VICI

Swiss Intelligence Services

By creating VICI Swiss Competitive Intelligence, I wanted to provide private individuals and companies with some of the most advanced tools of digital investigation in the world. This will enable them to be informed about their digital environment, to protect themselves and this to secure positively influence their business.

In short, I wanted to create the NSA for everyone.

Daniel Donnet-Monay, CEO

World-class cyber intelligence and cyber protection for businesses and individuals

VICI is the first line of protection for companies, institutions and individuals against cyberattacks. By collecting intelligence from the deepest layers of the dark web to the surface web, we anticipate threats and thwart attacks, protect your data and ensure the smooth running of your business.

Our services to protect you

VICI stands guard where the action takes place

Hackers now target not only large or small companies but also institutions and private individuals, using often devastating cyberattacks.

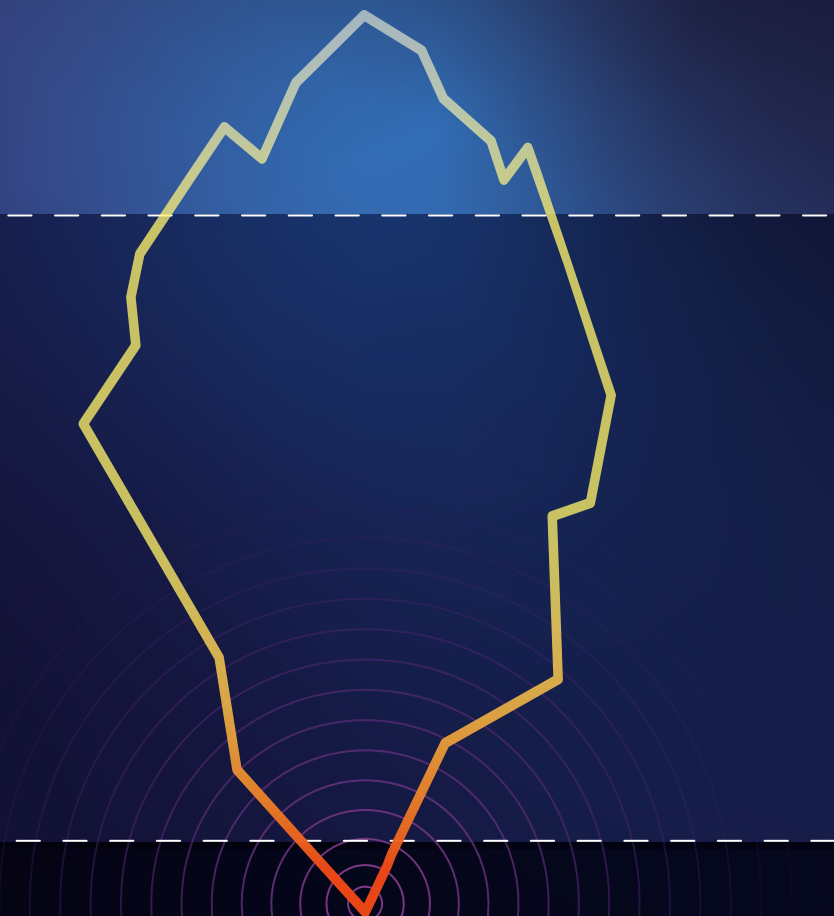
Thanks to our unique ability in the industry to operate in the deepest layers of the dark web, to closely monitor the hackers who communicate with each others while preparing their attacks; we are able to recognize the threats that target you, to anticipate and protect you before these attacks occur.

VICI Swiss Competitive Intelligence SA is a Swiss cyber intelligence and cyber protection agency that offers you the most advanced means of digital forensics in the world, to preserve your data, your know-how and your market shares.

4%

SURFACE WEB

Public Internet, accessible by search engines: Google, YouTube, Facebook, etc.



90%

DEEP WEB

Private databases, intranets, scientific studies, academic information, etc.

6%

DARK WEB

Data not accessible by traditional browsers, encrypted communications, illegal information and activities.

If the dark web, the deep web or the surface web is talking about you, you will know it thanks to VICI and have the means to protect yourself.

Cyberattack protection radar

The best defense against cyberattacks is anticipation.

Our Operational Cyberattack Control Center (OCCC) constantly monitors mentions of you or your business, from the deepest layers of the dark web to the surface web and in all languages. OCCC specialists then analyze these mentions, their frequency, their relevance and determine the threat they represent. If the danger is confirmed, we trigger an emergency procedure by immediately informing you of the measures to be implemented and the flaws to be rectified.

Are hackers talking about you or your company?

VICI's teams monitor the number of mentions of your business on the dark web. The more your company name or domain name is mentioned, the greater the risk level of cyberattack.

Have your employees' email addresses and passwords been compromised?

VICI's teams list and inform you about the various personal data leaks involving your company or your employees.

Do you have connected objects within your company?

Information that passes through printers, cameras or connected watches can end up accessible on the dark web. This gives hackers more entry points to penetrate your digital network.

Operational intelligence

"He who holds the information, holds the power."

Our analysts search the entire Internet, mainly the deep and dark web, to collect useful data about your market (competitors, prices, etc.) that will allow you to be very responsive and to take the best decisions for your business.

We also operate inside your structure, counter-attacking any entity that has infiltrated due to a hack or human error (counter-intelligence).

Operational intelligence
(outside your organization)

To retrieve the data that will be useful to your business, our analysts search the entire Internet: mainly the dark web and the deep web. This is where hackers communicate and malicious acts are prepared, where the most sensitive strategic and operational information about your markets and your competitors is exchanged, and where the sale and exchange of products related to your intellectual property is negotiated.

Even if it is "too late" once your data is for sale in the dark web, it's essential for you to be aware of that in order to take appropriate actions.

Operational counter-intelligence
(within your organization)

Counter-intelligence consists of opposing the action of an entity that has infiltrated your information system, due to willful malice within your organization or human error such as employee phishing.

We first conduct an audit of your computer security to identify the vulnerabilities that allow the leakage of your data: human error, corruption of an employee or hack of a connected machine (computers and smartphones of course but also printers, cameras, etc.). We then move on to the counter-intelligence phase, in particular by broadcasting false information to your attacker to create deception, so that you can no longer be harmed and that you never lose the initiative.

Strategic intelligence

The best trade route for your business.

Our experts in cyber intelligence and augmented AI collect and cross-reference strategic data that will allow you to define the best policy for your company and to guide it on the best commercial path in the medium and long term, by anticipating its threats, strengths, weaknesses and opportunities without any limits of language, geographical areas and sovereign borders.

IT security audit

Why carry out a security audit?

Whether internal company risks (malicious acts, espionage, lack of employee awareness, errors, incidents, etc.) or external risks (viruses, intrusions, data theft, phishing, etc.), the security of your information system is essential for the smooth running of your organization.

Our experts conduct a complete audit of your system to determine its overall level of security and to review the access policy for your data and your network. We list the weak points and especially the vulnerabilities, then draw up a list of recommendations to remove these vulnerabilities and implement protection and security policies adapted to the functioning of your organization.

External security audit

Our experts put themselves in the shoes of an intruder and try, by all possible means, to break into the desired platform. They try to compromise the system by looking for vulnerabilities in it, the same way a hacker might. They then use these flaws to infiltrate as much as they can, if possible until they obtain sensitive data or take total control of your system.

Our analysts document their actions as they go and can then provide you with a detailed report explaining how they managed to find and exploit your external vulnerabilities. This information is accompanied by recommendations for corrective actions to be implemented in order to fill these gaps. We are also available to assist you in implementing the recommended corrective actions.

Internal security audit

The internal security audit involves placing an auditor directly on your network. Connected as an employee, guest, or anyone with legitimate access to your company's network, our expert attacks services, endpoints, and your other computing resources. This procedure makes it possible to effectively measure the risk in the event of physical compromise of your network, infection of an endpoint or attack by a member of your company (industrial espionage, malicious intent, etc.).

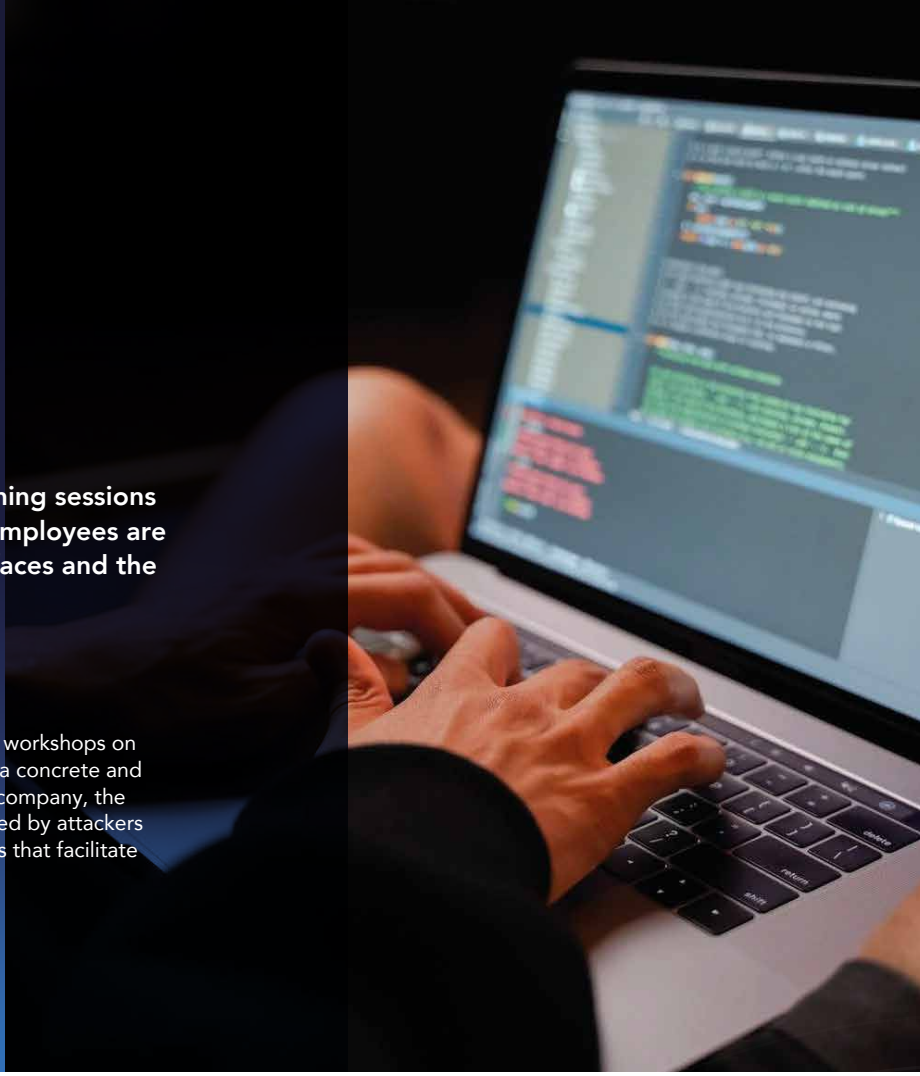
Of course, our experts do not exploit the flaws they find on your systems outside the context of this intrusion test, and do not keep the data that they could possibly have recovered. All the data collected is returned to you at the same time as the final report, and these two elements, strictly confidential, are only shared between the audit stakeholders.

VICI

VICI Swiss Competitive Intelligence SA

Avenue de la Gare 17
1003 Lausanne

(+41) 21 311 29 42
contact@vici-agency.com



Cyber threat awareness

Our teams offer you awareness and training sessions on cyber threats, so that you and your employees are better aware of the risks your business faces and the best practices to implement.

Cyber threat awareness workshops

We organize in your company an awareness-training workshops on cyber threats for your colleagues and employees. In a concrete and practical way, we address the risks incurred by your company, the types of attacks that can target you, the methods used by attackers so that you can better detect them, the internal flaws that facilitate hacking, and finally the solutions to these flaws.

Digital extraction

We collect all data - including deleted data - on devices such as smartphones, computers, tablets, photocopiers, drones, etc. that is useful in the context of investigations or legal inquiries. Our expert is a Certified Forensic Analyst for the admissibility of files with the appropriate authorities.

Find the evidence you need

We analyze the content of the devices concerned to allow you to move forward with your procedures or after the departure of a former employee who has left their professional devices, and we extract all the data.

Types of data collected from devices

- Geolocations
- Photos received or taken
- WhatsApp messages, SMS
- Emails
- Contact numbers
- Etc.

Judicial admissibility

For an employee or former employee with company-owned business devices, digital extraction is legal and permitted.

For private legal matters, supervised by a lawyer, prior judicial authorization is required. The file provided with the extracted elements will be admissible before a judicial authority.

A team of experts at the service of your cybersecurity

For you we stand guard in the depth of the dark web, where the action takes place.

Daniel Donnet-Monay, CEO

A team of specialists ensures your online security

After having supported individuals and business leaders for more than 20 years with the fiduciary company "At All Global Services SA" (AAGS SA), Daniel Donnet-Monay - Lieutenant-Colonel in the Swiss army - has grasped the current challenges of digitization, online influence and the vulnerability of information systems.

His military and professional experience naturally led him to found VICI Swiss Competitive Intelligence in 2019, a Swiss cyber intelligence agency enabling individuals and companies to benefit from some of the most advanced means of protection, investigation and influence available.

The technological tools as well as the various fields of expertise of the specialists and military members of VICI Swiss Competitive Intelligence make it possible to provide a complete analysis and realistic solutions adapted to each problem.

Comprehensive expertise at your service

Computer science

- Expert in cybersecurity (Federal diploma IT Cybersecurity)
- Systems and network engineer (Federal diploma)
- Information system architect
- Expert in project management assistance
- Expert in virtualization, mathematics, expert in coding and code review
- Developer (Federal diploma)
- Data Mining Analyst
- Expert in cryptology and encryption
- Forensic Analyst

Military

- Lieutenant-Colonel (battalions, Special Forces)
- High-level military executives (army staff, logistics, leadership)

Business intelligence

- Information science experts
- Strategic watch (sectoral, competitive, technological, normative, etc.)
- OSINT, HUMINT and CYBINT investigations
- Study of competing networks
- Know Your Customer (KYC) and Enhanced Due Diligence (EDD) reports
- Competitive analysis, benchmark, and market study

VICI
Swiss Intelligence Services

VICI Swiss Competitive Intelligence SA

Avenue de la Gare 17
1003 Lausanne

(+41) 21 311 29 42
contact@vici-agency.com