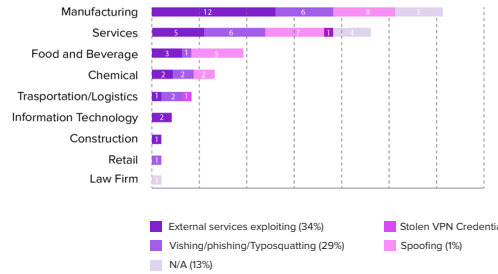
During H1 2024 the YIR Team managed a total of 77 cases, including:

44 Incidents with “high” or “critical” severity (IR)

9 Forensic investigations (FOR)

25 Business Email Compromise (BEC)

Attack vectors by type of industry



The Incident Response market is evolving, and with it, the types of attacks that are most frequent. In fact, it is already evident that in the first quarter of 2025, there has been a noticeable increase in business email compromise attacks, while ransomware attacks, which involve encrypting systems, have seen a decline. But what is driving this shift in the market? According to our estimates, recent attacks against criminal organisations by security agencies such as Europol and the FBI have had a significant impact on ransomware groups, which currently appear to be undergoing internal reorganisation.

CYBER THREAT INTELLIGENCE

In H1 2024, the YCTI team reported a total of **1,386 significant events**, including:

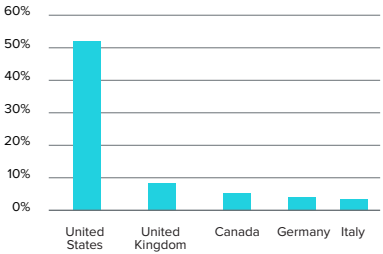
952 **Cyber Intelligence, Data Leakage and VIP Protection events**

104 **Early Warning events**

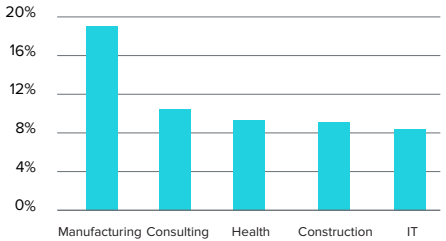
330 **Anti-Phishing events and consequent activities to combat these attacks**

CYBER THREAT INTELLIGENCE

Top 5 sectors for Countries events H1 2024



Top 5 sectors for Ransomware events H1 2024



The Cyber Threat Intelligence team has identified a significant increase in “deep fake” scams targeting C-level executives in the first part of 2024. Cyber criminals are using AI tools and technologies to steal money from medium and large companies.

RED TEAM

TOP 10 YRT 2023:

01 - Active Directory security and poor account management

02 - Partial coverage by protection systems

03 - Bad Practice in application development by suppliers - NEW

04 - Nonconforming management of confidential information

05 - Badly configured VPNs - REVIEW

06 - Inefficiencies in detection processes - REVIEW

07 - Incomplete or inaccurate reconstructions of security events - REVIEW

08 - Ineffective password policies

09 - Poor control of public attack surface area - REVIEW

10 - Haphazard application of Two-Factor Authentication

RED TEAM

120 Employees with email account

10,1% Employees report the email as phishing

41,3% Employees open the phishing email

34,2% Employees interact with the link or button it contains

27,7% Employees enter one or more valid credentials in the trap form

40.000
Unique passwords recovered from hash

58%
Success rate in less than 2 weeks

Ineffective or incompletely applied **password policies**

Failure to apply blacklists

Poor awareness on the part of users

The spear phishing campaigns carried out by YRT in 2024 targeted narrower groups and adopted a more tailored approach. As a result, there has been a significant increase in the percentage of victims, particularly in terms of interactions with malicious links and credential theft. The most popular themes are those related to welfare initiatives.