United Innovations

Survey of Tools for Secure Infrastructures and Processes

Release 2 / 2023

www.security-innovations.eu

Foreword

Dealing with risks is by no means limited to the area of cybersecurity. The pilots of major airlines are also looking closely at the question of how to ensure a safe flight experience as an airline. There, they are pushing to anchor security goals in the target agreements of all managers. This makes safety part of the corporate culture.
A similar approach is being applied to the digital transformation of companies. Here, too, it has been learned that these projects will only be successful if the corporate culture and the way employees think are changed in a positive way. What's more, you can't be content with letting employees "know" through general communication, but you have to motivate them to want to complete the projects successfully despite any difficulties that arise. This applies in particular to support from top management and the will of middle management.

If you classify the transformation from a company that appears to be more or less fair game to a "security-first company" as a strategic change project in the security sector, then you have to address, motivate and focus the entire company on the goal, from the top down to the technical experts. This goes well beyond the usual awareness campaigns. Every person in the company must feel called upon to point out weak points and immediately eliminate deficiencies in their own environment.
To achieve this, top management, for its part, must issue clearly understandable and measurable goals and quickly provide the resources needed to achieve them. Employees, for their part, must act prudently and without wasting time, e.g., immediately follow the security recommendations of BSI and others, constantly scrutinize their security measures and analyze the capabilities of attackers.
In the hope that this issue of our Technology Survey will provide you with one or the other piece of assistance, I wish you a lucky hand in mastering your tasks.

Dr. Gerd Große

Head of United Innovations
Chairman of the Board of GFFT e.V. &
Managing Director of GFFT Technologies GmbH

Content

Calendar

18/10/2023
14:00-14:45

Use Case Award: High Speed Encryption (german)

As part of our Use Case Awards, we present innovative use cases in the area of IT security. The participants can discuss these and evaluate them as a jury. The three best-rated use cases of a season pitch for victory at a final event (F2F). This event will focus on the topic of High Speed Encryption. Thales Security will present a use case. Info & Registration

09/11/2023
15:30-17:30

GFFT Consortium Project: Plant Security (german)

In partnership with NTT, the Security Lab offers practical support to industrial companies dealing with complex facility security concerns. We aim to gather and share insights on challenges and solutions within these organizations, collaboratively devising solutions for their most pressing issues.
Info & Registration

16/11/2023
15:30-17:30

GFFT Consortium Project: Zero Trust (german)

Join the GFFT Security Lab for practical support in detecting and preventing cyber threats using the Zero Trust Security Framework. We help businesses exchange knowledge, address challenges, and implement effective security measures. Info & Registration

28/11/2023
15:30-17:30

GFFT Consortium Project: Innovations in IT Service Management & Process Mining (german)

Service management deals with process optimization and automation in companies. It comprises IT Service Management (ITSM) and Enterprise Service Management (ESM). Modern solutions transform manual ways of working into digital workflows. The Security Lab supports companies in overcoming challenges and solutions. Info & Registration

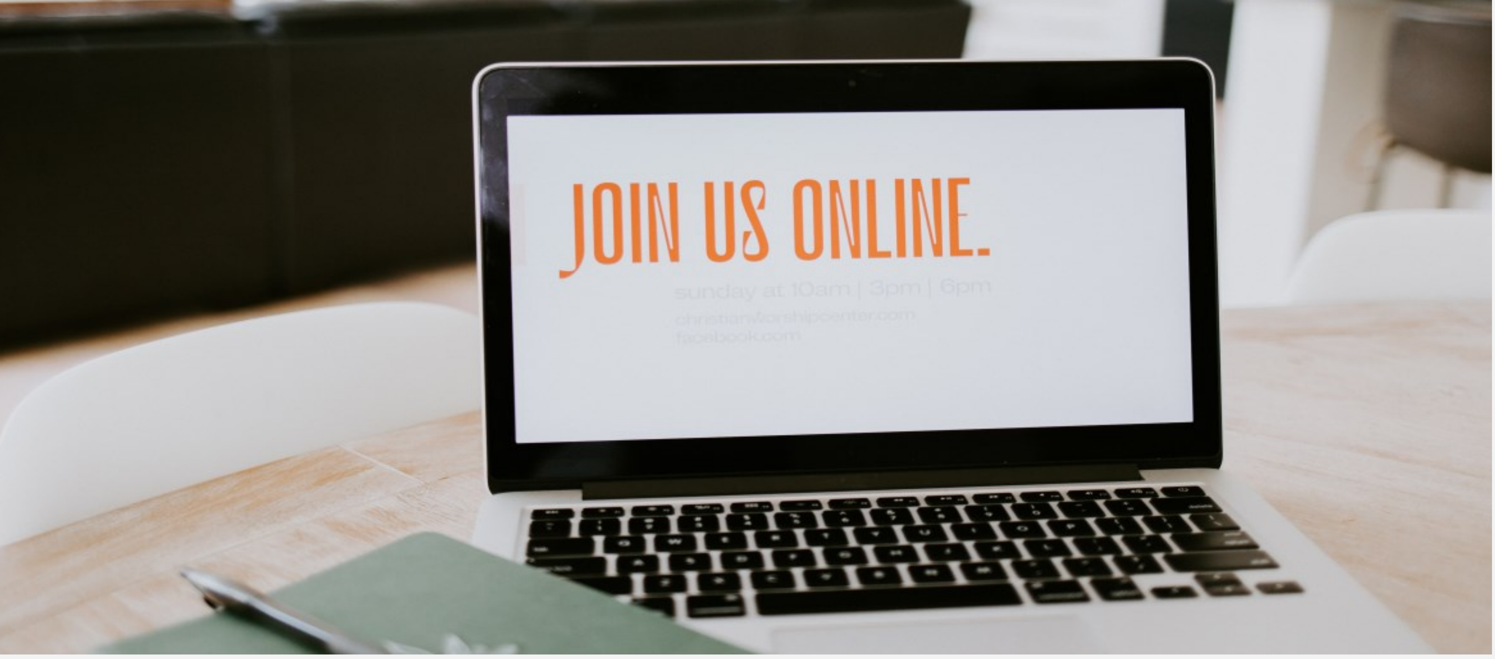


Image credits: Samantha Borges unsplash

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

30/11/2023
16:00-18:30

GFFT Symposium on the Future of Enterprise Security (german/english)

This symposium will discuss the future of enterprise security.The current challenges will be presented in panels and the innovation topics of the next year will be highlighted.The German Startup Cup will showcase three of the new tool providers currently on the market. By means of a survey, the finalist will be selected for the presence final in summer. Info & Registration

30/01/2024
16:00-18:30

GFFT Symposium on the Future of OT & IoT Security (german/english)

This symposium delves into the future of OT and IoT security. Through panel discussions, we'll address current challenges and shed light on the innovation themes anticipated for the upcoming year. As part of the German Startup Cup, we'll introduce three emerging tool providers currently in the market. Info & Registration

United Innovations

- The innovation network -

United Innovations (UI), a subsidiary of GFFT e.V., is a driving force behind innovation in Germany, Europe, and beyond.

Our comprehensive platform boasts an extensive network and a diverse range of offerings, including the techL© technology database, surveys, awards for evaluating new technical solutions, startups, and scientific prototypes, as well as hosting various events and supporting proofs of concepts and launch projects.

Join Our Network at UI

Our focus extends across a wide range of topics positively impacted by IT, including manufacturing, logistics, business processes, and cybersecurity. Our services encourage knowledge sharing, incremental improvements, proactive development of new solutions, and talent recruitment. Embrace the power of collaboration and be a part of our innovation network.

Contact

info@gfft-ev.de
+49 6101 95498-10

Social Media

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

▶ www.youtube.com/GFFTeV

Imprint

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

Web

www.united-innovations.eu

Print

Flyeralarm GmbH

Review German Startup Cup + Use Case Award 22/23

DEUTSCHER STARTUP-POKAL
UNITED INNOVATIONS AWARDS

USE CASE AWARD
UNITED INNOVATIONS AWARDS

The winners of the German Startup Cup and the Use Case Award in the Cybersecurity 2022/23 categories.

Onekey prevailed among the startups - Secuinfra received the trophy for the most convincing use case. The event was hosted by the non-profit Gesellschaft zur Förderung des Forschungstransfers e.V. (GFFT), while PHOENIX group acted as sponsor of the final event.

German Startup Cup

In front of around 100 guests, the startups Sematicon, Cybervize and Onekey presented their innovative business models in the field of cybersecurity. A jury of experts evaluated the presentations, while the entire audience present determined the winner via live voting. Here, Jan Wendenbrug from the startup Onekey prevailed over the competition with 48% of the votes. Cybervize came in second with 27%, closely followed by Sematicon with 25%.

Keynotes and Panel Discussions

Daniel Hofmann, CISO of the Phoenix Group, gave a keynote on cybersecurity. In his lunchtalk, Cup President Professor Dr. Zimmerli asked whether the topic of AI was a hype or a myth, and there was intensive discussion on the panel about how to promote innovation in Germany.

There was lively discussion at the plenary session on the question of how Germany could be transformed into an IT innovation country. "The problem is that we are currently trying to drive innovations for tomorrow with outdated structures and people from yesterday," formulated Dr. Andreas Nauerz, CTO of Bosch Digital. He advocated daring to do more than planning everything 200% through. Julia Stumpenhagen (SVA) spoke out in favor of "technological courage".

Other startups and technology providers of the competitions and partners of United Innovations presented themselves at information booths. Throughout the day, participants had plenty of opportunity for networking and personal conversations.

More information and pictures of this year's cup can be found on the next page and under the following link.

The winners of the Use Case Award and German Startup Cup in the categories Cybersecurity and Software/KI (from left): Florian Eder (Phoenix group), Julia Stumpenhagen (SVA), Christian Bersch (Delphix), Dr. Theo Steininger (Erium), Jan Wendenburg (Onekey), Ramon Weil (Secuinfra) and Dr. Gerd Große (GFFT).

Photo: GFFT/phoenix

DEUTSCHER STARTUP-POKAL

UNITED INNOVATIONS AWARDS

USE CASE AWARD

UNITED INNOVATIONS AWARDS

GFFT
United
pwc
DEUTSCHER STARTUP-POKAL
Einführung zur Paneldiskussion
"Banken als Motor des nachhaltigen Wandels?!"
Peter Hoffner
Vorstand für den Markt Banken, PPI AG
#pwcexperiencecenter

Calling all innovators - New Season of Startup Cup & Use Case Award!

Get ready for an exciting new season of the Startup Cup & Use Case Award! We extend a warm invitation to aspiring startups and companies with innovative Use Cases to embark on this thrilling journey. Two captivating symposia will carefully select startup finalists for the grand finale. Engaging panel discussions focusing on Cybersecurity topics await your participation. Don't miss out on the opportunity to showcase your technology to the world!

Apply now:

German Startup Cup: www.united-innovations.eu/deutscher-startup-pokal-saison-2023-24/

Use Case Award: https://www.united-innovations.eu/use-case-award/

Click here to watch our best-of film from the 2023 finals »

Best-of | Finals
DEUTSCHER STARTUP-POKAL & USE CASE AWARD
CYBERSECURITY | KI & SOFTWARE
GFFT Deutscher Startup-Pokal

Siegerehrung Startup-Pokal Cybersecurity
DEUTSCHER STARTUP-POKAL
UNITED INNOVATIONS AWARDS
48%
ONEKEY GmbH

3

Solution Strategies for your individual Progress

General progress in companies does not proceed randomly but happens often in many companies at the same time. It seems as if companies move in a channel that depends on the same external influences such as newly identified threats, new technologies, legal requirements, or the introduction of standards. For example, many companies are working at more or less the same time on introducing SAP S/4HANA. They evaluate different steps, obtain advice on implementation plans, and introduce necessary tools for data preparation.

The more similar the companies are, e.g., two medium-sized production companies, as greater the similarities and as higher the saving potential that can be achieved through co-operation. It is easy to see that implementation time, cost, and quality equally benefit from a joint approach.

All projects can be found in the

Security Lab

www.security-innovations.eu/themen

Service Management meets Process Mining

An article by Daniel Delling

Initial situation

Standardised tools and solutions from well-known manufacturers are often fundamental building blocks in the modern enterprise service management (ESM) architecture. They often provide companies with the necessary tools to unify, manage and control IT and non-IT processes, services and products - at all stages, starting with the design phase, through provisioning and lifecycle management, up to the end-of-life.

Up-to-date data and information, e.g., from portfolio-, configuration-, asset-, financial- and operations-management, provide transparency about the status of all service components and their dependencies. This data and information provide an essential baseline for optimisation initiatives along the entire value chain and across departments and external providers and suppliers.

In addition, these standardised ESM solutions optimise business costs and ensure data security and compliance. They thus offer an ideal starting point - especially as a simple and straightforward entry point - for process mining. The optimisation of processes in companies, with a view to their own value chain, is a path with a lot of development potential for many companies.

Project

Within the framework of the project, we focus on the technology and methodology of process mining and show how it can be used for different areas and requirements of companies. You will get first insights in which areas process mining can and should be used, which use cases are meaningful and beneficial and which project procedure is applied.

Benefit for the user

In the context of service management, we can go beyond existing reports on "tickets and SLAs", to identify possible weaknesses in processes, workflows, interfaces and responsibilities in order to document starting points for optimisation and automation (in that order). Live analyses of processing, handover, waiting and holding times along the value chain and the service management practices involved make it possible to intervene and take corrective action in day-to-day operations if necessary.

ESM systems are suitable as a starting point for process mining because they:

- are a central, mainly technology-driven element in the overall ESM architecture
- are important central data and information source
- enable case investigation through measurements, reports and dashboards
- focus on the effective and efficient delivery of services and their continuous improvement

Process mining also complements

- the focus on the overarching operational processes
- overcoming silo boundaries based on data and facts
- support for strategic development
- highlighting changes in the value stream in real time
- Help with the identification and understanding of value streams
- identify bottlenecks and their root causes
- tifying possible weaknesses in terms of compliance and security concerns
- identify unused or non-value adding components
- the possibility for proactive development and optimisation

- the ability to prove internal and external compliance conformity

It is also a way of paving the way for future technologies such as Robotic Process Automation (RPA) or Artificial Intelligence (AI) based on value streams.

Daniel Delling
Manager Competence Center
Service Management
SVA System Vertrieb
Alexander GmbH

Detailed information in the techL-profile:
SVA System Vertrieb Alexander GmbH

Fully Managed- versus Co-Managed-Detection & Response – what service does your IT security need?

An article by Ramon Weil

High-performance IT security is fundamentally based on two pillars: on the one hand, the prevention or at least the slowing down of successful cyber attacks through comprehensive security mechanisms and, on the other hand, the rapid detection and defense against successful cyber attacks that were able to circumvent the security mechanisms.

The more digitization advances, the more challenging it becomes to protect companies against damage from successful cyberattacks. Sophisticated malware, ransomware, malicious scripts and advanced persistent threats (APTs), which mostly find their way into the network via social engineering, threaten the IT security of companies worldwide.

In the last few years, a trend has intensified that has now become one of the greatest threats in the field of cyber defense: there is a lack of the necessary manpower. The shortage of skilled workers is also having a full impact on the IT Security sectors. Small and medium-sized companies in particular are finding it difficult to fill vacant positions. Specialized IT Security service providers offer urgently needed support here with Managed Detection & Response (MDR) services. This additional, external manpower relieves the burden on in-house IT Security teams or offers companies the opportunity to have their "own" IT Security team.

What does Managed Detection & Response mean?

The sole use of classic security measures has long since ceased to guarantee effective IT Security. Today, active, fast and comprehensive threat detection and response is more important than ever. To this end, many companies are already using a wide variety of "Threat Detection and Response" tools, which aim to detect and report attack activities in a timely manner and thus significantly increase the level of security: **EDR (Endpoint Detection & Response)**, NDR (Network Detection & Response) or XDR (Extended Detection & Response) are currently considered relevant security solutions that effectively counter current and future cyber threats.

Behind the three letters of **EDR, NDR or XDR** are, in summary, "detection and response" models that detect cyber threats, i.e. recognize them, and manage them in various forms. The solutions are used to detect attacks on corporate networks at an early stage and stop them as quickly as possible.

The IT Security teams responsible receive immediate notifications of identified anomalies and security-relevant data that could indicate acute threat situations through detection and response solutions. This enables them to respond appropriately in the shortest possible time and avert major damage to companies.

Why Managed Detection & Response Services?

According to a large-scale study, a lack of manpower endangers cybersecurity in 85% of all companies. There is no relief in sight on the labor market; on the contrary, all indicators point to the problem becoming even more acute in the coming years.

Managed Detection & Response Services (MDR) address precisely this glaring vulnerability. The term stands for managed detection and response of attacks. Here, the focus is not on technology or a solution, but on a service provided by specialized IT security service providers. By using an MDR service, companies can access services from professional IT security providers that specialize in detecting, analyzing and defending against cyber attacks - ideally 24/7. For example, by using an orchestration tool (**Security Orchestration Automation and Response, or SOAR**), the IT Security analyst externally responsible for a company can immediately initiate appropriate defensive measures when a real threat is detected and confirmed. MDR services can be used according to a company's needs and relieve internal IT Security teams of routine tasks or the time-consuming processing of false alarms.

What does a Fully Managed Detection & Response Service include?

A Fully Managed Detection & Response Service is to be understood as a "complete package", in which all the IT Security tools necessary or deemed useful for a company are provided by a service provider and managed and operated for the company.

This can be, for example, a supplemented by a SOAR system for faster, partially automated analysis and defense against a cyber attack. All systems that can initially detect a potential IT Security incident, provide further information for assessment or initiate protective measures are connected to SIEM and SOAR. In concrete terms, this can involve, for example, the connections of the EDR/NDR/XDR solutions already mentioned.

With the Fully MDR service, security service providers implement and operate all the necessary IT Security tools and monitor the customer's networks and end devices 24/7 for anomalies.

What is a Co-Managed Detection & Response Service?

A Co-Managed Detection & Response service is characterized by individual and flexible utilization: The management and administration of specific security tools is transferred to a service provider. The approach of Co-Managed Detection & Response services is based on the fact that many organizations and companies have already invested in IT security tools such as AntiPhishing, SIEM, EDR/NDR/XDR and SOAR, but then found that a seamless, efficient operation fails due to a lack of sufficient manpower.

Co-Managed Detection and Response Services should not be seen as a substitute, but rather as a supplement to the existing IT Security architecture to ensure that identified IT Security threats can be responded to immediately and appropriately. Thanks to the expertise and manpower of the MDR service provider, this happens so quickly that significant damage to the company concerned is averted or at least greatly reduced. In addition, Co-Managed Detection and Response services offer another advantage that should not be underestimated: customers receive high-quality consulting services and a valuable transfer of knowledge. This is because close, cooperative collaboration is a key part of all co-managed service approaches. Experienced, external specialists compensate for the lack of expert knowledge within the company - and the company's internal IT benefits from their experience and know-how through professional exchange.

Individual use of IT Security services based on a modular principle with flexible, hybrid approaches: Co-Managed Detection & Response services close gaps in cyber defense when resources, expertise or specialists are lacking and represent a valuable alternative to complete in-house concepts or fully managed services.

Conclusion

Experienced IT Security professionals are hard to come by on the job market. Small and medium-sized companies in particular are all too often left without the urgently needed human expertise, even if technical security solutions are available within the company. Managed Detection & Response services fill the gaps in cyber defense. While Fully Managed Detection & Response services provide all necessary tools and services as a complete package, modular and flexible Co-Managed Detection & Response services compensate for missing resources and capacities in specific areas.

Ramon Weil
Founder/ CEO
SECUINFRA GmbH

Detailed information in the techL-profile:
SECUINFRA GmbH

Incident Response Check

An article by Dr. Stefan Rummenhöller

Initial situation

Given the speed with which attackers can spread across the corporate network today, good preparation is the most important building block for minimizing damage, whether financial or reputational.

Successful cyber attacks are usually accompanied by the impairment of business-critical processes. The resulting financial damage must be minimized as quickly as possible. Data destruction, data theft or loss of reputation can also lead to damage that companies must avoid or mitigate.

In order to achieve these goals, the Incident Response Service ensures in advance of a cyber security incident that affected companies have access to the right tools and processes as well as the necessary expertise to contain threats as quickly as possible in the event of an attack.

Project

As part of the assessment, r-tec reviews its technical and organizational response capabilities. The company receives an independent assessment of the existing processes, procedures and technical solutions for detecting and handling security incidents. To do this, r-tec uses international best practices and, in particular, extensive experience from completed customer incidents, as well as in-depth knowledge of the current threat situation and new attack techniques.

Individual coordination takes place in advance, and r-tec subsequently provides the users with the questionnaire on the basis of which the assessment will be carried out. The format used is an interview lasting about half a day, during which all the relevant information is gathered in order to determine the current maturity level. The maturity level indicates how well the company is prepared with tools, processes and organizationally for a security incident and how well it can respond to it.

Benefit for the user

By evaluating the existing processes, procedures and technical solutions for detecting and handling security incidents, users can be made aware of problems that would cause them to lose valuable time in an emergency.

The company receives an evaluation to determine its individual maturity level. In addition, optimization potentials are identified and recommended measures are developed to improve incident response capabilities.

Dr. Stefan Rummenhöller
Founder & Managing Director
r-tec IT Security GmbH

Detailed information in the techL-profile:
r-tec IT Security GmbH

4

Applicable Use Cases & Success Stories

Often, progress is generated by using new technologies and/or adopting the experiences of others.

The task of the leading technology providers and new startups is to simplify cost-intensive processes or solve upcoming challenges with new tools. They usually invest a lot of money analyzing the problem areas and thinking about feasible solutions with initial customers.

The task of consulting companies is to look at the companies' current processes and introduce helpful changes. The use of appropriate tools can accompany this task.

In both cases, a lot of know-how can be used to make rapid progress. This chapter presents several use cases and success stories that may serve as an impetus. The contact persons named in each case are happy to discuss your challenges. Just get in touch with them!

All projects can be found in the

Security Lab

www.security-innovations.eu/themen

Use Case: London South Bank University

An article by Michael Veit

Description of the Solution

With a complex and vast IT estate across multiple sites, London South Bank University's IT team needed specialist help to stay ahead of constant and growing security threats. They turned to Sophos fora24 hour, 365 days a year service. Alex Denley is Director of IT Innovation and Transformation at London South Bank University. When he joined the University in 2017 he realised that it took significant operational overhead to protect such a large and varied technology stack across many sites that presented big challenges. These challenges mainly centred around compliance and the safe storage of student data while maintaining a proactive approach to IT security. This is where the Managed Detection and Response service from Sophos has been able to help.

Use Cases

In 2020, the University's on-premise cybersecurity solution from Sophos was soon to go end-of-life and the Sophos team advised they should upgrade to Sophos Central with Intercept X. This would provide cloud-based and centralised security ensuring that all endpoints were protected and easily managed from a central point. This immediately reduced the administrative burden of such a large and complex IT estate. More recently Alex approached Sophos to reduce cyber risks even further by discussing the benefits of a 24/7 managed IT security service to continually ensure compliance and protect data.

Alex realised that an outsourced team of information security experts could provide around-the-clock surveillance and expertise to ensure the University was always safe, secure and compliant. The cost and time it would take to manage the same level of service in-house was prohibitive. The Sophos team therefore recommended Sophos Managed Detection and Response (MDR) as an unparalleled service in the IT security sector. Alex already knew that Sophos understood the needs of Higher Education and could deliver a personable, immediate service at a competitive price to protect the University's systems, data and technology.

Benefit for the user

The University now benefits from a highly proactive approach to information security, managed by a team of Sophos experts who are available to combat threats 24/7. Alex and his team have 24/7 reassurance that their network, systems and data are secure, protected, and compliant. Moreover, the IT team has been able to refocus its attention onto projects that have a direct impact on the student experience. Additionally, the internal IT experts are now able to get involved in security from a more strategic perspective, rather than being involved in the detail of individual incidents. The University is no longer firefighting security issues due to the proactive and constant surveillance from the Sophos MDR experts. This gives Alex and the leadership team at the University peace of mind. Finally, the Sophos account management team and the industry experts on the MDR team deliver excellence every day. They are trusted strategic partners to the University that ultimately add value to the student experience.

Michael Veit
IT Security Expert
Sophos Technology GmbH

Use Case: Digital sovereignty through encryption and key management

An article by Armin Simon

According to the World Economic Forum, digital sovereignty means "the ability to be in control of your own digital destiny - the data, hardware and software you rely on and create. Given the exponential growth of data and the fact that modern organizations are increasingly reliant on digital platforms, the need for digital sovereignty is growing in all countries.

What does digital sovereignty mean in the cloud?

For a successful cloud strategy, there are three main pillars that support the goals of digital sovereignty: Data sovereignty, software sovereignty and operational sovereignty.

- Data sovereignty means that companies retain control over their data through encryption and access management. This ensures that sensitive data does not fall into the hands of a foreign entity without explicit permission, which would be a violation of European jurisdiction.

- Software sovereignty means that workloads are executed independently of a provider's systems. This gives companies the freedom to store data and run workloads where they want in order to optimize performance, flexibility and overall resilience.

- Operational sovereignty means that an enterprise gains visibility and control over the provider's operations. This ensures that criminal actors or malicious processes cannot access or prevent access to valuable data, such as in the case of privileged user access or a ransomware attack.

The Thales solution for digital sovereignty

Encryption plays a central role in digital sovereignty. The role of encryption in achieving data sovereignty is very obvious. Data can be processed by authorized users of decryption keys, but not by anyone else.

Key management is also essential for achieving software sovereignty, i.e., vendor-independent use. After all, it is important to achieve interchangeability of the providers; for this purpose, of course, the key sovereignty must remain in one's own organization.

Good operational sovereignty is achieved when several providers are used and/or repatriation is planned from the outset. Here, too, the central administration of encryption and its keys plays a decisive role.

Thales CipherTrust Manager

Thales CipherTrust Manager provides enterprise-wide key and secrets management and enables the various aspects of digital sovereignty to be implemented.

The solution integrates with hundreds of third-party products, especially with all cloud hyperscalers.

Armin Simon
Regional Sales Director
Thales Data Security

Detailed information in the techL-profile:
Thales CPL GmbH

5

New Technologies

Generally speaking, startups are a good measure of the innovative strength of the respective region. The more successful startups are founded, the more dynamic and competitive the innovation location is. Dynamic economic areas tend to attract more highly qualified entrepreneurs and employees, increasing the region's prosperity.

In the subject areas surrounding enterprise IT, startups also strengthen the competitive power of companies.

A high level of dynamism means that potential can be exploited more quickly with new solutions. It would be a great advantage for the local economic area to have its own strong software startup scene. This not only requires funding from the state and venture capitalists but also strong utilization of the solutions developed here among the many companies.

All information about the

German Startup Cup

www.united-innovations.eu/deutscher-startup-pokal

Cybervize

An article by Alexander Busse

Harnessing the power of Artificial Intelligence to bring cost-effective, comprehensive cybersecurity to small and medium-sized businesses.

About the startup

Established in 2021, Cybervize is a trailblazing tech startup, focusing on fortifying cybersecurity for small and medium-sized businesses (SMEs). With the invaluable backing of CISPA Incubator, an integral part of the CISPA Helmholtz Center for Information Security, Cybervize is built on a solid foundation of cutting-edge cybersecurity research and innovation. Additionally, our affiliation with the "SpeedUpSecure" accelerator initiative promotes our growth and learning, encouraging innovative cybersecurity solutions.

Our founder, Alexander Busse, brings 25 years of cybersecurity expertise from the corporate world, having served in leadership roles in esteemed consulting firms. His in-depth market knowledge and entrepreneurial acumen drive Cybervize's commitment to superior cybersecurity, ensuring data safety and protection against cyber threats for all organizations.

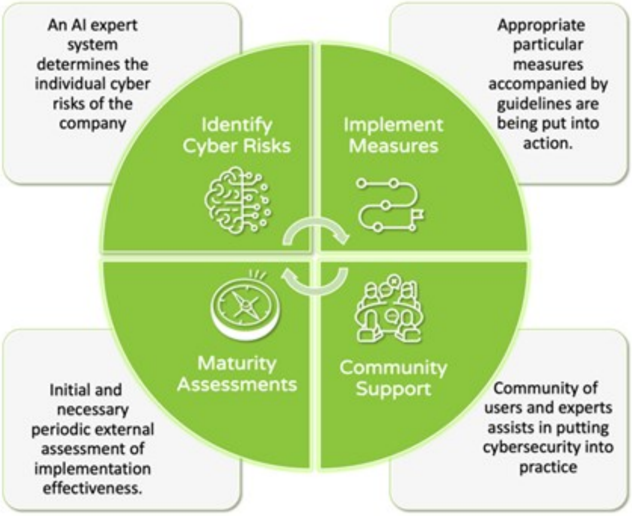
We are committed to leveraging state-of-the-art technology to tackle escalating cyber threats, making cybersecurity accessible, efficient, and manageable for SMEs, and enabling the secure operation of their business processes.

Technology

Cybervize's unique technology hinges on the AI-driven automation of significant aspects of Information Security Management System (ISMS) implementation and operation. This is deployed through an expert system and a Software-as-a-Service (SaaS) solution, resulting in a comprehensive, affordable cybersecurity package crafted for SMEs.

Our technological edge lies in our use of knowledge graphs. These graph-based structures intelligibly represent knowledge for both human and AI interpretation, enabling the AI system to understand the interconnections and dependencies within an organization's cybersecurity framework.

Our system provides a suite of services, from company data onboarding, risk assessment, and gap analysis, to creating a mitigation concept. The SaaS tool further documents the compliance and implementation of measures, with our human advisors offering additional guidance and support.


An AI expert system determines the individual cyber risks of the company
Identify Cyber Risks
Implement Measures
Appropriate particular measures accompanied by guidelines are being put into action.
Maturity Assessments
Community Support
Initial and necessary periodic external assessment of implementation effectiveness.
Community of users and experts assists in putting cybersecurity into practice

By fusing AI capabilities, the versatility of knowledge graphs, and human expertise, Cybervize presents a dynamic, tailored, and affordable cybersecurity solution for SMEs. This amalgamation of technology and expertise constitutes a resilient cybersecurity ecosystem that adapts to evolving threats and safeguards businesses robustly.

Benefit for the user

Cybervize offers a unique respite for SMEs grappling with complex cybersecurity issues. By delivering a comprehensive solution amalgamating AI power and human expertise, Cybervize alleviates these companies' cybersecurity management burden.

Adopting the OCTAVE Allegro Method for risk assessment ensures a comprehensive understanding of a company's information security needs.

Its asset-centric approach defines a manageable scope from the onset, streamlining the threat identification, analysis, and planning process.

Moreover, Cybervize's AI-powered expert system provides risk mitigation recommendations, considering the company's existing measures. It also outlines a pragmatic guide for IT to implement requisite measures, supplemented by support from Cybervize's human advisors.

Lastly, Cybervize's SaaS tool documents the enforcement and compliance of measures, delivering a real-time risk profile of the company. Users can also commission assessments for an external estimation by Cybervize's human advisors.

In essence, Cybervize’s solution benefits are three-pronged: it addresses the cybersecurity risks faced by SMEs, provides a cost and time-efficient solution, and integrates AI capabilities with human expertise for a comprehensive cybersecurity approach.

Alexander Busse
CEO
Cybervize GmbH

Ory

An article by Leonie Habermann

Ory Network is a global, high availability and low latency login access network that protects identities and other first party data.

Ory delivers information security using advanced AI analytics for data created by system access including authentication, authorisation and API traffic. Ory Network helps its customers use zero-trust security across their stack including data protection, compliance and risk management. Ory Network delivers state of the art solutions for access security including Passkeys, passwordless login, social login, second factor authentication, multi factor authentication and hardware tokens. Ory is an open source organization welcoming collaboration and contributions to its leading products from an active global community. With more than 30,000 community members and over 250 GitHub repositories, Ory maintains the world's leading open-source identity management, authentication and authorization ecosystem and community. Ory Network builds on this knowledge and experience.

Technology

Zero trust security is part of the internet's evolving model for improved access protection and control and also forms the underlying principle of Ory Network. In order to maximize interoperability between globally distributed infrastructures, Ory's open source products implement leading standards and interoperability conventions in Ory Network. Ory implements the Internet Engineering Task Force open authorization 2.0 protocol including OpenID Connect. Ory's access permission product is developed in accordance with the Google Zanzibar specification. The Identity management product provides user login and registration, multi-factor authentication and user information storage. Ory's system architecture follows the "2 Factor" approach to cloud native services using APIs. Based on Google's Beyond Corp specification, Ory also has a product for API security using a reverse proxy. Currently Ory Network combines the above services with a sophisticated management layer and a multi tenant database system.

Benefit for Ory Network Members

With 81% of attacks originating through compromised credentials[1] it's crucial for almost every company to implement zero trust security models. Real time analysis of security threats, user access events and authorisation requests improves application security and protects end user information. The key is providing a first-class customer experience, robust security and data protection, and ensuring compliance with legal regulations – requirements often diametrically opposed. A user is not only an individual or customers but can also be a device, application, workload, data center or any other connection to the network. **True Multi Region:** Ory is building out a global network offering data storage in all (major) cluster regions in the world. This allows low-latency for a great user experience and local storage of personal identifiable information to comply with different data protection laws. **Open Source Ecosystem:** Ory's open source based ecosystem provides battle-hardened software components that have been tested by thousands of users. **Modularity and open standards:** Due to its modularity, its cloud-native APIs and its commitment to Open Standards Ory allows its customers to gradually adopt Ory Network and for simplified integrations into applications, systems, APIs and access gateways. **Usage based pricing:** Ory offers fair pricing that is based on active users and scales with our customer's business. Key features are available in any plan as security should not be a pricing compromise.

[1] Cisco Zero Trust Report. January 27, 2020, https://www.cisco.com/c/dam/global/en_uk/products/pdfs/cisco-ciso-day-zero-trust.pdf

Leonie Habermann
Managin Director
Ory Germany GmbH

6

State of Research

The joint exchange of innovation know-how leads to savings, but not to a competitive edge. To achieve this, one must break new ground, which is both time-consuming and expensive, and also requires questioning previous methods. For this step, it makes sense to harness the power of academic research partners. This is accompanied by other advantages such as access to young researchers and the use of public funding.

In this chapter, we present projects in which practical partners are sought:

- Projects whose results are so good that a spin-off is planned.
- Projects that are in the application phase and whose intended results may help your company move forward.
- Ideas for future products from which the scientists expect great commercial market success.

The contact persons mentioned in each case are happy to exchange views with you about the future and their plans derived from it. Just get in touch with them!

All projects can be found in the

Security Lab

www.security-innovations.eu

Data Protection Research for Real-World Applications

An article by Prof. Dr. Lena Wiese

Researching the tradeoff between data protection and data analytics

The importance of data protection and data security has increased significantly in recent years, mainly due to the vast amount of personal or business-critical information that private individuals, organizations and public authorities collect, process and exchange in digital form. This information can be misused for a variety of purposes, ranging from personalized advertising to continuous monitoring or even identity theft. As a result, there has been an increased demand for privacy-enhancing technologies (PETs) to protect the privacy rights of individuals or business secrets of companies.

These facts highlight the growing need for constantly improved privacy protection measures to prevent data breaches in an ever-changing digital society. The Database Technologies and Data Analytics research group explores security methods with practical applications – in particular, with a focus on data protection in medical applications in cooperation with the Bioinformatics research group at the Fraunhofer Institute for Toxicology and Experimental Medicine. We present three of our research fields in the following.

Data anonymization

Anonymization procedures can protect privacy in such a way that it is no longer possible to identify individuals in large datasets. The challenge, however, is not only to maintain data privacy, but also to ensure that the shared data are informative enough to be useful for data analytics in the sense for example of personalized medicine. The development of highly-specialized anonymization solutions while taking modern data analytics into account is necessary to prevent the identification (de-anonymization) of individuals in publicly available datasets. Formal privacy metrics play a critical role in assessing and evaluating the effectiveness of technologies to reduce privacy risks. By combining diverse established techniques in the project PrivacyUmbrella (funded by BMBF/NextGenerationEU), we aim to enable stronger anonymization guarantees while maximizing usefulness for data analytics.

Cross-company Intrusion Detection

Vulnerabilities in IT infrastructures are ubiquitous today, and threats to these infrastructures are continuously emerging over time. For this reason, organizations should develop proactive and preventive monitoring strategies (Intrusion Detection Systems, IDS) for these threats to detect them as early as possible and respond quickly. To gain a holistic view of the threat landscape in cyberspace, there is an urgent need to move beyond on-premise intrusion detection that only analyzes attacks on an individual basis. Instead, it is essential to analyze data from different companies collectively to gain a national or global overview, and to analyze historical attack data retrospectively for new attack patterns to train better machine learning models for intrusion detection.

However, disclosing company internals as well as sensitive personal information such as individual surfing behavior of employees or customers would violate data privacy laws in such analyses. To prevent sensitive information from being revealed, we use cryptographic procedures in the project CryptScan (funded by the Hessian Distral framework) to ensure the protection of these confidential or personal data. With carefully chosen encryption mechanisms, it is even possible to perform search operations, comparisons or even abstract calculations on the encrypted data without having to decrypt the data first. In this way, privacy can be protected, while at the same time valuable information about attacks and intruders can be obtained from the data.

Genomic Privacy

Thanks to modern high-throughput technologies, genome data are nowadays generated and analyzed on a large scale. Such individual biomedical data contain information about disease risks, the analysis of which contributes to the diagnosis or prediction of diseases. We are developing fundamental machine learning technologies while maintaining privacy. We focus on the analysis of large genomic datasets based on biclustering while maintaining data security through advanced cryptosystems such as Homomorphic Encryption in the project CloudDBGuard (funded by DFG). In terms of usable security, we also aim to develop a secure application that is easy to understand even for less technically experienced users (e.g., medical staff, biomedical researchers).

Prof. Dr. Lena Wiese
Professorship Database Technologies
and Data Analytics
Goethe University Frankfurt/Main

Photo: copyright Fraunhofer ITEM

Integrating the human factor

An article by Stefan Sütterlin

The Cyberpsychological Lens: Understanding Human Influence on Socio-Technical Systems in IT-Security.

> *If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology"*
>
> *(Bruce Schneier, 2000)*

Initial situation

In the realm of IT-Security, the inherent dichotomy exists wherein humans are tasked to shield machines against assaults orchestrated by other humans, leveraging machines. Although it's universally recognized that humans remain central actors and recipients in IT security incidents, the integration of multidisciplinary angles remains an elusive aspect in the professional education of IT -Security specialists. This gap was recognized by a collective task force, encompassing entities such as the IEEE Computer Society (IEEE-CS), the Association for Computing Machinery (ACM), and the International Federation for Information Processing (IFIP). These organizations released cybersecurity curricula, advocating for the incorporation of diverse disciplinary insights into cybersecurity education, a scope extending to policies, law, risk management, ethics, and crucially, the human factor.

The pivotal role played by human cognition, decision-making, and interpersonal information exchange within security-sensitive socio-technical systems has propelled the evolution of methodologies, instruments, and safer practices in sectors such as aviation or critical medical care. Established elements of a broader domain of human factors, such as biased decision-making processes in medical scenarios, or situational-awareness-oriented design techniques to augment information processing in aviation control, have been assimilated into research and development practice. Relevant tools designed to evaluate cognitive processes and predict human performance at various systemic levels stem from the convergence of cognitive, biological, and social psychology.

Projects

Our interdisciplinary consortium, via a series of nationally and internationally sponsored research projects, addresses these challenges by adapting and implementing research techniques rooted in behavioral (neuro-)sciences within various applications in the IT-security domain. Our research collaborators span private businesses, and civil or military entities primarily across Europe.

Highlighted projects

We provide consulting services to organizations on the key determinants of successful cyber-security awareness education. Acknowledging the glaring absence of science-based quality indicators and a regulatory-induced skew between significant demand, high costs, and abundant consulting and training offers with questionable sustainable impact, we deliver unbiased advice, incisive inquiries, and checklists to aid organizations in obtaining the most effective awareness training package, ensuring robust ROI and sustainable results. Consultancy firms leverage our science-based approaches to enhance their product offerings.

In the ACDICOM (Advancing Cyber Defence by Improved Communication of Recognized Cyber Threat Situations) project, funded by the Norwegian Research Council, we collaborate with international partners to explore effective communication methods of identified cyber threats, predominantly, but not exclusively, within the military sector.

The EEA-sponsored ADVANCES (Advancing Human Performance in Cybersecurity) project aims to develop a science-based interdisciplinary framework to cultivate and assess general and specific competencies of the present and prospective cybersecurity workforce, in conjunction with partners from the Baltic states, Norway, and Liechtenstein.

In the forthcoming EU-sponsored ATHENA project, led by the Dutch Ministry for Infrastructure and Water Management, we aim to amplify cyber resilience of critical infrastructure within the water sector through innovative and co-created competence building by consortium partners and their suppliers.

Benefit for the user

Our research provides immense value to the users as it aids in the evaluation of relevance and improvement potential at the intersection of humans and technology. The rising awareness of the necessity to address cybersecurity issues to safeguard organizations underlines the importance of incorporating a human perspective for successful technological solution implementation and supplementing security measures where they may fall short. We aid users in comprehending the predictors of human performance, unleashing their cyber operators' potential, and offering a meta-level guide for critically evaluating cost-intensive external consultancy propositions.

Prof. Dr. Stefan Sütterlin
Professorship Cyberpsychology
Albstadt-Sigmaringen University

Research Project: SecDER - Making virtual power plants resilent

An article by Christian Müller

Redefining AI Security Paradigms: The Emergence of Neuro-Explicit Artificial Intelligence and Its Potential for Bolstering Robustness, Transparency, and Trustworthiness in Modern AI Systems

The traditional scope of safety research and functional safety predominantly concentrated on the probabilities of error, with less association with artificial intelligence (AI). In this approach, AI was often viewed as a black box, kept isolated. However, in an era where AI technologies have become increasingly pervasive, the boundaries between functional safety and cybersecurity have started to blur, necessitating a holistic understanding of both potential functional failures and security threats.

In this evolving landscape, the rise of neuro-explicit AI emerges as a promising solution, offering a significant improvement in understanding and robustness of AI systems by integrating a wider spectrum of knowledge. Before diving deep into this, it's essential to understand the concept of symbolic AI, which operates on processing symbols and rules to model and generate intelligent behavior.

Symbolic AI, although less prevalent in the era of deep learning and neural networks, remains an essential approach in areas where logical reasoning and knowledge modeling are vital. The interdisciplinary field of neuro-symbolic AI combines neural networks with symbolic AI, leveraging the strengths of both and allowing for deeper data analysis and interpretation.

Neuro-explicit AI takes this integration one step further. It not only combines neural networks and symbolic knowledge but extends the scope to incorporate other forms of explicit knowledge, including physical laws and mathematical models. While still actively researched, neuro-explicit approaches are promising in enhancing AI performance, explainability, and robustness across various fields such as healthcare, robotics, autonomous vehicles, and language processing.

Neuro-explicit AI provides effective tools for improving AI safety in the context of both AI safety and security. The integration of explicit knowledge serves as "grounding," anchoring the neural networks in a secured knowledge foundation. This makes perturbations, whether adversarial attacks or natural data variations, easier to detect and makes the AI system more robust to attacks and disruptions.

Adversarial attacks, known security risks where manipulated input data are purposely used to impair a neural network's performance, can be mitigated by the inclusion of explicit knowledge. The symbolic knowledge model can represent causal relationships and domain-specific knowledge to guide data processing and detect implausible results. For instance, it can help prevent misclassifications of images by recognizing manipulated inputs as inconsistent with the symbolic knowledge model.

Neuro-explicit AI also better handles natural changes in data that may occur in real-world scenarios. The symbolic knowledge model can serve as a reference to assess and monitor changes in the input data. For example, if an autonomous vehicle encounters altered traffic conditions, the symbolic knowledge model can assist in evaluating the plausibility of the decisions suggested by the neural network.

Moreover, another advantage of neuro-explicit AI in terms of safety is the possibility of formal verification. As the symbolic knowledge model enables an explicit representation of rules and relationships, formal methods can be applied for verification and consistency checking, enabling the early identification and rectification of potential weaknesses and inconsistencies in the model.

However, it's important to note that the integration of explicit knowledge into AI models requires additional effort. Appropriate methods need to be developed to capture, model, and integrate the knowledge into the neural networks, and safety considerations must be included in the development process to identify and address potential attack vectors.

Looking forward, the future of neuro-explicit AI promises exciting developments and opportunities for AI system security. With continuous advancements in machine learning and AI, we will witness increasingly sophisticated and complex models based on a combination of neural networks and explicit knowledge. Neuro-explicit AI models will help increase the trustworthiness and safety of these systems by offering real-time plausibility checking and verification capability.

As research and development progress, we will also see a wider application of formal methods for the verification and validation of neuro-explicit AI systems. By leveraging formal models and methods, potential weaknesses can be identified and rectified early, leading to even safer and more reliable AI systems.

Christian Müller
Head of Competence Center Autonomous Driving
Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI)

Secure Software Development at THA

An article by Prof. Dr. Dominik Merli

Software development for infrastructures or products is increasingly popular with SMEs. High time pressure and limited personnel resources, however, often take their toll on security, endangering companies and their customers. The funding project "Higher IT Security through Secure Software Development" (HITSSSE) at the Augsburg Technical University of Applied Sciences aims to improve this situation.

HITSSSE provides recommendations for action and technical aids as generic solutions for SMEs, addressing technical hurdles and the human factor.

Security Adventure – addressing people

Many attacks on IT infrastructures are related to the human factor. Phishing emails, tailgating, CEO fraud, and baiting: these methods take advantage of this human vulnerability and can give potential attackers access to sensitive data and systems. However, if companies help their employees to be aware of the threats and accept security measures, such attacks are preventable.

Project HITSSSE developed a prototype of a video game that guides players through various security-related challenges in everyday work. The Security Adventure has two functions. On the one hand, it builds up knowledge by playfully addressing IT security awareness or secure software development topics. On the other hand, it aims to increase the willingness of employees to deal with IT security.

The game runs on a conventional PC. In addition, the HITSSSE team provides a classic arcade machine running the Security Adventure that, combined with the pixel look of the game, also appeals to employees' nostalgia and minimizes barriers to entry.

CI-in-a-Box – encapsulated CI/CD infrastructure

Integrating CI/CD pipeline tools into a company's internal infrastructure is often challenging. Usually, using embedded system target hardware results in configuration problems. To prevent these issues, the HITSSSE team's CI-in-a-Box provides a fully encapsulated CI/CD infrastructure, offering software developers a secure platform to try out and learn about automated CI/CD pipeline processes.

In general, such an infrastructure should allow for flexibility, reproducibility, and robustness. Therefore, the CI-in-a-Box is compact and mobile, thus offering flexible and adequate usage as needed. In addition, developers can install the software environment they need with one click and easily reset it. An upstream OPNsense firewall establishes an internal network, allowing the CI-in-a-Box to be operated separately from the corporate network.

For easy access to the CI-in-a-Box and the CI/CD processes, it provides sample projects to support the use and integration of the platform.

Security Annotations – marking sensitive code

For SMEs, data about processes, people, or systems baked into software are valuable resources. These assets are worth protecting. If such data is manipulated or falls into the wrong hands, this can impair a company's profitability and ability to operate. For this reason, the idea of Security Annotations should make it easier for SMEs to get started with IT security in software development.

With this concept, it is possible to permanently mark security-sensitive source code and assign it to assets and potential vulnerabilities. Annotations and the linked additional information are stored in a commit-specific manner, generating documentation tailored to the security status of the entire code base.

This documentation is relevant for developers and project managers, connecting software development with risk management.

The HITSSSE team created an extension for the IntelliJ development environment, making it easier to set the security annotations. In addition, a sample project provides first insights and an example for guidance.

Eventually, companies should find it easier to implement a secure process for developing products and software that improves IT security in infrastructures and products. Embracing these solutions and adopting a comprehensive approach to IT security will enable SMEs to mitigate risks, protect their customers, and thrive in an increasingly interconnected digital landscape. Visit www.hitssse.de for more information on HITSSSE.

Prof. Dr. Dominik Merli
Head of HSA_innos
Augsburg Technical University of
Applied Sciences

Project HITSSSE is sponsored by the German Federal Ministry for Economic Affairs and Climate Action.

Engineering secure cyber threat intelligence based systems

An article by Dr. Florian Klaus Kaiser, Prof. Dr. Marcus Wiens, Prof. Dr. Frank Schultmann

Initial Situation and Motivation

Cyber-attacks keep states, companies and individuals at bay, draining large amounts of corporate resources. This is attack techniques develop rapidly and there is a great increase of the threat landscape. Considering the effects of digitalization in industrial production and especially the influence of Industry 4.0, the enormous possibilities offered by digitalization in these processes while introducing substantial risks and novel susceptibilities highlight the great need for increasing the security of software defined systems and networks. A promising opportunity is thereby offered by traces left by attackers within the system. These can provide a starting point for investigations and analyses of these traces can generate actionable insights for cyber risk management.

Today, security analysts' investigations start with monitored data that is sent to an organization's security information and event management system. The system aggregates and correlates the data from the sensors and generates alerts when a suspicious event is detected. On the basis of these alerts, security analysts derive hypotheses on the state of the underlying system and draw conclusions on potential attacks. Hereby human analysts are employed to understand the attack and decide on their reaction on alerts. Despite the great importance of these tasks, security analysts have little time to devote to them and automation levels are low.

Project

Within our work on engineering cyber threat intelligence based secure systems, we develop a threat knowledge base overcoming boundaries between different threat intelligence sources unifying the information of different cyber threat intelligence feeds. Furthermore, we employ the information to assist cyber security professionals in threat hunting and incident response, as well as in the forensic investigation of attacks. The methods developed automate the process of tracing back the attack vector, inferring hypotheses on the attackers' objectives and the future course of action, and propose reasonable reactions in attacks.

These automated approaches taking advantage of Cyber Threat Intelligence on past attacks hence bear the potential to empower security professionals and by doing so, increase cyber security. The methods developed are mainly based in data analytics and take advantage of artificial intelligence and link prediction techniques. We propose the implementation of antifragile bio-inspired systems composed by means of passive defense. The developed approaches can be used for automating processes in security operation centers and for assisting human analysts within their daly work. Furthermore, our developed approaches can help in decreasing the time between breach detection and response and support the process of choosing the most effective solution to defend against attacks.

Dr.-Ing. Florian Klaus Kaiser
Head of Research Group
IIP-KIT and KASTEL-KIT
Karlsruhe Institute of Technology

Prof. Dr. rer pol Marcus Wiens
Principal Investigator
KASTEL-KIT
TU Freiberg

7

Survey of Technologies

At regular intervals, we ask the experts for building blocks that they currently need. By far, the most frequent response is the desire for tool research for a specific topic. Our team has therefore been expanded to include young students, for whom tool research is a good additional element of their education. In this chapter, you will find a collection of technologies that we think deserve your interest.

Only a short outline of the product is presented. The attached link leads directly to the product datasheet in our techL-database, where more detailed information and contact persons can be found.

All innovations be found in the technology database

techL

www.techl.eu

7 Survey of Technologies

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 profile

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 profile

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 profile

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 profile

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 profile

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 profile

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 profile

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 profile

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 profile

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 profile

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 profile

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 profile

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 profile

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 profile

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 profile

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 profile

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 profile

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 profile

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 profile

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 profile

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 profile

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 profile

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 profile

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 profile

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 profile

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 profile

Wetog

As WETOG, we find ourselves in one of the most important roles of our time – offering our customers the possibility to use digital communication and data exchange in a GDPR-compliant and secure way, while retaining complete ownership of their data. Understanding the value of data, we deliver a platform secured by our revolutionary encryption technology"LIQRYPT. WETOG's integrated communication and working tools do not require any additional elements, guaranteeing complete safety and efficiency. With our SaaS solution, MADE in GERMANY, we face the duty to make your digital workspace a safer place.

techL profile

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 profile

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 profile

www.security-innovations.eu