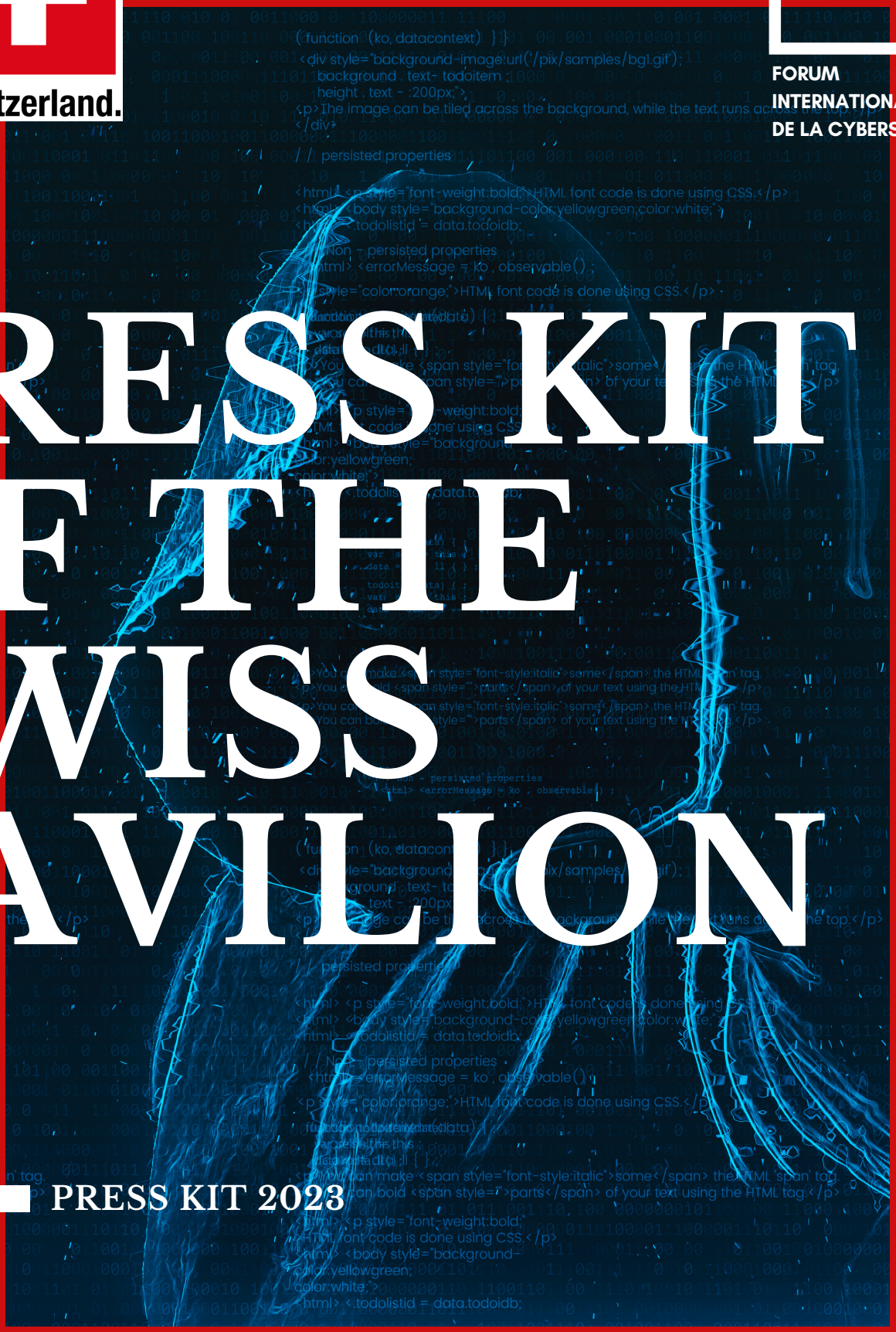
Switzerland.

FIC

FORUM
INTERNATIONAL
DE LA CYBERSÉCURITÉ

PRESS KIT OF THE SWISS PAVILION



PRESS KIT 2023

ELCA SECURITY - EXOSCALE - PRODAFT -
QR CRYPTO - SAPORO - SHAREKEY - STARBOARD
ADVISORY- TUNE INSIGHT - UBCOM

TABLE OF CONTENTS

INTRODUCTION

Cybersecurity in Switzerland: a dynamic and efficient ecosystem

With its reputation for quality and innovation, Switzerland also expresses its know-how in the digital field. Its strong points are: methodology, pragmatism, and its internationally renowned "Swiss made" label.

Recently, some successful cyberattacks have been relayed by the media and served as an electric shock.

In Switzerland, as elsewhere in the world, the growth of cybercrime is strong. The reality of cyberattacks is far greater than the reported incidents.

All the States have organized themselves and Switzerland as well: the National Center for Cybersecurity (NCSC), created in 2019 and transformed into a federal office in 2022, will be attached this year to the Federal Department of Defence, Protection of population and sports (DDPS).

The NCSC is the reporting point for cyberattacks, mandatory for critical infrastructures. It reviews incidents and gives an assessment and recommendations. It collaborates with the cantons, municipalities, economic and scientific circles, society and international partners, and encourages the exchange of information.

Switzerland also exerts influence in the field of international Internet governance, cooperation in the field of security in cyberspace. Florian Schütz, federal delegate for cybersecurity since August 2019, was also appointed, in January 2022, chairman of the working group on security in the digital economy (SEN) of the OECD.

Switzerland has assets in the field of cybersecurity: its neutrality, its confidentiality, its security. Cantonal and academic initiatives help develop innovation and a high-performance ecosystem in the cybersecurity sector.

As the Swiss economy is liberal, Swiss companies operate in a less restrictive world, focused on business more than compliance. It is up to companies to take charge of their security. Nevertheless, the implementation of regulations (LPD for example, close to the GDPR) is necessary for international trade, and lead to the establishment of standards.

Digital sovereignty, which is one of the pillars of cybersecurity, has been the subject of numerous debates, in particular when the Swiss Confederation chose, in 2021, five Internet giants to provide cloud services: four Americans (Amazon, IBM, Microsoft and Oracle) and Chinese Alibaba. However, in 2022, the Confederation indicates that it will create an independent digital infrastructure, including cloud services. Objective: to guarantee the highest possible level of security for particularly sensitive personal data. They must be inviolable and subject to Swiss law.

In an interview with the Swiss newspaper Le Temps on December 13, 2022, Cédric Moret, CEO of Elca, said "it is commonly accepted that Switzerland has one of the best rail networks in the world, one of the densest and best organized. In the digital domain, Switzerland is at a similar turning point: the establishment of digital infrastructures can only be achieved through an ambitious partnership between the public authorities and private high-tech companies".

Many Swiss companies have developed in all IT and IT security professions: **Elca Security, Exoscale, Prodaft, QRCrypto, Saporo, Senthorus, Sharekey, Starboard Advisory, Tune Insight, UBCOM, exhibitors at the Swiss Pavilion, at FIC Europe 2023!**

Marie de Freminville
marie.defreminville@starboard-advisory.com
+41 76 537 89 86
www.starboard-advisory.com

Starboard Advisory
› GOUVERNANCE › CYBERPERFORMANCE › FINANCE

ELCASecurity

How to transition to a Modern Security Operations Center (SOC)?

With the growing in cyber-attacks, all organizations are forced to realize the importance to have a centralized Security Operation Center (SOC).

Interview with Fabrice Guye – General Manager Senthorus

Gartner made the assumptions in their SOC Model Guide published on 19th Oct 2021 that:

- By 2025, 90% of SOCs in the Forbes Global 2000 will use a hybrid model by outsourcing at least 50% of the operational workload.
- By 2025, 33% of organizations that currently have internal security functions will attempt and fail to build an effective internal SOC due to resource constraints, such as lack of budget, expertise and staffing.

ELCA sees the trend that more and more organizations are looking to outsource the SOC services to an MSSP (Managed Security Services Provider).
What are the important best practices for a modern SOC and how to choose a provider accordingly?

- **Operating and Engagement model:** Define the SOC operating model based on your organization's requirements, Current SOC State and Future Objective & Roadmap.
  We need a provider with compatible engagement model. A hybrid engagement model allows more flexibility and more effective collaboration, but harder to manage as well.
- **Sustainable and effective processes:** It is important to continuously improve your processes and tailor them to fit your needs.
  You need support from your provider to be transparent, flexible beyond a standardized engagement process.
- **Technology & capabilities:** SOCs face complex challenges. Technologies and capabilities for detection and response to threats set the foundation for the SOC. Automation and Treat Intelligence make your SOC future-proof.
  You need a provider who is familiar with the available technologies and can select best offering for your defense.
- **Services:** 24x7 capabilities are required to build and manage the SOC as well as continuous improvement of processes and service components to cope with the threat landscape constantly evolving.
  You need a provider who can provide setup and integration efficiency. Always define SLAs and communication processes clearly with your provider.
- **Data sovereignty:** Keep the control on the sensitive data is a key topic and therefore having a MSSP provider provide its customer with full control, ownership and admin rights on his data is a must.

Not only you need to avoid vendor locking mechanisms but more over you need a partner who provide the necessary transparency.

To support our customer, ELCA has created a new dedicated entity named: Senthorus.

The company provides a wide range of managed security services through state-of-the-art Swiss-based SOCs. We can be your 24x7 SOC provider and help you to improve your security processes.

ELCASecurity

From Appenzell to Ticino and Jura to Vaud, RAILplus covers the metre-gauge railways of the whole of Switzerland.

In an environment where cyber crises are increasingly common and can affect all economic actors, RAILplus has drawn on ELCA's experience to conduct crisis exercises among its members.

Since late summer 2022, the experts of the RAILplus cyber security competence centre have been visiting each of its members to conduct a cyber crisis exercise. The aim is to test processes that are rarely used by railway companies in half a day. The participants used all their energy during the exercises to use their skills to involve and coordinate the different teams and to train decision-making in times of crisis to limit the damage that the attack would have caused to their company.

The main lessons learnt from all RAILplus members who carried out this exercise are undoubtedly an assessment of their preparedness for a cyber crisis and how well interdepartmental communication works. A greater interest among participants in topics related to cyber security was achieved. The advice given by the experts after the exercises helps members to strengthen their ability to deal with such events and to be better prepared for a possible serious incident.

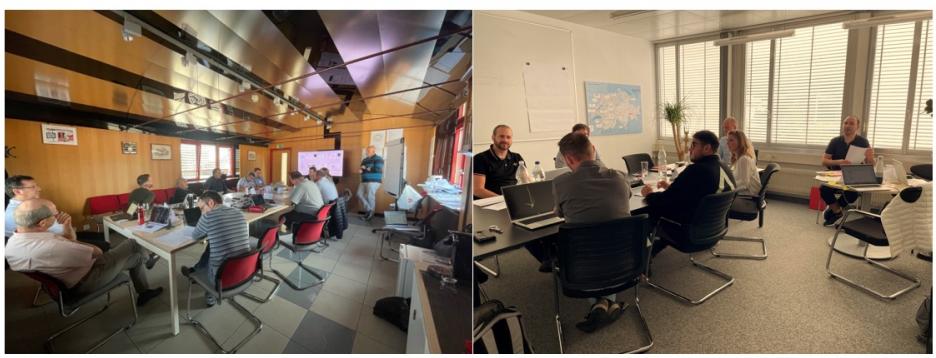
The usefulness and necessity of this exercise was given by the participants in the form of feedback to the ELCA experts. Here are two examples:

"A very instructive exercise for the entire crisis team. After the Covid crisis and the energy crisis, it was natural for TRAVYS to test our ability to deal with a cyber attack"

Daniel Reymond, Director of TRAVYS

"This exercise allowed us to test our processes and communication in the face of a realistic cyber crisis scenario. All participants learned a lot from this exercise, which led to an instructive exchange between the departments"

Ralf Rechsteiner, IT Manager at Appenzell Railways



TRAVYS, Yverdon **Appenzell Railways, Herisau**

Crisis teams gathered to deal with a cyber attack on their organisation

ELCASecurity

About Elca Security :

ELCA Security is a team of experienced cybersecurity experts at your service to help you understand cybersecurity and support you in your approach to information security. With 15+ years of expertise, several key solution partners and hundreds of cybersecurity projects performed, we offer assistance from advisory, consulting, solution development, integration and managed services. Our mission statement is to serve any company or public organization when it comes to anticipation, protection, detection and defense. ELCA Security is a subsidiary of the ELCA Group based in Switzerland.

www.elcasecurity.ch - @ElcaSecurity on Linkedin

Press contact :
Stéphane Clerc
+41 21 613 22 58
+41 79 621 05 65

EXOSCALE

Arrow Electronics adds Exoscale's cloud services to ArrowSphere platform

Agreement broadens European data sovereignty channel partner offer on ArrowSphere across Germany, Austria, and Switzerland

ArrowSphere helps channel partners to manage, differentiate and scale their cloud business. Its marketplace includes all the leading hyperscale providers, as well as public and private IaaS, PaaS, SaaS and cloud software offerings. The platform provides end-to-end cloud lifecycle management with features like automated provisioning, comprehensive billing integration, reporting and predictive analytics.

ArrowSphere also offers integrated DevOps and customisable storefronts that enable end customers to manage their own transactions. With a footprint of data centerslocated across Europe, Swiss-based Exoscale delivers highly secure cloud services, which are compliant with many security frameworks such as Swiss FINMA (Finance), HIPAA (Health), TISAX (Automotive), organizations with particular obligations around data sovereignty.

Exoscale's pay-per-use core cloud services include compute, storage, and networking. Its portfolio also covers managed and scalable Kubernetes, and database as a service (DBaaS) engines such as MySQL, PostgreSQL, Redis ®, and OpenSearch.

Exoscale services are simple to access with a user-friendly interface which reduces the risk of misconfiguration and security vulnerabilities, and benefit from transparent and predictable pricing.

Alexis Brabant, vice president sales of Arrow's enterprise computing solutions business in EMEA said, "Our channel partners seek out well-supported cloud solutions for their customers that are simple to access, manage, and scale. This agreement helps ensure even greater depth and breadth of European-based cloud services for channel partners with end-customers who depend on data sovereignty for GDPR compliance.

Mathias Nöbauer, CEO of Exoscale, said, "At Exoscale we are providing state-of-the-art infrastructure and services to help teams build and run modern, cloud native applications - simple, scalable and safe. This agreement will allow us to extend our reach and benefit from the extensive experience and local knowledge of the Arrow teams in their countries. It helps us to cement our presence as a European cloud provider across the EMEA region, and caters to the needs of those who value European sovereignty and European data privacy legislation."

ArrowSphere helps channel partners to manage, differentiate and scale their cloud business. Its marketplace includes all the leading hyperscale providers, as well as public and private IaaS, PaaS, SaaS and cloud software offerings. The platform provides end-to-end cloud lifecycle management with features like automated provisioning, comprehensive billing integration, reporting and predictive analytics. ArrowSphere also offers integrated DevOps and customisable storefronts that enable end customers to manage their own transactions.

About Arrow Electronics

Arrow Electronics guides innovation forward for over 220,000 leading technology manufacturers and service providers. With 2021 sales of $34 billion, Arrow develops technology solutions that improve business and daily life. Learn more at fiveyearsout.com.

EXOSCALE

About Exoscale :

Simple interfaces, secure infrastructure, scalable cloud services. At Exoscale we aspire to help businesses and engineers to run their workloads and applications securely in the cloud. With a focus on building an easy-to-use, reliable and performant cloud platform Exoscale is the trustworthy, privacy-minded partner for cloud-native applications.
Start virtual machines, managed databases, or Kubernetes clusters in just a few clicks, store petabytes of data and easily integrate your on-premises or multi-cloud deployment taking advantage of the most common DevOps tools. Our simple and intuitive interfaces make powerful concepts easy to use for teams of any size.
We commit to take a stand for our core values of security and privacy by adhering to global and local security frameworks and certifications from the world's most stringent auditors. This allows Exoscale customers a smooth and safe adoption of our cloud platform.

www.exoscale.com - @Exoscale on Linkedin and Twitter

Press contact :
Barbara Labes
barbara.labes@exoscale.com
Sabrina Spilka
sabrina.spilka@exoscale.com

Thorough reporting on cybercriminals' operations

PRODAFT is a leading cyber security company that has been challenging the conventional approach to cyber intelligence since 2012. By providing a cyber threat intelligence platform that prevents and mitigates substantial cyber-attacks before they happen - rather than dealing with the harmful consequences - PRODAFT places its proactive and intelligence-led solution into the spotlight.

The necessity of timely insights and intervention

Nowadays, all organizations should realize the importance of up-to-date and efficient cybersecurity measures to ensure their operations are running smoothly and without extra risks. If they fail to recognize the need to do so, they can face major financial or reputational losses. With the rise of more malicious threat actors, opting for basic protection measures such as firewalls, network or other security measures is not sufficient. Those solutions cannot recognize the threat lurking at the source – namely the schemes and vicious plans taking place in the deep and dark net, underground forums or hacking chats. Cybercrime efforts have been evolving steadily over time, and with some threat groups operating RaaS or MaaS servers, in addition to phishing, malvertising, zero-day exploits, state-sponsored attacks and other dangerous campaigns, businesses find it increasingly difficult to keep themselves protected. Whether it is the lack of human resources, technology, or just mere underestimation of the cybercriminal tactics, organizations fall prey to those attacks in a matter of minutes. The aftermath of such attacks can be enormously detrimental for any business entity.

Thorough understanding of the cybercriminal infrastructures

Understanding the vulnerabilities and consequences that can be faced by the organizations if they fail to protect themselves well in advance, we realized the importance of revealing and sharing all detailed information about the APTs and their future moves. That is why we periodically publish reports on current cyber threat groups that are relevant for both the public and law enforcement entities. In our reports, we focus on providing a thorough overview of the adversaries that cuts through the noise: their hierarchical organizations, affiliations, internal structures, attack vectors, targeting, motivations and other operational details. Thanks to our all-around-the-clock PTI (PRODAFT Threat Intelligence) team, we managed to successfully prevent thousands of ransomware incidents. If you wish to read our reports (regarding threat actors such as WizardSpider, Silver Fish, Ghostwriter, PYSA, Conti or the ill-famous powerhouse FIN7), you can download them for free on our website: https://www.prodaft.com/resources/latest-reports. Our reports have been featured in various media (Bloomberg, ZDNet, The Hacker News, Bleeping Computer, among others) to inform the international community and spread awareness about the adversaries. We realize that an environment focused on education, intelligence, and proper understanding of the threat actors' activities is essential for the successful mitigation of cybercrime endeavours.

A unified cyber security solution

It is no surprise that cybercrime, especially viciously calculated supply chain attacks, are growing exponentially. In most cases, companies need to have way more advanced solutions to be able to successfully mitigate those threats. Realizing the importance of timely protection, we decided to embed our vision in our name – PRODAFT stands as an acronym for Proactive Defense Against Future Threats. With this commitment in mind, we carefully developed our main service – U.S.T.A.

A Unified Cyber Threat Intelligence Platform

U.S.T.A. is one of the first cyber threat intelligence platforms ever developed. For over a decade, U.S.T.A. has been a trusted partner of hundreds of organizations with its unmatched capabilities. Standing for **U**nified **S**ystem **T**hreat **A**nalysis, the platform is unique in its ability to deliver intelligence-led data that are customized and relevant for each customer and their respective verticals. Various detection mechanisms and intelligence collection tools, reinforced by HUMINT and real-time investigation by security analysts, were created to ensure that any persistent threats are handled accordingly. Not only a proactive approach but also actionable, timely, and verified insights make the U.S.T.A. platform a key player in preventing data breaches and detrimental cyber-attacks.

Various mechanisms to monitor suspicious activities

To meet the challenges of complex cyberattacks, U.S.T.A. is reinforced with dozens of intelligence collection tools that monitor thousands of sources. The platform monitors different aspects and areas of various deep and dark web, hacking forums, black markets, communication, and open-source platforms to observe these constantly changing landscapes better. To remain undetected among these communities of threat actors, our team members have developed personas that have been active on these channels for years.

The platform provides comprehensive data outputs for its users through four main modules:

1) *Tactical intelligence* – includes custom threat reports that feature incidents or trends that affect the member specifically, depending on its industry or region

2) *Security Intelligence* – includes custom malware analysis reports, vulnerability notifications, leak database and stolen corporate credentials notifications

3) *Fraud intelligence* – includes stolen credit card and fraud method notifications, stolen ID and passport feeds and stolen customer credential notifications

4) *Brand protection* – includes phishing site detection & takedown and suspicious/ malicious social media content detection & takedown

Some of the aforementioned features are autonomous, while others require an analyst's interception – depending on the complexity of the case. The platform does not require any on-site installation or configuration. It works as a web-based platform that does not need to conduct any vulnerability assessment or active footprinting procedure of the systems to acquire information. If you feel that your organization would benefit from this product, feel free to request a demo through our website https://www.prodaft.com/usta-trial-access.

Knowledge sharing & collaboration opportunities

Although we always look beyond borders and our operational offices are already scattered across the globe, we had a clear vision of scaling up further in the European market. With this plan in mind, we successfully expanded our operations and opened another office in the Netherlands (den Haag) at the beginning of last year.

Cybersecurity conferences on the most pressing issues

As not only the Dutch market but also the European region present intriguing opportunities to grow our cybersecurity efforts, we realized the importance of sharing our expertise with relevant parties. That is why at the end of January 2023, we hosted our first event in the Netherlands, inviting both private companies and public & law enforcement authorities. Focused on the evolution of organized cybercrime and the infostealer industry, we shed light on the history and transformation of the cyber-security sphere over the years and some of the most important, globally relevant cyber-security issues. On top of that, we centred our attention on the implications those issues have on Dutch cyber resilience. Our speakers emphasized the recent increase in threat actors' targeting of the European region and their overwhelmingly large pool of financial and technological resources. Many of the threat groups operate like corporate entities, with the ability to collect enormous amounts of victim data – and in this sense overperform the data-gathering capabilities of legally operating organizations. What's more, due to the gaining popularity of dark markets and ransomware servers, cybercriminals can exploit their victims with less effort and fewer risk factors, turning this illicit field into an appealing one. Due to those realities, we at PRODAFT find it essential to share our knowledge and expertise through various seminars, conferences, and our upcoming webinars.

Interested in a collaboration?

Since we are not planning to slow down our development, we continue providing insights into the constantly changing cybersecurity landscape and the challenges within. We are planning to organize even more events in the future, both individually and together with our partners. As such, we are always on the lookout for competent and passionate partners, whether from the public, private or academic sphere. Working together on the remediation steps, helping the victims on the ground, or just expanding the R&D practices, we are continuously looking for new collaborating opportunities. Do you think we could benefit from joining our resources or data sets? Do you have great ideas about a project that could contribute to our cybersecurity efforts and lead to prolific outcomes? Talk to us or reach out to info@prodaft.com to share your thoughts!

About Prodaft :

PRODAFT is a leading cyber threat intelligence company founded in 2012. For over a decade, we have been focusing on a proactive approach to cyber security by intercepting and mitigating threats before they happen. Accordingly, the company vision is embedded in our name – PRODAFT is an acronym for Proactive Defense Against Future threats. Our mission is to keep citizens, businesses, and governments safe from any major security threats by providing timely, accurate, actionable information.

https://www.prodaft.com/- @PRODAFT on Linkedin and Twitter

Press contact :
Viktoria Vargová
media@prodaft.com
+41 76 801 07 51

QUANTUM RESISTANT CRYPTOGRAPHY

Quantum Resistant Cryptography (QRC) and Conteon Inc Make Retail Transaction Infrastructure Quantum Safe

Developing the quantum-safe infrastructure necessary to process retail transaction in real-time, without internet, eliminating the need for passwords and biometrics.

January 11, 2023 New York, New York - Quantum Resistant Cryptography (QRC) and Conteon Inc announced today they will partner to make financial transactions and user asset tokenization safe and secure. Combining Conteon's hybrid hardware architecture with QRC's advanced encryption algorithms safeguards against the interception of or the tampering with user financial transactions, now and in the post-quantum future.

Conteon's Ukrainian founders have invented an Emitter that becomes the bridge between DeFi and the classic Fintech infrastructure. The Conteon Emitter allows users to securely interact with payment or critical infrastructure using QR, Bluetooth, and NFC and without using passwords and active biometrics. The Emitter provides an API for the tokenization and/or sale of assets for both crypto and classic currency, as well as the creation of user-scoring certificates and operational tokens for interaction with classic financial instruments.

"QRC's patented quantum-resistant encryption algorithms significantly improve the security of Conteon for storing sensitive information in blockchain and transferring data over open 5G+ or on-orbit inter-communication ways such as StarLink that could be used in software solutions of Conteon Emitter," said Yurii Chudinov, Co-Founder and CTO of Conteon Inc.

"Conteon has created a unique bridge between DeFi and the classic Fintech infrastructure. Their Emitter eliminates passwords and active biometrics and allows users to interact with payment and critical infrastructure through interactive algorithmic-hardware protection using QR codes, Bluetooth and NFC," said Stiepan Kovac, Founder and CEO of QRC. "We are proud to partner with Conteon to make their innovative solution cryptographically safest and most secure today and in a post-quantum world."

Both Companies will work together to improve existing solutions and develop new ones in the quantum-safe infrastructure, practices, and extensions of NIST frameworks to provide benefits and secure operation environment to their clients.

About Conteon Inc

Conteon Inc is a crypto fintech company providing infrastructure to proceed cheap and secure to conduct P2P transactions and payments both by fiat and cryptocurrency. The Conteon develop unique hardware - The Conteon Emitter. It is a patent pending technology which performs hardware multi-signature for retail transactions and tokenization user assets of any type. Also, the Conteon Emitter includes unique algorithms that provides input data-based entropy generator for encryption algorithms

Media Contact for Conteon Inc: Sergii Demianenko / demian@conteon.io

QUANTUM RESISTANT CRYPTOGRAPHY

OrbitsEdge and Quantum Resistant Cryptography (QRC) Make Space Infrastructure Quantum Safe

OrbitsEdge and QRC are working together to deliver the quantum-safe in-orbit infrastructure necessary to process and analyze the vast amounts of data being created in space.

December 1, 2022, Cocoa Beach, Florida - OrbitsEdge and Quantum Resistant Cryptography (QRC) announced today they will be working to make datacenters in space quantum-safe. This will substantially increase computing power in orbit and reduce the bottlenecks of analyzing space data on Earth, protected by the safest and most secure quantum-resistant cryptography on the market today.

OrbitsEdge is dedicated to providing the infrastructure required for commercial off the shelf (COTS) computer hardware and software to survive the space environment. QRC will protect and secure the data for transmission, enabling quantum-resistant classical electronic payloads in space. The OrbitsEdge SatFrame™, with its cutting-edge radiation shielding and thermal management, has enabled inexpensive data-center-grade computers to survive the space environment. Integrating QRC's quantum-resistant algorithms means SatFrame components can withstand the threat of hacking by quantum computers in addition to the harsh physical environment of space.

"The advanced encryption that QRC provides ties in very well with on-orbit computation and high levels of storage," said Richard Ward, CTO and Founder of OrbitsEdge. "OrbitsEdge facilitates analysis above the transport layer and improves the overall quality of the data that is sent down to Earth. QRC Americas secures that data using its safest and most secure quantum-resistant cryptography."

"As leaders like General Paul M. Nakasone have said, the number-one defense against the quantum computing threat is to implement quantum-resistant cryptography on our most important systems," said Stiepan Kovac, CEO of QRC. "OrbitsEdge is revolutionizing space infrastructure by making traditional computer hardware useable in space. We are proud to be working with Orbits Edge to keep their data and communications safe both now and in the post-quantum future with QRC."

Today's method of shipping data back to terrestrial clouds is no longer practical. The OrbitsEdge & Quantum Resistant Cryptography partnership will provide faster and extremely secure web services solutions for earthbound companies to sustainably and cost effectively succeed in space.

About OrbitsEdge, Inc.

OrbitsEdge was established in 2019 to bring high powered Edge computer to the space environment. We deliver high-performance computing micro datacenters to orbit, with which to process and analyze the vast amounts of data being created in space. Our cornerstone infrastructure solution will substantially increase computing power in space and reduce the bottlenecks of space data on Earth.

Media Contact for OrbitsEdge: Siddarth Boyanapalli / sidd@orbitsedge.com

QUANTUM RESISTANT CRYPTOGRAPHY

About Quantum Resistant Cryptography (QRC) :

QRC provides simple, reliable, forward-thinking solutions that are energy-efficient, quantum-resistant, 5G/6G+ compatible and enable future-proof communications, public infrastructure, financial transactions, and private data protection. QRC's unique patented quantum-safe technology in 5G systems is the only solution recommended by the United Nations International Telecom Union (UN ITU-T). QRC runs on existing server infrastructure, so low CAPEX. Ransomware, custom cyber protection options and further post-quantum evolutions are also provided.

www.qrcrypto.ch - @qrcrypto on Linkedin

Press contacts:
(French/German/Spanish) Steipan Kovac
Stiepan@mailfence.com
(English) Christy Raedeke
Christy@qrcrypto.ch

SAPORO
ORDER IN CHAOS

Saporo clinches €4 million fundraise for its "anticipative" cybersecurity services

Using graph theory and artificial intelligence, Saporo aims to protect SMEs with predictive stress tests that identify potential cyber attack paths.

Lausanne-headquartered Saporo is announcing a pre-seed fundraise to the tune of €4 million to grow its cybersecurity offer with a focus on protecting healthcare, banking and insurance IT systems.

The round is led by Franco-German VC XAnge with participation from Session VC and Lightbird Ventures.

Saporo's cybersecurity software-led service is used by IT professionals to try out cyber defences against hypothetical attacks and adjust user account privileges automatically, reducing the scope for attackers to capitalise.

Once an organisation's attack surface has been probed, the Saporo platform builds data on the web of relationships that link computers, user accounts and assets to identify various entry points for attackers, using graph theory and artificial intelligence.

Cybersecurity professor Éric Blavier helped establish Saporo with the help of his fellow two co-founders, the siblings duo Olivier and Guillaume Eyries.

Their hard work paid off in January 2022 with the official product launch, and the company now wants to grab a market foothold serving SMEs with up to 30,000 employees.

With their platform, the Eyries have tried to bring some of the skillsets typically thought of as being specialised cybersecurity knowledge to a product that also works for general IT administrators and business application owners, who might lack in-depth expertise.

By broadening the knowledge pool, Saporo wants to reassure businesses they can keep IT protected and tackle the cybersecurity meltdown that's seen various critical systems dependent on IT and connectivity affected.

"Security cannot remain a security expert problem only," says Eyries, "We need to empower teams who build and make changes daily to consider the security impact of their decision and help them secure systems by design,"

Speaking on behalf of Lightbird Ventures, managing partner Benjamin Solenthaler said there were case studies of Saporo's solution where organisations had achieved an 80% reduction in their "internal attack surface".

Session VC founding partner Martin Altorfer added: "Today, too many issues seem to make the shortlist of priorities for most organizations.

"However, strengthening the defense is imperative, especially when situations and technology change daily.

"Saporo takes the hardest part of the job away, giving customers the data and recommendations to act now by prioritizing the risk. We believe this incredibly powerful solution will make a profound change in assessing risks."

https://tech.eu/2022/12/06/saporo/ - December 6th 2022

SAPORO
ORDER IN CHAOS

Tech4Trust Award Ceremony crowns Saporo

The winners of season 3 of theTech4Trust program were revealed at the awards ceremony held yesterday at the Swiss Cyber Security Days 2022. The final event of the Trust Valley accelerator program rewarded 3 startups in cybersecurity and digital trust chosen among 12 finalists. The winner is Saporo. Tune Insight & PRODAFT come 2nd and 3rd. Hestia receives the Social Impact Award from the Herbert & Audrey Rosenfield Foundation

It is on the main stage of the Swiss Cyber Security Days, after a highly anticipated keynote by US National Cyber Director Chris Inglis, that the three winners were distinguished. Chris Inglis' words, mentioning "resilience by design" and calling for collaboration through public-private partnerships and international cooperation, resonated strongly with the aspirations of the start-ups involved in the Tech4Trust program and more generally with the DNA of Trust Valley.

"We are proud to bring together strategic partners from the public, academic and corporate spheres to accelerate the resilience and security of digital systems through collaborative work, the promotion of talent and access to a fertile network of trusted investors," said Lennig Pedron, Trust Valley's executive director. "Strong Network, which won 2nd prize in Season 2 in March 2021, has just raised 5.2 million, a record for a seed."

Saporo, who won the 3rd edition of Tech4Trust, reflects these ambitions: based in Lausanne, but with 1/3 of its staff in the United States, the startup co-founded by Guillaume and Olivier Eyries and Eric Blavier enables organizations to model and measure their resistance to anticipate attacks and make better-informed decisions about managing their risk without the need to think like an attacker.

Prioritizing and reducing user and system access risks

Saporo's technology proactively stress-tests user and system access risks before attackers can exploit them. The product uses machine-learning driven analysis and graph theory to test an organization's attack surface, and the relationships between assets, users, and computers, against millions of threat scenarios.

The technology continuously and contextually quantifies the security impact and exploitability of systems configurations. Saporo can then measure how much effort would be required for attackers to compromise resources. This allows organizations to identify and prioritize paths that attackers could take in various attacks like ransomware.

Olivier Eyries, one of the three co-founders of Saporo, expresses his great satisfaction with the Trust Valley acceleration program: "Six months ago, we only had an idea and no fundraising, hardly any network. Six months later, we have raised 2.5 million, we have 7 clients in Switzerland and France, and 12 employees. Tech4Trust acts as a badge of trust that propels us and encourages investors to talk to us. We remain humbled and delighted with this result and will get right back to work.

The second prize goes to Tune Insight. Based at EPFL Innovation Park, the startup develops secure computing solutions for sensitive and confidential data. In third position comes PRODAFT. The Y-Parc based company offers proactive threat intelligence to its customers against the constantly evolving attack techniques in the cyber world. Last startup recognized with the Social Impact Award was Hestia. The Geneva company builds sustainable personal data pipelines, respectful of the data contributors and responsive to changing circumstances.

SAPORO
ORDER IN CHAOS

Two and a half years ago, this high economic impact initiative conceived by Trust Valley, supported by the Canton of Vaud, academic institutions such as EPFL and UNIL, and leading companies such as Kudelski, Elca, SGS, SICPA and the GCSP, aimed at promoting and connecting key players in digital trust and cybersecurity, came into being. Tech4Trust is the first digital trust and cybersecurity acceleration programme. The only one of its kind in the world, this signature Trust Valley programme helps the most promising companies prepare their business for commercialization through top-notch mentoring by captains of industry, strategic support and training from leading industry partners. (55 mentors, 26 coaches, +10 trainers, +20 speakers)

https://www.startupticker.ch/en/news/tech4trust-award-ceremony-crowns-saporo-
April 7th 2022

About Saporo :

Saporo's unique approach using graph theory helps companies build and maintain secure systems by design. To achieve these results, the product stress-tests user and system access risks. It uses graph theory and artificial intelligence analysis to test an organization's attack surface and the relationships between assets, users, and computers against millions of possible attack paths.

www.saporo.io - @Saporo on Linkedin

Press contact :
hello@saporo.io

Redefining C-Suite Communications Privacy

Suppose you are the CFO of a corporation who is preparing a presentation with sensitive financial data for the Board of Directors. Or you might be the Head of Human Resources planning to implement a staff reduction within specific departments whose affected employees have been identified. Or perhaps you are an Executive reaching out to a peer at another company to discuss a potential corporate transaction. You very likely need a collaboration tool to communicate with your team or other business contacts to exchange messages and documents whose content is highly confidential. You might even want to keep secret that you communicate with someone altogether. How can you be sure that your highly sensitive data and confidential communication remains *private*? And that no one has access to any information – whether an external agent, an intermediary, a service or infrastructure provider, or technical administrator – along the communication path?

It is easy to mix *security* with *privacy*. Several collaboration tools provide end-to-end security, by ensuring that the data communication pipes and storage are secured to prevent eavesdropping or alteration, and by encrypting the data itself some times. However, when you read their Terms of Service – something that actually no one really bothers to read before accepting and consenting – you are actually entrusting your Service Provider with your–login and password, with the tacit understanding that they will protect them and not access them for any other reason than logging in. Careful reading of such Terms of Service shows that no Service Provider commits that your data will never be accessed, nor can demonstrably prove that your data have not been misused. In reality some providers analyze your data to monetize it. They might have to disclose such data if requested by court order. Or data may be inadvertently leaked as a result of a data hack. Sharekey was conceived to tackle these limitations and risks, based on a vision of its two Founders – Hervé Blanc and Sauro Nicli.

Sharekey, the Swiss-based, privacy-focused collaboration platform provider they have created, is both *secure* and *private*. Accepting its Terms of Service requires Zero Trust in the collaboration platform itself and in any data service providers because the data and the encryption private keys used to protect them are owned by the end user and not revealed to anyone outside their devices. Encrypted data stored in Sharekey's cloud with your private key cannot be revealed because even Sharekey does not own the decryption keys. Sharekey end users choose what to share and with whom by exchanging shared keys – this "share keys" mechanism stands behind their company name.

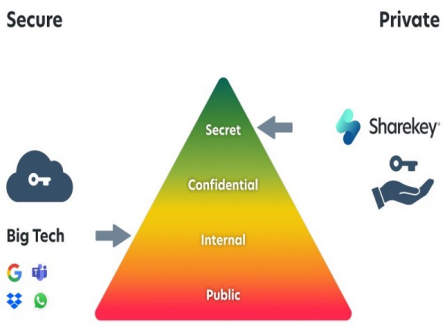
"All collaboration apps have access to your data. Sharekey proposes a true private collaboration application with the mission to guarantee business privacy with an app-to-app encrypted platform – based on Zero Trust," says Hervé Blanc, Founder & CEO of Sharekey.

Sharekey®

An All-in-One Privacy-centric App for Business Collaboration

Sharekey targets the C-suite – Corporate Executives, Board Members, Senior Managers and Legal, Administrative and Financial staff that support them – who need a private collaboration workspace that works both within and across enterprise boundaries, where privacy and secrecy of communication are absolute – for example, the terms and conditions of an acquisition where some stakeholders (e.g., lawyers, bankers, etc.) are outside the enterprise's security perimeter.

The adjacent graphic positions Sharekey versus other collaboration tools. It targets the top of the pyramid, where the number of users may be small, but where the need for maintaining secrecy and confidentiality of exchanges is paramount. Obviously Sharekey can also serve as an enterprise-wide internal collaboration tool, enabling individual and group communication, file and folder sharing, as well as identity and access management.



Sharekey combines Slack, Dropbox and Zoom functionalities into a single enterprise-grade collaboration tool, all-in-one, focusing on privacy, not just security. Sharekey can be installed on any device – iOS, Android, PC, Mac, Web and Linux – which means that it can readily fit any enterprise IT infrastructure without requiring any operational changes besides installation (and deinstallation, when an employee leaves).

How Sharekey differs from other collaboration tools

Many consumer-oriented collaboration solutions have found their way into the workplace and corporate boardrooms "by osmosis". Sharekey differs in one essential way – it is not just a way to ensure secure end-to-end communication. It provides app-to-app security *and* privacy. The end point for Sharekey is not the device on which the app resides, but the app itself. The private encryption key that is used to secure a communication channel never leaves the crypto wallet installed on the user's device so that no one has access to it. In a sense, it is like a secure pipeline – much like a VPN – between peer Sharekey apps. The devices, the networks and the cloud are blind to what is exchanged as well as between whom such exchanges are taking place.

Sharekey's app-to-app encrypted solution allows additional features that are not possible with most of the current collaboration tools. For instance, it isn't possible to have the same WhatsApp or Signal account on multiple mobile devices without losing the communications history on the second mobile device, nor is it easy to synchronise your Telegram secret chats across multiple devices. It can be done, but the process is cumbersome and requires the use of cloud services, with whom non-encrypted data need to be shared.

Sharekey is built to work seamlessly in a multi-device environment, because the data, even when stored on Sharekey's cloud servers – 1000 meters deep inside a Swiss mountain – remain encrypted with your key, which never, ever leaves your device. When you need to sync data with a new device, you simply log into your Sharekey app on that device and – voilà – the data is given access to and both devices will remain always synched. This is particularly helpful when new collaborators join a multi-party communication channel. With other collaboration apps, the previous exchanges might not be available to the new participant. This is not business friendly.

Sharekey can also serve as an emergency tool during cyber-attacks, when other communication and collaboration resources may be offline.

Unlike other collaboration platforms, Sharekey's code is open source, readily available for inspection and audit by security professionals.

When sharing keys to allow data sharing, Hervé Blanc points out that "With Sharekey, when you share confidential information, you have full control of your data. You own it because you encrypt it with your own key, and you control it because you can share it with access privileges with only those contacts you chose. Users can be Viewers, Editors or Administrators. You can make that choice."

Because users exchange keys only when they communicate and collaborate – never actual data –, your encrypted data is stored only once in the Sharekey cloud. Sharing data means "sharing the keys to allow access to the data". This feature becomes increasingly critical as energy consumption and sustainability come business concerns.

Sustainable, eco-resilient app

Sharekey has designed its solution to be eco-resilient. Its data centers run on renewable energy and its sharing protocols are "green by design." For instance, when sharing files and folders, only the lightweight encryption key – the "shared key" – is exchanged, which allows the recipient to decide if data should be downloaded or not, avoiding unnecessary file transfers. This is especially efficient in large multi-party collaboration.

No data analytics can be conducted, as all data is encrypted. Sharekey's cloud cannot aggregate nor process metadata, nor install tracking analytics, avoiding additional energy consumption. In our current climate, every little bit helps to minimize the negative impact of IT operations on the environment while reducing costs overall.

Under Swiss Privacy Laws, not the CLOUD Act

As a Swiss-registered company and with its infrastructure entirely in Switzerland (including its highly secure data storage and network access guaranteed by Exoscale), all user data stored by Sharekey is protected by one of the strongest privacy laws available in the world – the Swiss Federal Data Protection Act, unlike the Cloud Act that US-based cloud providers are subjected to. Only a court order issued by a Swiss judge can cause the data to be retrieved, but even so the data is not exposed! After all, Sharekey does not hold the decryption keys, which reside in the crypto wallets of its users.

What's coming next?

Sharekey currently supports multimedia communication (chats, datarooms, voice calls, video conferencing), encrypted storage, role-based data sharing and multi-device synchronization. Next year, Sharekey will become the first application to offer true app-to-app encrypted Online Collaboration with the ability to view and edit multiple file types simultaneously among various users. Another feature – called "Pin to Blockchain" – will offer the ability to record electronic signatures on a blockchain.

Awards & Prestigious Clients

Sharekey has garnered a lot of industry attention. Recently Sharekey received the Public Award at the PwC Cyber Security & Privacy Day in Luxembourg and the Gold Medal for Innovation at the IT Night 2022 in Paris. During 2021, the company received several awards (Swisscom Startup Challenge, VentureLab Leaders, Top 10 Swiss Cybersecurity Startups 2021) that greatly increased its visibility, especially in Switzerland. These awards prove the innovation of this application.

Recently one of the largest insurance companies in the world has implemented its solution as a way for its top management to collaborate privately on sensitive matters.

Sharekey is becoming a trusted Partner for large corporations and business elites to manage their communication and data sharing with all external stakeholders in a highly secure, private and green manner. This is ushering in a new era of private data sharing collaboration.

CIO Review Europe
December 2022
SHAREKEY selected among the Top 10 Collaboration Solutions Companies in 2022
https://www.cioreviewеurope.com/sharekey

SHAREKEY Swiss awarded the Gold Medal for the Most Innovative Solution

We are thrilled to share that SHAREKEY Swiss AG has been recognised as the Most Innovative Solution at the IT Night 2022 in Paris! 🥇
We are one step closer to our goal to secure Business Privacy across Europe 🔐
Big thanks goes to our team for all your hard work & passion. Without you this would have not been possible.
Thank you to the Jury for choosing us among 80+ amazing companies.
Last but not least, big applause to the entire organisation of REPUBLIK IT for organising such a great event.

See you soon at #CYBERNIGHT 🚀
Let's keep delivering on our promise!

IT NIGHT 2022 - Paris, May 2022

SHAREKEY Swiss AG received the People's Choice Award

SHAREKEY Swiss AG received the People's Choice Award 🏆
at the PwC Luxembourg Cybersecurity & Privacy Day 🇱🇺
We are deeply honoured to receive this Award.
👍 THANK YOU to All Participants for your vote 🗳️
👏 Big applause to PwC Luxembourg, Koen Maris for his amazing Leadership, the Cybersecurity & Privacy, Marketing & Event Teams for organising such a great event.
👌 Big thanks also goes to our Team for all the hard work & passion invested in our app.
It was a true pleasure to interact with Clients & Partners and have meaningful discussions.
As announced during the event, we are also very proud to be represented & distributed by UBCOM in Luxembourg 🇱🇺 and in various European Countries.
We are one step closer to our mission
👉 Secure Business Privacy across Europe 🔐

PwC Cybersecurity & Privacy Day - Luxembourg, October 2022

About Sharekey :

SHAREKEY is a new collaborative application, based in Switzerland, all-in-one (messaging, drive, call, video conferencing, online collaboration, calendar, notes...), easy to use, designed to secure Business Privacy. Created by Executives for Executives, SHAREKEY is the solution for Decision Makers, Board Members, Legal & Finance. Built in a crypto wallet, SHAREKEY is a collaborative suite encrypted app-to-app. It simplifies the sharing of confidential information, both inside & outside an organisation, on any device.

www.sharekey.com - @Sharekey on Linkedin

Press contact :
Hervé BLANC
+41 76 226 7600 - herve.blanc@sharekey.com

TUNE INSIGHT

Strengthening collective cyber resilience

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

armasuisse
Science and technology

TUNE INSIGHT

The constant increase in cyber threats requires new solutions. Therefore, the Cyber-Defence Campus, armasuisse Science and Technology, is working with the EPFL spin-off Tune Insight to test its secure threat intelligence sharing software. The collaboration with Tune Insight develops and investigates novel solutions for the secure exchange of cyber threat data. This shall enable Swiss organizations, such as critical infrastructures within the health or other sectors, to collectively improve their defences against malicious cyber attacks.

As the number of cyber attacks increases dramatically, defence systems lose effectiveness if they do not have access to an updated and comprehensive knowledge base. Such data can be used to determine the patterns of new incidents and train advanced models that can predict and detect them. Current efforts for sharing threat intelligence data (e.g the Malware Information Sharing Platform, MISP, or OpenCTI) work on a centralized (replicated) database, where all participating organizations have to share their threat data.

Cybersecurity information is highly sensitive and confidential. This creates tension between the benefits of improved threat-response capabilities and the drawbacks of disclosing critical information to others. This usually results in patterns where people are reluctant to share relevant information due to the free-rider problem: while some parties disclose information by sharing, others avoid sharing anything and only benefit from third parties. This considerably limits the efficacy of data sharing. Tune Insight's software resolves this trade-off when sharing cybersecurity information. It enables the participants to collaborate using even critical and valuable cybersecurity information without having to transfer or disclose details to each other. This allows participants to extract valuable insights and build machine-learning models on larger and more relevant collective threat intelligence data and thus enables stronger defence.

Armasuisse Science and Technology collaboratively deploys and tests this new software solution together with Tune Insight, the University Hospital Zürich (USZ) and other critical health infrastructures.

Secure collective cyber intelligence and resilience is a critical capability of today's organizations, especially in the area of critical infrastructures. It is therefore essential to collaborate with various organizations through secure cyber threat data sharing to enhance threat-response capabilities.

Tune Insight announces pre-scale deployment in Swiss hospitals for precision oncology

Major milestone for Tune Insight in SPHN-funded project to facilitate oncology data collaboration amongst Swiss hospitals: production deployments in CHUV (Lausanne), HUG (Geneva) and USZ (Zürich).

In the context of a pilot project funded by the Swiss Personalized Health Network (SPHN), Tune Insight announces the deployment of its secure data collaboration software in production environments at CHUV | Lausanne university hospital, HUG - Hôpitaux (Geneva) and Universitätsspital Zürich.

Tune Insight's solution enables secure data collaborations between multiple organizations, without having to transfer or disclose sensitive or confidential data such as patient information to other participating organizations.

In collaboration with the Swiss Personalized Oncology (SPO) project and relying on Tune Insight software, hospitals will be able to generate personalized survival curves supported by data from multiple hospitals instead of only their own data.

This deployment involved a close technical cooperation to overcome the networking and operational challenges of the hospital environments, while complying with the highest security standards and the strictest data regulations.

Katrin Crameri, PhD, MPH, Director of the SPHN Data Coordination Center and SIB Swiss Institute of Bioinformatics' Personalized Health Informatics Group, highlights the importance of this milestone: "I am very happy with the progress so far. Production deployment in key hospitals is a major milestone that paves the way to cross-hospital collaboration for more personalized oncology, in alignment with SPHN's vision of harnessing health-related data for exploration and research purposes without compromising patient privacy."

TUNE INSIGHT

Open-source Multiparty Homomorphic Encryption Library Lattigo v4.1.0 is out!

Tune Insight announces the release of version 4.1.0 of Lattigo, its popular Multiparty Homomorphic Encryption open-source library. Lattigo is an open-source Go module that implements Ring-Learning-With-Errors-based homomorphic-encryption primitives and Multiparty-Homomorphic-Encryption-based secure protocols and offers equivalent performance to C++ libraries.

The library originated from a research project in 2019, actively developed by the EPFL laboratory for data security (LDS). It is acknowledged by the community as a state-of-the-art library for homomorphic encryption. Since the release of version 3 earlier in 2022, Lattigo has been supported and maintained by Tune Insight SA. The library supports Homomorphic Encryption in distributed systems and microservices architectures, for which Go is a common choice, thanks to its natural concurrency model and cross-platform portability. Notable features of the Lattigo library include:

- A low-level optimized polynomial-arithmetic package that can be used to implement any R-LWE based scheme.
- Optimized implementations of the full-RNS BFV, BGV, and CKKS schemes, as well as their respective multiparty versions.
- Advanced encrypted arithmetic, such as arbitrary linear-transformations, Look-up tables, homomorphic encoding/decoding, and vectorized polynomial evaluation.

Besides its functionalities, Lattigo has been described as "really convenient and research-friendly" by developers, making it a widely used library in academic research and prototyping all around the world. Lattigo is also one of the libraries acknowledged by the HomomorphicEncryption.org standardization group, it is one of the upcoming reference backends for HEBench, and it is part of the current draft Homomorphic Encryption standard. Lattigo is also listed on Amazon AWS Cryptographic Computing site, with C++ bindings available on AWS Labs GitHub; these bindings have been used to enable Lattigo as the underlying library for Amazon Web Services Homomorphic Implementors Toolkit.

Lattigo is also a yearly top contender in the iDash challenge, being regularly used by the winning teams. Tune Insight relies on Lattigo as the underlying cryptographic library that supports its secure data collaboration platform, enabling multiple organizations to collaborate securely on sensitive or confidential data, while remaining in full control of their data.

You can find more details about Lattigo at https://github.com/tuneinsight/lattigo

About Tune Insight :

Tune Insight is a Swiss B2B software startup that powers privacy-preserving collaborative analytics and federated machine learning on encrypted data, without ever moving or revealing raw data. We enable organizations to fulfill their need for data collaborations and valorization while overcoming regulatory hurdles and cyber risks.

https://tuneinsight.com - @Tuneinsight on Linkedin, Twitter and Youtube

Press contact :
contact@tuneinsight.com

UBCOM
CYBER PROTECTION & SOVEREIGNTY

« Europe is not prepared for Ukraine-related cyber warfare »

The repercussions of Russia's invasion of Ukraine are global, especially in the digital realm. To protect itself from cyberattacks by its invader, Ukraine has put out a call to hackers around the world. CEO of the cybersecurity consulting agency UBCOM, Frans Imbert-Vier observes warning signs that underlie a tipping point into a generalized cyberwar. And, according to him, European states are not equipped to deal with the threat.

Heidi.news - Are we in the first cyberwar in history?

Frans Imbert-Vier - I don't think we can say that the current conflict is strictly speaking a cyberwar. On the other hand, the situation could well change in that direction in the next few days. The Russians are discovering that they can use a very powerful non-lethal lever with computers, the effects of which will be almost as dramatic as missile fire. Expect to see lights flashing at European crossroads, as I like to say to illustrate what is going to happen. The cyber dimension of the conflict is going to affect everyone's life.

What is the current trend you are seeing digitally?

Five days ago, our cyber threat measurement tools were detecting about five to ten toxic flows from Eastern European countries. On the first day of the invasion, we grew to 90,000 flows. And today, we have exceeded one million. The situation could quickly get out of control.

It should be noted that Ukraine is a rear base for the manufacture of "cyber bombs", namely malicious computer programs. Ukrainian cybercriminals work hand in hand with Russian cybercriminals. Recently, one of the major players in Russian cybercrime supported Vladimir Putin's invasion of Ukraine. Just last night, Ukrainian cybercriminals decided to react by using all malicious computer programs against Russia. This malware is programmed to hit specific targets, but the problem is that you can never be sure that targeting a particular state will not cause collateral damage.

Ukrainian cybercriminals did not just drop these "cyber bombs", they also published them so that European actors who want to can also use them against Russia. By publishing these elements, they allow Russia to take countermeasures as well. It is still difficult to evaluate the effects of this operation.

Are European states prepared to face this threat?

Unfortunately not. The civil institutions whose mission is to protect the digital ecosystem of the States are totally out of date in this respect. In France, the Ministry of the Interior has mobilized prefects to prepare for a possible mass cyberattack. The French National Agency for Information Systems Security (ANSSI) and the cyber division of the French National Gendarmerie are for the moment very silent on this subject. I have no information about possible reactions in Switzerland either.

+300%

IN THE TARGETING OF USERS IN NATO COUNTRIES BY GROUPS SUPPORTED BY THE RUSSIAN GOVERNMENT

UBCOM
CYBER PROTECTION & SOVEREIGNTY

What could be the consequences for the countries of the European Union and Switzerland?

Cyber attacks can have many effects. Emergency services could be paralyzed, power generators could face problems or even ATMs could be shut down. If emergency services were to be impacted, there could be fatalities.

In the long run, the most vulnerable to a cyberwar situation are companies. Imagine a small company with ten employees in Neuchâtel, which has no real IT defenses. It could be infected by the Harmonic Wiper virus, which is making its comeback in the last few days after more than seven years of absence. This malicious program deletes all data, without any compensation. Its purpose is to paralyze the infrastructure. Our agency has proof that this virus is used by state operators: we have detected IP addresses from Russian military bases.

Some of our customers, especially in the health sector, have been targeted by Harmonic Wiper. The problem is that a company that sees all its data completely erased, if it does not have an external backup, may have to close down. If these attacks become widespread, this could lead to dozens of bankruptcies, resulting in an economic crisis. I hope I'm wrong and sound like a fool, but I think we're going to be hit hard by this digital conflict.

Do you think that the European states will learn from this situation?

Probably, although not all governments will react. I hope that Switzerland will realize that it needs a cyber command in the same way that it needs fighter planes for its air defense. Germany has decided to double its military budget and allocate 20% to cyber defense issues.

The UK has also indicated its desire to move to an offensive digital strategy...

Yes, it's called "hackback." It's a political strategy that aims to assert that there will be a response in case of an attack. Europe is not very willing to engage in this. France has clearly said that it will not practice hackback.

Aren't Western governments also responsible for this cyber insecurity?

By encouraging the development of malicious programs such as Pegasus, they contribute to the escalation of cybercriminals' capabilities. If the situation is so dramatic, it's partly because this strategy contributes to weakening the network, right? In 1996, Bill Clinton made a speech about the free Internet. That's when the Cyber Act was born.

UBCOM
CYBER PROTECTION & SOVEREIGNTY

Any American company that produces a digital solution that is marketed abroad must provide a backdoor to the State Department to obtain an export license. These backdoors are then used by intelligence agencies. One of the arguments used to justify this policy is the fight against terrorism.

But it is mostly about economic intelligence. Our agency UBCOM exists as a reaction to these methods. To protect companies against economic surveillance as much as possible. I know that there are demands within International Geneva for States to stop participating in the market of security breaches. If I share this desire on an ethical level, I think it is totally utopian. The United States will never agree to give up its economic intelligence. And unfortunately, that's a big part of why we have a malicious cyberspace.

Frans Imbert-Vier, UBCOM CEO, for Heidi News
February 28, 2022 - Martigny, Swizterland
https://www.heidi.news/cyber/l-europe-n-est-pas-preparee-pour-la-cyberguerre-liee-a-l-ukraine

UBCOM
CYBER PROTECTION & SOVEREIGNTY

A Swiss company specializing in digital sovereignty opens an agency in Portugal

October 26, 2022 – Lisbon, Portugal. UBCOM, a Swiss strategic consulting firm in cybersecurity and digital sovereignty, has opened an office in Portugal, in DNA Cascais, with the aim of reaching the national market and all Portuguese-speaking markets.

Based in Switzerland and with offices in France, Luxembourg and now Portugal, UBCOM's mission is to help governments and companies defend their digital sovereignty, i.e. to protect sensitive data, whether personal, strategic or operational, in the global market against economic intelligence and industrial espionage. UBCOM also provides political protection of information, adapting digital and information security strategies to local laws and regulations to protect the owner and intellectual property.

For Frans Imbert-Vier, CEO and co-founder of UBCOM, "the decision to expand the business in Portugal is directly related to the fact that Portugal is an early adopter ecosystem, open to innovative solutions in the digital sector and this is due in particular to the legislative initiatives implemented to strengthen the country's cybersecurity, but also to the excellent universities, which train the talents of tomorrow. It is also worth highlighting the government's effort, included in the state budget, for the creation of cross-cutting competencies in society in cybersecurity."

The Global Cyberspace Security Index 2020 report, which measures the commitment of 193 countries to cybersecurity issues, ranks Portugal 14th (it was 42nd in 2018) and 8th in the European ranking (it was 25th in 2018).

However, as Frans Imbert-Vier points out, "Portugal is facing, like all countries, increasing cyber threats, as evidenced by the numerous attacks that have targeted companies and public bodies, in some cases leading to serious service interruptions or even affecting some critical services. This shows that there is still a long and necessary way to go in terms of cybersecurity. »

On the other hand, Frans Imbert-Vier adds that "UBCOM's experience in the healthcare sector, protecting hospitals, clinics or pharmaceutical and analytical laboratories, is also an opportunity, as this sector has been the target of constant attacks. »

Bruno Correia, CEO of UBCOM Portugal, says that "by providing their know-how, they intend to support the economy and the country by responding to the great challenges of digitalization, but also create and stimulate local employment."

UBCOM
CYBER PROTECTION & SOVEREIGNTY

In the first phase of its entry into Portugal, UBCOM will focus on three main solutions: Ubscan, Detoxio by Serenicity and Mailshield.

Ubscan is the first vulnerability scanning and certification software charged by IP. Ubscan identifies all weaknesses and vulnerabilities of information systems and all equipment with an IP address (servers, printers, IoT). This is a fundamental diagnosis to correct vulnerabilities and increase the level of security of systems.

Detoxio from Serenicity, an exclusive service from UBCOM, analyzes and blocks in real time toxic flows that can alter, destroy or steal data from organizations.

Mailshield, on the other hand, is designed to protect one of the most important, if not the most important, communication tool in the enterprise - email. Mailshield checks the status of DNS configuration, ensures that emails are sent to the right destination, detects spoofing and phishing attempts, and discovers the origin and severity of email threats.

According to Bruno Correia, "These are entry-level services, with scalable pricing, that allow companies of any size to perfect their digital security strategies."

About UBCOM :

UBCOM is a strategic consulting and secrecy protection agency created in 2014. It acts in cyber risk prevention and protects your tactical and strategic information assets against economic intelligence and industrial espionage. Its experts advise and propose concrete solutions in cybersecurity, secrecy protection and digital sovereignty.

https://www.ubcom.eu/ - @ubcom.eu on Linkedin, Twitter, Youtube, and @ubcom-pt on Linkedin and Twitter

Press contact :
(French/Swiss/ Luxembourgish) Juliette Goutte
+33 6 76 10 18 66 – jg@ubcom.eu
(Portuguese) Luis Rosendo
+351 917228592 - luis.rosendo@generator.pt

CONTACT

Starboard Advisory
Marie de Freminville
marie.defreminville@starboard-advisory.com
+41 76 537 89 86

Elca Security
Stéphane Clerc
+41 21 613 22 58
+41 79 621 05 65

Exoscale
Barbara Labes
barbara.labes@exoscale.com
Sabrina Spilka
sabrina.spilka@exoscale.com

Prodaft
Viktoria Vargová
media@prodaft.com
+41 76 801 07 51

QR Crypto
(French/German/Spanish) Steipan Kovac
Stiepan@mailfence.com
(English) Christy Raedeke
Christy@qrcrypto.ch

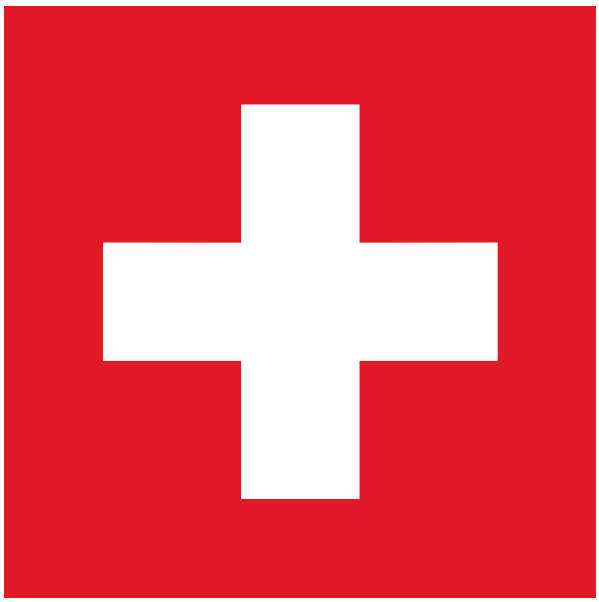
Saporo
hello@saporo.io

Sharekey Swiss AG
Hervé BLANC
+41 76 226 7600 - herve.blanc@sharekey.com

Tune Insight
contact@tuneinsight.com

UBCOM
(French/Swiss/ Luxembourgish) Juliette Goutte
+33 6 76 10 18 66 – jg@ubcom.eu
(Portuguese) Luis Rosendo
+351 917228592 - luis.rosendo@generator.pt

PRESS KIT



Switzerland.

SWISS PAVILION