# CYBER-IT

***CYBER IS A MARATHON NOT A SPRINT***

## INCYBER FORUM

*Event review : all you need to know about AI and the futur of cybersecurity*

## INTERVIEWS

*Quick chat with phenomenal cyber professionals*

## TOP 10 CYBER JOBS

*Cybersecurity Careers and salary trends*

## SPECIAL REPORT

# LOCKBIT

## WHO ARE THEY ? ARE THEY STILL ACTIVE ?

@arnaud_leroy

## EDITORIAL

What if I just created a little magazine? Just for fun. This is the first question I asked myself.

You are now reading the results of a small but passionate personal assignment!

I like trying new things, innovating, taking risks, but above all, I love cybersecurity and I am very tech savvy. I am not an editorial pro or even a journalistic prodigy, far from it, but I wanted to try and create a magazine that might be as interesting and insightful to others as much as it is for me.

This first issue is dedicated to one of the world's most formidable hacker groups, whose name automatically makes you think about ransomware: Lockbit ! In this report, you will discover the group's genesis and its most notable infamous projects.

I will also take a look back at the International Cyber Forum which took place in Lille (France) last March. A quick review on new technologies and trending tools showcased during the event.

As the demand for skilled cyber professionals is growing, we will explore the Top 10 trending Cybersecurity career paths.

And to end on a nice note, I had a quick chat with some key players of the French cybersecurity world, who kindly took the time to answer my questions. We had honest, candid conversations where they shared precious feedbacks and guidance about their career.

I hope you enjoy this little magazine as much as I enjoyed creating it.

Best regards
Arnaud Leroy

PS: A huge thank you to all of you for your ongoing support and your feedback on Linkedin since I announced the launch of this magazine.

# SOMMAIRE


4 **SPECIAL REPORT**
**LOCKBIT**
**From genesis to apocalypse ...**

12 **INCYBER FORUM**
**Event review**

16 **INTERVIEWS**
**Who are they ?**

20 **TOP 10 cyber jobs**
**Career paths, salaries, training and benefits ...**



IN CYBER FORUM EUROPE

SPECIAL REPORT

# LOCKBIT

## From genesis to apocalypse ...


## The origin of a plague

2019 was a decisive year in the world of cybercrime. It was during that year that a plague, which still strikes to this day, was born despite the efforts of many major law enforcement agencies around the world: Lockbit !

At the time I am writing this, the group has committed more than 1,700 attacks.
Lockbit is currently one of the most active and feared cybercriminal groups in the world. The organization is known for its sophisticated attacks and its ability to target high-profile companies.

On September 3, 2019, Lockbit appeared on the cyber scene for the first time, but it wasn't until March 2020 that they launched their first ransomware-as-a-service (RaaS) attack, and allowing other cybercriminals to use this malware for their own purposes in return for a commission.

Initially, the software became known as '.abcd', named after the extension that was added when encrypting the data it got its hands on.

By 2020, Lockbit was already claiming a large number of victims. It specifically targets businesses and government agencies, rather than individuals.
The group claims that its members were born in former republics of the Soviet Union. As a result, it does not attack Russian interests or former USSR countries.

Compared to its competitors, LockBit appears to be much more organized, as they are structured like a start-up company. In the programme created for its affiliates, the LockBit cybercrime group goes so far as to advise the industry targets to be avoided in order to incur the wrath of law enforcement agencies: healthcare institutions, the education system and oil & gas.

« **27% of ransomware cases handled by ANSSI (French National Cyber Security Agency) have been attributed to Lockbit over the last two years.** »


# Goodbye Lockbit, hello Lockbit 2.0 & 3.0

The first mentions of LockBit 2.0 in cybersecurity reports date back to early 2022.
It is likely that the group launched LockBit 2.0 gradually, while quietly testing the new version before launching it on a larger scale.

The first mentions of LockBit 2.0 in cybersecurity reports date back to early 2022.

It is likely that the group launched LockBit 2.0 gradually, while quietly testing the new version before launching it on a larger scale.

Since then, ransomware attacks spread continuously. During this first year of activity, they targeted high-profile victims such as Titan- HQ in May, from whom they stole more than $6 million in customer data.

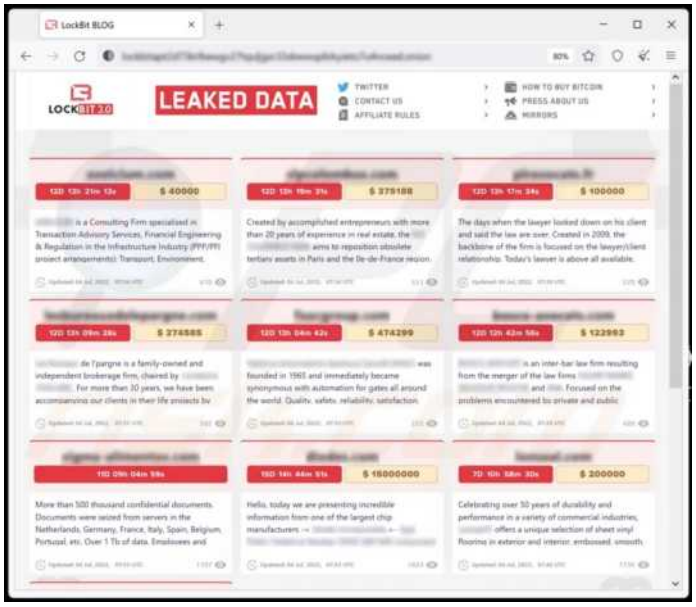
Travelex, a British foreign currency exchange specialist, was also hit by Lockbit's ransomware, which stole up to USD 2.3 million.
In February 2022, the police infiltrated Lockbit's systems and seized millions of dollars in ransom money. The group was forced to temporarily suspend its activities.

However, it was only a month later, in March 2022, that Lockbit resumed its activities and launched a series of attacks against leading companies. In May 2022, Lockbit released version 3.0 of its malware and significantly improved its evasion techniques so they could prevent detection by antivirus softwares.

They upgraded the malware and introduced a backup deletion function to make data recovery almost impossible for the victims.

Following a disagreement between certain leaders within the group, the source code was published by a developer on the Github platform in September of the same year.

Following this publication, the number of versions derived from Lockbit 3.0 is estimated at 400, according to Kaspersky.




*Screenshot of Lockbit's website before Operation Cronos*

# Lockbit against the rest of the world

The first arrests related to the group of cybercriminals began in October 2022. Tension escalated due to Operation Cronos, a collaborative effort involving 11 countries' law enforcement agencies.


*Screenshot of Lockbit's website during Operation Cronos*

**October 2022** marked a significant turning point in the fight against LockBit.
Canadian authorities intercepted Mikhael Vasiliev, a 33-year-old Russian-Canadian national, suspected to be an influential member of the group of cyber attackers.

During the investigation, the analysis of seized material revealed his involvement in more than a hundred attacks which occurred in France and there also seemed to be connections to other hacking groups such as Blackcat, Ragnarlocker and Darkside.

For Lockbit, the string of misfortunes continued for several months with a real-life manhunt. In **May 2023**, the FBI offered a $10 million reward for any information leading to the identification of Mikhail Pavlovich Matveev, alias 'Wazawaka'. According to the US agency, "Wazawaka" played a critical role in the development of the ransomware used by LockBit.

Despite the major efforts orchestrated, LockBit still stood up to the authorities. In **June** of that very same year, seven international cybersecurity agencies joined forces to block LockBit and published some guidelines for businesses and organization in order to help them protect themselves against this ransomware menace.

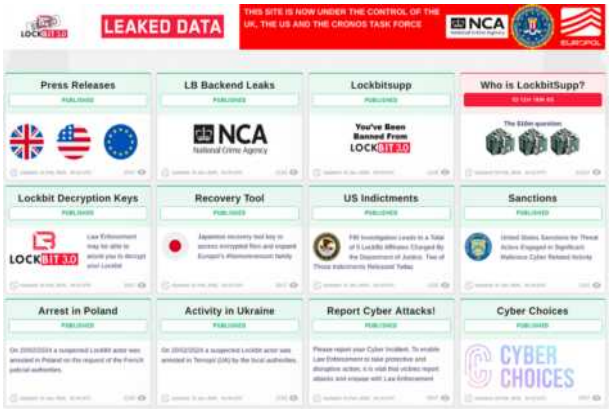
This initiative shows the seriousness of the threat represented by LockBit and the requirement for major international organizations to fight it.

In **June 2023**, the US authorities arrested Ruslan Magomedovich Astamirov, a 20-year-old Russian national probably from Chechnya, on suspicion of belonging to the LockBit group and participating in ransomware attacks between 2020 and 2023.

This arrest highlights the diversity of profiles existing within LockBit's members and the complexity of the fight against these cybercriminals.
The arrest of Mikhael Vasiliev and the identification of 'Wazawaka' by the FBI are major setbacks for LockBit. However, the arrest of Ruslan Magomedovich Astamirov showcased the group's ability to reinvent itself and recruit new members.

At the beginning of 2023, LockBit suggested to its affiliates to deploy a third ransomware program during their upcoming cyber-attacks: known as LockBit Gree, it based on the source code of "Coni" (another leaked ransomware).

The mobilization of international cybersecurity task force and the publication of a protection guide against LockBit proves the growing global awareness of the threat that this cybercriminal group represents. The fight against LockBit promises to be long and complex, but the cooperation of international task forces as well as the transparency in information sharing between public and private players are key to the success of this challenge.




*Screenshot of Lockbit's website during Operation Cronos*

EUROPOL
EUROPEAN LAW ENFORCEMENT AGENCY

# Operation CRONOS, the beginning of the end ?

Operation Cronos supported by several international law enforcement forces, including the French Gendarmerie Nationale, led to the capture of the core of Lockbit's infrastructure and will mark February 2024.

A meticulous investigation and unfailing international collaboration!

Operation Cronos is the result of a diligent investigation conducted over several years by Europol (The European union Agency for Law Enforcement), the NCA (UK National Crime Agency) and the national authorities of several countries. The investigators collected digital evidence, analyzed millions of financial transactions and conducted highly complex surveillance operations to identify the members of the Lockbit network and trace several of their illegal activities.

The success of this operation relied on steady international effort between law enforcement agencies from several countries. Investigators shared valuable resources and coordinated their actions, all while working on different continents, proving the undeniable power of collective efforts to fight against the growing threat.

NCA
National Crime Agency

The beginning of this operation goes back to 2022, when French authorities contacted Eurojust (European Union Agency for Criminal Justice Cooperation) to improve coordination of this wide operation, which involved 11 countries (the UK, the USA, Japan, Switzerland, Canada, Australia, Sweden, the Netherlands, Finland, Germany and France). Several servers were seized, 34 to be exact according to some sources. The authorities got their hands on a thousand decryption keys.

The seizure of these keys enabled the creation of a decryption software, which is available for those affected by Lockbit's ransomware, for free. The group has also been financially impacted, as more than two hundred crypto-asset portfolios were seized.
A number of important pieces of data were discovered on the seized servers, including a list of Lockbit's victims and a significant amount of data stolen from them.
The ransomware's source code was also discovered on one of these servers, along with a handful of documents providing a better understanding of the ransomware's complexity.

The ransomware's source code was also discovered on the servers and a number of documents highlighting the sprawling expansion of the group. As it turns out, their popularity is also due to their effective affiliation system.

It also appears that LockBit's developers were building a new version of their file encryption system, potentially to get prepared for the upcoming launch of Lockbit 4.0.

An outdated PHP server helped the police to exploit the servers.
The masterminds are still at large but they proved to be very resourceful, as they got their website back online in only five days.
The head of the group, the kingpin commonly known as "LockbitSupp", replied to the authorities in charge of Operation Cronos with a long letter in which he admitted being rather negligent recently.

Here is a quick extract from the document issued by Lockbit's leader :

*«... after five years swimming in money, I have become very lazy ... Due to my personal negligence and irresponsible behavior, I let my guard down and did not upgrade PHP in a timely manner.. »*

Will he stop there? He doesn't seem like it! He further wrote:

*« The leak of the panel's source code also happened at competitors' sites; that didn't stop them from continuing their tasks, and it won't stop me either. »*

*« What conclusions can be drawn from this situation? It's very simple: I need to attack the government more, and more often, and such attacks will force the FBI to reveal my weaknesses and vulnerabilities, which will make me stronger. By targeting the government, you will know whether or not the FBI has the capability to attack us »*

**The story goes on and the next steps have already started...**

# Operation CRONOS, new revelations...

The authorities struck again on May 7,2024, with Operation Cronos making international headlines as they announced a new takeover of the group's website and a countdown indicating that important revelations about LockbitSupp would be revealed in due course.

It is a real battle that has been going on for several months between the authorities and Lockbit. This time, the authorities are going all out to show that they are still in control of the situation despite the recent data leaked by Lockbit's hackers (notably data from the city hospital of Cannes in France, where 61GB of data was released on May 1, 2024).

At this time, Lockbit's website just got under the control of the authorities again.
One day before the fateful date of **May 7, 2024**, a new countdown appeared on Lockbit website indicating that the identity of the group's founder would be revealed soon, along with some other lockbit's partners information. At 2.00 p.m. on Tuesday May 7, the authorities communicated updates about Operation Cronos and openly published a statement about the alleged identity of the hacker known as LockbitSupp, one of the leaders of the criminal organization.

The individual presented by the FBI (Federal Bureau of Investigation), NCA (UK National Crime Agency) and Europol (The European union Agency for Law Enforcement) as the gang's mastermind is said to be a 31-year-old man going by the name of Dmitry Yuryevich Khoroshev.

Here is an excerpt from the press release:

*«Khoroshev aka LockbitSupp, who lived anonymously and offered a $10 million reward to anyone who revealed his identity, will now be subject to a series of assets freeze and travel bans. »*

The authorities will offer the same amount of money (i.e $10 million) as a reward to anyone who can provide legitimate information leading to Dmitry Khoroshev's arrest. This announcement undeniably shakes the network set up by Lockbit and weakens the authority of the group's partners.

The NCA states that it has identified 194 affiliations with the group for the purpose of acquiring and using ransomware in the form of RAAS (Ransomware As A Service), while providing a portion of the revenue generated by their activities. However, the documentation provided by the authorities mentions that only 80 affiliates benefited from this system.

Between June 2022 and February 2024, Lockbit is said to have conducted 7,000 attacks.
The group's official website only records a fraction of the attacks perpetrated, which could indicate that the success rate of these attacks is not as significant as we tend to believe.

Some hackers already began to turn against Lockbit and expresse it verbally on private forums and other chat rooms used by cyber-criminals.

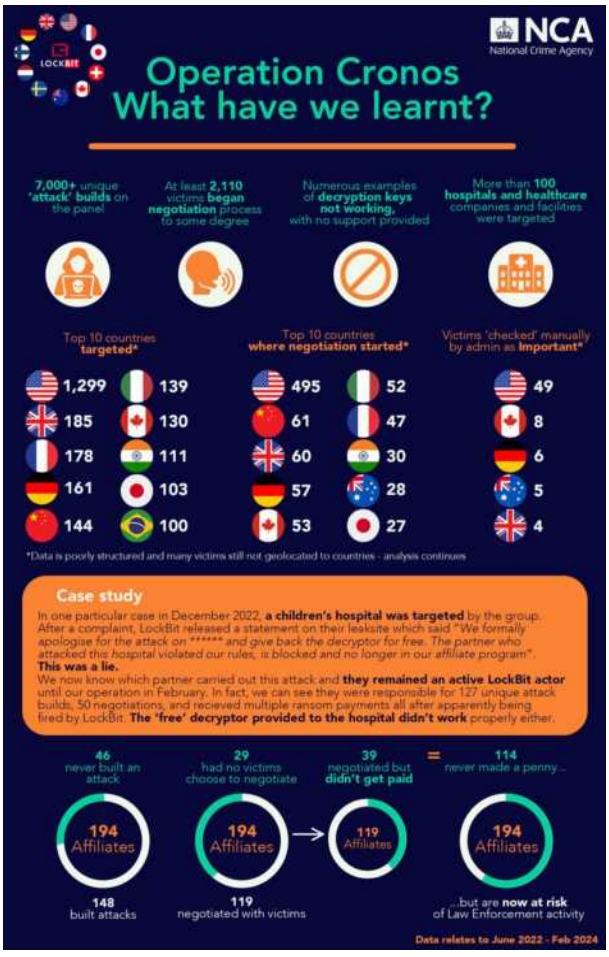
Another shocking revelation has been revealed ... last February, Lockbitsupp is said to have offered to provide the authorities with information on its competitors.

Is this real, or is it a sneaky move to destabilize the gang's structure a bit more?

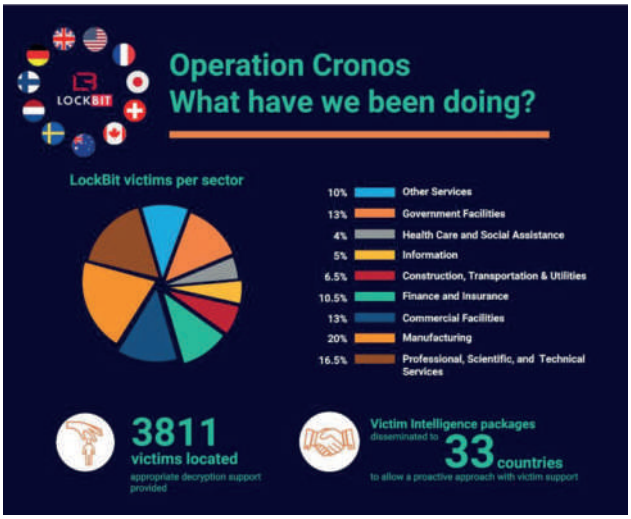
# NCA: the art of revelation

Documents from the FBI (Federal Bureau of Investigation), the NCA (UK National Crime Agency) and Europol (The European union Agency for Law Enforcement) are highly instructive as they reveal comprehensive information about some details which, until recently, remained rather vague.

The documents related to the countries affected by ransomware attacks, published by the NCA, reveal the ranking of the top countries targeted by the attacks, and we can clearly notice that the USA are far ahead with 1,299 attacks so far, followed by the UK (185 attacks) and France at the third place with 178 attacks recorded.




Then, a second document ranks the industries most targeted by ransomware attacks around the world so far and private companies are the primary victims, closely followed by government services. The healthcare industry comes last, with a total number of attacks at 4%. Nevertheless, the number of threatened hospitals and other healthcare facilities is growing continuously.




## Immediate response

For once, Lockbit wants to respond to the authorities, and apparently, have launched a "contest" in which they are offering $1,000.00 to anyone who can contact the notorious Dmitry.

Here is an extract from Lockbit's response:

*« To enter the contest, you have to contact relatives or the poor guy, who probably failed to mix crypto-currencies in exchange from mine, attracted the attention of the FBI, and along with it the $10 million reward for his capture. »*

**Is this the end of an era for cybersecurity or just another exciting twist ?**

# Lockbit, ethically immoral (?)

During the early years of the hacking group, they had a certain ethical code (if we can describe it as such...) but this so called “code of honor” has been shattered on several occasions recently, particularly during the last attacks on French hospitals.

Lockbit intended to respect a certain ethical conduct when the group was created (is it really ethical when you take money by force from a company or organization though?). They cancelled an attack orchestrated by one of their affiliates.

The Hospital for Sick Children (SickKids) located in Toronto, Canada, dedicated to children’s health and renown research center, experienced an unusual situation towards the end of 2022. A member of Lockbit's partnership system failed to respect the rules put in place by the group of hackers, which was not to hack any hospital's health data, that could result in endangering individuals’ health conditions.
Fortunately, according to the hospital's official press release, there were no casualties, but the attack did result in delays in patients care and delivery of medical test results.

When this attack was announced, Lockbit apologized via a note posted online:

*"We sincerely apologize for the attack on sickkids.ca and return the decryptor for free.*
*The partner who attacked this hospital violated our rules, is now blocked and is no longer part of our affiliate program."*

Yet, things have changed, but not in a positive way!
A few months earlier, in August of the same year, the hospital in the city of Corbeille-Essonnes (France) was attacked by the same Lockbit ransomware (it could have led to the death of patients…).

It is hard to comprehend... Since then, attacks on hospitals have exponentially increased, the Armentières hospital in Northern France on February 11, 2023, had to operate in “degraded” mode for several days putting patient’s health at critical risks.

Another example is the attack on the Simon-Veil hospital in Cannes (France) recently claimed by Lockbit.

photo - techhq.com

On April 16, 2024, the hospital was attacked by ransomware and robbed of some of its confidential data, with the threat to leak the data if the ransom, worth several million of euros, was not paid in due course.

The data included patients' medical record information, pediatric and psychological assessments. When the hospital did not respond to the ransom's requirements, the group executed their threats and disclosed 61GB of data on their website.
All the hospital employees’s data is also included (iD card, bank account details, pay slips, personal data, etc.).

Lockbit is still active and apparently their organization has not been much disrupted by Operation Cronos. The recent attacks are a way of proving to the world and its affiliates that they are still number one, but for how long?

Only time will tell!

# Methodology & highlights

How can a group like Lockbit claim so many victims, spread so widely and have such a global impact in a world that is becoming so acutely conscious about cyber issues?

## Root cause

Lockbit's ransomware uses a variety of methods to infiltrate its victims' computer systems. The most common techniques include:

**Phishing**: this well-known but unfortunately still all-too-effective method involves sending fraudulent e-mails to users, enticing them to disclose their most personal data, such as passwords and/or IDs.

**Exploiting security shortcomings**: by targeting obsolete or unprotected computer systems, ransomware can infect a computer without attracting attention.

**Installing malicious software**: some programs may contain backdoors that allow users to re-enter a system while staying very discrete and undetected.

## The Attack

**Exploitation:** this phase requires multiple social engineering techniques or brute force attacks to infiltrate a network. Attackers look for security vulnerabilities to gain access to the target system.

**Infiltration**: once inside the network, the attacker's goal is to gain elevated privileges and deploy the ransomware. This can include escalating privileges and navigating the network to identify various potential targets.

**Deployment**: at this stage, the ransomware is deployed on the network and attempts to spread to other workstations connected to the compromised network.

These attacks and propagation phases are essential.

## Data encryption

Once installed on a compromised machine, Lockbit will begin to encrypt the files present on the computer, making them impossible to access for the computer's user. This generally includes personal or professional documents, images, videos and other media files, as well as system folders essential to the running of the operating system.

## Ransom demand

After encrypting the data, Lockbit displays a ransom note on the user's computer screen. This note includes instructions to pay a ransom in cryptocurrency (usually Bitcoins), as well as a given deadline. If the victim does not pay within the set timeframe, they get threatened to get their data permanently destroyed or leaked on the darkweb.

**Major attacks chronology**

**2021**

February - Accenture
May - Colonial pipeline
July - OCDE
Décember - Gouv Costaricien

**2022**

January - Thales
August - Continental
September - CHR Essonnes
December - Sick Kids

**2023**

January - Nuxe
May - Taïwan semiconducteur
October - Boeing
November - Banque chinoise

**2024**

January - Subway
April - CHR Cannes

Cyber is a marathon not a sprint


# How does AI fit into the cyber world?

Ready for AI? Reinventing cyber security in the age of AI...

A quick rebranding but the same winning formula! The IN CYBER forum formerly known as FIC (Forum International de la Cyber) is back with a theme that keeps gaining momentum over the years: artificial intelligence and its role and impact in cybersecurity.

The InCyber forum brings together a multitude of individuals, including experts, software solution providers, users, schools, research centers and government services.
This year, from March 26 to 28 at the Grand Palais in Lille (France), all eyes were on a subject which concern, intrigues and frightens some: AI.

Is AI a tool or a threat? How can it bring us solutions where mankind reaches its limits?
The year 2023 saw the advent of generative AIs with ChatGPT or Google's Gemini (ex BARD) and many others, emerging and gaining more mainstream access and visibility.

From the creation of images, texts or even videos, they can be a real asset and a significant time-saver if used properly. Still, there are some risks and they are advancing as fast as the technological progress (or even faster). Lately, there has been an emergence of malicious AIs based directly from ChatGPT. They can be used to process hacking operations or to hijack images for harmful purposes...
The InCyber forum 's keynotes were a good opportunity to dive into the European AI Act and its seven key principles to ensure the controlled and enlightened development of AI in Europe and beyond.

**« Tomorrow's world will depend on what we collectively decide to do today »**

*InCyber Forum organizers*

## A practical example of how AI can help

During my visit, I could attend an interesting presentation from Palo Alto presenting the benefits of AI for security operations centers (SOCs), more particularly the help and added value it can provide to cyber analysts.

The conference led by Julien Billochon showcased a solution called CORTEX XSIAM, showing the power of AI and Deep Learning. The POC (proof of concept) highlighted the following elements:
A screen displaying more than 2,400 registered incidents, then the data is processed through an AI-managed system which helps categorizing and prioritizing the risks and drastically reduce the number of priority incidents to less than 100. Nearly 80% of these incidents and their risks have been proactively processed by the comapny's DBOT.
At this stage, approximately twenty incidents remain to be processed, so thanks to this tool the time saved for SOC analysts is very significant.

This 2024 edition showcased many new features, but also new events such as the "**Web3 Security Summit**", the "**InCyber Connect**" and its workshops tailor-made for CISOs, plus the "**InCyber Tour**".
The forum also debuted its own first Cyber party, the "**InCyber Night**", at the Grand Bazaar Saint-So.

**20 000**
**visitors**

**103**
**countries represented**

**700**
**exhibition partners**

## Artificial intelligence and the growing challenges faced by cybersecurity

While artificial intelligence is the subject of much debate, its crucial contribution to the fight against cybercrime is undeniable. While we face a growing shortage of qualified cybersecurity professionals, the cyberthreats still increase and AI is emerging as a valuable ally to strengthen the security of information systems.

Tools like Chat GPT and other generative AI models can provide critical support to corporate security operations centers (SOCs). By automating critical data analysis tasks, AI helps experts to focus on more strategic missions, like designing and implementing solutions to protect and fight cyberthreats.

The InCyber Forum highlighted experts' growing concerns about the rising number of cyberattacks, particularly in the wake of Paris 2024 Olympic Games. Intrusions into ticketing services and personal data breaches are disturbing real-life examples of the rapid evolution of the cyber menace.

## AI: A Double-Edged Sword but Promising

While AI is a valuable tool for cybersecurity, it can also be used for malicious purposes. Experts have warned about the risk of using AI for misinformation and information manipulation, particularly in the context of elections. Perfectly targeted phishing campaigns, based on the analysis of online behaviors, pose a real threat to democracy.

Integrating AI into cybersecurity strategies is essential to keep pace with the constantly evolving threats and effectively protect the information systems of businesses and institutions. The InCyber Forum has demonstrated the growing mobilization of industry players to harness the potential of AI in the service of digital security.


## The European Cyber Cup: a showcase for cybersecurity talents

The European Cyber Cub (ECC) represents over 20 competing teams, 200 players and 6 events. This year, **the GCC team** won the competition !

## Team feedback

Team GCC (which stands for Galette Cidre CTF) is a small group from the members of the CTF club at ENSIBS, a cyber-defense engineering school. GCC, more than a team, it is a student club, where we meet regularly to share our knowledge through workshops.

The team participating to EC2 was selected based on each team member's skills, and to this end we launched a survey where everyone could rate his/her skillsets and motivation for each event. The goal was to get experts in each category, but also people who were flexible and helpful in each event/competition.

We trained for EC2 throughout the year via the GCC sessions, but also by taking part in other CTFs. Additionally, we ran 3 special training sessions on EC2 forensics, trying to solve challenges from preceding years. During one of these sessions, an ENSIBS alumnus who is now a forensic expert, came to help us. He introduced us to some tools and techniques he found relevant for the upcoming EC2.
Unfortunately, the cancellation of the web3 test was a clear setback for our team.

You have to get started to succeed. In cybersecurity, we often say to ourselves "I'm not good enough, I can't do it". Nonsense, in CTF, you have to try! And even if, in the end, you don't manage to solve a challenge, the time spent looking for a solution will allow you to make great progress. Besides, writeups are often available after each CTF challenge, so you can learn new techniques and understand the reasoning used to solve the various challenges. Think of the CTFs as an exercise, not a competition - you are here to make progress..

**Léo CHAIGNEAU**
**GCC-ENSIBS President**

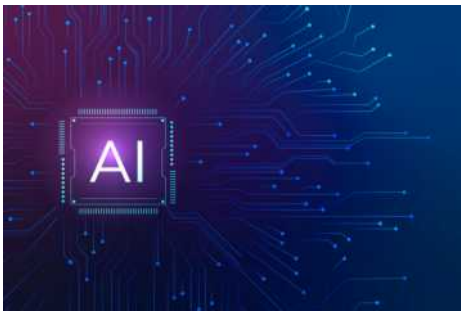
* *For privacy reasons, some faces have been hidden.*

## PALMARES

**1st** - EC2 2024
**1st** - HTB University CTF 2023 - 955 teams
**1st & 2nd** - ESAIP CTF
**2nd & 3rd** - ECW CTF
**2nd** - EC2 2023
**4th & 5th** - BreizhCTF 2024
**9th** - Crew CTF - 382 teams
**31st** - HTB CyberApocalypse CTF 2024 - 5694 teams

InCyber Forum's insights from **Olivier Cimelière**

# Artificial intelligence & digital scams: are we doomed to be fooled ?




Gartner, a major consulting firm, estimates that 20 % of the phishing attacks conducted in 2023 were AI-based, and that this trend is set to increase. How can we protect ourselves? What organizational processes can we implement? What solutions are available to combat these threats? A number of specialists shared their analysis at a round table held as part of the InCyber Forum 2024 in Lille (France).
In February 2024, a Hong Kong-based company was the target of a "president scam" made believable by an AI-generated deepfake videoconference. Confident and trusting he was having a meeting with his colleagues, an employee agreed to make several bank transfers for up to 24 million Euros in what turned out to be a spectacular fraud. For the experts, this is the world's first case of the famous "president scam" tailored by generative artificial intelligence.

Scams on digital and communication networks are nothing new. However, the addition of AI to boost the ability to mislead individuals and companies, is preoccupying for IT and cybersecurity professionals. Antoine Bajolet, a member of Clusif (French non-profit promoting cybersecurity) and CISO of Henner - an insurance brokerage group - broadly distinguishes three categories of digital scams: hacking, which involves intrusion into an organization's IT systems; disruption threatening ones reputation; and scams based on e-mails or text messages committing identity theft in order to steal money and/or sensitive information.

## Public enemy No. 1: spear phishing

According to Antoine Bajolet, it is in this last category that the danger gets most obvious, AI is now used for fraudulent purposes, through a powerful hacking method commonly known as spear phishing. This method perfectly reproduces the visual, graphic and semantic codes of a given sender, while adding contextual elements to personalize the message and seduce the target's suspicions. AI has considerably improved the capabilities of spear phishing as it can now reproduce an individual's exact identity and the way they express themselves.

The recipient will either reply or click on an illegitimate malware link enabling hackers to access an organization's computer system. Antoine Bajolet mentions the case of Pikabot, a sophisticated and dangerous malware that has been around since 2023.

Jean-Baptiste Roux, Vice-President Europe Sales at Sosafe, a company providing cybersecurity solutions to various industries, shares the same concerns. AI-engineered spear phishing generates a much higher click-through rate than traditional scams due to its ability to imitate familiar contexts. As a result, people are more prone to fall for these scams. Referring to a recent Sosafe study, Jean-Baptiste Roux explains that, in 2024, generative AI, which makes social engineering tools more elaborate and more complex to detect, will challenge human's psychology significantly with an unprecedented number of similar scams.

## When in-house expertise "encourages" scams

Philippe Loudenot, Director of Cyber Strategy at Forecomm, a company designing cybersecurity solutions for businesses, shares the same perspective. AI makes it possible to accelerate and massively scale digital scams. For him, "the worst is yet to come. The only limit will be the human mind and its ability to create malicious products. It's essential that we keep and cultivate a critical approach, we should allow ourselves a little more time to pause and reflect while reading a message rather than clicking the link without any second thoughts. This is still the best protection".

Antoine Bajolet confirms that scams are usually effective because "the root of them all is human error". This error can also come from within an organization. In certain customer service chat discussions, developers may open up to the bot (to feed it) providing confidential data, which are then combined with more basic data. Unfortunately, the data can potentially leak outside the organization when it should have remained in a secure internal environment. This data can inspire hackers to design new, more advanced scam methods.

## Human vigilance, the best defense

Specialists are not panicking yet. Protective solutions do exist, and they are not just technological. For Antoine Bajolet, the first is common sense and vigilance, such as taking a closer look at the domain name (DNS) used in the message. Most of the time, an organization uses a single, official DNS to communicate with its audiences. It is a good practice to carefully check the domain name extension (.fr, .com or something more exotic!) and its spelling. Pirates use similar domain names (with the exception of one character or a reversed letter) to usurp a sender's identity, it can be very subtle.

Antoine Bajolet adds that the methods used by malicious AIs hardly change at all. We need to apply the IT security measures that exist in every organization rigorously and constantly. They remain entirely relevant to manage AI-based scams. In case of extreme doubt, don't hesitate to pick up the phone and call a colleague to check whether the message is genuine or fraudulent, and whether it really comes from him/her or from a fake avatar. Keeping a critical eye is still an excellent preventive measure against digital scams.

Jean-Baptiste Roux points out that AI-based scams are inspired by human behavior, as people process information faster and faster, without necessarily paying attention or taking a step back from a very well-designed scam. He also finds that companies tend to resort to AI without even thinking about the introduction of a strict company governance framework. An estimated 300 million users have now adopted AI in their business practices, without any guidelines and procedures in place to help secure the use of data or protect intellectual property. This is an issue that organizations need to be more aware of. At a time when 100% AI-automated malware is spreading, the issue is indeed critical.

**Comments by Olivier Cimelière**

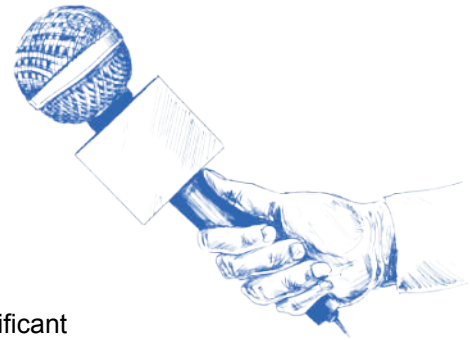
**About the author**

**As a former press and radio journalist who graduated from Celsa School, Olivier Cimelière went on to hold corporate communications responsibilities at major international companies such as Boehrin- ger Ingelheim, Nestlé Waters, Ericsson, Google, Ipsos and Generali. In 2013, Olivier Cimelière founded Heuristik Communications, now known as Heuristik Reborn, a consulting firm specialized in communications strategy, reputation management, crisis management and editorial influence for business executives and companies of all sizes.**

**He has also been the author of the Blog du Communicant since 2010, and has published two books about the digital revolution in journalism and communications. He is a regular contributor to various French media (LCI, Les Echos, Public Sénat).**

INSIGHT movers and shakers of today's cybersecurity world

# We know them from their daily posts, but who are they?



Over the last few weeks, I have discussed with a number of people who have had a significant impact on the cyber and IT world. They are consultants, SOC (Security Operations Center) managers, training managers or CEO of cybersecurity companies and they took the time to answer a few questions during our casual chat sessions.
Here are a few insights I collected during these great conversations.

## MATHIEU PICHON
SOC Manager

### Hi Mathieu, thanks for taking the time to answer my questions. First of all, who are you ?

"Hello Arnaud, my name is Mathieu Pichon and I'm a manager in a Security Operations Center (SOC)"

### Can you explain your academic background ?

"Yes! I made a career change, and then obtained a Bac +2 through an accelerated program. I've mostly been self-taught in my cybersecurity career"

### What are your work's day-to-day missions ?

"My job involves a wide range of tasks, but the main ones are strategic and technical decision-making, planning operations and deployment, also providing support to the company's employees"

### What's a typical day like for you ?

"As mentioned above, it is very broad, no day is really the same, each one as rich as the next"

### What do you like and dislike about your job ?

"I particularly appreciate the fact that every week is different. On the other hand, I admit that sometimes, the technical email replies I have to provide can be tedious. Also, personal time off management and technical tickets management can be challenging"

### Thank you, do you have anything you would like to add ?

"I think it's important to remember that this job requires effective stress management skills, the ability to make critical decisions quickly, as well as expertise and, above all, a PASSION for cybersecurity"

## LAURENT MINNE
### Senior cybersecurity engineer

**Hi Laurent, I'm lucky enough to discuss with you regularly. Can you tell us who you are in a few words ?**

"Hi Arnaud, I'm Laurent Minne, Senior Cybersecurity Engineer, and I've been passionate about IT security for many years. I've been working for Thales Belgium since the end of January as an integration, verification, validation and qualification engineer. The most important point is that I've been self-taught for some thirty years now, and I'm still learning every day, even after flying for 48 hours"

**Can you describe your career path in a few words ?**

"We should go back in time a little, I have an unconventional profile; I began my professional career as an electrical equipment mechanic, while working as second chef in a seaside restaurant in the south of France at the same time. As soon as I returned to Belgium, I embarked on a long career with a facility management company as a handyman with a small IT security business.

In 2013, I took a leap of faith and decided to go freelance, mainly focusing on IT security, with systems and network administrator skills. My assignments were as diverse as they were numerous, and I was lucky enough to work alongside great people. At the same time, I continued to learn new techniques, disciplines and got the opportunity to work with passionate people.

Sharing, helping each other, intensive work fueled my passion for computer security (then Cyber-security) and it was in 2023 that I decided to create a community, a French-speaking collective (all volunteers) around CyberSec called “Be-- Cyber Community” in the form of a Discord channel whose missions are to share, help each other, build collaborative skills by offering various workshops, webinars and giving access to plenty of resources to the members"

**Excellent ! And what are your daily missions ?**

"They are diverse; as I'm an early riser, I take the time to do the warm-up and look for interesting tools and resources for upcoming Linkedin posts. My main task at the moment is to analyze risks about various technologies, research information about the Security Discipline, find new sources of inspiration for upcoming projects.
In the evenings, I'm mainly involved in co-managing the Be-Cyber Community, helping other communities such as Edu.Cyber, Cyber V, Kaisen Linux and some associations. I study open source and free projects related to Cyber Threat Intelligence and researches, among others"

**What's a typical day like for you ?**

"The ideal day is when I've learned something, otherwise it would get boring !"

**What do you like about your job ?**

"Working with extraordinary, competent, intelligent and passionate people. I am slightly repeating myself, but sharing information is essential for me in order to achieve the ideal day"

**Perfect ! Do you have anything you would like to add ?**

"Thank you for this interview. When companies of all sizes will understand that IT security is a journey, not a destination, they will go further.
For young people wishing to join the world of Cybersecurity; don't remain passive, study, practice daily, work hard, don't be afraid to fail, don't think about the salary, think about what you're passionate about and then the salary will come"

## FREDERIC LOISEL
### CEO of Armoring

**Hi Frédéric, it's a pleasure to share this moment with you, can you tell me a little more about yourself ?**

🎙 "Hello Arnaud! I've been a computer enthusiast since I was very young, and I've also played a lot on the Atari 520 STF, Amiga 500, Sega Megadrive, Playstation 1 & 2, etc..."

**Can you tell me a little bit about your background ?**

🎙"I passed my baccalauréat D and joined the French Navy at 19. After six years in the Navy, four of which were spent at the CORSEN Regional Sea Rescue Center, I worked for a good twenty years as an IT manager in several French SMEs and ETIs. And a few weeks ago, I created my own company, ARMORING."

**What are your day-to-day missions ?**

🎙"I'm currently developing my new business, which focuses on cybersecurity awareness, and I'm working on the creation of a new product designed to help companies to anticipate and get prepared for cyber crises.
The release is scheduled for June-July 2024 (teasing!)"

**What's a typical day like for you ?**

🎙 "I start my day early, especially when I'm not travelling. I take an hour-long walk to clarify my thoughts and come up with new ideas. Then I devote myself to creating content for the upcoming workshops I will be running. I also spend a lot of time reading and keeping an eye on things"

**What do you like and dislike about your job ?**

🎙"I love interacting with people who want to share knowledge and, most importantly learn new things all the time.
That is why I went back to school to study for an MBA at the "École de Guerre Économique", an enriching experience which allowed me to make new connections and meet fascinating people.
What I dislike is when my colored pens are not aligned or the sheet of paper next to me is not placed at the right angle on the table"

**Any final words ?**

🎙"Always stay humble and listen to people.

🚨🕓👨‍💼 Frédéric : "I wish you all a beautiful day and stay tuned for some new upcoming crisis management stories on my profile""

ARMORING

## SIVANESAN SIVATHASAN
### Cyber training manager & consultant

**Hi Siva, can you tell us more about who you are ?**

"Hi Arnaud! I'm a training manager at M2i Formation and also a cybersecurity consultant.
I'm passionate about new technologies and, like many, self-taught"

**Can you tell me about your background ?**

"My background is atypical. Although my level of education is limited to a Bac+2, I got various cybersecurity and IT certifications equivalent to a Bac+5.
The experience and knowledge I have now mainly comes from professional experience, self-study and research on the Internet"

**In a few words, what are your day-to-day missions ?**

"On a day-to-day basis, my missions consist of training professionals and students on the different aspects of cybersecurity. I also complete a thorough cyber watch to follow up on new technologies and trends and be aware of the latest updates in this constantly evolving field"

**And what's a typical day like for you ?**

"My typical day is usually filled with courses preparation, presentations and interactions with my students. I also discuss with customers to improve the security of their IT systems infrastructures"

**What do you like and dislike about your job ?**

"What I like about my job is the opportunity to help others to protect themselves in this over-connected world. Although my days may seem repetitive, I continue to learn every single day on so many different levels. However, sometimes the technical and human challenges can be a source of frustration"

**Thank you, it was a real pleasure! Do you have any closing thoughts ?**

"Thank you! I will say that I am passionate about what I do and find great satisfaction in sharing my knowledge with people.
As Socrates said: “Knowledge is the only thing that grows when you share it"

# TOP 10
# Cybersecurity jobs

With the news constantly confirming that cyber risks are on the rise, the development and recruitment of IT security professionals has become a major priority for organizations, globally. The Healthcare industry, local authorities, the military and other institutions must also respond to this new reality. On a global scale, it is now essential to build a solid response with strong technical and strategic expertise. Cybersecurity-related positions can legitimately be considered as the professions of the future.
Here are the top 10 trending jobs (don't worry, many more exist!).

*ll of the following jobs can be accessible with strong determination and self-training. This list and the mentioned guidelines are purely for information purposes only (I would like to thank Guardia School for their inputs).*

HACKER

PENTESTER

SOC ANALYST

CYBERSECURITY CONSULTANT

CYBERSECURITY ENGINEER

CISO

CYBER THREAT ANALYST

CYBERSECURITY ARCHITECT

SECURITY PROJECT MANAGER

CRYPTOGRAPHER

# 01 HACKER

A Hacker is not a Cracker!

Hacker = Hackers are motivated by the desire to improve the security of computer systems and help protect data and digital infrastructures.

Cracker = crackers often have malicious motivations, such as stealing sensitive information, extortion, data destruction or sabotage.

**Education level** : Bac +5
**Labour market / skills demand** : High
**Starting salary** : 4,000.00 Euros (monthly)

## Education

You should be comfortable in computer science and specialized in cybersecurity in order to become an ethical hacker.
You will need a minimum of 3 years' higher education, or you can go on up to 5 years. There are several options for training: university, engineering school or a school specializing in cybersecurity.

## Pros & Cons

Choosing a career as a hacker means to commit to a profession of passion as you become part of the ongoing battle for cyber defense and cyber resilience. The salary can also be an attractive leverage, depending on the professional missions you seek. However, hackers work for long hours securing companies information systems. The job requires a fairly high level of commitment and dedication.

## Salary

The salary depends on the size of the company and the candidate's experience. On average, a junior hacker working in France will earn 4,000.00 Euros per month, versus 7,500.00 Euros for more senior profile. In the United States, the average annual salary is around USD 80,000.00
An increasing number of professionals are also rewarded for solving bugs through bug bounty platforms.

# 02 CYBERSECURITY ENGINEER

**Education level** : Bac +5
**Labour market / skills demand** : High
**Starting salary** : 3,000.00 Euros (monthly)

## Education

If your goal is to become a cybersecurity engineer, then you should be able to take on several years of study to reach the level Bac +5. This will make you an IT specialist, but also an expert in cyber issues. To train for this, you need to attend a school specializing in cyber security or an engineering school. Some companies may require that the applicant has additional security/product certifications.

## Pros & Cons

Supervision and administration of IT systems, threat and vulnerabilities analysis, security features testing, security incident response... The cybersecurity engineer profession is intense, perfect for those who appreciate a challenge and want to take on significant responsibilities. The job is demanding: you should be able to catch up quickly, and keep a constant cyber/tech watch, because technologies and vulnerabilities evolve as quickly as the cybersecurity engineer's missions.

## Salary

The salary of a cybersecurity engineer varies according to the size of the company employing him/her, his/her experience and their location. On average, a junior cybersecurity engineer working in France will earn 3,000.00 Euros a month and 5,000.00 Euros for a senior profile.

# 03 PENTESTER

**Education level** : Bac +5
**Labour market / skills demand** : High
**Starting salary** : 3,000.00 Euros (monthly)

### Education

You will need a degree in computer science (Bac +3 to Bac +5) with a major in cybersecurity. A school specializing in cybersecurity can help. Security/products certifications may also be required. It is worth noting that some pentesters are self-taught, as this is a new profession which tech-savvy individuals are passionate about. Some malicious crackers changed their path along the way and became pentesters (ethical hackers) for major organizations and companies.

### Pros & cons

Contrary to popular belief, a pentester is not a lonely, introverted nerd. She or he is a consultant. They must make sure that the data/information they process is easy to digest for their audience as they test their client's systems vulnerability. You must not be afraid to express yourself to your audience, management, team members or customers. The job is demanding, as it demands to be technically qualified and have a range of soft skills. You should also keep a close eye on the latest technologies' advancement.

### Salary

A pentester's salary varies according to the size of the employing company, experience and location.
On average, an entry-level pentester in France will earn 3,000.00 Euros per month, and up to 5,000.00 Euros for a senior pentester.
In the United States, the average annual salary for a pentester is around USD 110,000.00

# 04 CYBERSECURITY CONSULTANT

**Education level** : Bac +5
**Labour market / skills demand** : High
**Starting salary** : 3,500.00 Euros (monthly)

### Education

You will need a 5-year degree. A level of study that already makes you an expert in cybersecurity. This is what companies usually ask for when recruiting for this position.
For example, you can study for an engineering degree or a Master 2 with a major in cybersecurity.

### Pros & cons

The benefits of working as a consultant are that you get to work on a wide variety of projects, gaining valuable experience on various technologies. It also allows you to find out which subjects you are the most interested in. There's no routine in this profession as moving from one project to another means that the priorities and audience can change regularly.
You will still need to update your skills on a regular basis.

### Salary

The salary varies depending on the candidate's experience and the profile of the company they applied to. A junior consultant can expect to earn between 3,000.00 Euros and 3,500.00 Euros per month. After a few years, their salary can easily range between 4,500.00 Euros and 5,800.00 Euros per month, depending on whether they are working in a consulting firm or on in a customer's company.

# 05 SOC ANALYST

**Education level** : Bac +5
**Labour market / skills demand** : High
**Starting salary** : 2,900.00 Euros (monthly)

### Education

You should have a 3 to 5-year degree in computer science, with a major in information systems security, to become a SOC analyst. Initial experience in network and systems engineering is required.

### Pros & Cons

The SOC analyst career path means opting for a job that is meaningful, since joining the SOC means being at the core of a company's cyber-defense strategy.
On the downside, there's the pressure of responsibilities. Indeed, it's important to be able to be calm under pressure, as the SOC analyst operator has to manage and process extremely sensitive data.

### Salary

At a time when the topic of cybersecurity affects all professional spheres, more and more companies are equipping themselves with a SOC. In France, the average entry-level SOC analyst earns between 2,600.00 Euros and 3,200.00 Euros per month. Experienced SOC analysts can earn up to 48,000.00 Euros per year. Abroad, in Switzerland for example, a SOC analyst operator can earn up to CHF 100,000.00 per year.

# 06 CYBERSECURITY ARCHITECT

**Education level** : Bac +5
**Labour market / skills demand** : High
**Starting salary** : 5,000.00 Euros (monthly)

### Education

You will need a 5-year degree in computer science specializing in information systems security.
You must also have at least 8 years' experience in information systems' technical architecture. Cybersecurity architects should be rigorous and stress-resistant, as they manage and monitor all the different aspects of the company's information system.

### Pros & Cons

A career as a cybersecurity architect is rewarding for anyone wishing to handle the most critical cybersecurity issues.
This IT security expert is managing the company's information system. The cybersecurity architect is not only an experienced engineer, but also a manager and administrator. On the other hand, the pressure of the job's responsibilities can be challenging.

### Salary

In France, junior cybersecurity architects earn an average of 40,000.00 Euros - 60,000.00 Euros per year. With more experience, they can earn up to 80,000.00 Euros per year. In the United States, architects can earn between USD 92,000.00 and USD 222,000.00 a year. Salaries can vary depending on the company, the level of experience required for the position and the location.

# 07 CISO

**Education level** : Bac +5
**Labour market / skills demand** : High
**Starting salary** : 5,800.00 Euros (monthly)

### Education

The Chief Information Security Officer needs a 5-year degree from an engineering school or university, with a major in cybersecurity.
A minimum professional experience of 5 years in cybersecurity is necessary.

### Pros & Cons

This position is key within the company's leadership team. As the leader of the company's security strategy, the CISO has a direct influence on the organization's strategic decisions.
However, this role comes with its own challenges.
The CISO should continuously evolve with technology, they also should analyze various threats and regulatory compliance matters and all of this while managing the pressure and high exposure that comes with the role's responsibilities.

### Salary

The average salary for a CISO is around 100,000.00 Euros, with salary range starting from 40,000.00 Euros and rising up to 150,000.00 Euros annually. With a few rare exceptions, salaries can get up 200,000.00 euros.
These wide variations are due to the size of the organization and the CISO's level of expertise.
Internationally, in the USA for example, a CISO can earn between USD 80,000.00 and USD 200,000.00 per year.

# 08 CYBERSECURITY THREAT ANALYST

**Education level** : Bac +5
**Labour market / skills demand** : High
**Starting salary** : 3,500.00 Euros (monthly)

### Education

Cybersecurity threat analysts can work freelance. After a few years of experience on the job, you can easily take a leap of faith to work independently. It allows you to work on projects that align with your career goals with more flexibility. Freelance work requires more discipline, professionalism and expertise than a regular salaried position.
The cybersecurity threat analyst can also choose to join a cybersecurity experts' firm, which will position them on various missions.

### Pros & Cons

Choosing to make a career as a cybersecurity threat analyst means being passionate about the job as you use a variety of cyber defense tools. It is a very trending job at the moment.
However, projects can be intense and very demanding. During the solution testing phase of cyber solutions, workload can intensify while remaining steady during the operational phase of a project. It can also increase significantly during pentesting projects, new technology/ product testing phases.

### Salary

In France, the average monthly salary for a cybersecurity threat analyst position is between 3,200.00 Euros and 3,500.00 Euros. A more senior profile can expect approximately 4,000.00 Euros - 5,000.00 Euros, annually.
In the USA, a cybersecurity threat analyst can earn an average of USD 86,000.00 per year.

# 09 CRYPTOGRAPHER

**Education level** : Bac +5
**Labour market / skills demand** : High
**Starting salary** : 2,800.00 Euros (monthly)

### Education

You should embark on a long training process (minimum five years) to acquire all the skillset and knowledge required to become a cryptographer. You should have very good technical skills. It is recommended to get an engineering degree with a major in cryptography, information security and coding.
Or you could opt for a Master's degree from a school specialized in cybersecurity, offering courses in cryptography and information systems security.

### Pros & Cons

Cryptology is a career path involving a level of passion and dedication that you rarely choose by accident. If you love spending hours trying to solve complex code, this could be your dream job!
However, you will need to be patient, meticulous and resistant to pressure, as cryptographers work in extremely critical situations.

### Salary

Cryptographers are in high demand on the job market. Indeed, with the job market extremely favorable to recruitment in the cybersecurity sector, cryptology profession is a career choice offering excellent prospects and opportunities.
In France, an entry-level cryptographer can expect to earn between 2,500.00 Euros and 2,800.00 Euros per month.
Mid-career, salaries can reach 4,900.00 Euros per month.

# 10 CYBERSECURITY PROJECT MANAGER

**Education level** : Bac +5
**Labour market / skills demand** : High
**Starting salary** : 4,000.00 Euros (monthly)

### Education

A degree in computer science (Bac+3 to Bac+5) specializing in IT is recommended. You should have at least one year of experience in cybersecurity or IT project management.
Some companies also require security/product certifications, such as ISO 27001 (cyber risk assessment, threat analysis, incident management).

### Pros & Cons

If you like project management and teamwork, this job could be just what you are looking for.
As a cybersecurity expert, you should be able to adapt to your audience, and be comfortable to work with a variety of stakeholders, including company management, team members and customers.
The job is demanding and challenging as you evolve in a fast-paced environment: you should be proactive and get informed on the latest cybersecurity trends as the field is constantly evolving.

### Salary

Compensation for a cybersecurity project manager varies according to their skills and professional experience, but also the company they apply to. On average, a junior security manager working in France will earn 4,000.00 Euros a month, compared to 6,000.00 Euros for a senior profile. In Switzerland, a cybersecurity project manager's average salary is approximately CHF 9,000.00.

Arnaud Leroy - 2024 May