United Innovations

Survey of Tools for Secure Infrastructures and Processes

Release 2 / 2024

www.security-innovations.eu

United Innovations

Network of **Excellence**

The UI Network of Excellence links method and technology experts from major companies with active scientists in their fields, aiming to foster close, personal bonds among key innovators.

www.united-innovations.eu/network-of-excellence

EDITORIAL

Kathrin Scheld

Dear readers,

The beginning of July marked an extraordinary event in the realm of innovation and entrepreneurship. On July 2nd, we hosted the grand finale of the German Startup Cup at Phoenix Pharma in Mannheim. This symposium was a remarkable success, featuring engaging panel discussions and insightful keynotes addressing some of today's most pressing challenges.

The highlight of the event was the announcement of the winners in Cybersecurity and Software & AI. The competition was fierce, showcasing the incredible talent and ingenuity of the participating startups. It is heartening to see such innovation driving our industry forward, and we are proud to celebrate these achievements in this edition.

In addition to the coverage of the German Startup Cup, we are honored to include a laudatory speech dedicated to Prof. Dr. Elisabeth André, delivered by Prof. Dr. Antonio Krüger from DFKI. This tribute highlights Dr. André's significant contributions and leadership in our field.

Furthermore, we bring you an exclusive interview with Philipp Kalweit, widely recognized as Germany's youngest professional hacker and a prodigious talent in cybersecurity. His insights provide a fascinating glimpse into the mind of a young innovator at the forefront of our industry.

This edition also includes a series of thought-provoking articles such as "Shifting the Focus from Breaking RSA to Benchmarking Quantum Computers," "Unified Hardware Accelerator Design for Post-Quantum Cryptography," and "Cyber Threats from Quantum Computers: What is a Crypto Center of Excellence?" These pieces are designed to provoke discussion and inspire action as we navigate the complexities of cybersecurity in the quantum age.

In this issue, we are excited to present an interview with Kaspersky on the concept of Cyber Immunity. Additionally, there is an interview on easily implementable cyber-immune security with BOLL Engineering AG. Also included is Kaspersky's Threat Radar, offering insights into current and emerging threats.

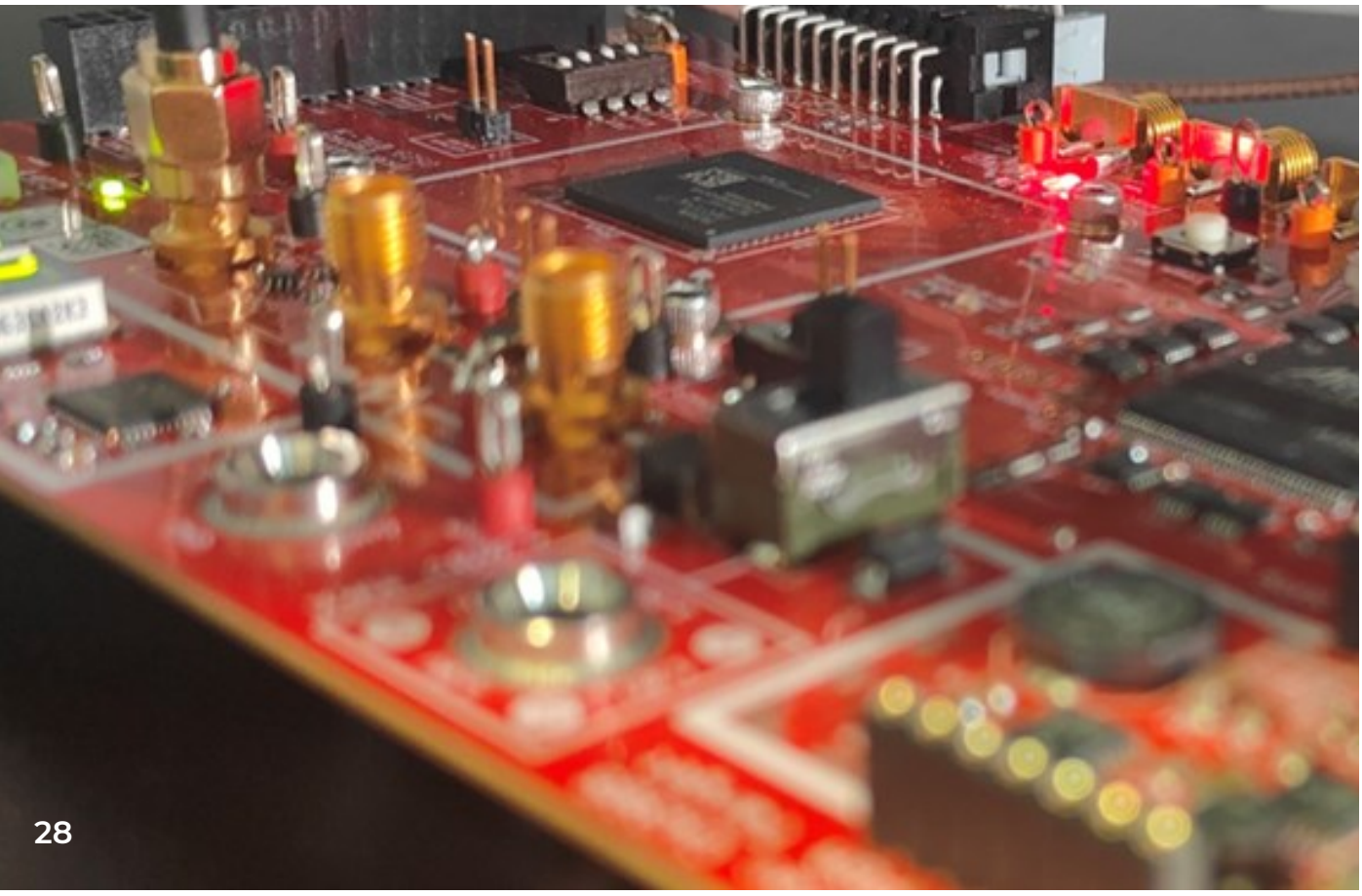
As we reflect on the recent symposium and the dynamic content of this issue, it is evident that innovation and resilience are key to overcoming the challenges we face. The future of cybersecurity depends on our ability to adapt, innovate, and collaborate. I am confident that the insights and knowledge shared in this magazine will contribute to these efforts.

In closing, I wish to express my gratitude to all contributors, speakers, and participants who made the symposium a success. Your dedication and expertise are invaluable to our community. I hope you find this edition both informative and inspiring.

Enjoy reading,

Kathrin Scheld

CMO
GFFT Security Lab GmbH



14 Interview
Philipp Kalweit's journey from tech enthusiast to successful IT professional.

34 Cyber-immune protection insights from Kaspersky experts for daily company security.

28 Designing hardware for secure communications in the quantum era.

CONTENT

3 EDITORIAL

6 CALENDAR

UNITED INNOVATIONS

8 **ABOUT US**
United Innovations: Pioneering Europe's Innovation Landscape through Collaborative and Cutting-Edge Strategies.

10 **GERMAN STARTUP-CUP 2023/24:**
Winners Announced in Cybersecurity and AI & Software Categories

12 **Celebrating a Pioneer:** Honoring Prof. Dr. Elisabeth André's Contributions to Human-Centric AI

FOCUS & RESEARCH

14 Philipp Kalweit: From Passion to Profession: A Young IT Expert's Journey (Interview)

18 Using AI to Transform IT

20 "Artificial Intelligence in cybersecurity is a double-edged sword" (Treath Radar)

24 Applied Cyber Security Research Lab: Combining IT/OT and Quantum Safe Cryptography

26 Shifting the focus from breaking RSA to benchmarking quantum computers

28 Unified Hardware Accelerator Design for Post-Quantum Cryptography

30 Cyber Immunity: IT products with "inherent" protection

34 Companies need easy to implement cyber-immune protection

38 Trust Through Openness - Opportunities for Secure Open-Source Hardware

40 IT Security, Consulting, Development Prof. Dr. Dirk Heuzeroth

42 Cyber threats from quantum computers: What is a Crypto Center of Excellence?

44 Platforms and Infrastructure to Operate GenAI in Your Company's Basement

NEW TECHNOLOGIES

48 heylogin GmbH

49 Primary Target GmbH

50 SANCTUARY Systems GmbH

CALENDAR

01/10/2024
15:30-17:00
ITSM: Tech-Insights proactive IT-Management/Operations (german)
Info & Registration

10/10/2024
15:30-17:00
OT-Security: Tech-Insights plant security (german)
Info & Registration

12/11/2024
15:30-17:00
Green IT: Management Insights “Cloud instead of data center” (german)
Info & Registration

28/11/2024
16:00-18:30
Symposium on Enterprise Security 2024/2025 (german)
Info & Registration

27/02/2025
16:00-18:30
Symposium on OT Security 2024/2025 (german)
Info & Registration

If you are interested in participating in a workshop or event, please send us an E-Maill to info@gfft-ev.de. You will then receive the dial-in data.

All events and further information can also be found at
www.security-innovations.eu/kalender

Discover Our YouTube Channel!

Did you know that our magazine has been on YouTube for quite some time? Visit our channel at the following link: GFFT YouTube Channel. On our YouTube channel, we offer a wealth of valuable content:

- Startup Pitches: Discover emerging startups and their innovative ideas and products.
- Use Cases: Learn how creative solutions are implemented in practice and the value they provide.
- Panel Discussions: Follow engaging discussions with experts from various industries on current topics and trends.

Stay informed and get inspired. Subscribe to our channel to never miss new videos and always stay up to date.

United Innovations

Driving European Innovation Forward

United Innovations (UI) is a dynamic force reshaping Europe's innovation landscape. Our mission is to enhance efficiency in large corporations and promote the adoption of cutting-edge methods and technologies. UI focuses on increasing the success rate of new technologies in Europe, bolstering the continent's reputation as a leading innovation hub.

At UI, we emphasize collaboration through our innovation network, enhancing efficiency, quality, and reducing costs. Our partnerships expedite innovation cycles, facilitating the successful launch of new advancements.

Our innovation strategy revolves around identifying innovation needs, assessing current methods and technologies, and establishing effective innovation processes, including the development and implementation of new solutions.

United Innovations invites you to be part of this vibrant evolution in Europe's innovation sector. For more information, visit www.united-innovations.eu or follow UI on LinkedIn.

Contact

info@united-innovations.eu
+49 6101 95498-10

ABOUT US

Social Media

www.linkedin.com/company/gfft-ev/

www.youtube.com/GFFTeV

https://twitter.com/GFFT_eV

Imprint

GFFT Innovationsförderung GmbH
Dr. Gerd Große
Niddastraße 6
61118 Bad Vilbel

Web

www.united-innovations.eu

Print

Flyeralarm GmbH

GERMAN STARTUP-CUP 2023/24: Winners Announced in Cybersecurity and AI & Software Categories

Discover The winners of the German Startup Cup in the Cybersecurity and AI/Software categories have been announced: AskUI and heylogin emerged victorious. The non-profit Society for the Promotion of Research Transfer (GFFT) is the initiator of the cup, while the innovation network United Innovations organized the event. The PHOENIX group hosted the event at their headquarters in Mannheim. "As a leading healthcare provider in Europe, it is particularly important to us to promote the exchange between research, startups, and business," said Dr. Roland Schütz, Member of the Board IT & Digital/CIO of PHOENIX group.

On July 2, numerous innovative startups such as heylogin, Primary Target, and SANCTUARY Systems presented their groundbreaking solutions in the field of cybersecurity to around 160 invited guests. All participating startups delivered impressive pitches and demonstrated outstanding innovation. An expert jury evaluated the presentations, while the entire audience determined the winner via live voting. Dominik Schürmann from the startup heylogin emerged victorious.

The software and AI startups AskUI and UltiHash also faced the audience's vote. Jonas Menesklou from AskUI celebrated winning the coveted Startup Cup.

During the event, future-oriented strategies in agile enterprises were discussed. Prof. Dr. Volker Gruhn from Adesso, Dr. Andreas Nauerz from Bosch Digital, Dr. Roland Schütz from the PHOENIX group, and Dr. Gerd Große from United Innovations explored strategic approaches that companies should pursue in the panel discussion "Future of Agile Enterprises."

In lectures and keynotes, Ralf Pürner from Deloitte, Tim Roder from Innovation Park Artificial Intelligence, and Prof. Dr. Antonio Krüger from DFKI discussed how AI is changing the way companies operate.

In the panel "Security in Agile Enterprises," Erik de Bueger from Sumo Logic, Daniel Hofmann, CISO of PHOENIX group, Dr. Andreas Hamprecht,

GERMAN STARTUP-CUP

UNITED INNOVATIONS AWARDS

CIO & CDO of DB Regio, Prof. Dr. Sabine Rathmayer, Head of Business Cyber Security at the Bavarian University of Applied Sciences, and Christopher Rupprecht, CISO of SCHUFA, concluded that AI fundamentally changes the perception of IT security in companies and that joint efforts are needed to combat cybercrime.

"Quality Meets Agility" was the theme of the third panel with Dr. Dominik Deschner, CIO of MVV Energie, Carsten Frey, Director IT of KfW, Axel Reinsch, CIO of Röchling, and Fabian Brechlin from Rewion.

At information booths, other startups and technology providers of the competitions, as well as event partners from United Innovations, presented themselves. Participants took advantage of the entire day for networking and personal discussions.

Application for the Next Season

Startups can now apply for the next season of the German Startup Cup. For more information and to apply, please visit: www.united-innovations.eu/deutscher-startup-pokal-bewerbung/.

Celebrating a Pioneer: Honoring Prof. Dr. Elisabeth André's Contributions to Human-Centric AI

Prof. Dr. Elisabeth André and Prof. Dr. Antonio Krüger in Conversation Following the Laudation at the Symposium

On July 2nd, at the Symposium and final of the German Startup Cup for Cybersecurity + AI & Software, Professor Antonio Krüger delivered a laudatory speech honoring Professor Dr. Elisabeth André. This event also marked the awarding of honorary membership to Professor André by the GFFT (Gemeinnütze Gesellschaft zur Förderung des Forschungstransfers e.V.). The following is a condensed version of that laudation, preserving the essential highlights of her illustrious career and contributions.

Laudation for Prof. Dr. Elisabeth André:

The illustrious career of Professor Dr. Elisabeth André is filled with numerous achievements, publications, positions, awards, and significant life milestones. Born in Saarlouis, she pursued Computer Science at Saarland University, focusing her diploma thesis on language and social competence in technical systems. This early interest evolved into her main research area.

In 1988, the same year the German Research

Center for Artificial Intelligence (DFKI) was founded, André became its ninth employee. She worked in the "Intelligent User Interfaces" research group, led by her PhD advisor, Prof. Dr. Wolfgang Wahlster. Her work has consistently aimed at making technology more human-centric, improving accessibility, and creating inclusive digital services.

André's research interests encompass human-machine interaction, multimodal interfaces, affective computing, haptic user interfaces, and social-interactive agents. She has elegantly bridged multiple disciplines, including artificial intelligence, intelligent user interfaces, and socio-technical systems.

In 1995, while working on digital presentation agents at DFKI, André earned her doctorate from Saarland University. She co-designed Cyberella, an early virtual presentation agent supporting users in achieving their goals. By 2000, she became a professor at the newly established Institute of Computer Science at the University of Augsburg, where she still leads the "Human-Centered Artificial Intelligence" chair with a team of over 30 members.

In 2010, the National Academy of Sciences Leopoldina elected André as a member, recognizing her contributions to mobile hardware, eye-tracking systems, touch-sensitive surfaces, biosensors, and anthropomorphic robots. Her work in computer-based analysis of body signals has pioneered new educational and therapeutic methods, such as social and emotional learning through computer-based role-playing.

André's development of the Open Source Framework Social Signal Interpretation (SSI) in 2013 has been widely adopted in various projects. In 2017, she was honored by the ACM SIGCHI and inducted into the SIGCHI Academy as the second German member. The German Informatics Society recognized her in 2019 as one of the ten most influential figures in German AI history.

In 2021, André received the prestigious Gottfried Wilhelm Leibniz Prize for her work in conversational emotional agents. Her research addresses trust in human-machine communication, pain recognition in health assistance, and machine autonomy acceptance. Her development of SSI has provided a significant contribution beyond computer science, enabling robots and virtual characters to recognize and respond to human emotions.

André describes her work on communicative agents as a new paradigm for human-machine interaction, emphasizing the need for machines to interact with humans as naturally as possible. Her hybrid AI approach integrates observable signals and situational context to improve the recognition of affective states, making human-machine communication more intuitive and efficient.

Recognized as one of the world's most influential scientists in her field, André's dedication to nurturing young scientists is also noteworthy. In 2022, she became a full member of the Bavarian Academy of Sciences and was inducted into acatech in 2024, becoming the first member from the University of Augsburg. As part of acatech, she advises on future technology and policy issues.

André is also a member of the Plattform Lernende Systeme and co-leads the working group on Work/Qualification and Human-Machine Interaction, focusing on human-centered design in future work environments and industry 4.0.

In conclusion, Elisabeth André's career is a testament to her pioneering spirit and dedication to advancing human-centric AI. Her achievements and contributions have significantly shaped the field, making her a deserving recipient of the GFFT honorary membership. Congratulations to Professor André on her remarkable scientific accomplishments and this well-earned recognition.

Thank you for your attention.

Antonio Krüger, CEO DFKI

Philipp Kalweit

From Passion to Profession: A Young IT Expert's Journey

Image source: Philipp Kalweit

As a young shooting star, are you taken seriously in the scene?

That is indeed a legitimate question. If you look at my professional colleagues, I'm generally relatively young compared to the rest of the industry, even if you can also attribute a certain amount of experience to my seven years of professional experience. I started out at the age of 16, which was certainly a somewhat more difficult time for my credibility than it is now at the age of 24.

Perhaps we should focus less on age and more on previous project activities and the associated experience. I looked after one of my first customers, a KRITIS company with a six-figure workforce, when I was 17 years old. A customer who, by the way, is still loyal to us as a partner. In the beginning, we had to prove ourselves as one of six suppliers in terms of quality and price. We are now the only partner for the company - we have proven ourselves against the six competitors. At the age of 19, I was an external IT security manager for an ECB-regulated bank, and at 22 I worked for a group in the energy sector.

Ultimately, I still have a long career ahead of me. Whether this is ultimately enough to be taken seriously as a "young shooting star" in the scene is up to each observer. Much more important, however, is the question of whether we are "taken seriously" as a company. With customers from the KRITIS environment, the public sector and SMEs, as well as colleagues with an academic background and over ten years of professional experience, the answer is clearly yes!

What drove you to get involved with IT topics as a child?

Personal passion - quite clearly. I was fascinated by IT processes and programming languages from an early age. The endless possibilities, the constant solving of problems and the associated solution finding. You never get bored and you always find something new to get to grips with. I came into contact with computers at an early age in elementary school, and that's when the spark was ignited.

With your knowledge, you could certainly earn more money in the "less conventional" sector. How tempting is that?

What knowledge in the field of penetration tes-

ting is basically just a tool. I can use it to generate added value for society by finding vulnerabilities in software or using it specifically for data theft. The same applies to operating a car - whether I use it as a means of transportation, for example, or deliberately cause an accident with personal injury. It is more a question of one's own ethical principles than of temptation.

What are the most common omissions that companies make when it comes to IT security?

It often starts with the company's strategy. A holistic security strategy with a security culture, clear and recurring messages in the form of guidelines: If password policies are not standardized, the assignment of passwords is correspondingly lax. Lack of use of multi-factor authentication and, in particular, outdated software solutions. The last point in particular is crucial, as vulnerabilities already known to the manufacturer and security researchers are marked with a CVE identifier and listed in freely accessible databases. If patches are not applied in good time, an attacker may well be able to gain access to the system with the help of these "low hanging fruits". In other words, via vulnerabilities that are known to everyone.

To summarize:

- Security culture (security awareness)
- Outdated software
- Weak passwords and lack of use of multi-factor authentication

What needs to change in education policy in Germany so that the next generation is introduced to IT topics?

In my opinion, awareness of the subject area already exists. However, this is probably a problem of skilled staff. Many teachers are not trained in IT topics and the necessary infrastructure (WiFi, notebooks, tablets...) is also weak. Incentives should be created to provide existing teachers with further training in these topics and to specifically promote computer science as a teaching profession.

You once said that you want to "change the image of hackers and attitudes towards IT security." What exactly do you mean by that?

Hardly any other topic is as relevant to society as a whole and at the same time as mystified as IT security. The profession of penetration tester in particular has existed for over twenty years, but is hardly known to most people in our society. We want to educate, explain and demystify so that IT security can be understood, implemented and taken for granted by everyone. Only if we understand something and it is commonplace for us can and will we use it on a daily basis.

You are also a founder/entrepreneur. What can politicians do to improve the framework conditions for ambitious, young entrepreneurs with good ideas?

Less bureaucracy, greater use of new technologies, i.e. process optimization at the commercial register and tax office and tax relief. Because new ideas thrive on agility and rapid implementation.

Hacking, IT security - all very technical, rational topics. Tell us about a very emotional experience you had in connection with your job.

I meet all kinds of people in my job and look forward to a new IT challenge every time. You won't believe me, but even after seven years in the job, I still jump for joy and sometimes even do a little happy dance every time a project is accepted. So it's emotional for me almost every day - in a positive sense. But if you want to hear a story that I can't get out of my head, it's this one:

A few years ago, we once audited a BaFin-regulated universal bank. Within three days, we were able to remotely control the safe deposit

Image source: Philipp Kalweit

boxes, take over fingerprint sensors, suspend camera surveillance... the IT manager in charge was blindsided. That was very emotional for me. Imagine you've been working passionately on something for over 15 years and believe you're doing everything right and suddenly an external consultant comes along and points out serious shortcomings. This is frustrating and can sometimes also scratch your own ego. This is where you need a lot of finesse and genuinely sincere, encouraging words.

The story may not be particularly beautiful, but even if you don't realize it at first, it still has a beautiful meaning: the forester can't see the wood for the trees. That's why an independent outsider is needed from time to time. However, the saying also means that the forester is still the smartest person in the forest. Even if the IT manager is shaken and blindsided at first, he will still be happy about the improvement in IT security in the long term.

Our assignments are sometimes emotional, but usually end well.

Thank you very much for the interview.

Using AI to Transform IT

An article by Alexander Laubert, Lakeside Software

Since ChatGPT transformed life as we know it in November 2022, the potential of large language models (LLMs) has captivated enterprises across all industries. While IT stakeholders recognize the allure of these shiny new tools, they also acknowledge the challenges of harnessing the power of LLMs for specific IT use cases.

One of the fundamental issues with generic LLMs such as ChatGPT is they have been built and trained on general internet content and data, inherently limiting their ability to address niche issues for IT use cases such as IT transformation projects, IT help desk optimization, and digital employee experience (DEX) initiatives. There is a path forward, however: developing and integrating AI models tailored to the unique needs of IT.

AI purpose-built for IT depends on the depth, breadth, history, and quality of the data feeding the model; therefore, in the realm of IT data intelligence, robust, well-structured data is the cornerstone of effective AI. This data-centric approach can elevate AI from superficial generative use cases to purpose-built solutions that empower IT teams to transition from reactive to proactive operations.

The Imperative of Contextual Data in AI Trained for IT Use Cases

At Lakeside Software, we champion the concept of AI that can speak to IT. This vision hinges on the premise that fit-for-purpose AI must be trained on contextual data specific to IT. This approach not only enriches the models but also ensures their relevance and reliability in solving IT-specific challenges such as reducing IT tickets and the mean time to response and proactively addressing IT issues before they have an impact on the end user or the business.

For instance, endpoint data serves as a goldmine for AI in IT. Each endpoint within an enterprise environment generates valuable, context-specific data. Built and trained on this data, AI models can produce trustworthy, relevant outputs. This is particularly crucial for transforming IT operations from reactive to proactive.

The Lakeside SysTrack platform enables this proactive IT approach. Collecting more than 10,000 data points every 15 seconds from each endpoint within an enterprise estate, SysTrack amasses an unparalleled dataset that feeds into the AI model for that individual enterprise. This extensive data collection enables the model to swiftly match real-time data with the enterprise's historical data, facilitating rapid and accurate IT issue resolution. Our AI eliminates the common "swivel" problem, where IT professionals must consult multiple sources to resolve a single ticket.

What's more, we recently introduced the Lakeside SysTrack Intelligence Package, which incorporates natural language query, Intelligent Support, and anomaly detection into SysTrack's capabilities. This advancement enables IT teams to level up the maturity curve towards predictive IT, using well-structured data that spans up to three years of the enterprise endpoint data to identify and address trends over time. This historical understanding is essential to ensure successful IT transformation projects such as Windows 11, as well as seamless Merger & Acquisitions projects.

Proactive IT: The Future of Enterprise IT

AI that can speak to IT is transformative not only in resolving issues swiftly but also in assisting IT team members with root cause analysis and resolution. This intelligent AI support elevates the

help desk's capability to address widespread issues affecting numerous endpoints across the digital estate. The true value of AI tailored for IT shines in these scenarios, where it significantly enhances operational efficiency and responsiveness.

Consider the impact across various industries. AI purpose-built for IT can safeguard the uptime of frontline worker devices, preventing costly downtime. Think of rugged mobile devices on factory floors, digital kiosks and scanners at airports, or mobile digital carts in healthcare settings. By predicting and preempting endpoint issues, AI helps IT teams save time, mitigate headaches, and reduce costs.

For example, in a hospital setting, mobile digital carts equipped with patient data and medical tools are critical for efficient care delivery. Downtime of these devices can lead to significant delays in patient care, adversely affecting outcomes. AI-driven predictive maintenance can preempt such issues, ensuring seamless operation and optimal patient care.

Similarly, in the manufacturing sector, rugged mobile devices are essential for tracking inventory and managing production lines. AI can predict device failures or performance degradation, allowing IT teams to address issues before they disrupt operations. This proactive approach not only enhances productivity but also reduces maintenance costs and operational disruptions.

Integrating AI into your IT Strategy

It is imperative for IT leaders to integrate AI into the IT strategy at large. This approach is crucial not only for operational efficiency but also for driving business growth. With the right dataset, AI can act as a powerful accelerator for End User Computing, propelling IT teams towards a proactive and predictive future.

To successfully integrate AI into your IT strategy, consider the following steps:

1. **Identify Key Data Sources:** Focus on collecting comprehensive, high-quality data from all endpoints within your enterprise. This data will be the foundation of your AI for IT models.
2. **Invest in Purpose-Built AI Solutions**: Seek out AI solutions specifically designed for IT. These tools should be capable of analyzing and leveraging your unique data to provide actionable insights.
3. **Foster a Culture of Continuous Learning**: Encourage your IT teams to engage with AI tools and continuously refine their skills. A culture of learning and adaptation will ensure your team can fully harness the power of AI.
4. **Monitor and Measure Impact**: Regularly assess the impact of AI on your IT operations. Use metrics and KPIs to gauge improvements in efficiency, response times, and overall IT performance.

The Inevitable Journey Towards AI Integration for IT

The journey towards AI made for IT is both exciting and challenging. By focusing on well-structured, contextual data and investing in purpose-built AI solutions, IT leaders can transform their operations from reactive to proactive, driving significant business value.

As we look to the future, it is clear that AI will play an increasingly vital role in IT. By embracing this technology and integrating it into our strategies, we can ensure our IT operations are not only efficient but also resilient and forward-thinking.

Let’s lead the way in harnessing AI for IT, setting a benchmark for innovation and excellence in the industry.

Alexander Laubert
Director DACH
Lakeside Software

“Artificial Intelligence in cybersecurity is a double-edged sword”

Cybersecurity and the changing threat landscape present new challenges for organizations: For example, the use of artificial intelligence (AI) is making cyber attacks – such as phishing emails – harder to detect. Frank Jonas, Head of Enterprise Sales Germany at Kaspersky, shares the latest trends in the threat market.

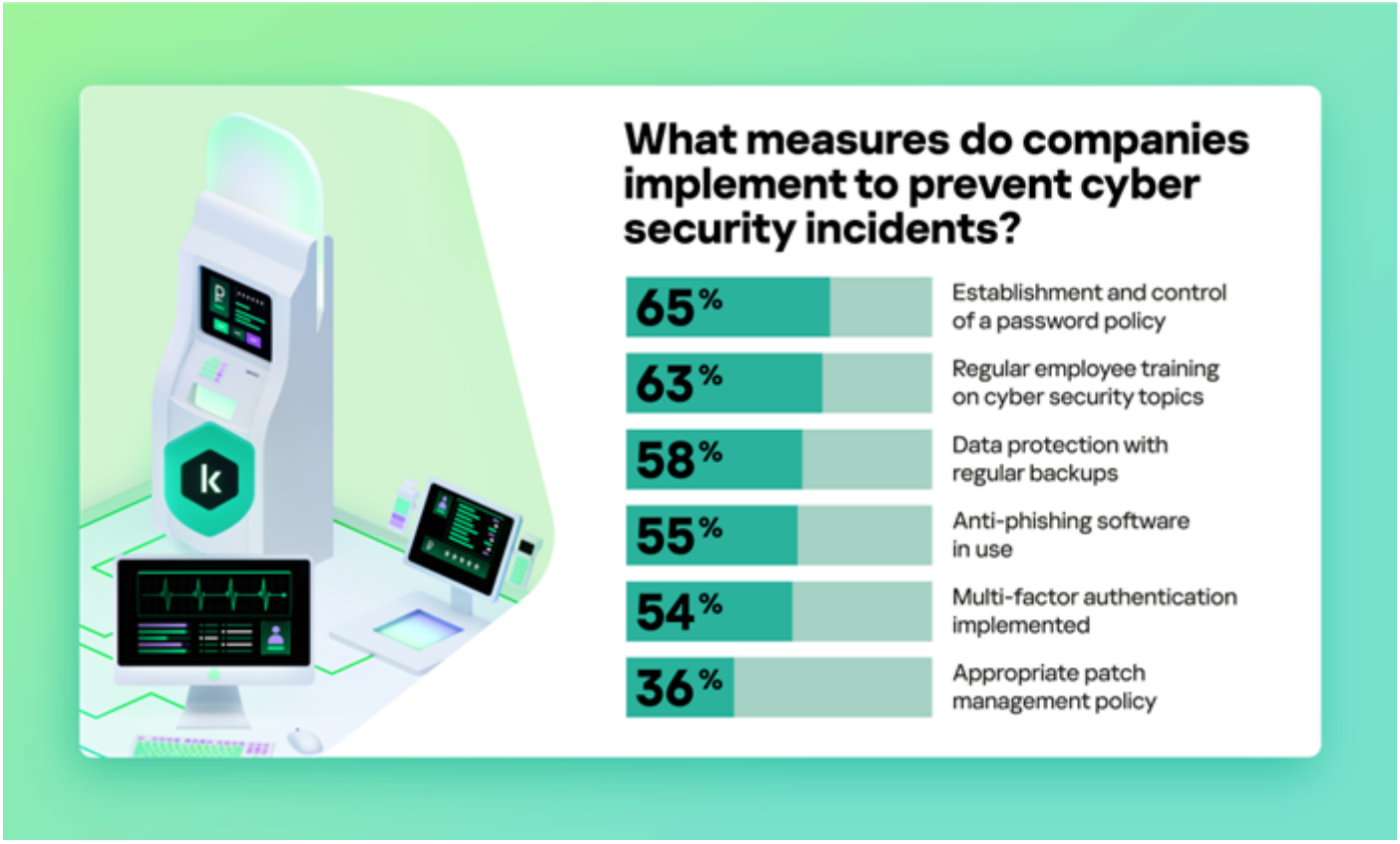


Image source: Kaspersky

United Innovations: Frank, what are the biggest challenges in the current threat landscape?

Frank Jonas: «Analyses from the Kaspersky Security Bulletin (1) show that cybercrime is increasingly becoming a business model. Cybercriminals are optimizing their business in much the same way as legitimate companies (2). They are expanding their operations and outsource certain activities. Malware-as-a-Service (MaaS) is booming. This makes it relatively easy for less sophisticated cybercriminals to launch cyber attacks by renting the appropriate malware tools. At the same time, attack methods are becoming more complex.»

Do organizations know how important it is to stay on top of current threats?

«According to a Kaspersky study, the C-suite recognizes that cyber attacks pose the greatest

threat to businesses. However, technical jargon and complicated industry terms often scare off senior executives. 38% of enterprise C-suite decision makers find even basic cybersecurity terms like malware, phishing, and ransomware confusing (3). In addition to this knowledge gap, the current shortage of IT security professionals (4), budget constraints, and untrained staff are worsening the risk (5).»

What do companies need to consider in their cyber protection efforts?

«The current threat landscape and new regulatory requirements, such as NIS 2 (6), are forcing companies to address all levels of cybersecurity: technology, processes and people. In addition to technical protection tools such as powerful anti-malware or rollback of malicious actions, companies need efficient IT security processes. They also need to make their team aware of cybersecurity. According to the latest Kaspersky Managed Detection and Response (MDR) Report, 25 percent of serious security incidents are caused by human actions (7).»

What specific measures should companies take in this context?

«In terms of business processes, companies should think about having a crisis plan for cyber incidents – an incident response plan. This will help organizations prepare to respond quickly in the event of a cyber attack. My colleagues like to quote John F. Kennedy, who said in 1962: "The best time to repair the roof is when the sun is shining." Companies should also implement policies for strong passwords and regular software patches.

In addition, cyber hygiene is becoming increasingly important; companies need to prepare their teams for current attack scenarios through security awareness trainings, regardless of position or department. And let's not forget the C-suite: they also need support with understanding cyber threats and with taking the right decisions when planning budgets or in the event of an attack. Training and policy enforcement should be high on the agenda.»

Where do companies stand in terms of protection?

«Unfortunately, there is still a lot of room for improvement. A recent survey conducted by Kaspersky among IT decision makers in Germany shows that the actual level of cybersecurity implemented is rather sobering. Even the most basic security measures are lacking: Only 65% have a password policy that is monitored; just over half, 58%, create regular backups; and only 15% conduct attack simulations. Moreover, only 21% have an incident response plan in place (8).»

Can the internal IT handle all of this?

«In times of staff shortages – which, in addition to budget constraints, affect mid-sized companies in particular – companies usually need support. Today, organizations of all sizes are increasingly turning to external expertise to cover all facets of cybersecurity. A reliable cybersecurity partner offers its customers state-of-the-art cyber protection technology, services and awareness training as a complete package. At Kaspersky, we call this All-in-one cyber protection (9).»

What other trends are you seeing in the current threat landscape?

«Kaspersky operates in more than 200 countries and territories, gathering real-time intelligence from around the world. Our elite group of international experts – Kaspersky's Global Research and Analysis Team (GReAT) – is recognized worldwide. This enables us to give companies a 360-degree view of the current threat landscape. Based on our Threat Intelligence (TI) they can prepare for new risks and proactively protect their systems against upcoming attacks (10).

One key observation is that operational technology is a growing target for cybercriminals (11). As a result, we strongly recommend that industrial companies deploy a dedicated industrial cybersecurity solution and ICS Threat Intelligence reporting (12).

Another trend is the increase in mobile threats. Our researchers have seen a significant increase in attacks on mobile devices worldwide in 2023, to approximately 33.8 million. That's nearly 52% more than previous year. Therefore, it is critical to remain vigilant and implement robust security measures on mobile devices to adequately protect against the ever-evolving cyber threats (13).»

How do you perceive the role of artificial intelligence in terms of cybersecurity?

«Artificial intelligence in cybersecurity is a double-edged sword. AI and machine learning (ML) can improve tasks such as malware detection and phishing prevention. Kaspersky has been using AI and ML to solve specific problems for nearly two decades already. However, the same dynamic also poses risks as cybercriminals use it for more sophisticated attacks (14).

On top of that: The current AI hype gives rise to an additional kind of risk. Our Digital Footprint Intelligence Service has discovered thousands of stolen credentials for popular AI tools like ChatGPT, Grammarly, and Canva on the darknet (15). The compromised credentials come from infostealers, a specific type of malware that steals user credentials. Effective enterprise security solutions that monitor compromised accounts on the darknet and notify organizations when users of their online services have been compromised are becoming increasingly important (16).»

References

(1) https://securelist.com/ksb-2023-statistics/111156/

(2) https://securelist.com/corporate-threat-predictions-2023/108456/

(3) https://go.kaspersky.com/ti-separated-by-a-common-language.html

(4) https://www.kaspersky.com/blog/portrait-of-infosec-professional-report-2024/

(5) https://media.kasperskydaily.com/wp-content/uploads/sites/86/2024/05/23140825/Enterprise_cybersecurity_Report_23-05-24-1.pdf

(6) https://go.kaspersky.com/nis2-directive.html

(7) https://securelist.com/kaspersky-mdr-report-2023/112411/

(8) https://go.kaspersky.com\IR-Report-DE.html

(9) https://go.kaspersky.com/all-in-1-cyberprotection.html

(10) https://go.kaspersky.com/de_uchub.html

(11) https://ics-cert.kaspersky.com/publications/reports/2024/03/19/threat-landscape-for-industrial-automation-systems-statistics-for-h2-2023/

(12) https://www.kaspersky.de/about/press-releases/2024_industrieunternehmen-in-deutschland-im-visier-immer-mehr-gerate-von-cyberbedrohungen-betroffen

(13) https://securelist.com/mobile-malware-report-2023/111964/

(14) https://securelist.com/story-of-the-year-2023-ai-impact-on-cybersecurity/111341/

(15) https://www.kaspersky.com/about/press-releases/2024_kaspersky-more-than-36-million-ai-gaming-credentials-compromised-by-infostealers-in-3-years

(16) https://dfi.kaspersky.com/blog/dark-web-threats-response-guideline

Frank Jonas
Head of Enterprise Sales
Germany
Kaspersky

Detailed information in the techL profile: Kaspersky

Applied Cyber Security Research Lab

Combining IT/OT and Quantum-Safe Cryptography

An article by Esther Hänggi and Sebastian Obermeier, Lucerne University of Applied Sciences and Arts (HSLU)

Operational technology (OT) is used to supervise and control industrial environments. These systems are crucial for society as a whole and therefore highly security critical. Due to their long lifespans, they cannot be easily updated. This poses a particular challenge in light of future attacks by quantum computers. The Lucerne University of Applied Sciences and Arts (HSLU) in Switzerland is researching on the intersection between quantum-safe cryptography and OT cyber security.

OT Cyber Security – Challenges for Recovery

Modern education needs both theoretical and practical learning experiences. At HSLU, we have created a special lab called “Krinflab”, which represents a substation of an energy company and is used for both research and education. The lab is unique in its double use for cyber security teaching and research purposes. It features a combination of old and new devices and systems to cater to both basic and advanced research and teaching needs, enabling hackathons with a broad audience [1].

Figure 1 - Krinflab

When the lab is used to train cyber security professionals, its state changes, especially after cyber-attack exercises. Thus, the lab needs to be reset to a known good state, comparable to real systems after a (potential) cyber-attack. To achieve this recovery efficiently demands high degrees of automation with as little as possible recovery time.

Our experience from numerous research projects and lectures showed that most IT components are well prepared for automated recovery and re-instantiation of known good states. OT hardware and software, however, imposes hurdles like forced interactive installations or license activation due to its legacy character [2].

The slow update cycles of OT devices entail that we cannot expect changes regarding better automation soon. While missing software automation features that are standard in IT might seem like a simple nuisance, a quick recovery of critical systems after an attack is of essence. Moreover, the closely related issue of the inability to upgrade software – and therefore also adapt cryptographic algorithms – poses a real danger with the upcoming threats by quantum computers. We are therefore investigating quantum-safe technologies and their use for OT environments.

Quantumlab – Applications of Quantum-Safe Cryptography

A large proportion of the cryptography used today is threatened by attacks using quantum computers and will eventually have to be replaced by novel techniques withstanding these attacks.

Two approaches to become “quantum-safe” are typically discussed: the first bases security on mathematical problems which are presumed to be difficult to solve even for a quantum computer. The new algorithms derived from them are called post-quantum cryptography. They run on “normal” hardware and can therefore in principle be used on the present-day infrastructure. Several properties specific to OT, however, pose additional difficulties compared to IT: on one hand, as mentioned above, the inherent issue of changing or updating the system as such. On the other hand, the computational and memory limitations which are common among OT systems, also partly due to their long lifespan. OT devices are not

always apt to run all post-quantum cryptographic algorithms since they have different properties from the currently used ones, such as key size or needed computing time [3]. The Quantumlab therefore researches under what circumstance which algorithms can be used, as well as possible paths of migration.

A particular emphasis lies not only on communication standards, but also on certificates and certificate management, which is still not widely used in OT environments. Certificate management solutions are demanded by several standards, but there are hardly any concepts for OT environments, especially not involving post-quantum resistance.

The second approach to achieve security in the presence of quantum computers is to base security on physical properties, in particular, quantum physics. This “quantum cryptography” is mainly used to share secure keys between two parties (which can then be used to communicate securely) or to create random numbers for keys locally. Quantum cryptography requires specific hardware, for key distribution e.g. a direct optical fiber connecting the endpoints. The OT domain is comparatively well-prepared to accommodate quantum cryptography, since the endpoints are usually stationary and often already are connected by optical fiber e.g. in the energy sector.

Following the concept in OT, we have created a Quantumlab, in which we research the integration of quantum cryptographic devices into existing IT and OT infrastructure. We develop and study secure applications using these devices. E.g., a quantum random number generator is used to encrypt files [4], cf. Figure 2. This demonstrates how important unpredictable random numbers are through scrambling an image.

Figure 2 – Quantum demonstrator

Quantum cryptography is typically utilizing quantum properties to securely exchange cryptographic keys between two parties. Securely means, that it can be detected if any third party has read the exchanged key. In a recent research study it was possible to generate secret keys at a rate of 64 Mbps over a distance of 10.0 km and at a rate of 3.0 Mbps over a distance of 102.4 km with real-time key distillation [5]. These rates make quantum key distribution usable for environments like OT as well.

References

[1] Obermeier S., Tresoldi G., Tellenbach B., Lenders V. (2024): HydroLab: A Versatile Hydroelectric Power Lab for Security Research and Education. 21st International Conference on Security and Cryptography (SECRYPT 2024), Dijon, France, July 2024.

[2] Obermeier S., Jösler Th., Renggli St., Unternährer M., Hämmerli B (2023): Automating Recovery in Mixed Operation Technology/IT Critical Infrastructures. IEEE Security & Privacy, vol. 21, no. 5, pp. 43-54, Sept.-Oct. 2023.

[3] Hänggi E., Tellenbach B, Wildfeuer Ch. (2023): Quantum and post-quantum cryptography. In Swiss Academy of Engineering Sciences SATW (Hrsg.), Technologies in focus - Online publication: https://technology-outlook.satw.ch/en/technologies-in-focus/quantum-and-post-quantum-cryptography .

[4] Drexel J., Hänggi E., Méndez Veiga I. (2023): Quantum Random Number Generator Showcase. In World Quantum Day, https://worldquantumday.org/events/quantum-random-number-generator-showcase/

[5] Grünenfelder, F., Boaron, A., Resta, G.V. et al. (2023): Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems. Nat. Photon. 17, 422–426. https://doi.org/10.1038/s41566-023-01168-2

Prof. Dr. Esther Hänggi
Lucerne University of Applied Sciences and Arts (HSLU)
Applied Cyber Security Research Lab
Rotkreuz, Switzerland

Prof. Dr. Sebastian Obermeier
Lucerne University of Applied Sciences and Arts (HSLU)
Applied Cyber Security Research Lab
Rotkreuz, Switzerland

Shifting the focus from breaking RSA to benchmarking quantum computers

An article by Manpreet Jattana and Thomas Lippert, Goethe-Universität Frankfurt am Main

Quantum computers have gained major interest in the last two decades as a breakthrough technology. It is hard to forget the hype in the news around breaking the RSA encryption from the 1990s. Significant hardware developments have also occurred since this period. However, these developments did not break any of the RSA encryption used today. Prime factorisation is also not at all the only goal of quantum computing. The reality is that current quantum computers are error-prone and noisy. We need quantum algorithms to benchmark such devices to eventually improve them. In this article, we mention one such algorithm and test it on real quantum hardware.

RSA and quantum computers

Secure communication over open channels like the Internet is an important concern for both society and industry. The widely adopted RSA encryption for secure communication is fundamentally based on the difficulty of factorization. State-of-the-art classical algorithms to find prime factors are based on the general number field sieve. The factorization of RSA-250 (containing 829 bits) recently achieved using these algorithms, however, remains far from the 2048 bits or more, which are commonly used and do not pose a threat to our security.

In 1994, Peter Shor proposed an algorithm that factors integers on quantum computers exponentially faster than the best-known classical algorithms. A modern version of Shor's algorithm to factor 2048-bit integers needs 2048+1 logical error-corrected qubits. Even very optimistic estimates in the literature suggest that given physical quantum gate error rates of 0.001, one will need 177 days and at least 13,436 physical qubits to factor a 2048-bit RSA integer[†]. Some current devices have around 100 physical qubits and have serious problems with gate error rates.

Let us confront this with reality: without oversimplifying the problem, the modern version of Shor's algorithm has been used to factor the numbers 15, 21, and 35 on real quantum computing hardware. Going beyond 35 is currently proving to be an experimental challenge due to the noise and errors of such quantum devices. As a small-scale alternative, quantum computer emulators run on classical computers can be used to study the workings of the algorithm. These can go much beyond real quantum hardware to factor integers for now. The largest number factored so far 549,755,813,701[*] using 40 qubits, is still very far from the classical state-of-the-art.

The issues associated with current and near-future quantum computers are less about the security of the RSA encryption but about the quality of the qubits and their error rates. In this regard, it becomes important to be able to benchmark different types of quantum computing technologies that are competing to become the leading technology. We have developed several such benchmarking tools and discuss one of them below.

Benchmarking quantum computers

Our benchmarking method for gate-based quantum computers consists primarily of two components: a problem defined in terms of a Hamiltonian and a solution approach defined in terms of a quantum circuit or ansatz. A quantum circuit is a visual model used to represent operations on gate-based quantum computers. It is analogous to classical circuits but operates on qubits using quantum gates instead of bits and logic gates.

Figure 1 shows the quantum circuit we use for our benchmarking of 4 qubits of a 127-qubit device. The quantum computer is initialised in the state given by |0000> in the ket notation. This is followed by R_x or R_y rotations, Controlled-NOT gates, parametrised (θ_1, θ_2) R_z gates, Controlled-

[†] E. Gouzien and N. Sangouard, Factoring 2048-bit RSA Integers in 177 Days with 13,436 Qubits and a Multimode Memory, *Phys. Rev. Lett.* **127**, 140503, (2021).

[*] D. Willsch, et. al, Large-Scale Simulation of Shor's Quantum Factoring Algorithm, *Mathematics*, ***11*** (19), 4222, (2023).

NOT gates, and finally R_x or R_y rotations. In this benchmark, we do not even entangle all the qubits but only pairs of them.

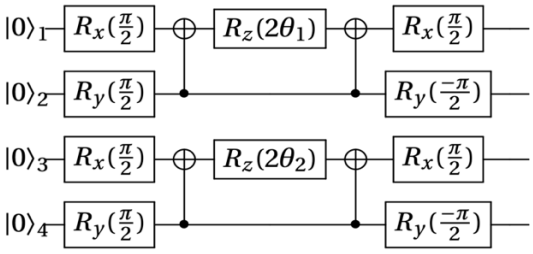


Figure 1: A quantum circuit to find the ground state energy of benchmark problems.

At least two different problems have been identified for which the ansatz shown in Figure 1 can be used. These are the mean-field model and the Majumdar-Ghosh model. Their analytical solutions are known. We pick the former and test it on an IBM-Q device. The Hamiltonian is given as $H = \sum_{(i,j)}(\sigma_i^x\sigma_j^x + \sigma_i^y\sigma_j^y + \sigma_i^z\sigma_j^z)$, where σ are the Pauli operators, and (i,j) sums over all pairs of N lattice sites. The solution (ground state energy) is given by the expression $3(a—N)/2$ where a=1 for odd N and a = 0 for even N. In our case, N = 4 and a = 0, giving the ground state energy equal to —6 .

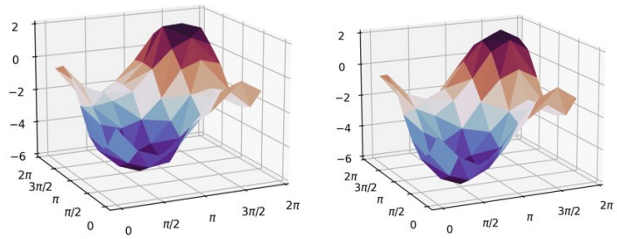


Figure 2: Benchmarking results showing energy landscapes using IBM-Q Osaka (left) and an ideal emulator (right).

The experiment was performed in June 2024. The results are shown in Figure 2. We obtain the energy landscape of the ansatz consisting of two parameters using an 8 x 8 grid by plotting the energy obtained at each point. We observe a qualitative agreement of the IBM-Q device to the ideal emulator. However, the depths of the valleys in both cases located at (π/2,π/2) are different. The emulator finds the energy –5.99 and the real device finds –5.28 when using 1000 samples. This indicates a quantitative disagreement even when using only 4 qubits, which can be crucial in some other cases of practical interest.

IBM-Q's quantum devices currently cost $1.60/s of computing time. For our rather small benchmark, the costs would be approximately $1.60*64*7 ≈ $717. Often, there is a waiting queue for cloud-based devices. Additionally, cloud-based quantum devices do not allow deeper access to the system hardware, which is important for researchers. To overcome these issues, Goethe University Frankfurt has purchased its own small-scale quantum computer named «*Baby Diamond*», which will be installed and operational by the end of 2024.

Conclusion

State-of-the-art classical algorithms remain very far from factoring integers to break the RSA encryption. Quantum computers have been theoretically proven to be exponentially faster and can, in principle, crack RSA. However, the quantum computing community is facing significant hurdles in creating hardware that is both scalable and tolerant of errors and noise. The need of the hour is to provide benchmarking algorithms to help test and develop better hardware. We showed one example of such an algorithm and tested it on IBM-Q cloud-based hardware, known to be one of the best existing technologies. Still, our results for only 4 qubits show a discrepancy of >10% for the ground state energy, demonstrating through our benchmark that the technology is far from being able to break large encryption schemes.

Dr. Manpreet Jattana

Postdoc
Goethe-Universität
Frankfurt am Main

Associated Fellow
Johanna Quandt Young Academy

Prof. Dr. Dr. Thomas Lippert

Professor
Goethe-Universität
Frankfurt am Main

Director
Jülich Supercomputing Centre
Forschungszentrum Jülich

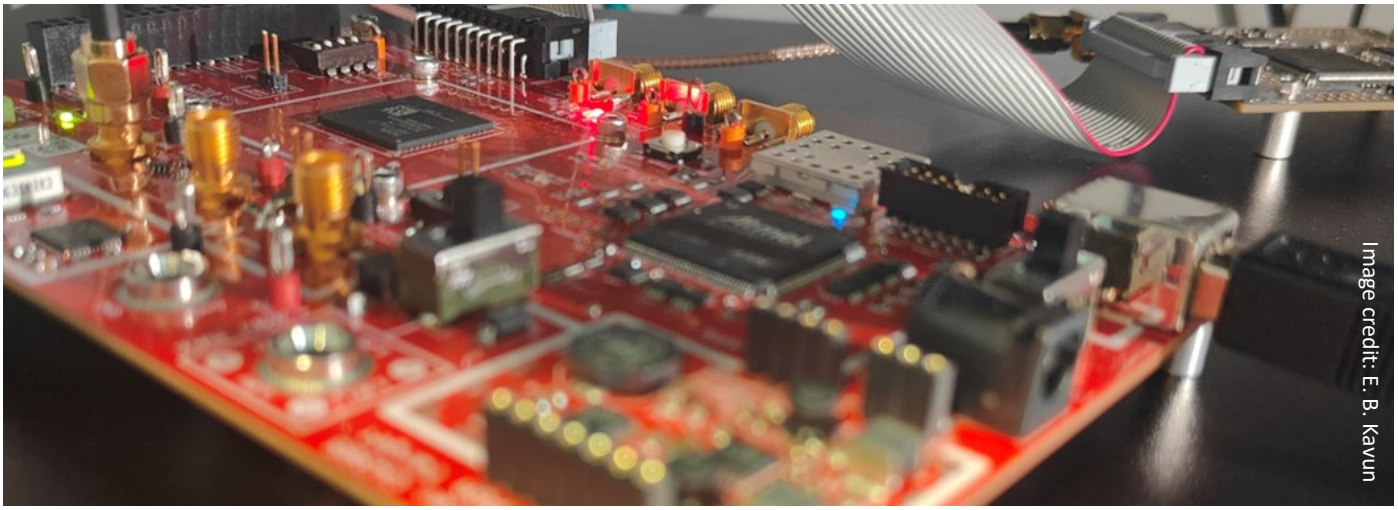
Acknowledgement

We acknowledge the use of IBM Quantum services for this work. The views expressed are those of the authors, and do not reflect the official policy or position of IBM or the IBM Quantum team.

Unified Hardware Accelerator Design for Post-Quantum Cryptography

How can we secure global communications in the quantum era? – With the rapid advancements in quantum computing, the foundation of our current encryption methods is at risk. So, how do we protect sensitive data and maintain secure communication channels in this new era?

An article by the Secure Intelligent Systems Research Group, FIM, University of Passau



The new NSF/DFG-funded research project at the *University of Passau (Uni Passau)*, Germany and *North Carolina State University (NCSU)*, US aims to develop a unified hardware accelerator capable of supporting both US and German post-quantum cryptographic standards, namely NIST's CRYSTALS-Kyber and BSI's recommendation FrodoKEM. The project will address the critical need for secure, efficient, and adaptable cryptographic solutions in the face of emerging quantum computing threats.

The advent of quantum computing poses a significant threat to the security of classical encryption methods used in the global communication infrastructure. Quantum algorithms can solve complex mathematical problems exponentially faster than classical algorithms, threatening the security of widely used cryptographic schemes such as RSA and elliptic curve cryptography. This brings an urgent need to develop and deploy new post-quantum algorithms that can withstand quantum attacks.

To address this challenge, international standardization bodies have been working on novel cryptographic standards. In the United States, the National Institute of Standards and Technology (NIST) is leading the effort, while in Germany, the Federal Office for Information Security (BSI) is recommending specific algorithms for quantum-safe communication. However, a significant challenge arises when different countries adopt different standards. For instance, BSI recommends the FrodoKEM algorithm [1] for post-quantum key encapsulation, whereas NIST has selected CRYSTALS-Kyber algorithm [2] for the same

[1] Alkım *et al.*, FrodoKEM, Technical Report, NIST, 2020.
[2] Bos *et al.*, CRYSTALS-Kyber: A CCA-secure Module-lattice-based KEM, IACR ePrint, 2017.

purpose. Such variations require the development of hardware capable of supporting multiple standards.

The newly-funded US National Science Foundation (NSF) / German Research Foundation (DFG) project «A Unified Hardware Design for the USA and German Post-Quantum Standards», led by *Dr. Elif Bilge Kavun (Uni Passau)* and *Dr. Aydın Aysu (NCSU)*, targets the design of a unified hardware accelerator that can efficiently support both of the mentioned post-quantum key encapsulation protocols. This involves several non-trivial tasks:

- Algorithmic Innovations: Developing joint arithmetic operations for both algorithms.
- System Re-architecting: Enhancing the architecture to improve operational support and memory access schemes.
- Custom Hardware Design: Creating unified components such as arithmetic units, cryptographic primitives, and specific steps like sampling, encoding/decoding, and compression/decompression.
- Security Enhancements: Implementing countermeasures against timing and power/electromagnetic information based side-channel attacks using constant-time hardware and masking techniques.

After a detailed analysis and benchmarking of both FrodoKEM and CRYSTALS-Kyber algorithms to identify the most critical and resource-intensive operations, the project will continue with optimizing each algorithm for the unified hardware design. Following this, the focus will shift to designing the critical hardware blocks including arithmetic units and cryptographic primitives with hardware parallelization as the main implementation focus to address bottlenecks in polynomial/matrix arithmetic and hashing operations.

The development of such a unified hardware solution has far-reaching implications. It addresses a multi-billion-dollar market and aligns with global standardization efforts such as those led by NIST and European bodies. This project is expected to facilitate the secure and efficient implementation of post-quantum cryptographic standards, ensuring a smooth transition to quantum-safe systems for applications requiring high-performance and security. Additionally, the project aims to promote further research in the field by organizing international workshops to provide opportunities for young as well as underrepresented researchers.

The project outcomes will be significant for securing global communications in the quantum era. Through a unified hardware accelerator for post-quantum cryptographic standards, the researchers will not only address current security challenges, but also implement a robust and adaptable cryptographic infrastructure for the future.

Prof. Dr. Elif Bilge Kavun
Assistant Professor
University of Passau

Cyber Immunity: IT products with “inherent” protection

Can IT systems withstand cyberattacks without any additional, applied security tools? And if so, how can this be implemented practically?
Waldemar Bergstreiser, General Manager Central Europe at Kaspersky provides insights and answers.

Image source: Kaspersky

At the dawn of computer security in the late 1980s, antivirus software emerged as a response to the first malware. Since then, the industry has been playing catch-up, and the challenge for cyber-defense solutions has been to recognize new malware and techniques as quickly as possible and offer the appropriate protection. During more than 30 years of this game, the stakes have changed significantly. Today, cybersecurity, data protection and countering advanced APT attacks are becoming a priority and corporations are spending almost a third of their IT budget on protection against cyberthreats.

United Innovations: Mr. Bergstreiser, considering the ever-evolving cyber threat landscape of today’s world and the challenges that go with this for companies, wouldn’t it be necessary for cybersecurity to make an evolutionary leap to change the nature of the game?

Waldemar Bergstreiser: “Definitely, this moment has already come! Since 2012 Kaspersky has been

driving the transition from protection against cyberthreats to immunity from them. But don't get me wrong, in certain areas such as corporate protection, current cybersecurity solutions are still very effective. The problem is that there are some systems on which anti-malware solutions simply cannot be installed, such as small boxes of IoT gateways or electronic control units in a connected car, to name just a few. If you combine this with the challenge of needing to manage a multitude of systems of different kinds, different requirements and different levels of complexity, you end up with a Herculean task. Besides, many risks are not really assessable in advance. So, in addition to the traditional means of protection, a new approach is needed where security is a core element of the connected device, system, or security solution itself. We call it the Cyber Immune approach."

What does the term Cyber Immunity mean?

"Kaspersky Cyber Immunity® is Kaspersky's own, cost-effective methodology for developing secure-by-design IT systems. The Cyber Immune approach is rooted in our in-house developed KasperskyOS operating system – a platform for building Cyber Immune products. Cyber Immune IT products have an "inherent" protection, which is the ability to withstand cyberattacks without any additional – that is applied – security tools. The overwhelming majority of types of attacks on a Cyber Immune system are thus ineffective and unable to impact its critical functions; we minimize the number of potential vulnerabilities. Cyber Immunity is Kaspersky's vision for the future of all IT systems."

How does this work in practice?

"To make a system Cyber Immune, it needs to be developed according to a specific methodology and with the right components. Firstly, you need to clearly define a security goal of the system – for example, to enable confidentiality and integrity of data transferred from a device to a cloud. The system will need to meet this goal in any use case. Secondly, all system components, such as applications and drivers, must be isolated from each other so that if one component is compromised, it won't access another. It's just like separating apples, oranges and peaches into different baskets: if the fruits in one basket start decay, they won't affect another basket. Thirdly, the communication between components must be controlled; only the previously specified type of communication is allowed. The kernel of such an immune system should be as compact as possible, in order to minimize the possibility of bugs and vulnerabilities and to narrow the attack surface. As a result, security turns into an integral feature of the system. No third-party application will be able to take control of the system, because the affected component will remain isolated and will not be able to allow other parts to be compromised."

Do you already offer Cyber Immune products, are they a reality?

"There's a lot of talk about Secure-by-Design products and resilience in general. Kaspersky Cyber Immunity® goes beyond mere words, as it is already being commercially implemented in a range of products. Currently, Kaspersky offers Cyber Immune KasperskyOS-based products for Industrial IoT security and for building and protection of the remote workspace infrastructure. We offer Cyber Immune secure gateways, thin clients, mobile platform solutions, secure automotive gateways and many more."

Will KasperskyOS be used in mobile devices, too?

"At the moment we are going through an active research and development phase aimed at the implementation of the KasperskyOS operating system on professional mobile devices. Corporate mobile and professional handheld devices must be protected from cyber threats as much as possible.

We believe, that this state can be achieved through the implementation of the concept of Cyber Immunity, and the development of the methodology. KasperskyOS is a part of this technology stack. It's already used as a basis of Cyber Immune thin clients and IoT gateways, and in the future mobile devices could also become a new member of the cyber immune family. We will share the news once we get there."

What are the core benefits?

"I'd like to focus on three main points which are of huge added-value for companies. First: Innate security. Cyber Immune products are able to resist against as-yet-unknown threats. Second: Reduced costs. Companies relying on Cyber Immune products do not require additional security tools and hence can rely on a competitive Total Cost of Ownership – particularly, because our Cyber Immune solutions comply with regulatory standards such as Common Criteria, ASPICE, ISO 26262 and others. And third: Versatility. The clear separation of the business and security logic makes sure, there's a high degree of flexibility when changing policies need to be catered for as the code is not being impacted."

Do you have partners for your Cyber Immunity products in Europe already?

"Globally we have already several examples of successful cooperations. For example, in September 2023, we signed an OEM agreement with Centerm, the world's leading thin client manufacturer, for global deliveries of KasperskyOS-based software products. And also on the European market we see an interest towards our Cyber Immunity products. Just recently we secured a regional partnership with Boll Engineering in Germany, Austria and Switzerland for the distribution of Kaspersky Thin Client. And we are looking forward to welcoming more new partners who will join us in building a Cyber Immune tech era."

What are your objectives for the foreseeable future?

"Cyber Immunity has a long road ahead: its application will expand to various projects and solutions that have increased requirements for cybersecurity in the field of critical infrastructures, smart cities, the automotive industry and other areas. And in the foreseeable future, we hope that this approach will help raise the security of these industries to a qualitatively new level and reduce the likelihood of cyberattacks and their consequences."

Waldemar Bergstreiser
General Manager
Central Europe
Kaspersky

Detailed information in the techL profile: Kaspersky

Companies need easy to implement cyber-immune protection

Cyber attacks on companies of all sizes and in all sectors are almost a daily occurrence. So how can companies make themselves cyber-secure? Waldemar Bergstreiser, General Manager Central Europe at Kaspersky, and Thomas Boll, CEO of Kaspersky partner BOLL Engineering AG, provide insights and answers as to how Kaspersky Thin Client 2.0 addresses this challenge.

Image source: Kaspersky

Thin clients are used in most companies. Their biggest advantage is their ease of operation, as they only run the software required to access centrally managed applications. However, this software – like any other – is vulnerable to cyber attacks. Kaspersky has developed a secure variant, which Waldemar Bergstreiser, General Manager Central Europe, and Thomas Boll, CEO of BOLL Engineering AG, present in this interview and explain why it is being well received in the market.

United Innovations: Who is Kaspersky Thin Client 2.0 suitable for?

Waldemar Bergstreiser: «Kaspersky Thin Client 2.0 can be deployed efficiently in organisations with a large network of sites and a geographically distributed infrastructure. It is suitable for deployment in government institutions, transportation and industrial companies, financial institutions and in retail, in a smart city infrastructure and in companies in the automation

and manufacturing sectors – just to name a few.»

Thomas Boll: «It is an non-vulnerable IT system that is particularly interesting for companies for which it is difficult to protect individual components. Such systems in general are a valuable addition to protect an existing IT security environment even more sustainably.»

What are the product's strengths?

Thomas Boll: «With Thin Client 2.0, Kaspersky is taking a completely new approach: it works with the in-house developed KasperskyOS operating system and is basically not vulnerable to an attack. Kaspersky refers to this approach as "cyber immunity" – a concept that convinced us thoroughly. In addition, there is a holistic management platform: infrastructure, conventional end devices and the thin clients are managed and controlled via one single environment.»

Waldemar Bergstreiser: «Kaspersky Thin Client 2.0 provides seamless access to web applications and supports remote environments based on Citrix Workspace platforms and VMware Horizon infrastructures using HTML5 technology. It provides a connection to customised business applications operated on Microsoft Remote Desktop Services, Windows Servers and Terminal Servers running Windows 10 and 11. In addition, Kaspersky Thin Client 2.0 ensures faster deployment of applications on the remote desktop, shortens boot times and updates itself more quickly thanks to its compact operating system image. Due to the automatic connection, it is ready for use in only two minutes.

Thanks to the cyber immune architecture, no additional security software or other security tools are required to defend against cyber attacks. This significantly reduces the total cost of ownership.»

Cyber immune… what does it mean exactly?

Waldemar Bergstreiser: «As mentioned by Thomas Boll, Cyber Immunity is a concept developed by Kaspersky; cyber immune products will be developed so securely that they don't offer cybercriminals a target from the outset. It is our own cost-effective methodology for developing IT systems. The approach is based on our proprietary KasperskyOS operating system – a platform for creating cyber immune products. Cyber immune products have such a comprehensive protection that the majority of attack types on such a system are ineffective and cannot affect its critical functions; we minimise the number of potential vulnerabilities. Kaspersky Thin Client is such cyber immune product.»

Kaspersky has a large partner network. Why did you decide to collaborate with BOLL for the market launch of the Thin Client 2.0?

Waldemar Bergstreiser: «We have been enjoying a close business and technical cooperation with BOLL for many years already. BOLL is a distributor with a high level of technical expertise who is able to evaluate products in an in-depth manner and precisely assess the market thanks to its proven experience. Even before the market launch, we carried out PoCs (Proof of Concepts) in the DACH region with BOLL. The pilot projects took place in both SMEs and large companies in sectors such as manufacturing, government organisations, healthcare and retail. This gave us valuable insights and a thorough understanding of local technical requirements, business priorities and market expectations. The long-standing cooperation between our local team and BOLL's team is based on a dynamic and, above all, constructive feedback culture that benefits both sides.»

Why did BOLL include Kaspersky Thin Client 2.0 in its portfolio?

Thomas Boll: «We are always on the lookout for

innovative, good solutions in the field of cybersecurity. It is in BOLL's DNA that we identify and evaluate new technologies and products and do the triage, testing what makes sense and what doesn't. If we consider something sound, we try to establish it on the market and "enable" it for our manufacturers and partners – Kaspersky's Thin Client 2.0 is exactly that type of product. Kaspersky Thin Client 2.0 is the first solution based on Cyber Immunity and it is a great opportunity for us to be involved right from the start.»

Product launches can be challenging from time to time. How is Kaspersky Thin Client 2.0 accepted by the market?

Waldemar Bergstreiser: «Kaspersky Thin Client was developed for industries with increased cyber resilience requirements. It is a ready-to-use endpoint that can be seamlessly integrated into modern, customised desktop infrastructures. It is characterised by simple administration, cost efficiency and fast, powerful and user-friendly protection. Demand is correspondingly high, as the Thin Client is particularly suitable for applications with high security requirements, such as changing users or exposed systems.»

Thomas Boll: «Let me give you an example: the young Swiss IT service provider Aclue's CEO, Ajdin Zutic, is enthusiastic about the solution. This is not only because KasperskyOS massively reduces the attack surface; onboarding for new customers and users is significantly faster than with other solutions, Zutic speaks of 15 minutes. As a managed service provider, Aclue also has end-to-end control over the device, and the customer's employees can start working immediately via VDI (Virtual Desktop Infrastructure). Ajdin Zutic told me: "There are many reasons for us in favour of the new Thin Client. In my opinion, this is the first time that a game changer with a focus on security is active again. The effort needed to develop a completely new microarchitecture underpins Kaspersky's commitment."»

Waldemar Bergstreiser
General Manager
Central Europe
Kaspersky

Thomas Boll
CEO
BOLL Engineering AG

Detailed information in the techL profile: Kaspersky

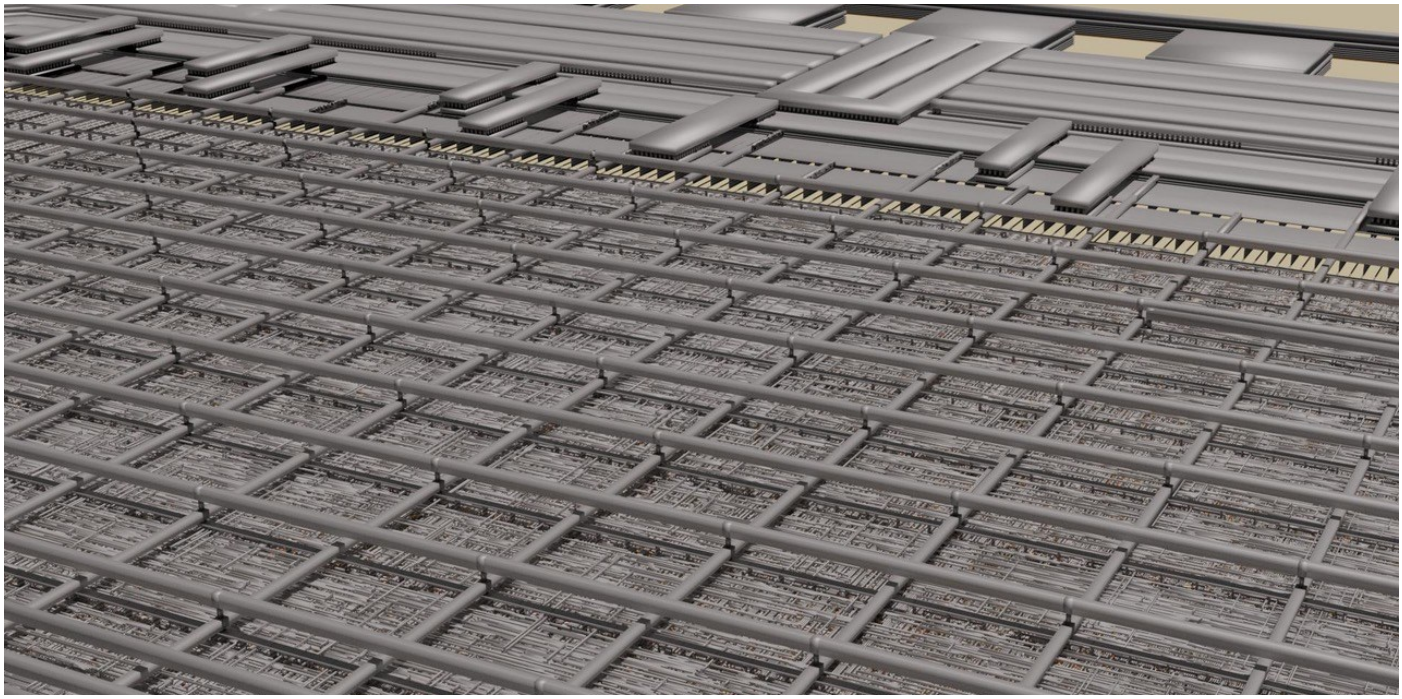


Figure 1: An Open-Source RISC-V Processor using an open 130 nm process by IHP

Trust Through Openness - Opportunities for Secure Open-Source Hardware

New ways of applying Kerkhoff's principle to the design of digital hardware

Cryptographic algorithms and standards serve as a crucial foundation for modern IT systems security. Kerckhoff's principle is a fundamental concept for modern cryptographic systems, which states that a cryptographic system should be secure even if everything, except the secret key, is known about the system. For good reason, complete transparency is therefore required to enable verification, later certification and the necessary security research on them. Nowadays in software development, this way of thinking is deeply rooted in all processes and has therefore become routine. A strict open approach to hardware design is not common, as hardware construction is traditionally carried out in closed development processes. This makes verification and certification processes more difficult, and therefore pricier. Hence, the field of open-source hardware offers opportunities to improve practical IT security and security research to strengthen the entire chain of current IT systems.

Open-Source Hardware

The advantages of an open development approach are accepted in the software world. In the realm of hardware creation, such strategies are relatively new and contrast sharply with the current design paradigm, which strongly relies on nondisclosure agreements and patents.

Free access to source code and development tools has become a matter of course for generations of developers since the birth of the GNU project 40 years ago. Currently, a remarkably similar procedure can be observed in the field of hardware development. The free RISC-V ISA and its free implementations has led to numerous high-quality open-source development tools for FPGAs and new hardware design languages (e.g., Chisel and SpinalHDL). As a next step, it is now possible to develop ASICs. Good examples of this include the Skywater project and the open PDK[1] of the Leibniz Institute for High Performance Microelectronics (IHP), which enables broad access to hardware design from enthusiasts to professional developers, startups, and researchers.

[1] https://github.com/IHP-GmbH/IHP-Open-PDK

All these developments require powerful and free development tools, comparable to the GNU Compiler Collection (GCC). In particular, the OpenRoad project[2] plays a central role here as a synthesis tool for the construction of ASICs. The manipulation and verification of layouts and the check of specified design rules (DRC) is supported by community-driven efforts like klayout[3]. Overall, all these efforts lead to an end-to-end tool chain that delivers producible layouts of smaller CPUs. Simple HSMs or other security-relevant applications like secure and smart sensors are already in range.

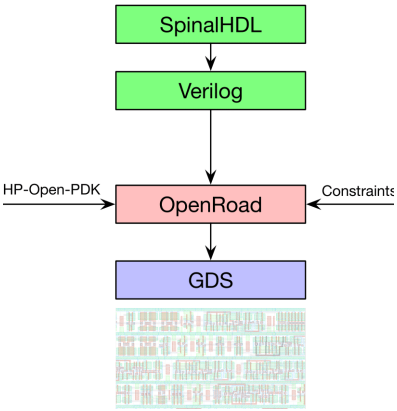


Figure 2: The development process — a rough overview

Therefore, it is possible for the first time to fully check even the hardware of safety-critical systems. Furthermore, research into the security sector will be improved in numerous ways. For example, implementations of cryptographic algorithms could be compared and evaluated through a strict peer review process, and knowledge of the hardware structures would enable new investigations into side-channel and fault injection attacks.

Recent Developments and Research Activities

The DI-Sign-HEP project is an example of this approach, working on a manageable and commercially viable hardware security module (HSM) with a tool chain that's completely open source, right down to the ASIC. The recently awarded research project DI-SIGN-HEP aims at the following goals:

Research is being conducted into how an open, formally verified and easily manageable HSM basic module can be integrated into the standardized HSM framework "Caliptra". The goal is to find, fix and close functionality gaps in open EDA tools and also to develop a manageable verification tool.

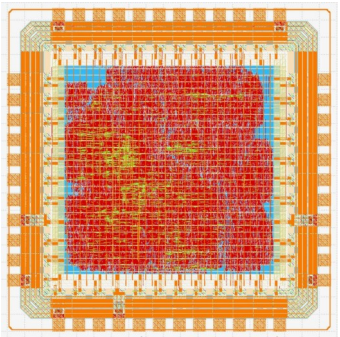


Figure 3: Ready to use GDS-layout

Essentially, the outcomes of the previous VE-HEP project are being utilized, and certain deficiencies in the instruments are being rectified and incorporated into the Caliptra system, which has been established by Microsoft, Nvidia, Google, and AMD as a component of the "Open Compute Project." To strengthen the EU's digital sovereignty, the project will use IHP's Open130-G2 PDK.

The basic HSM will be expanded to include components for the root-of-trust element, like a random number generator and secured non-volatile memory. This roots-of trust element is the anchor in security architectures that is needed to continue to implement security services and protection measures securely. The trustworthiness of open hardware will also be strengthened by this project. As part of the project, various protection profiles required for the certification of the HSM module will be evaluated and further certifications prepared to facilitate industrial application. Finally, integration into a demonstration is being sought.

Prof. Dr. Steffen Reith
Professor of Theoretical Computer Science and Cryptography
FB DCSM
Hochschule RheinMain
Wiesbaden

Prof. Dr. Marc Stöttinger
Professor of Computer Engineering and Security
FB DCSM
Hochschule RheinMain
Wiesbaden

[2] https://theopenroadproject.org/
[3] https://www.klayout.de/
[4] SIGN-HEP: Secure industrially applicable standardized HSM (https://hep-alliance.org/)

IT Security, Consulting, Development Prof. Dr. Dirk Heuzeroth / Institute for Cyber Security, Media University Stuttgart

About the company

IT Security, Consulting, Development Prof. Dr. Dirk Heuzeroth is a company providing security and data protection services with a focus on the implementation and auditing of information security management systems and the corresponding controls, as well as pentesting and offering service as data protection officer.

The Institute for Cyber Security at Media Universtity Stuttgart has also been founded by Prof. Dr. Dirk Heuzeroth. The institute focuses on raising security awareness and providing security education to students, as well as pupils, the general public and companies through Serious Games and regular Hacking exercises.

Technology

The core component of an Information Security Management System (ISMS) is risk management. Risk management deals with the identification, analysis, evaluation and treatment of risks usually arising from a permanently changing threat landscape. Statistics from insurance companies [1] show that phishing is the dominating threat, as entry point into a company's infrastructure and access to credentials. A targeted variant of this attack is spearphishing, which is often used for or in combination with business e-mail compromise. One main cause for the success of these kinds of attacks is the human factor, i.e. the attacker abuses human kindness, curiosity, greed or the fact the we as humans are not able to conentrate all over the day. This leads, for instance, to clicking on phishing links and opening attachements. Essentially, this means that the human factor is a risk that needs to be handled. Options to handle this risk are on the one hand technological solutions that detect and block potentially unwanted or malicious actions using threat intelligence and aritifical intelligence. On the other hand raising awareness is an important option.

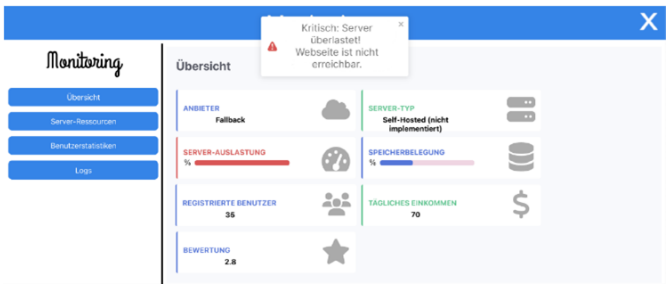
Common approaches to raise security awareness employ online or in-person training sessions which use questionnaires to check the success of the training. Although performed regularly, the events or even incidents caused by phishing do not decrease. Thus, another approach should be investigated as an alternative, in order to produce sustainable awareness. At the Institute for Cyber Security we have been developing Serious Games for this purpose. The idea is to play these games regularly, because it is fun to play and at the time to learn more about cyber security, thus creating a permanent awareness.

Our flagship Serious Game is called «PictureIT» and can be used for free in the current version [2], see also Figure 1.

Figur 1: PictureIT - Start Screen

The game is interactive and explains background information on IT security. The player has to build and operate an as secure as possible infrastruc-

ture to implement a picture upload service, similar to the well-known Instagram platform. In the build-phase the player has to make several decisions, which have certain costs. Because of a limited budget, decisions must be prioritized, especially concerning the security aspects. In the operation phase, incidents occur depending on the decisions made during the build-phase, and therefore depending on the existing as well as missing controls. The player must handle these incidents using a corresponding dashboard and tools like e-mail and web forms to inform the relevant authorities and affected users if applicable. This is shown in Figures 2 and 3.



Figur 3:PictureIT Incident Management

Figur 2: PictureIT -Form to inform the authorities:

Benefit for the user

Using Serious Games like PictureIT provides a means for continuous security awareness training, which combines learning cyber security with fun. In summary the benefits are:

- Continuous security awareness training
- More sustainable success compared to trainings that take place just every couple of monthes or yearly
- Play anywhere with just a browser

  Combines learning cyber security with gamification and therefore more fun, as our surveys show.
- Configurable and therefore flexible architecture that allows to add nearly arbitrary scenarios and to customize the game to the needs of a company, for example.

References

[1] HISCOX Cyber Readiness Report 2022 -Ransomware Update: https://www.hiscoxgroup.com/sites/group/files/documents/2022-11/22161-Hiscox-cyber-readiness-mini-report-Ransomware-update-2022_EN_0.pdf

[2] PictureIT: https://pictureit.ics.hdm-stuttgart.de/

[3] Roland Schmitz, Dirk Heuzeroth: "Serious Games for IT-Security Education", 1. ITG Workshop on IT Security, 2020. https://publikationen.uni-tuebingen.de/xmlui/handle/10900/100439

[4] Alina Arthur: "Konzeption und Erstellung eines Prototyps zur Darstellung von Security-Incidents im Serious Game PictureIT", Bachelor Thesis, Hochschule der Medien Stuttgart, 21.12.2023.

[5] Anne Naumann: "Konzeption und Erstellung eines Prototyps zur Behandlung von Security-Incidents im Serious Game PictureIT", Bachelor Thesis, Hochschule der Medien Stuttgart, 21.12.2023.

[6] Felix Messner: "Design and Implementation of an Event-Based Architecture of an Interactive Game Phase of a Cyber Security Game", Master Thesis, Hochschule der Medien Stuttgart, 04.06.2021.

[7] Martina, Harms: "Redesign der Benutzeroberfläche des Serious Game PictureIT und Evaluation durch Nutzertests", Bachelor Thesis, Hochschule der Medien Stuttgart, 10.11.2021.

[8] Johanna Kilgus: "Untersuchung und Realisierung von 2D- und 3D-Animationen im Web – Evaluation anhand des Serious Games PictureIT", Bachelor Thesis, Hochschule der Medien Stuttgart, 12.07.2022.

[9] Alexander Schimanko: "Konzeption und Design der Integration von Serious Games zur Erhöhung des Sicherheitsbewusstseins", Bachelor Thesis, Hochschule der Medien Stuttgart, 12.09.2022.

[10] Maria-Luisa Stefan: "Implementierung der Integration der Serious Games PictureIT und ITventures", Bachelor Thesis, Hochschule der Medien Stuttgart, 02.03.2023.

[11] Matthias Robert Koch: "Implementierung eines Serious Games zur Vermittlung von Security-Awareness", Bachelor Thesis, Hochschule der Medien Stuttgart, 21.09.2020.

[12] Anna Katharina Lindner: "Schwerpunkte zur Konzeption eines Serious Game zur Vermittlung von IT-Sicherheitswissen", Bachelor Thesis, Hochschule der Medien Stuttgart, 12.09.2020.

Prof. Dr. Dirk Heuzeroth
Founder
IT Security, Consulting, Development
Director
Institute for Cyber Security, Media University Stuttgart

Detailed information in the techL profile: IT Security, Consulting, Development Prof. Dr. Dirk Heuzeroth

Cyber threats from quantum computers: What is a Crypto Center of Excellence?

An article by Armin Simon, Thales Deutschland GmbH

Cybersecurity experts agree that the advent of quantum computing marks the dawn of a new era in cryptography. Quantum computing is making steady progress. Gartner estimates that by 2029, it will be able to weaken existing cryptographic systems to such an extent that they can no longer be used securely.

The National Institute of Standards and Technology (NIST) has selected the following four methods to replace current algorithms with quantum-safe ones:

- CRYSTALS-KYBER (key generation) and CRYSTALS-Dilithium (digital signatures) were both selected for their high security and excellent performance.
- FALCON has been standardized by NIST for use cases where CRYSTALS-Dilithium signatures are too large.
- SPHINCS+ was standardized to avoid relying solely on lattice-based cryptography for signatures.

The US Department of Homeland Security (DHS) and NIST have established a working group to help companies protect their data and systems: the „National Cybersecurity Center of Excellence (NCCoE) in the Migration to Post-Quantum Cryptography Project Consortium“.

Smooth transition

Companies should take stock of their current cryptographic systems and protected data and prioritize the transition of their systems. These early preparations will ensure a seamless and efficient transition once the new post-quantum cryptography standards are available.

DHS and NIST have defined the following six steps to help crypto teams implement:

1. Organizations should create an inventory of the most sensitive and important data sets that need to be secured over a longer period of time. This information can be used to analyze which data is at risk of being decrypted by a cryptographically relevant quantum computer in the future.
2. To ensure a seamless transition in the future, organizations should also conduct an inventory of all systems that use crypto technology.
3. Organizations should review which regulations in procurement, cybersecurity and data security need to be updated to meet the requirements of the post-quantum era.
4. Organizations should use inventories to identify where and why public key cryptography is used and then flag those systems as quantum vulnerable.
5. Prioritize the cryptographic transition based on the company's business units, goals and requirements.
6. Organizations should use the inventory and prioritization data to design a transition plan for their systems.

The concept of the Crypto Center of Excellence

For a successful post-quantum strategy, CISOs and other IT security leaders need the support of the entire organization. According to Gartner analysts, the most successful strategy for managing and controlling the use of cryptography is to build a centralized team with the necessary knowledge to formulate the appropriate policies for the organization. This is where the concept of the "Cryptographic Center of Excellence (CCoE)" comes into play. A CCoE can be defined as follows in terms of people, processes and technology: It is about educating and preparing employees. In addition, initiatives should be introduced to encourage other business units and the requirements, timeframes and needs of the organizational department should be made known so that they can be integrated into the post-quantum transition strategy.

Crypto-agility

Crypto-agility is an essential component of a CCoE. It is a strategy that strengthens a company's resilience to crypto threats. It allows companies to react quickly to vulnerabilities in cryptographic processes by replacing them with secure algorithms. In the post-quantum era, crypto-agility is critical when organizations need to protect themselves from quantum attacks on crypto algorithms.

Armin Simon
Regional Sales Director Germany,
Data Protection
Thales Deutschland GmbH

Platforms and Infrastructure to Operate GenAI in Your Company's Basement

Hosting, operating and monitoring generative AI (GenAI) solutions is challenging, in particular if cloud resources provided by OpenAI or Azure cannot deliver in terms of privacy and cost efficiency. How can companies build and operate platforms for hosting foundation models as part of a GenAI solution on their own?

An article by Dennis Wegener & Benny Stein, Fraunhofer Institute for Intelligent Analysis and Information Systems

In recent years, generative AI has revolutionized various industries by enabling the creation of highly sophisticated and creative outputs. However, the journey to harnessing the full potential of generative AI has just begun, especially for organizations opting to self-host these solutions. Unlike in the case where cloud resources from OpenAI, Microsoft Azure or their competitors are used, self-hosting requires extensive computational power, substantial data storage, and robust infrastructure — but also offers tempting benefits like data privacy and cost efficiency. In this article we discuss self-hosting of generative AI and report on the technical and operational hurdles involved. Additionally, we will provide detailed information on how we have built our own platform for multi-modal foundation models, offering insights into the necessary steps and considerations for successful implementation.

Generative AI and foundation models have caught significant attention after the release of ChatGPT in 2022. Today, interest in these models has expanded to numerous fields and business units, highlighting the substantial demand for AI solutions based on foundation models. Many instances of generative AI are available: *Closed-source* foundation models and GenAI services are generally provided via commercial APIs or public cloud platforms, whereas *open-source* alternatives are distributed through model artifacts ("checkpoints") on platforms like Hugging Face[1]. In both scenarios, getting a grip on high-performance and cost-efficient generative AI services is challenging. So far, not many production-ready on-premises solutions exist yet. Additionally, the alarming increase in concerns about implementation costs reported in [1] shows the necessity of alternative solutions to public cloud services, especially as costs for public cloud services usually scale linearly with usage.

Numerous platforms are available for accessing, demonstrating and comparing large language and more general foundation models. These include[2]:

1. **OpenAI**[3]: The most prominent platform offering ChatGPT, various versions of GPTs, DALL·E, and Sora for text, image, and video generation as a service based on (closed-source) models.
2. **Amazon Bedrock playgrounds**[4]: A platform for testing inference on different models before they can be deployed in an application (non-public). Additionally, PartyRock[5] provides a code-free playground for building AI applications based on Bedrock.
3. **NVIDIA AI Playground**[6]: This platform allows users to test models from an increasingly larger catalog via model-specific demo user interfaces (UI).

[1] https://huggingface.co/
[2] Note that this list is incomplete and rapidly evolving. The snapshot described here may soon become outdated.
[3] https://openai.com/
[4] https://docs.aws.amazon.com/bedrock/latest/userguide/playgrounds.html
[5] https://partyrock.aws/
[6] https://www.nvidia.com/en-us/research/ai-playground/

4. **Databricks AI Playground**[7]: A playground to test, prompt, and compare different large language models (non-public).
5. **Vercel AI model comparison**[8]: Focused on an SDK for comparing different models, this platform also aims at simplifying the development of Java-/TypeScript interfaces.
6. **Hugging Face** offers the largest collection of open-source models, including an inference API and a UI for testing individual models.

In addition to platforms where models are hosted, there are platforms that serve as gateways to other providers. These gateways aim to simplify the comparison and replacement of LLMs by offering a more unified interface:

7. **Kong AI Gateway**[9]: Currently supports the providers OpenAI, Cohere, Azure, Anthropic, Mistral and some self-hosted models.
8. **MLflow Deployments Server**[10]: Can be set up locally in minutes, with providers specified by a simple configuration file.

In the following, we outline how to build a self-contained, on-premises infrastructure for inference based on multi-modal foundation models that operate on text, images, audio, embeddings, and their combinations. It is designed to comply with data privacy, access management, IT security, trustworthiness, and — most importantly — usability for a wide range of downstream research and business scenarios. Our own instance of this setup is used by AI researchers and engineers to rapidly develop proofs-of-concept for GenAI-centric applications. Moreover, it is regularly used in workshops for companies beginning to adopt GenAI for their businesses.

Use Cases, Models and Features

The platform addresses all common conversation scenarios: text in—text out (for text generation and chatbots), text in—audio out (for speech synthesis), text in—embedding out (for retrieval systems), text in—image out (for image or more general content creation), and audio in—text out (for transcriptions, speech recognition and audio chatbots). Each of these scenarios can be supported by different capable open-source models (with permissive licenses).

The following models have been tested on various tasks and are currently accessible in our instance:

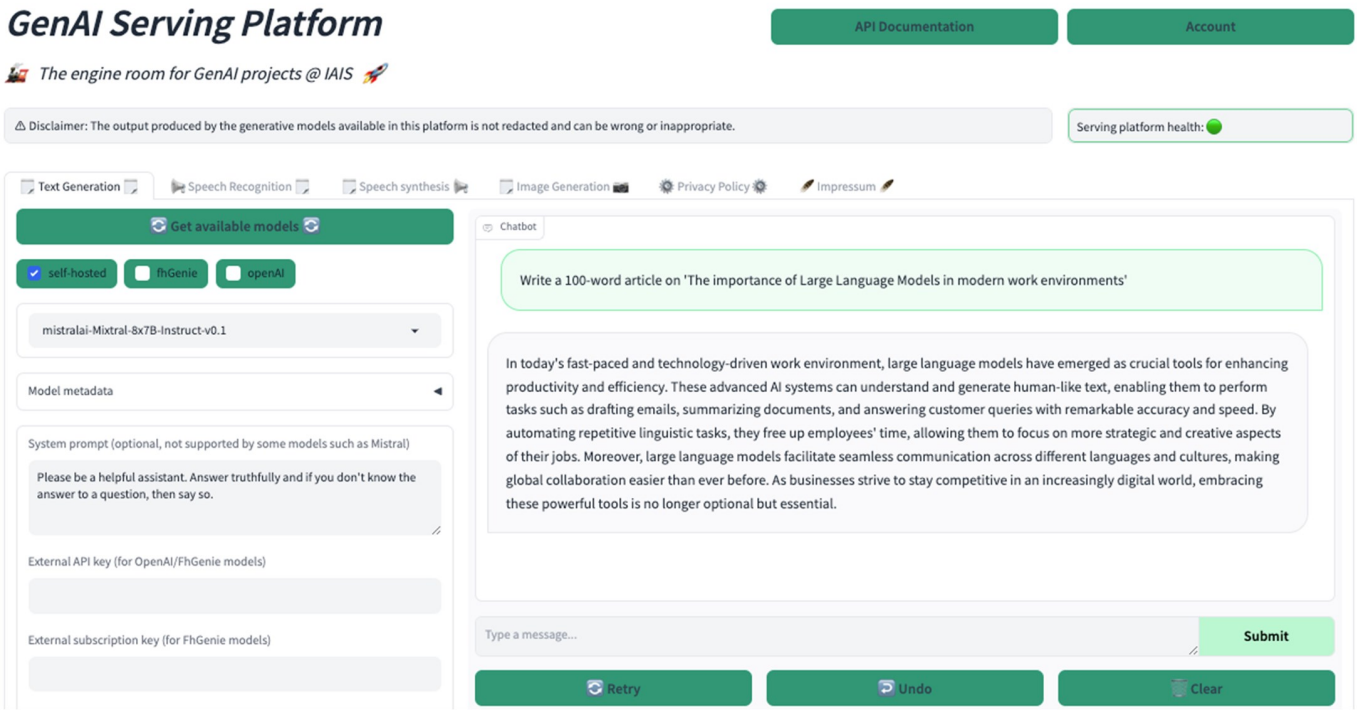


Fig. 1: User Interface for immediate model access and exploration

[7] https://docs.databricks.com/en/large-language-models/ai-playground.html
[8] https://sdk.vercel.ai/
[9] https://docs.konghq.com/gateway/latest/ai-gateway/
[10] https://www.mlflow.org/docs/latest/llms/deployments/index.html

Model	Input	Output
Meta: Llama 3 8b & 70b chat	text	text
MistralAI: Mistral-7B-Instruct-v0.3	text	text
MistralAI: Mixtral-8x7B-Instruct-v0.1	text	text
StabilityAI: Stable Diffusion SD-XL 1.0	text	image
OpenAI: Whisper-large-v2	audio	text
primeLine: Whisper-large-v3-german	audio	text
NVIDIA: FastPitch (en-US)	text	audio
Meta: MMS text-to-speech (DE)	text	audio
SentenceTransformers: all-mpnet-base-v2 (embedding model)	text	vector

Each of these I/O combinations requires a different type of user interface, which is why we have a separate tab for each modality in the UI shown in Fig. 1. In addition, the functionality of the models is accessible through a dedicated API, which allows for larger workloads and in general more traffic on the system. After all, the applications we build on top of the models don't use the UI.

About the Technical Architecture

The architecture contains the following elements:

1. *Frontend*: The user interface shown in Fig. 1 is based on Gradio. It provides different tabs for Text Generation, Automatic Speech Recognition, Speech Synthesis and Image Generation. In each tab, the user can select a model from the list of available models and can interact with it. The frontend communicates with an Identity Access Management (IAM) system for authentication and with the API server for model access and inference.
2. *Backend*: We use a node concept for the model backends. Each node represents a model serving component which serves a single or multiple models. We use NVIDIA Triton Inference Server, vLLM and Hugging Face's Text Generation Inference (TGI) as serving components. The nodes provide standard interfaces and are KServe- or OpenAI-compatible.
3. *API*: The API server is written in Golang and offers clients a standardized interface to various node protocols of the backends by adapting the inference requests. It supports all conversation scenarios described before. Moreover, responses can be requested to be synchronous, asynchronous (via sequential queueing) or streamed. Asynchronous inference results are cached until retrieved by the user.
4. *Moderation*: Requests and responses can optionally be sent to a moderation service that uses classifiers for toxicity, prompt injection and personally identifiable infor-

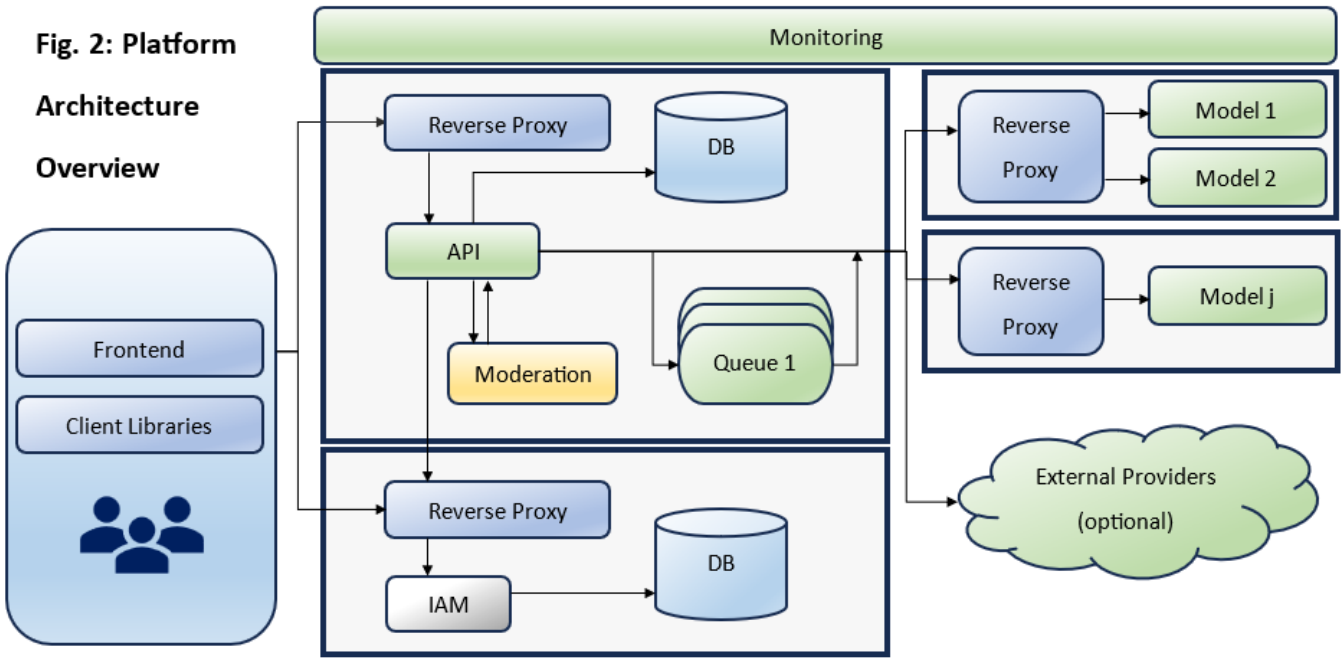


Fig. 2: Platform Architecture Overview

mation to detect content that should be filtered.

5. *Databases*: We use the following two database instances: Redis for caching results per user and storing global and node configurations, and a PostgreSQL database for storing all user-related information. The latter is only accessed by the IAM system.

6. *Monitoring*: We provide health and metrics endpoints for the frontend and the API server and use the health and metrics endpoints that the model backends provide. The metrics endpoints are consumed by a Prometheus instance and visualized in Grafana dashboards to gain insights about traffic, cost, energy consumption, GPU (= Graphics Processing Unit) load and usage statistics for models and users.

Lastly, the architecture is extensible and checks common security boxes like TLS communication between all servers, RBAC for the platform and a dedicated IAM system that takes care of authentication and authorization. This enables usage in production settings.

Technical Requirements

The technical requirements to run such an infrastructure (with and without tweaks) are as follows:

Foundation models require GPUs for performance reasons. The model size correlates with the GPU device's VRAM. A rough but convenient estimate is the following: Twice the number of model parameters (in billions) approximately gives the required VRAM (in GB), so 2 x 7 = 14 GB VRAM for a 7B parameter model. For up to four 7 billion parameter models, a single NVIDIA A100 or H100 GPU with 80 GB VRAM is sufficient (with some necessary overhead). With the use of quantization techniques — a common tweak to reduce the effective model size — even larger models fit on such a GPU. As an example, a 4-bit quantized version of the powerful 8x22B Mixtral model developed by Mistral AI fits on such a device. Of course, quantization can also be a cost-effective option for hosting models on much smaller GPUs. After all, the price tag on NVIDIA A100 and H100 GPUs is impressive and cheaper (but less performant) GPUs like the V100 or some of the NVIDIA RTX 3000/4000 series do the job in smaller settings, too. Other requirements are quite modest, as the machines only require standard CPUs, a common network and should have a containerization software such as Docker installed. So, the biggest hurdle is the cost factor of the GPUs.

Wrap-up

We showed how to set up an infrastructure for foundation models that allows for cutting-edge demonstrations of their capabilities. This infrastructure can run in on-premises production environments. It allows for UI- and API-based access and provides access management and robust monitoring.

Our solution is already used in many customer and research projects, with increasing demand. For more information, just get in touch with us – or have a look at our various activities and offers around Generative AI [2].

References

[1] https://lucidworks.com/ebooks/2024-ai-benchmark-survey/
[2] https://www.iais.fraunhofer.de/generative-ki

Dr. Dennis Wegener
Teamlead MLOps
Fraunhofer IAIS

Dr. Benny Stein
MLOps Engineer
Fraunhofer IAIS

Detailed information in the techL profile:
Fraunhofer IAIS

heylogin GmbH

We make security simple for users

Although the world is becoming increasingly digitalized, we still use passwords for our IT security. With software as a service becoming the norm, the number of passwords that users need is getting increasingly unmanageable.

heylogin GmbH was founded to change this. The most important goal: to eliminate the password. To achieve this goal, we rely on modern technology and hardware encryption. Since 2020, our focus has therefore been on our password manager heylogin.

As a German company, not only data security but also data protection is a major concern for us, which is why we rely on German servers, European service providers and are GDPR-compliant.

2-Factor secure by design

heylogin relies on hardware encryption instead of a master password and uses the smartphone's or security key's secure element. This means that every login is securely encrypted and employees do not have to think up and remember passwords. Another important component is end-to-end encryption with modern cryptographic algorithms. This ensures that only a person with authorization can access the stored data.

When used, the 1-click overlay offers the convenience of a single sign-on solution (SSO) on every website without incurring additional costs. This is an advantage for both users and admins, as heylogin can be easily integrated into existing SSO use without employees having to change their habits. Logins can also be shared via teams, with multi-level rights for team members.

For admins, the management interface offers all the functions needed to manage the organization: from disconnecting devices in the event of loss to the audit log and the integration of cloud services such as Azure Active Directory or Google Workspace, everything is included.

The benefits for our users

The most important benefit is the freedom from passwords. heylogin saves and generates passwords automatically, so nobody has to bother with Post-It's and weak passwords anymore. Instead, you only need to unlock it once a day with your smartphone or Security Key and you can log in anywhere with just one click. With the new Global Login Search feature, desktop apps can also be operated. Taken together, this leads to greater acceptance and usability, even among less tech-savvy users.

Admins can manage everything in one place: create new accounts and prepare onboarding, share and track passwords and easily approve new software access. All without the risk of shadow IT. This effectively eliminates the password in everyday life and replaces it with a convenient and secure 2-factor mechanism.

Dr. Dominik Schürmann
CEO
heylogin GmbH

Detailed information in the techL profile:
heylogin

Primary Target GmbH

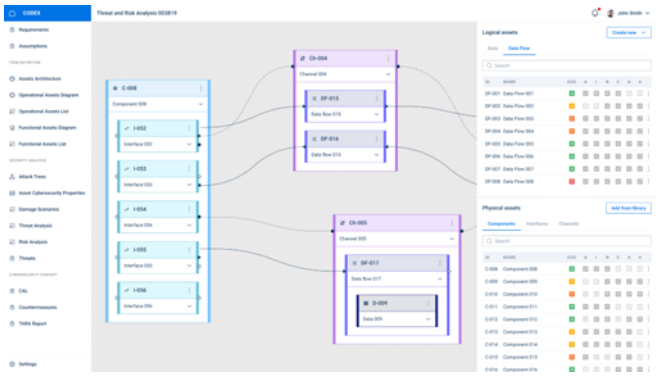
About the company

In 2022, Oscar Angress & Jürgen Vollmer founded the cybersecurity company Primary Target in Munich, Germany, to develop a software tool to support and automate the threat analysis and development process for secure industrial objects. With a staff of 12, the company is initially targeting the private and commercial vehicle market, but is expanding to include defence, medical devices, ships, aircraft, drones, machinery and more. The technology has won several awards, and the risk assessment is patented. The development of the software is supported by the German government.

Technology

The increasing complexity of industrial products leads to insecure products and makes automated processes and the use of algorithms an absolute necessity. Describe the secure workflow:

- Define scopes and assign user rights
- Import architecture and/or electronic signals.
- Establish requirements and assumptions
- Build or import functional data flow
- Tag data or assets with security priorities down to the data level.



Results of the CodeX software tool

- Automatic assessment of potential risks based on threat scenarios and generated attack trees. The software automatically generates possible scenarios to visualise which assets require special security treatment to ensure overall functionality. AI-based result analysis and user assistance to protect against possible attacks is planned.
- Our ever-growing database contains several thousand threats that are already well categorised and assessed using patented algorithms.
- The classification of all threats, vulnerabilities and countermeasures is based on the OSI layer model. Taking into account cybersecurity properties, the process can be automated to an unprecedented level.
- The software is fully customizable allowing you to build your own plugins or interfaces to e.g. external penetration tests labs or proprietary tools.
- A countermeasure selection process for potential threats to assets is built in.
- Apply the most effective countermeasure or sequence to protect. Optimisation can be performed iteratively by evaluating the impact of each countermeasure.
- The result is a guided Threat Assessment and Remediation Analysis (TARA).
- Individual dashboards to visualize workflows, risks and protection

Benefit for the user

The software tool enables you to comply with regulations (such as ISO 21434), secure development and manage the complexity of the process.

- Visualized security flow
- 90% faster time to market / production
- 35% reduction in development costs
- Reduced risk of attacks, penalties and fines
- Significantly reduce human error
- TARA of a component can be reused ten times faster and cheaper for any other customer
- Automated compliance and security audits
- Fast, fact-based risk analysis

Oscar Angress
Technical Lead
Jürgen Vollmer
Sales & Marketing
Primary Target

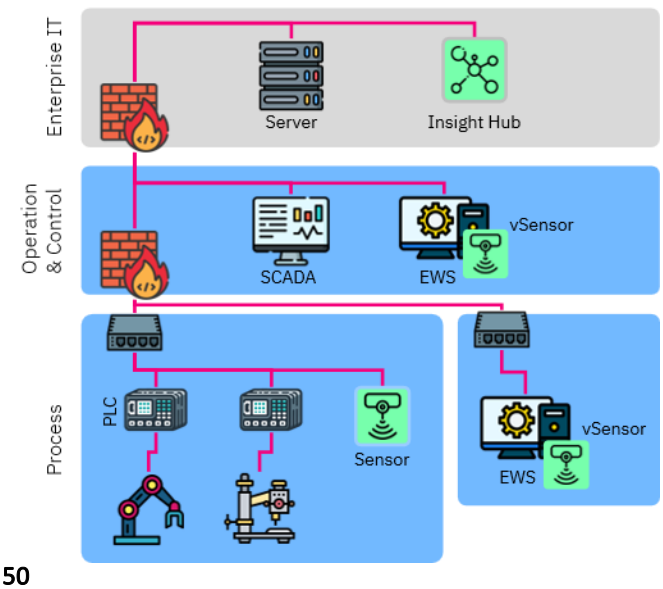
SANCTUARY Systems GmbH

About the company

Founded in 2020, SANCTUARY specializes in providing cutting-edge cybersecurity solutions tailored for industrial automation and space applications. Our expertise includes on-device security solutions for embedded systems using virtualization and hardware-backed trusted computing. We are pioneers in trust technologies between devices, implementing robust Public Key Infrastructure (PKI) to ensure secure communications even in challenging network conditions. Finally, our OT Asset Management Solution, SANCTUARY Insight, delivers comprehensive visibility and control over operational technology assets.

Technology

Struggling to manage and secure your growing OT landscape? SANCTUARY Insight empowers you to take control with a comprehensive, automated solution. Our innovative platform seamlessly blends passive and active discovery, providing unparalleled visibility into your entire OT landscape. Effortlessly identify all devices, from network equipment to field sensors, and gain granular insights with native protocol communication, ensuring zero disruption to your critical operations.



Actionable security recommendations guide you in addressing vulnerabilities, while intuitive dashboards keep you informed and in control. Insight utilizes sensors installed within the production network to identify all IT and OT devices. These sensors can be deployed as hardware or software components and gather detailed information about each device.

Benefit for the user

Our OT Asset Management solution offers a seamless and efficient approach to safeguarding your operational technology environment. By prioritizing proactive risk management, we eliminate the frustration of false-positive security alerts, allowing you to focus on what matters most. Say goodbye to the tedious task of manually keeping asset lists; our solution automates this process, ensuring accuracy and saving you valuable time. Experience zero disruption to your operations and enjoy the flexibility of a software-based sensor, or utilize cost-efficient hardware provided by us, eliminating the need for costly investments. Whether you prefer a one-time scan or continuous monitoring, the choice is yours, giving you the control and peace of mind you need.

- Hybrid Asset Discovery
- Change Management Support
- Vulnerability Management
- Proactive Risk Management – no false alerts

Dr.-Ing. Emmanuel Stapf
Managing Director
SANCTUARY Systems GmbH

Detailed information in the techL profile:
SANCTUARY Systems GmbH

Survey of technologies

We regularly consult experts on their current needs, with tool research being a frequent request. This chapter highlights key technologies we find noteworthy, providing brief product summaries and links to detailed datasheets and contacts in our techL database.

All innovations be found in the technology database

techL

www.techl.eu

Apheris

Apheris is the leading federated machine learning and analytics platform that enables organizations to build data applications and AI across boundaries without sacrificing data privacy or intellectual property. Our platform allows businesses to safely work across organizations, geographies, or use cases, while seamlessly integrating into existing tech stacks. As data privacy regulations continue to evolve, Apheris provides a compliant and secure solution for organizations to extract value from their data. With Apheris, you can confidently drive innovation and growth through the power of data.

techL

Asvin

asvin provides a solution to distribute updates safe and secure over the air to IoT devices. asvin is using de-centralized technoligies to provide a resilient and secure update solutions for devices during their lifecycle. By asvin the security state of devices can be monitored and reports on threat landscapes can be generated.

techL

Authada

AUTHADA is a cybersecurity company that revolutionises existing identification procedures with its innovative digital identification and signature solutions. Banks, insurers, telecommunication providers or even eCommerce companies can use AUTHADA to identify their customers online or on-site in seconds and in compliance with the law via the electronic identity of the identity card. Due to the Qualified Electronic Signature, contracts no longer require a handwritten signature at the regulatory level and can be con-cluded completely digitally. The solutions thus provide the optimal basis for digital transformation and process optimisation in companies.

techL

Betterscan

The Only Open Cybersecurity Software that secures both Cloud and Apps. A simple and powerful DevSecOps software to automate thousands of checks and eliminate human errors in Source Code and Cloud Infrastructure. Integrateable into anything.

techL

Bitahoy

Most cyber security solutions focus on fixing the symptoms instead of the root cause. That's why we developed the industry's most complete cyber risk management platform, created to give our clients a complete overview of their risk posture. Founded in Germany, we help our customers worldwide to bridge this gap and own their cyber risk in their daily operations.

techL

BreakinLabs

BreakinLabs specializes in penetration testing and IT security audits. We test the customer's IT systems using the methods of hackers and uncover dangerous as well as security-relevant vulnerabilities. In addition, we are currently creating an interactive platform for prospective and experienced IT specialists. In this way, we are imparting the necessary know-how for independent security audits of the company. For our commitment in the area of offensive IT security, we were recently appointed partner of the BSI project "Alliance for Cyber Security".

techL

CodeShield

CodeShield empowers software developers to build secure software and integrates seeminglessly into the software development process. Based on new research technologies, CodeShield detects known and yet unknown vulnerabilities. CodeShield does not only scan the application code but also included third-party libraries.

techL

Comcrypto

The comcrypto Mail Exchange Gateway (MXG) is an email gateway for DSGVO-compliant protection of email sending. MXG protects 100% of all outgoing emails with minimal effort for senders and recipients.
Advantages:
Automatically secure email sending
Minimize disruptions to email workflow
Visibility into the current security level of outbound email and associated receiving servers
No need to install client software or plug-ins

techL

Comuny

With Trinity Identity Wallet software development teams and system integrators design mobile authentication solutions cost effective and compliant to the new European legal framework (eIDAS 2.0). They reduce their effort by integrating the mobile SDK with numerous plug-and-play features. Nearby they design their identity use cases flexibly in the absence of UI/UX design restrictions. The decentralized data management allows secure storage of personal data in a mobile wallet and data management on the mobile device. Trinity moves key identity provider functions from data center into a mobile white label SDK. This enables a scalable an cost effective cloud operation of still necessary backend components even for highly regulated markets.

techL

Crashtest Security

Crashtest Security Suite is an agile pentesting software for web applications and API interfaces. The intuitive and simple user interface enables holistic security reporting and visualizes the scan history of a software project. The application allows easy export of scan results, making the current security status measurable and visible. The automation of penetration testing creates the possibility to test continuously by starting scans at specific time intervals or via webhook from a CI/CD toolchain. A free wiki integrated in the application supports the developer in fixing found vulnerabilities.

techL

DeepSign

Auch die besten Sicherheitsvorkehrungen garantieren im Falle einer Cyber-Attacke keinen ausreichenden Schutz, wenn der Faktor Mensch das Ziel der Angreifer darstellt. Um diese Angriffsfläche zu eliminieren, bieten wir mit INVISID eine KI-basierte Authentifizierungsmethode, die einen validen Nutzer anhand eines Verhaltensmusters aus Maus- und Tastaturinteraktionen verifiziert. Diese vollständig automatisierte Technologie schützt den Nutzer durchgehend, unbemerkt und ohne Komforteinbuße vor dem Diebstahl seiner digitalen Identität.

techL

deviceTRUST

The central contextual platform for enterprises, enabling users to work with their digital workspace from any location, with any device, over any network and at any time, giving IT departments all the information and control they need to meet all security, compliance and regulatory requirements.

techL

Devity

DEVITY is your specialist in IT security for the Industrial Internet of Things. Based on the research of the team members, the team develops and operates an application for efficient configuration and installation of IoT devices such as sensors, industrial computers and machines to simplify access to secure operation of IoT infrastructures for industrial companies across Europe. The solution consists of two components - an SDK for devices and the KEYNOA web application. A feature of the solution is unique identities that are assigned to each device produced. DEVITY ensures that these identities are passed down the supply chain in a trusted manner and can be used for mass installation.

techL

emproof

Emproof delivers high levels of security and IP integrity for embedded systems, using unique techniques that protect algorithms and data while securing the entire device. Our solution, Emproof Nyx, prevents reverse engineering, securing your valuable intellectual property and protecting against exploitation attacks.

techL

Enginsight

Whether it's applications, servers, agents, IoT devices or industrial equipment, Enginsight provides LIVE security monitoring for all applications and devices on the network. A high-performance, out-of-the-box solution for IT security and monitoring. The user can start directly with all security analyses without configuration. After installation (<1h), the most dangerous attack vectors can be captured and evaluated (e.g. unauthorized access, hacker attacks). The fast implementation and immediate provision of all relevant analyses paired with an economical and transparent pricing model for SMEs is unique worldwide.

techL

F5 Networks GmbH

As enterprises embark on digital and autonomous transformation, they are adopting multiple cloud providers to consume best of breed platform services and moving their applications closer to end-users or machines that are generating enormous amounts of data. Our mission is to enable customers to harness the power of this distributed applications and data with our platform for distributed cloud services. This platform Volterra provides the ability to build, deploy, secure, and operate applications and data across multi-cloud or edge. Volterra operates a SaaS service to provide application management, infrastructure, and secure connectivity services across distributed customer sites in public cloud, private cloud, or edge sites.

techL

Fraunhofer Institute for Intelligent Analysis and Information Systems IAIS

As part of a leading applied research organization, the Fraunhofer Institute for Intelligent Analysis and Information Systems IAIS in Sankt Augustin/Bonn and Dresden excels in AI, Machine Learning, and Big Data. With 380 employees, it supports companies in optimizing products, services, and developing new technologies. Fraunhofer IAIS drives digital transformation with AI applications in industry, health, and sustainability, and offers training, education, and AI testing for security and trustworthiness.

techL

Goriscon

The data-driven solution "embedded GRC" is the core product of GORISCON and enables companies to implement information security, data protection and risk management in a targeted, efficient manner: integrated, intelligent, automated. As an integrated management system, eGRC forms the foundation for controlling and evaluating company-specific security needs. eGRC allows a cross-dimensional view of the security status: like the Magic Cube, individual elements, the components, are not bound to one dimension, which means that a dimension can be viewed in different forms depending on requirements. The software user is spared a high degree of complexity: the integration of working fields is automated by the eGRC Cube.

techL

Hanko

Hanko Authentication Service enables passwordless, decentralized FIDO authentication and prevents credential compromise through phishing, data breaches and password reuse. The focus is on user experience and open web standards.

techL

heylogin

Heylogin replaces passwords with a swipe-to-login on the phone. It works with all websites and saves 3 hours / month of your employees' time. For project managers, it eases on- and offboarding of employees. For CEOs, it gives back control over all your companies' logins.

techL

Inlyse

Inlyse is a cutting-edge AI-based IT security platform which identifies malware and cyber-attacks within seconds. It is the first IT security solution that combines intelligent picture recognition mechanisms with self learning neural networks in order to identify and stop advanced malware, zero-day exploits and APT attacks without regular updates. While existing solutions solve just one problem at a time, our team has built a secure, useful, & easy-to-use product for everyone. It includes easy integration, management, and cloud access. The modular system architecture of inlyse enables enterprises to select and use our complementary IT security plugins to close specific weaknesses in their IT infrastructure in a fast and easy way.

techL

inSyca IT Solutions

In order to remain relevant for their customers in the future, aiming to offer excellent service, companies need to set focus on modern technologies and automated communication processes. In that, e.g., Electronic Data Interchange (EDI) and Cloud Computing play a crucial role when meeting the requirements in B2B and e-commerce.
As inSyca, we have fully dedicated ourselves to e-business communication, providing solutions to connect business partners for an error-free, smooth order processing and an efficient supply chain. We offer guidance and support for companies wanting to meet the technological challenges of digital transformation.

techL

IT Security, Consulting, Development Prof. Dr. Dirk Heuzeroth (Einzelunternehmen)

IT Security, Consulting, Development Prof. Dr. Dirk Heuzeroth (Einzelunternehmen) offers security and data protection services, focusing on implementing and auditing information security management systems and controls, as well as pentesting. It provides services as a data protection officer, consulting in secure software development, and custom training in IT security, hacking, and secure software development. The company also performs custom software development and is developing a health app.

techL

Kaspersky Labs GmbH

Kaspersky, founded in 1997, is a global cybersecurity company. Half of its 5,000 experts focus on in-house R&D. It protects over a billion devices with leading threat intelligence and security solutions, serving businesses, critical infrastructures, governments, and consumers. Its portfolio includes advanced endpoint protection and specialized solutions, safeguarding over 220,000 corporate clients.

techL

KraLos

In an increasingly digitalized world, cyber threats are everywhere. At KraLos, we understand the challenges businesses face and provide advanced cybersecurity solutions to protect your digital presence. Our services at a glance: Web Application Security: Protect your web applications from attacks and data leaks with WEBOUNCER. Secure communication without a backdoor or connection to the Internet with SHADOWKEY

techL

Nexis GmbH

NEXIS Controle is the technology-leading software and comprehensive solution for cross-system analysis, risk assessment as well as visual (re-)modeling of authorization structures. The application sets itself the goal of being an easy-to-understand platform for IT and also business departments to work together on secure role and authorization management. NEXIS Control is manufacturer-independent and supplements all existing IAM solutions with powerful analysis, modeling and collaboration functions or as a stand-alone solution for successful implementation of existing access governance and automation requirements.

techL

Nviso

NVISO Eagle Eye is a threat hunting solution for enterprise networks. It allows the security team and analysts to centrally collect logs from clients, servers and network devices such as firewalls, analyze them using various advanced methods and thus detect cyber attacks and incidents in the network and initiate appropriate countermeasures. Eagle Eye uses a specially developed EE Outlier Engine in addition to well-known mechanisms such as YARA Rules to detect irregularities and thus differs from previous SIEM solutions.

techL

Onekey

ONEKEY is a specialist in automated security & compliance analysis for devices in production (OT) and the Internet of Things (IoT). ONEKEY independently analyzes firmware for critical security vulnerabilities and compliance violations via automated "Digital Twins" and "Software Bill of Materials (SBOM)", without source code, device or network access. Vulnerabilities for attacks and security risks are identified in the shortest possible time and can thus be specifically remediated. The solution enables manufacturers, distributors and users of IoT technology to quickly automate security and compliance checks before use and 24/7 throughout the product lifecycle.

techL

Pro4bizz

SIEM 360 plus with Service Management via REST API: The extension allows the integration of IBM QRadar SIEM with Matrix42. It is based on the SIEM 360 system customized for the customer, including individual adaptation to the IT infrastructure, fine-tuning of the rules and implementation of specific use cases. The close integration of service management into the SIEM system creates an end-to-end security workflow. Security incidents are automatically detected and generate a service ticket in Matrix42. Processing is done individually based on the context data provided. After successful problem resolution, the status of the ticket is updated in Service Management and the status of the assigned security incident is automatically adjusted in SIEM.

techL

Red Sift

OnDMARC is a cloud-based application that enables organisations to quickly configure SPF, DKIM and DMARC for all their legitimate email sources. This instantly blocks any email impersonation based phishing attacks. OnDMARC also gives you totally visibility of your email landscape giving you a clear idea of the scale of the phishing problem specific to your organization. Only DMARC gives you insight into what's happening globally, on your domain, and not just attacks that cross your network boundary. Dynamic SPF is a unique feature to OnDMARC which helps users overcome the inherent problem of 10 SPF lookup limits and mitigates the need to manually make changes to your DNS for updates.

techL

SANCTUARY Systems GmbH

SANCTUARY offers advanced cybersecurity solutions for industrial automation and space applications. We specialize in on-device security for embedded systems using virtualization and hardware-backed trusted computing. As pioneers in device trust technologies, we implement robust PKI for secure communications in challenging networks. Our OT Asset Management Solution, SANCTUARY Insight, provides comprehensive visibility and control over operational technology assets.

techL

Sematicon

sematicon AG offers easy-to-implement and technologically trend-setting solutions for the industry, which aim at protecting business-critical processes effectively without influencing applicable standards. At the same time we fulfill all requirements for increasing data protection during the exchange of sensitive data – be it via old or new systems. Our products are based on an architectural design according to international and well-established standards. They are characterised by transparent operation and high cost efficiency. In addition to sophisticated firmware solutions, our house's portfolio is completed with high-quality and industrially usable hardware solutions. sematicon-solutions are 100% made in Germany.

techL

Sepio Systems

Sepio is here to provide the actionable visibility to continuously manage risk of all known and shadow assets at any scale. Actionable visibility, objective truth, and infinite scalability are the pillars of Sepio's Asset Risk Management (ARM) solution that enable companies to grow securely and efficiently. Our mission is to instill confidence for companies who need to manage risk of their continuously expanding, uncontrolled ecosystem of connected assets. With Sepio, security and IT teams will manage asset risk with confidence and painlessly, relieving them of the burden of complicated and expensive deployments, noise, or cost.

techL

ShardSecure

Regain control of your data with ShardSecure. In the face of rising storage costs, cyberattacks, and operational complexity, we help companies simplify their data protection. Our innovative solution lets companies enjoy the flexibility and cost savings of securing their data wherever they want: on-premises, in the cloud, or in hybrid-cloud architectures. Organizations can enjoy stronger security and resilience without surrendering control of their data, putting their confidentiality at risk, or redesigning their workflows. ShardSecure provides strong data privacy, robust data resilience, native ransomware protection, agentless file-level protection, easy plug-and-play integration, and more.

techL

Smart Data

With PREVISEC, we are building a single source of truth for businesses to ensure their security and risk management compliance, organize effective incident response and create state of the art crisis preparedness and management. The platform for incident and crisis management defines a centralized data pool and provides (management) stakeholders with an extremely clean interface. This makes it effortless for response teams to keep everyone up to date on their activities and progress. Planned response based on incident scenarios supports notification and fast reaction in case of incidents. Any actions taken with reference to security incidents are documented in PREVISEC.

techL

Vereign

Vereign establishes authenticity in digital interactions by connecting verified identities via computing devices, applying them to electronically sign documents, wordpress articles and e-mails and securing hashes of the digital exchange with one-time keys on the blockchain for an immutable audit log. Designed as a self-sovereign identity suite and federated authentication layer that resides with the user, both corporations and individuals can run their own instances and use it directly from within major e-mail clients and office suites. The interactions result in a verified and active address book disclosing personal data selected and maintained by the contacts themselves.

techL

XignSys

The XingSys Servicekonto.Pass was developed specifically for the requirements of public administrations. With the help of the SK.Pass and the personal smartphone, citizens can authenticate themselves easily, securely, and without a password to all digital administrative services that require the confidentiality application to be substantial and low-code according to eIDAS. The SDK is available as a native library for Android and iOS and can be easily and quickly integrated into software ecosystems thanks to "low-code integration".

techL

ZecOps

ZecOps is a stealth mode cybersecurity automation company headquartered in San Francisco with offices in Tel Aviv, London, Singapore and Buenos Aires. ZecOps learns from attackers' mistakes with the goal of discovering the course of action and objectives of the entire campaign, burn the threat actors exploits & persistence mechanisms and increase the attacker's campaign costs.

techL