United Innovations

Survey of Tools for Secure Infrastructures and Processes

Release 1 / 2024

www.security-innovations.eu

GERMAN STARTUP-CUP

UNITED INNOVATIONS AWARDS

German Startup-Cup

Categories Cybersecurity and AI & Software

Date: Tuesday, 2nd July
Location: Mannheim, Germany

PHOENIX group

www.united-innovations.eu/startup-cup/Security-AI-Software

EDITORIAL

Dr. Gerd Große

Dear readers,

A few days ago, it became public that internal conversations between Bundeswehr generals were overheard by Russian spies. This did not really surprise us. Anyone looking at the current state of the security efforts of all major organizations and the quality of the attackers would have thought something like this was possible. The emails of Microsoft managers responsible for security have also been read by a Russian hacker group these days.

For security experts in the know, the statement by our defence minister that this incident was the only successful eavesdropping operation by state-organized spies was certainly more surprising. This may rather indicate that the other attacks are simply unknown. As we good citizens can't do anything about this threat anyway, we may be helped by the experience that transparency about each other's actions also helps to avoid conflicts.

Large companies will be reluctant to display this kind of pragmatism. It is not only potentially costly to their existence if competitors know the company secrets they have acquired. Neglected data protection is also a breach of the law and remedying the deficiencies is expensive. The scale of the task is considerable, as many companies are still struggling with basic security first and foremost. It does not take much wisdom to describe current efforts against attackers as hopelessly inadequate.

The question therefore arises as to which direction the defense must take. Objectively speaking, two measures will be increasingly considered: Firstly, strategies will be developed that place security as a core element at the beginning of all IT architectures. Keywords such as security by design or a security operating system as the basis of the computer come to mind here. On the other hand, costs will be reduced through services that guarantee the security of several companies at the same time. An example of this would be external security operation centers. There is still a lot of potential to be exploited in both areas.

In the hope that cybersecurity will continue to gain ground through innovation, I hope you enjoy reading this magazine.

Dr. Gerd Große

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

10

12

26

CONTENT

CALENDAR

16/05/2024 15:30-17:00 Consortium project OT-Security: Insights plant security (german)
Info & Registration

13/06/2024 15:30-17:00 ITSM consortium project: Insights Proactive IT Management (ITM) (german) Info & Registration

---

02/07/2024 Symposium and final of the German Startup Cup for Cybersecurity + AI & Software Info & Registration

---

20/09/2024 15:30-17:00 Consortium project corporate security: Insights SOC (german)
Info & Registration

10/10/2024 15:30-17:00 Consortium project OT-Security: Insights plant security
Info & Registration

14/11/2024 15:30-17:00 Consortium project ISTM: Insights ITSM & Process Mining and Proactive ITM 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

United Innovations GFFT PHOENIX group

Highlight Event

German Startup Cup & Use Case Award Finale 2024

Date: 2nd July, 2024
Location: PHOENIX Group, Pfingstweidstraße 10-12, 68199 Mannheim, Germany
Event Type: Full-day in-person event

Join us at the annual GFFT Symposium for the grand finale of the German Startup Cup and the Use Case Award in Cybersecurity and AI & Software categories. This prestigious event showcases the pinnacle of innovation, recognizing outstanding achievements in the tech industry.

Dive into a day filled with high-level panel discussions, inspiring keynotes, and the chance to explore groundbreaking technologies and solutions presented by exhibitors and innovative startups. This symposium serves as a vital platform for discussing current trends and future developments in cybersecurity, artificial intelligence, and software technologies.

The insights gathered here will contribute to a public call for action to bolster our industrial sector. Together, we aim to tackle the challenges ahead and play an active role in the advancement of Germany's economy. We warmly invite you to be part of this initiative, pushing the boundaries of digitalization and discussing IT's critical role in our future.

More Information: For registration details, additional information, and the event agenda, please refer to page 11 in this magazine. Don't miss this opportunity to engage with leaders in the field and shape the trajectory of technological innovation.

We look forward to welcoming you to an event that promises to be a milestone in driving forward the digital era.

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

Discover the forefront of cybersecurity innovation as heylogin, Primary Target, and SANCTUARY Systems vie for victory at the German Startup Cup 2024 in Mannheim, judged by a panel of esteemed industry leaders.

The 3 innovative finalists for the final of the German Startup Cup on July 2, 2024 in the Security category at the Phoenix group in Mannheim have been announced: heylogin, Primary Target and SANCTUARY Systems.

In two exciting and well-attended semi-finals, the day's winners Dr. Dominik Schürmann from heylogin on 30th November 2023 and Patrick Jauernig from SANCTUARY Systems on 30th January 2024 prevailed in direct competition with the other startups. As the best runner-up, Jürgen Vollmer from Primary Target secured third place in the final. All three will be competing for the favor of the expert jury and the expert audience in July.

We would like to thank our dedicated jury of experts:

- **Mirko Ross** - CEO and founder Asvin GmbH
- **Jan C. Wendenburg** - CEO, ONEKEY GmbH
- **Tim Maier** - Information Security Officer, Groz-Beckert KG
- **Robert Rohrberg -** Corporate Information Security Officer, Salzgitter AG
- **Martin Zöllner -** Chief Information Security Officer, Huf Group
- **Prof. Christoph Skornia -** Vice President for Digitalization and Sustainability, Ostbayerische Technische Hochschule Regensburg
- **Andreas Pellengahr** - Head of Global Identity & Access Management, Merck KGaA
- **Tim Ohlendorf** - Cyber Defense Center, Gematik GmbH
- **Björn Kaleck** - Head of Global IT Infrastructure, ZWILLING J.A. Henckels AG

With their targeted questions about the startups' business models, they made a significant contribution to the success of the event. A big thank you also to the three other startups KraLos, Betterscan ans Autobahn Security who took part in the German Startup Cup.

GERMAN STARTUP-CUP

UNITED INNOVATIONS AWARDS

Register Now

Secure your place now for the exciting symposium on the topic of agile companies and the final of the German Startup Cup in the Cybersecurity and AI & Software categories on 2nd July in Mannheim.

The symposium will focus on identifying innovation potential in the areas of cybersecurity as well as AI and software technologies. With top-class panel discussions, for example with Dr. Andreas Nauerz (Bosch Digital) and inspiring keynotes such as Dr. Roland Schütz (Phoenix group) and "Future of AI" by Prof. Dr. Antonio Krüger (DFKI), we offer a platform for discussing the latest trends and developments in these key areas. In addition, numerous exhibitors and innovative start-ups will be presenting pioneering technologies and solutions at their stands.

The insights and impetus gained from the symposium will subsequently be bundled in a public appeal to strengthen the industrial location. As a joint initiative, we will rise to these challenges and actively contribute to the further development of the German economy. We cordially invite you to join us in driving digitalization forward and discussing the essential role of IT.

Click here to register for Final-Event:
https://www.united-innovations.eu//startup-cup/Security-AI-Software

Zero Trust Security for Companies

An article by Julian Steil, Rewion GmbH

Image generated with DALL·E by OpenAI.

In the digital era, IT security is a core concern for businesses facing escalating threats and the evolution of technological systems. At the heart of this dilemma is the Zero Trust Security Framework, offering an apt response to modern technology requirements. It departs from the traditional "Trust but verify" approach and instead implements a "Never trust, always verify" policy. In this regard, Zero Trust marks a shift from the centralized "castle" mentality to a decentralized architecture redefining security in the age of cloud services, remote work and an accessible digital world.

The Security Castle

To defend themselves against cyber threats organizations have built up a “security castle”. With the network perimeter as the main defend mechanism companies created their castle wall and protected themselves from the outside. This is still a strong way of protection as, if correctly done, the network shields the environment against the outside world. However, this protection is not sufficient anymore to cope with modern requirements.

Modern requirements

With the digital transformation, the cloud world and our dynamic way of collaborating with each other the security castle needs to open more and more to the outside world. A company’s IT landscape transforms to be decentralized. This means, to protect resources, systems and data that is outside of this castle, organizations need a new approach – Zero Trust.

Introduction to Zero Trust

Zero Trust, developed out of the necessity to rethink traditional security models, establishes

three fundamental principles: constant authentication, minimal access, and the assumption of security breaches. This model aims to anticipate, prepare for, and minimize the impacts of attacks.

Protecting an organization

Zero Trust encompasses all IT components and addresses the fundamental silos in IT: identities, data, devices, applications, infrastructure, and networks. In the Zero Trust framework each of this silos need to work together to provide a end-to-end security. Security measures and policies need to be implemented throughout each silo and complemented with a comprehensive monitoring and logging system.

Zero Trust Principles

The principles of explicit verification, "Least Privilege" access, and the assumption of security breaches form the backbone of Zero Trust. These principles promote continuous monitoring and evaluation to detect and respond to anomalies early on. It is not a question of “if our organization gets attacked”, it is a question of “when our organization gets attacked”. Therefore, companies need to embody the Zero Trust principles to protect their organization.

Key Aspects in Zero Trust

The implementation of Zero Trust requires a holistic view and an understanding of the organization. It lays the foundation for a dynamic and scalable policy model that controls authentication and access through the whole organization. The deep understanding of the company’s IT landscape and their users is fundamental for a Zero Trust transformation.

Challenges and Risks:

Despite its advantages, Zero Trust presents challenges, particularly the complexity of implementation and the lack of technical standards. Companies must be willing to adjust existing processes and structures, and develop broad know-how to fully harness the benefits of Zero Trust.

The Zero Trust Security Framework symbolizes a paradigm shift in IT security, providing a robust response to the complex security challenges of the modern digital landscape.

Julian Steil
Consultant IT-Security
Rewion GmbH

Detailed information in the techL profile: Rewion

Creativity Security Operations Center: Cyber Defense with a 360-Degree View for IT and OT

An article by René Odermann, telent GmbH

Image generated with DALL·E by OpenAI.

More frequent, faster, and more dangerous: With increasing cyber attacks on industrial plants, the question of how to protect production from internet-based threats becomes increasingly important for operators. The premier league of cyber defense is a Security Operations Center – but only if its team is equally proficient in cybersecurity as well as technical processes and industrial control systems.

Cyber threats become an immediate danger to industrial plants as soon as they connect directly or indirectly to the internet. This is happening rapidly due to advancing digitization and networking towards Industry 4.0. Consequently, Operational Technology (OT) networks are no longer isolated islands but are becoming increasingly vulnerable through interconnected system components.

The most effective form of cyber defense is a Security Operation Center (SOC). It's comparable to a command center that monitors IT and OT across all levels of a company with a 360-degree view. This involves integrating all security-relevant systems of a company and analyzing them with processes, technical tools, and cybersecurity experts. While SOCs have long been established in the IT world, they pose a new challenge for OT. Common software solutions for pro-

tecting IT products cannot simply be implemented in OT because, for example, they do not speak the same language as plant controls and do not understand their industrial protocols. Another problem for cybersecurity is the long lifecycles of industrial plants, whose older operating systems are no longer supported by security updates.

A security concept that considers both IT and OT requires not only comprehensive knowledge in IT security but also a deep understanding of OT infrastructures and their automation, process, and network control technology. This expertise, possessed by telent through years of support for communication and data networks, particularly in Critical Infrastructure (KRITIS) environments, is consolidated by the systems integrator in its new SOC for IT and OT. The technical foundation is the cybersecurity platform of the European specialist Radar Cyber Security, which automatically checks both areas for security issues. The SOC team verifies the results in the context of specific detection scenarios, individually defined for each customer in advance. Since the SOC is modular, companies not subject to the strict requirements of the KRITIS sector can select from a wide range of Managed Services to gradually increase their security level according to their needs.

A Security Information and Event Management (SIEM) supports the SOC team in monitoring. It includes the Security module "Log Data Analytics" (LDA), which automatically categorizes and analyzes thousands of log data entries for their security relevance. However, expertise is needed to distinguish false alarms from real ones among the countless anomalies. Other security modules such as "Vulnerability Management & Compliance" (VMC) scan the entire IT/OT infrastructure for security vulnerabilities, while "Network Behavior Analytics" (NBA) detects dangerous malware and anomalies. The integrated security solution "Endpoint Detection & Response" (EDR) captures data from endpoints in IT and OT. The SIEM not only accesses IT assets, as usual, but also OT asset log data such as control systems, PLCs, and sensors thanks to a passive OT monitoring solution. The Advanced Correlation Engine consolidates all information for comprehensive risk detection.

Large companies often have sufficient personnel and financial resources to establish an in-house SOC. For smaller and medium-sized enterprises, it is more efficient to purchase SOC services externally – also as an audit-compliant solution that meets the requirements of the IT Security Act 2.0. A real added value in a SOC specialized in both IT security and OT infrastructures is created by the interdisciplinary team, which deals with cybersecurity on a daily basis and is well-informed about current developments.!

René Odermann
Head of Sales & Business Development Cybersecurity
telent GmbH

Detailed information in the techL profile: telent

In the Crosshairs of Cybercrime: How Companies Can Fortify Against the Rising Threat

The situation is dramatic, as the threat in cyberspace is higher than ever before. The German Federal Office for Information Security (BSI) emphasised this in its latest situation report. Nobody can feel safe anymore, because not only large corporations are affected, but also small and medium-sized companies. According to many experts, every German company will fall victim to a cyber attack at some point. So it's not a question of if, but when. It is therefore only understandable that the focus is shifting to cyber risks and their defence - and absolutely necessary.

After all, the effects of an attack can be devastating and, in the worst case, even threaten a company's existence. According to calculations by the digital association Bitkom, cybercrime losses in Germany totalled 203 billion euros in 2022, according to the Economic Protection Report. Ransomware attacks, in which systems are compromised in such a way that business-critical data is encrypted, cause considerable damage. Such attacks entail a great deal of work in terms of damage limitation and recovery and can severely damage a company's reputation. In addition, ransomware attacks only offer the prospect of decryption against payment of a ransom. As if that wasn't bad enough, the blackmailers also threaten to publish the previously stolen data.

Every company should therefore prepare for an emergency in order to be able to react appropriately. However, it is even more important to massively intensify prevention. Attackers are also be-

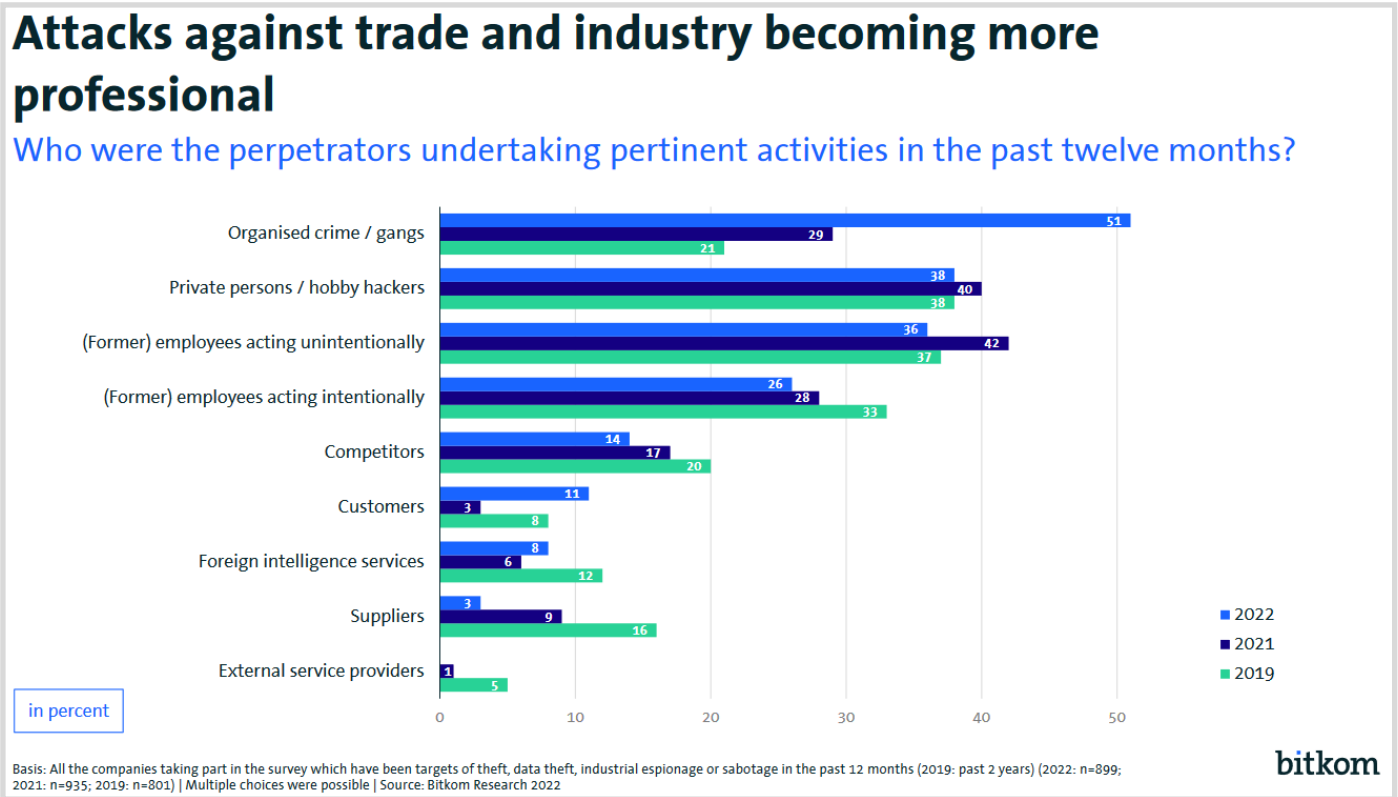

Photo by freepik

coming increasingly professional and are organising themselves into units based on a division of labour. There are regular teams of system administrators, developers and the actual hackers. However, this also means that not everything can be left to the IT department on the company side. On the contrary, IT security is business-critical and affects the entire company.

For this reason, many companies already have Security Operations Centres (SOC), i.e. specialised units that bundle all services relating to IT security. They are involved in analysing and defending against attacks as well as in prevention and risk minimisation. This is undoubtedly a major challenge and requires a high level of expertise. It is understandable that not all companies can muster this expertise and want to provide it around the clock on their own. In this case, it makes sense to outsource these services to specialised service providers. As threatening as the situation is in the face of increasing cyber risks, there is still a viable way for every company to arm itself. So the situation is threatening, but companies are not defenceless - and that is good news.

Ramon Weil
Founder & CEO
SECUINFRA GmbH

Detailed information in the techL profile: SECUINFRA

Zero Trust and (Why It Isn't Always About) Identity

What is the relationship between zero trust and user identity? There's no doubt that identity is a fundamental component of an effective zero trust approach, but there is also a danger that organisations become so overly focused on this one element, they forget there are others.

An article by Neil Thacker, Netskope, Inc.

To believe that achieving zero trust is all about user identity is, I believe, a fundamental misunderstanding of the concept. This misconception can lead to potential vulnerabilities that, in turn, can result in major cybersecurity events—the kind of events that the organisation was attempting to avoid by adopting zero trust in the first place.

Identity matters, but it's becoming increasingly unreliable

Identity is indeed a fundamental factor of zero trust and, for many years, companies have used multi-factor authentication (MFA) to ensure their sensitive data is protected. However, the threat landscape is evolving and some experts now estimate that up to 70% of MFA options are as easy to breach with social engineering and phishing.

Outside of the cybersecurity world, we would not place our trust in someone based on one factor alone. Trust is a multifaceted process that must build up over time. Likewise, there must be multiple forms of verification in order for zero trust to be achieved. Oversimplifying the complexity of this process risks giving the false impression of safety, and opens the potential for a major cyber breach.

Multiple security measures, a single point of control

Zero trust must start with the assumption that your system can and will be compromised. The more measures put in place to protect it, the more trust we can put into it. Crucially, a single Policy Enforcement Point (PEP) must be used to control the traffic of information flowing in from these different measures.

Identity authentication is one of the first, and one of the most commonly used, measures for zero trust and should be a core part of any strategy. This includes things like decentralised identity, more advanced MFA frameworks and password-free biometric methods. However, it is not sufficient by itself .

Here are seven other elements businesses should build into their PEP to ensure a secure, robust zero trust infrastructure:

Device

It's not just who you are, but what device you're using. A fully authenticated user on a compromised device is still a security risk. Zero trust should differentiate corporate and personal devices, examine device health, patch levels, and security configurations before granting access.

Location

With the rise of hybrid working, organisations should anticipate users attempting to access material from different locations. Therefore, there must be a system that can flag unusual trends. For instance, if a user attempts to login one day from London, and then in the next hour from the other side of the world, this should be flagged in the system—it should not be left up to chance. Similarly, the system should flag if someone is logging in at the same time from two disparate locations.

App

With the rise in cloud services, there are many competing apps that perform the same function. Therefore, security teams should be vetting and approving specific apps for corporate use and, where necessary, putting in place advanced controls and/or restrictions on unapproved applications to mitigate potential data loss.

Instance

Within each cloud app, there are also different types of instances of the same app. For example, many organisations allow employees to use their personal cloud apps such as personal instances of Microsoft 365. This however can lead to an issue especially if confidential corporate data is being shared to a personal app. Therefore each instance of each app should also be understood.

Activity

Zero trust extends into how applications interact with each other and how they access data. Even within a single user's session, the actions an application takes on behalf of that user are subject to scrutiny.

Behaviour

Identity may grant users initial access, but behaviour thereafter should be continuously scrutinised. If an employee (or entity) starts accessing large volumes of data suddenly or downloads sensitive files, alarms should sound, even if the user was initially authenticated.

Data

At the heart of zero trust is data—it's all about ensuring data integrity and confidentiality. This means encrypting data at rest and in transit, and monitoring data access patterns for anomalies, regardless of the user's identity. This would include measures to automate data categorisation and implementation of specific or enhanced controls should that category require.

Identity is undeniably a cornerstone of the zero trust model, but it remains just one piece of a complex structure. If an organisation overly fixates on identity, they're setting themselves up for failure, and leaving themselves at risk to the kind of cyber breach that zero trust is designed to prevent.

True zero trust is only achieved when an organisation has an integrated, holistic approach that considers every touchpoint, user, and device. By incorporating all eight elements into their zero trust approach (including identity), organisations can operate with far greater confidence and security can become a true enabler, making it possible to innovate and adapt to whatever the business needs, whether that means adopting new applications, integrating AI, expanding into new markets or encouraging hybrid work.

Neil Thacker
CISO
Netskope, Inc.

Attacks on Artificial Intelligences

With the rapidly increasing use of AIs such as ChatGPT, the risk for this class of software to be attacked is also increasing. We have investigated and compared the attack possibilities.

An article by Prof. Dr. Sachar Paulus and Christian Höfig, Hochschule Mannheim

AI technologies are currently attracting a great deal of attention due to the success of ChatGPT (and thus also of other largescale language models). In addition to the consequences for scientific honesty, which should be viewed critically, the extent to which these AI applications actually tell the truth and how they handle the information entrusted or transmitted to them is also a cause for concern. One particular aspect here is: how easy is it for an attacker to attack and manipulate an AI? Which attacks are likely to be the easiest / most successful? We took a closer look at this as part of a bachelor's thesis at the Faculty of Computer Science at Mannheim University of Applied Sciences.

A basic distinction can be made between general software attack methods and AI-specific attack methods. In the case of the latter group, a distinction can also be made according to the time at which the attack takes place: in the training or usage phase (technically this phase is called the inference phase).

Like any software, an AI application can also be attacked using "classic" methods. We have considered the following attack methods: Injection, ransomware, APT, DoS, man-in-the-middle and buffer overflow. Even if these methods make it possible to attack the operator's infrastructure (e.g. encryption of the database to blackmail the operator, or DoS to prevent the use of the service), we primarily examined them in their role as preparatory work or precursors for the attack on the AI itself.

Attack targets on the AI itself can be classified as follows:

- Determination of decision parameters of the model on which the AI is based (e.g. to predict decisions),
- Modification of the model to manipulate decisions / responses of the AI,
- Identifying confidential information (e.g. contained in training data) and
- Modification of requests and responses to an AI in order to manipulate a specific requester by means of AI responses.

As part of Christian Höfig's bachelor thesis, 15 different types of attacks on AI were examined and compared by means of a literature analysis (to determine typical attacks on AI), a comparative study using attack trees (to structure the various attack paths in the same way) and a risk assessment using the OWASP Risk Rating method. The work also implemented two prototype attacks using the example of an AI model for detecting skin cancer and demonstrated the simplicity of the implementation.

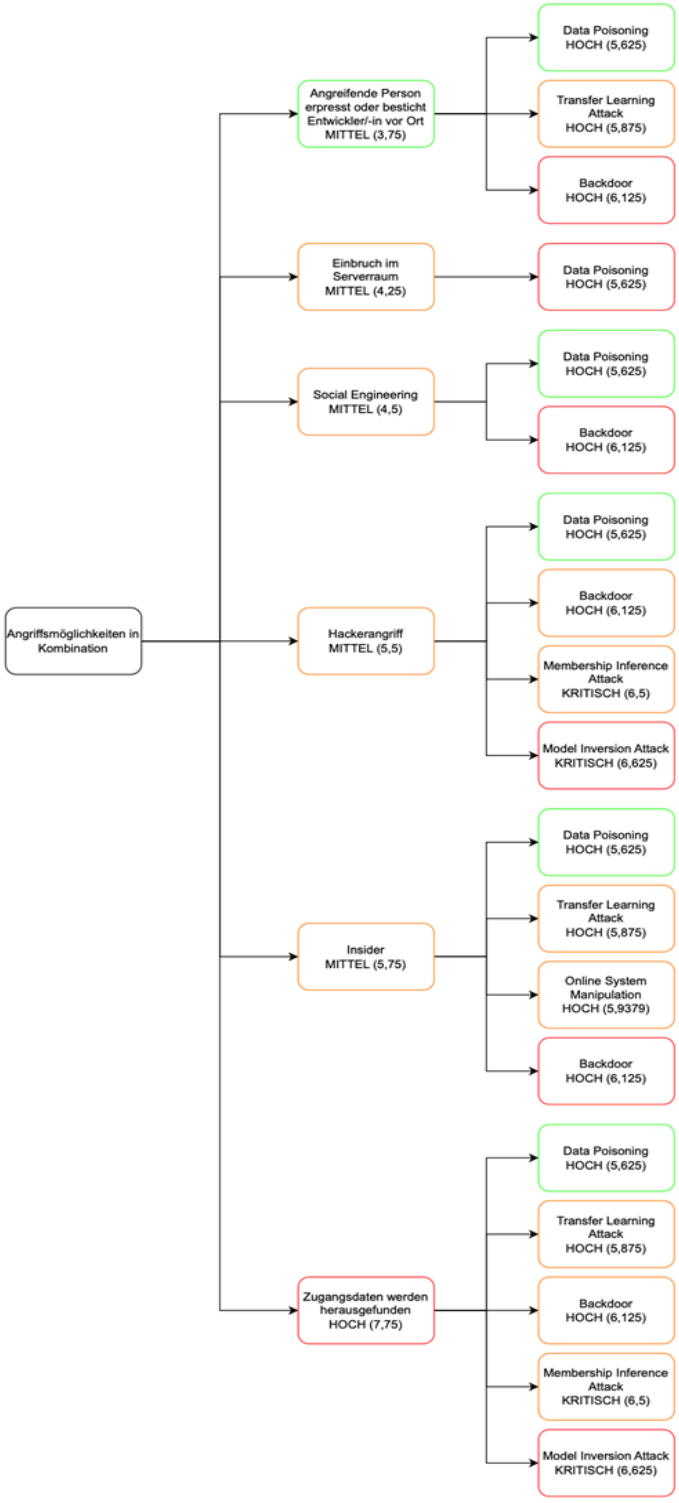

Fig 1: Overview of the path and attack on an ML model

The graphic in Figure 1 shows an overview of the combination of the risk assessment of the attack path and the content of the attack on a machine learning model. Not surprisingly, the identification of access data (e.g. via phishing, APT, man-in-the-middle) is the most likely attack path. The "Membership Inference Attack" and "Model Inversion Attack" are two highly rated attacks that determine the AI's decision parameters or aim to manipulate decisions.

How can we protect ourselves against this? The following aspects were identified as effective countermeasures:

1. augment data records and check for anomalies,
2. secure access to the model through strong authentication and authorization,
3. check user input for plausibility,
4. do not use data from insecure or dubious sources, and
5. assure a high level of security awareness with the operator´s employees.

Prof. Dr. Sachar Paulus
Fachgebiet IT-Sicherheit
Hochschule Mannheim

References

Höfig, C. (2024). *Angriffe auf Künstliche Intelligenzen* [Bachelorarbeit]. Hochschule Mannheim.

Systemic opportunities and risks of IT security

An article by Prof. Dr. Dr. h.c. Ortwin Renn, Research Institute for Sustainability - Helmholtz Centre Potsdam

In order to adequately grasp and analyze the complexity and dynamics of IT security, a systemic perspective on the opportunities and risks of digitization in relation to security aspects is essential. This perspective makes it possible to better understand the manifold interactions between the prerequisites, conditions and consequences of IT security and, on the basis of this understanding, to design options together with all stakeholders. Unlike many other controversial fields of technology, such as genetic engineering or nuclear energy, the opportunities and risks of digital technologies are not inherent in the technology itself, but arise predominantly from the way in which digital applications and services are designed and regulated (Renn et al. 2021).

This openness to design requires close and constructive cooperation between all stakeholders. This is particularly true in the area of IT security, where all stakeholders are working together in a security partnership to ensure that even the weakest link in the chain still has sufficient resilience against cyber attacks or other security deficits (Daud et al. 2018).

The systemic view of IT security integrates insights into technical diversity, economic forms of organization, regulatory frameworks and social or individual behavior. All four areas of influence are interconnected and mutually dependent. The prerequisite for successful IT security governance, however, is the maintenance of technical functionality even under stress or cyber attacks (resilience) (Björck et al. 2015). This requires protection against internal and external disruptions, a competent defense against cybercrime and attacks by private or state actors, and globally coordinated control and user-friendly further development of the Internet.

Building on reliable and consistent availability of the network, further requirements can be placed on the design of digital services and applications. Within the framework of the systemic view of IT security, the aim is, on the one hand, to ensure sovereignty and participation in digital events by all population groups and organizations and, on the other hand, to enable digital services with minimal or at least manageable risks of data misuse, hacker attacks and fraud.

The digital services offered are free for most users. Whether search engines, navigation services, social networks, communication forums or functional control processes - all of these are provided by providers without financial consideration. Payment is made indirectly through the provision of data, which in turn can be exchanged for money by the providers with advertising customers. This new form of payment opens up access to digital services for all sections of the population, including those with only low purchasing power. The prerequisites for this are the possession of an Internet-capable device, Internet access and the ability to find one's way around the Internet (digital literacy).

The practice of today's data economy, however, endangers data security, especially also the sovereignty over one's own data. The protection of privacy, transparency about further data use, misuse of data are essential risks that contribute to a feeling of powerlessness and of being "at the mercy" of digital providers (Scholz et al. 2021) . Although this form of data transfer takes place legally and often even with the user's consent, many feel powerless, squeezed into a complex data-shifting orbit.

In addition, the emerging Internet culture suggests certain attitudes, beliefs and lifestyles that contradict the original idea of a home for diversity (Acatech 2021). Keywords here are cancel culture and political correctness (Scheepers and Ellemers 2019). At the same time, the anonymization of social networks is increasingly blurring the line

between objective criticism, personal insults and threats.

The climate of debate is becoming harsher, echo chambers are becoming more attractive, and the culture of factual disputes is being replaced by insinuations, gloating and polarization (Renn 2023).

Anonymity in social media opens up the possibility of expressing one's own opinion without fear of reprisals; at the same time, however, it creates the risk of a one-sided debate that can be characterized by mutual recriminations, personal insults and threatened acts of violence. In the long term, these processes endanger social coherence, democratic decision-making and social identity.

In addition, there is the risk that third parties will deliberately use the possibilities offered by the Internet to rob, defraud, blackmail, damage their reputation, or otherwise harm people. Despite continuous improvements in cyber security, this risk of cyber attacks has grown in recent years, according to the BSI (Schünemann 2020). Entire mafia structures have now emerged that systematically use Internet access to blackmail users. The spread of fake news and misinformation is also becoming increasingly successful thanks to sophisticated methods of deception using AI, manipulative sound and image editing, and other technical innovations.

New social initiatives and effective government regulations are needed to better deal with these social risks. These initiatives should bring together all relevant stakeholders in discourses to jointly create rules that can prevent the risks from expanding. The goals of these initiatives include, for example, improving digital literacy in all segments of the population, free access to the Internet, improved identification options for anonymous users who spread hate mail, and, above all, clear rules and laws on data security and data sovereignty.

If the risks continue to increase, the productivity and performance of digital services will be permanently diminished, and the acceptance of digital innovations will suffer at the same time. The future of digital services depends heavily on the will of the players involved to shape it in line with sociall and ethical criteria. There is no doubt that digitization offers enormous potential for individuals and society. At the same time, however, digitization is associated with many risks, some of them systemically profound, which can and should at least be limited, if not avoided, based on objectives that respect ethical values and the common good.

Prof. Dr. Dr. h.c. Ortwin Renn
Affiliate Scholar
Research Institute for Sustainability - Helmholtz Centre Potsdam

References

Acatec & Körber Stiftung (2021): Technik Radar 2021. Kurzbroschüre. Acatech: München

Björck, F., Henkel, M., Stirna, J. & Zdravkovic, J. (2015). Cyber Resilience – Fundamentals for a Definition. In: Rocha, A., Correia, A., Costanzo, S. & Reis, L. (Hrsg.): New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing, Band 353. Springer: Cham, S. 311-316, https://doi.org/10.1007/978-3-319-16486-1_31

Daud, M., Rasiah, R., George, M., Asirvatham, D., & Thangiah, G. (2018). Bridging the gap between organisational practices and cyber security compliance: can cooperation promote compliance in organisations? International Journal of Business & Society, 19 (1): 161-180

Renn, O. (2023). Gefühlte Wahrheiten. Orientierung in Zeiten postfaktischer Verunsicherung. Budrich: Frankfurt am Main

Renn, O.; Beier, G. & Schweizer, P.-J. (2021). The opportunities and risks of digitalisation for sustainable development: A systemic perspective. GAIA, 30 (1): 23-28

Scheepers, D. & Ellemers, N. (2019). Social Identity Theory. In: Sassenberg, K. & Vliek, M.L.W. (Hrsg.): Social Psychology in Action. Springer: Cham, S. 129-143, https://doi.org/10.1007/978-3-030-13788-5_9

Scholz, R. W., Beckedahl, M., Noller, N. & Renn, O.: Sozial robuste Orientierungen für einen verantwortungsvollen Umgang mit digitalen Daten: Zusammenfassung und Perspektiven. In: R. W. Scholz, R.W.; Beckedahl, M.; Noller, S. & Renn, O. Hrsg.): DiDaT Weißbuch: Orientierungen zum verantwortungsvollen Umgang mit digitalen Daten – Orientierungen eines transdisziplinären Prozesses. Nomos: Baden -Baden, S. 1-69.

Schünemann, W.J. (2020). Cybersicherheit. In: Klenk, T., Nullmeier, F., Wewer, G. (Hrsg.): Handbuch Digitalisierung in Staat und Verwaltung. Springer VS: Wiesbaden, S. 1-11, https://doi.org/10.1007/978-3-658-23669-4_17-1

Taddeo, M. (2019). Is Cybersecurity a Public Good? Minds & Machines, 29: 349–354, https://doi.org/10.1007/s11023-019-09507-5

Cybersecurity in Organic Drone Swarms

An article by apl. Prof. Dr. Mathias Pacher and Prof. Dr. Uwe Brinkschulte, Goethe-Universität Frankfurt am Main

Drone swarms are today of major interest for several applications such as monitoring and controlling missions e.g. for police authorities or military forces. We use Organic Computing techniques to control a drone swarm in a highly dependable way. However, since we have to use wireless links for the communication between the drones and the ground control station, we have to ensure that the communication is unharmed by potential attackers. Our project deals with two dimensions of security: First, we use encryption and second, we use trust metrics to evaluate the trustworthiness of other drones in the swarm.

Organic Computing

The complexity of embedded distributed systems is strongly growing in the last years. In addition, they are used in several application domains such as automobiles, trains, working spaces and so on. This imposes several requirements on the reliability of such systems: The driver of a car wants the car work properly even if there are software failures e.g. in the entertainment or the navigation system or even if some processors fail.

That is where the idea of Organic Computing (OC) starts: We observe and mimic strong dependability features in biological creatures. If e.g. a cell in the human body dies, the person usually does not even recognize this. In general, we can observe so-called self-X features (X=healing, optimization etc.) in biological creatures. The major aim of OC is now to implement such self-X features in technical embedded systems.

We developed two main contributions to OC:

1. An Artificial Hormone System (AHS): The AHS is a task distribution system implemented as middleware. It is inspired by the human endocrine system and uses artificial hormones (short messages) to enable task distribution. It is completely decentralized and has therefore no single-point-of-failure. Moreover, it offers features such as self-configuration (task distribution is done automatically), self-healing (tasks are re-distributed in presence of task or processors failures) and self-optimization (task distribution is optimized depending on the current system state). Additionally, we can provide real-time bounds for the self-X features of the AHS.
2. The Artificial DNA (ADNA) system: The idea of the ADNA system is that most embedded systems consist of a limited set of basic blocks such as ALUs, memory, controllers etc. This means we can describe the structure of the embedded system by a small netlist. We call this netlist Artificial DNA because its function is similar the biological DNA. The ADNA is spread on all processors of the embedded system where the local ADNA builder extracts the resulting tasks from the ADNA. They are then distributed by the AHS. The ADNA system works properly. A demonstration video where a autonomous balancing vehicle is controlled by several Raspberry Pis can be found here.

Securing an Organic Computing controlled drone swarm

In the project (The project is funded by the Hessian Ministry of the Interior and Sport) presented here, we develop a drone swarm with ground control station controlled by our ADNA/AHS approach. The system architecture is shown in Figure 1. The advantage of using the ADNA/AHS system for controlling the drone swarm is that the OC dependability features mentioned above are inherently available for the drone control system making it dependable. This means that control tasks of a drone can easily be switched to another drone in case of a failure, thus providing graceful degradation.

We work with both a drone simulator (AirSim, https://microsoft.github.io/AirSim/) to test new strategies as well as with self-built drones for real-world flight tests.

The Hessian police flight squadron is our partner in this project and our main source for flight maneuvers the drone swarm has to perform.

However, as the ground control station and the drones are connected per WiFi, the communication is vulnerable and potential attackers might compromise the communication or might even try to infiltrate the swarm by own drones.

Our project countermeasures these attacks in two dimensions:

1. We encrypt the communication: This means we add a signature such as SHA-128 to the hormone telegrams to ensure integrity. The payload data in the ADNA messages is encrypted to ensure privacy of the data.
2. We use trust algorithms: Trust is a social concept meaning that if e.g. two humans know each other they might help each other if needed. This concept can be transferred to our ADNA/AHS system: the drones evaluate the trust metrics for each other drone and use these values for configuring the AHS and to decide if they take the payload data in the ADNA messages. This concept is therefore an extension of today often used zero trust architectures.

Benefit by the project

The work on this project offers benefits for scientific research on the one hand, as it helps us securing the ADNA/AHS system against attackers. On the other hand, the project has impact for the Hessian police flight squadron as they need innovative new solutions for drone surveillance missions since they currently have to use proprietary products from Asian companies.

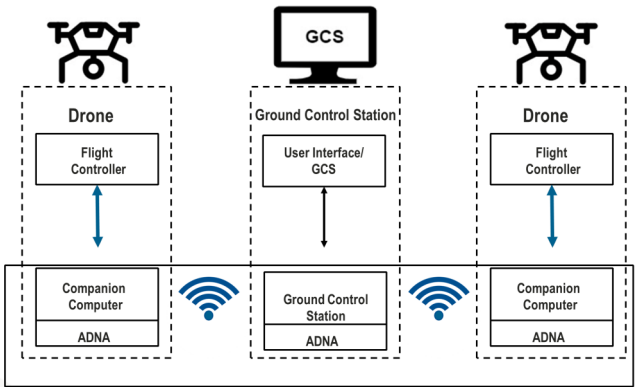

Figure 1: The system architecture

Mathias Pacher
apl. Professor
Goethe-Universität
Frankfurt am Main

Uwe Brinkschulte
Professor
Goethe-Universität
Frankfurt am Main

Research Project: SecDER - Making virtual power plants resilient

An article by Oliver Küch and Anna Spiegel,
Fraunhofer-Institut für Sichere Informationstechnologie SIT

Photovoltaic and wind energy plants that produce in a network are exposed to a wide range of risks. Even a minor disruption in IT or plant technology can have far-reaching consequences for functionality. In the SecDER research project, six partners from science and industry have investigated how the power system can become more resilient with virtual power plants.

The background to the need for research is the transformation of the energy system: In a decentralized energy system, many small and distributed plants work together and are jointly operated by a control system - the virtual power plant. The decentralized units communicate via a smart grid in real time and can become the target of cyber attacks in the process. Operation is also technically challenging: The plant park uses a wide variety of generation and storage technologies to optimize the use of sun, wind and storage in such a way that it results in a reliable and economical power supply.

In the future, the security of power supply will depend to a large extent on the resilience of virtual power plants.

A tool for IT security and smooth plant operation

What's special about SecDER is that it takes an equal look at plant operations and data processing and bundles them into one application.

On this basis, a detection system for attacks and technical faults can then be set up in a virtual laboratory. This simulation environment can be used to virtually replicate the real behavior of the plants and test strategies for resilient defense against cyber attacks and technical faults at virtual power plants. These results will then be further developed in practice.

Attack detection and resilience

In SecDER, Fraunhofer SIT has developed strategies for detecting attacks on the IT of virtual power plants and for securing ongoing operations in the event of a successful attack. The researchers formulated recommendations for action for the resilient operation of VPP and incorporated their findings into a demonstrator. For example, they developed a Resilience Monitor, named "HealthDashboard", where the relevant resilience information are summarized. Furthermore, they developed a Resilience Index, which measures the overall resilience of the VPP. "A particular focus is on ensuring that systems can continue to do their job - even in the event of an attack. Finally, we also ensure that the operators of such plants have means at their disposal that give them an advantage over attackers - we wanted to design systems in such a way that they can be brought into a trustworthy state at any time", explains George Gkoktsis, researcher at Fraunhofer SIT.

Photo by The Sky on Unsplash

Adapting existing ICT concepts to energy supply

Another focus of the research project is on various protection measures. Up to now, IT protection systems have been developed individually for each virtual power plant. As part of SecDER, common IT systems are to be adapted to the needs of the energy industry. In particular, this includes security requirements and standards for the platforms and networks used.

Systems for anomaly detection, which classify unusual behavior as an indication of an attack, are known from other applications. The aim was to investigate whether such systems can also increase security in the operation of virtual power plants. Machine learning concepts are already being used extensively. In practice, however, they are highly susceptible to interference. The aim of SecDER was therefore also to investigate Trustworthy AI. Researchers looked into Adversarial Machine Learning and how this can affect the VPP.

About SecDER

The research project, funded by the German Federal Ministry for Economic Affairs and Energy (BMWi) and supported by Project Management Jülich, started on April 1, 2021, and was running for 36 months, it is currently being finalised. The total funding volume amounts to 2.7 million euros. Scientists from the Fraunhofer Institutes for Energy Economics and Energy System Technology (IEE) and for Secure Information Technology (SIT), as well as from Hannover University of Applied Sciences and Arts, have been working together with companies in the industry to develop an information system for faults in decentralized power supply.

Further detailed results of the SecDER project will be published in the course of 2024.

Oliver Küch
Innovation Manager,
Digital Hub
Fraunhofer-Institut für
Sichere Informations-
technologie SIT

Co-Autorin: **Anna Spiegel**, Fraunhofer-Institut für Sichere Informationstechnologie SIT

C-ORG – Comprehensive ORGanization

How crucial is the incorporation of comprehensive intra- and inter-organizational structures for achieving consistent rights in business application systems? What specific challenges arise from the inconsistent assignment of actors? How does C-ORG contribute to achieving consistent rights allocation, ensuring adherence to (security) policies, and reducing maintenance efforts during organizational changes?

An article by Prof. Dr. Alexander Lawall, IU International University of Applied Science

Consistent access rights in business application systems necessitate the incorporation of comprehensive intra- and inter-organizational structures. The core challenge in current approaches arises from the inconsistent assignment of access rights, particularly impacted by organizational changes such as hiring, relocation, and departure of actors within companies. This inconsistency results in the violation of (security) policies within organizations. The novelty of this work primarily lies in the development of an organizational metamodel and a corresponding declarative query language. This composition enables consistent rights allocation, ensuring adherence to (security) policies in business application systems. Additionally, it reduces the maintenance effort in these systems during the mentioned organizational changes.

Various application systems exist within companies, encompassing programs developed for specific business areas, along with associated data and infrastructure. These systems are classified based on organizational levels such as the strategic, management, and operational levels. Enterprise-wide application systems focus on automating processes across different organizational levels and business functions, categorized by features like system type, target audience, and functional areas. Security, in terms of access rights and obligations, is a crucial factor in deploying these systems, with internal and external security policies playing a role. C-ORG specifically considers security models for access control, addressing the growing need to adapt access control to inter-organizational collaborations and globalization. It emphasizes the importance of incorporating both internal and external security policies into access control models and integrating inter-organizational structures, thus ensuring the consideration of security requirements within a company. A security mechanism is required to depict both intra-organizational and inter-organizational contexts.

Problem and Motivation

Many application systems manage redundant information about organizational structures, including actors and their permissions. The decentralized information representation results in high administrative overhead during organizational changes, leading to increased susceptibility to errors in enforcing security policies. This, in turn, causes inconsistencies, anomalies, lack of compliance, and violations of security policies.

The continuous turnover of actors and restructuring of the organizational structures necessitate ongoing maintenance regarding access rights in each application system. Provisioning within application systems poses a challenge during activities like hiring, departure, relocation, or changes to the attributes and relations of actors. The core

issue revolves around the inconsistent assignment of actors for rights and obligations.

Specifically, the assignment of actors involves challenges in complete enumeration, variant diversity, and inadequacy. Contemporary access control models rely on the complete enumeration of actors, requiring modifications in all affected applications of application systems during organizational changes. This makes the assignment more prone to changes introducing vulnerability to changes and a discrepancy with reality. Secondly, variant diversity emphasizes the need to consider diverse organizational contexts for precise configuration of access rights. The discrepancy between contemporary approaches (i.e. Role-based and Attribute-based approaches) and real-world scenarios complicates this issue. The third subproblem, inadequacy, highlights the disparity between actual circumstances and the representation of rights in application systems, considering the power of the metamodel and currency of the model.

Solution: C-ORG

C-ORG integrates practical requirements with content from the theoretical knowledge base. The core focus is on developing an organizational metamodel and corresponding formal languages, formally representing organizational structures. The metamodel for intra- and inter-organizational structures and declarative assignment of actors in application systems is the goal.

Representation of Organizational Structures: The metamodel encompasses elements for representing various intra- and inter-organizational organizational forms (e.g., single-line, multi-line, staff-line, matrix, tensor, network, project, and virtual organizations). It formalizes different categories of relations within the metamodel, connecting entities such as organizational units, functional units, and actors. Relations' validity can be restricted based on attributes of actors, parameters, contexts from application systems, and dependency on the acting functional unit/role.

Declarative Assignment of Actors: A declarative query language facilitates querying actors based on organizational entities, relations, and attributes modeled in the organizational model. The language allows querying actors through associated organizational units, functional units, and specific actors. Extending the query language with relations enables querying actors based on organization-specific relations (e.g., deputy, supervisor, and reporting relationships) within the organizational model. Including actor attributes (e.g., certificates, qualifications, salary grouping, and employment date) in the query language provides a detailed description of required conditions.

Internal Language for Restrictions and Propagation: Internally (inside the model), a language is used to describe restrictions on relations based on actor attributes, parameters, and contexts from application systems. This language is also utilized for propagating elements of the organizational model within inter-organizational collaborations, ensuring up-to-date representations of involved companies' states and preventing unauthorized access, erroneous actor assignments, incorrect message recipients, and outdated content in various systems (e.g., Content Management and Customer Relationship Management Systems).

Prof. Dr. Alexander Lawall
Professor of Cyber Security
IU International University
of Applied Science

AN ASSESSMENT OF THE SITUATION:

On the way to digital service management with ITSM, ESM & CSM

The topic of service management plays an important role for the entire IT landscape and for companies in general. It encompasses various aspects, including Enterprise Service Management (ESM), IT Service Management (ITSM) and Customer Service Management (CSM). Nowadays, many IT decision-makers discuss these concepts, but misunderstandings often arise due to different definitions and interpretations. This position statement attempts to create clarity and provide an annotated definition and understanding of these terms. **An article by Axel Himmelreich, SVA System Vertrieb Alexander GmbH**

Definitions and understanding

IT Service Management (ITSM)

ITSM comprises measures, methods and technologies that aim to ensure the best possible support of business processes by the IT department. The focus here is on the transformation of information technology towards internal customer and service orientation. The focus is on ensuring and monitoring business services, i.e. IT services that can be consumed by internal customers. ITSM enables the continuous improvement of efficiency, quality and profitability of the IT department.

Enterprise Service Management (ESM)

ESM extends the ITSM approach to include measures, methods and technologies that ensure the best possible support for business processes throughout the company. This is achieved by aligning the specialist departments with a holistic internal customer and service orientation. The monitoring of all business services, both for external and internal customers, is important. ESM aims to continuously improve the efficiency, quality and profitability of the entire company.

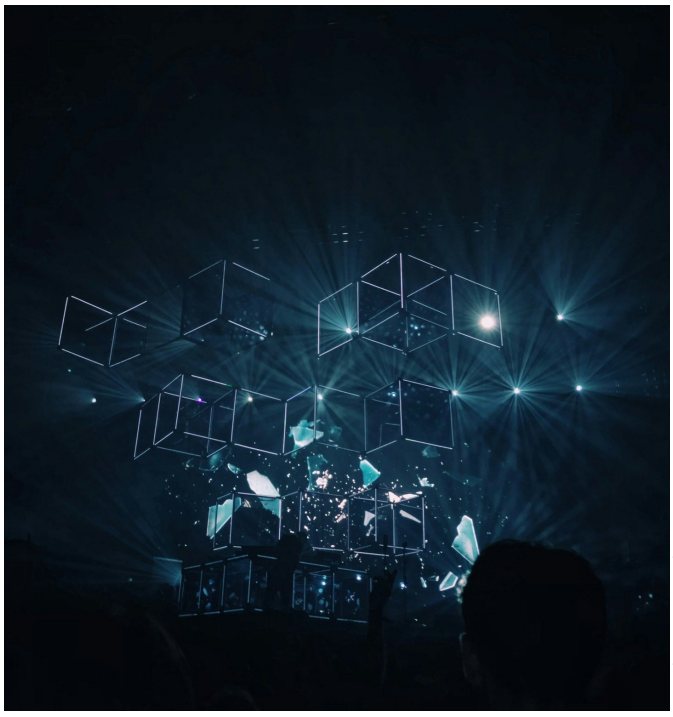

Photo by fabio on Unsplash

Customer Service Management (CSM)

CSM focuses on measures, methods and technol-

ogies that provide the best possible support for business processes that are explicitly consumed by or affect external customers. CSM supports the transformation from a customer-centric to an explicit customer orientation. The application of CSM principles makes it possible to continuously improve quality, customer satisfaction and customer loyalty.

Integration of the models

The three concepts of ITSM, ESM and CSM interlock and expand on each other. While ITSM is integrated both within the company and vertically, the focus of ESM extends horizontally across different areas. By aligning the processes with the principles of CSM, a comprehensive picture is created that extends horizontally from the internal company context to the external company approach. Through the integration of process platforms, these models can be used both in depth and in breadth across companies.

Quintessence 'Digital Service Management (DSM)'

Although the definitions and commentaries presented do not form a universally valid set of rules, they do provide a foundation for joint discussions. This facilitates professional exchange within the service management community and contributes to a better understanding and application of the topics in the daily work context. In view of current developments, it is also becoming apparent that the DSM concept can be seen as an emerging trend and hype in this area.

DMS refers to the management of digital services in an organization. It encompasses the planning, delivery, monitoring and optimization of digital services to increase efficiency, quality and customer satisfaction. DSM uses technologies such as IT service management tools to manage the entire lifecycle of digital services and ensure that they meet business requirements. It helps to ensure seamless and effective integration of digital technologies into everyday business.

DSM will, in our opinion, significantly influence and evolve the way companies practice service management.

Axel Himmelreich
Sales & Value Engineer and Business Process Advisory,
SVA System Vertrieb Alexander GmbH

Detailed information in the techL profile:
SVA System Vertrieb Alexander

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

Autobahn Security GmbH

Autobahn Security is a pioneering force in the cybersecurity landscape, offering a Software as a Service (SaaS) platform that revolutionizes the way IT security teams manage and prioritize vulnerabilities. Based on decades of white-hat hacking and security consulting experience for Fortune 500 companies, Autobahn Security has cemented its reputation as a trusted partner for organizations across diverse industries, including finance, insurance, telecommunications, healthcare, and more.

Technology

The technology underpinning Autobahn Security is designed to *aggregate*, *analyze* and *re-prioritize* vulnerabilities from various sources like Qualys, Nessus, Rapid7, MS Defender or even Pentesting Reports. This innovative approach simplifies the often overwhelming data produced by these sources, transforming them into easily understandable remediation guides. Autobahn Security's algorithm calculates a unique Hackability Score, which serves as a single, effective KPI. This score aids IT teams in gauging their cybersecurity stance from a hacker's perspective, focusing on vulnerabilities that are easiest for attackers to exploit. This KPI can be understood by anyone – from Development and IT, over Marketing to Management.

The platform’s standout feature is its Cyber Fitness Workouts. These are step-by-step guides crafted to offer actionable solutions for identified vulnerabilities. The workouts are designed for ease of understanding and implementation, even by non-security experts, ensuring that organizations can efficiently address security flaws.

This not only makes the remediation process more manageable but also substantially reduces the time and resources required for effective vulnerability management.

Benefit for the user

Using the Autobahn Security platform significantly enhances the efficiency of security operations by automating the prioritization and remediation process, saving valuable man-hours and cutting operational costs. Customers from Autobahn Security are able to reduce the time between Detection and Remediation of vulnerabilities by 70% to 90%, in the first week of using the software.

Companies are able to identify and remediate those issues without any Cyber-Security knowledge, freeing them from the pressure of competing for expensive and scarce personal resources in this field. It provides a dynamic and up-to-date view of the whole organization's security posture, enabling quick response to all emerging threats. The reduction in Hackability Score directly correlates with a lowered risk of data breaches, thereby protecting against severe financial and reputational damage. Last but not least, the platform's scalability ensures it caters to both large enterprises and small-to-medium businesses, making it a versatile tool for diverse organizational needs.

Christopher Hablitzel
Head of Sales
Autobahn Security GmbH

Betterscan.io

Betterscan.io is a cloud-native cybersecurity software designed to secure both cloud environments and applications. It functions as a DevSecOps tool, automating thousands of checks to eliminate human errors in source code and cloud infrastructure. This software can be integrated into various systems and platforms, facilitating a streamlined approach to cybersecurity.

Key features and characteristics of Betterscan.io include:

1. Security Focus: Developed with a strong emphasis on security, Betterscan.io aims to avoid common security mistakes and pitfalls.

2. Single Platform Solution: It supports modern technologies and is accessible via REST API. The platform is lightweight, fast, secure, and can be integrated with CI/CD systems. It's a "plug out" solution, meaning it doesn't require connecting to external systems for its core functionalities.

3. Wide Language and Technology Compatibility: The software is compatible with a variety of programming languages and technologies, including PHP, Java, Scala, Python, PERL, Ruby, .NET, C#, C, C++, Swift, Kotlin, and many more. It also supports Infrastructure as a Code (IaC) security, secret scanning, and has features for AI/OpenAI GPT integration.

4. Comprehensive Scanning and Analysis: It includes features for SCA (software composition analysis) and supply chain risks, covering the OWASP TOP 10 and supporting the addition of any open-source and proprietary checks.

5. Integration Capabilities: Betterscan.io integrates with popular version control and repository hosting services like Git, GitHub, GitLab, BitBucket, and Google Source Repositories.

6. User-Friendly Reporting: It offers actionable reports accessible via a web browser or CLI (Command Line Interface), and supports quick scanning through incremental/differential snapshots analysis.

Benefit for the user

Betterscan.io positions itself as a comprehensive solution for securing business infrastructures and codebases, providing tools and features that cater to a wide range of cybersecurity needs in the modern digital landscape.

Marcin Kozlowski
Founder
Betterscan.io

Detailed information in the techL profile:
Betterscan.io

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 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

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 profile

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 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 seemingless 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

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

Comuny

Trinity Identity Wallet enables the design of mobile authentication solutions that are both cost-effective and compliant with the new European eIDAS 2.0 framework. Development teams and system integrators can reduce their workload by using a mobile SDK with various ready-to-use features, without UI/UX design constraints. It offers decentralized data management for secure personal data storage on mobile devices. Trinity shifts crucial identity provider functions to a mobile white-label SDK, facilitating scalable and cost-effective cloud operations for backend components, even in highly regulated markets.

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

DeepSign

Even the best security precautions do not guarantee sufficient protection in the event of a cyber attack if the human factor is the target of the attackers. To eliminate this attack surface, we offer INVISID, an AI-based authentication method that verifies a valid user based on a behavioral pattern of mouse and keyboard interactions. This fully automated technology protects the user from digital identity theft continuously, unnoticed and without any loss of convenience.

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

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 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

Enterprises are embracing digital transformation by using multiple cloud providers and moving applications closer to data sources. Our mission is to empower customers with our distributed cloud services platform, Volterra, which supports building, deploying, securing, and operating applications and data across various environments. Volterra offers a SaaS service for application management and secure connectivity across distributed sites in public, private, or edge clouds.

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

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 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

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

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

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

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

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 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

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

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

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