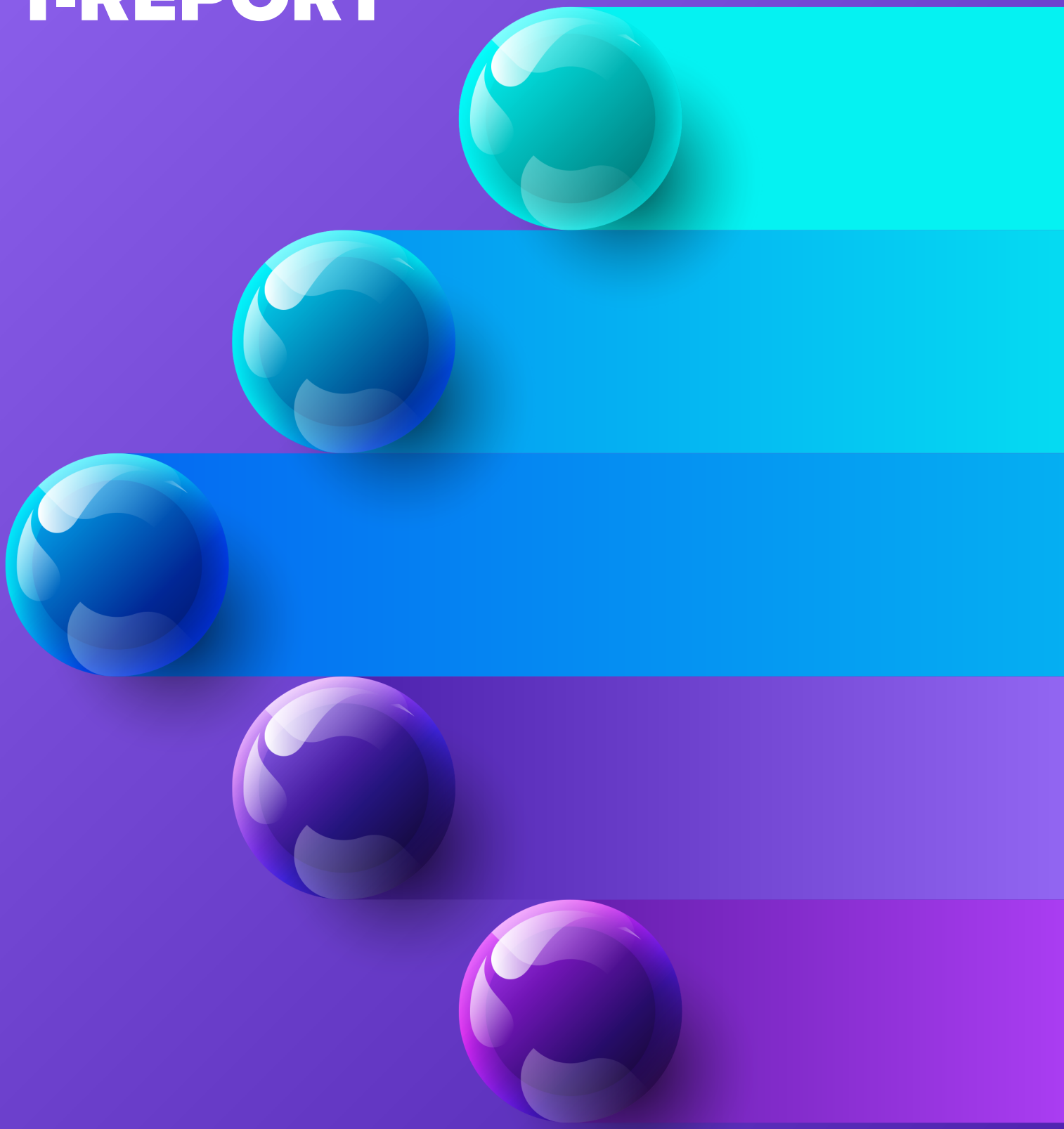
YARIX
a vargroup company

2024 Y-REPORT



Contents Index

Contents Index

Introduction

New in 2023

The purpose of this document is **to provide an accurate, up-to-date overview of the scenario regarding the IT threats** which hit Italy and other international players during 2023, in order to analyse and assess the trends and the mitigation actions necessary to reduce the impact of cyber attacks.

The report, first issued in 2019 and published here in its fourth edition, **aims to process the data received and analysed by the Var Group's Security Operation Center** and the **main areas covered by its Digital Security business line**, and to supply a full survey of IT security trends during 2023.

A new appendix on cyber security in the Automotive industry has also been introduced.

This section, which focuses on the new regulatory trends responding to the need to apply more and more effective, tighter protocols in the automotive field as elsewhere, was developed thanks to input from Var Group Digital Security German firm CYRES Consulting.

About us: Digital Security Var Group

Digital Security is the Var Group business unit dedicated to the IT security universe.

It is a pole of excellence, with locations in Italy and Europe, working to guarantee advanced defence in all sectors of cyber security, delivering specialist expertise to tackle digital security challenges with determination and agility.

Heading the Digital Security business unit, **Yarix** is recognised as a leader in the cyber security field, having directed its mission to the development of specific solutions for businesses and government organisations, public health trusts, schools and universities.

It was Italy's first private sector company to be admitted to **FIRST**, the global protection network that includes players such as NASA, Apple and Google with the aim of combating emerging threats.

A member of the Digital Security division of Var Group GmbH since 2022, **CYRES Consulting** is a pillar in the provision of consultancy for the implementation of cyber security in engineering and development, especially in the automotive industry.

Its interdisciplinary team of experts, headquartered in Munich, Germany, works together with a network of partners and independent consultants to provide state-of-the-art consultancy and training services, always in line with the current regulatory framework.

Introduction

Method

The report studies the data which Yarix received and analysed during 2023, its period of reference. **Information is sourced from a specific panel of businesses monitored by the Security Operation Center** which reflect the Yarix customer base, embracing a vast range of sectors of the Italian economy. **Data concerning the management of IT incidents** affecting companies which were not previously customers is also included. The enterprises in the panel analysed have an average of more than a thousand employees and generate turnovers in excess of 50 million Euros.
Data was statistically normalised and homogenised to enable its use as a reliable quantitative output and as the basis for qualitative evaluations. **All data collected was automatically anonymised and aggregated to guarantee data protection**, eliminating all links between the information and the businesses concerned.

The report is structured in four sections and an appendix, each analysing and assessing the data collected and processed by the relevant team.
The data is derived from a representative panel of the various sectors of the Italian and European economy, including the following industries:

- Automotive
- Banking & Finance
- Chemical
- Critical Infrastructure
- Energy & Utilities
- Food and beverage
- Gaming
- Mass Distribution
- Healthcare
- Information Technology
- Manufacturing
- Shipping Industry
- Retail
- Transportation

The report provides an objective, informed analysis of the data collected, in order to highlight indicators of trends and anomalies, identify the main trends during the period examined and suggest the relative countermeasures for mitigation of the issues detected.

It also takes a closer look at the cyber attacks which are an important factor on the current Italian and international IT security scene.

The Teams

SOC - Security Operation Center

The **Security Operation Center** is the team dedicated to the management of IT security. Its main task is **to constantly monitor and analyse IT networks to ensure the rapid identification of and response to security threats and other events which may put the security of the customer business's data and resources at risk**.

The Yarix Cognitive Security Operations Center (YCSOC) is one of Italy's most advanced: a cyber control room equipped with cutting-edge physical and biometric security measures, based on predictive and cognitive computational forms. **Active 24x7x365**, it enables businesses to protect strategic corporate assets by responding effectively to fast-evolving IT risks.

In 2023, **the Yarix SOC's efficacy was further upgraded by the implementation of Egyda, the platform developed in-house that uses Artificial Intelligence and Machine Learning** to support analysts during the collection and categorisation of information, for a faster, more efficient response to threats.

YIR - Incident Response

Yarix **Incident Response** (YIR) Team handles all aspects of **IT violations, from investigation to crisis management**, providing an effective response to security incidents. Our experts manage **containment actions**, analysing and using the information available to assess the scale and severity of threats in order to implement the measures required to intercept and neutralise them. **The YIR Team sweeps into action from the moment of engagement, supporting the security staff manning the infrastructure under attack** and providing consultancy throughout the entire response phase: detection, containment, eradication and crisis management.

YCTI - Cyber Threat Intelligence

The Yarix **Cyber Threat Intelligence** (YCTI) Team consists of specialised analysts who draw on their specific skills and experience in the cyber security sector **to interpret the information available on the web** (Clear, Dark and Deep Web) **to prevent and fight threats such as cyber crime, hacktivism and planned operations for data theft or the blocking of company activities**.
These experts are able to move around the dark web with covert profiles, infiltrating black markets and forums where malware, exploits and other attack tools are distributed, to interact directly with the Threat Actors.

YRT - Red Team

The Yarix **Red Team** (YRT) is a group of certified professionals with impressive expertise and years of experience **who are able to genuinely put a company's level of security to the test**. By adopting the methods and mentality used by attackers themselves, with advanced tools and techniques and applying internationally recognised methods, they are able to measure the actual level of risk an organisation is exposed to when faced with a simulated cyber attack, so that weak points can be identified and a **suitable remediation plan** drawn up.

CYRES Consulting

A member of the Digital Security business line of Var Group GmbH, **CYRES Consulting is staffed by an interdisciplinary team of experts**, supported by a network of independent partners and consultants, whose mission is to assist customers in the **strategic integration and operational implementation of cyber security in the automotive industry**, **at both organisational and project level**.
As well as bespoke consultancy, CYRES has an **Academy** which offers a vast range of IT security training programmes and has established itself as the world's biggest learning database in the field of IT security applied to the automotive industry, thanks to its training courses, on-demand videos and certification schemes.

Section 1

SECURITY OPERATION CENTER

Security Operation Center

311 thousand security events

The data analysed in this report relates to about **311 thousand security events** (**+78%** compared to the previous year) detected by the monitoring systems installed by the Yarix Security Operation Center (YSOC), part of the Var Group Digital Security business unit.
The analysts have examined this database and **integrated and combined it with additional Threat Intelligence information** from in-house sources and from partnerships with institutions, organisations and other companies. Last but not least, this document also considers the **information provided by the FIRST** (Forum of Incident Response and Security Teams) **circuit**, the largest, most respected international community for the joint prevention and management of security incidents.

Terminologies

The difference between a security event and a security incident is a subtle one and may sometimes lead to confusion and misunderstandings concerning the data being analysed. For clarity, the following are the definitions used for these two terms, which will apply throughout the report.

// Security event

An IT security event is an identified occurrence in the state of an IT system, service or network which **indicates a possible violation of the set security levels**, or an unknown situation which may be of significance for the security of the company's data and assets.

// Security incident

An event or chain of events consequent on an intentional or accidental action in the context of the monitored IT System which may cause the **loss of confidentiality, integrity or availability of the company's data and the services provided by the IT assets protected**, or the use of assets for the purpose of **committing unlawful actions or harming third parties**, in violation of corporate regulations or the law.

The security events analysed include, for example:

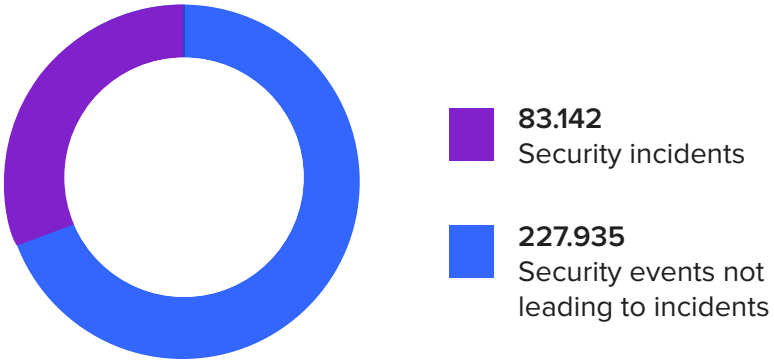
- events caused by malicious code and malware;
- exploitation of known vulnerabilities;
- presence of systems connected to Botnets;
- data exfiltration;
- intrusions;
- compromising of systems and/or applications and/or services;
- DoS/DDoS attacks;
- unauthorised editing or deletion of data;
- sending of phishing emails;
- communication with IP addresses, domains or URLs linked to malicious activity.

A total of 311,077 events were analysed, of which 83,142 evolved into security incidents of varying degrees of severity (fig. 1).

Security Operation Center

Total events analysed

Figure 1

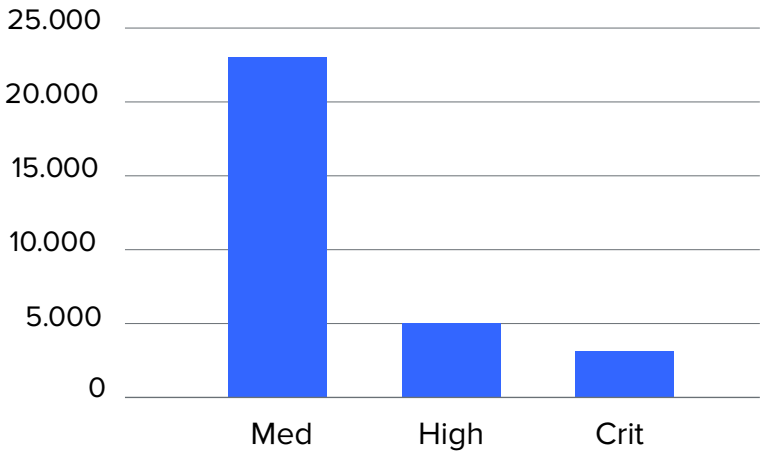


The severity of events and incidents is calculated on the basis of the guidelines set out in operating manuals of the service's individual customers and defined using agreed metrics and procedures in accordance with national and international standards.

Using this classification, the types and severities of the incidents detected for individual customers were aligned in the infographic below (fig. 2)

Events subdivided by severity

Figure 2



Events with "critical" severity (fig. 2) were upgraded to security incidents, and in this case analysis was also followed by **Emergency Response actions undertaken by the YIR (Yarix Incident Response) Team**.

The team supported customers in the management and resolution of incidents and the subsequent post-incident analysis to identify the origin of the compromising or attack, the possible collateral damage and persistent activities put in place by the attacker.

Security Operation Center

Emergency Response activities provide the customer with support during management of the security incident. The aim is to identify and analyse security events, assess their priority and decide the procedures to be adopted once an incident has been confirmed, through to the restoration of normal operation. This process ensures that a detailed forensic analysis can be performed at a later time. **It also guarantees that controls will be improved thanks to the lesson learned**, preventing or limiting the consequences if the same type of incident were to happen again.

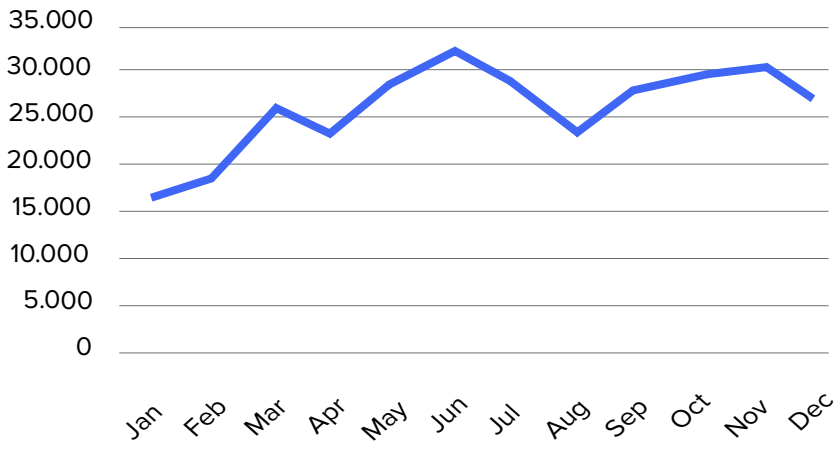
Specifically, a series of actions are carried out in response to notification of an IT incident:

- Assistance is provided to the people and entities involved in the management of security incidents;
- In response to incident notifications, the people and entities involved are alerted and the evolution of the incident is monitored;
- Information about the most common vulnerabilities and the security tools to be adopted is shared;
- Assistance is provided to the people and entities involved in the adoption of the preventive measures considered necessary to reduce the incident risk to acceptable levels;
- Directives are issued on the minimum security requirements for devices with network access, with verification of compliance;
- Technical update courses are organised at all levels, and especially for end users;
- Security tools and methods are kept updated to the state of the art;
- Existing methods and tools are tested and new ones are developed for specific needs.

2023 saw a sharp increase in the total number of events analysed and managed, with the rate of events reported per month almost doubling (+87%) compared to 2022 (fig.3).

Distribution of events in 2023

Figure 3

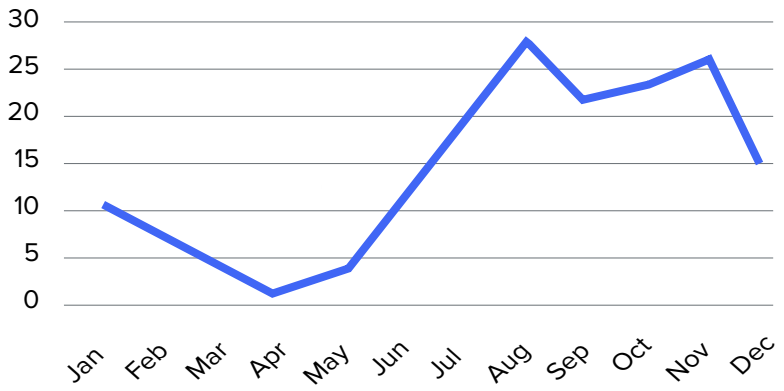


Security Operation Center

There was also a **significant increase (+300%) in the number of events of critical severity**. This was due to the many critical vulnerabilities which emerged in consumer apps and the development of new monitoring scenarios, which enabled more effective threat identification on the part of the SOC team (fig. 4).

Distribution of events of critical severity in 2023

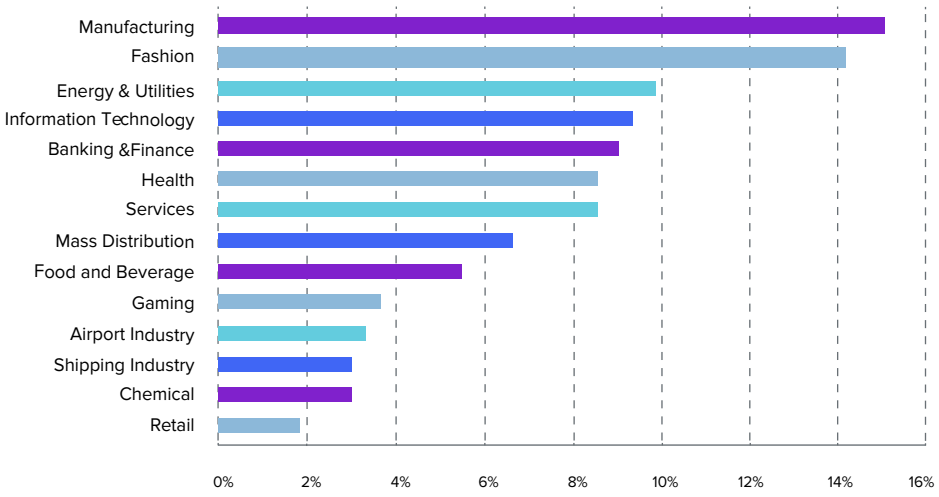
Figure 4



The analysis then focused on the type of industry impacted.
This classification is strongly shaped by the sample considered which, as already mentioned, consists of customers which use the Yarix SOC service. Therefore, statistical tools were used to minimise the impact of any sectors with more or larger companies than others. (fig. 5).

Security events in 2023 subdivided by industry

Figure 5



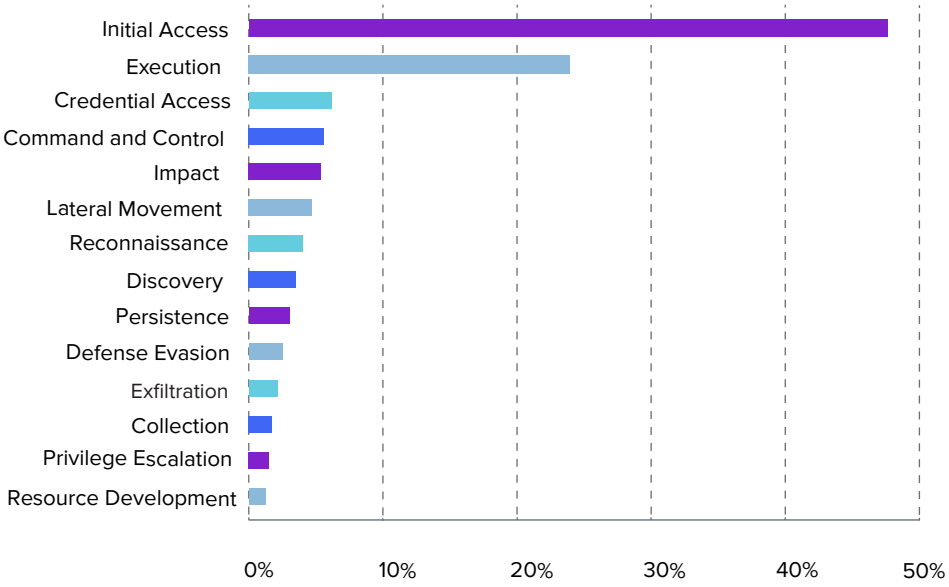
Security Operation Center

It is worth noting that the two industries which recorded the most attacks, with incidence over 10%, were **Manufacturing and Fashion, with 15% and 14%** respectively. This trend is due to a number of factors: while Manufacturing reflects the presence of production facilities containing obsolete equipment which in some cases cannot be updated, for Fashion the key issue is the high exposure of online shops and businesses' global presence, with foreign subsidiaries which often account for a large proportion of security events.

Further to analysis of the security events, they were then categorised on the basis of the tactics identified by MITRE ATT&CK (fig. 6).

Mitre ATT&CK Tactics 2023

Figure 6



As the graph shows, **the largest group relates to the initial phase of the attack** (initial access). This is largely because the data comes from customers with an active SOC service, which identified and blocked the attack before it had time to become critical.

Security Operation Center

Egyda

During the last year we have worked on the **Egyda project, focused on the use of hyper-automation, machine learning (ML) and artificial intelligence (AI) within the Security Operation Center**, which substantially improved our defence mechanisms against IT threats.

This project underlines our commitment to using leading-edge technologies to improve the security and efficiency of our operations.

Hyper-automation was one of the pillars of this project, enabling us to introduce extensive automation of data collection and analysis processes, a procedure previously performed manually by our SOC analysts. This change not only optimises the detection and management of security incidents but also relieves our analysts from repetitive tasks, freeing them to concentrate on the most complex scenarios.

For example, our system now automatically aggregates and correlates data from different sources and applies advanced algorithms to detect patterns and anomalies in real time. This capability is fundamental for effective management of the huge volume of data the SOC processes.

Our machine learning tool, **YUBA**, exemplifies our hands-on approach to cyber security. YUBA is specifically designed to analyse the models by which users log into the various cloud services and identify deviations from their usual behaviour which may indicate a security breach. By continually learning from historic data and in real time, the YUBA engine constantly enhances its ability to forecast and detect unauthorised accesses or potential compromise.

This system operates on an unsupervised learning principle in which it forms clusters of typical login behaviours and flags up as suspect any activity which diverges from these models. Combined with the application of specific intelligence feeds, this innovative tool has not only improved our threat detection rates but also reduced the incidence of false positives, thus boosting operating efficiency.

In Egyda, AI has been focused on supporting our analysts in prioritising and managing the threats detected. We've developed an AI-guided **decision-making framework that assesses the severity and potential impact of each threat**. This system uses supervised models trained on past data, which generate a numerical score indicating the probability that a threat requires attention.

This score helps the analysts to give priority to urgent events and concentrate on the most critical issues, to guarantee a swift, effective response. What's more, AI improves incident response capabilities by suggesting optimal remediation steps and automating routine decision-making processes, thus speeding up the overall security response.

Security Operation Center

Egyda

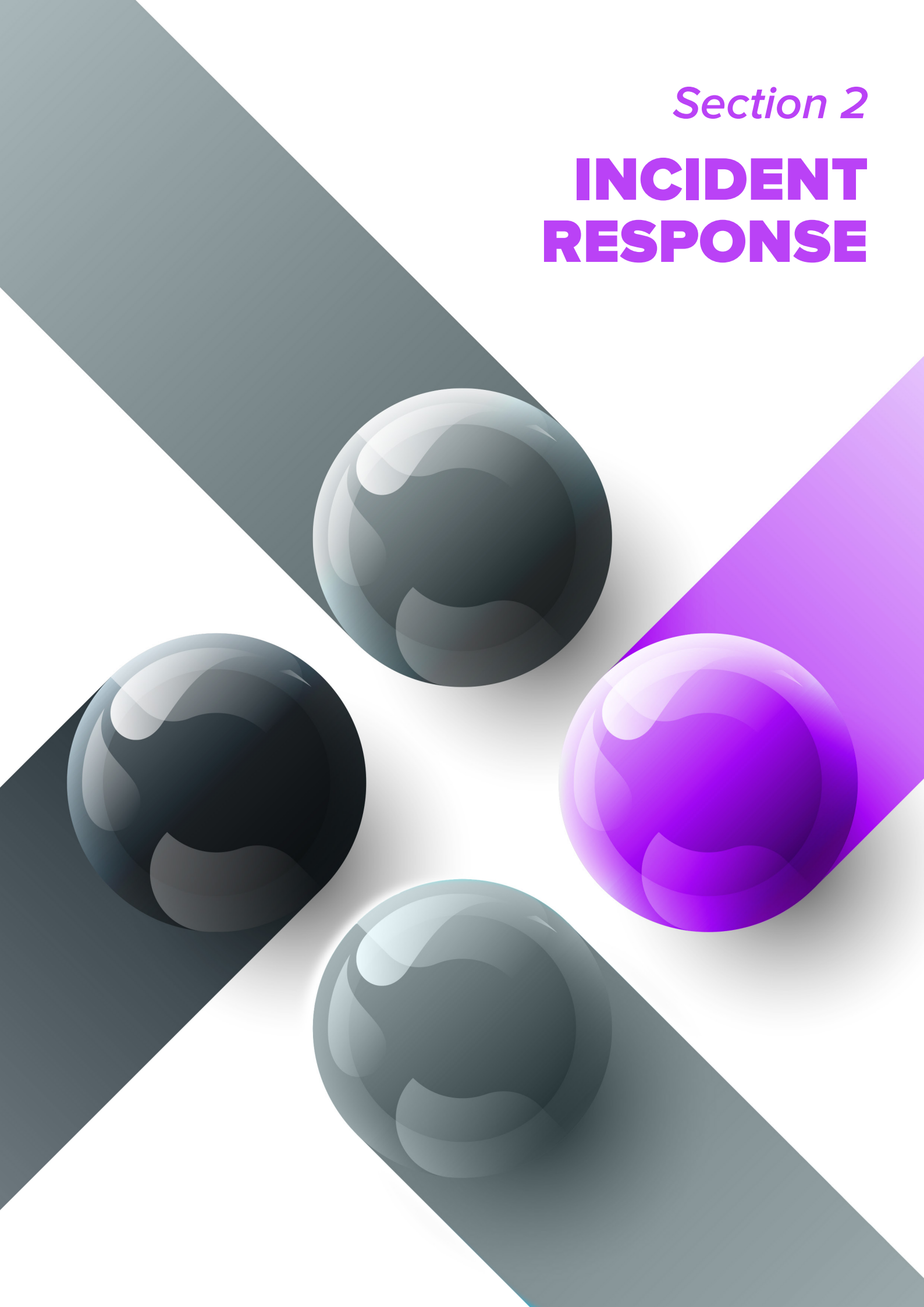
In conclusion, t**he Egyda project has transformed the approach to cyber security in the context of the SOC, integrating hyper-automation, machine learning and AI to create a more robust, efficient, proactive security environment**.

This progress has placed us in the forefront of technological innovation with regard to cyber security, ready to tackle the challenges of a more and more complex array of digital threats.

Our solutions not only detect but also forecast and prevent security breaches before they can impact operations. Future prospects include the adoption of even more sophisticated AI tools such as the introduction, in some phases, of LLMs (Large Language Models), which allow even greater flexibility in the administration of the mass of data managed by the SOC.

Section 2

INCIDENT RESPONSE



Incident Response

83 major incidents

This section analyses the data relating to the **security incidents managed by the Yarix Incident Response** (YIR) ***Team***.

In 2023, the YIR Team responded to and resolved 83 major incidents (**+18%** compared to 2022), many of which, as in previous years, required a very high level of technical capabilities. The resolution of many of these cases involved undocumented technical factors and the development of custom methodologies.

This trend reflects the exponential increase in the Tactics, Techniques, and Procedures (TTPs) skills that Threat Actors (TAs) are introducing as they add persistence, lateral movement and the exploiting of vulnerabilities to their modus operandi.

The Incident Response (YIR) Team manages a security incident in a number of phases, intended to meet the needs of organisations partially or totally compromised by a cyber attack, in which the IT structure's confidential data and its integrity or availability is at risk.

Emergency Response activities

The management of events of this kind requires an organised, structured approach. **This is provided through adoption of an Incident Handling methodology derived from international best-practices** and consolidated with previous experience in the specific field. In particular, Emergency Response activities comprise:

- collection of precise information, using communication techniques which give an understanding of the current status perceived by the company at the time of engagement;
- assessment of the incident's impact on the IT resources, classifying the impacted assets by service importance and business criticality;
- identification, collection and analysis, in order of priority, of the security events and artefacts linked to the attack, to trace how the attack took place and identify the indicators of compromise (IOCs);
- containment of the attack and making-safe of the perimeter, involving analysis and debugging of the systems with eradication of all malicious items identified within the infrastructure;
- support for the restoration of normal business operations;
- implementation of the lessons learned to limit the consequences if the same event is repeated.

For correct management of the incident, analysis of the logs and other artefacts in the systems within the infrastructure attacked is crucial for **reconstructing the malicious activities and identifying the point of entry exploited by the TA**.

This task has become more complex because TAs are increasingly removing the traces of their activities, rendering most of the information necessary for analyses unavailable.

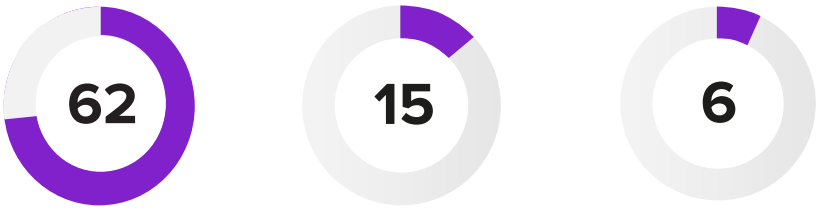
Incident Response

For faster, more efficient containment and eradication, as early as last year the Incident Response Team developed a full set of automations useful for eradicating the most persistent threats and making safe the devices used for lateral movement and privilege escalation.

This year, the most important development has been in attack reconstruction, a highly automated process that can rapidly provide fundamental data to the Incident Response Leaders, who are called upon to take crucial decisions for the compromised business.

YIR 2023 data overview

During 2023 **the YIR Team managed a total of 83 cases**, including:



Incidents with "high" or "critical" severity (IR)

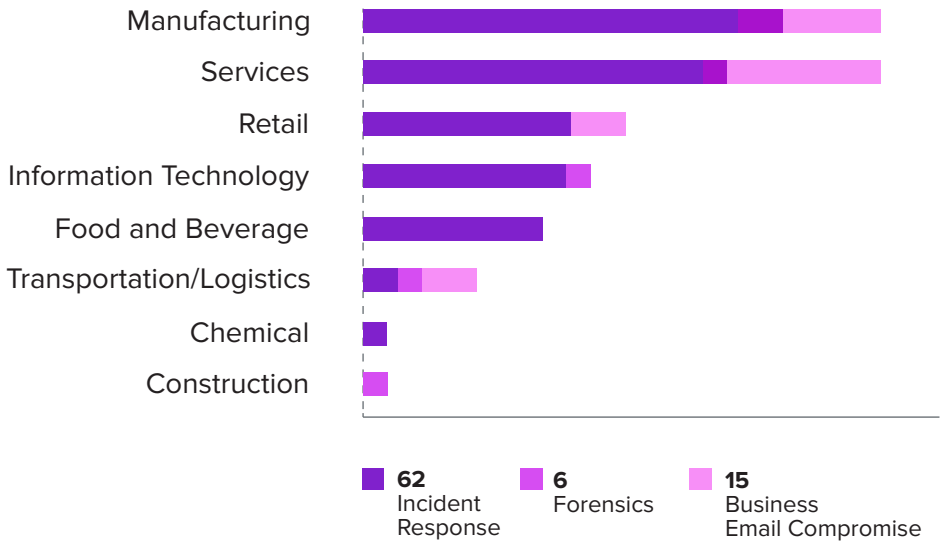
Forensic investigations (FOR)

Business Email Compromise (BEC)

The analysis then focused on the type of industry impacted:

Analysis by type of industry

Figure 7



The hardest-hit sectors were **Manufacturing (24 cases – 28.92%), Services (22 cases - 26.5%) and Retail (11 cases – 13.25%)**.

Incident Response

Attack vectors

On the basis of the findings of the analyses of the incidents, the attack vectors which allowed systems to be compromised subdivide into:

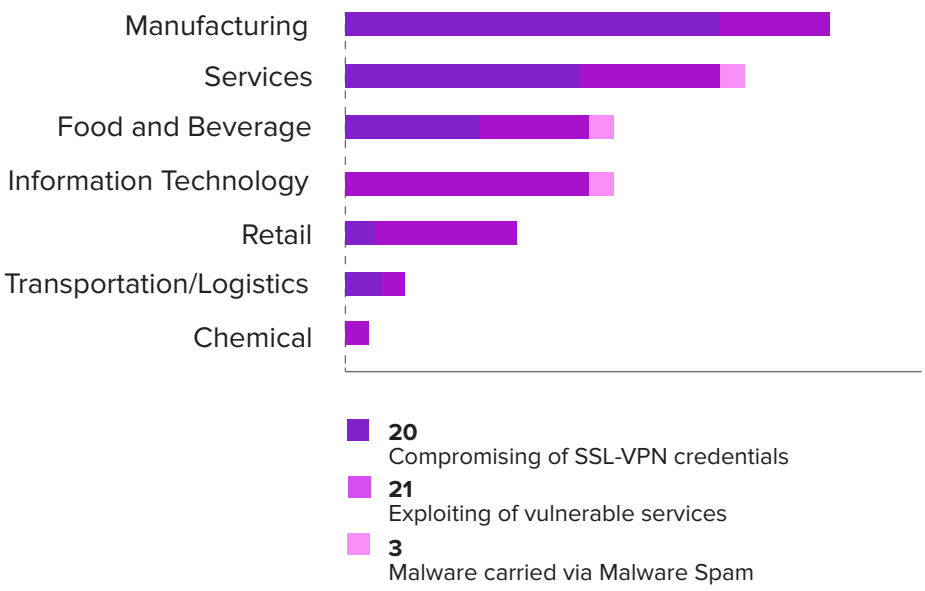
- Compromising of SSL-VPN credentials
- Exploiting of vulnerable services
- Malware carried via Malware Spam (Email Campaigns)

An analsis of the previous points reveals the following:

- The SSL-VPN services most often exploited are those with LDAP single sign-on or, even more frequently, those with local users on the firewall;
- Other vulnerabilities exploited by attackers relate to the publication of services such as administrative interfaces of firewalls, Citrix, RDP, Exchanges and customised services and those based on open-source technologies;
- One of the services most often used to gain remote access to infrastructure is email; specifically, we analysed a number of attacks which used the human factor to gain access.

Attack vectors by type of industry

Figure 8



TTPs and Threat Actors

For the incidents not included in the above table, it was not possible to identify the point of entry with any certainty. Therefore, even if the Incident Response still succeeded in tracing the evolution of the incident, it is not included in the statistics.

Incident Response

Threat Actors 2023

Analysis of the Tactics, Techniques and Procedures (TTPs) enabled us to **profile the various Threat Actors (TAs) which attacked the infrastructures of the affected businesses**.

The analysis of the “tactics”, in particular, enabled us to identify the way in which a TA decides to carry out their attack from start to finish. The technical approach used to obtain intermediate results during the malicious activity is described by the “techniques” adopted by the attacker. Finally, the attack’s organisational approach is defined by the “procedures” used by the Threat Actor.

The image below illustrates the Threat Actors identified during the analyses, classified by number of attacks carried out.

Threat Actor

Akira Hive Ransom House
Noescape **FindOm** Phobos
BlackBasta Prometei Botnet
Alfa team **Lockbit 3.0** **Babuk**
DeepBlueMagic BlueSky
Rhysida **Play** Royal
Vice City

Total Identifications	**27**
Unknown actors	**35**

Incident Response

Evolution of attackers

The analysis shows that, as in the previous year, **LockBit still tops the table of the most active, effective TAs**. In fact, in spite of the latest law enforcement raid on the LockBit infrastructure, nicknamed “Operation Cronos” [1] , the Threat Actor seems to have taken this opportunity to perform an internal reorganisation of its assets and affiliates and to then regroup stronger than ever.

In the attacks observed by the Incident Response Team, **LockBit showed exceptional skills in the techniques used to manage lateral movement and exfiltration, adopting different custom toolsets to enable its affiliates to speed up their compromising activities**.

In contrast with the previous year, there is a fair amount of diversification in the style of the encryption activity undertaken by the most active Threat Actors. Attacks which **encrypt the VMDK files in the physical hosts** occur with more or less the same frequency as those which encrypt the files in the filesystems.

This type of behaviour reveals that the gang is providing its affiliates with functional, effective payloads for use in any compromising scenario.

As in the previous year, the most widely used tools are still the best known, such as Mimikatz, Cobalt Strike, LaZagne, etc., together with custom tools probably developed by individual affiliates to simplify compromising activities.

Unlike in previous years, **the Incident Response Team found that affiliates of the Major Threat Actors, like LockBit, Play, BlackBasta and Akira, used a widely varying skill set**. This indicates less selection within the affiliation process, enabling Threat Actors to significantly increase the number of attacks and thus the number of ransom payments.

[1] https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

Section 3

CYBER THREAT INTELLIGENCE

Cyber Threat Intelligence

Data overview YCTI 2023

Following on from the information reported by the Security Operation Center (YSOC) and Incident Response (YIR) Teams, we will now set out the point of view of the Yarix Cyber Threat Intelligence (YCTI) department and its targeted analyses for year 2023.

In 2023, the YCTI team reported a total of **2,571 significant events**, including:

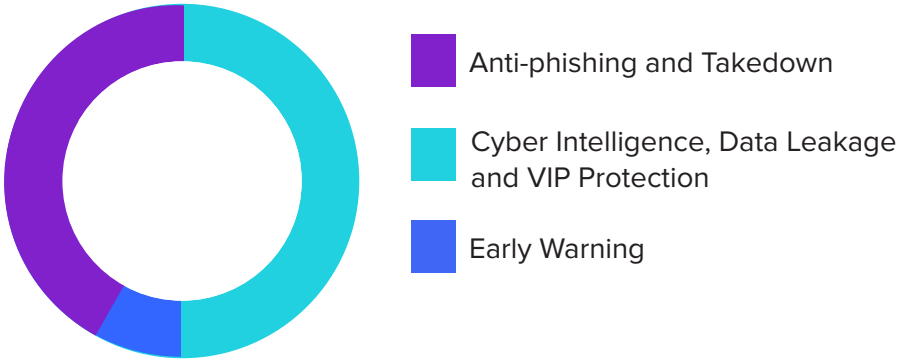
- 1,093 Cyber Intelligence, Data Leakage and VIP Protection events;
- 189 Early Warning events;
- 1,289 Anti-Phishing events and consequent activities to combat these attacks.

The CTI events analysed include, for example:

- Events linked to the sale of credentials or compromised accounts on the Deep Web and Dark Web;
- Events on critical and 0-day vulnerabilities actively exploited by the TAs (Threat Actors);
- Events involving data breaches, data leaks or sale of confidential information and data on the Deep Web and Dark Web;
- Events with major or critical impact emerging after OSINT / HUMINT activities;
- Events involving the identification and take-down of fraudulent domains or websites (fake shops, bank phishing, fraudulent mobile apps, spear-phishing...)

Events managed YCTI 2023

Figure 9



Cyber Threat Intelligence

The team issued a specific notification **report** for every Cyber Threat Intelligence event, **supporting the customer in the incident's management by providing the evidence collected and advising on the appropriate countermeasures and the recommended mitigation and remediation actions**.

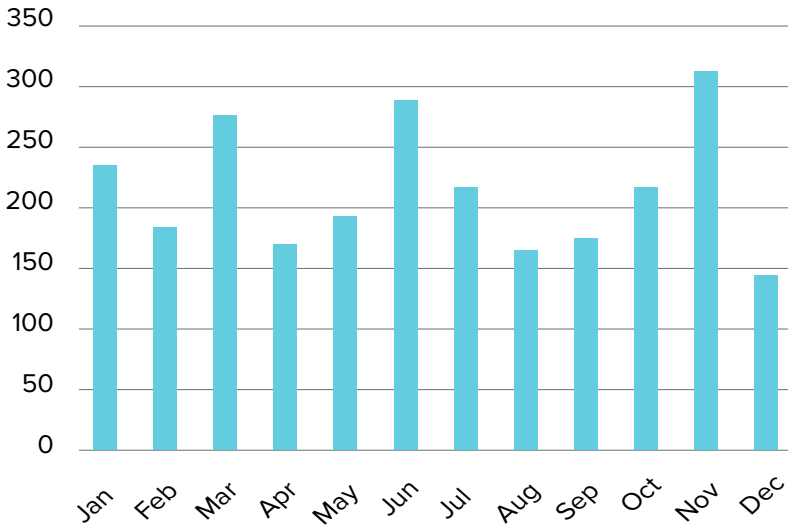
79 events with critical severity

During the period of reference, the YCTI team analysts identified **79 events with critical severity**. This enabled the proactive avoidance of incidents which might have compromised the entire organisation, making it the victim of potential ransomware attacks or the exfiltration of critical information.

The graph illustrates the distribution over time of the significant events (2,571) managed by the YCTI Team.

Time distribution

Figure 10



Ransomware trend

With regard to ransomware incidents at the global level, during 2023 the YCTI Team mapped and analysed a **total of 4,474 events carried out by 65 ransomware groups**. The following is the list of the Top 10 most active ransomware groups:

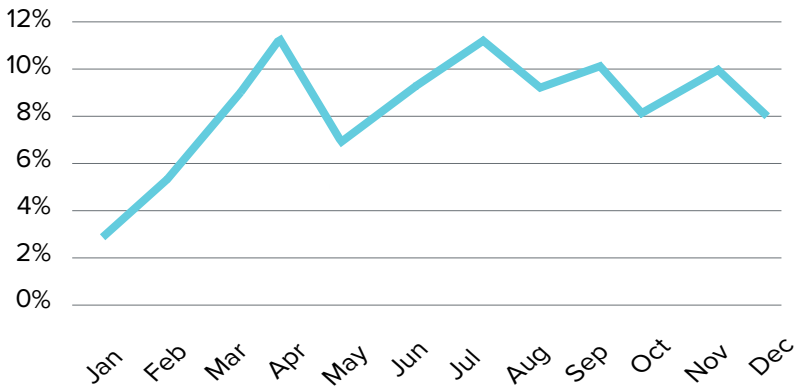
- LockBit (22%)
- AlphV/BlackCat (9%)
- Cl0p (9%)
- Play (7%)
- 8base (5%)
- Malas (4%)
- Akira (4%)
- Bian Lian (3%)
- Medusa (3%)
- BlackBasta (3%)

Cyber Threat Intelligence

LockBit was again the most active ransomware group during 2023, accounting on its own for 22% of total attacks, followed by ALPHV/ BlackCat and Cl0p (9%), Play (7%), 8base (5%), Malas and Akira (4%), and BianLian, Medusa and BlackBasta (3%). **These 10 ransomware gangs were responsible for 68% of the total attacks recorded by the YCTI Team**.
8base, Akira, Malas and Medusa, four ransomware groups which appeared during the last year, were also in the Top 10 list. Together, these four criminal gangs were responsible for 16% of the total attacks monitored during 2023.

Monthly Ransomware trend in 2023

Figure 11



The monthly trend of events reveals a growth in the number of ransomware threats during the first four months of 2023, after which the level stabilised with peaks in the months of April, July, September and November.

The statistics relating to the countries targeted by the ransomware gangs are just as significant. Italy is at fifth place in the list of most targeted countries.

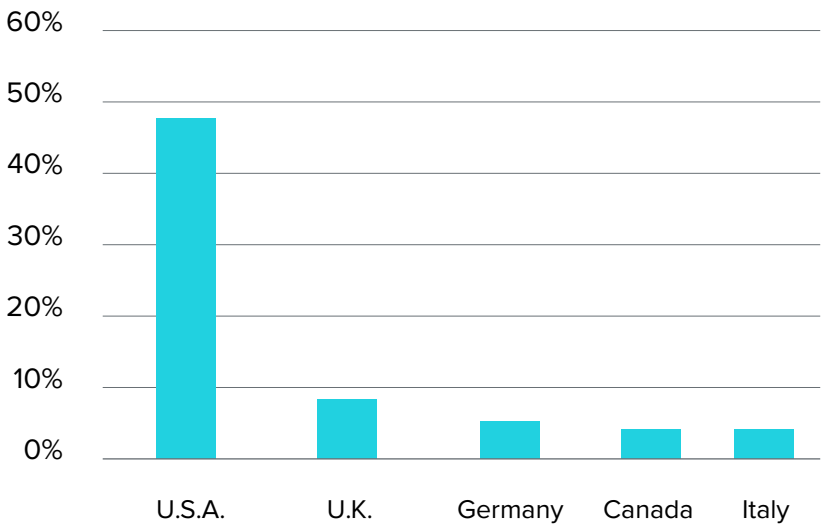
The following are the **Top 5 countries** globally the organisations of which suffered the most ransomware attacks in 2023.

- United States
- United Kingdom
- Germany
- Canada
- Italy

Cyber Threat Intelligence

Top 5 Countries for Ransomware events 2023

Figure 12



Organisations based in the United States were the hardest hit in 2023, having suffered 48% of total attacks. They are followed by organisations from the United Kingdom (7%), Germany (5%), Canada (4%) and Italy (4%).

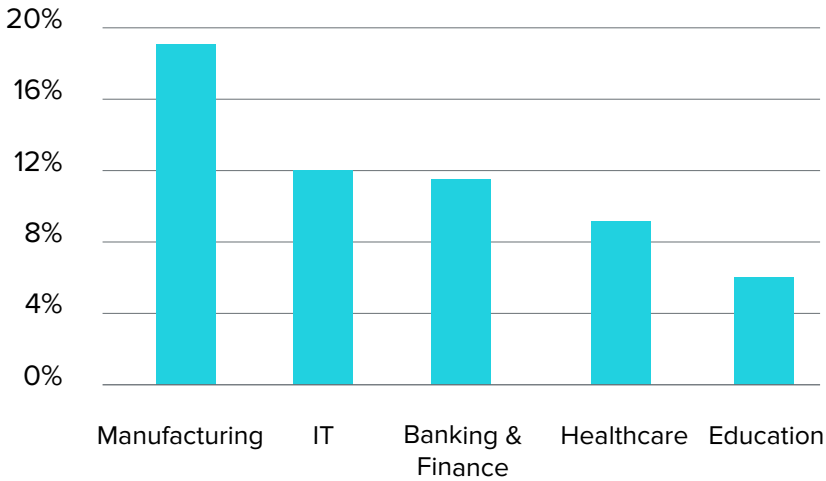
The total attacks suffered by the Top 5 countries amount to 68% of the total events recorded in 2023. It should be noted that the 2023 ranking of Top 5 countries is similar to that already reported last year.

The following is the Top 5 of sectors hardest hit by ransomware attacks during 2023:

- Manufacturing
- IT
- Banking & Finance
- Healthcare
- Education

Top 5 sectors for Ransomware events 2023

Figure 13



Cyber Threat Intelligence

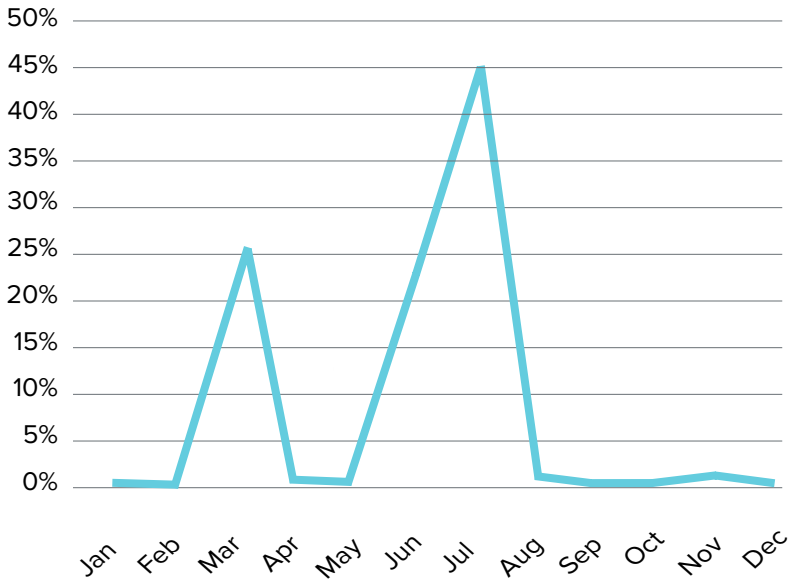
Manufacturing is at the top of the list, with 19% of total attacks in 2023. It is followed by IT (12%), Banking & Finance (11%), Healthcare (9%) and Education (6%). All together, the attacks against the Top 5 sectors account for 57% of the total events recorded in 2023.

Focus Cl0p

As was also the case last year, during 2023 some ransomware groups could be seen **to exploit specific vulnerabilities**. In particular, the YCTI Team observed a peak in **attacks carried out by the Cl0p gang** further to the discovery and active exploitation of two vulnerabilities in specific file transfer apps. According to the data analysed by the YCTI Team, the discovery and exploitation of these vulnerabilities coincided with peaks in attacks by the ransomware gang, seen in particular in March 2023 (26% of total attacks) and during the months of June and July 2023 (24% and 44% of recorded attacks respectively).

Vulnerability overview

Figure 14



The following is an overview of these vulnerabilities.

GoAnywhere

GoAnywhere: In February 2023, **Fortra reported a vulnerability called CVE-2023-0669** in the GoAnywhere Managed File Transfer (MFT) app, **which allowed attackers to run code from remote on instances with exposed administrative consoles**. The patch was then issued on 7 February, the month in which Cl0p confirmed that it exploited the vulnerability and succeeded in exfiltrating data from more than 100 organisations.

Cyber Threat Intelligence

MOVEit

MOVEit: At the end of May 2023 Progress Software reported vulnerability CVE-2023-34362 in the MOVEit Transfer and MOVEit Cloud products. **This SQL injection (SQLi) vulnerability affected exposed MOVEit** web applications on the Internet, enabling attackers to access the databases hosted on the applications concerned. Microsoft observed the exploitation of the vulnerability and attributed it to ransomware group Cl0p, which then laid claim to the use of this exploit on its Data Leak Site (DLS).

It is not clear whether Threat Actor Cl0p only used the vulnerabilities to subtract data and then extort money from the victim organisations to prevent release of the files, or whether it also encrypted the affected systems. However, there is no doubting the high impact of the exploitation of these vulnerabilities, given the widespread use of the transfer applications affected by both private and government organisations globally.

Compromised credentials

In 2023 the YCTI observed a growth in interest and the **market relating to credentials compromised by Infostealer malware** within underground environments. This type of malware, mainly distributed through phishing campaigns and pirated software, is designed to collect sensitive information (including credentials saved on the browser, credit cards, cookies and wallets) from the infected system and send it to the cybercriminal. Especially if they are linked to critical services and are still valid, **the exfiltrated credentials can be used to obtain initial access to a corporate system**. This modus operandi is commonly used by the ransomware gangs.

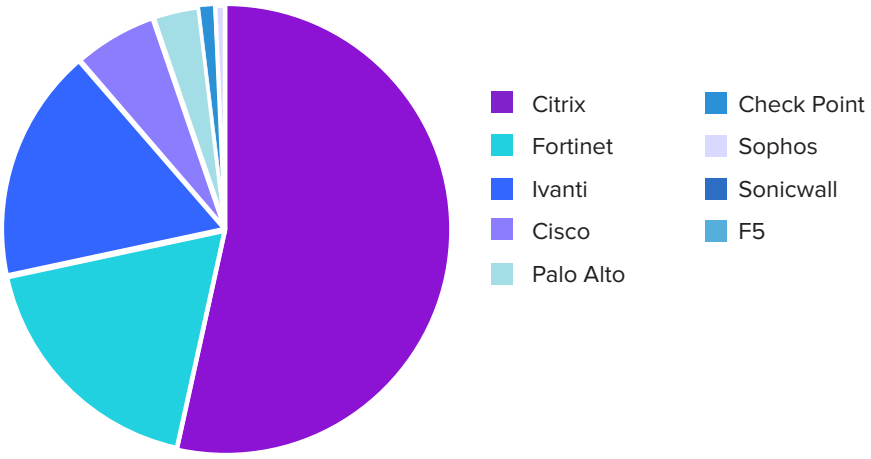
During 2023 the YCTI Team identified more than 193 million **credentials compromised by Infostealers (+180% compared to 2022) exfiltrated from more than 2.8 million different compromised systems**. Apart from the larger market and increased interest already mentioned, this growth is also due to the distribution during 2023 of new Infostealer malware and the addition of new sources obtained from the YCTI Team's ongoing undercover research.

Cyber Threat Intelligence

Critical compromised credentials by vendor

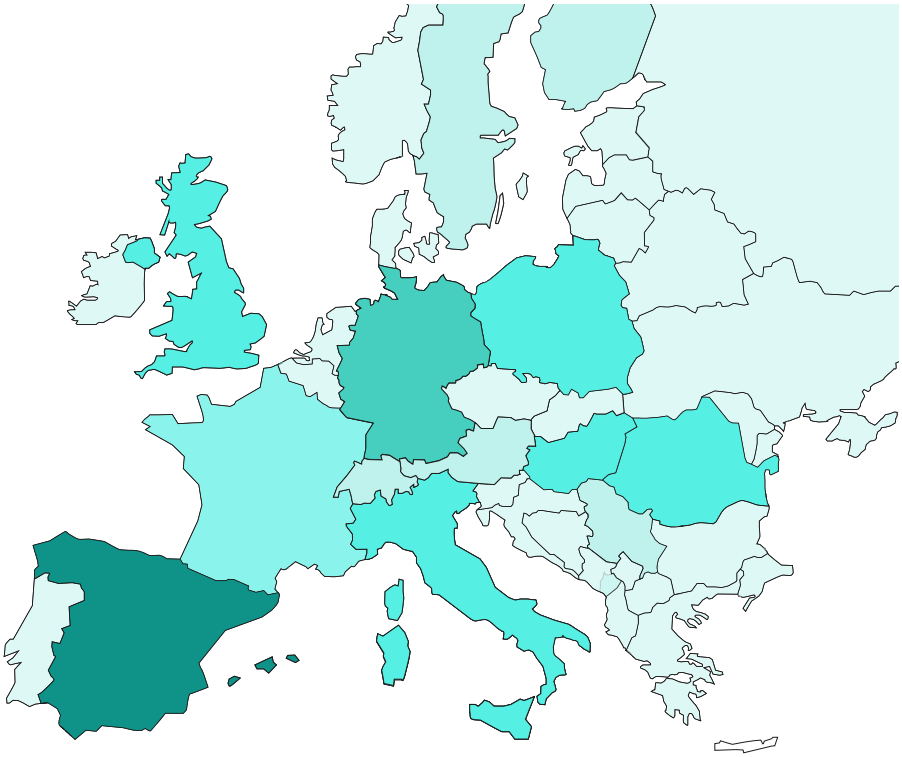
More than 60 thousand credentials identified are linked to critical corporate portals, such as VPNs and Firewalls, relating to a variety of vendors:

Figure 15



In terms of the number of compromised systems identified, Italy is in 20th place at the global level with a total of more than 38 thousand infected devices (+123% compared to 2022) and third within Europe, preceded by Spain (60 thousand) and Germany (47 thousand) and followed by France (36 thousand), Poland (32 thousand) and the United Kingdom (29 thousand).

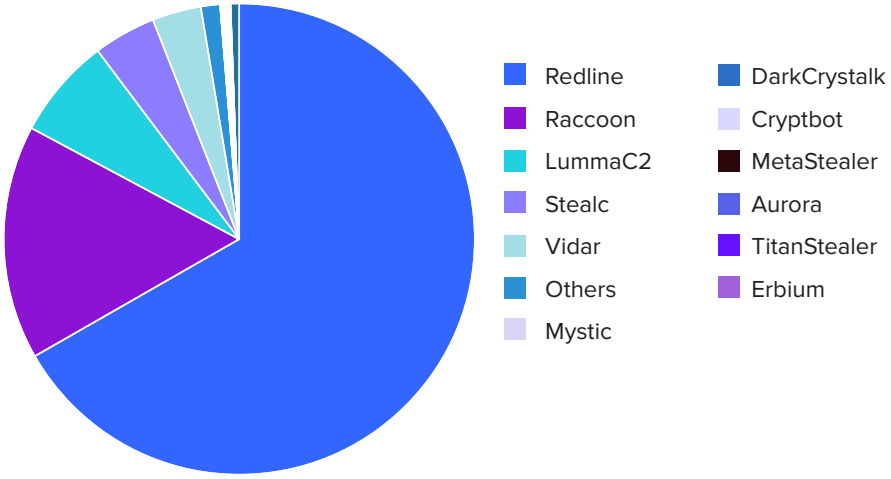
Infostealer infections in Europe



2023 was also characterised by the presence of a vast variety of Infostealer malware. The most common within Italy was Redline with more than 25 thousand infections (67%), followed by Raccoon (16%) and LummaC2 (7%). The following are the different types of Infostealer malware identified in Italy:

Infostealer malware infections in Italy

Figure 16



The growth in the market for compromised credentials was also observed on the black markets monitored by the YCTI Team, **where credentials exfiltrated from more than 82 thousand Italian hosts (+11.5% compared to 2022) were identified on sale**.

Fraudolent shops and #fashionmirror operation

A inizio 2023 il team **YCTI ha condotto un'investigazione che ha portato alla luce un'infrastruttura e una rete di oltre 13 mila shop fraudolenti**.

L'operazione denominata **#fashionmirrror che ha coinvolto oltre 48 brand del fashion con grandi marchi del Made in Italy e internazionali** è stata prontamente segnalata alla Polizia Postale e delle comunicazioni e sono state condotte le operazioni di contrasto e smantellamento dei domini fraudolenti identificati.

Dalle indagini condotte è emerso che il 90% dell'infrastruttura appariva collocata negli USA, Panama e Turchia; analisi più approfondite sulla posizione reale dei server hanno permesso di rilevare delle tracce dell'infrastruttura criminale anche in Europa.

L'investigazione **#fashionmirror è stata inoltre citata nel corso del 2024 da parte della testata giornalistica Le Monde**[2], che ha condotto un indagine che ha portato alla luce ulteriori shop fraduolenti, di cui una buona parte già individuati e investigati dal team YCTI durante l'operazione svolta nel 2023.

Il team YCTI, tramite la propria divisione di brand abuse **ha l'obiettivo di monitorare e contrastare attivamente siti fraudolenti, studiando e mappando costantemente i Threat Actor** che sono dietro a queste operazioni e a queste infrastrutture criminali.

Nel corso del 2023, oltre all'operazione citata #fashionmirror, **il team ha tracciato e identificato oltre 5 cluster differenti di Threat Actors**, la maggior parte di origine cinese che hanno lo scopo di mantenere attive infrastrutture legate ad e-commerce fraudolenti.

[2] https://lnkd.in/eJ4Z8TjA

Section 4

RED TEAM

Red Team

Comment on 2023 YRT trends

From the offensive security point of view, 2023 could be described as a year of transition: as the compulsory implementation of **TIBER-IT** [3] **and DORA**[4] **frameworks** approaches, they are starting to become more and more common. Therefore, a large number of Italian companies are making proactive preparations, establishing more structured, comprehensive security assessment projects.

The number of single projects managed by the Yarix Red Team (YRT) was slightly lower than in the previous year, 230 compared to 275 for 2022, and accounted for more or less the same number of days. This reflects a rise in the number of bulkier tasks and an increase in commitment and budget on the part of the companies involved in this type of analysis, which was by no means inevitable.

There was a particularly sharp rise in requests for **Social Engineering** assessments, especially through Spear Phishing campaigns (+50%). Obviously, companies are increasingly recognising the importance of working on their human resources and of stimulating employees' awareness and reactivity by means of realistic simulations.

Therefore, over time the YRT has built up a more and more sophisticated service, **in which the customer experiences a custom attack by a Threat Actor determined to specifically target the business and its staff**. The Red Team delivers a realistic experience by fielding creativity and improvisation, instead of relying on ready-made scenarios.

On the basis of the Spear Phishing campaigns conducted during 2023, the YRT is able to define the profile of the average Italian business and its awareness:

[3] https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.htmlhttps://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

[4] https://www.eba.europa.eu/activities/direct-supervision-and-oversight/digital-operational-resilience-act

Red Team

500 Employees with email account

41,4% Employees open the phishing email

21,9% Employees interact with the link or button it contains

13,4% Employees enter one or more valid credentials in the trap form

Weak Strong Credentials average robustness

12,7% Employees report the email as phishing

As already reported during 2022, there is a continuing demand for advanced Red Teaming projects, with a careful eye on the preliminary phases of Threat Intelligence, in accordance with the dictates of DORA (with the Threat-Led Penetration Test) and TIBER (which stands for Threat Intelligence-Based Ethical Red teaming). Although the speed of change is gradual, the need to thoroughly assess defensive capabilities and the ability to react to an adverse event is emerging in a number of industries. In general, overall knowledge and the culture are evolving, making investments and strategic choices in terms of IT security focused less on technology and more on services and the smooth management of events overall.

Red Team

In line with this trend, 2023 saw the large-scale take-up of Purple Team Exercise projects. This training approach consists of beneficial open collaboration between attack and defence to achieve the meticulous tuning of monitoring and response systems and configuration, with a view to providing efficient, effective cover.

Mention should be made here of a new flare-up in on-premises scenarios: during the last few years there was an explosion in attacks that could be conducted from anywhere in the world, but in 2023 we saw a growth in attacks conducted physically at headquarters, plants or depots with the aim of stealing company data or devices or both. **New physical hacking techniques and the spread of easy-to-use** tools like Flipper Zero brought scenarios of this kind back under the spotlight, and a further surge is very likely if they are included in the DORA compulsory tests. The major difference from past approaches is the demand for a stronger focus on threat scenarios (threat-based approach) rather than a mere list of issues in themselves, such as shortcomings in Wi-Fi networks which would not be exploitable in a realistic context.

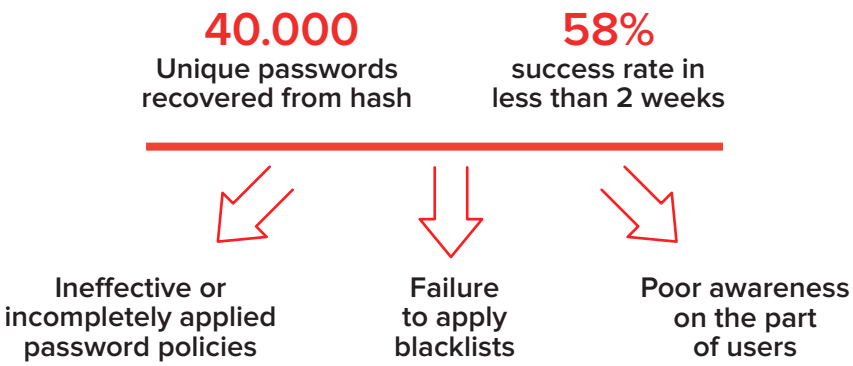
Active Directory

Mention must also be made here of the subject of Active Directory (**AD**) security. The amount of attention paid to this area has soared in the last few years thanks to research and vulnerabilities which have received public attention (especially the work done by SpecterOps), leading to the creation of a corresponding series of offensive security tools (first and foremost BloodHound). However, unfortunately the security level of implementations within companies has lagged behind these developments. Curiosity is therefore growing about this issue and the need to obtain AD security assessments that extend beyond mere checklists of issues and reveal actual risks, especially in real attack contexts (e.g. theft of credentials of a user of a given type).

As a further step, often linked to poor Active Directory security practices, assessment of the robustness of credentials is recommended. More and more organisations are requesting practical analysis of the level of maturity of their password policies, extending beyond just interviews or analysis of the policies themselves and focusing on credentials, by simulating the behaviour of a Threat Actor attempting to obtain passwords and then crack them for its own purposes. Naturally, accessing a company's domain credentials is a very delicate operation, which must be carried out in accordance with clearly defined confidentiality constraints. **Therefore, during 2023 YRT constructed its own physical off-line cracking infrastructure, which enabled it to reconstruct an impressive number of credentials in a controlled environment**. This activity focuses on the added value of the creativity deployed by the Threat Actor, which is often able to identify and reconstruct bad habits on the part of businesses and then organise precisely targeted, very effective Dictionary Attacks.

Red Team

Thanks to the cracking activities conducted during 2023, the YRT achieved the following results:



Finally, to conclude, a comment on the 2023 trends, which reveal the desire to extend cyber security concepts to innovative technologies and services such as LLMs (Large Language Models), Deepfakes, Automotive and Web3 Security, in which the YRT is investing in training, research and development, as well as in relation to Threat Actors.

Focus on CVE and publications

During 2023 the YRT published the following articles on **YLABS[5], the Yarix online blog with in-depth coverage of cyber security topics:**

- **SIRI WI400: XSS on Login Page – CVE-2022-48111**: the first CVE registered in the name of YRT during the year, thanks to the fruitful partnership with Siri Informatica
- **PrivEsc on a production-mode POS**: technical description of a chain of known vulnerabilities adapted and exploited in the context of analysis of a production-mode POS
- **Vade Secure Gateway Multiple XSS (CVE-2023-29712, CVE-2023-29713, CVE-2023-29714)**; 3 additional CVEs linked to the French software a year after their identification during an assessment
- **GIS3W**: Persistent XSS in G3WSuite 3.5 – CVE-2023-29998; fifth and last CVE registered by YRT during the year, from the partnership with GIS3W
- **Pizza, Pasta and Red Teaming**: insights and ideas for an Italian-style report: discussion of a possible approach to structuring complex Red Teaming reporting.

[5] https://labs.yarix.com/

Two considerations must be made here. On the one hand, any unknown vulnerabilities detected by the YRT emerge during real, authorised engagements, during which issues which cannot yet be officially resolved are often encountered, increasing the added value of the test itself. On the other, while an ever-greater willingness to follow a Coordinated & Responsible Disclosure process is emerging in Italy, there is still a long way to go: in many cases the ostrich algorithm is still applied, or the bureaucratic processes rapidly stitched together are so complex and intricate that they discourage the necessary search for vulnerabilities.
In the long term, this could turn out to be a boomerang of zero-days pushed under the carpet and subsequently exploited in real attack contexts. This may apply to Italy in particular, but in some cases the same can also be said of even important international players.

The added value of a Red Team today

Before moving on to the final section on the YRT Top 10 2023, we would like to mention another point worth thinking about. Commercial "Automated Penetration Test" tools and the advance of innovative AI implementations are generating concerns and fears within the community: Is the role of the analyst going to become superfluous?

For people who view the design of operations like Vulnerability Assessments, Penetration Tests or Red Teaming activities as mere mechanical security tasks based on checklists and "copy and paste" documents created with innovative scanners, there may be some cause for concern. Today it is more important than ever to focus on the skills, experience and added value that Offensive Security can provide by virtue of being Proactive Security. If it all boils down to the outsourcing management of a commercial product, what is to stop a business from saving money by using the same tools, "which do everything on their own" for themselves?

This is the fundamental point. We have to break down the barriers of the past and bring the Red Team and the Blue Team as close together as possible, with a view to improvement in every area (and beyond). We must focus on the continual improvement of reporting and the strategic information it can provide. This means that instead of "paper sitting in a drawer" it becomes the source not only of a prioritised working plan but also, in some cases, of inputs for strategic thinking that can extend beyond the perimeter of action, and major investments to protect the business and everything it generates. "Attack is the best form of defence" may be a cliché, but it is true, nonetheless. If to this we add the possibility of "interviewing" the attacker for detailed knowledge of the operations conducted, bearing in mind how unfeasible this is in a real threat context, probably the added value becomes clearer.

So automated Penetration Test tools and innovations in the field of AI become not the enemy to be defeated but rather an incredible weapon to be exploited. If you have the skills to do so, of course.

Red Team

YRT TOP 10 2023

For 2023 we have again drawn up the **TOP 10 of bad practices** identified and exploited during the YRT's Red Teaming activities.

First, here is a comparison between the 2022 and 2023 rankings

TOP 10 2022	TOP 10 2023
1 Critical systems with support no longer available	**1** Active Directory security and poor account management
2 Haphazard application of Two-Factor Authentication	**2** Partial or inefficient coverage by protection systems
3 Lack of awareness on the part of users	**3** Bad Practice in application development by suppliers - NEW
4 Nonconforming management of confidential information	**4** Nonconforming management of confidential information
5 Active Directory security and poor account management	**5** Badly configured VPNs - REVIEW
6 Partial coverage by protection systems	**6** Inefficiencies in detection processes - REVIEW
7 Inefficiencies in defensive processes	**7** Incomplete or inaccurate reconstructions of security events - REVIEW
8 Ineffective password policies	**8** Ineffective password policies
9 Vulnerabilities in exposed critical systems	**9** Poor control of public attack surface area - REVIEW
10 Badly applied logic segregation	**10** Incomplete application of Two-Factor Authentication

As an experimental exercise, the order of this year's ranking is also an attempt to represent its hazard level, rather like the famous OWASP TOP 10s.

2023 has 5 total or partial new entries:

- Bad Practice in application development by suppliers - REVIEW
- Badly configured VPNs - REVIEW
- Inefficiencies in detection processes - REVIEW
- Incomplete or inaccurate reconstructions of security events - REVIEW
- Poor control of public attack surface area - REVIEW

A rapid description or a note explaining the changes in relation to the new trends observed is provided for each of these below.

Red Team - 2023 | YRT TOP 10

01 - Active Directory security and poor account management

After accessing an internal network, usually we encounter a series of issues that businesses have been ignoring for decades and which tend to be too expensive to put right. Active Directory security is the most fertile terrain of all, since it is very critical with regard to the availability of services and yet at the same time badly managed and never subjected to targeted monitoring or hardening. There are therefore countless paths that can easily allow privileges to be raised to domain administrator or local administrator level in most of the accessible infrastructure managed.

2023 Update: although they are not particularly new, Active Directory attack techniques often find the defensive infrastructures and monitoring systems unprepared.

02 - Partial coverage by protection systems

Many businesses have made major investments in continuous monitoring or the adoption of advanced defence systems. However, here again there are problematical areas, such as systems which are not monitored because they are too “fragile” or too critical for external interference to be permitted, not to mention possible human error during deployment, or misalignment between the actual and monitoring perimeters. Exceptions in coverage, especially once everything is thought to be under control, lead to a false sense of security and are low-hanging fruit anyone wishing to act undetected.

2023 update: during 2023, attack simulations focused on a class of businesses that have invested in monitoring services and solutions but have also opted for a way of meeting a need which may be the most economical (e.g. open source) but is often incomplete and unreliable.

03 - Bad Practice in application development by suppliers - NEW

The issue of the secure management of third parties is a current hot topic, with new, important regulatory constraints also in the offing. In fact, there are a number of known attacks in which this type of factor is really crucial: once the security of the business’s perimeter has been addressed, it is fundamental that no supplier should lower the standard level of quality and thus provide a possible entry-point or a way of bypassing the security measures in place.

This category is intended to highlight in particular the crucial importance of having application solutions developed by suppliers who comply strictly with an S-SDLC (Secure Software Development Lifecycle) and are able to demonstrate this. In other words, it is unacceptable for businesses to use suppliers that have never performed a code analysis or organised an application Penetration Test. Alarming bad practices often emerge in this area, reflecting the fact that for some suppliers the issue of IT security is a topic they never consider.

04 - Nonconforming management of confidential information

The poor management of confidential information still continues, all too often, to be a huge source of data for Threat Actors. This point covers first and foremost poor management of email accounts, often used as storage for critical documents and passwords, or even configuration files, backups, manuals, unprotected scripts and ridiculously revealing names (Password.*).

2023 Update: another specific factor which emerged in this area during the last year was the nonconforming use of company network shares, which are often poorly protected and become a source of access to mouthwatering data for a Threat Actor.

05 - Badly configured VPNs - REVIEW

This category, a 2023 new entry, is a further verticalisation of the previous “Badly applied logic segregation”
In the case of VPN accesses in particular, there is still insufficient awareness of the need to assign the networks and the services accessible to the individual user or host in an extremely targeted manner. Quite the contrary: often remote users all have the same visibility within the internal network, which includes servers containing confidential data or business-critical information such as backups.

2023 Update: the detail we wish to highlight in this review is the lack of hardening and of tests for specific mechanisms. Businesses have realised that they must restrict the privileges supplied via VPN accesses, but all too often they have overlooked the importance of testing the possibility of agile bypassing of specific constraints. For example, if the business requires its employees to use “Client X”, to which it has applied a set of well-made restrictions, it must also make sure that it is not also possible to access the system via “Client Y”, in which all these restrictions might not be applied, meaning that they are totally bypassed.

06 - Inefficiencies in detection processes - REVIEW

This category, a 2023 new entry, is an initial verticalisation of the previous “Inefficiencies in defensive processes”.
Whether it is the response to critical alerts or the poor correlation of individual events, it is the quality of the service, and not of the tool, that often makes the difference in critical situations. As has been shown, in these cases attackers use advanced evasive techniques, once again exploiting gaps or inefficiencies in event management processes.

2023 Update: in this category, the focus is on the lack of tuning of the security solutions implemented. Very often, businesses believe that once they have bought a licence for an IDS/IPS, an SIEM or an XDR they become immune to attack and able to block any threat. In fact, as with any defensive technology, these systems have to be adapted to their context of use, to the most plausible threat scenarios and to the latest modes of attack. Purple Team Exercises therefore have to be planned at regular intervals (e.g. annually) to raise defensive capability above the level of a default infrastructure which may not be suitable for all situations, especially if the Threat Actor the business is most likely to be competing with is not a script kiddie but someone with superior skills, able to bypass default detection capabilities.

07 - Incomplete or inaccurate reconstructions of security events - REVIEW

This category, a 2023 new entry, is a further verticalisation of the previous “Inefficiencies in defensive processes”.

2023 Update: the attacks conducted during the year highlighted the need to approach this category in more detail, with specific coverage of detection processes. The aim is to emphasise the discrepancy between what has been detected and the actual attack parameter concerned. For example, if the Blue Team’s reconstruction of a Password Spraying attack in an Office365 environment identifies the attack correctly, flagging up 10 affected accounts on which it forces a password change, this may give a false sense of security, with the impression that the event has been blocked and the issue has been swiftly cleared up. In fact, if the real attack were to have involved even just one more compromised user not picked up by the reconstruction, this would still be a win for the Threat Actor. This underlines the need for Red Teaming activities or Purple Team Exercises for in-depth testing of defensive capabilities and the ability to reconstruct the malicious event.

08 - Ineffective password policies

Concerning bad practice in the management of company passwords emerges with regard to the internal domain in particular, but inevitably involving all the exposed services. The tendency is only to do the absolute minimum to comply with default password policy requirements, which are often too unspecific and totally unfit for purpose. This implies extreme vulnerability to fairly rudimentary Dictionary Attacks that have identified the name of the company or the geographical location of the targeted plant. In particular, the use of shared patterns, which can bring the whole house tumbling down once reconstructed, is often crucial.

2023 Update: as explained in the previous points, this tendency is still very much with us and is deeply rooted at the level of poor IT management internally, in relation to external suppliers and with regard to end users.

09 - Poor control of public attack surface area - REVIEW

This category, a 2023 new entry, is a further verticalisation of the previous “Vulnerabilities in exposed critical systems”.
End-to-End Red Teaming often reveals standard vulnerabilities on poorly controlled perimeters which are, however, used by and known to employees in general. So, for example, even unsophisticated Cross-Site Scripting on the employee portal can persuade victims to enter their credentials or download a file containing malware. The more critical the system, in terms of confidentiality of the data managed or direct communication with the internal network, the stricter, more continuous and more timely the updating process must be.

2023 Update: in relation to the findings during the year, the key point is the need to reach beyond the technical concept of vulnerability. In more and more cases, the exposure of vulnerable services arises not from a lack of awareness of the importance of minimising the possibilities of access from the public network but rather from the absence of continuous, effective monitoring of the exposed areas. In many instances, specific areas of the company and, even more frequently, “thoughtless” suppliers, publish unapproved services on their own initiative, perhaps simply to run temporary tests, unbeknown to the company. In the worst cases, these entry-points are excellent opportunities for Threat Actors, skilled in picking up these situations fast, unlike companies themselves, which often do not have processes for the continual monitoring of their exposed surface area.

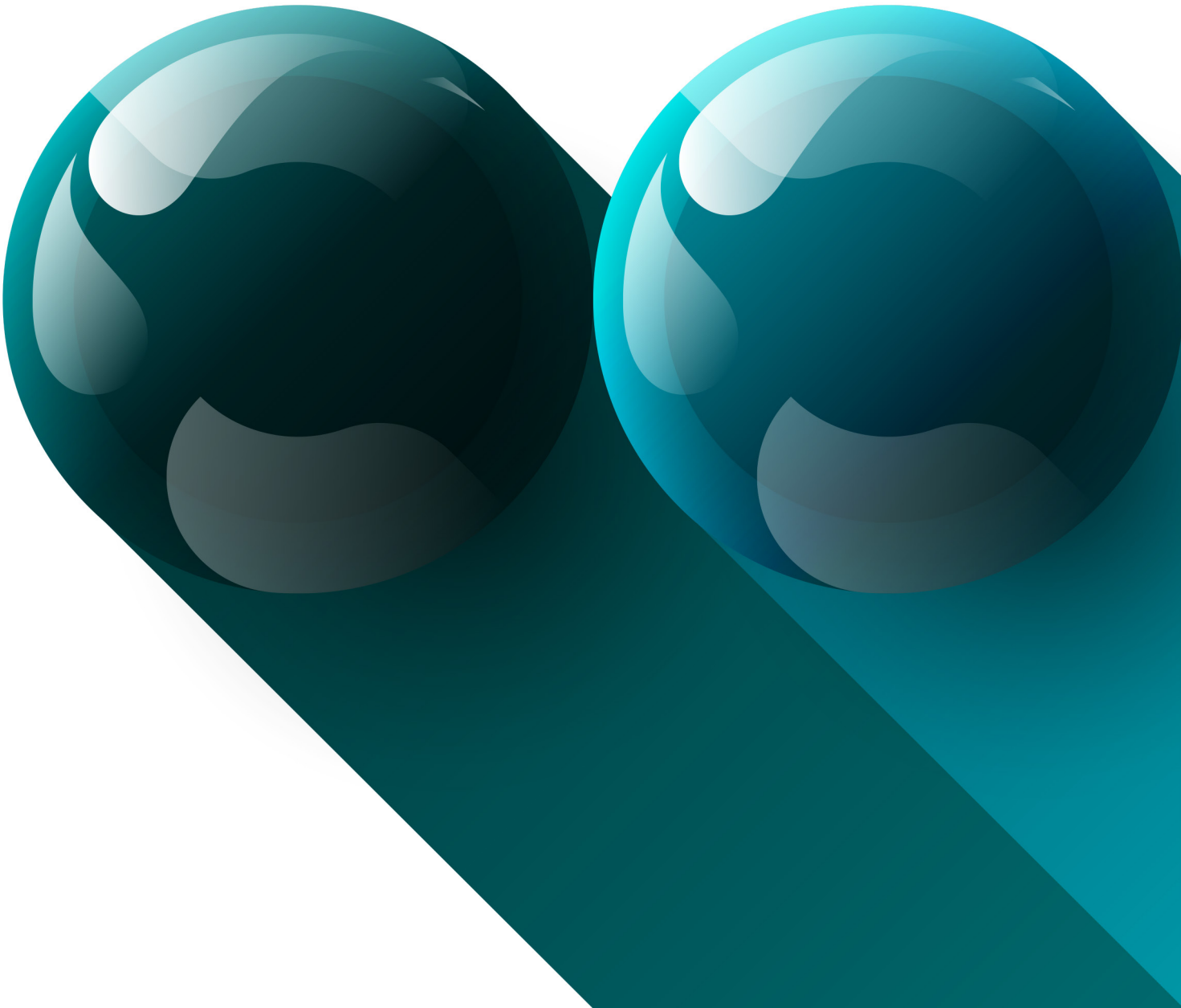
10 - Haphazard application of Two-Factor Authentication

The law has to be the same for everyone. In the last few years, many companies have invested strongly in the application of two-factor authentication on critical interfaces such as email, VPNs and critical portals. For practical or organisational reasons, this mechanism is still too often only applied in a hit-and-miss way. For example, a CEO who shares his email account with his PA, a supplier that offers remote maintenance on the electrical system from its own device, and so on down to warehouse employees who do not have their own company device, might all be exempt from this security measure and become an easy target for a Threat Actor.

2023 Update: here again, during 2023 this bad practice continued to be very widespread.

Appendix

AUTOMOTIVE CYBER SECURITY



Automotive Cyber Security

UN R155 and its significance for the automotive industry

The **UN Regulation No. 155 (UN R155)** introduced by the United Nations Economic Commission for Europe (UNECE WP.29) marks a turning point for the automotive industry and the entire value chain associated with vehicle development. **The goal is for cybersecurity to be officially required in vehicles**.

This regulation came into force in July 2022 for the type approval of new vehicle types and must be fully implemented for all newly registered vehicles by July 2024. Far-reaching, legally binding regulations for cybersecurity in vehicles have consequently been defined for the very first time.

The scope of UN Regulation No. 155 covers the currently **59 member states that have acceded to the UNECE Convention on the Harmonization of Vehicle Regulations** (based on the 1958 UNECE Member States Agreement), including all member states of the European Union, which remains one of the largest commercial markets for the industry.

This requires the UNECE regulations to be transposed into the national law of the member states, i.e. the individual countries must integrate the UN R155 requirements into their legal framework.

Global manufacturers who want to sell in the relevant target markets are therefore legally obliged to set up and maintain a comprehensive Cybersecurity Management System (CSMS) to obtain market approval for their vehicles. Alternatively, they could potentially be faced with sales bans.

Although other automotive markets, which are important for international car manufacturers, are not among the signatory states of the above-mentioned UNECE agreement, such as India, China and the USA, they are also following suit with comparable legally binding cybersecurity regulations or by adapting industry standards, which are also relevant for car manufacturers, to develop and sell cybersecure vehicles in these countries.

UN R155 covers all new vehicle types and is primarily aimed at securing vehicles against cyberattacks, while creating a management framework for the continuous implementation, management, and improvement of cybersecurity. The aim is to enforce vehicle users' security and protect their safety, as well as to ensure the availability of vehicle functions and the integrity of vehicle data. It is important to understand from the outset that achieving this goal requires more than just cybersecurity implementations in the development and production phases of the product

Automotive Cyber Security

New technologies increase the importance of cybersecurity in vehicles

The need for this regulation is evidenced by **rapid technological developments in the automotive industry**, including an ever higher level of connectivity in vehicles, an increasing range of internal and external vehicle services, the introduction of autonomous driving functions and the use of big data. These developments have led to new attack vectors.

Massive attacks on vehicles or entire vehicle fleets conducted remotely by dedicated hacker attacks become a realistic possibility if cybersecurity in the vehicle is not properly ensured.

Risks of cyber-attacks, data leaks and tampering are therefore on the rise. UN R155 addresses these risks by introducing strict security requirements and regular reviews of cybersecurity measures.

This has far-reaching implications not only on cars, but across vehicle categories and industries. UN R155 necessitates new cybersecurity requirements for the traditional passenger car market. Moreover, related vehicle categories such as commercial vehicles, special vehicles, emergency vehicles, buses and, in the currently situation, motorcycles and other possible forms of automotive mobility also fall within the scope of application.

This comprehensive approach to the scope in terms of **cybersecurity requirements** for different vehicle types is intended to provide protection against cyber threats for as many end users as possible.

The rule of thumb is that manufacturers and their suppliers in the automotive industry who develop and install E/E systems should always check the extent to which they are affected by these regulations in their business relationships and activities, as well as the relevance of their products to cybersecurity.

Effects on OEMs and suppliers

The implementation of UN R155 has far-reaching consequences for Original Equipment Manufacturers (OEMs) and their suppliers worldwide. The requirement to implement a CSMS not only places the responsibility for ensuring cybersecurity on OEMs, but also requires them to keep an eye on their supply chains. In concrete terms, OEMs assume the risk for suppliers' cybersecurity-related work.

It is difficult to estimate an exact figure, but it can be assumed that **thousands of companies in Europe alone are directly or indirectly affected by these regulations**. Implementing a CSMS ensures that both OEMs and suppliers are continuously conducting risk assessments, closing security gaps and adapting to the rapidly changing cyber threat landscape.

Automotive Cyber Security

Across the whole industry, the **ISO/SAE 21434 Road vehicles - Cybersecurity engineering standard** is attracting particular attention as the most important point of reference. The discussion, interpretation and organisation-specific implementation of the standard is currently being accelerated at a fast pace worldwide. There is still a need to intensively examine the details of the requirements and to determine the most efficient way possible to respond to them, since the standard defines what needs to be done rather than the manner in which this is achieved. This challenge must still be tackled in the day-to-day practice of implementing cybersecurity.

Cyber security requirements

In the current debate regarding cybersecurity requirements, new granular risk assessments must be carried out by the various players in the value chain. It has quickly become clear that very different answers to the same cybersecurity requirements need to be found for large OEMs and many large and smaller suppliers, as well as for technology providers and start-ups that want to enter the market with their new approaches and solutions.

This is intensified by **different security protection goals**: in addition to the actual system/product and the associated information streams and (PII) data, cybersecurity as a quality factor is always also about real operational risks. From product liability, contractual penalties, and financial risks to reputational and business losses. Another factor also receives special attention when it comes to vehicles as a means of transportation: physical security.

Safety meets security: the need for holistic cybersecurity

In line with cybersecurity requirements, the area of functional safety in the vehicle industry was professionalised several years ago. In a similarly systematic manner, it is placing the focus on correct and error-free functioning of systems. The physical integrity of the driver and the vehicle environment must now be sustainably harmonised with cybersecurity requirements. **Both areas aim to ensure the reliability, safety, and security of critical vehicle systems**. This requires a coordinated approach with the help of coordinated security concepts, right from the development phase and over the entire lifecycle of the vehicle.

Additionally, **the area of software updates is also being regarded as a separate area of responsibility**. The management and implementation of software updates (legally specified by UN Regulation No. 156 Software Update Management System in the vehicle industry) also plays a fundamental role in the interplay of security requirements.

There are numerous other necessities in terms of ensuring continuous cybersecurity activities, the monitoring of the vehicle fleet, e.g. by a dedicated vehicle operations center, effective incident response management and even far-reaching obligations, including the decommissioning of a vehicle bundle, several tasks that must be tackled in a coordinated manner.

Automotive Cyber Security

Differentiation from information security and IT

It is already apparent that the requirements for implementing cybersecurity in vehicle development go far beyond the traditional tasks of information security in a company. At the same time, however, there are also important new intersections and connections that are particularly driven by new technologies, systems and specialist skills, such as when it comes to establishing holistic solutions as an organisation, in the backend, in production and operational processes, and at the level of quality and management systems.

Enhancing agility for cybersecurity

In light of the automotive industry's rapid digitalisation and connectivity, it is essential that cybersecurity managers continuously review and adapt their security strategies. The integration of advanced technologies into vehicles opens up new points of attack and new requirements for a flexible approach to cybersecurity challenges. Ensure that you periodically check how well you, your organisation, your processes and your products are set up.

Encourage interdisciplinary collaboration

The complexity of increasing vehicle security requirements (in development, production, and aftersales, as well as at an organisational level) requires close collaboration between developers, engineers, testing, quality, purchasing and other divisions, as well as third-party service providers. Building a holistic approach that transcends boundaries between disciplines is essential to meet the diverse challenges of cybersecurity and effectively manage risk.

Fully understand top-level management commitments

A strong commitment at C-level and decision-maker level is essential for the successful implementation and maintenance of cybersecurity measures. This includes both the provision of necessary resources and the fostering of a security culture within the organisation. Cybersecurity operators should ensure that senior management understands the regulatory requirements and integrates them into their business strategies.

Genuine development of security awareness

It is becoming increasingly important to establish cybersecurity awareness and expertise beyond the traditional IT and development departments in all specialist areas relating to automotive products. Engineers, developers, product managers, commodity owners, purchasers and other non-IT professionals should have a basic knowledge of automotive cybersecurity principles. A company-wide security culture helps to ensure that all employees recognise potential risks and act accordingly.

Automotive Cyber Security

Paving the way for knowledge and skill building

What is the status of your cybersecurity competence centre? In a rapidly evolving environment, continuous investment in cybersecurity knowledge and skills and the right approach to experience/best practice is key. This includes upskilling existing employees as well as recruiting new talent with specialised knowledge. Promoting lifelong learning is critical to keep pace with changing cybersecurity challenges.

Promoting cybersecurity as a driver for quality

It is no longer acceptable to consider cybersecurity as a costly “add-on”. Given the growth of technologies and how they are used in development and within the organisation, a proactive approach to identifying and defending against potential cyber risks is required. If approached correctly, the right adjustments based on implementation/guidance for cybersecurity can provide far-reaching leverage for improving quality and competitiveness, as well as regulatory compliance.

CONCLUSIONS

Conclusions

Cyber security is no longer an option

In a more and more connected, technologically advanced world, cyber security is no longer an option: it is an imperative need. The increase in cyber attacks of varying nature and complexity demonstrates that today, **no sector is immune**. We have witnessed a sharp increase in the total number of security events and incidents, almost twice that of 2022. This increase is particularly sharp for events of critical severity, which soared by 300%. In line with this trend, in 2023 the YCTI team identified more than 193 million compromised credentials, a rise of 180% over 2022. This growth has been attributed to the **distribution of new Infostealer malware and the addition of new sources of intelligence**, the main entry-points used by attackers alongside the exploitation of exposed services and email-vectored malware. In fact, 2023 statistics reveal that **41.4% of employees open phishing emails**, **21.9% interact with links or buttons they contain and 13.4% enter valid credentials in trap forms**, revealing a level of awareness which still has room for improvement.

From the manipulation of sensitive data through to the sabotage of entire fleets of vehicles, cyber attacks are becoming more and more sophisticated and dangerous. In response to this growing threat, new regulations, requiring swift, strategic action on the part of businesses, have been introduced. **Regulations such as the Digital Operational Resilience Act (DORA), the TIBER attack simulation framework and UN Regulation R155 set strict standards for the management of IT security**. UN R155, in particular, marks a turning-point in the automotive industry, by requiring the integration of security management systems (CSMS) to ensure protection against cyber attacks for more and more connected and autonomous vehicles.

In this fast-changing context, **collaboration between different security teams has become fundamental**. **Integration between the Security Operation Center (SOC) and the Red Team in Purple Teaming activities has enabled better preparation for and response to attacks, combining simulated attack and defence to test and strengthen security measures. Similarly, integration between Cyber Threat Intelligence (CTI) and the Red Team has promoted an intelligence-based approach for attack simulations**, while cooperation between the SOC and Incident Response (IR) has reinforced incident response plans and attack prevention assessments.

Conclusions

Innovating is essential

The growing complexity of threat scenarios has made innovation in this sector absolutely essential. **The introduction of automation and artificial intelligence projects significantly supports' analysts work**. These technologies not only speed up data collection and analysis but also improve precision in detecting threats and generating rapid responses. The **Egyda project has marked a turning-point, introducing hyper-automation, machine learning (ML) and artificial intelligence (AI) to improve threat detection and management**. These technologies have enabled greater efficiency in analysing and responding to incidents. It is no less important to underline the need to continue to develop and implement solutions that exploit advanced technologies such as Large Language Models (LLMs), to manage the huge volume of data and further improve capabilities for detecting and managing threats or simulating attacks.

To conclude, in today's digital panorama, **security demands an integrated, innovative approach**. The new regulations not only set higher standards but also push companies to stay one step ahead of the cyber criminals. Cooperation between different security teams and the adoption of advanced technologies are essential to build a secure, resilient digital environment. With this approach, we can protect critical information and infrastructures while simultaneously guaranteeing security and trust.