NASK

NATIONAL RESEARCH INSTITUTE

Cybersecurity

Research & Development

Centre for Research and Development
Strategic Client Support Division

Research Projects
Index
Journal N° 1/2019 Rev. 1.7

A Word from the Director

Dear Friends of NASK

Cybersecurity is a must, It is constantly needed by private people, enterprises as well as public and government institutions. Step by step for over 25 years NASK - the Polish National Research Institute - has managed to build the tools, the team and its know how to be able to answer to the big challenge of cybersecurity that are vital to our country.

I am very happy to introduce a whole range of our scientific projects and implementations which have lead us to develop various tools of incident detection, incident response, data analysis and data sharing. These days we understand more than ever before that cybersecurity goes hand in hand with capability to analyze big data sets and to implement artificial intelligence tools.

At NASK, we are aware that Cyberthreat Intelligence with its systems, data and algorithms needs constant improvements. Therefore, I want to encourage you to share with us your perspective. Let us join forces in responding to this complex challenge. I strongly believe that multi level and multi national cooperation is the key to securing cyberspace.

In this folder we present our story of cybersecurity solutions at Polish National Research Institute NASK. We look forward to read your story.

Hoping to hear from you before too long!

ABOUT US

WHAT IS NASK?

Research Insitute

carring out international projects on innovative cybersecurity solutions

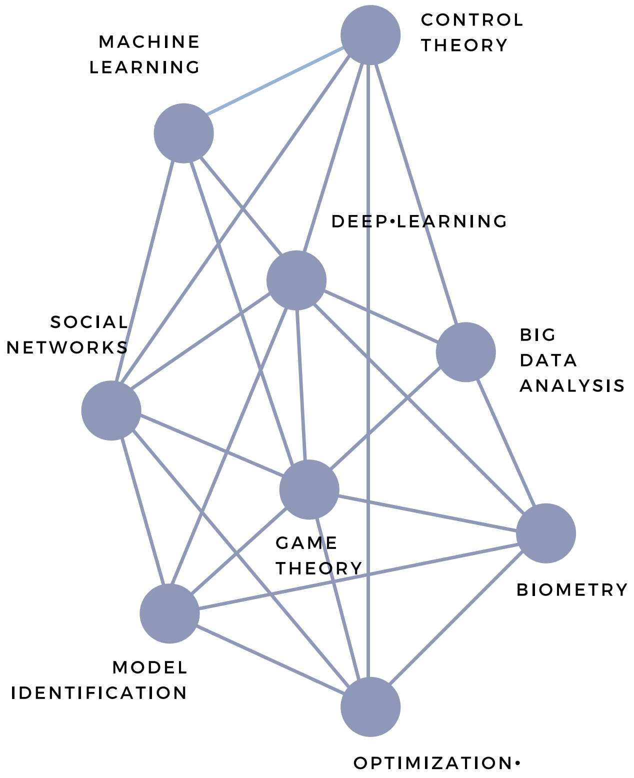
Governmental institution

Prerfoming national cybersecurity tasks according to the Act on National Cybersecurity System

Experienced market player

providing cybersecurity services (CyberThreat Intelligence) for banking and critical infrastructure••as•well as telecommunication services

RESEARCH AND DEVELOPMENT



RESEARCH INTERESTS

Cybersecurity calls for complex solutions and a holistic approach. Hence our researchers are not only reaching for common tools used in cybersecurity but they are also looking for answers in different yet inspiring disciplines.

This interdisciplinary approach has been proven right as their research on game theory social networks or energy-efficient CPU turned out to be crucial for the design of innovative and highly effective systems for detecting and mitigating cyberattacks.

10•

Of the entire team are scientists

25

Years experience in IT &Security

over 700

Employees

100%

Government-backed

DETECTION

EARLY WARNING

With our research and innovation we put great efforts to be
one step ahead of cyberattacs

NASK Cybersecurity

DETECTION

ARAKIS Enterprise
NASK

EARLY WARNING SYSTEM FOR CYBERTHREATS IN IT AND OT NETWORK•

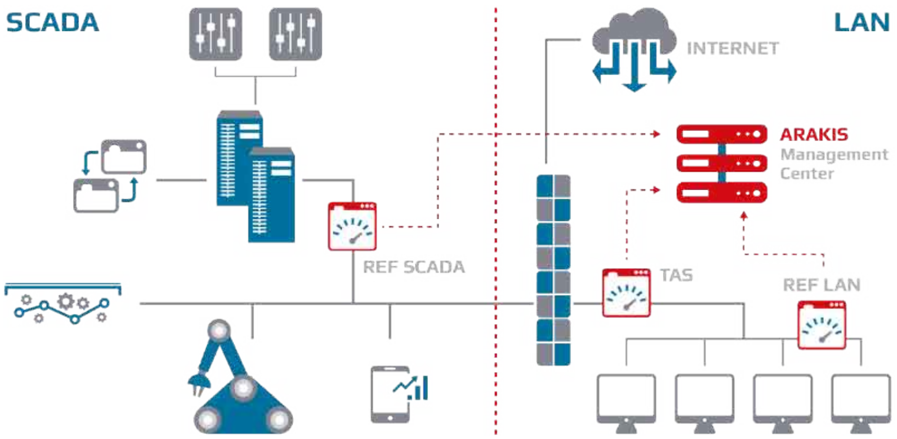
Arakis is an Early Warning System reporting on cyberthreats in IT and OT networks offered both as an Enterprise and GOV versions The latter as part of the Arakis project has been developed in cooperation with ABW. The Internal Security Agency and set out in the Act on the National Cybersecurity System.

The main goal of the system is to identify all activities threating the IT and OT infrastructure.
ARAKIS is based on honeypots that are designed to lure and catch attackers in a controlled trap This allows to distract attackers from crucial parts of the company's strategic infrastructure as well as to gather information about adverse actions of the attacker that can be used for further analysis.

INNOVATION

A quick and effective detection of cybersecurity incidents in the observed network requires interoperability of mechanisms for aggregating and correlating the data gathered by sensors. And this requires a complex and coherent architecture using state-of-the-art solutions. The architecture of ARAKIS is a result of a lot of research efforts successfully addressing numerous network security engineering and scientific problems
These include the design of:

- polynomial complexity algorithms generating signatures from honeypot attack traces and
- machine learning algorithms detecting server communication patterns.



DETECTION

ARAKIS Enterprise

NASK

EARLY WARNING SYSTEM FOR CYBERTHREATS IN IT AND OT NETWORK

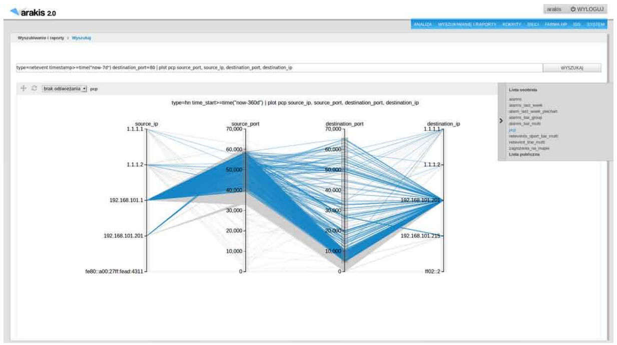
ARCHITECTURE

The ARAKIS infrastructure consists of four types of data collecting sensors:

- REF LAN: uses information collected by honeypots emulating usual Windows or Linux server services like SSH, SMB, MS SQL, mySQL or VoIP
- REF FWD: an additional sensor for monitoring and correlation of logs from http servers. Machine learning used for user behavior patterns enables detection of early symptoms of unknown attacks.
- REF TAS: (Traffic Analysis Sensor) enables to analyze analyzes traffic by automated correlating collected data with the data from n6 platform. A knowledge produced this way consists of among others actual information about C&C servers or injected workstations.
- REF SCADA enables emulating of PLC regulators or SCADA management systems services Working in passive mode it doesn t influence the stability of sensible SCADA networks.

A modular architecture of ARAKIS makes it easy to add new services or functionalities An important part of the system is the Graphic User Interface which enables:

- system components' management,
- data visualization and analysis,
- search mechanisms with unique AQL syntax (Arakis Query Language),
- automatic reporting integrated with SIEM,
- dashboards personalisation.



```
type=netevent timestamp>=time("now-7d") destination_port=80 | plot pcp source_port, source_ip, destination_port, destination_ip
```

```
type=hn time_start>=time("now-360d") | plot pcp source_ip, source_port, destination_port, destination_ip
```

Our engineers developed an unique ARAKIS Query Language that allows visualization of all kinds of system data with maps, graphs, charts and others, as well as a various range of statistics. The language can be also used to define periodical reports with varying level of detail-from executive summaries to detailed forensic reports.

DETECTION

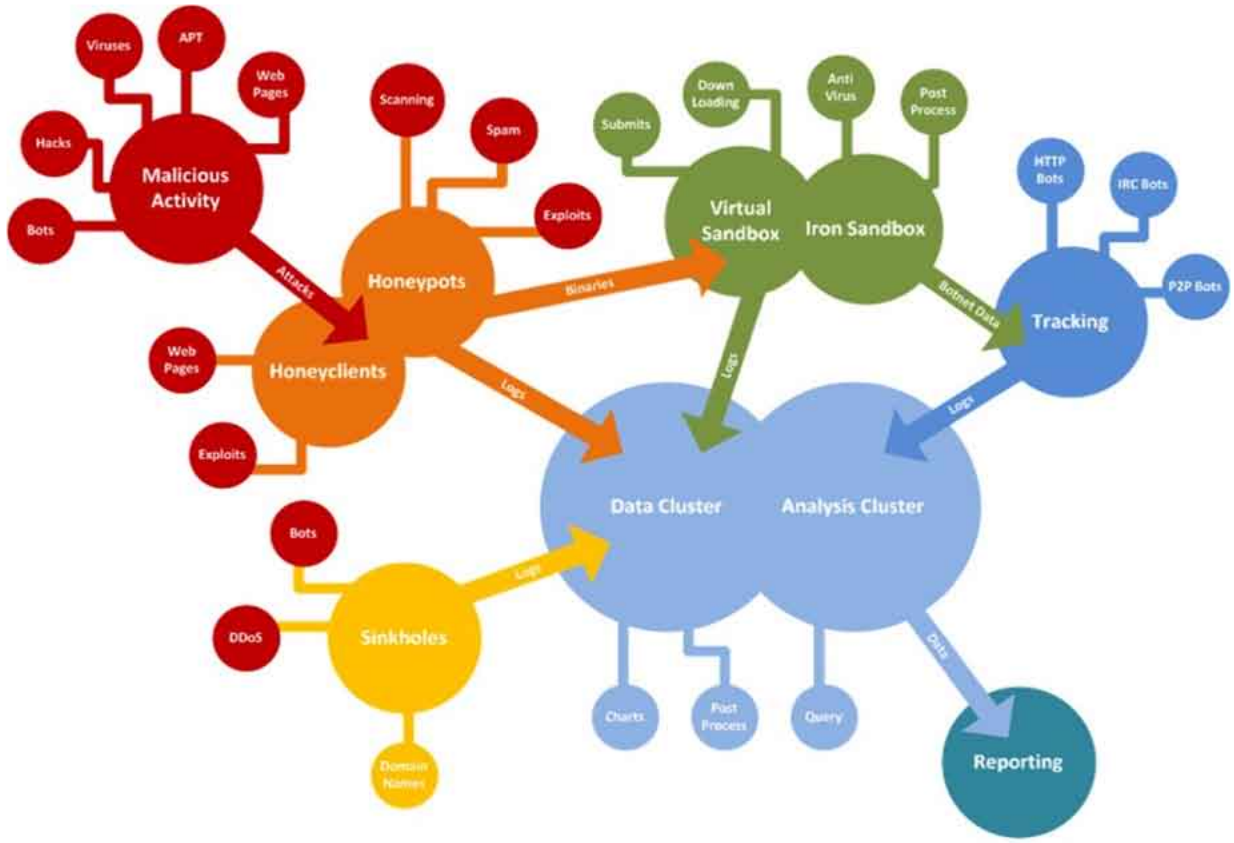
SISSDEN

shadowserver

SECURE INFORMATION SHARING SENSOR DELIVERY EVENT NETWORK CONTACT USCUSTOMER PORTAL

This project is realized in co-operation with SHADOWSERVER. The project develops the tools necessary to deal with large volumes of collected data and then correlate it with data obtained from other sources. The core of SISSDEN is a worldwide sensor network, which is deployed and operated by the project consortium.
NASK is performing the coordinator role of such a large international project.

An innovation and a big challenge that our researchers have successfully addressed has been the design of both the architecture of such complex and scalable system and algorithms or other tools enabling its functionalities.
The huge database resulting from the project is absolutely crucial for practical implementations of early warning and mitigation systems for cybersecurity for both national as well as market purposes.



THE SHADOWSERVER
MODEL

DETECTION

SISSDEN

SECURE INFORMATION SHARING SENSOR DELIVERY EVENT NETWORK CONTACT USCUSTOMER PORTAL

Our researchers have developed an innovative architecture of a global sensor network (212 sensors in 52 countries which enable the monitoring of about 900 000 IP addresses), **which resulted with the biggest database with the most amount of precise selected and informative data needed for identification of malware and suspicious behavior. The collected data is based on end user experience.**

The project has resulted with a range of interesting solutions:

- Methods of continuous botnet configuration tracking, including both the extensions of the previous system for the extraction of configurations gathered malware probes as well as a new system for emulating real bots in order to track any configuration changes.
- A complex set of methods for Darknet analysis which enable ongoing identification of various types of observed incidents
- A method for SMTP dialects analysis which allows identification of a client and server software type used for e-mail exchange solely by analyzing the smallest differences in the protocol implementation It could be used for autonomous (independent from the spam content) spam identification as well as identification of botnets responsible for individual spam campaigns.

INNOWACJA

Our researchers have developed an unique algorithm which is able to detect PGA (Packet Generation Algorithms) solely from observations of network traffic. However in contrast to usual PGA detection solutions the advanced math behind our system allows us to detect different types of relations between single fields of packet headers within a group and only then creates a rule.

DETECTION AND REACTION

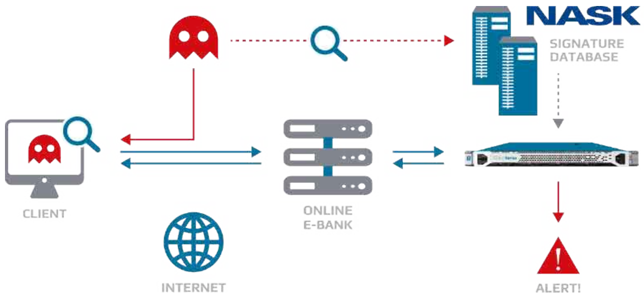
Despite best warning mechanisms cyberatacs will still occur now and then. But we don‘t want to sit on our hands: **we aim to react - effectively and quickly**

REACTION

BotSense
NASK

ONLINE BANKING MONITORING SYSTEM

BotSense is a system designed for banking, responsible for real-time detection of attempted takeovers of client accounts and unauthorized transactions. This has become a substantial threat with the thrive of online banking.



For developing a system that allows clients to use online banking services in a secure and fearless way NASK has been awarded with ”Portfel WPROST 2017’ in the category ”Security,” which is an important award in the financial sector.

7

million

of online-banking accounts in Poland effectively monitored by BotSense

IDEA

The spectacular success of this product results on the one hand from effectively designed and realized concept of its architecture (Javascript code is being embedded in the online banking website code so that no client personal data are needed). But on the other hand from a long experience, that NASK has gathered in cybersecurity over the years and that contributed to development of both the internal tools feeds and databases as well as cooperation with other cybersecurity teams.
Malware signatures used in BotSense are processed by NASK researchers using probes provided by CERT Poland.

REACTION

fldx NASK

ANTI DDOS DETECTION AND MITIGATION SYSTEM

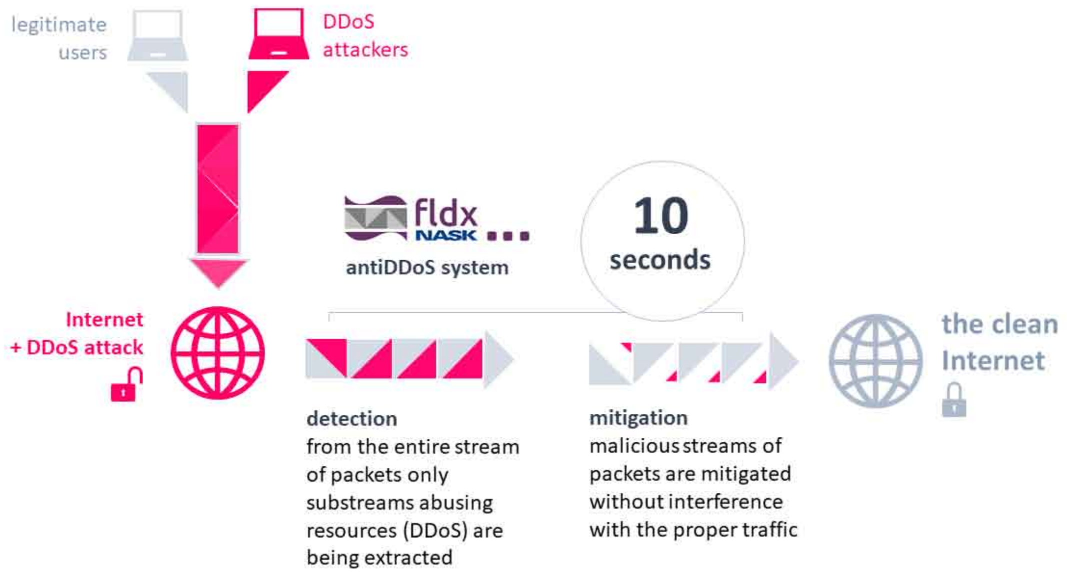
FLDX is a state-of-the-art detection and mitigation system for volumetric attacks called called Distributed Denial of Service (DDoS).

The system is able to perform its tasks in an automatic or semi-automatic mode or to serve as a decision support system for a human operator.
The effectivness of anti DDoS systems is measured not only by the results of its performance (whether an attack has been detected and mitigated or not) but also by the mitigation time. The unique scientific approach implemented in the FLDX system has proven to provide very competitive mitigation time of only 10 seconds.

INNOVATION

FLDX is a system which is able not only to detect known attacks but also to self-adjust its detection mechanism into changing dynamics of cyberattacks and therefore is able to react to new and unknown incidents patterns.

Additionaly the technology used in FLDX based on a mathematical model designed by NASK researchers, guarantees a seamless mitigation process that does not affect the rest of the network. FLDX precisely separates the infected connections from the healthy ones, and thus attacks can be effectively mitigated without the need to block any other services.



detection from the entire stream of packets only substreams abusing resources (DDoS) are being extracted

mitigation malicious streams of packets are mitigated without interference with the proper traffic

REACTION

REGIONAL CENTER FOR CYBERSECURITY

The goal of RegSOC Project is to prepare and initiate a prototype instance of the model Regional Center for Cybersecurity (RegSOC) for public entities, based on the research and development results. The ability of extending the cooperation to private sector will be checked. In cooperation with National Cybersecurity Center. The Center may constitute an element of the multilevel System for Cybersecurity of Republic of Poland.

The project will allow to raise levels of security protection, introduce procedures of reducing probability of unwanted events and raw up methods of lowering of their consequences, by means of tasks planned in the project.

The project will be carried out by the Consortium of following institutions: Wroclaw University of Science and Technology (WCSS) - The Leader, National Research Institute NASK, Institute of Innovative Technologies EMAG.

The project is co-financed by the National Centre for Research and Development as part of the CyberSecIdent-Cybersecurity and e-Identity program.

Expected results are as follows:

- Hardware&Software appliance for public entities, able to operate as standalone autonomous device within local administration domain, as well as integrated with RegSOC;
- A cybersecurity monitoring platform for needs of the RegSOC. The platform will be the software and organizational solution (management models and organizational procedures);
- A procedural and organizational model of operation of the regional centers in cooperation with NCCyber, along with the internal software integrating RegSOC with National Cybersecurity Platform (NPC);
- A model RegSOC initiated at the University, with client components deployed at the selected entities interested in the project's results;

BIG DATA ANALYSIS

When it comes to cybersecurity what matters most is information, meaning collected, analysed and properly procesed data

Forensic Lab

ADVANCED DIGITAL FORENSIC LABORATORY

Warsaw University of Technology

The aim of the project is to create an advanced digital forensic laboratory and relevant methodologies and procedures. The lab will provide the user with a complete set of tools and devices to collect all kinds of electronic evidences and conduct comprehensive analysis.
It is divided into two modules: mobile and stationary. The design of the methodology and operating procedures of the laboratory will help to increase the detection of cybercrimes and thus increase the security of cyberspace by eliminating harmful activities, particularly those related to organized crime.

Methodologies and procedures of laboratory operation created within the project will allow to increase the detection rate of cybercrimes and thus to increase the security of cyberspace by eliminating harmful activities, in particular related to the activities of organised crime groups. The creation of forensic investigation laboratories is the next step in the development of CERTs and is a natural necessity for law enforcement agencies.

Results of laboratory activities may directly lead to creation of new secure ICT products or services in cyberspace by exploring current vulnerabilities and threats.

Cybercrime forensics

The project will enable direct cooperation primarily between NASK and WUoT and secondarily with law enforcement agencies, which require precise and fast methods for collecting and analysing digital evidence.

IMPACT

The impact of the Project on the development of knowledge in the areas covered by the Programme will consist in better recognition of the issue of investigation of attacks and their effects. Thanks to the solutions developed, entities using post-breaking analysis methods will gain an advantage over entities which do not have this knowledge by the possibility of rapid introduction of new security measures. As a result, they will gain a competitive advantage by being more resilient to identified attacks.

ANALYS

NCP NATIONAL CYBERSECURITY PLATFORM

NATIONAL CYBERSECURITY PLATFORM

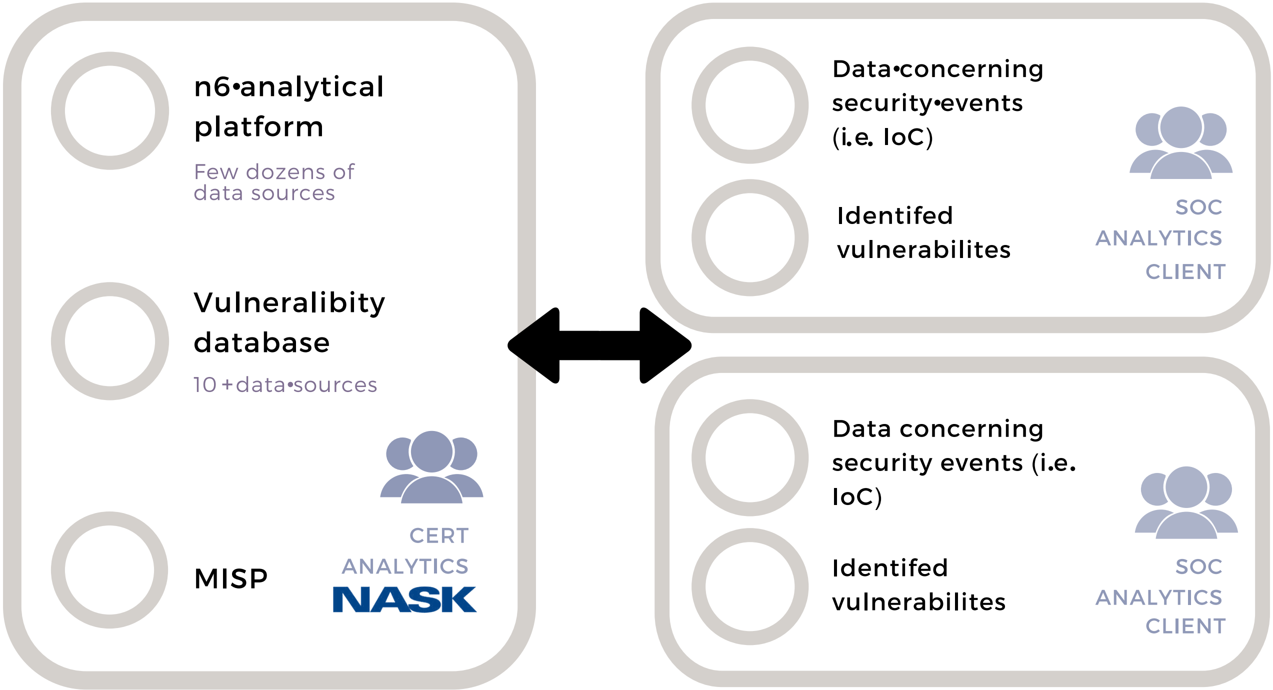
The National Cybersecurity Platform (NPC) is a comprehensive, integrated system for continuous monitoring, detection, and warning of threats identified in a near real-time in the State's cyberspace The NCP prototype will provide effective mechanisms to coordinate actions to prevent detect and mitigate the impact of incidents that violate the security of ICT systems vital to the functioning of the State.
NPC provides advanced access control and dissemination mechanisms for secure information sharing within the platform Information is gathered both by Computer Security Incident Response Team (CSIRT) and Security Teams operating in Participants' organisations.

Novel methods and tools are developed focused on:

- cyber events correlation,
- situation awareness evaluation,
- static and dynamic risks assessment,
- multidimensional visualization with multimodal user interface,
- threats detection in IoT, TCP/IP and industrial networks.

INNOVATION

DISTRIBUTED KNOWLEDGE AND CROWDSOURCING IDEA



n6•analytical platform

Few dozens of data sources

Vulneralibity database

10+data•sources

MISP

CERT ANALYTICS

NASK

Data•concerning security•events (i.e. IoC)

Identifed vulnerabilites

SOC ANALYTICS CLIENT

Data concerning security events (i.e. IoC)

Identifed vulnerabilites

SOC ANALYTICS CLIENT

ANALYSIS

NCP NATIONAL CYBERSECURITY PLATFORM

NATIONAL CYBERSECURITY PLATFORM

A part of the NCP is an expert system supporting the choice of methodologies and metrics to establish ICT security requirements and reporting significant incidents that violate the information security of the infrastructures encompassed by the NIS Directive on security of network and information systems.

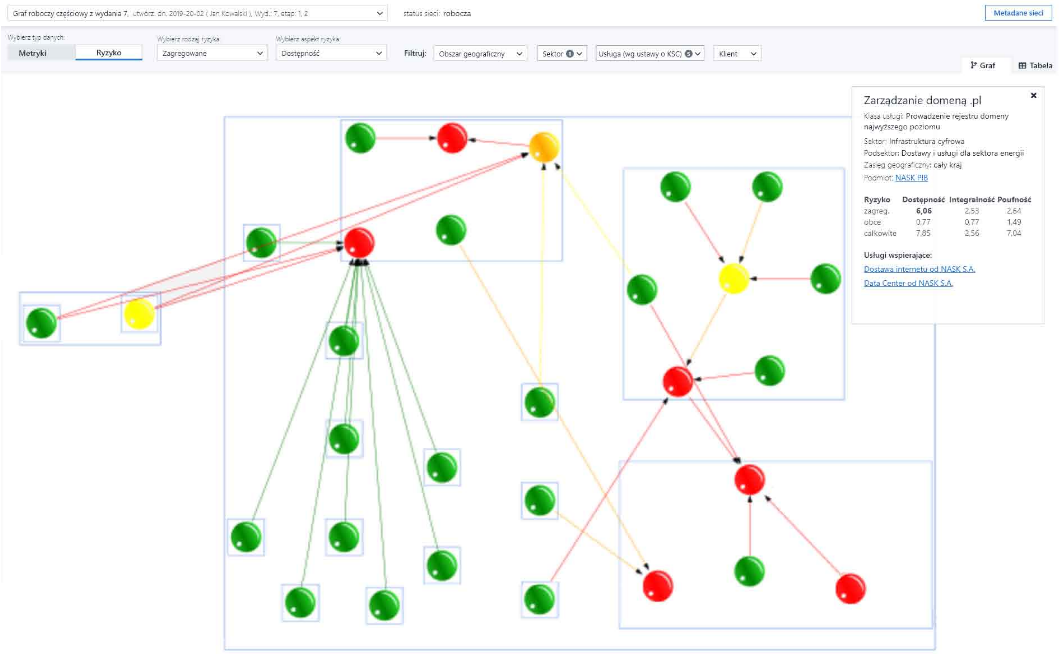
In order to assess the risk of threat propagation one can genarate a map which will visualize links between essential services offered by different providers This helps to assess how different sectors of the economy interefere whith each other and what their impact on the State's security is.

INNOVATION

As for risk analysis a novel method of hierarchization has been developed It allows to define the critical degree of links between elements of ICT and internal supporting services.

Several algorithms for risk prediction have been implemented to create a correlation matrix that describes the mutual influence of confidentiality, integrity and accessibility that is how violating of one of these aspects affects the others.

In order to visualize critical correlations color marking has been implemented This approach brought up the problem of graph cycling. The issue has been resolved by acurate defining of cycle and correlation paths.



Graf roboczy częściowy z wydania 7, utwórz. dn. 2019-20-02 (Jan Kowalski), Wyd.: 7, etap: 1, 2

status sieci: robocza

Wybierz typ danych: Metryki | Ryzyko

Wybierz rodzaj ryzyka: Zagregowane

Wybierz aspekt ryzyka: Dostępność

Filtruj: Obszar geograficzny | Sektor 1 | Usługa (wg ustawy o KSC) 5 | Klient

Zarządzanie domeną .pl

Klasa usługi: Prowadzenie rejestru domeny najwyższego poziomu

Sektor: Infrastruktura cyfrowa

Podsektor: Dostawy i usługi dla sektora energii

Zasięg geograficzny: cały kraj

Podmiot: NASK PIB

Ryzyko	Dostępność	Integralność	Poufność
zagreg.	**6,06**	2,53	2,64
obce	0,77	0,77	1,49
całkowite	7,85	2,56	7,04

Usługi wspierające:

Dostawa internetu od NASK S.A.

Data Center od NASK S.A.

ANALYSIS

BioMobi

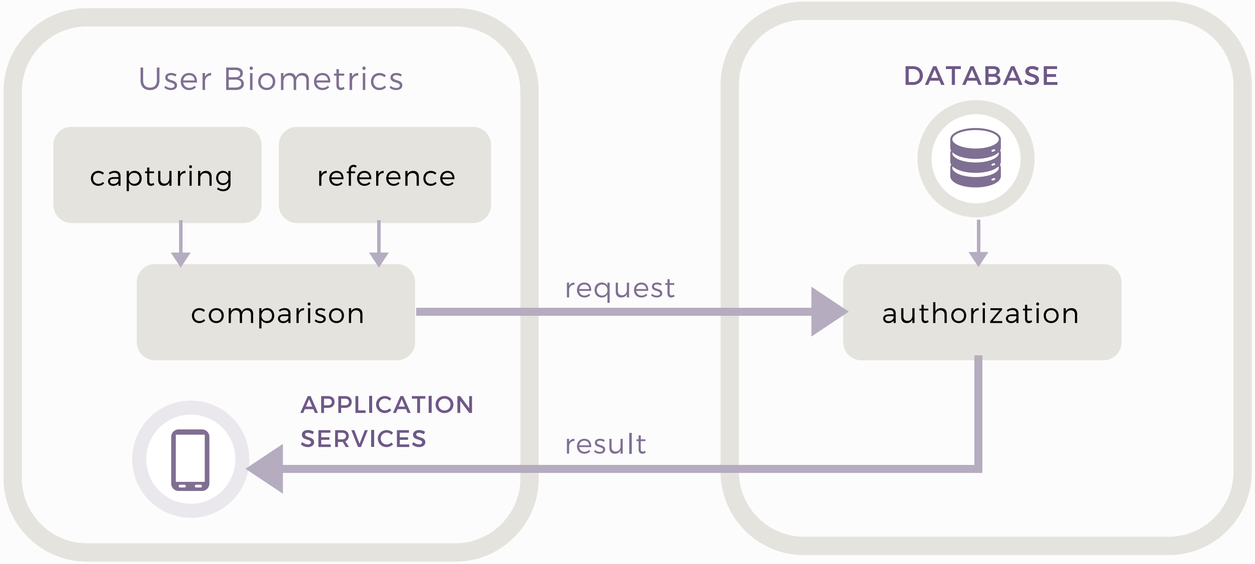
MOBILE REMOTE AUTHENTICATION SYSTEM USING NON SPECIALIZED MOBILE DEVICES

The goal of the project is to build a mobile remote multi modal adaptive biometric authentication system using of the shelf mobile devices.
We employ of the shelf devices to make the biometric authentication more accessible. The solutions will be adaptive by adjusting biometric authentication safety level to the demands of the authorizing party bank, hospital, government,office, universities etc. By multi modality we mean application of a wide class of biometric modalities, like face voice, fingerprint, hand, iris and others, in order to meet the end user s-preferences. Because of the use of mobile devices. special attention is given to the safety of data acquisition. A remote system induces high security demands to data transmission and storage.

INNOVATION

Innovative outcomes:

- independent system working on common non specialized mobile devices, spreading access to biometric authentication
- in house biometric algorithms•for different biometric modalities using AI methods, like deep convolutional networks
- development of in house algorithms increasing system robustness to presentation attacks, thus making biometric data acquisition safer in uncontrollable conditions
- adaptive design enabling the use of various biometric modalities depending on user preferences yet meeting security demands
- new specialized methods to assure secure data capture comparison, and storage, and the safety of biometric data.

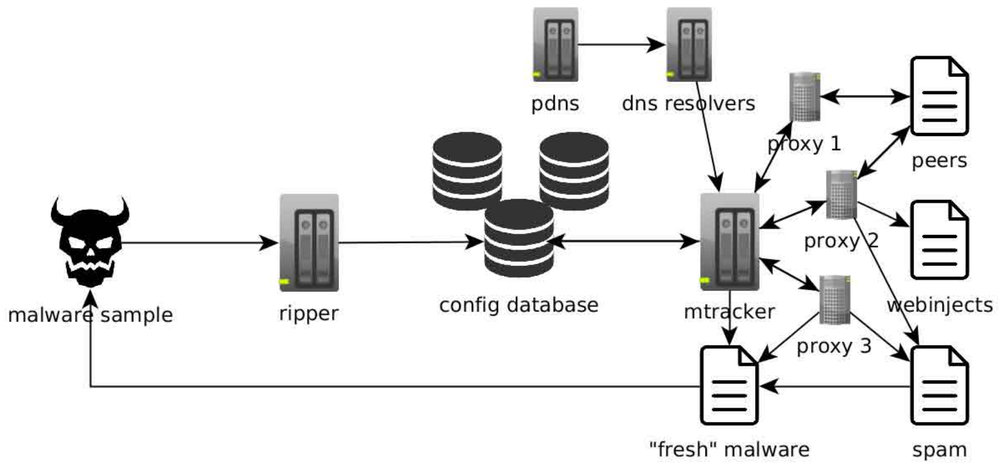


m Tracker

ADVANCED DATA AQUISITION AND ANALYSIS

mTracker creates feeds of actionable security information that are processed by relevant entities.
A typical analysis of malware network traffic and communication rests on executing the malware in a controlled environment (e.g. a dedicated long-term sandbox) and observing its behavior through a large set of filters, analyzers and monitors.
We came up with a different approach.

All configurations are now being tracked from a few different proxies independently. This also allowed us to solve the problem of geolocalised campaigns - it's very common that a malware sample checks its location and refuses to infect computers outside of its target zone (most notable example is Dridex) or has a different set of injects/modules for every country (e.g. Emotet). Additionally sometimes C&C servers are kept in a Tor network, so they can be reached only through a Tor proxy. The most recent feature (so far) that we have implemented in our system is DNS augmenting. Nowadays, the usage of the .bit Top-Level Domain (TDL) is gaining populariy among malware creators. Thus, if we want to support .bit-based malware we need to provide our own DNS resolver (.bit domains are not present in root TLD zone). After implementing this feature, we noticed another opportunity - sometimes C&C domains are taken down soon after the start of the campaign, but the server is still working and responding to its original IP address. So when a domain fails to resolve (or resolves to a sinkholed domain) we re using data from our passive DNS instead:



ANALYSIS

NECOMA

NIPPON EUROPEAN CYBERDEFENSE ORIENTED MULTILAYER THREAT ANALYSIS

The project has been carried out in cooperation with a European-Japan commercial-scientific consortium. Researchers from NASK have been working specifically on developing tools for big data aggregation and advanced inference mechanisms applied for cyberthreat analysis.
Data used as a learning set for classifiers and rule-based algorithms needs to be large and precisely selected. This will maximize the efectiveness of threat detection and minimize false positive errors, respectively. Hence, a new innovative methodology of source assessment has been developed, which allows to control the quality of the incoming data.

One of the key tools was the n6 platform-an own malware database established by CERT Poland-used for automatic gathering, processing and sharing information about cybersecurity incidents.
The n6 platform has played a crucial role in the entire NECOMA project and thus further work on its development of n6 has become one of the project's objectives. This n6 extension includes additional feature of incident streaming in order to minimize potential delays in communication, as well as publishing n6 SDK as open GPL license.

INNOVATION

The FP-Growth (Frequent Pattern) algorithm has been implemented - URLs are being parsed and compressed into a FP tree, which is then further explored with "divide-and-conquer" strategy (Y. Han and others, 2000).

The implementation of this data mining method has proven to be substantial for the preparation of the learning dataset for the Support Vector Machine classifier. New suspicious patterns are properly classified as "related" or "non-related" with the malicious campaign.

総務省
Ministry of Internal Affairs and Communications

SEVENTH FRAMEWORK PROGRAMME

SHARING

KNOWLEDGE AND DATA SHARING

By collecting and processing data
we produce knowledge
that we want to share in order to minimize
vulnerability of potential victims.
Together we are strong!

KNOWLEDGE

Cybersecurity Certyfikation

POLISH SCHEME FOR SECURITY AND PRIVACY **EVALUATION AND CERTIFICATION** OF IT PRODUCTS AND• SYSTEMS COMPLIANT WITH **COMMON CRITERIA**

KSO3C is a project which aims at creating a cybersecurity evaluation and certification scheme. It is a joint initiative of three institutes i.e. National Institute of Telecommunications. NASK - Research and Academic Computer Network and Institute of Innovative Technologies EMAG, operating under direct supervision of the Polish Minister for Digital Affairs. The aim of the project is to develop and implement the Polish national scheme for IT Security & Privacy evaluation and certification based on the Common Criteria approach. The project is a direct response to the European Commission's initiative focused on developing the European Certification Framework for the IT products and services security and privacy.

A final product of the Project will be a fully operational scheme, capable of issuing globally accepted certificates. The scheme will be an open structure which may include any entity applying to be the IT Security Evaluation Facility (ITSEF) once it meets all requirement with respect to impartiality and transparency, according to the EU rules of conformity assessment for products, services or processes.

KSO3C

Common Criteria ®

NEW METHODS

Certification and evaluation of electronical devices require most advanced techniques of testing its potential vulnerabilities.
Hence, the project objective is to develop methods and techniques for security and privacy evaluation with high level of assurance, based on an innovative approach to the assessment of vulnerabilities by means of advanced attack techniques, both invasive and non invasive ones, including:

- reverse engineering
- extension of AVA_VAN methods
- side-channel attacks
- or methods of precise attacking the cryptographic modules or chips, such as laser-injection (fault-injection)

KSO3C (CYBERSECIDENT/381282/I/NCBR/2017) PROJECT IS SUPPORTED BY THE NATIONAL CENTRE OF RESEARCH AND DEVELOPMENT UNDER THE CYBERSECIDENT PROGRAMME

DATA

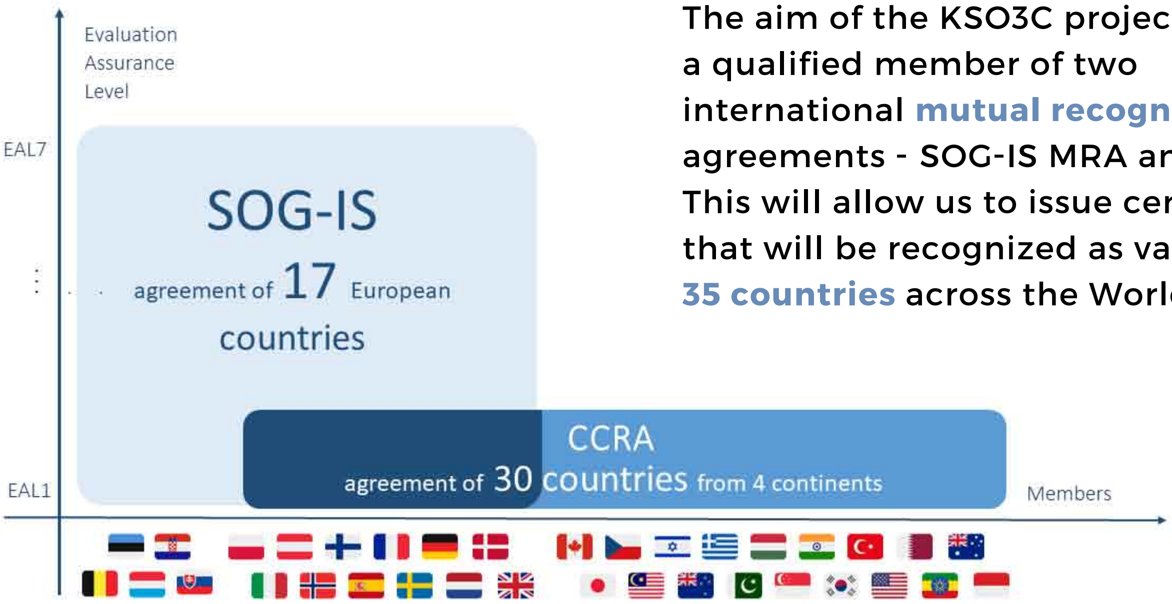
Cybersecurity Certyfikation

POLISH SCHEME FOR SECURITY AND PRIVACY **EVALUATION AND CERTIFICATION** OF IT PRODUCTS AND SYSTEMS COMPLIANT WITH **COMMON CRITERIA**

The standard defines the so called Protection Profiles (PPs) which formulate security functionalities of a given type of product. PPs are evaluated by qualified staff in terms of their consistency and effectiveness of the proposed security measures. This helps vendors in being able to formulate their needs in terms of security and developers in creating safer products. In order to evaluate the later ones a developer can formulate a so called Security Target for his product. Based on it the product can by evaluated by a trusted third party that will verify that the safety requirements are met, security measures are effective against known threats and no known vulnerabilities are present.

THE IMPACT

Apart from the technical standard of Common Criteria the involved entities will be accredited against the ISO/IEC 17025 and 17065 standards accordingly. This will ensure the highest standards in terms of impartiality and confidentiality are met.



Evaluation Assurance Level
EAL7
EAL1
SOG-IS
agreement of 17 European countries
CCRA
agreement of 30 countries from 4 continents
Members

The aim of the KSO3C project is to be a qualified member of two international **mutual recognition** agreements - SOG-IS MRA and CCRA. This will allow us to issue certificates that will be recognized as valid in **35 countries** across the World

n6

MALWARE DATABASE

It is an open structure designed for gathering, processing and sharing information about cybersecurity incidents. The most important feature of the n6 platform is an automated data acquisition system that allows to gather billions of information on incidents from the entire world The data is coming from different channels. One of them is the result of active detection by external systems or internal cybersecurity tools monitored by NASK. An additional data source concerning client networks is the results of CERT Poland operations.(CERT is a team operating at NASK).

The key feature of the database is an extended tagging system which brings a well established structure to the gathered malware data.
This enables to conviniently catalog incidents and asign them precisely to particular subjects. The structure consists of a specially designed packet which preserves the original malware source format. The information concerning the attack source is shared as URLs, domains, IP addresses and malware names.
This project is open for cooperation, thus any network owner, provider or administrator is invited to apply for access to the data gathered in the platform.

SOASP

CUCKOO SANDBOX EXTENSION

The NASK team has developed an extension for open source Cuckoo Sandbox system, which has been originally integrated in CERT Polska. This extension offers statistical analysis of malware probes focused on processing of unzipped binary files. The ongoing work covers protection against antiscan techniques and unhooking.
Future versions SOASP will also enable to get the static configuration (e.g. IP address or domain) of the malware’s C&C server, exract cipher keys for communication and implement YARA rules for defined situations.

„No more ransom“ Website

A PLATFORM PROVIDING SUPPORT FOR CYBERATTACK VICTIMS

Due to growing number of ransomware attacks an online service No More Ransom has been established in order to fight against this threat and to offer help to its victims. The initiative came from Europol. National High Tech Crime Unit. Kaspersky Lab and McAfee. The majority of the activities offered within the project focuses on education and awareness, i.e. teaching its users how to prevent their devices or networks from being infected. There are also decryptors for some types of ransomware to be found on the website.

VALUABLE HELP

CERT Poland, operating at NASK joined the project by sharing its own decryptors against CryptoMix, CryptoShield and Mole, which belongs to the CryptoMix family but uses different types of encryption. This software has been downloaded over 6000 times from about 3000 different IP addresses. In some cases the ransomware fees have reached even several tens of thousand of USD, which means huge savings for the potential victims thanks to the NASK decryptors.

EUNITY Program

EUNITY aims to encourage, facilitate and develop the dialogue between Europe and Japan on cybersecurity, in order to:

- encourage, facilitate and support the ICT dialogue between relevant EU and Japanese stakeholders on matters related to cybersecurity and privacy R&I trends,
- ensuring a broad participation of the relevant stakeholders in workshops and cross channeling the collected information between EU-based groups such as ECSO, EOS, NIS, and the CSA.
- identify potential opportunities for future cooperation between European and Japanese R&I ecosystems,
- foster and promote European cybersecurity innovation activities and increase the international visibility of EU activities in cybersecurity

EDITORIALS

Principal Editor
Prof. Ewa Niewiadomska Szynkiewicz

Journal's editor, general concept and design
Inez Okulska Ph.D.

Editorial board
Inez Okulska Ph.D.
Paweł K. Kostkiewicz M.Sc.Eng.

Contributors
Michał Karpowicz Ph.D.Eng.
Michał Marks Ph.D.Eng.
Paweł K. Kostkiewicz.M.Sc.Eng.
Przemysław Puławski.M.Sc.Eng.

Proof reading
Przemysław Puławski M.Sc.Eng.

NCP NATIONAL CYBERSECURITY PLATFORM

The National Centre for Research and Development

KSO3C

KSO3C and NPC, BioMobi, RegSoc,`Fòrensic
Lab Projects are upported by the National
Centre of Research and Development
under the CyberSecIdent Programme

Research and Development

NASK is National Research Institute motivated by the challenge to support the development of innovative ideas and technology transfer.

Our mission is to enforce and to efficiently exploit interactions between science and industry. Our researchers and engineers use this unique experience to develop technology-intensive solutions focused on ICT innovation, cybersecurity, biometrics and artificial intelligence. We transfer ready-to-deploy technologies to public administration, critical infrastructure and industrial partners.

Key activities of NASK are related to ensuring the security of Internet and help to bring safety to the cyberspace. Computer Security Incident Response Team (CSIRT). operating within the structure of NASK, is tasked with responding to cybersecurity threats in networks.

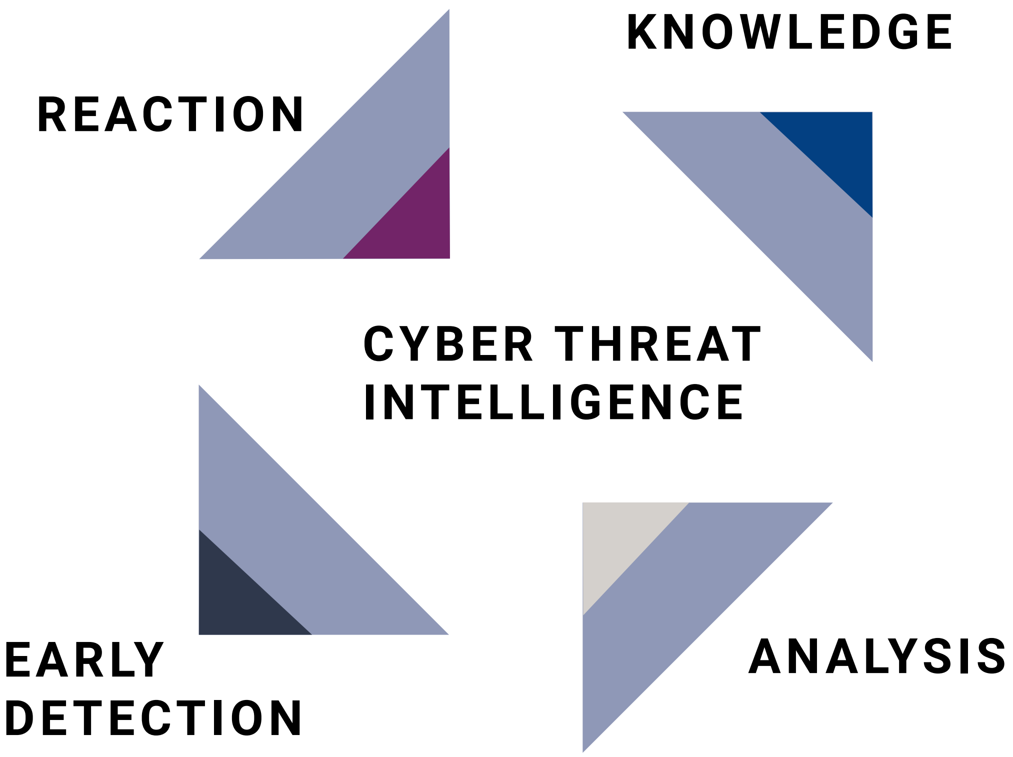
NASK is also engaged in training and educational activities, focusing on cybersecurity and safe use of new technologies.

Prof. Ewa Niewiadomska-Szynkiewicz
Deputy Director
Research Director at NASK

NASK

What is the difference between NASK and market oriented cybersecurity services providers? NASK creates solutions that will serve current and future needs of our implementations NASK researchers define a commercial problem in terms of scientific one and then by means of more theoretical or even abstract tools find a solution that not only meets the requirements but also is innovative.

The main work at NASK Research and Development is focused on cybersecurity i.e. detection reaction to incidents data acquisition and processing as well as sharing of gathered information.



REACTION

KNOWLEDGE

CYBER THREAT INTELLIGENCE

EARLY DETECTION

ANALYSIS

| National Research Institute NASK ul. Kolska 12, Warsaw, Poland | +48 22 380 82 00 | www.nask.pl |