United Innovations

Survey of Tools for Secure Infrastructures and Processes

Release Q1 / 2023

www.security-innovations.eu

Foreword

In the future, companies should take cybersecurity just as seriously as implementing the business model. This is a major challenge because we can see a strongly asymmetrical situation. An attacker only has to succeed at one point, but the defenders have to work flawlessly across all points of attack. The attackers exchange attack patterns and successful methods and organize themselves like a company trimmed for success, while the defenders usually only hold their own with a small team.

Since the bulk of investments are focused on further development and operation of the company's own market offering, it hurts companies greatly to divert significant financial resources to cybersecurity. The situation is also complicated by the fact that corporate communications are constantly increasing; important trends here are home office, data traffic between partner companies, social media, securing production facilities, etc. In order to achieve safeguarding quickly, effectively and cost-efficiently, companies need to collaborate as closely as possible and drive standardization.

United Innovations supports this approach by making know-how widely available and by providing instruments for solving new problem areas. In particular, it seems important to us to facilitate the introduction of innovations through a building block concept. Analogous to the Lego world or prefabricated houses, improvements can be introduced faster, with less risk and at lower cost. This survey, the techL© technology database and the events all follow this concept and present individual building blocks. Research at universities can then lead to the definition and prototypical realization of new building blocks and find their way into the corporate world.

In this Survey, we present readers with a number of solution strategies (Chapter 3) and use cases (Chapter 4). Startups and research results are presented in Chapters 5 and 6. With Chapter 7, we conduct tool research for all readers.

If using it as a report seems too unwieldy for you, you can also find all the information in our technology database techL (www.techl.eu).

In the hope that the information we have compiled, filtered and evaluated will help you, I hope you enjoy reading it.

Dr. Gerd Große

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

Content

Calendar

20.04.2023
15:30-17:30

Insights Infrastuctute & Networks Track: Key Management Lifecycle (Introduction & Discussion) (german)

Key Management Lifecycle includes all operations required to create, maintain, protect and control the use of cryptographic keys. Keys have a lifecycle: they are created, live for a period of time, and then are retired.
Info & Registration

27.04.2023
15:30-17:30

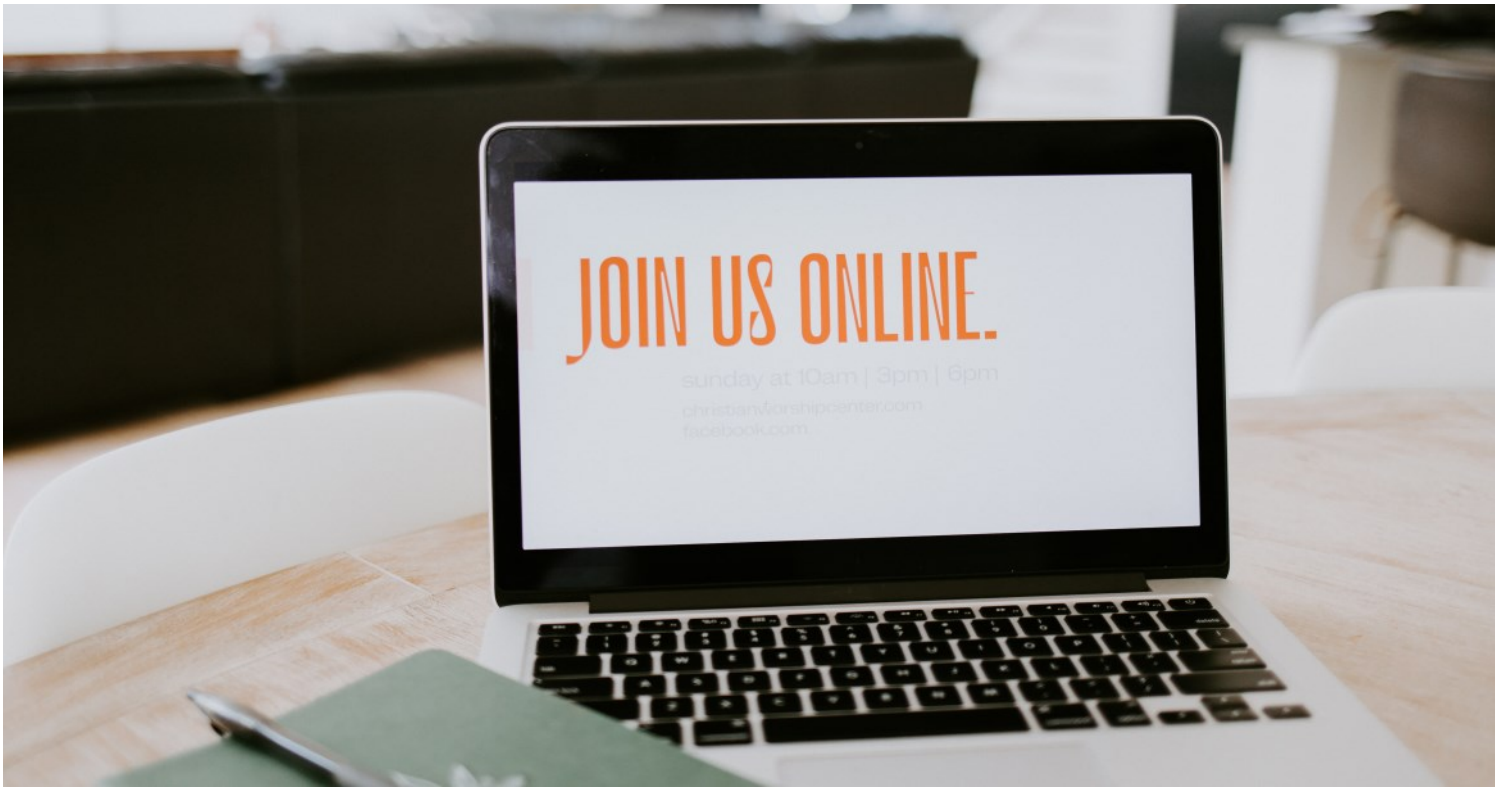
Insights Security Management Track: Security Operation Center (Concept) (german)

The Security Operation Center (SOC) is an operational unit tasked with detecting attempted attacks and enabling countermeasures to ensure that attempted attacks do not turn into attacks with serious consequences.
In cooperation with A1, the Security Lab provides companies with simple practical support. The basic idea is to collect and exchange knowledge about challenges and solutions at companies and to compile solution paths for the most pressing difficulties. In this (open) meeting of our consortium partners, the focus is on the common concept.
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

Image credits: Samantha Borges unsplash



11.05.2023
15:30-17:30

Insights OT-Security Track: Asset Security (Concept Asset Visibility) (german)

The safeguarding of industrial plants is a current and very complex topic in many companies. Often, company representatives are unsure which solution approach is practicable in which situation and what can achieve the greatest improvement.

In cooperation with NTT, the Security Lab provides industrial companies with simple practical support. The basic idea is to gather and share knowledge about challenges and solutions at companies and to compile solution paths for the most pressing difficulties. In this (open) meeting of our consortium partners, the focus is on the common concept of asset visibility.
Info & registration

22.06.2023
16:00-16:45

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

United Innovations
- The innovation network -

The United Innovations (UI) platform is a subsidiary of GFFT e.V., a non-profit society dedicated to research transfer. Its primary objective is to drive innovation in Germany, Europe, and beyond. With its extensive network, the platform is committed to achieving this goal.

United Innovation supports the innovation process in each topic area with the same offerings: (a) the technology database techL©, (b) the surveys, (c) the awards for evaluating new technical offerings, startups and scientific prototypes, (d) many events and (e) proofs of concepts and launch projects.

Executing Innovation together

All countries have to deal with various challenges today, including climate change, digitization, and cyber threats. In the face of global competition, the ability to harness the expertise of businesses and researchers to address emerging challenges and develop innovative solutions swiftly will be essential. At UI, we support all companies to define their innovation goals and achieve them through close collaboration with our extensive network of corporate partners.

Join our network

We focus on a wide range of topics that can be positively impacted by IT, including manufacturing, logistics, business processes, and cybersecurity. Our services promote knowledge sharing, incremental improvements, upfront development of new solutions, and recruitment. Join our network and improve yourself.

DEUTSCHER STARTUP-POKAL
UNITED INNOVATIONS AWARDS

Startups from the digital sector will have the opportunity to showcase their innovative technologies and products to a panel of experts and the wider audience. Leading companies in the industry will act as co-hosts and sponsors of the event, providing valuable expertise and support to the participating startups.

USE CASE AWARD
UNITED INNOVATIONS AWARDS

The Use Case Award highlights the best practices and innovative solutions to current challenges, which are also featured in the techL technology database. These exceptional use cases are further showcased during our Insights events, providing a platform to share and learn from the best practices of industry leaders.

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

Social Media

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

twitter.com/GFFT_eV

www.youtube.com/GFFTeV

Web
www.united-innovations.eu

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

Print
Flyeralarm 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 cooperation. 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

Security Emergency Management

An article from Annika Gamerad

Initial situation

Emergency management is part of the IT security strategy and has the task of maintaining or restoring critical business processes. Carefully thought-out action strategies are used to respond appropriately to various emergency scenarios.
Components of emergency management include preventive measures for emergency preparedness and plans for coping with emergencies and restoring business processes. All aspects required to continue critical business processes in the event of an emergency must be considered as part of emergency management. Prevention, detection, response, business continuity, and post-incident recovery. The use of cyber insurance is also part of IT emergency management.

Project

In cooperation with suresecure, the GFFT Security Lab provides companies with simple practical support. The basic idea is to collect and exchange knowledge about challenges and solutions in half-day workshops at all consortium partners. To compile solution paths for the most pressing difficulties and to make the knowledge available again to all partners via the insights or individual workshops. An individual initial workshop will be held with each partner of the consortium project at the beginning, in which the current state and the challenges of the next 6 months will be identified.

Benefit for the user

For users, the project has the great advantage of being able to inform themselves about the topic of emergency management and to exchange ideas with like-minded people and experts, to classify emergency management in different corporate contexts and management systems, and to become familiar with both preventive and reactive measures and to be able to implement them practically in the respective company. The project also offers students the opportunity to formulate their own specific challenges and questions and to identify possible practical solutions. The direct exchange with experienced incident managers on cyber emergencies and the presentation of best practice examples and exemplary (mostly anonymous) success stories also serve to support the development of these solutions.

Annika Gamerad
Event Management Specialist
suresecure GmbH

Detailed information in the techL-profile: suresecure GmbH

Incident Response Check

An article from 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
Gründer & Geschäftsführer
r-tec IT Security GmbH

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

Security Awareness

An article from Frank Müller

Initial situation

In everyday dealings with IT systems, awareness is an elementary security measure. This means that an awareness of the problem of cyber security must be created. As part of a security awareness training, employees are trained on the various topics relating to computer security in the company. The aim of security awareness is to make participants aware of IT security issues on a permanent and meaningful basis and to provide them with the necessary knowledge to deal with the various security threats during their daily work.

Project

In cooperation with Axsos, the GFFT Security Lab provides companies with simple practical support. The basic idea is to gather and exchange knowledge about challenges and solutions in half -day workshops among all consortium partners. To compile solution paths for the most pressing difficulties and to make the knowledge available again to all partners via the insights or individual workshops. An individual initial workshop will be held with each partner of the consortium project at the beginning, in which the current state and the challenges of the next 6 months will be identified.

Benefit for the user

- Minimize corporate risk for cyber incidents through ongoing employee awareness training.
- Recommend online training platforms for all employees with evidence of training/ actionstaken
- Effective employee training through actions tailored to your corporate environment

AXSOS puts together a campaign package for companies that includes different building blocks such as phishing emails, learnings, quizzes or posters, carried out within a defined period of time. The AXSOS approach is based on the Security Awareness Programme Framework (SAPF) of LucySecurity.

SAPF provides a modular guide for building comprehensive cybercrime awareness initiatives. The SAPF guide enables efficient implementation of a preliminary project for setting up an awareness program.

The implementation levels 'SCOPE', 'PLAN', 'RUN' and 'EVOLVE' allow to cover all levels of the organization: normative, strategic and operational. This effectively and sustainably ensures the effectiveness of preventive measures in the area of cyber risks.

Frank Müller
Vorstand/CEO
AXSOS AG

Detailed information in the techL-profile: AXSOS AG

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

Cybersecurity Trend Predictions - These five developments can be expected in 2023

An article from Detlev Riecke

From criminal penalties for CISOs, the extinction of the password, and a new era of data protection to overwhelmed IT security teams and new methods of attack by hackers on the workforce, the year 2023 suggests some significant developments in the IT security industry.

Detlev Riecke is regional vice president for the DACH region at ForgeRock, an identity and access management (IAM) company. The IAM industry has seen significant market growth over the past few years: Regulatory mandates have increased tremendously and the enterprise attack surface for cyberattacks has grown dramatically due to trends such as Internet of Things, cloud technologies and remote work. Last year alone, more than two billion usernames and passwords were compromised - and more than 50 percent of these security breaches can be attributed to unauthorized access.

For 2023, Detlev Riecke predicts five key developments that will keep the IT security industry busy:

1. More and more CISOs are being prosecuted for covering up data breaches.

CISOs have more at stake today than ever before - both personally and professionally. The conviction of Uber's former CISO for his role in covering up a data breach made headlines around the world and sends a clear message that IT security leaders will be held criminally accountable if they fail to properly fulfill their duties. The vast majority of CISOs will act correctly in the event of a security or data breach. However, the growing media interest in high-profile data breaches and the increasing board-level focus on data protection issues will tempt some CISOs to intentionally cover up data breaches. In the long run, covering up data breaches is more damaging to a company's brand and reputation than any security or privacy breach. In some cases, however, corporate culture and the pressure to put the company's reputation ahead of one's professional responsibilities can be immense. Unfortunately, this means that more CISOs are likely to be prosecuted for similar offenses in the coming year.

2. Employees are becoming the central linchpin in the battle between IT security and hackers.

Digital technologies are becoming more widely used in businesses. Both companies themselves and hackers recognize that employees are the biggest vulnerability in this ecosystem. Human error is increasingly becoming a gateway for attackers, and at the same time, the methods used by threat actors when posing to employees as their colleagues or as enterprise software are becoming more creative. This is also demonstrated, for example, by the recent media social engineering attacks, in which users were bombarded with multi-factor authentication alerts until they gained access to sensitive data or systems.

Organizations need to adapt their protection measures accordingly and budget more resources to both protect employees directly and minimize security risks. Educating the workforce through regular training on IT security risks is essential to avoid fraud made possible by human error, but at the same time it is also very time-consuming. AI-powered security processes can help busy and understaffed IT security teams fight the battle against hackers and other cyber threats by identifying and detecting unusual or potentially dangerous access in real time.

3. The days of passwords will be numbered.

The username-password model has been a dying breed for years. And although the end of the password has been looming for some time, the coming year will be a milestone for the adoption of passwordless authentication methods. The key driver for alternative technologies such as biometric authentication methods or behavioral analytics, will be the new FIDO2 web authentication standard. The standard is supported by the largest tech companies - Apple, Microsoft and Google - and enables users to reliably authenticate without a password across multiple devices, browsers and platforms.

Together with multi-factor authentication, these technologies can make the typical user experience more seamless, smarter and more secure. They can also be additionally combined with dynamic risk analytics to anticipate cyber threats in real time, rather than just reacting to them. That's good news for IT security teams and businesses looking to deliver the most seamless, personalized user experience possible - and bad news for passwords, whose days are hopefully now numbered.

4. A new era for data protection is being ushered in.

The issue of data protection is moving up the agenda of policy makers, not least because of increasing public awareness of privacy issues. Both the European Commission and the U.S. government have committed to reshaping transatlantic data flows in 2022. This goal is to be advanced through a revision of the now defunct Privacy Shield agreement. The joint project highlights a growing effort by lawmakers around the world to establish new and expanded rules for data sharing to more effectively protect the privacy of (end) consumers. With the addition of new privacy requirements, European companies are increasingly faced with the challenge of reconciling these with the use of innovative technologies and services from providers outside Europe. In order to not only meet all regulatory requirements, but at the same time provide secure, seamless and scalable end-to-end access processes, cloud-based identity and access management is becoming increasingly important.

5. AI-powered cybersecurity will be at the forefront of defending against cyberattacks.

The adoption of artificial intelligence in cybersecurity has already increased significantly in recent years. This trend is expected to extend to identity and access management in 2023. Digital workplaces and remote work open up a wide range of attack opportunities for threat actors, such as unauthorized access to user accounts and their resulting takeover. These increasingly sophisticated attack and fraud models, combined with an ever-increasing shortage of skilled cybersecurity professionals, ensure that organizations must adapt their cybersecurity solutions and processes to continue to have the upper hand in the fight against cyber threats. Accordingly, organizations must leverage all the tools at their disposal to stay one step ahead of attackers and secure their systems while ensuring a seamless user experience. AI-powered cybersecurity is one of the most effective of these tools in the enterprise arsenal and will be at the forefront of defending against cyberthreats in the future.

About ForgeRock:

ForgeRock is a global leader in digital identity. The company delivers modern and comprehensive identity and access management solutions for consumers, employees and things, providing easy and secure access to the connected world. With ForgeRock, more than 1,300 global organizations orchestrate, manage and secure the entire identity lifecycle, from dynamic access controls, governance and APIs to authoritative data storage - usable in any cloud or hybrid environment. Headquartered in San Francisco, California, the company has offices around the world.

Detlev Riecke
Regional Vice President
ForgeRock Deutschland GmbH

Detailed information in the techL profile: ForgeRock Deutschland 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/startup-pokal

Queryella

An article from Dr.-Ing. Leonid Glanz

Our private and professional communication vastly takes place in the digital world. We use our smartphones and many apps, generating more and more data daily. Some of this data can be intercepted by third parties and used for unauthorized purposes. We at Queryella aim to protect data from misuse by scanning apps for potential security or privacy issues. This goal is achieved by providing an unprecedented depth of analysis.

Solution

Queryella provides an automated analytics platform that leverages the latest research in security and privacy. It combines static and dynamic analysis using artificial intelligence to identify IT security issues or potentially sensitive data leaks in binary files.

Meta Data Analysis

In the first step, our platform analyzes an app's metadata to identify its starting points, permissions, input types, activities, services, and various interaction options. Subsequently, the essential information from the metadata is used to check whether it is consistent with the stated privacy policy. This check is automated using AI support to enable matching of the privacy declaration and the information from the app.

Library Analysis

Our platform avoids having to analyze all components in each app multiple times because the app is analyzed for known dependencies and their versions. These dependencies are matched against known vulnerability databases to identify potentially harmful or outdated ones.
In the future, this analysis can also be used to check whether all used dependencies have been listed in the bill of materials (SBOM). Due to our long experience in code structure analysis, we can detect even obfuscated libraries. Furthermore, the detected libraries are compared with a database of sensitive data flows created by us, thus enabling faster data flow detection.

Static Analysis

Our static analysis identifies individual vulnerabilities and traces their static reachability from a starting point.
However, the heart of our static analysis is the identification of sources and sinks of sensitive data and their data flow. This analysis also involves tracking whether the code can be reached from a starting point to reduce the number of false positives. The identification of sources and sinks is supported by AI so that our platform can investigate for each API version all new sources and sinks.

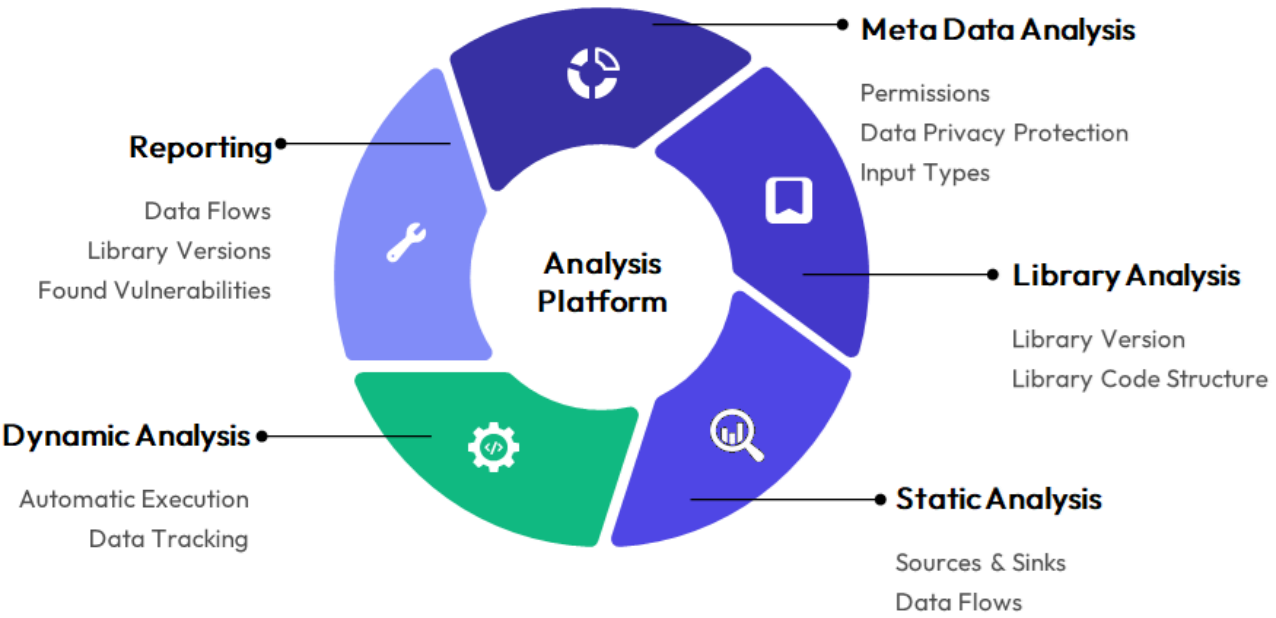


Image credits: TU Darmstadt

Dynamic Analysis

The dynamic analysis executes apps using AI support to trigger different events. During the execution, our platform tracks various data points to analyze the behavior of known advertising libraries or other data communications. Using dynamic analysis, the user can identify further information about data breaches and potential vulnerabilities. The platform will allow mapping different app scenarios in the future, as some apps show other behavior depending on the usage scenario.

Combining Static & Dynamic Analysis

Since a static analysis does not execute apps, many characteristics of the app behavior need to be over-approximated and can thus lead to false assumptions in the results. Dynamic analyses execute only individual paths through the app so that not all paths are covered, and some weaknesses can be missed. Combining static and dynamic analyses compensates for their weaknesses and leads to more accurate results.

For example, specific data flows are identified statically and then executed dynamically to analyze the flow more accurately. In doing so, our platform can deliver reliable results even when common measures have been used that prevent the analysis. This feature is enabled by identifying critical points or hidden data in the code, capturing the contextual information of those points, generating missing information, and bringing the collected code paths to execution. Critical points are identified using a machine learning model trained to recognize anomalies in the data.

Reporting

All analyses can be customized to meet individual customer needs. In doing so, our platform provides a user-friendly and intuitive interface that allows our customers to quickly and easily understand the results of the analyses. This characteristic allows them to respond quickly to identified security issues and take the appropriate action to protect their data and business interests. Our platform can be used for individual apps and large portfolios, making it scalable to any size. It also allows users to continuously monitor their apps so that new security vulnerabilities can be identified directly. With the different analysis techniques, we enable a more accurate assessment of critical risks and thus reduce the effort for security analysts to deal with irrelevant information generated by common open-source analysis tools.

Company

Queryella is a startup that evolved from a team of researchers at TU Darmstadt, Germany. Through extensive expertise in code analysis, IT security, and data protection, we are continuously improving our technologies and solutions and adapting to the ever-changing security situation of our customers.

We are actively searching for collaboration partners to expand our platform for the secure future of apps. If you would like to learn more about us and how we can help to improve the security and privacy of your mobile apps, feel free to contact us. More information at: www.queryella.de

Dr.-Ing. Leonid Glanz
Head of Research & Development at Queryella
TU Darmstadt

Detailed information in the techL profile:
Queryella

Onekey

An article from Jan Wendenburg

About the startup

ONEKEY is a leading European 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. Easily integrated into software development and procurement processes, 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. Leading international and national companies, such as ATOS, SWISSCOM, SNAP ONE, KUDELSKI, NAGRA, TRIMBLE, VERBUND AG, ZYXEL and many others use the platform today - For research institutions and non-profit organizations, the ONEKEY platform is available at special conditions.

Technology

The ONEKEY platform provides fully automated security binary analysis of IoT and OT firmware - without the need for source code, network connectivity or physical device access. In the software component analysis, the binary code of the software is deciphered, all components are identified and a software bill of materials (SBOM) is automatically created, which can be exported e.g. in CyloneDX format or other formats for further processing. In the subsequent security analysis, potential zero-days, i.e. unknown vulnerabilities, are identified and a comprehensive cryptographic analysis is performed. Here, information leaks, hard-coded passwords, obsolete components and certificates, insecure configurations or coding patterns as well as known vulnerabilities (CVE) are detected and automatically assigned to the respective components and clearly displayed. Integrated compliance checkers detect violations of regulatory standards such as IEC 62443, EU Cyber Resilience Act and many more. Compliance violations are thus identified in just a few minutes, automatically reported to the customer and can be remedied early on in development.

Benefit for the user

Equally important for manufacturers and operators of IoT/OT devices is ONEKEY Monitoring. This provides continuous 24/7 monitoring and analysis of firmware images throughout the product lifecycle. The ONEKEY SaaS platform provides users with immediate results and provides detailed reports through the intuitive cloud user interface. The platform is operated from a certified data center located in Germany and integrated into a global data center network. Alternatively, the ONEKEY platform can be customized and deployed as an on-premise solution in a company's own data center. For companies that still have little expertise in the area of IoT security, a hybrid offering of an automated platform with supplementary, professional cyber security services, such as penetration tests and specialist consulting from experienced security experts, is available

Jan Wendenburg
CEO
ONEKEY GmbH

Detailed information in the techL profile: ONEKEY GmbH

Smart Data

An article from Alexander Berger

About the startup

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.

Technology

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. For most companies, using the platform is the first time that they are able to grow an end-to-end incident process database which allows for powerful analysis and smart risk mitigation decisions. The platform supports the strategic work with plenty of chart views and specialized KPIs targeting risk, cost and response.

Any incident could escalate to an emergency or a crisis. In tense situations, PREVISEC supports teams providing a digital workroom featuring specialized tools: The digital crisis room. Here, emergency and crisis management teams are supported in properly taking well targeted decisions and documenting them in an audit-proof way. The room also facilitates communication and collaboration across departments in order to eliminate the pain of jumping around between several tools.

Benefit for the user

There is only way to support incident and crisis management teams tackling dynamic risk in a world described as VUCA: Siloless and cross-functional response with PREVISEC.

Alexander Berger
CEO
SMART DATA Deutschland GmbH

Detailed information in the techL profile:
SMART DATA Deutschland 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

Research Project: Secure Software Supply Chains in the Industrial IoT

An article from Patrick Jauernig

Initial situation

An important cornerstone of Industrie 4.0 is consistent networking of production machines with devices that take over the control of the machines, collect their data, pre-process it and forward it to cloud systems, where it is analyzed with the help of intelligent algorithms. To meet the high functional demands of Industrie 4.0 applications, these devices, often IoT gateways or industrial PCs, must combine a variety of software components from different vendors on a single device.

The combination of proprietary software with third-party software and open-source software results in a complex software supply chain for IoT gateways and industrial PCs, as well as for many other embedded devices, which makes the IT security of the devices, and thus the production in which they are used, vulnerable to cyberattacks. Current IoT gateway products rely primarily on encryption of data communication and a protected boot process of the system software ("Secure Boot"). However, neither mechanism provides protection against security-critical vulnerabilities in individual software components.

Project

The SANCTUARY Zero-Trust platform is a software solution that is already integrated within the actual product development. The platform combines virtualization with the strong security guarantees of trusted computing to achieve a strong isolation of third-party software and open source software. This strongly isolates individual software components from each other, preventing a cyber attacker from spreading beyond the boundaries of the flawed software on the system - leaving all other software components on the IoT gateway intact. Assigning secure identities to each software component also allows secure communication channels to be created between them. In this way, the Zero-Trust platform replaces blind trust in supplier software with explicit trust relationships between components. In addition to IoT gateways and industrial PCs, the Zero-Trust platform can also be used on other embedded systems such as automotive or satellite systems.

Benefit for the user

The SANCTUARY Zero-Trust platform strengthens security and reliability for complex software stacks on embedded systems while preserving real-time system characteristics. The Zero-Trust platform is legacy-compatible and can be easily integrated into existing ecosystems. Applications automatically benefit from the security services of the Zero-Trust platform, such as our virtual TPM/HSM technology or health monitoring services.

The integration of the platform is done systematically and close to the product, i.e., in many cases a security analysis is performed first to assess the current state of the product and define goals for security. Then, the Zero-Trust platform is prototyped to fit the desired platform. The actual integration of the Zero-Trust platform into the actual product and a final security analysis guarantee maximum security for your product.

Patrick Jauernig
SANCTUARY Systems GmbH
TU Darmstadt

Detailed information in the techL profile:
SANCTUARY Systems GmbH

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

Authdata

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

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

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

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

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

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

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

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

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

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

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

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

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

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