KIBERNETSKI CUNAMI

Ali smo pripravljeni na spremembe ZInfV?

KIBERNETSKI CUNAMI

Ali smo pripravljeni na spremembe ZInfV?

Pozdravni nagovor

Marjana Majerič

izvršna direktorica GZS

KIBERNETSKI CUNAMI

Ali smo pripravljeni na spremembe ZInfV?

KIBERNETSKI CUNAMI

Ali smo pripravljeni na spremembe ZInfV?

Pozdravni nagovor

Igor Zorko

podpredsednik za malo gospodarstvo pri GZS

KIBERNETSKI CUNAMI

Ali smo pripravljeni na spremembe ZInfV?

Ali smo pripravljeni na spremembe ZInfV?

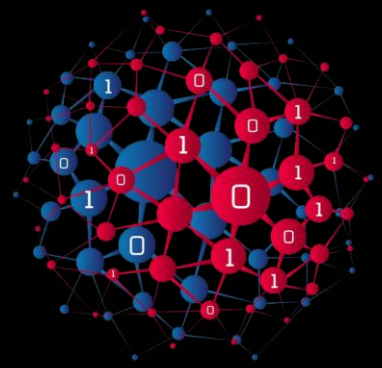
Navigating the EU Cyber Security Landscape: Technologies, Roadmaps, and Challenges

Roberto Cascella

CTO, European Cyber Security Organisation (ECSO)

ECS

EUROPEAN CYBER SECURITY ORGANISATION



Empowering
European
Cybersecurity
Communities

Navigating the EU Cyber Security Landscape: Technologies, Roadmaps, and Challenges

Roberto Cascella

CTO

Cyber Tsunami - 18 October 2024

Who we are

Created in 2016 as the contractual counterpart to the European Commission for implementing **Europe's unique Public-Private Partnership in Cybersecurity (2016-2020)**

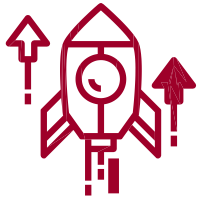
The aim of the partnership was to foster cooperation between public and private actors to allow people in Europe to **access innovative and trustworthy European solutions**

Today, ECSO builds upon the many successes of the Partnership and with its cross-sectoral membership base contributes to **developing cybersecurity communities** and builds the **European cybersecurity ecosystem**

ECSO is the **Leader of the ECCO project**, aimed at developing the European Cybersecurity Community, linked to the ECCC Regulation (NCCs etc.).

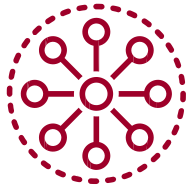
Overview of ECSO Members

Large companies (users and providers)

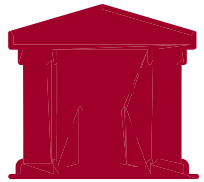


SMEs & start-ups

Research centres, Universities



European, National and Regional clusters & associations



Local, regional and national public administrations

Investors

End-users and operators of critical infrastructures and essential services

As of today, ECSO counts more than **300** Members
+ a few thousand indirectly via Associations

Cybersecurity policies and initiatives

- The EU Security Union Strategy (July 2020)
- The EU Cybersecurity Strategy (December 2020)
  - resilience, technological sovereignty and leadership;
  - operational capacity to prevent, deter and respond;
  - a cooperation to advance global and open cyberspace.

Source: EU website https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en

Revised rules on the security of network and information systems

Development of a European Cyber Shield through a network of AI-enabled Security Operations Centres that can detect signs of cyberattack and enable preventive action before damage occurs

High standards of cybersecurity for all connected objects

Dedicated support to SMEs

Attracting and retaining the best cybersecurity talent

Investing in research and innovation

Securing 5G networks and supply chain

Cybersecurity policies and initiatives

- The EU Security Union Strategy (July 2020)
- The EU Cybersecurity Strategy (December 2020)
  - resilience, technological sovereignty and leadership;
  - operational capacity to prevent, deter and respond;
  - cooperation to advance a global and open cyberspace.

Source: EU website https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en

- The European Cybersecurity Competence Centre (ECCC)
  - Strategic Agenda published March 2023
- Legislations and certification

EU Policymaking

In Brief

EU policymaking has been very active in the latest mandate,
with multiple pieces of legislation being proposed and some already officially published.

The upcoming challenges concern the finalisation of some policies and their implementation.

NIS2 Directive

Cyber Solidarity Act

Product Liability Directive

Cybersecurity for EU Entities

Cyber Resilience Act

AI Act

EU Digital Identity

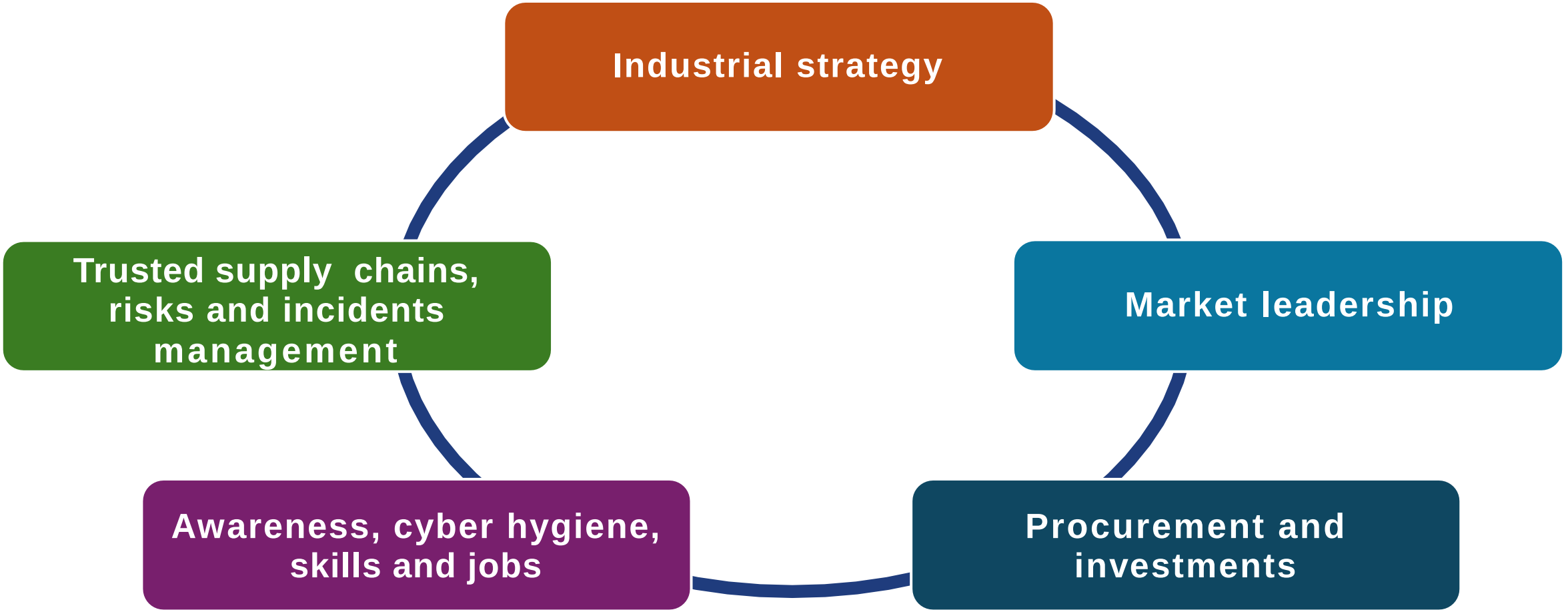
DORA


Key objectives
Ecosystems / Frameworks for cyber security
Growth development areas
Systems / Applications
Strategic and enabling technologies / solutions

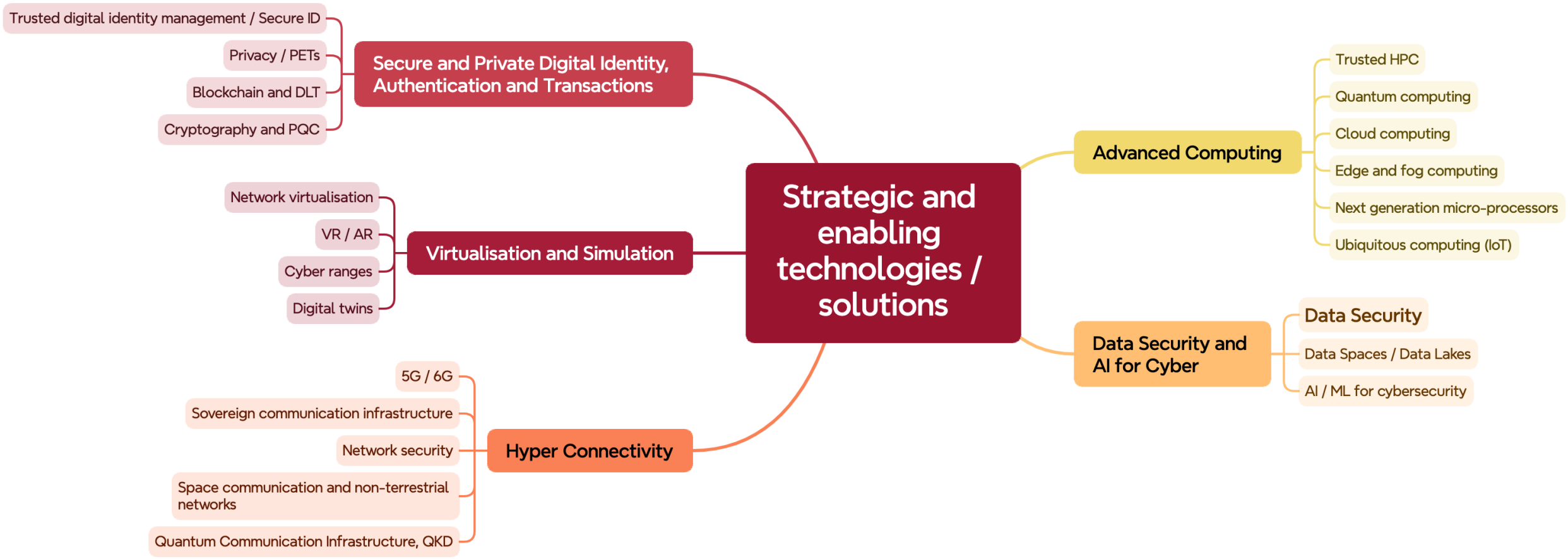
Key objectives

Cyber Resilience	**Enhance the ability to withstand, adapt to, and recover from cyberattacks**
Strategic Autonomy	**Strengthen the European Cybersecurity Ecosystem / Market, increasing Strategic Autonomy**
Competitiveness	**Foster Growth, Innovation and Competitiveness of the European Cybersecurity Industry**

Growth development areas



Technology Roadmap for critical cyber technologies to support the development of strategic cyber capabilities in Europe



ECSO WGs and activities

WG Trusted Supply Chains

- Understand the impact of policy implementation
- Prepare for CRA implementation
- Build trustworthiness in European Supply Chains

WG Investments & Market Development

- Investments: Invest4Cyber; European CybersecurityInvestment Platform ; Cyber Investor Days; STARtup Award
- SMEs to Market: Internationalisation; Network of SMEs' founders; Cyber Solution Days; STARtup / CISO Choice Award
- Regional Approaches: Cyber EDIH Network; Cooperation across Regions, SMEs as users
- CyberHive - Marketplace and Label CYBERSECURITY MADE IN EUROPE
- Monthly Cybermarket Report & Market Intelligence / Policy & Market
- trends International (non EU) relations (e.g. coop. with Ukraine)

CYBERSECURITY™ MADE IN EUROPE

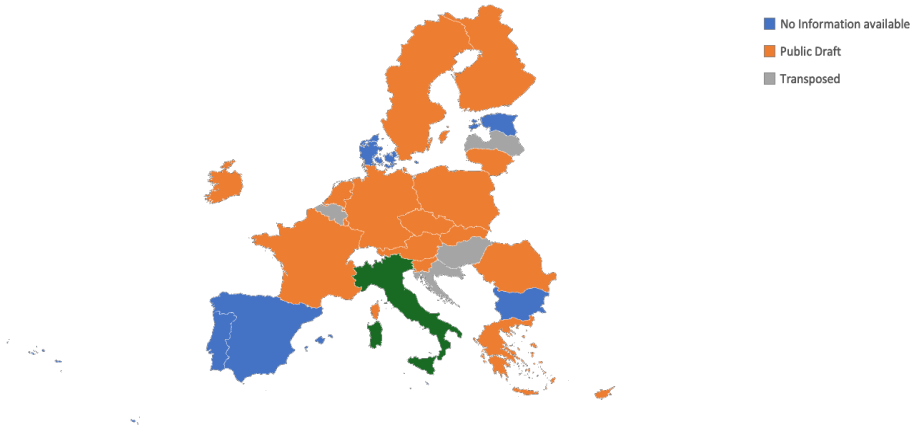
cyberhive EUROPE

ECSO WGs and activities

WG Cyber Threat Management

- CISOs Trusted Cooperation: EU CISO Network - Dialogue & Cooperation among CISOs across countries and vertical sectors
- CTI Sharing: SOCs, European CTI Alliance
- Use of Trusted Solutions / Services: Support to implementation of EU legislations: NIS2, etc.; Cyber Solution Days / CISO Choice Award; support to implementation of Trusted Solutions & Service

Transposition Overview: Fragmented Approach

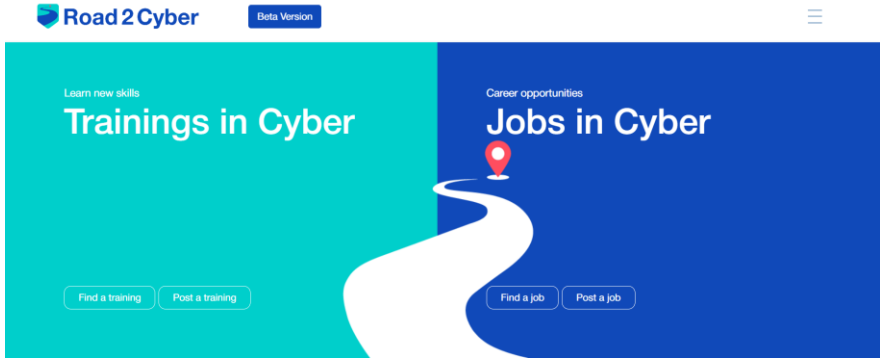


5 Countries have fully adopted the NIS2 Directive into the National Law: Belgium, Croatia, Hungary, Italy and Latvia. **17 countries** have published drafts: Austria, Cyprus, Czech Republic, Finland, France, Germany, Greece, Ireland, Lithuania, Luxembourg, Netherlands, Poland, Romania, Slovakia, Slovenia, Sweden. **6 Countries** have not published draft yet: Bulgaria, Denmark, Estonia, Malta, Portugal, Spain.

Road 2 Cyber

An ECSO and Women4Cyber initiative to address the talent shortage in EU

1 centralized platform **50+** trainings **100+** job openings **1** European HR Community



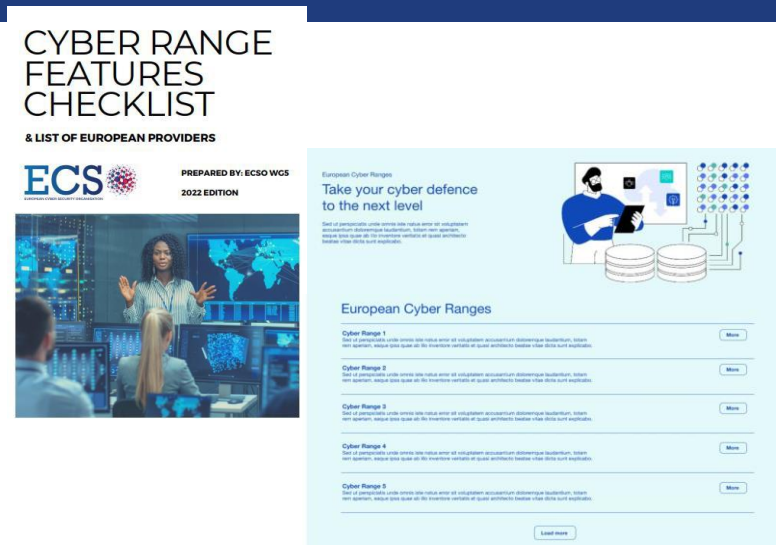
Road2Cyber: the spirit of lifelong learning

Accompanying job seekers throughout their journey in cybersecurity, supporting career progression & upskilling/reskilling, access to job market.

Other paths to improve skills in cyber

Access to Cyber Ranges

- Identify and promote available cyber ranges and cyber range-enabled services across Europe
- Utilise cyber ranges to enhance your skills via a practice field within which to validate processes, technologies and skills/competences
- Access ECSO's Cyber Ranges Checklist and use it to define your needs (end users) or tailor your offer (providers)



WG (6) on Technologies & Innovation and Defence + Space

Vision

A strong, resilient and increasingly autonomous European cybersecurity ecosystem with an efficient and secure digital transition of the industry and society.

Ongoing work

Define the vision to strengthen the European cybersecurity ecosystem and pursue the Strategic Research and Innovation Roadmap.

Publish technical papers to identify challenges and **analyse** relevant cyber security technologies for dual use technologies and space.

- Blockchain, IoT, Digital Twins, Secure SW Supply chain – already published
- AI and Quantum (ongoing)

Monitor the future Horizon Europe and Digital Europe Programmes and investment opportunities for R&I.

Collaborate in various initiatives with the Data Spaces Support Centre, the SNS IA on 6G security, the ECMWF and with European associations in the Transcontinuum initiative.

TCI
TransContinuum Initiative

Cybersecurity Strategic Vision

A strong, resilient and increasingly autonomous European cybersecurity ecosystem with an efficient and secure digital transition of the industry and society.

Strategic Pillars

Digital self-reliance, which encompasses the capability to develop and implement strategies to enhance resilience against cyber threats and attacks

Digital strategic autonomy, enabler of sovereignty, aimed at bolstering Europe's potential while minimizing its dependence on external suppliers.

European strategic sovereignty as the ability of European Member States to independently define and enforce laws or regulations dealing with digital issue

Ensuring that European Fundamental rights are protected, including the right to privacy and self-determination.

Cyber threats

- Supply chain compromise of SW/HW dependencies
- Social engineering & Insider Threat
- operations and disinformation
- Ransomware attacks
- Cyber espionage & cyber terrorism
- Cloud-based threats
- Profiling and behavioural model attacks
- Infrastructure attacks
- Data destruction or destruction, wiper attacks
- Crypto jacking
- Cyberattack-as-a-service
- DDos
- Insider threat

Some relevant trends impacting cybersecurity

GEOPOLITICAL

- Cyberspace will continue to become a force multiplier
- Creation of EU multinational cyber structures
- US and China will reduce technological dependency
- Non-EU ownership over submarine cables
- Non-EU companies will control VPN providers
- Non-state actors in cyber operations
- Cyber threats in information campaign to create instabilities

ECONOMIC

- Increase in cybercrime
- Disruptive Technologies will increase consistently EU GDP
- Increase in cyber spending
- Adversarial machine learning deployed to target critical infrastructure

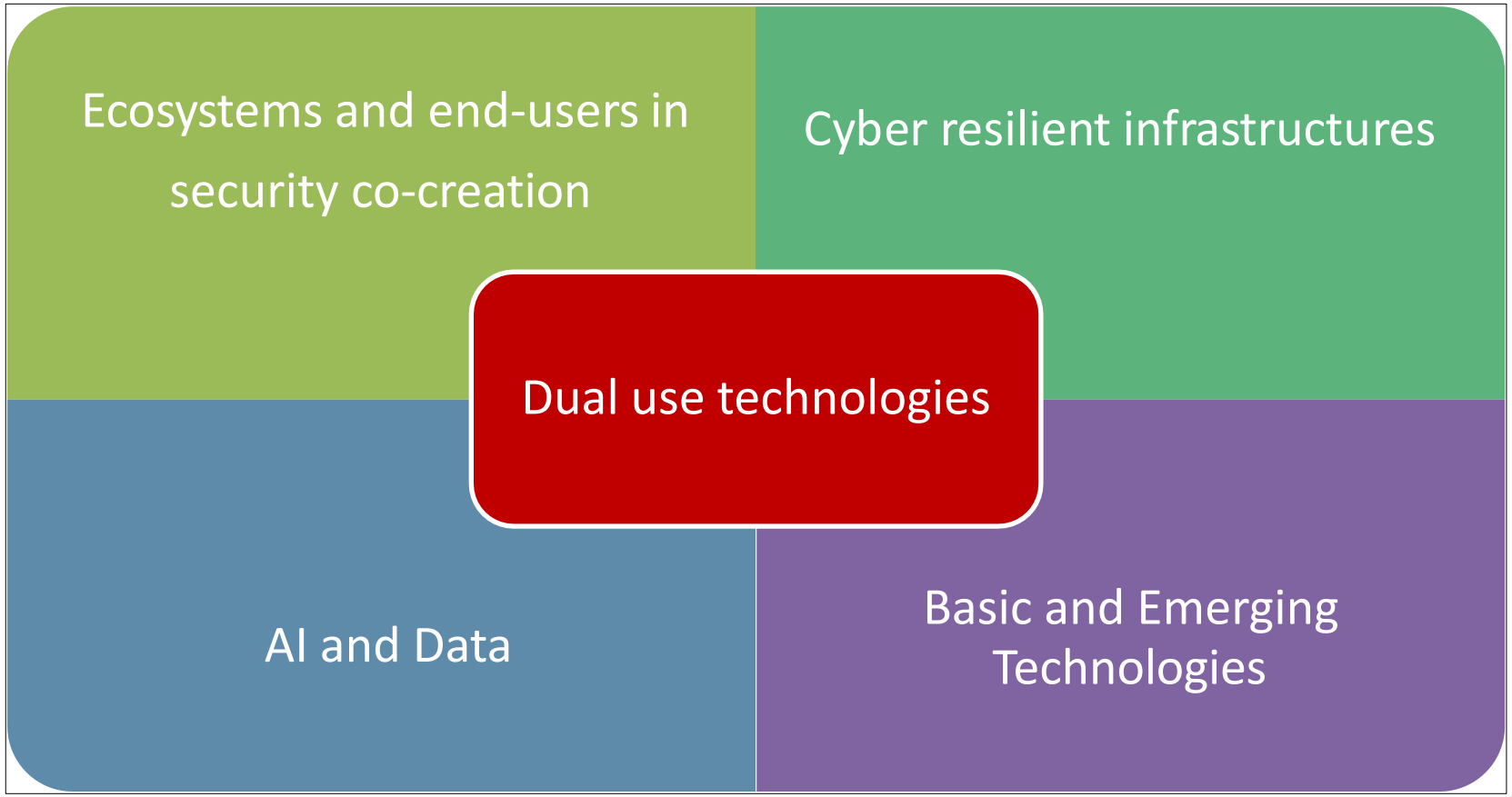
SOCIAL

- Surge in attacks to privacy and data protection
- Increase in digital connectivity
- Growth of Tech Sceptics
- Use of disruptive technology for fake news campaigns
- Increase in cyber education and awareness
- Increase in digital skills shortages
- Growing involvement of national governments in digital matters

TECHNOLOGICAL

- Global landscape characterized by Intelligent, Interconnected, Distributed and Digital technologies, such as AI, 6G, IoT, edge and cloud computing.
- Quantum technology (PQC, QKD)
- Augmented reality, virtualisation, digital twins and metaverse
- Data spaces
- Privacy Enhancing Technologies (PETs)
- IT predominately impacting OT operations
- IAM and decentralised identities
- New approaches such as Zero Trust, OpenSource, Automation, Converge of IT/OT
- New strategic emerging sectors: Robotics, Avionics, Autonomous driving, Space, Bionics, etc.

Challenge areas



SWG6.1 Ecosystems and end-users in security co-creation

Cybersecurity capacity building and *supply chain security challenges, including support to organizations in creating and assessing secure products and services*

- Support automated cybersecurity assessment, evaluation and certification of products thanks to AI and simulated environments for testing
- Resilient systems: Adaptive Software Hardening, Self-Healing systems and RASP
- Digital forensics mechanisms and analytical support
- Extended Reality Environments and Digital Twins for cyber-ranges
- Cybersecurity Maturity Model for SMEs
- Supply chain Security

SWG6.2 Critical infrastructures

Challenges linked to resilience, high-availability and performances of critical infrastructures, considering the digital transformation and regulations

- Continuous and Collaborative Cyber-physical Risk Assessment and Management, also considering operational requirements of CIs
- Use of emerging technologies (especially Digital Twin and AI) to strengthen CI resilience and operations
- Regulatory compliance
- Situational awareness and coordinated handling of security-related events, attacks and incidents

SWG6.3 AI and data

Fortify the future of data and AI landscapes looking into comprehensive data security aspects to fortify system resilience and focusing on related aspects such as data sovereignty

Data protection (anonymisation, minimization, encrypted data processing, synthetic data generation, ...)

Development of security defences based on big data and AI – use of generative AI

Adversarial AI attacks (data poisoning, evasion attacks, model inference/extraction)

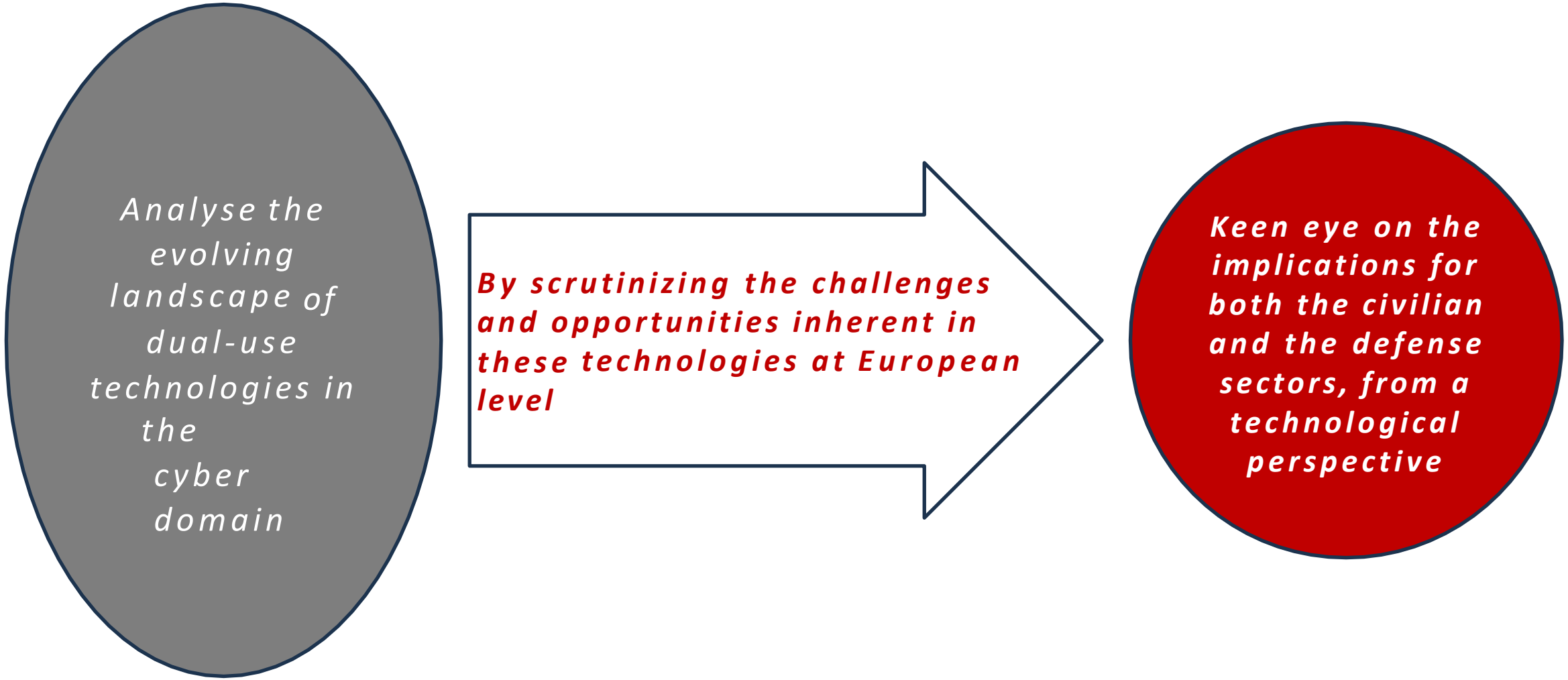
Abuses of AI (deep fakes, disinformation, etc.)

SWG6.4 Basic and Emerging technologies

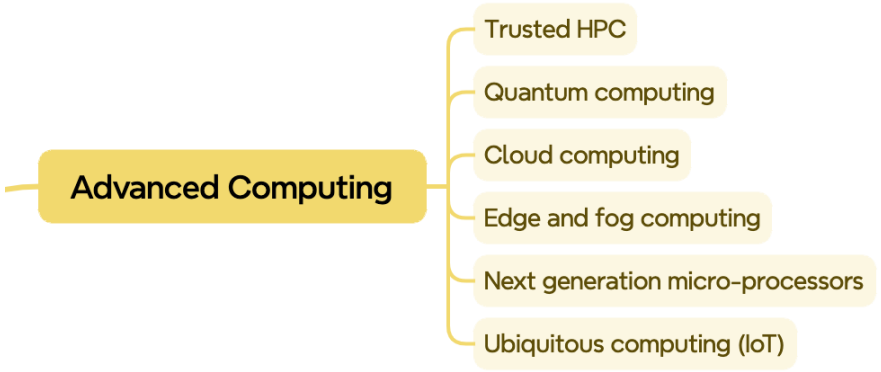
Horizontal foundational and upcoming technologies with the potential of influencing the overall cybersecurity ecosystem across multiple verticals

- Cryptography and key distribution (QKD/PQC/Homomorphic encryption)
- Trusted electronics, Open-Source HW
- Zero-trust technologies and methodologies for automated security assessment of incremental system changes
- Block chain, IoT, Digitial twin

SWG6.5 Dual use technlogies



Call to actions

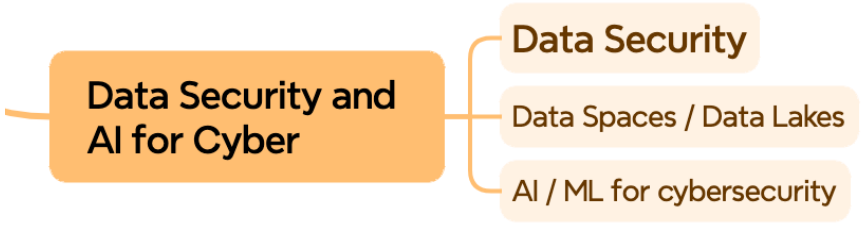


Cross challenges

- Growing adoption of cloud services for data storage, application deployment, and other critical functions
- Different sectors have varying security requirements for their cloud network infrastructure
- Quantum computing is still at early stage but with large potentials to enhance the development of cybersecurity

- Implementation of trusted secure environments in microchips and adaptive security solutions
- Confidential computing (in processors, graphic processors, FPGA) by using hardware-based TEE to improve data and application security in a separate and trusted area of microchip
- Security solutions for the convergence of continuum computing from edge to cloud
- End-to-end cloud based security solutions addressing new emerging threats
- Quantum to enhance computing capabilities, e.g. to develop new AI-based solutions or to test / develop new post-quantum crypto algorithms
- Integrated approaches that protect both the digital and physical components

Call to actions



Cross challenges

- Data quality and identification of sensitive data (projection)
- Growing unstructured data volumes and increased demand for secure data solutions
- Protection of sensitive information and operational continuity
- Data life-cycle management and data governance
- Regulations and compliance with safeguard sensitive data

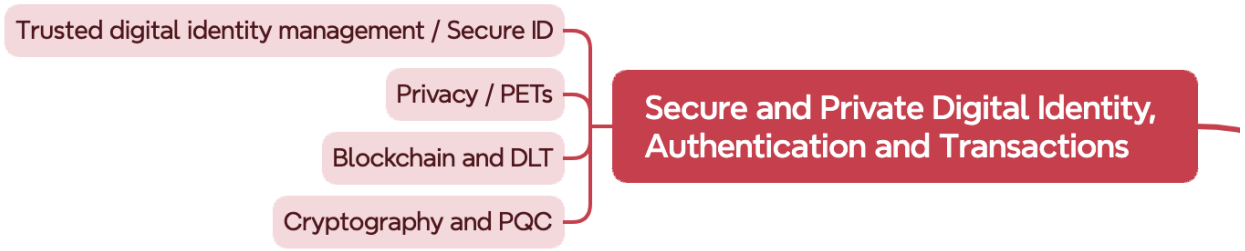
- Improved secure data sharing and promotion of interoperability of data to simplify access and usage
- Next-generation data backup and recovery solutions that are immutable and tamper-proof, ensuring data integrity even after a cyberattack
- Advanced and AI/ML-powered analytic capabilities to collect and analyse vast amounts of data from various sources ➔ ex. for threat intelligence
- Automatic security tasks: automatic detection and response to mitigate automated cyberattacks, including dynamic recovery capabilities (self-healing) and autonomous response
- New GenAI security applications from design of security solutions to training, including understanding of threats to contextualisaiton of threats including remediation and response)

Call to actions

Cross challenge: growing adoption of virtualized technologies with the potential to integrate multiple emerging technologies

- Integration of physical / digital world security into metaverse
- Digital twin solutions to prove new security solutions before deployment, including pre-emptive analysis cross-platform attacks and security evaluation (including risk) at different layers

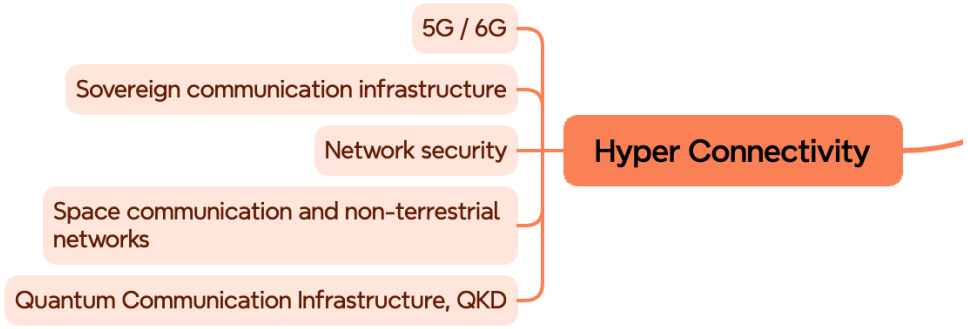
Call to actions



- Advanced data minimization and masking techniques
- Federated learning mechanisms for privacy preservation and data security

- Efficiency, performance and scalability of fully homomorphic encryption, zero-knowledge proofs, multi-party computation, differential privacy, etc…
- Develop robust encryption methods to protect data (e.g. personal, classified information, system configuration and biological)
- Evaluation of existing quantum-resistant encryption methods
- Develop new cryptographic primitives that are quantum resistant and migration towards quantum-resistant crypto
- DLT and blockchain to improve access controls, data immutability and traceability, along with decentralisation and scalability of cybersecurity solutions

Call to actions

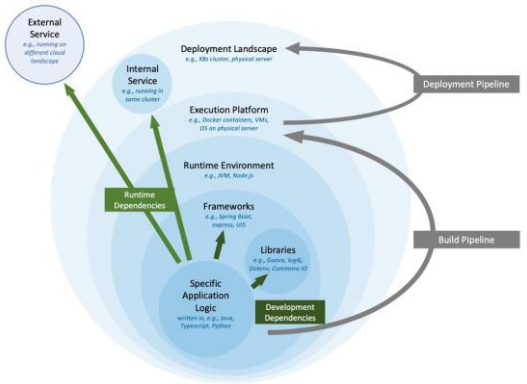


Cross challenges

- Convergence for a secure ecosystem integrating different technologies
- 5G/6G as infrastructures for many and different critical applications
- Integration of non terrestrial networks and space connectivity

- Enhanced self-preservation of the infrastructure with improved capabilities to cope with known and unknown cascading infrastructure failures (e.g. Threat intelligence and risk management solutions)
- End-to-end security coupling network and application security
- Holistic security assurance and management across multiple domains including unified threat, risk & vulnerabilities management
- Cognitive, autonomic, end-to-end orchestration of future network services, supporting secure, dynamic computing resource pooling and balancing between the edge and the cores

ECSO Technical Paper on Software Supply Chain Security



Foundational work at the center of many current regulatory efforts as well as well current cybersecurity issues to manage a trusted supply chain

What Prompted this research?

- ➢**Widespread adoption of software, including open source**
- ➢**Increased complexity of SW development and limited awareness of dev processes**
- ➢**Recent attacks exploiting supply chain vulnerabilities & how SW packages are built**
- ➢**Reliance on 3rd party contributions, tools and components**

14 Specific recommendations to secure the supply chain organised a s

Frameworks and Development practices

How to reduce the risk exposure

Concrete innovations needed

Skill gap

Cybersecurity suffers from a huge gap of experts[1].
Demand will continue to rise, and the gap cannot be bridged without involving half of the available workforce.

347.700+ in Europe

3.99 million worldwide

Cybersecurity workforce

5.5 million worldwide

440,000 new jobs +8.7% YoY

This is exacerbated by a lack of female representation, with women making up only 25% of the workforce worldwide (around 20% for Europe)

25% WOMEN IN THE CYBERSECURITY WORKFORCE (EST)

According to Microsoft, closing the gender gap in STEM careers would help increase the EU's GDP per capita by up to 3% by 2050.

Courtesy of WOMEN 4CYBER EUROPEAN CYBER SECURITY ORGANISATION

[1] ISC² "2023 Workforce Report

ECS

EUROPEAN CYBER SECURITY ORGANISATION

Avenue des Arts 46 Kunstlaan
1000 Brussels
Belgium
secretariat@ecs-org.eu

www.ecs-org.eu

European Cyber Security Organisation (ECSO)

@ecso_eu

KIBERNETSKI CUNAMI

Ali smo pripravljeni na spremembe ZInfV?

Ali smo pripravljeni na spremembe ZInfV?

ZInfV-1: regulatorne zahteve in odgovornost podjetij za informacijsko varnost

Matjaž Mravljak

direktor Inšpekcije za informacijsko varnosti, URSIV

REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE ZA INFORMACIJSKO VARNOST

URSIV

zit SeKV

Združenje za informatiko in telekomunikacije
Kibernetska varnost

ZInfV-1: regulatorne zahteve in odgovornost podjetij za informacijsko varnost

Matjaž Mravljak, direktor Inšpekcije za informacijsko varnost
Urad Vlade Republike Slovenije za informacijsko varnost

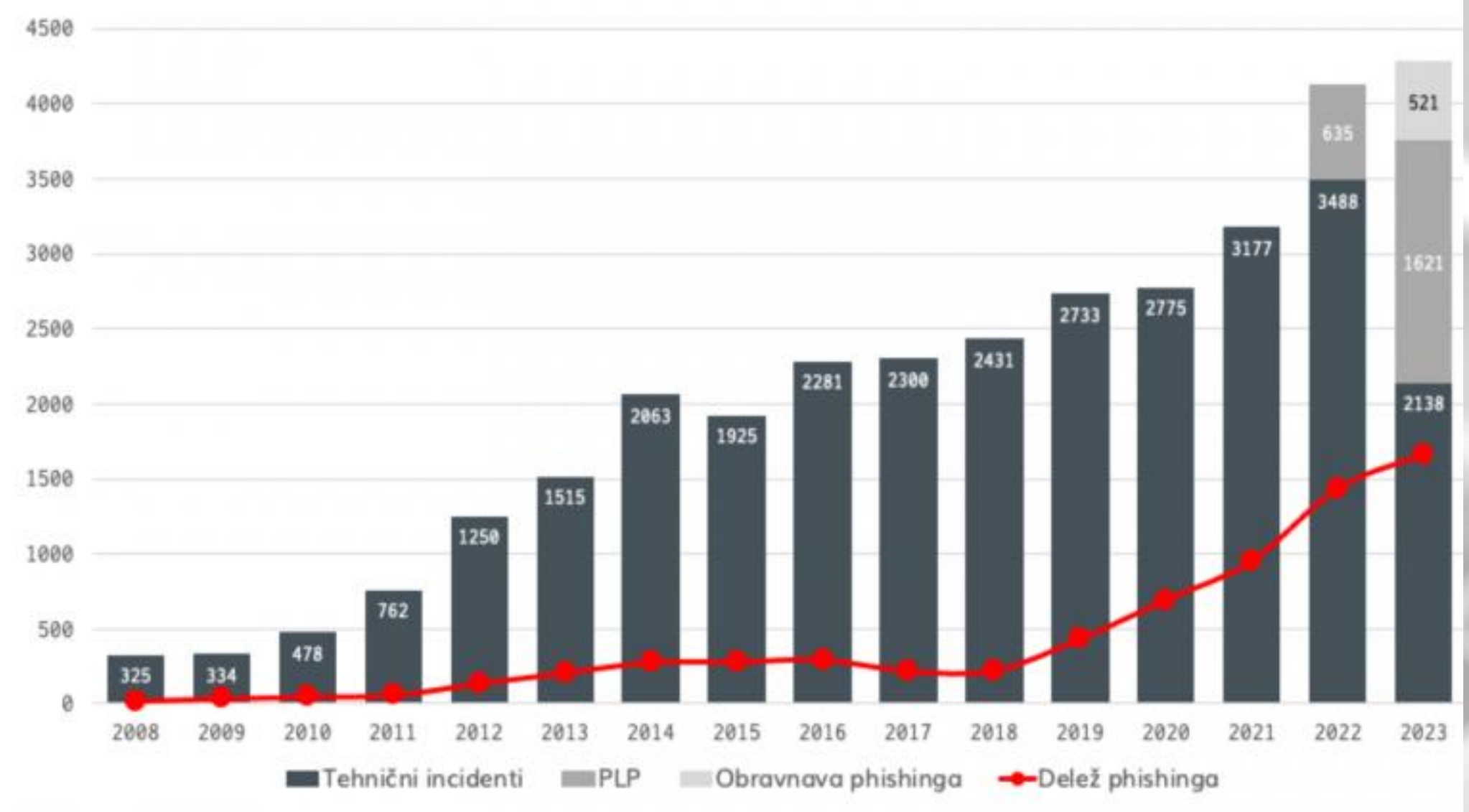
Ljubljana, oktober 2024

Uvod

Uvod v NIS 2

- V Evropski uniji je bilo v 2022 izvedenih **43 % kibernetskih napadov na mala in srednje velika podjetja**, ki niso imela vzpostavljenih ustreznih varnostnih mehanizmov.
- Od tega **83 %** napadenih malih in srednjih podjetij **ni bilo pripravljenih na okrevanje po kibernetskem napadu**.
- Vsak dan v 2022 je bilo v EU poslanih **3,1 milijarde lažnih e-poštnih sporočil**, del teh lažnih sporočil je kljub varnostnim ukrepom **pristal v e-poštnih predalih ljudi.**
- V Evropski uniji je v 2022 znašala **skupna materialna škoda** (posredna in neposredna) **zaradi kibernetskih incidentov in napadov** približno **150 milijard evrov**.

Uvod v NIS 2



https://www.cert.si/kibernetska-varnost-2023-v-

Uvod v NIS 2

DIREKTIVA (EU) 2022/2555 EVROPSKEGA PARLAMENTA IN SVETA z dne 14. decembra **2022**

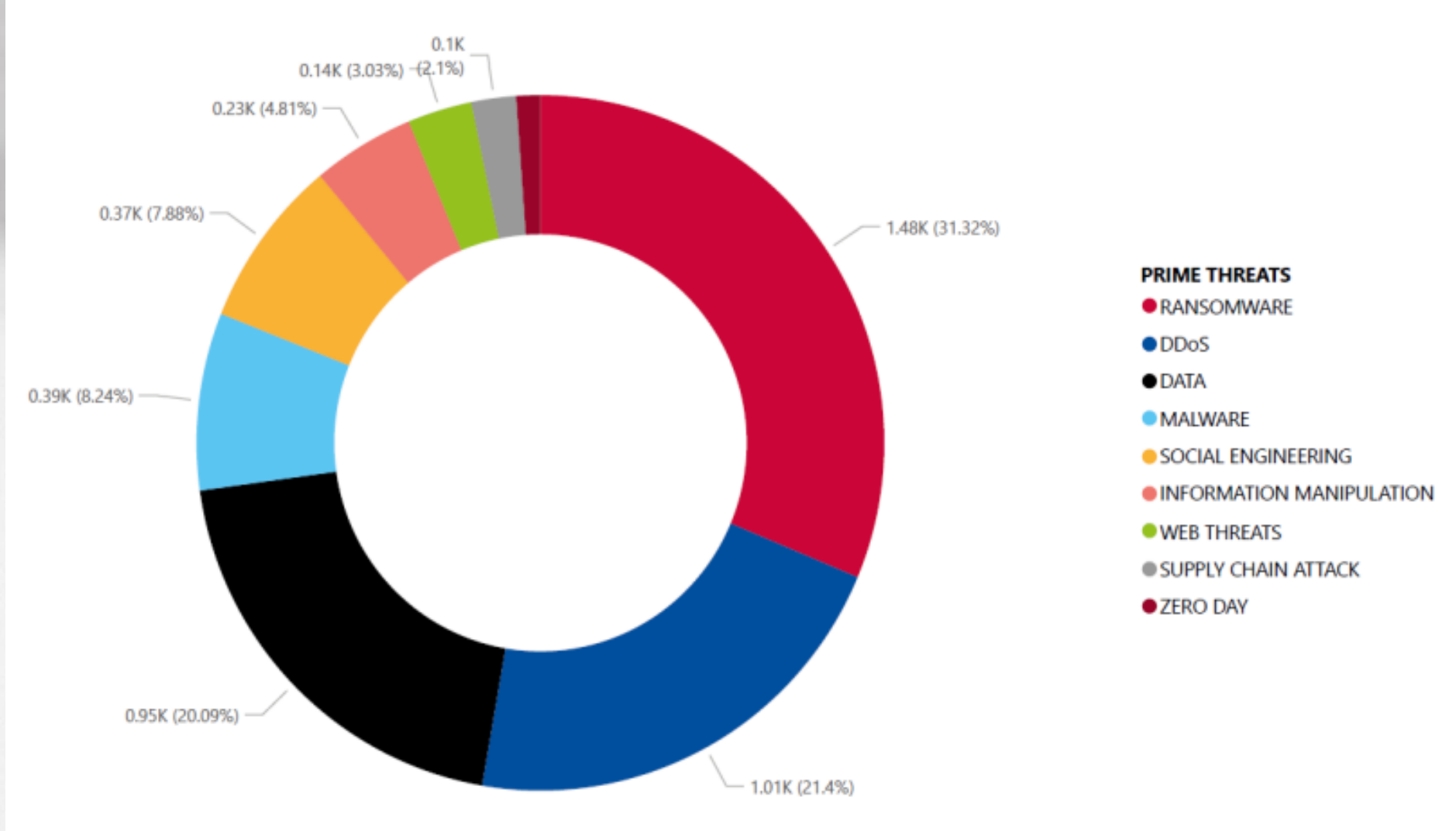
o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148

DIREKTIVA (EU) 2016/1148 EVROPSKEGA PARLAMENTA IN SVETA z dne 6. julija 2016

o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji

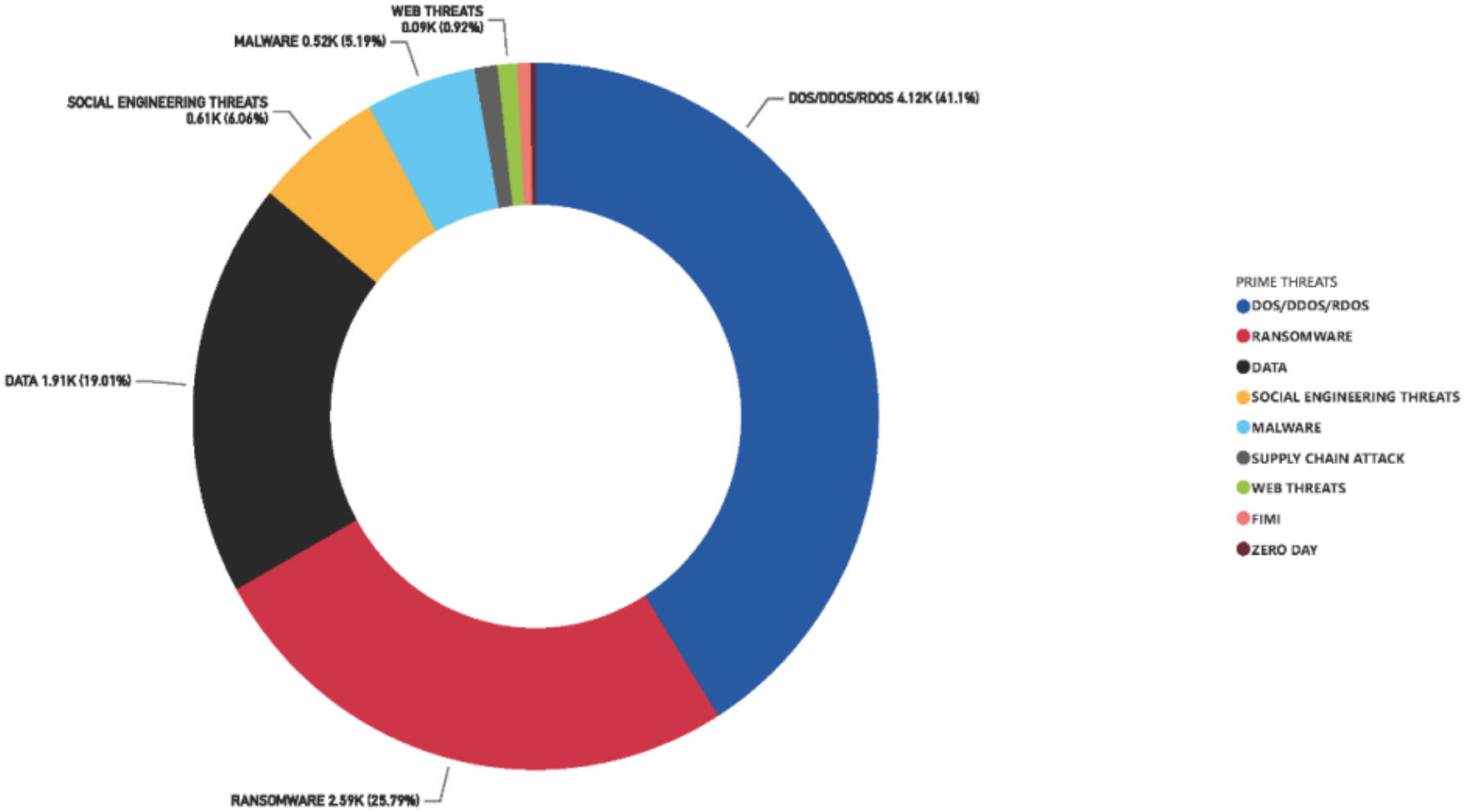
Uvod v NIS 2

Kibernetski incidenti v EU julij 2022 – julij 2023 (ENISA)



Uvod v NIS 2

Kibernetski incidenti v EU julij 2023 – julij 2024 (ENISA)



Uvod v NIS 2

- Je **vseevropska horizontalna zakonodaja** (nanaša se na različne sektorje gospodarstva, gospodarske družbe, javni sektor, operaterji, ipd.) **o kibernetski varnosti**.
- **Krepi varnostne ukrepe** in jih podrobneje določa ter sloni na **pristopu upoštevanja vseh nevarnosti** (fizična varnost, varnost dobavnih verig, politike kriptografije, večfaktorska avtentifikacija).
- Vzpostavlja osnovni okvir za **usklajeno razkrivanje ranljivosti**.
- Krepi **skupno situacijsko zavedanje in kolektivno sposobnost odzivanja na kibernetske napade** znotraj Evropske unije.
- Zagotavlja **povečanje splošne ravni kibernetske varnosti** v EU.
- **Rok za njen prenos** v nacionalno zakonodajo (z ZInfV-1) ter za notifikacijo te zakonodaje Evropski komisiji (EK) je **17. 10. 2024**.

BISTVENI SUBJKEKTI (visoko kritični sektorji)

PRILOGA I: **VISOKO KRITIČNI SEKTORJI**:

1. **energija** (elektrika, daljinsko ogrevanje in hlajenje, nafta, vodik);
2. **promet** (zračni, železniški, vodni, cestni);
3. **bančništvo** (kreditne institucije);
4. **infrastruktura finančnega trga** (upravljalci mest trgovanja, centralne nasprotne stranke);
5. **zdravje** (izvajalci zdravstvenega varstva, referenčni laboratoriji, medicinski pripomočki);
6. **pitna voda** (dobavitelji in distributerji pitne vode – glavna dejavnost);
7. **odpadna voda** (zbiranje, odvajanje in čiščenje odpadne vode – glavna dejavnost);
8. **digitalna infrastruktura** (DNS, TLD, storitve zaupanja, operaterji javnih elektronski komunikacijskih omrežij ali storitev, podatkovni centri, storitve oblaka);
9. **upravljanje storitev IKT** (ponudniki upravljanih varnostnih storitev);
10. **javna uprava** (centralni nivo državna uprava, lokalni (regionalni) nivo);
11. **vesolje** (upravljalci talne infrastrukture, podpora opravljanja vesoljskih storitev).

POMEMBNI SUBJKEKTI (drugi kritični sektorji)

PRILOGA II - **DRUGI KRITIČNI SEKTORJI**:

1. **Poštne in kurirske storitve** (izvajalci določenih poštnih in kurirskih storitev);
2. **Ravnanje z odpadki** (izvajalci – glavna dejavnost);
3. **Izdelava, proizvodnja in distribucija kemikalij** (proizvodnja in distribucija določenih snovi);
4. **Pridelava, predelava in distribucija živil** (prodaja na debelo, industrijska pri(e)delava);
5. **Proizvodnja določenih vrst izdelkov** (medicinski pripomočki; računalniki, elektronski in optični izdelki, proizvodnja električnih naprav, proizvodnja drugih strojev in naprav, proizvodnja motornih vozil, prikolic, polprikolic, proizvodnja drugih vozil in plovil);
6. **Digitalni ponudniki** (spletne tržnice, spletni iskalniki, platforme storitev družbenega mreženja);
7. **Raziskave** (raziskovalne organizacije).

ZAVEZANCI PO NIS 2

BISTVENI SUBJEKTI:

- Vsi subjekti, iz Priloge Direktive 2022/2555 I, ki imajo **vsaj 250 zaposlenih** in **letni promet vsaj 50 milijonov EUR** oziroma letno bilančno vsoto vsaj 42 milijonov EUR.
- Ponudniki kvalificiranih storitev zaupanja in registri vrhnjih domenskih imen ter ponudniki storitev DNS, **ne glede na njihovo velikost**.
- Ponudniki javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev, ki imajo **vsaj 50 zaposlenih** in letni promet oziroma **letno bilančno vsoto vsaj 10 milijonov EUR**.
- Subjekti javne uprave na državni ravni in mestne občine.

ZAVEZANCI PO NIS 2

BISTVENI SUBJEKTI:

- Subjekti, ki so določeni kot kritični na podlagi zakona, ki ureja kritično infrastrukturo.
- Subjekti, ki so bili v skladu z Zakonom o informacijski varnosti določeni kot izvajalci bistvenih storitev pred 16. januarjem 2023.
- Vsi drugi subjekti vrste iz Prilog Direktive 2022/2555 I ali II, ki jih država članica identificira in jih na predlog pristojnega nacionalnega organa **določi vlada z odločbo**.

ZAVEZANCI PO NIS 2

POMEMBNI SUBJEKTI:

- Vsi subjekti, ki izvajajo vrste dejavnosti iz **Prilog I in II Direktive**, in niso določeni kot bistveni subjekti, imajo pa **vsaj 50 zaposlenih** in letni promet oziroma **letno bilančno vsoto vsaj 10 milijonov EUR**.
- Subjekti, ki so v državnih načrtih zaščite in reševanja opredeljeni kot **službe državnega pomena**, če bi nedelovanje njihovih omrežnih in informacijskih sistemov ogrozilo izvajanje nalog zaščite in reševanja.
- Subjekti iz Prilog I in II Direktive, ki jih na podlagi zakonskih kriterijev **določi vlada z odločbo.**

ZAVEZANCI PO NIS 2

KRITERIJI ZA DOLOČITEV BISTVENEGA ALI POVEZANEGA SUBJEKTA Z ODLOČBO:
Subjekt **sodi v katero od kategorij** iz Prilog Direktive 2022/2555 I ali II, **ne glede na velikost in:**

- **Je edini ponudnik storitve**, ki je bistvena za ohranjanje kritičnih družbenih ali gospodarskih dejavnosti v Republiki Sloveniji.
- **Bi motnja pri opravljanju storitve** subjekta lahko povzročila pomembno sistemsko tveganje, zlasti za sektorje, v katerih bi lahko taka motnja imela **čezmejni vpliv.**
- Je **subjekt kritičen zaradi** njegovega posebnega pomena na državni, regionalni ali lokalni ravni za določen sektor ali vrsto storitve ali za druge medsebojno odvisne sektorje v Republiki Sloveniji.
- Gre za **subjekt javne uprave na državni ravni ali na regionalni oziroma lokalni ravni**, če pri slednjem izhaja iz ocene tveganja, da opravljajo storitve, katerih **motnje bi lahko pomembno negativno vplivale** na ključne družbene ali gospodarske dejavnosti.

Zavezanci NIS 1 vs NIS 2

NIS 1

- Izvajalci bistvenih storitev (49)
- Organi državne uprave (18)
- Ponudniki digitalnih storitev (1)
- Povezani subjekti (450)

NIS 2

- **Bistveni subjekti** (visoko kritični sektorji)
- **Pomembni subjekti** (drugi kritični sektorji)

Srednja podjetja (704)
Velika podjetja (219)

OBVETNOSTI ZAVEZANCEV

<u>OBVEZNOSTI BISTVENIH IN POMEMBNIH SUBJEKTOV</u>:

- **izvedba samo-registracije** v aplikaciji pri PNO,
- **obvezno usposabljanje članov poslovodnih organov** na področju obvladovanja tveganj kibernetske varnosti,
- **priprava in vzdrževanje predpisane varnostne dokumentacije**,
- **implementacija (varnostnih) ukrepov** za obvladovanje tveganj za kibernetsko varnost,
- **priglašanje kibernetskih incidentov** pristojnemu CSIRT,
- **uporaba evropskih in mednarodnih standardov** in tehničnih specifikacij (v čim večji meri, **kjer to ne bo obvezno**).

RAZLIKE MED ZAVEZANCI

RAZLIKE PRI BISTVENIH IN POMEMBNIH SUBJEKTIH:

- izvajanje **periodične revizije skladnosti** sprejetih ukrepov in izvajanje **periodične samoocene skladnosti** sprejetih ukrepov (na dve leti),
- **izvajanje nadzora nad zavezanci**: *ex-ante* in *ex-post* nadzori (pogoji in ukrepi inšpektorja),
- **višina predpisanih glob** zaradi kršitve zakona.

GLOBE ZA PREKRŠKE

BISTVENI SUBJEKTI:

- Od **10.000 EUR do 10.000.000 EUR** oziroma od 0,5 % do 2 % skupnega letnega prometa pravne osebe.
- Od **1.000 EUR do 10.000 EUR** za odgovorno osebo pravne osebe.

POMEMBNI SUBJEKTI:

- Od **7.000 EUR do 7.000.000 EUR** oziroma od 0,3 % do 1,4 % skupnega letnega prometa pravne osebe.
- Od **1.000 EUR do 7.000 EUR** za odgovorno osebo pravne osebe.

VARNOSTNA DOKUMENTACIJA

PREDPISANA VARNOSTNA DOKUMENTACIJA ZAVEZANCEV:

1. natančen in posodobljen **popis informacijskih in drugih sredstev ter podatkov**, potrebnih za nemoteno delovanje omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev ter določitev njihovih upravljavcev;
2. **analiza obvladovanja tveganj**, vključno z določitvijo sprejemljive ravni tveganja in opisano uporabljeno metodologijo;
3. **politika in načrt neprekinjenega poslovanja**, vključno z **oceno vpliva na poslovanje**, navedbo postopkov zagotavljanja neprekinjenega poslovanja, določitvijo minimalne ravni poslovanja, upravljanjem varnostnih kopij in določitvijo vlog ter odgovornosti;

VARNOSTNA DOKUMENTACIJA

PREDPISANA VARNOSTNA DOKUMENTACIJA ZAVEZANCEV:

4. **načrt obnovitve in ponovne vzpostavitve delovanja omrežnih in informacijskih sistemov**, ki jih potrebujejo za svoje delovanje ali opravljanje storitev, vključno z opisom odgovornosti in postopkov za obnovitev delovanja teh sistemov po dogodku, ki povzroči prekinitev njihovega delovanja;

5. **načrt odzivanja na incidente** s protokolom obveščanja pristojnega CSIRT, vključno z opisom sistema za zaznavo in odziv na incidente informacijske varnosti ter opisom vlog in odgovornosti za odzivanje na incidente;

VARNOSTNA DOKUMENTACIJA

PREDPISANA VARNOSTNA DOKUMENTACIJA ZAVEZANCEV:

6. **načrt varnostnih ukrepov** za zagotavljanje celovitosti, avtentičnosti, zaupnosti in razpoložljivosti omrežnih in informacijskih sistemov oziroma za obvladovanje tveganj za kibernetsko varnost, ki upošteva in področne posebnosti bistvenega ali pomembnega subjekta.

7. **politika s postopki za oceno učinkovitosti varnostnih ukrepov** za obvladovanje tveganj za informacijsko in kibernetsko varnost, vključno z določitvijo kazalnikov učinkovitosti in izvedeno analizo zbranih podatkov;

MINIMALNI VARNOSTNI UKREPI

UKREPI ZA OBVLADOVANJE KIBERNETSKIH TVEGANJ:

- Zavezanci morajo pri izbiri varnostnih ukrepov **upoštevati najsodobnejše in ustrezne evropske ter mednarodne standarde**.
- Varnostni ukrepi **morajo zagotavljati raven varnosti** omrežnih in informacijskih sistemov, **ki ustreza obstoječim oziroma prepoznanim tveganjem**.
- Zavezanci morajo pri **ocenjevanju sorazmernosti varnostnih ukrepov** ustrezno upoštevati:

- stopnjo izpostavljenosti tveganjem,

- velikost subjekta,

- verjetnost pojava incidentov in

- resnost morebitnih incidentov, vključno z njihovim družbenim in gospodarskim (tudi čezmejnim) vplivom.

MINIMALNI VARNOSTNI UKREPI

UKREPI ZA OBVLADOVANJE KIBERNETSKIH TVEGANJ:
Varnostni ukrepi morajo temeljiti na pristopu **upoštevanja vseh nevarnosti**, in morajo obsegati **najmanj**:

1. **podporo vodstva subjekta** pri zagotavljanju informacijske in kibernetske varnosti in vključitvijo področja informacijske in kibernetske varnosti v letni načrt poslovanja oziroma letni program dela;
2. **zagotavljanje integritete kadrov** v povezavi z informacijsko varnostjo pred zaposlitvijo, med zaposlitvijo in ob prenehanju ali spremembi zaposlitve;
3. ***osnovne prakse kibernetske higiene in usposabljanje*** na področju informacijske in kibernetske varnosti;

MINIMALNI VARNOSTNI UKREPI

<u>UKREPI ZA OBVLADOVANJE KIBERNETSKIH TVEGANJ</u>:

4. **varnost človeških virov**, preverjanje identitete uporabnikov, zagotavljanje ravni dostopnosti informacij in upravljanje pooblastil za dostop;
5. **izvajanje in upravljanje varnostnih kopij podatkov**;
6. **zagotavljanje in ohranjanje dnevniških zapisov** o delovanju omrežnih in informacijskih sistemov;
7. **upravljanje omrežnih in informacijskih sistemov**, ki jih uporabljajo za svoje delovanje ali opravljanje storitev z **določitvijo odgovornosti za njihovo zaščito**;
*8. politike in postopke v zvezi z **uporabo kriptografije** in po potrebi s šifriranjem*;

MINIMALNI VARNOSTNI UKREPI

<u>UKREPI ZA OBVLADOVANJE KIBERNETSKIH TVEGANJ</u>:

9. **upravljanje prometa in komunikacij**;

*10. **varnost dobavne verige** z določitvijo ustreznih minimalnih zahtev povezanih s kibernetsko varnostjo za ključne dobavitelje ali ponudnike storitev*;

11. **fizično in tehnično varovanje** prostorov in dostopov do prostorov, kjer so ključni deli omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev;

12. **varnostne mehanizme v aplikativni programski opremi** za izvajanje dejavnosti, vključno z varnostjo pri pridobivanju, razvoju in vzdrževanju omrežnih in informacijskih sistemov ter ***obravnavanjem in razkrivanjem ranljivosti;***

MINIMALNI VARNOSTNI UKREPI

<u>UKREPI ZA OBVLADOVANJE KIBERNETSKIH TVEGANJ</u>:

13. **upravljanje in preprečevanje izrab tehničnih ranljivosti**;

14. **zaščito pred zlonamerno programsko kodo, zaznavanje poskusov vdorov in preprečevanje incidentov**;

*15. **uporabo večfaktorske avtentikacije** ali rešitev neprekinjene avtentikacije, kadar je to potrebno zaradi obvladovanja tveganj za kibernetsko varnost* in;

*16. **uporabo varovanih glasovnih, video in besedilnih komunikacij in varnih sistemov za komunikacije v sili znotraj subjekta,** kadar je glede na dejavnost subjekta to primerno*.

VARNOST DOBAVNE VERIGE

UKREPI ZA VARNOST DOBAVNE VERIGE:

- Zavezanci morajo pri oceni in izvedbi ustreznih varnostnih ukrepov za varnost dobavne verige **upoštevati ranljivosti, ki so specifične za posameznega neposrednega dobavitelja in ponudnika storitev ter splošno kakovost proizvodov ter praks svojih dobaviteljev in ponudnikov storitev** na področju kibernetske varnosti, vključno z njihovimi varnimi razvojnimi postopki.
- Zavezanci **morajo ugotavljati, kateri varnostni ukrepi so ustrezni in primerni za zagotovitev varnosti dobavne verige ter lahko preverjajo njihovo izvajanje pri dobaviteljih in ponudnikih storitev**. Pri tem upoštevajo rezultate morebitnih usklajenih ocen tveganja za kritične dobavne verige, ki jih pripravi Skupina za sodelovanje v sodelovanju z Evropsko komisijo in ENISA.

OBVEZNOST POROČANJA O INCIDENTIH

Bistveni in pomembni subjekti imajo dolžnost poročanja pristojnemu CSIRT, brez nepotrebnega odlašanja (najkasneje pa v 24 urah), o vseh incidentih, ki pomembno vplivajo na zagotavljanje njihovih storitev.
Incident se šteje kot **pomemben**, če:

- je subjektu **povzročil ali bi mu lahko povzročil** znatne operativne motnje pri opravljanju storitev ali finančne izgube ali
- je **vplival ali bi lahko vplival na druge fizične ali pravne osebe** s povzročitvijo precejšnje premoženjske ali nepremoženjske škode.

Bistveni in pomembni subjekti upoštevajo tudi **izdane izvedbene akte Komisije**, s katerimi ta podrobneje določi vrsto informacij, obliko in postopek priglasitve, in obvestila ter določene posebne primere, ko se incident šteje za pomembnega.

ODGOVORNOST PRI PRAVNIH OSEBAH

- **Odgovorna oseba pravne osebe je odgovorna za prekršek**, ki ga izvrši z opustitvijo dejanja, ki ga je bila dolžna storiti, da se prekršek prepreči (***opustitev***).
- **Odgovornost pravne osebe je pridružitvena** (akcesorna), kar izhaja iz dejstva, da pravna oseba odgovarja za prekršek, ki ga izvrši (neposredni) storilec.
- **Kadar ni mogoče ugotoviti neposrednega storilca prekrška**, **je dokazno breme** glede ugotovitve (druge) osebe, pooblaščene za določeno dejanje, **na poslovodstvu pravne osebe**.

ODGOVORNOST PRI PRAVNIH OSEBAH

- **Odgovorna oseba (pravne osebe)** je tista oseba, ki je pooblaščena opravljati delo v imenu, na račun, v korist ali s sredstvi pravne osebe.
- Kadar **poslovodstvo ne imenuje neposredno odgovorne osebe** (neposrednega storilca), **je odgovorna oseba v pravni osebi tista oseba**, ki je pooblaščena za izvajanje dolžnega nadzorstva.
- Šteje se, da je **za izvajanje dolžnega nadzorstva pooblaščen vodstveni organ**, za dolžno nadzorstvo nad vodstvenim organom pa nadzorni organ, razen, če je bila odgovornost za izvajanje dolžnega nadzorstva s pravnim aktom prenesena na drugo osebo ali organ.

UGOTOVITVE IZ INŠPEKCIJSKIH NADZOROV

NEKATERE UGOTOVITVE IZ INŠPEKCIJSKIH NADZOROV ZAVEZANCEV - IZVAJALCEV BISTVENIH STORITEV:

- Zavezanci **nimajo izvedenega ustreznega popisa sredstev** (če pa že, pa so to samo parcialne rešitve, samo za ozke segmente poslovanja, za katere se izkazuje, da niso povezani z izvajanjem bistvenih storitev).
- Zavezanci **nimajo (ali imajo samo delno) izvedenih popisov poslovnih procesov**, posledično **ni izvedene BIA analize**.
- Odgovorne osebe za neprekinjeno poslovanje so sicer prepoznane, **niso pa ti ključni kadri prepoznani v podpornih procesih** (ni zagotovljene dosegljivosti potrebnega ključnega kadra izven delovnega časa).
- **Ni določene minimalne ravni poslovanja**.
- Zavezanci **ne izvajajo rednega izobraževanja zaposlenih** na področju informacijske varnosti in **ne zagotavljajo zadostnega usposabljanja in izpopolnjevanja za ključen IT kader**.

UGOTOVITVE IZ INŠPEKCIJSKIH NADZOROV

NEKATERE UGOTOVITVE IZ INŠPEKCIJSKIH NADZOROV ZAVEZANCEV - IZVAJALCEV BISTVENIH STORITEV :

- **Upravljanje in preprečevanje izrab tehničnih ranljivosti je zelo oteženo,** ker ni ustrezno izvedenega in redno ažuriranega popisa sredstev je (odziv je šele na obvestila SI-CERT ali na obvestila zunanjih ponudnikov storitev, če ti sploh obveščajo).
- Velika večina zavezancev za IT področje najema zunanje ponudnike storitev, **varnostnih zahtev za ključne dobavitelje pa nimajo opredeljenih v internih aktih niti vključenih v pogodbe.**
- Zavezanci **nimajo potrebnega kadra/znanja za izvajanja dolžnega nadzorstva** nad izvajanjem storitev zunanjih ponudnikov (ni mogoče obvladovanje tveganj dobavne verige).
- Zavezanec ni predpisal in izvajal **testov postopkov upravljanja izrednih dogodkov**, ki imajo negativen vpliv na izvajanje bistvenih storitev.

ZAKLJUČEK

NAMESTO ZAKLJUČKA:

- Odgovorne osebe pravnih oseb oziroma **člani poslovodnih organov** bistvenih ali pomembnih subjektov **so odgovorni za uvedbo in izvajanje** (varnostnih) **ukrepov** za obvladovanje tveganj informacijske/kibernetske varnosti.

- Bistveni in pomembni subjekti (**člani poslovodnih organov**) **so odgovorni za informacijsko varnost** in skladnost s predpisi tudi v primeru, ko **izvajanje informacijskih storitev najemajo pri zunanjem ponudniku storitev**.

VPRAŠANJA?

REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE ZA INFORMACIJSKO VARNOST

URSIV

matjaz.mravljak@gov.si

gp.uiv@gov.si
www.uiv.gov.si
Twitter: @URSIV_Slovenia

URSIV

zit SeKV

Združenje za informatiko in telekomunikacije
Kibernetska varnost

KIBERNETSKI CUNAMI

Ali smo pripravljeni na spremembe ZInfV?

KIBERNETSKI CUNAMI

Ali smo pripravljeni na spremembe ZInfV?

Krepitev varnosti v industriji in kritični infrastrukturi z direktivo NIS 2

Boris Krajnc

certificiran etični heker in specialit za kibernetsko varnost, Telekom Slovenije d.d.

Krepitev varnosti v industriji in kritični infrastrukturi z direktivo NIS 2

Boris Krajnc, Telekom Slovenije, d.d.

Boris KRAJNC

Strokovnjak za kibernetsko varnost

TelekomSlovenije

Trend

Home > Resources > Blog Oct 11, 2024 16 Mins Read

Biggest Manufacturing Industry Attacks 2024

In 2024, the manufacturing sector will become a primary target for cyber attacks. According to data from the National Institute of Standards and Technology (NIST), the average cost of a data breach in this industry for small businesses has reached $105,000, and it takes an average of 277 days to identify and contain such incidents. Furthermore, **1 out of 5 breaches is caused by supply chain compromise**.

VIR: https://socradar.io/

Razlika med IT in OT?

Razlika me IT in OT

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IT

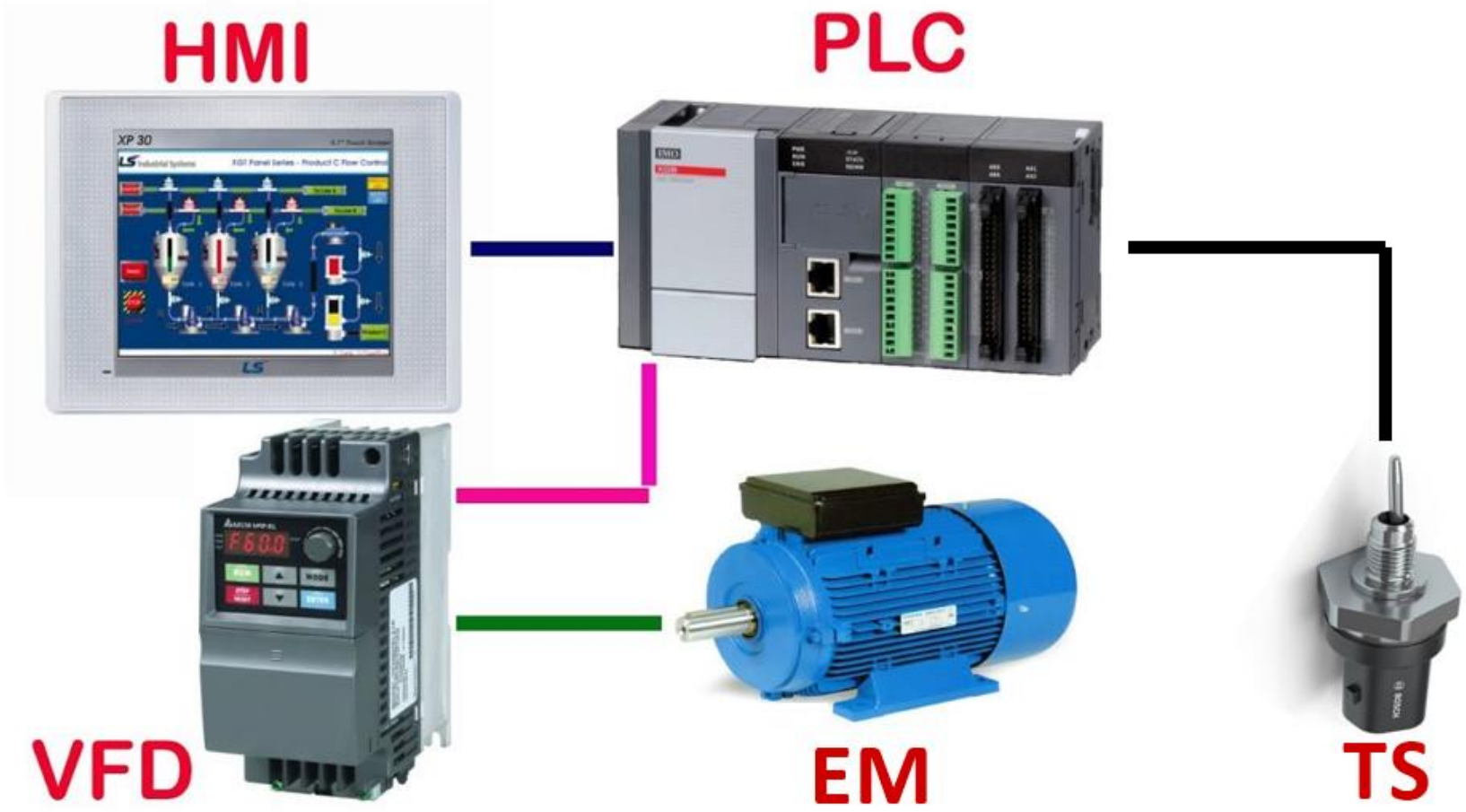
VARUJEMO PODATKE

OT

VARUJEMO PROCESE

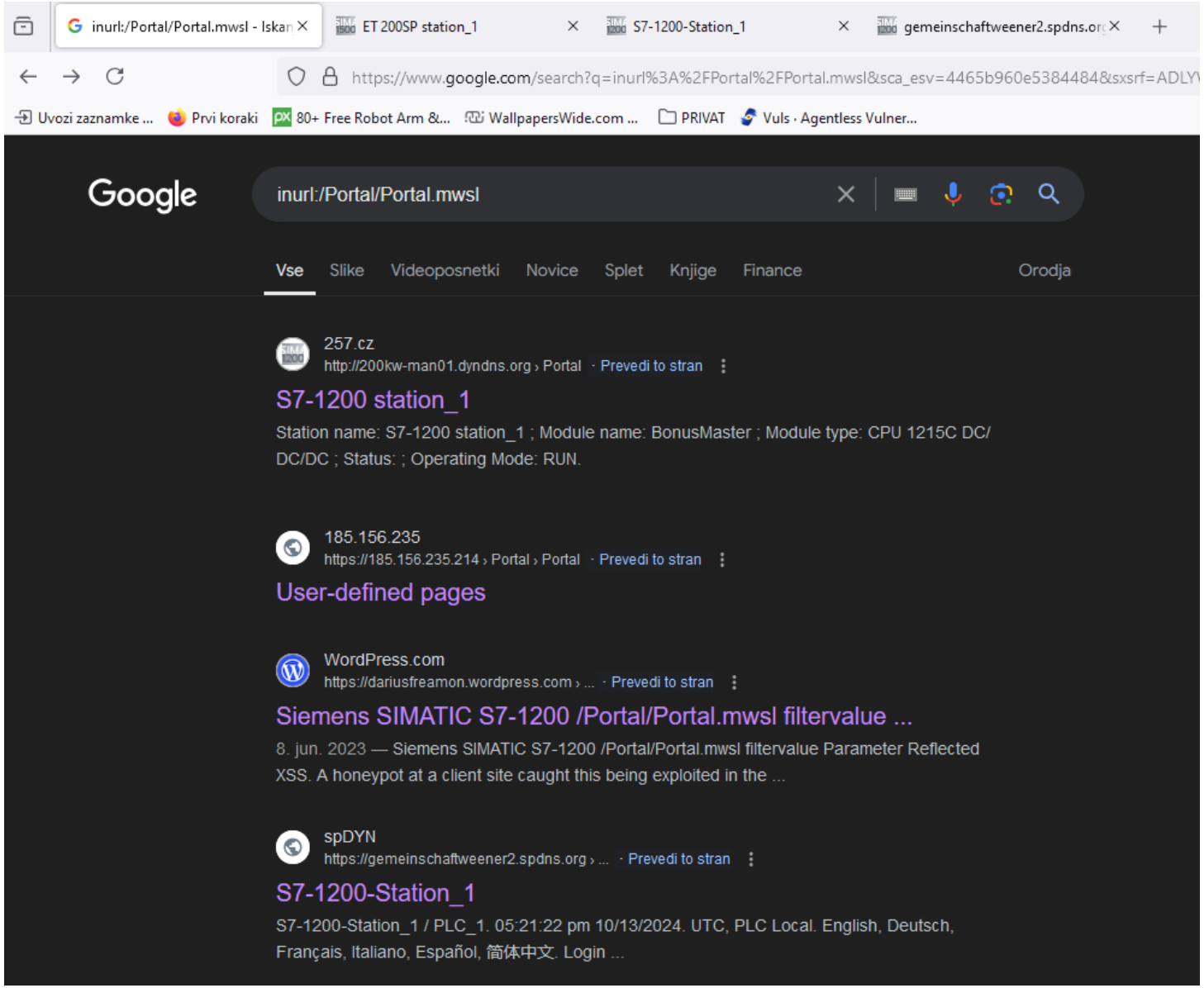
TelekomSlovenije

ODDALJENO krmiljenje v okolju OT



TelekomSlovenije

Dokler bo kot na „divjem zahodu“ .....



TelekomSlovenije

Dokler bo kot na „divjem zahodu“ …..

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

https://ge[redacted]/Portal/Portal.mwsl?PriNav=Start

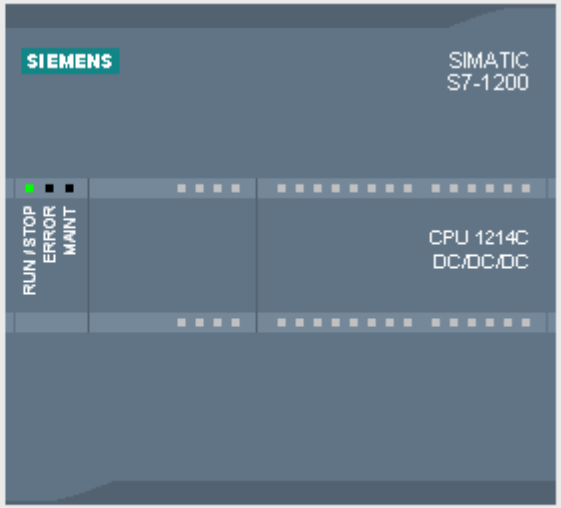
Uvozi zaznamke … | Prvi koraki | 80+ Free Robot Arm &… | WallpapersWide.com … | PRIVAT | Vuls · Agentless Vulner…

SIEMENS **S7-1200-Station_1 / PLC_1**

Username
Login

S7-1200-Station_1

- **Start Page**
- User-defined pages
- Introduction



General:

Project Name:	Haussteuerung V1.5_V16_FW4.4.1
TIA Portal:	V16
Station name:	S7-1200-Station_1
Module name:	PLC_1
Module type:	CPU 1214C DC/DC/DC

Status:

Operating Mode:	RUN
Status:	✓ OK

TelekomSlovenije

NIS2 Directive

TelekomSlovenije

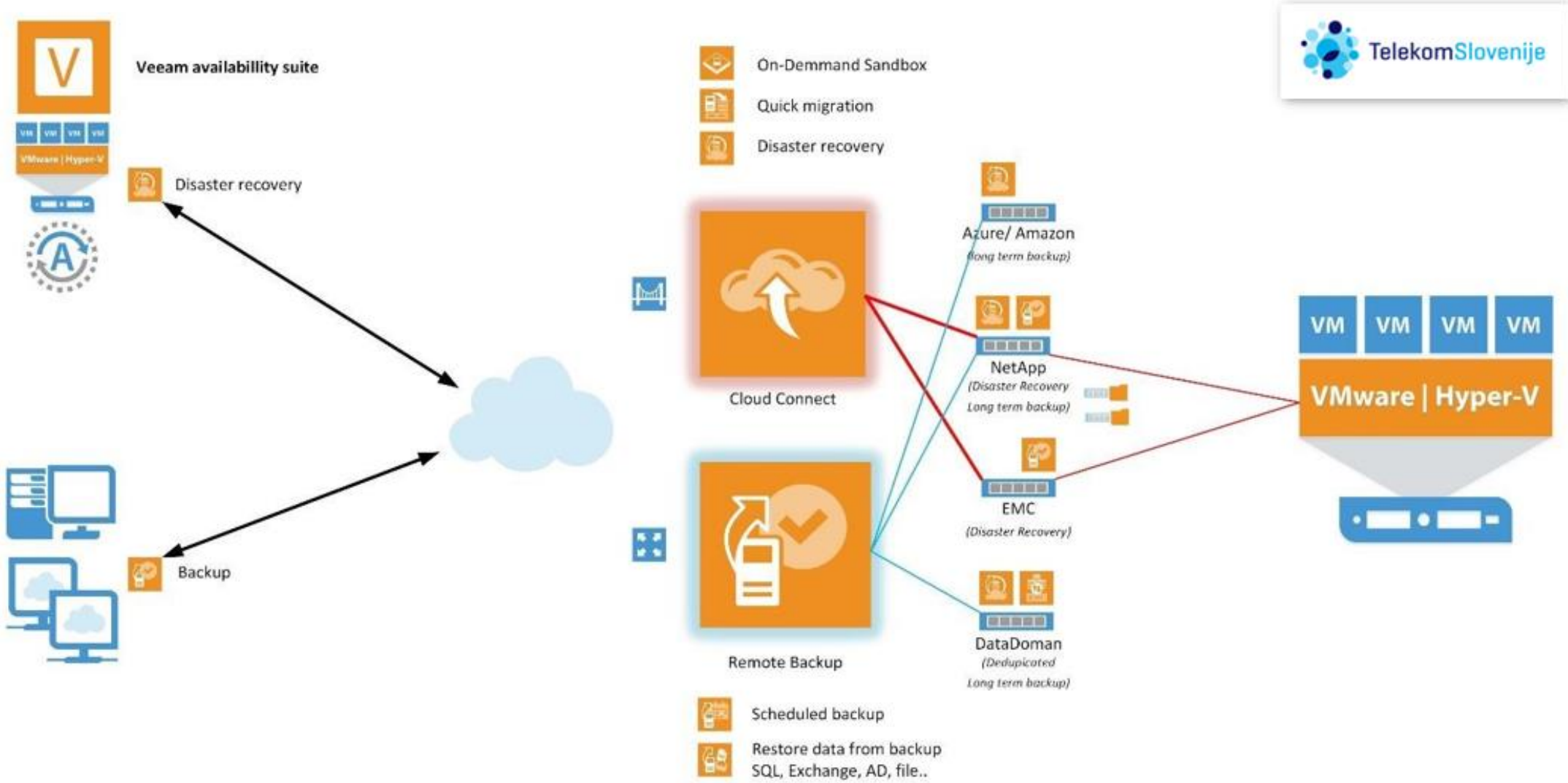
NIS2 – kaj je cilj direktive

- Izboljšana varnostna infrastruktura za IT in OT
- Uvajanje celovitih varnostnih standardov
- Boljša vidljivost in nadzor nad sistemskimi grožnjami
- **Povečana odpornost na kibernetske napade**

10 TOČK – NIS2

- Analiza tveganja in varnost informacijskih sistemov
- Obravnava incidentov
- Ukrepi za neprekinjeno poslovanje, kot sta varnostno kopiranje in obnova po nesreči
- Varnost dobavne verige
- Varnost sistemov in omrežij, vključno z upravljanjem ranljivosti
- Pravila in postopki za upravljanje in analizo tveganja
- Osnovna higiena kibernetske varnosti in usposabljanje zaposlenih
- Politika kriptografije in šifriranja
- Varnost človeških virov, kot so politike nadzora dostopa
- Več faktorsko preverjanje in varna komunikacija

BACKUP – 3 -2 (Telekom) - 1

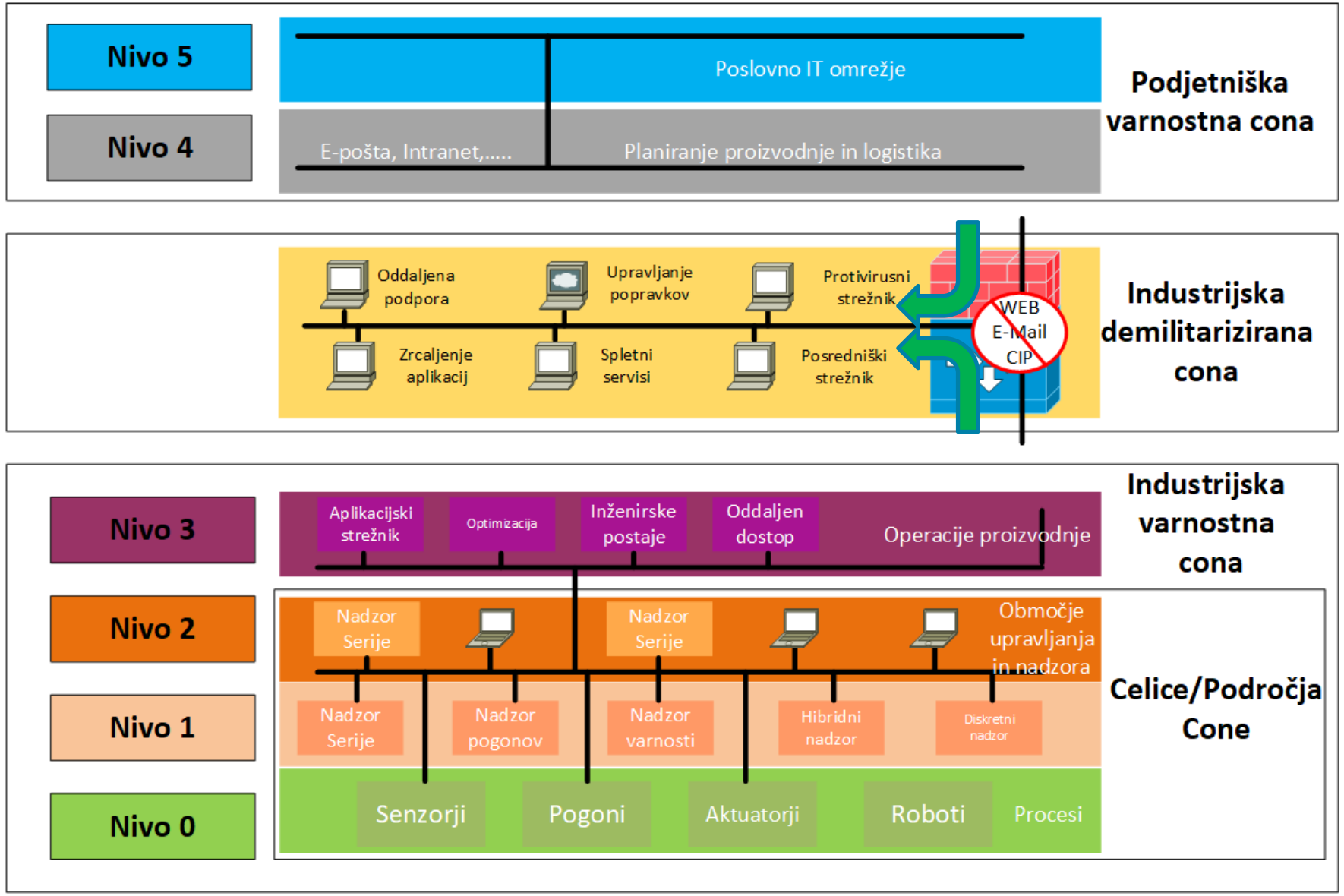


Pravilna arhitektura omrežja in razmejitev IT - OT

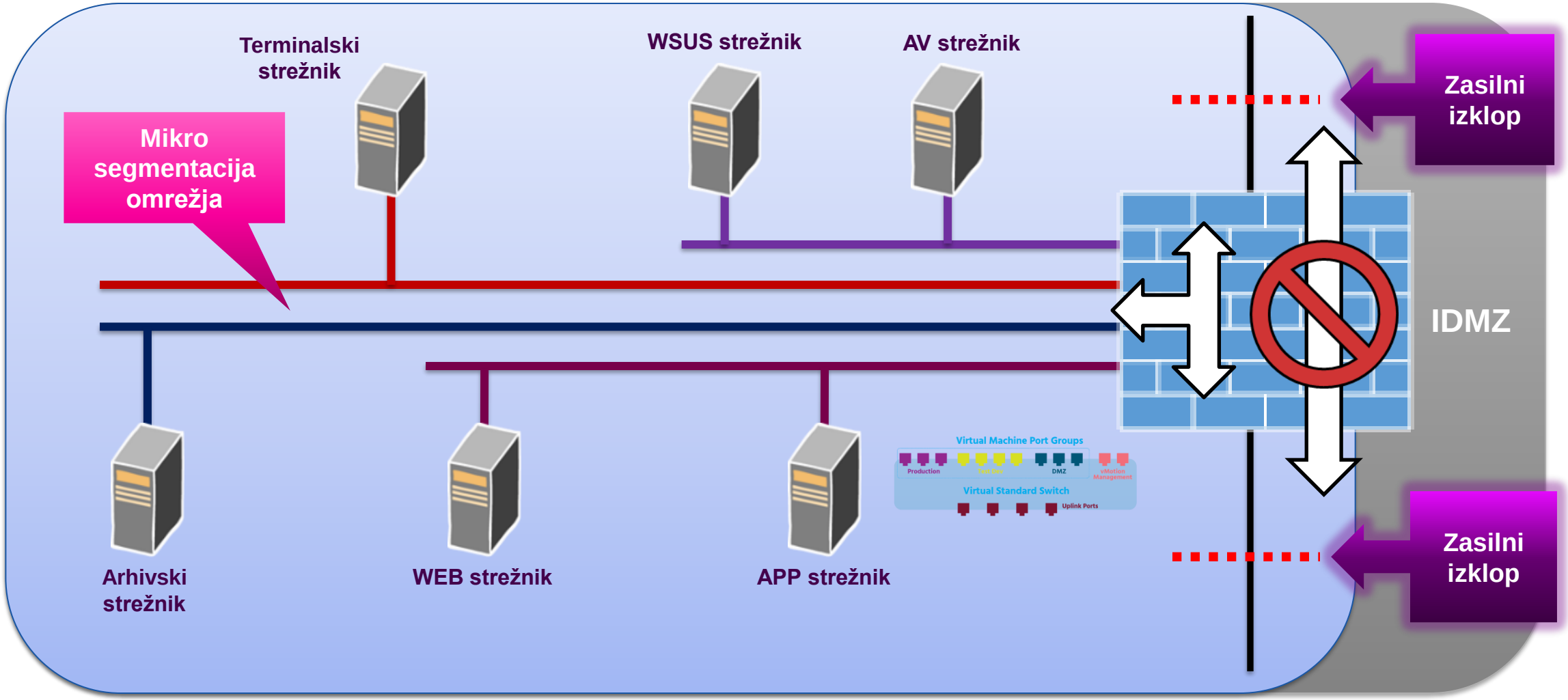
TelekomSlovenije

Referenčni model za okolja OT, ki ustreza NIS 2 zahtevam

„Purdue“ kot referenčni model



IDMZ – logični pogled



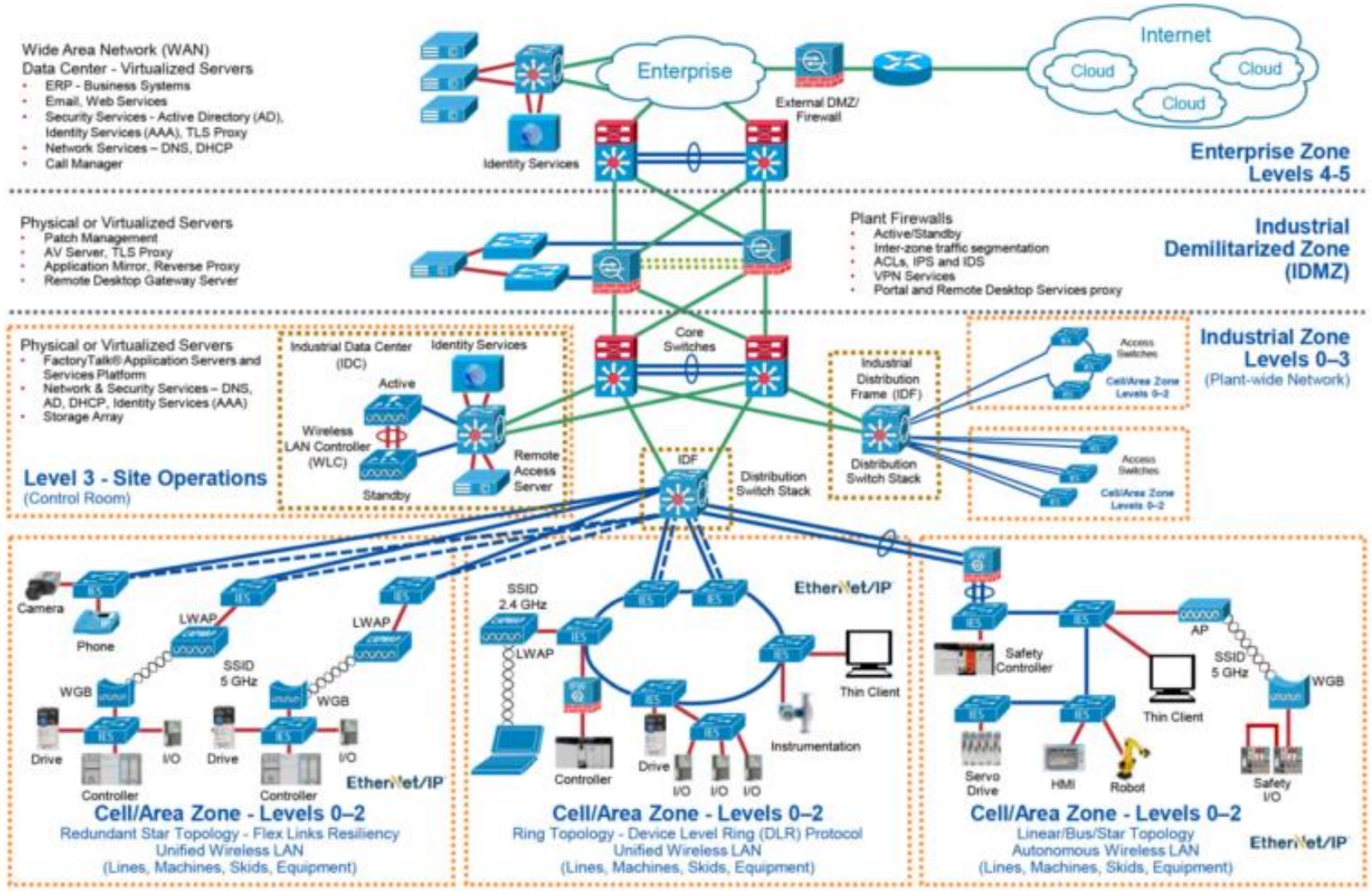
Komunikacija v „Purdue“ modelu

Rockwell Automation · cisco · zit SeKV

Združenje za informatiko in telekomunikacije
Kibernetska varnost

IT

OT



https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf

TelekomSlovenije

Pet dnevno izobraževanje: Kibernetska varnost v okoljih OT

TelekomSlovenije

Ozaveščanje in izobraževanja - NIS2

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Vsebina izobraževanja:

- poznavanje osnovnih načel za načrtovanje in izgradnjo varnih omrežij v okoljih IT in OT
- poznavanje naprav in njihovih pomanjkljivosti v okoljih operativne tehnologije
- poznavanje protokolov, ki so del okolja OT
- poznavanje in prepoznavanje hekerskih metod ter orodij
- razumevanje modela »purdue« in posameznih nivojev
- varovanje okolij operativne tehnologije

Komu je namenjeno:

- IT-ekipe, ki sodelujejo z vzdrževalci okolij OT (vzdrževalci omrežij, CISO, CIO, CTO, varnostni inženir)
- skrbniki procesnih sistemov (SCADA)
- inženirji procesne tehnike
- skrbniki centrov vodenja
- procesni inženirji
- vodje telekomunikacij
- vodje služb za nadzorne sisteme
- vodje služb za obratovanje in vzdrževanje
- vsi, ki so željni znanja in razumevanja varnosti na področju proizvodnje in kritične infrastrukture

Vidljivost in nadzor nad grožnjami

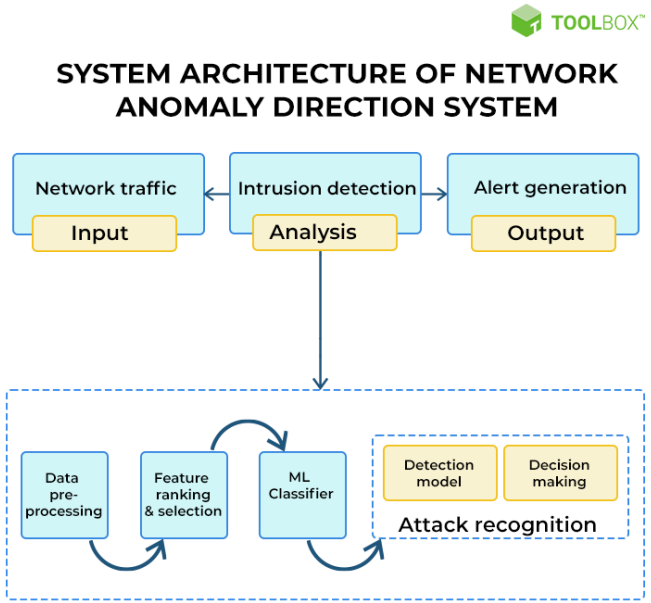
TelekomSlovenije

Uporaba umetne inteligence - UI

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

V industrijskih okoljih se UI lahko uporablja za:

- **Varovanje pred kibernetskimi grožnjami:**
- *Sistemi umetne inteligence lahko analizirajo promet in podatke v realnem času, prepoznavajo neobičajne vzorce in napade ter zagotavljajo proaktivno zaščito pred kibernetskimi grožnjami (Vidljivost OT okolja)*
- **Napredno vzdrževanje**
- **Avtomatizacija proizvodnje**
- **Kakovost nadzora / napredno analitično vzorčenje**



NOZOMI NETWORKS

FORTINET®

TelekomSlovenije

Nozomi Networks in NIS2

NOZOMI NETWORKS

- Risk analysis and information systems security policies
- Incident handling (prevention, detection, and response)
- Business continuity and crisis management
- Supply chain security
- Security in network and information systems
- Policies and procedures for cybersecurity risk management measures
- The use of cryptography and encryption

TelekomSlovenije

CKVO – Telekom Slovenije (SOC)

Center Kibernetske Varnosti in Odpornosti

TelekomSlovenije

CKVO (SOC)

LASTEN SOC (1000 naprav):
Trije (3) strokovnjaki za področje kibernetske varnosti - ANALITIKI

Strošek:
3 x 4.500€ BRUTO
SKUPAJ: 13.500€ /mesec
2 NE smeta hkrati na bolniško

VS

CKVO Telekom Slovenije(1000 naprav):
Petindvajset (25) strokovnjakov za področje kib. varnosti – Analitik -1. nivo
100 strokovnjakov – SPECIALISTOV za posamezna poodročja Alanlitik 2.nivo

Strošek:
1000 x 5 do 6€/naprava*
SKUPAJ: 5500€/mesec

* Cena se določi na podlagi dogovora, ponudnik – naročnik in je odvisna od več dejavnikov!

Operativni center kibernetske varnosti Telekoma Slovenije - CKVO

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

OT

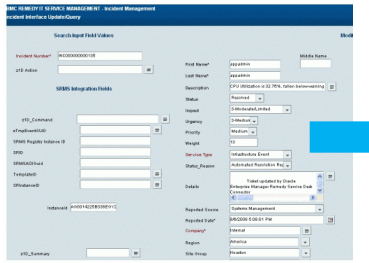
cynet
NOZOMI NETWORKS
Defender
IT
Active Directory
vmware
SEC tools

Varnostni dogodki

SOAR
Avtomatizacija

SIEM
Varnostni prestopki

Raven 1
TRIAŽA



TICKETING
Storitveno središče

Raven 2 **CSIRT**

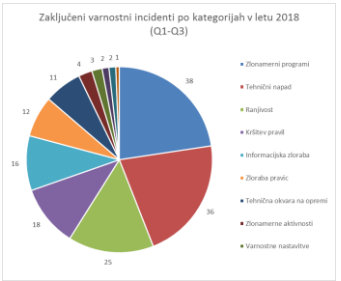
Eskalacija
Varnostni incident

- Sistemski inženir, admin
- Naročnik / Partner

CYBER THREAT INTELL - CTI

Obogatenje informacij (CERT)
- IBM X-force
- Trusted Introducer – Threat Intell.
- CERT, drugi CSOCi,
- DDoS in prometne analize

DASHBOARD



Nadzorna plošča in Poročanje

TelekomSlovenije

Zakaj CKVO Telekoma Slovenij (SOC)?

Združenje za informatiko in telekomunikacije
Kibernetska varnost

„Kibernetska varnostna služba“

- Ker **so tveganja** za nedelovanje podjetja zaradi kibernetskih
- Ker samo s tehnološkimi rešitvami **ne moremo preprečiti** v
- Ker so hekerji vztrajni in **neprenehoma poskušajo** na najla
- Ker je potrebno **neprestano spremljati** množico signalov, a
- Ker sistemski inženirji niso v vlogi varnostnih analitikov

Ker podjetja težko vzpostavijo lasten SOC, je rešitev **zunanje izv**

TelekomSlovenije

Vprašanja ?

TelekomSlovenije

HVALA

boris.krajnc@telekom.si

Telekom Slovenije, d.d.
Cigaletova 15
1000 Ljubljana

www.telekom.si
E: info@telekom.si

Sledite nam:

TelekomSlovenije

KIBERNETSKI CUNAMI

Ali smo pripravljeni na spremembe ZInfV?

KIBERNETSKI CUNAMI

Ali smo pripravljeni na spremembe ZInfV?

Nove tehnologije in trendi na področju kibernetske varnosti v svetu

Peter Novak

Vodja področja Cybersecurity rešitev, Microsoft

Microsoft Security

Microsoft Security

Secure your future with the AI-first end-to-end security platform.

Peter Novak
18.10.2024

zit SeKV

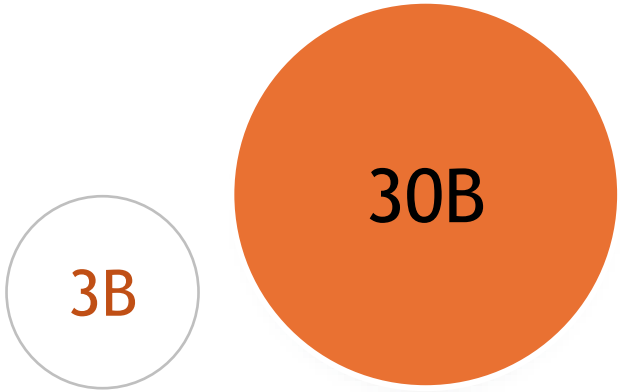
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Cyber threats have grown 10X

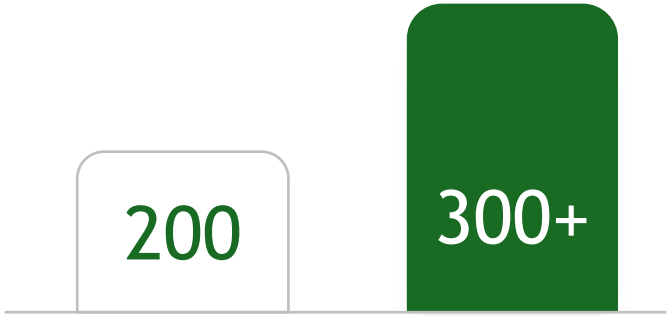
Median time for an attacker to access private data from phishing

1h 12mins

Password attacks per month



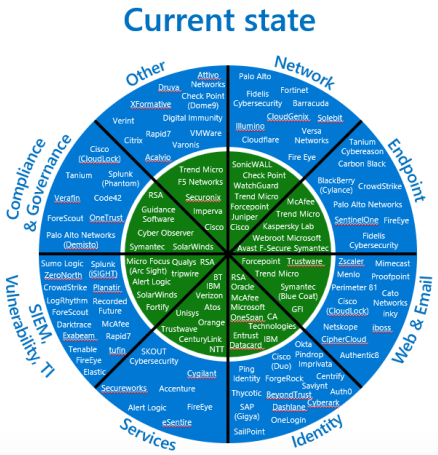
Threat actors tracked by Microsoft



SPEED | SCALE | SOPHISTICATION

Source: Microsoft Digital Defense Report

Cyber jobs feel 10X harder



Organizations use an average of 80 security tools

Source: Microsoft

Open jobs worldwide

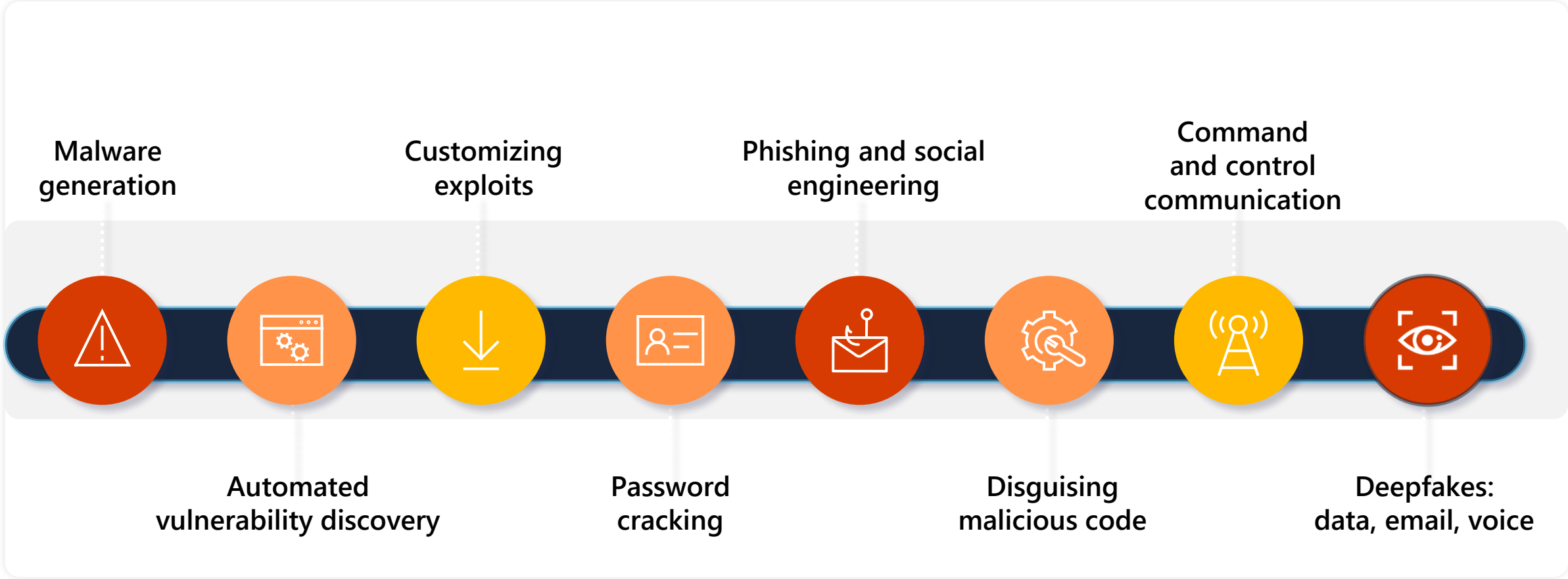
Source: ISC2

250

New regulatory updates tracked every day

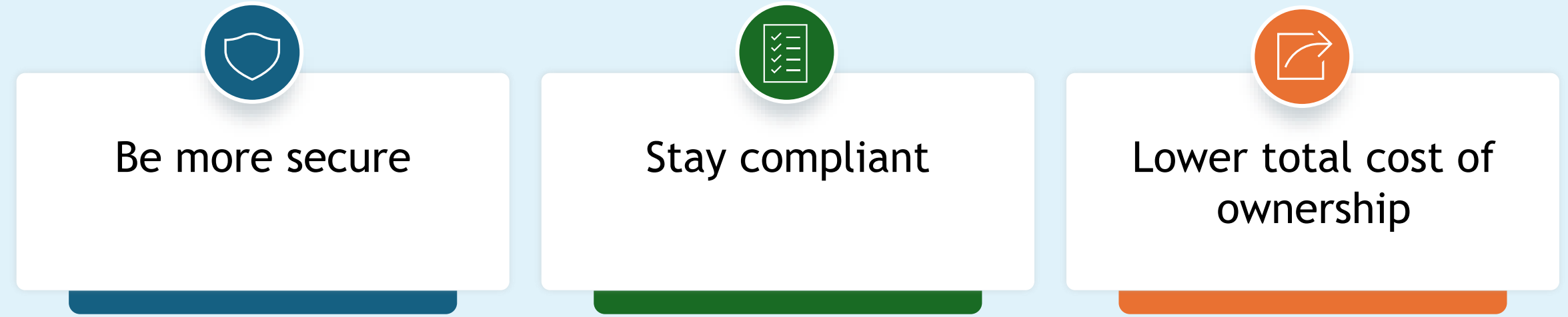
Source: IDC

And now attackers are leveraging AI



Security teams need better outcomes

Microsoft teams need the same



…in the age of generative AI

For Microsoft, security is job 1

> *…prioritizing security above all else is critical to our company's future"*

Satya Nadella
Chairman and CEO

2 Outcomes

A More Resilient and Transparent Microsoft

Advanced Security Tools

3 Principles of Microsoft's Secure Future Initiative

Secure by Design

Security comes first when designing any product or service

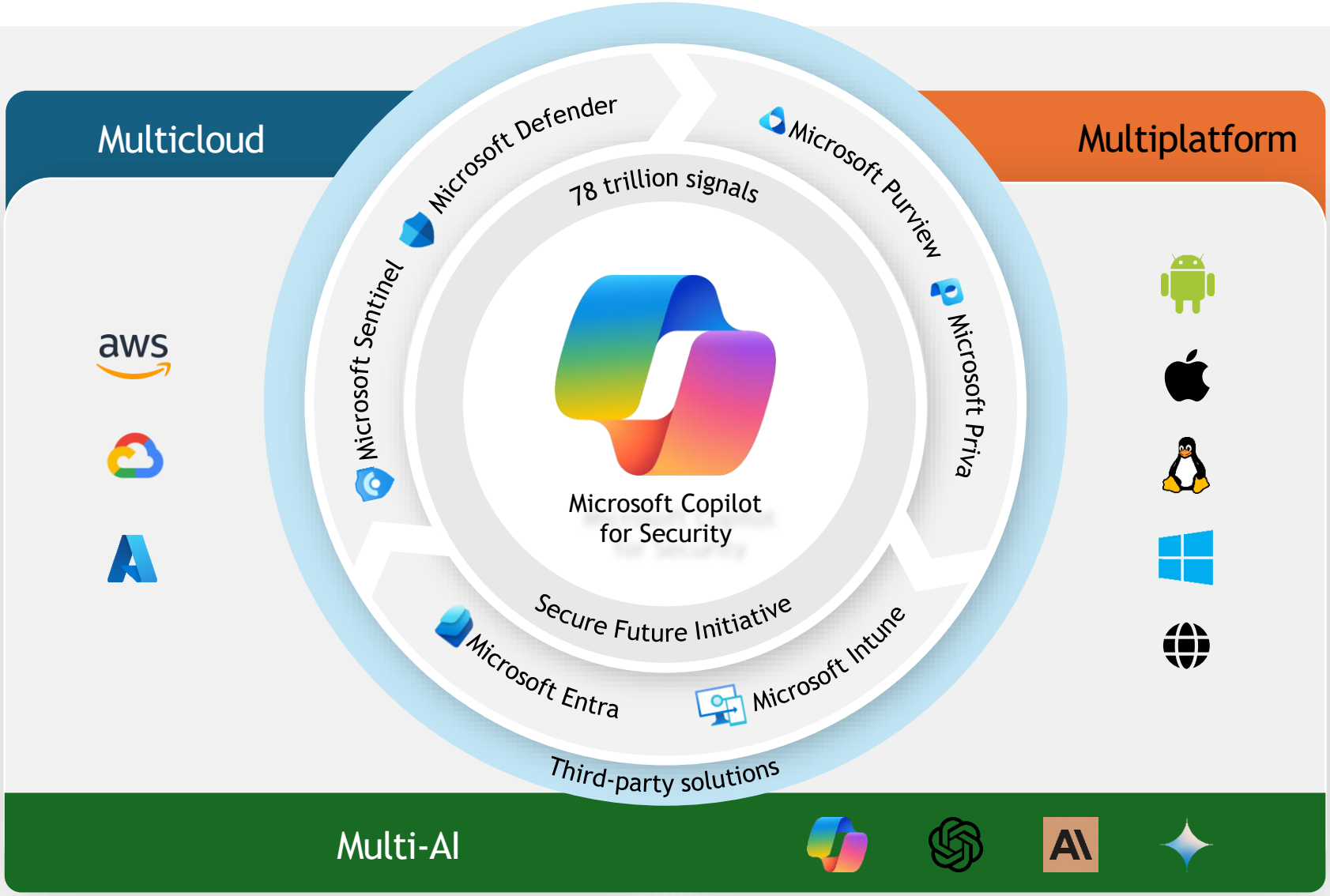
Secure by Default

Security protections are enabled and enforced by default, require no extra effort, and are not optional

Secure Operations

Security controls and monitoring will continuously be improved to meet current and future threats

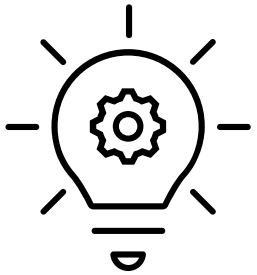
AI-first end-to-end security for the age of AI



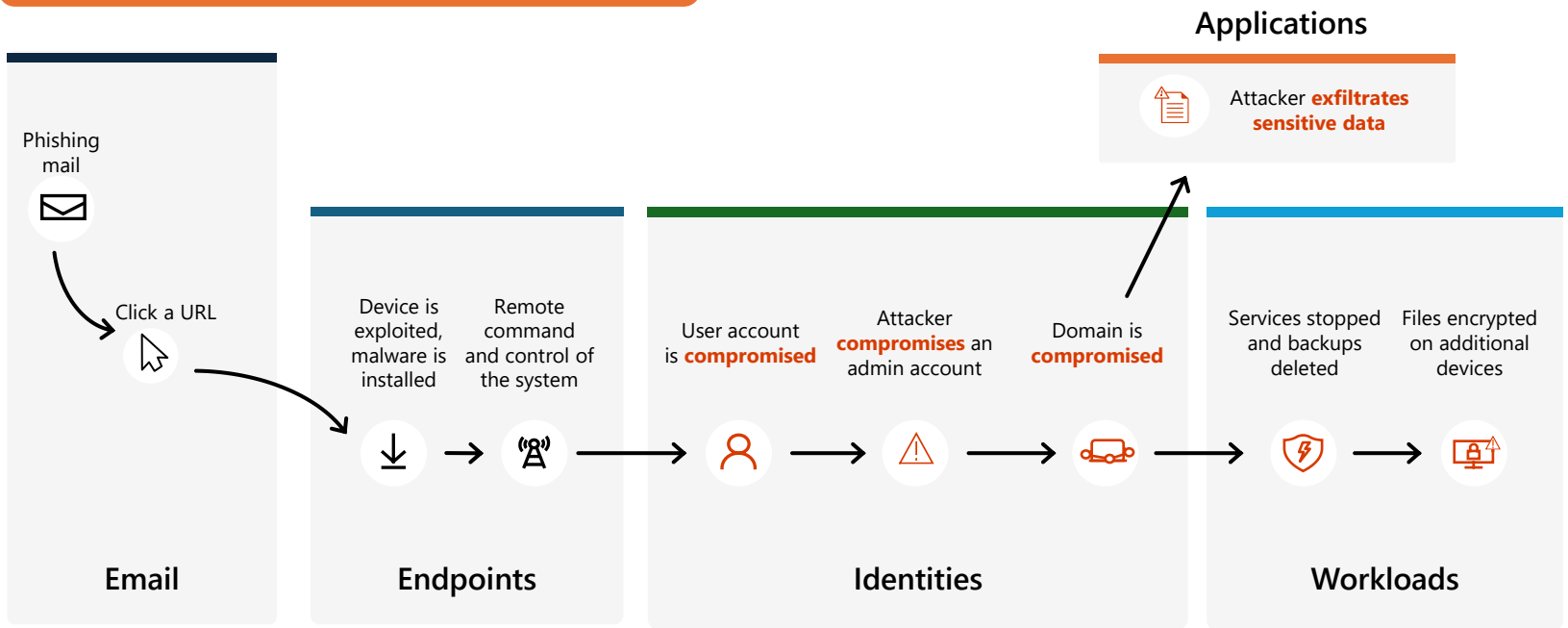
End-to-end threat intelligence and protection all in one

For keeping the lights on

- Identity management
- Device management
- Compliance management
- AI governance



And for when things go wrong



Smarter and faster tools for effective detection, response, and remediation

Our AI-first end-to-end platform can help you

Be more secure

Stay compliant

Lower total cost of ownership

Built by defenders for defenders, for defense at AI speed

Be more secure

Protect all your apps, data, endpoints, identities, infrastructure, and AI solutions.

Unmatched threat intelligence and best-in-class security tools designed for multicloud and multiplatform environments.

50+
product categories united and protected

78T
Signals synthesized per day integrated into security solutions

72%
reduced likelihood of a breach*

88%
reduced time to respond to threats*

35%
increase in accuracy for security novices when using Copilot for Security

300+
Pre-built classifiers to identify sensitive data processed by GenAI apps and AI interactions

Responding to the world's largest cyber attacks since 2008

*Source: Forrester

Stay compliant

Secure and govern your organization's data across your entire digital estate.

Accelerate the secure adoption of AI with ready-to-go data security and governance tools purpose-built for generative AI.

90+

Global certifications and attestations, including GDPR, ISO 27001, and SOC 1/2/3

400+

GenAI app risk assessments ready for use by your team

320+

Ready-to-use and customizable regulatory assessment templates to meet multicloud compliance requirements

99.9%

Uptime commitment for Microsoft 365 ensures continuous compliance management

Supports AI compliance with the EU AI Act, NIST AI Risk Management Framework, ISO 42001, ISO 23894, code-of-conduct policies, and more

Discover, protect, and govern the use of generative AI for Copilot, ChatGPT, Claude, Gemini, private LLMs, and more

Lower total cost of ownership

Simplify your security operations with seamlessly integrated end-to-end protection that consolidates fragmented tools, offering more cost savings and higher productivity.

60%
Cost savings

231%
Return on investment*

26%
Time saved by security novices when using Copilot for Security

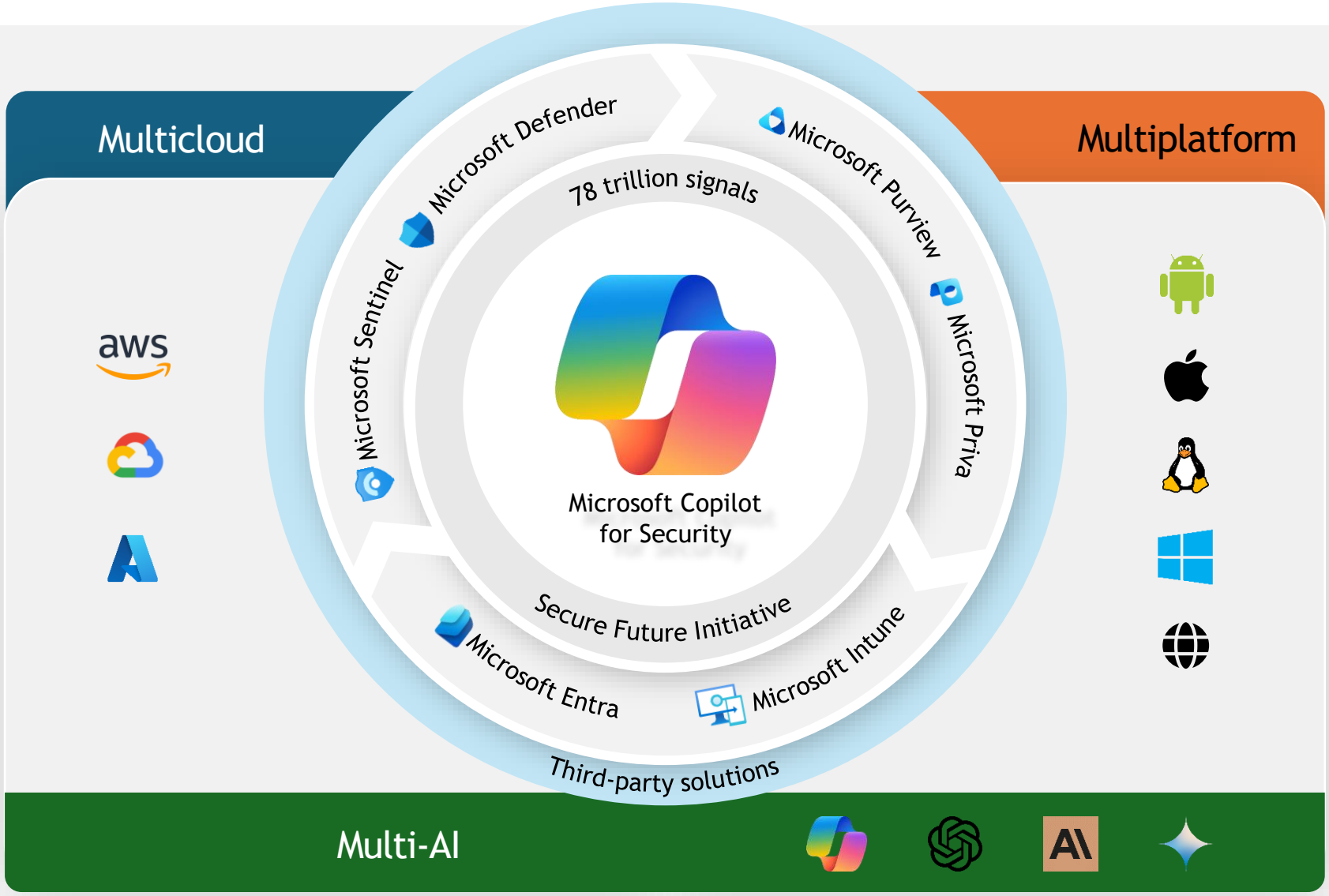
22%
Time saved by experienced security professionals when using Copilot for Security

$20B
Research & development investment

10,000
Security and threat intelligence experts working for you

*Source: Forrester

Microsoft Security can help you achieve more



Protect comprehensively with unmatched threat intelligence, best-in-breed protection, and generative AI

Do more for less by integrating 50+ categories and delivering 60% cost savings

Supercharge your talent by using GenAI to help you defend at machine speed

Safeguard your AI future by securing the development and adoption of AI solutions

Our goal is to help you secure your future

Explore what's possible with our experts

Get the latest threat intelligence at Microsoft Security Insider

Learn more about our platform

Link za prenos: Pročilo o digitalni obrambi Microsoft 2024

Hvala!

KIBERNETSKI CUNAMI

Ali smo pripravljeni na spremembe ZInfV?

KIBERNETSKI CUNAMI

Ali smo pripravljeni na spremembe ZInfV?

Sodobno digitalno okolje po uveljavitvi NIS 2 direktive – kako se pripraviti?

Uroš Majcen

direktor kibernetske odpornosti, Kontron SI d.o.o.

kontron

zit SeKV

Združenje za informatiko in telekomunikacije
Kibernetska varnost

Sodobno digitalno okolje po uveljavitvi NIS 2 direktive – kako se pripraviti?

Uroš Majcen

Izzivi ki čakajo organizacije 2024/2025

Skladnost ali zaščita?

- Organizacije bodo prisiljene spremeniti “mind set” glede kibernetske varnosti
- Dodatni stroški morebitnih novih tehničnih rešitev
- Prevzgoja zaposleni in IT ekipe
- Zagotavljanje skladnosti – časovno okno

Kako se pripraviti?

- 1. Zavedanje in odgovornosti poslovodstva
  - Razumevanje → čas, sredstva, znanje
- 2. Zagon procesa zagotavljanja skladnosti
  - Ne gre za “projekt” ali “big bang”, ampak gre za pot → glej 1
- 3. Izhodiščno stanje:
  - Če nimamo ničesar: “ura je vojgi”, bi rekli po kozjansko.
    - Zelo velik, ne pa nepremagljiv izziv
  - Če imamo določene zadeve:
    - Velik izziv, časovno in človeško obvladljiv
  - Če imamo ISO standarde: smo na dobri poti
    - Posodobitve, pregledi in dopolnitve

Izzivi ki čakajo organizacije 2024/2025

kontron

Skladnost ali zaščita?

› Skladnost NIS 2.0 direktivo se v velikem delu prekriva z GDPR in ISO27001

Aspect	NIS2	ISO27001:2022
Origin	EU Legal Act	ISO voluntary standard
Scope	Essential services, important entities, and certain digital service providers in the EU	Any organization
Purpose	Ensure a high common level of cybersecurity across the EU	Provide a framework for information security management
Requirements	Technical and organizational measures, incident reporting, cooperation, information provision, compliance with codes of conduct or standards of practice	Provide a framework for information security management
Annex A Controls	Not specified, but can be aligned with ISO/IEC 27002:2022	Specified and updated to reflect new technologies and threats
Certification	Not mandatory, but possible at the national level	Not mandatory, but possible at the international level

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Mapiranje zahtev

20. člen (Upravljanje)	
(1) Odgovorne osebe pravnih oseb oziroma člani poslovodnih organov (v nadaljnjem besedilu odgovorne osebe), ki so bistveni ali pomembni subjekti, so odgovorni za izvajanje ukrepov za obvladovanje tveganj za kibernetsko varnost v skladu z določbami tega zakona.	
(2) Odgovorne osebe iz prejšnjega odstavka odobrijo ukrepe za obvladovanje tveganj za kibernetsko varnost, ki jih subjekt izvaja zaradi izpolnjevanja obveznosti, določenih s tem zakonom, in nadzirajo njihovo izvajanje	Politika organizacija sistema varovanja informacij v organizaciji. (Lahko tudi kot del politike varovanja informacij v organizacija, ali kot del politike, ki opredeljuje upravljanje tveganj v organizacija). Formalni postopek odobritve ukrepov za obvladovanje tveganj (lahko v okviru sistem vodenja SUIV).
(3) Odgovorne osebe iz prvega odstavka tega člena se morajo izobraževati oziroma usposabljati na področju obvladovanja tveganj kibernetske varnosti in njihovega vpliva na dejavnosti oziroma storitve, ki jih izvaja subjekt.	Izvedba izobraževanj odgovornih oseb organizacije.
(4) Odgovorne osebe zagotavljajo redno usposabljanje zaposlenim, da pridobijo dovolj znanj in spretnosti, ki jih usposobi za prepoznavanje in ocenjevanje tveganj in za oceno praks obvladovanja tveganj za kibernetsko varnost ter njihovega vpliva na storitve, ki jih opravlja ta subjekt	Politika varovanja človeških virov, kjer so opredeljene zahteve po izobraževanju. Program/plan izobraževanja zaposlenih (zahteve informacijske in kibernetske varnosti). Sledljivost izobraževanja zaposlenih (kdo, kdaj, potrditev udeležbe,...).
(5) Ne glede na prejšnji odstavek odgovorne osebe zagotavljajo, da imajo vsi skrbniki informacijsko komunikacijskih sistemov zavezanca obveznost rednega letnega usposabljanja da pridobijo in ohranijo raven znanj in tveganj in za oceno praks obvladovanja tveganj za kibernetsko varnost ter njihovega vpliva na storitve, ki jih opravlja ta subjekt spretnosti, ki jih usposobi za prepoznavanje in ocenjevanje	Politika varovanja človeških virov, kjer so opredeljene zahteve po izobraževanju. Program/plan izobraževanja skrbnikov inf. sistemov. Sledljivost izobraževanja skrbnikov inf. sistemov (kdo, kdaj, potrditev udeležbe,...).

Mapiranje zahtev

21. člen (Varnostna dokumentacija bistvenih in pomembnih subjektov)	
(1) Bistveni in pomembni subjekti za zagotavljanje visoke ravni informacijske in kibernetske varnosti in odpornosti svojih omrežnih in informacijskih sistemov vzpostavijo in vzdržujejo dokumentiran sistem upravljanja varovanja informacij ter sistem upravljanja neprekinjenega poslovanja, ki temeljita na pristopu upoštevanja vseh nevarnosti in morata obsegati najmanj:	Vzpostavljen dokumentiran in formaliziran sistem varovanja informacij? Vzpostavljen dokumentiran in formaliziran sistem upravljanja neprekinjenega poslovanja? Zaposleni seznanjeni z vsebino dokumentiranih sistemov?
1. natančen in posodobljen popis informacijskih in drugih sredstev ter podatkov;	Popis informacijskih sredstev, ki vključuje: procese (storitve za končne uporabnike), lokacije, IT storitve, strojno in programsko opremo, komunikacije, podatke, zaposlene, storitve v oblaku,… Vzpostavljen proces rednega pregleda in posodobitve popisa (odgovorna oseba).
2. analizo obvladovanja tveganj, vključno z določitvijo sprejemljive ravni tveganja in opisano uporabljeno metodologijo;	Metodologija za izvedbo ocene tveganj z določitvijo sprejemljive ra tveganja. Izvedena ocena tveganj za inform. sistem subjekta (Poročilo). Vzpostavljen register tveganj in ukrepov za zmanjševanje tveganj. Seznanjenost odgovorne osebe (vodstva) s tveganji in priporočenir ukrepi. Seznanitev lastnikov tveganj. Potrditev tveganj in zagotovitev sredstev za odpravo tveganj s strar odgovornih oseb. Upravljanje aktivnosti odprave tveganj, oz izvedbe ukrepov (odgovornosti, roki, nadzor,...)
	Metodologija za izvedbo BIA. Izvedena BIA za procese ali IT storitve za končne uporabnike (poročilo).

Mapiranje zahtev

3. politiko in načrt neprekinjenega poslovanja, vključno z oceno vpliva na poslovanje;	
4. načrt obnovitve in ponovne vzpostavitve delovanja omrežnih in informacijskih sistemov, ki jih potrebujejo za svoje delovanje ali opravljanje storitev, vključno z opisom odgovornosti in postopkov za obnovitev;	Postopki za zagotovitev neprekinjenega delovanja IT storitev v primeru kriznih dogodkov.
5. načrt odzivanja na incidente s protokolom obveščanja pristojnega CSIRT, vključno z opisom sistema za zaznavo in odziv na incidente informacijske varnosti ter opisom vlog in odgovornosti za odzivanje na incidente;	Politika in proces odzivanja na incidente informacijske (kibernetsk varnosti (vloge in odgovornosti, opis sistema za zaznavanje, posto odziva, protokol obveščanja na pristojni CSIRT (SI-CERT; SIGOV CERT)).
6. načrt varnostnih ukrepov za zagotavljanje celovitosti, avtentičnosti, zaupnosti in razpoložljivosti omrežnih in informacijskih sistemov oziroma za obvladovanje tveganj za kibernetsko varnost, ki upoštevajo in področne posebnosti bistvenega ali pomembnega subjekta;	Načrt varnostnih ukrepov za obvladovanje tveganj.
7. politiko s postopki za oceno učinkovitosti varnostnih ukrepov za obvladovanje tveganj za informacijsko in kibernetsko varnost, vključno z določitvijo kazalnikov učinkovitosti in izvedeno analizo zbranih podatkov.	Politika s postopki za oceno učinkovitosti varnostnih ukrepov za obvladovanje tveganj za informacijsko in kibernetsko varnost. (Vključno s kazalniki učinkovitosti). Ostali priporočeni dokumenti in politike: a.) Informacijska varnostna politika za posamezna področja kibernetske varnosti. b.) organizacija varovanja informacij.
(2) Bistveni in pomembni subjekti določijo obseg sistema upravljanja in varovanja informacij ter neprekinjenega poslovanja ob upoštevanju rezultatov analize vpliva na poslovanje, kateri mora obsegati najmanj tista informacijska, komunikacijska in druga sredstva, podatke ter procese, ki so potrebni za njihovo delovanje ali opravljanje storitev	Politika: a.) obseg varovanja informacij (kibernetske varnosti); b.) obseg neprekinjenega poslovanja.

Mapiranje zahtev

22. člen (ukrepi za obvladovanje tveganj za kibernetsko varnost bistvenih in pomembnih subjektov)	
(1) Bistveni in pomembni subjekti morajo sprejeti ustrezne, učinkovite in sorazmerne tehnične, operativne in organizacijske ukrepe za zagotavljanje celovitosti, avtentičnosti, zaupnosti in razpoložljivosti omrežnih in varnost omrežnih in informacijskih sistemov, informacijskih sistemov oziroma za obvladovanje tveganj;	
(2) Varnostni ukrepi morajo temeljiti na pristopu upoštevanja vseh nevarnosti, katerega namen je zaščita omrežnih in informacijskih sistemov ter njihovega fizičnega okolja pred incidenti in morajo obsegati najmanj:	
1. podporo vodstva subjekta pri zagotavljanju informacijske in kibernetske varnosti in vključitvijo področja informacijske in kibernetske varnosti v letni načrt poslovanja oziroma letni program dela;	Krovna informacijska varnostna politika. Vodstveni pregled (v sklopu sistemov vodenja). Posodobljen letni načrt poslovanja (poslovni načrt) z elementi zagotavljanja informacijske (kibernetske) varnosti.
2. zagotavljanje integritete kadrov v povezavi z informacijsko varnostjo pred zaposlitvijo, med zaposlitvijo in ob prenehanju ali spremembi zaposlitve;	Politika varovanja informacij za zaposlene pred zaposlitvijo, med zaposlitvijo in ob prenehanju ali spremembi zaposlitve. Mentorski program za novo zaposlene z seznanitvijo politik varovanja informacij in dobrimi praksami glede kibernetske varnosti ob rokovanju s poslovnimi podatki in uporabo storitev Interneta.
3. osnovne prakse kibernetske higiene in usposabljanje na področju informacijske in kibernetske varnosti;	Politika varovanja informacij za zaposlene pred zaposlitvijo, med zaposlitvijo in ob prenehanju ali spremembi zaposlitve. Izobraževanje za zaposlene glede osnovne kibernetske higiene (seznanitev s kibernetskimi grožnjami pri vsakdanjih opravilih in kako se odzvati). Simulacije napadov ribarjenja in socialnega inženiringa
4. varnost človeških virov, preverjanje identitete uporabnikov, zagotavljanje ravni dostopnosti informacij in upravljanje pooblastil za dostop;	Politika za nadzor dostopov (uporabniški dostopi, privilegirani dostopi, partnerski dostopi, upravljanje identitet, uporabljanje vlog, varna raba gesel, . Dostopi do IT storitev na lokaciji ali storitev v oblaku).
5. izvajanje in upravljanje varnostnih kopij podatkov;	Politika upravljanja in varovanja varnostnih kopij. Uvedba varnostnih mehanizmov za zaščito varnostnih kopij: a.) 3-2-1-1-0 koncept b.) zaščita v. kopij pred nepooblaščenim spreminjanjem (immutable backup) c.) vpeljava izolirane zlate kopije podatkov (air gap).

Mapiranje zahtev

6. zagotavljanje in ohranjanje dnevniških zapisov o delovanju omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev, njihovih uporabnikov in administratorjev za obdobje najmanj šestih mesecev, lahko pa tudi za daljše obdobje, kadar iz analize obvladovanja tveganj in ocene sprejemljive ravni tveganj izhaja, da bi bilo tveganja ustrezno obvladovati z daljšo hrambo dnevniških zapisov. Ohranjanje dnevniških zapisov se zagotavlja primarno na ozemlju Republike Slovenije, sekundarno pa se lahko zagotavlja na ozemlju Evropske unije, razen subjektov s področja digitalne infrastrukture, bančništva in infrastrukture finančnega trga, kateri lahko ohranjanje dnevniških zapisov v celoti zagotavlja na ozemlju Evropske unije;	Politika varovanja dnevniških zapisov (lahko kot del politike upravljanja informacijskih sistemov ali upravljanje incidentov informacijske (kibernetske varnosti)). Politika varnostnega kopiranja in arhiviranja dnevniških zapisov skladno z zahtevami ZinfV-1 (lahko tudi kot del politike upravljanja in varovanja varnostnih kopij).
7. upravljanje omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev z določitvijo ustrezne odgovornosti za njihovo zaščito;	Politika upravljanja informacijskih sistemov, ki vključuje tudi omrežne IT storitve. Politika upravljanja privilegiranih dostopov.
8. politike in postopke v zvezi z uporabo kriptografije in po potrebi šifriranjem;	Politika varovanja klasificiranih podatkov. Politika varovanja podatkov s šifriranjem (vključuje zaščito podatkov v gibanju (data in move) in ob hrambi (data in rest) ter upravljanje šifrirnih ključev).
9. upravljanje prometa in komunikacij;	Politika upravljanja komunikacij (lahko tudi kot del politike upravljanja inf. sistemov)

Da povzamemo

- Gre za spremembno “mind set-a”
- O informacijski in kibernetski varnosti moramo začeti razmišljati v celotnem življenskem ciklu
- Kako začeti?
  - Moramo vedeti, kje smo in kaj ščititi?
    - Popis, BIA
  - Moramo vedeti, kakšna tveganja obstajajo?
    - RA
  - Izdelati letni načrt ukrepov
    - → tehnični ukrepi.
      - NIS2 in ZinfV1: ne obstaja črna škatlica, ki bo rešila vse probleme
  - Vedeti kdo, kaj in kako varovati
    - Politike, odgovornosti, načina odziva na incidente, imeti sposobnost zaznave


TRANSFORMATION IS A JOURNEY
NOT A DESTINATION

Kontakt

Uroš Majcen
Direktor za kibernetsko odpornost
E: uros.majcen@kontron.si
T: +386 30 609 499

Miro Faganel
Vodja oddelka prodaja – Varnost in omrežja
E: miro.faganel@kontron.si
T: +386 41 932 563

Kontron SI, d. o. o.
Leskoškova 6
1000 Ljubljana, Slovenia
www.kontron-slovenia.com

KIBERNETSKI CUNAMI

Ali smo pripravljeni na spremembe ZInfV?

Ali smo pripravljeni na spremembe ZInfV?

Upravljanje privilegiranih dostopov (PAM): Ključ do varnosti v digitalni dobi

Borut Jenko

vodilni inženir za kibernetsko varnost, Smart Com d.o.o.

zit SeKV

Združenje za informatiko in telekomunikacije
Kibernetska varnost

SMART COM

Upravljanje privilegiranih dostopov (PAM):

Ključ do varnosti v digitalni dobi

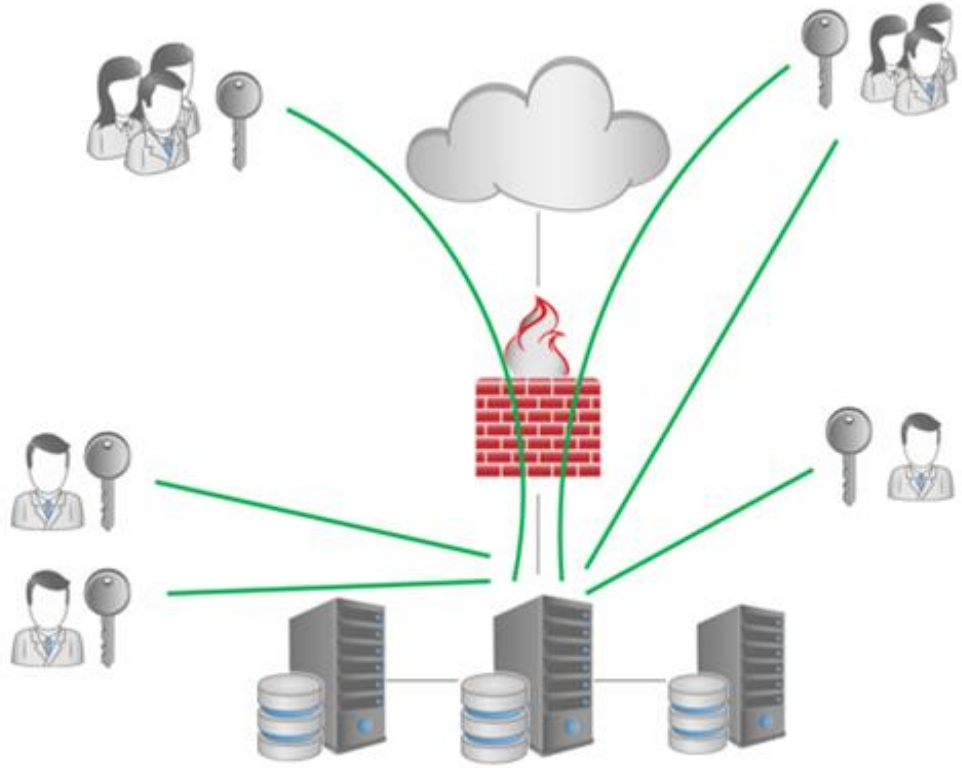
Borut Jenko
Vodilni inženir za kibernetsko varnost, Smart Com d.o.o.

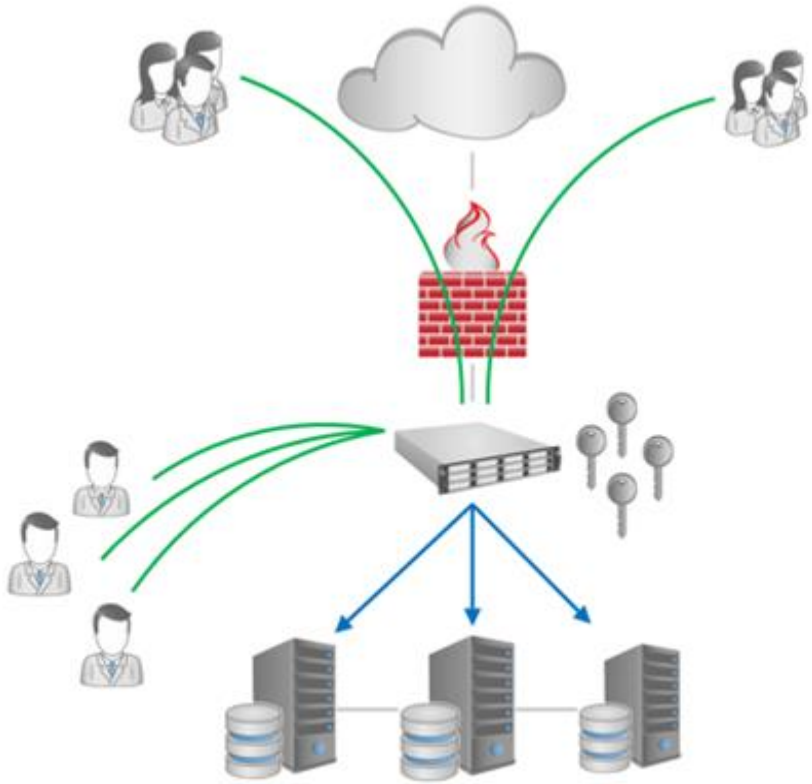
Ali smo res vsi „SUPER“ uporabniki?

Izzivi v digitalni dobi

Pomanjkanje vidljivosti in sledljivosti	Prekomerno podeljevanje pravic	Skupni uporabniški računi/gesla
Ročno upravljanje uporabniških računov	Dodeljevanje dostopa tretjim osebam	Fluktuacija zaposlenih

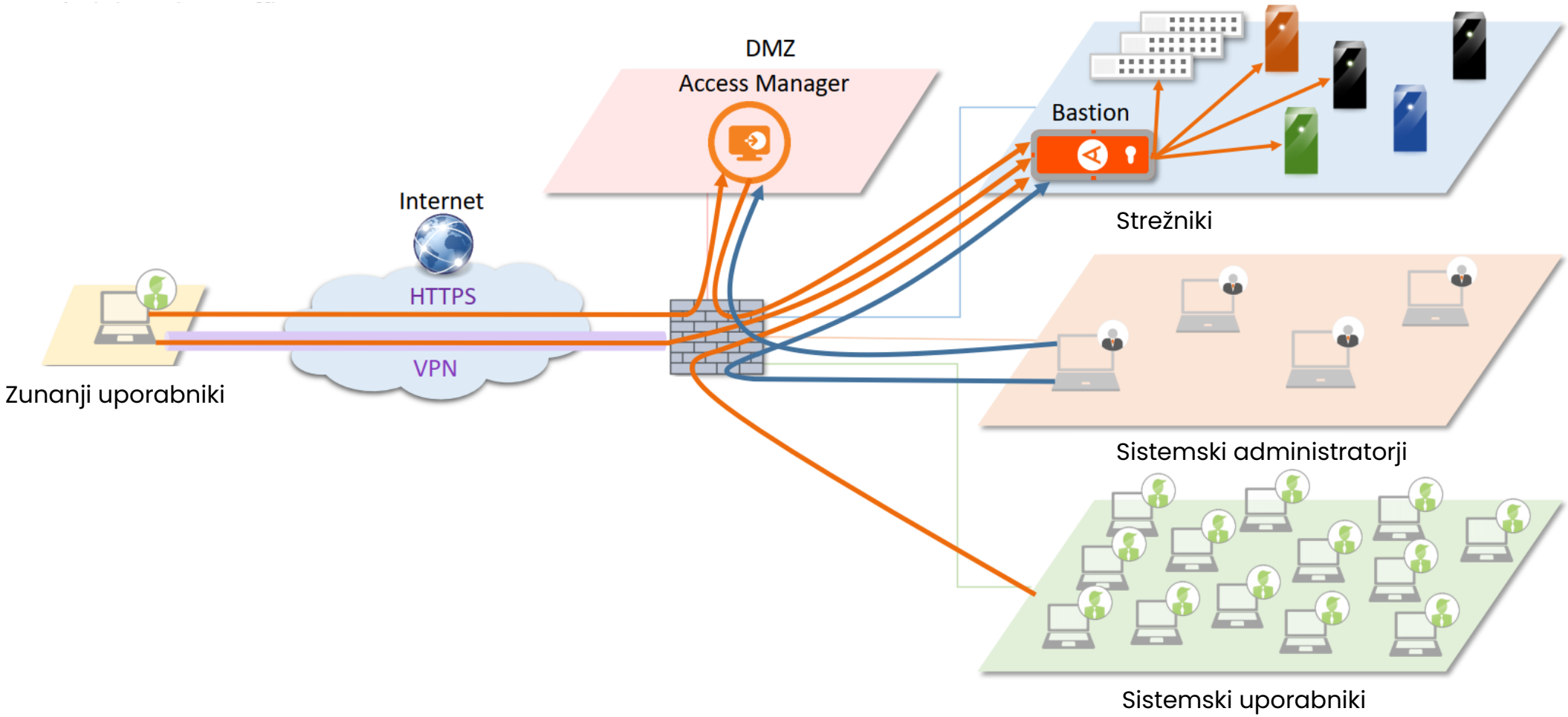
Kaj je Privileged Access Management (PAM)?





SMART COM

Kako integriramo PAM v omrežje?



SMART COM

Ključne komponente PAM sistema

- Identifikacija in avtentikacija
- Upravljanje in nadzor sej
- Upravljanje in nadzor gesel
- Odobritve
- Začasni dostop
- Centralna baza podatkov
- Integrirana rešitev

Upravljanje in nadzor sej

- Upravljanje privilegiranih dostopov na:
  - operacijskih sistemih Unix in Windows,
  - mrežnih napravah,
  - virtualnih sistemih,
  - konzolah in spletnih aplikacijah,
  - odjemalcih (sFTP, WinSCP, PuTTy).
- Snemanje in pregled sej
- Dostopi s potrjevanjem
- Zbiranje metapodatkov o sejah
- RDP, SSH, TELNET, VNC, WINSCP, ...
- Vgrajeni mehanizmi za blokiranje veriženih sej
- Prepoznavanje ukazov

Upravljanje in nadzor gesel

- Administrativno upravljanje z gesli
- Redne zamenjave in rotacije gesel
- Hramba SSH ključev
- Hramba gesel v trezorju
- Upravljanje z gesli (Microsoft, Linux/Unix, Cisco, Juniper Networks ...)

Zakaj je PAM pomemben v kontekstu NIS 2?

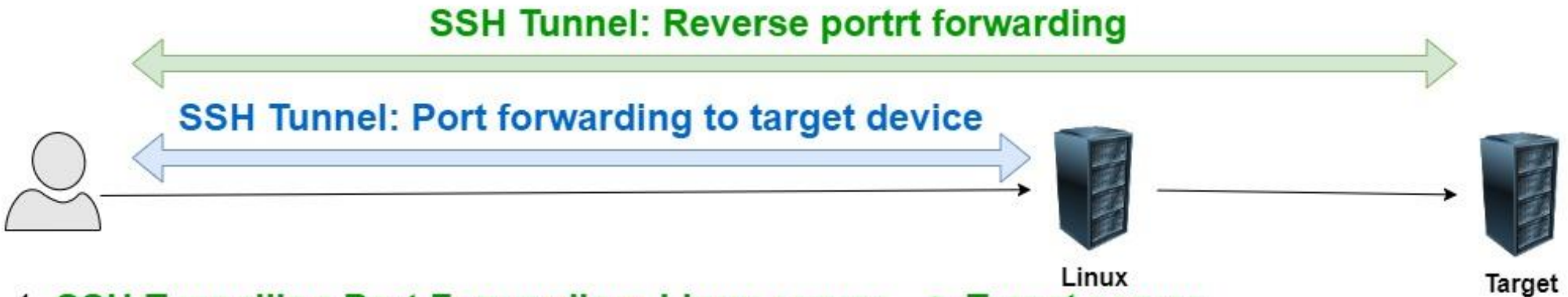
- Zmanjšanje napadalne površine
- Izboljšanje vidnosti in preglednosti
- Centralizirano upravljanje
- Zmanjšanje tveganja za eskalacijo privilegijev
- Izvajanje načela najmanjšega privilegija

Kako PAM pomaga pri izpolnjevanju zahtev NIS 2?

- Identifikacija in avtentikacija
- Nadzor seje
- Just-in-time dostop
- Upravljanje gesel
- Avtomatizacija
- Zaščita pred stranskimi premiki

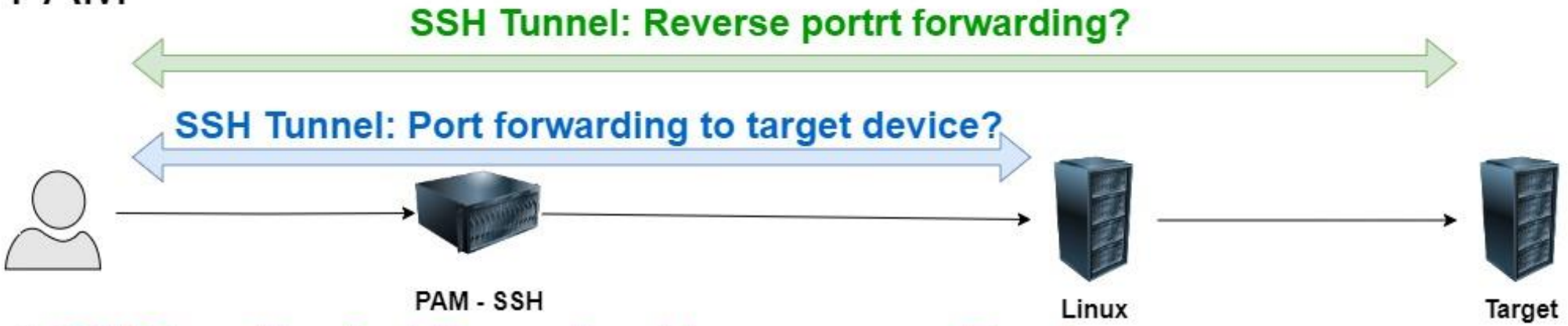
Primer uporabe PAM-a

w/o PAM



1. SSH Tunnelling Port Forwarding: Linux server ---> Target server
2. SSH Tunnelling Reverse Port Forwarding: Target server -> localhost:3128

PAM



1. SSH Tunnelling Port Forwarding: Linux server ---> Target server
2. SSH Tunnelling Reverse Port Forwarding: Target server -> localhost:3128

SMART COM

Imate vprašanja?

BORUT JENKO

Vodilni inženir za kibernetsko varnost

E: borut.jenko@smart-com.si

KIBERNETSKI CUNAMI

Ali smo pripravljeni na spremembe ZInfV?

Ali smo pripravljeni na spremembe ZInfV?

FutuResilience: Ali smo pripravljeni na prihodnje izzive kibernetske varnosti?

Luka Jelovčan

direktor Inštituta za Varnost in Strateške Raziskave (IVSR)

SlovenianCyberResilienceLab
Part of FutuResilience consortium

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

FutuResilience: Ali smo pripravljeni na prihodnje izzive kibernetske varnosti?

Luka Jelovčan
Inštitut za Varnost in Strateške Raziskave

FutuResilience in SCRL

SlovenianCyberResilienceLab
Part of FutuResilience consortium

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Grožnje prihodnosti?

Start-up in majhna podjetja

Vpliv kriz na kibernetsko varnost

FutuResilience
Building sustainable futures together

SlovenianCyberResilienceLab
Part of FutuResilience consortium

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Vpliv globalnih kriz na kibernetsko varnost

COVID-19

- **Dobavna veriga** — Spremembe v dobavnih verigah so vplivale na cene in dobavljivost IT komponent.
- **Delo od doma** — Novi vektorji napada in večji pomen notranjih groženj.
- **Pospešena digitalizacija** — Najprej funkcionalnost, potem varnost.
- **Nove oblike groženj** — Spletne prevare, phishing, lažne novice in ransomware.

SlovenianCyberResilienceLab
Part of FutuResilience consortium

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Krize prihodnosti in kibernetska varnost?

SlovenianCyberResilienceLab
Part of FutuResilience consortium

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Evropa je na precepu

Ekonomska varnost

Ekonomska varnost je ključna za nadaljnji razvoj in stabilnost Evropske unije. Hkrati, pa lahko nekatere gospodarske prakse same predstavljajo grožnjo varnosti EU.

COVID-19 in ranljivost dobavnih verig

Vojna v Ukrajini, zaprtje ruskega trga in globalni konflikti

Odmikanje od ZDA in krepljenje lastnih razvojnih zmožnosti

SlovenianCyberResilienceLab
Part of FutuResilience consortium

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Strategija ekonomske varnosti EU

Tveganja odpornosti dobavnih verig

1

Tveganja varnosti kritične infrastrukture

2

3

Tveganja varnosti tehnologije in odtekanja informacij

4

Tveganja ekonomske odvisnosti

SlovenianCyberResilienceLab
Part of FutuResilience consortium

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Tveganja varnosti tehnologije in odtekanja informacij

Tveganja, ki ogrožajo tehnološki napredek EU, tehnološko konkurenčnost in dostop do najsodobnejše tehnologije.

„Dual use“ tehnologija, predvsem na področjih:

- Kvantnega računalništva.
- Polprevodnikov.
- Umetne inteligence.

Industrijsko vohunjenje v kibernetskem prostoru EU.

SlovenianCyberResilienceLab
Part of FutuResilience consortium

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Napadi na javne in zasebne organizacije.

1

Državni in nedržavni akterji.

2

3

Dolgotrajni, usmerjeni in obširni napadi.

4

Različni vektorji napadov.

SlovenianCyberResilienceLab
Part of FutuResilience consortium

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Prikriti napadi in poudarek na brisanju sledi.

5

7

Uporaba zaupanja vrednih platform.

Veliko časa namenijo OSINT in „orientaciji“.

6

8

Socialni inženiring in izkoriščanje ranljivosti v tehnologiji.

SlovenianCyberResilienceLab
Part of FutuResilience consortium

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Notranje grožnje

Zaposleni ostajajo glavna tarča napadalcev:

- Digitalizacija in dostopnost osebnih podatkov.
- „MICE“ dejavniki.
- Izkoriščanje dostopa, razkrivanje informacij, sabotaže, …

Vpliv umetne inteligence in dezinformacij?

SlovenianCyberResilienceLab
Part of FutuResilience consortium

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

ZInfV-1 in NIS2

- NIS2 se direktno ne dotika industrijskega vohunjenja v kibernetskem prostoru – dviga pa splošno odpornost organizacij.
- Poudarek na varnosti dobavnih verig.
- Okvirji za ocenjevanje tveganj predstavljajo temelj za odzivanje na grožnje prihodnosti.

SlovenianCyberResilienceLab
Part of FutuResilience consortium

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Kibernetski izzivi prihodnosti?

… kot jih vidi Europol:

Umetne inteligenca 1

Decentralizacija interneta 2

3 RaaS

4 Kriptovalute

SlovenianCyberResilienceLab
Part of FutuResilience consortium

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Hvala za pozornost!

Luka Jelovčan
Inštitut za Varnost in Strateške Raziskave
luka.jelovcan@ivsr.si

KIBERNETSKI CUNAMI

Ali smo pripravljeni na spremembe ZInfV?

KIBERNETSKI CUNAMI

Ali smo pripravljeni na spremembe ZInfV?

Upravljanje kibernetskih tveganj - pasti ali priložnosti?

dr. Saša Javorič

vodilna presojevalka sistemovvodenja ISO 9001 in 27001, SIQ

UPRAVLJANJE KIBERNETSKIH TVEGANJ - PASTI ali PRILOŽNOSTI?

dr. Saša Javorič, SIQ

18.10.2024

Upravljanje tveganj informacijske varnosti

Tveganje IV: verjetnost, da bo grožnja (napadalec) izkoristila ranljivost informacijskega sredstva in povzročila škodo (posledico): negativni vpliv na **Z**aupnost, **C**elovitost, **R**azpoložljivost in/ali **A**vtentičnost informacij

Tveganje = kombinacija Verjetnosti (V) (uresničitve grožnje, ranljivosti) in Posledic (P)

Cilj upravljanja tveganj informacijske/kibernetske varnosti:

- Vpeljan sistematični pristop: razmišljanje / upravljanje na podlagi tveganj
- Poenoteni kriteriji ocenjevanja tveganj (primerljivost, ponovljivost ocenjevanja)
- Določene vloge, odgovornosti in pristojnosti za upravljanje tveganj
- Zgodnje odkrivanje ranljivosti, groženj in tveganj informacijske varnosti
  - Preventivno delovanje, odprava odkritih ranljivosti, predvidevanje
  - Zgodnje zaznavanje, spremljanje
  - Hiter odziv, hitra omejitev morebitne škode v primeru incidenta

Upravljanje tveganj - ISO 3100:2018

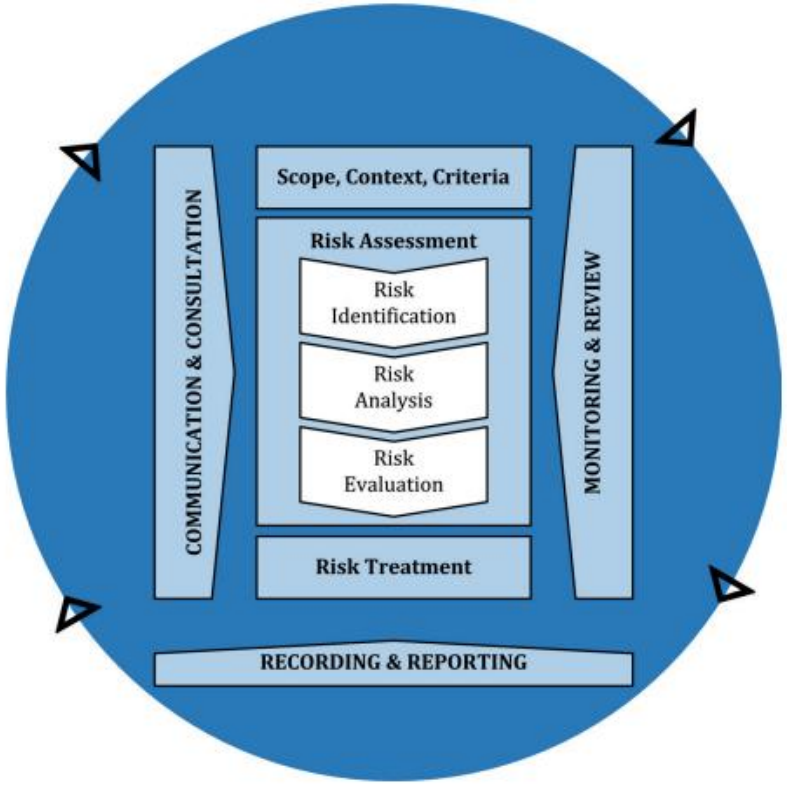
Sistematični pristop, sestavni del aktivnosti organizacije

- Obseg, kontekst organizacije
- Kriteriji za ocenjevanje tveganj

A. Ocenjevanje tveganj (*Risk Assesment*)

1. Prepoznavanje tveganj (*Risk Identification*) (informacijski viri, grožnje, ranljivosti, tveganja)
2. Analiziranje tveganj (*Risk Analysis*) (verjetnost, posledice)
3. Vrednotenje tveganj (*Risk Evaluation*) (primerjava s kriteriji za ocenjevanje tveganj, podpora za odločanje)

- Komuniciranje in posvetovanje z deležniki (ozaveščenost, strokovnost, vključenost)

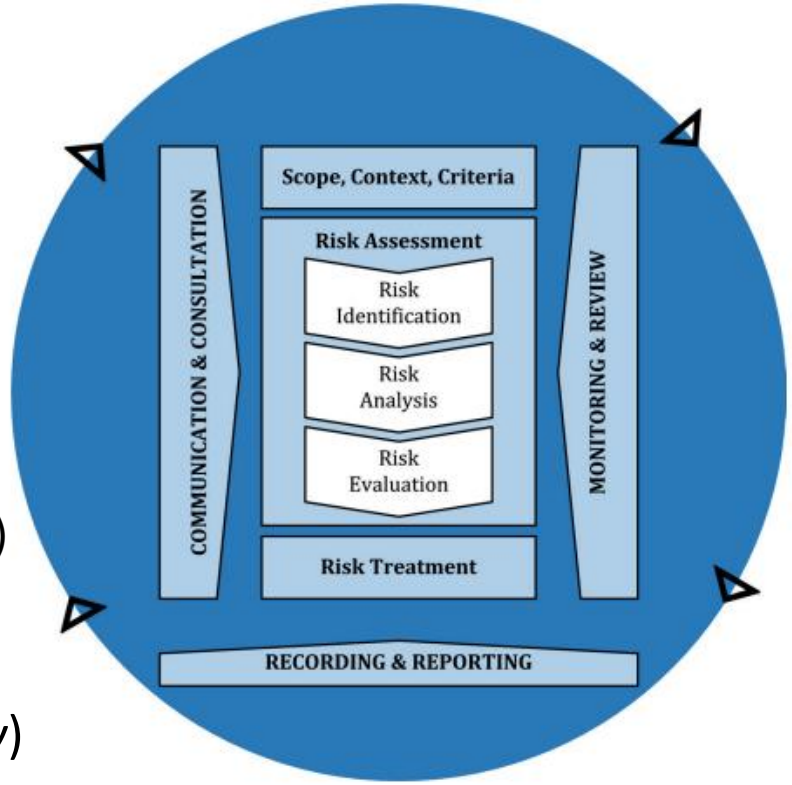


Upravljanje tveganj - ISO 3100:2018

Sistematični pristop, sestavni del aktivnosti organizacije:

B. Obravnavanje tveganj (*Risk Treatment*)

1. Izbira strategije obravnave tveganja (*Risk Treatment Option*)
2. Načrtovanje in implementiranje aktivnosti (*Planning, implementing Risk Treatment*)
3. Ocenjevanje uspešnosti (*assessing the effectiveness of treatment*)
4. Odločanje o sprejemljivosti preostalega tveganja (*the remaining risk is acceptable*?)
5. Nadaljnja obravnava za preostala nesprejemljiva tveganja



- Spremljanje in pregled (*Monitoring, Review*)
- Dokumentiranje in poročanje (*Recording and Reporting)*

Upravljanje tveganj – ISO/IEC 27005, 27001

ISO/IEC 27001:2022

4. Okvir (kontekst) organizacije

6. Načrtovanje

   6.1.2 Ocenjevanje tveganj IV

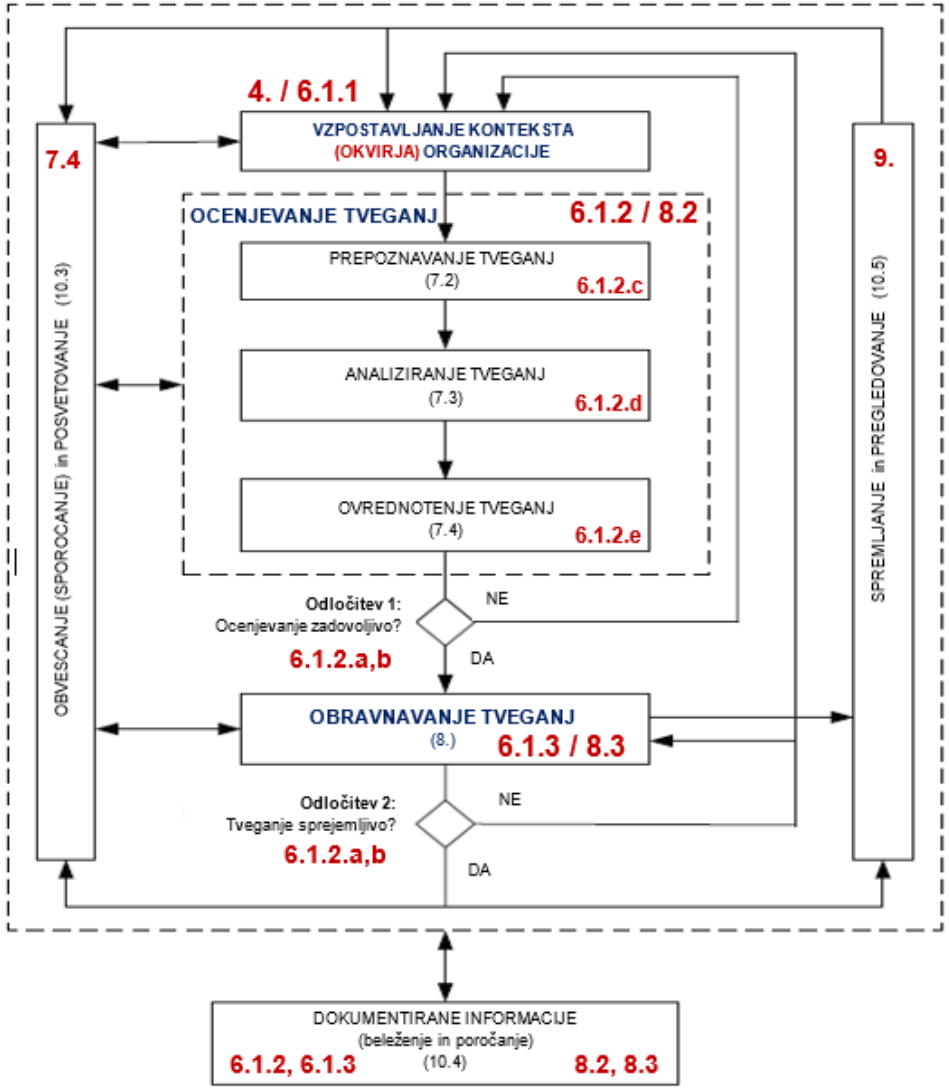
   - kriteriji
   - ponovljivost, primerljivost
   - prepoznavanje tveganj IV
   - analiziranje tveganj IV
   - ovrednotenje tveganj IV

   6.1.3. Obravnavanje tveganj IV

8. Delovanje

   8.2 Ocenjevanje tveganj IV

   8.3 Obravnavanje tveganj IV



4. … ISO/IEC 27001:2022

(7.2) … ISO/IEC 27005:2022

Kriteriji za ocenjevanje tveganj

Verjetnost (V)		Posledice (P)
1	Skoraj nikoli	Nepomembne (100 €)
2	Redko	Srednja škoda (100.000€)
3	Skoraj zagotovo	Zelo velika škoda (10 mio €)

Kriteriji tveganja (*Risk Criteria*)

- Kriteriji za ocenjevanje verjetnosti (V), posledic (P)
  - Kvalitativno določeni kriteriji: subjektivna ocena posameznika, ki ocenjuje; **ponovljivost, primerljivost** ponovnega ocenjevanja?
  - Kriteriji za posledice določeni le kot višina finančnih posledic (v €), vodstvo ni vključeno
  - Kriteriji, privzeti od druge organizacije, ki ne ustrezajo kontekstu organizacije
  - Kriteriji za ocenjevanje posledic brez upoštevanja vidikov Z, C, R, A
  - Pri ocenjevanju vidikov posledic Z, C, R, A upoštevana samo maksimalna vrednost
  - Prenizek rang (3) za informacijska tveganja
  - Opisi ne sledijo jeziku ocenjevalcev, niso razumljivi, niso enolično določeni

- Način določanja stopnje tveganja (ST)
  - Algoritem za izračun stopnje tveganja, ki nikomur ni razumljiv …
  - Dolgotrajen, zapleten postopek dodeljevanja uteži pri določanju ST

Kriteriji za ocenjevanje tveganj

Verjetnost (V)		Posledice (P)
1	Skoraj nikoli	Nepomembne (100 €)
2	Redko	Srednja škoda (100.000€)
3	Skoraj zagotovo	Zelo velika škoda (10 mio €)

Kriteriji tveganja (*Risk Criteria*)

- Kriterij za sprejem tveganja (ali je tveganje sprejemljivo ali ne, pooblastila)
  - Kriteriji za sprejem tveganj dvoumno določeni (nesprejemljiva, pomembna … tveganja)
  - Pravila za obravnavo nesprejemljivih tveganj niso določena
  - Meja sprejemljivosti ni določena / ni jasno določena
  - Pri meji sprejemljivosti ni upoštevana nagnjenost k prevzemanju tveganj (*Risk Apetite*)

- Sprejetje kriterijev
  - Kriteriji niso preverjeni skozi pilotno ocenjevanje
  - Kriteriji niso potrjeni s strani vodstva

- Orodja za upravljanje tveganj
  - Omejitve orodja (ne morem določiti kriterija, kot želim …)

Prepoznavanje tveganj

Prepoznavanje tveganja (*Risk Identification*)

- Pristop sredstev (*Assets*)
  - INFORMACIJE in INFORMACIJSKA SREDSTVA v okviru obsega, njihova vrednost (lokacije, prostori, podporne storitve, strojna in programska oprema, informacije, zbirke, ljudje, ugled organizacije/blagovne znamke … , zaupanje deležnikov …)
  - Določitev LASTNIKOV informacijskega sredstva (pristojnosti, odgovornosti)
  - Prepoznava GROŽENJ za posamezno informacijsko sredstvo (frekvenca)
  - Prepoznava RANLJIVOSTI, ki bi jih lahko izkoristile grožnje (izpostavljenost)
- Procesni pristop (*Processes*)
  - PROCESI IN AKTIVNOSTI organizacije v okviru obsega
- Pristop scenarijev (*Events*)
  - Scenariji, kako bi lahko VIR GROŽNJE izkoristil RANLJIVOST in povzročil ŠKODO?

Analiziranje tveganj

Analiziranje tveganja (*Risk Analysis*) - razumevanja narave in določitev stopnje tveganja

Ocenjevanje verjetnosti (V):

- Trendi – spremljanje, preventivno zaznavanje groženj, ranljivosti …
- Varnostni dogodki, izpostavljenost – kontekst, obseg (pojavljanje grožnje)
- Vpliv znanih ranljivosti informacijskih sredstev (izpostavljenost)
- Vpliv že izvedenih ukrepov glede IV (lastnik procesa, IT oddelek)

Ocenjevanje posledic (P):

- Celotna življenjska doba informacijskega sredstva (nastanek … uničenje)
- Vsi stroški v primeru izgube **Z**aupnosti, **C**elovitosti, **R**azpoložljivosti, **A**vtentičnosti
- Ocenjevanje po vseh vidikih - izguba **Z / C / R / A**

Določitev stopnje tveganja (ST):

- kombinacija verjetnosti (V) in posledic (P)

Prepoznavanje in analiziranje tveganj

Prepoznavanje in analiziranje tveganj (*Risk Identification & Analysis*)

- Podpora, razumevanje s strani vodstva
  - Ni časa za to … a spet se moram s tem ukvarjati …
  - Daj kar ti nekaj naredi, da bo kljukica, da smo to naredili … („one-man-band“)
  - Spet so ti presojevalci, ki bodo hoteli videti oceno …
- Kultura organizacije
  - Nič ni tveganje / vse je tveganje
  - Raje se potuhnem kot da bi se izpostavljali / Kdor najglasneje vpije, dobi največ sredstev …
  - Nič ne moremo narediti … kaj naj zdaj to v tabele pišem …
  - Če bo ta vendor imel težave, bomo imeli večje težave, se bomo z drugimi stvarmi ukvarjali …
- Nerazumevanje, nepoznavanje
  - Ne razumem, kaj hočete od mene …
  - Naj to IT naredi … to ni moje delo …
  - Kako naj to ocenim … ali ocenim glede na že vpeljane ukrepe ali brez njih?

Prepoznavanje in ocenjevanje tveganj

Prepoznavanje in analiziranje tveganj (*Risk Identification & Analysis*)

- Popisi informacijskih sredstev
  - Popisi sredstev premalo / preveč podrobni / pomanjkljivi
  - Lastniki informacijskih sredstev niso določeni / niso ustrezni (oddelek ali IT)
- Seznami tveganj
  - Premalo prepoznanih tveganj (neprepoznano) / preveč prepoznanih tveganj (neobvladljivo)
  - Preveč splošno določena (generična) tveganja / prepoznane samo grožnje, brez ranljivosti
  - Prepoznane so samo določene vrste tveganj (tveganje dobavne verige ni prepoznano)
  - Neustrezno ocenjena tveganja (kriteriji, nerazumevanje … ne upam se izpostaviti/kričim)
  - Zakaj bi si delal delo … manj kot prepoznam in ocenim tveganj, manj dela bom imel …
- Orodja za upravljanje tveganj
  - Omejitve orodja: vnaprej pripravljeni seznami,
  - Omejitve orodja: ni mogoče izbrati, vnesti …
  - „Prednosti“ orodja: „Copy-paste“ vnaprej pripravljeni seznami, ocene …

Vrednotenje tveganj

Vrednotenje tveganj (*Risk Evaluation*)

- primerjava rezultatov analize tveganja s kriteriji sprejemljivosti: določitev, ali je tveganje sprejemljivo ali nesprejemljivo

Sprejemanje tveganja:

- Meja sprejemljivosti - sprejemanje tveganja: stopnja tveganja glede na VSE vidike: **Z /C /R /A**
- Vpliv že izvedenih ukrepov glede IV (lastnik procesa, IT oddelek …)

Prioritiziranje tveganj:

- Kritičnost tveganja izgube **Z /C /R /A**
- Viri, ki so na razpolago (časovni okvir, ljudje, oprema …)

⇩

Seznam prioritiziranih tveganj IV

Vrednotenje tveganj

Vrednotenje tveganj (*Risk Evaluation*)

- Kriteriji, analiziranje:
  - Kriteriji niso ustrezni / razumljivi / enolično določeni
  - Meja sprejemljivosti ni ustrezna (že par let nimamo nesprejemljivih tveganj)

- Nesprejemljiva tveganja:
  - Zakaj bi si delal delo … manj kot prepoznam tveganj, manj dela bom imel …
  - „Popravljanje“ ocene (preveč / premalo ocenjeno glede na sprejemljivost)
  - Ne bom se izpostavljal, zakaj bi jaz kazal na nesprejemljiva tveganja …

- Sprejem nesprejemljivih tveganj:
  - Kako naj bom jaz kriv, če je vodstvo reklo, da je to sprejemljivo tveganje? Vloge in odgovornosti, pristojnosti?!

Obravnavanje tveganj

Obravnavanje tveganj (*Risk Treatment*)

Izbira metode/možnosti obravnavanja tveganj:

- Zmanjševanje / Sprejemanje / Izogibanje Delitev tveganja

Določitev ukrepov, kontrol za obravnavno tveganj:

- ISO/IEC 27001:2022, Dodatek A
- CIS / PCI DSS / SOC2 kontrole … ukrepi, določeni s strani organizacije

Načrta za obravnavno tveganj

- Priprava načrta, pregled in odobritev načrta za obravnavno tveganj (vodstvo)

Izvedba ukrepov iz Načrta za obravnavno tveganj

Preverjanje uspešnosti izvedenih ukrepov, preostalega tveganja

Poročanje, periodični pregledi in ocenjevanja tveganj

Obravnavanje tveganj

Obravnavanje tveganja (*Risk Treatment*)

- Ukrepi za obravnavo tveganj
  - Ukrepi niso ustrezni /niso učinkovito izbrani / niso določeni
  - Ukrepov ni mogoče določiti (tveganje je preveč splošno / nerazumljivo zapisano)
  - Lastniki ukrepov niso določeni, ne vemo, kdo mora kaj narediti (vloge, odgovornosti)
- Načrt za obravnavno tveganj
  - Lastniki ukrepov niso seznanjeni, da morajo kaj narediti …
  - Načrt ni sprejet, za izvedbo ukrepov ni na voljo virov (človeških, finančnih …)
  - Ukrepi niso prioritizirani (kaj naj najprej naredim, če je vse nujno?)
  - Način preverjanja uspešnosti ukrepov ni določen
  - Ni preverjanja statusa, ni poročanja o izvedbi / neizvedbi ukrepov
- Orodja za upravljanje tveganj
  - Omejitve orodja: vnaprej pripravljeni seznami, ni mogoče izbrati, vnesti …
  - „Copy-paste“ vnaprej pripravljeni seznami, ocene … ukrepi …

Obravnavanje tveganj

Obravnavanje tveganja (*Risk Treatment*)

- Izvedeni ukrepi za obravnavo tveganj
  - Nihče ne spremlja statusa izvedbe Načrta ukrepov za obravnavo tveganj
  - Lastniki tveganj ne javijo, ko izvedejo ukrep (pozabil sem …)
  - Nihče ne preverja, ali so ukrepi uspešni /ni določenega kriterija za preverjanje uspešnosti
  - Nihče ne izvede ponovne ocene, ali so preostala tveganja sprejemljiva / nesprejemljiva

- Periodično ocenjevanje tveganj
  - Ni določenih pravil za periodične preglede in ocenjevanja tveganj
  - Nihče se ne „spomni“, da bi moral ob večjih spremembah izvesti delno oceno tveganj (pred/ob večjih spremembah, incidentih, …)

UPRAVLJANJE KIBERNETSKIH TVEGANJ - PASTI ali PRILOŽNOSTI?

Vprašanja, komentarji?

Hvala za sodelovanje.

javoric.sasa@siq.si

KIBERNETSKI CUNAMI

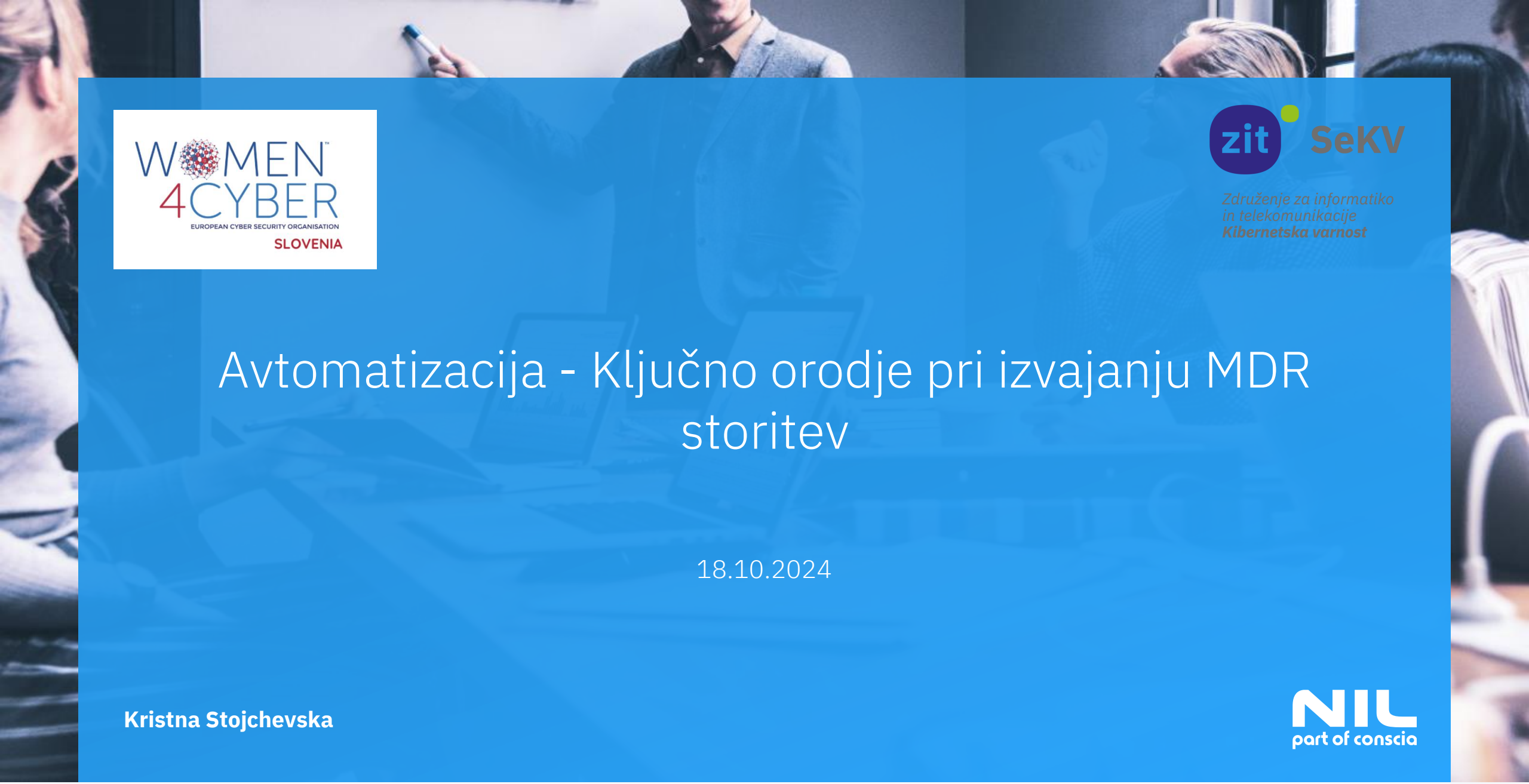
Ali smo pripravljeni na spremembe ZInfV?

Ali smo pripravljeni na spremembe ZInfV?

Avtomatizacija-Ključno orodje pri izvajanju MDR

Kristina Stojchevska

analitičarka za kibernetsko varnost, NIL d.o.o. in članica Women4Cyber Slovenija



Avtomatizacija - Ključno orodje pri izvajanju MDR storitev

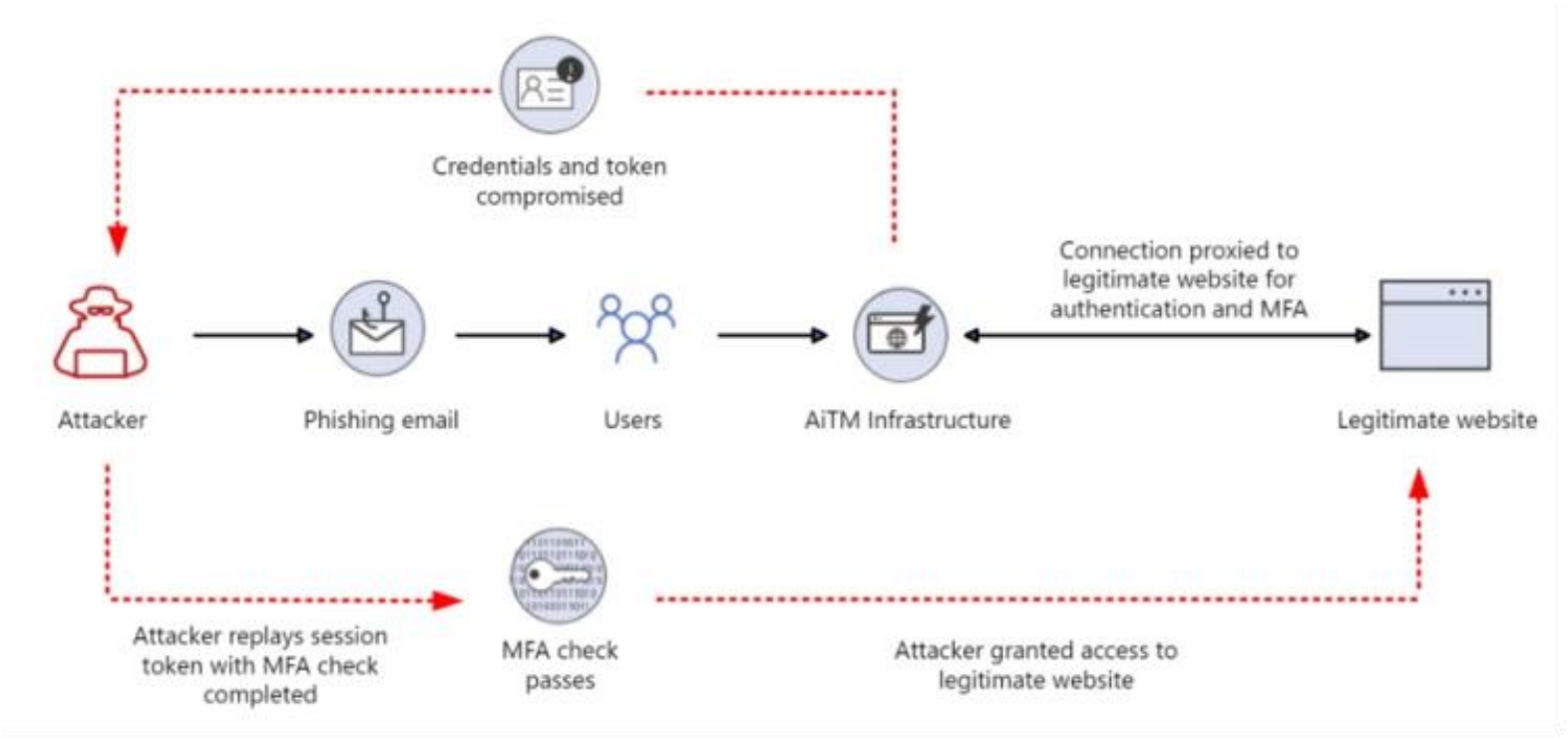
18.10.2024

Kristna Stojchevska

Avtomatizacija

1. Količina podatkov in število varnostnih incidentov v je stalnem porastu.
2. Avtomatizacija postaja ključno orodje.
3. Hitrejše in učinkovitejše prepoznavanje potencialne grožnje.
4. Krajši čas od alarma do zaznave.
5. Krajši čas od zaznave do odziva.

Primer napada Advesary in the Middle (AiTM)



Potek raziskave in mitigacija AiTM napadov brez avtomatizacije

1. Zaznava napada (tudi do 48ur).
2. Sprožen alarm v sistemu SOAR
3. Pričetek preiskave (phishing ali AiTM?)
4. Dodatno preiskovanje
5. Kreiranje baseline-a.
6. Potrjen napad, eskalacija na drugi nivo analitike, pisanje Incident Reporta in obveščanje stranke

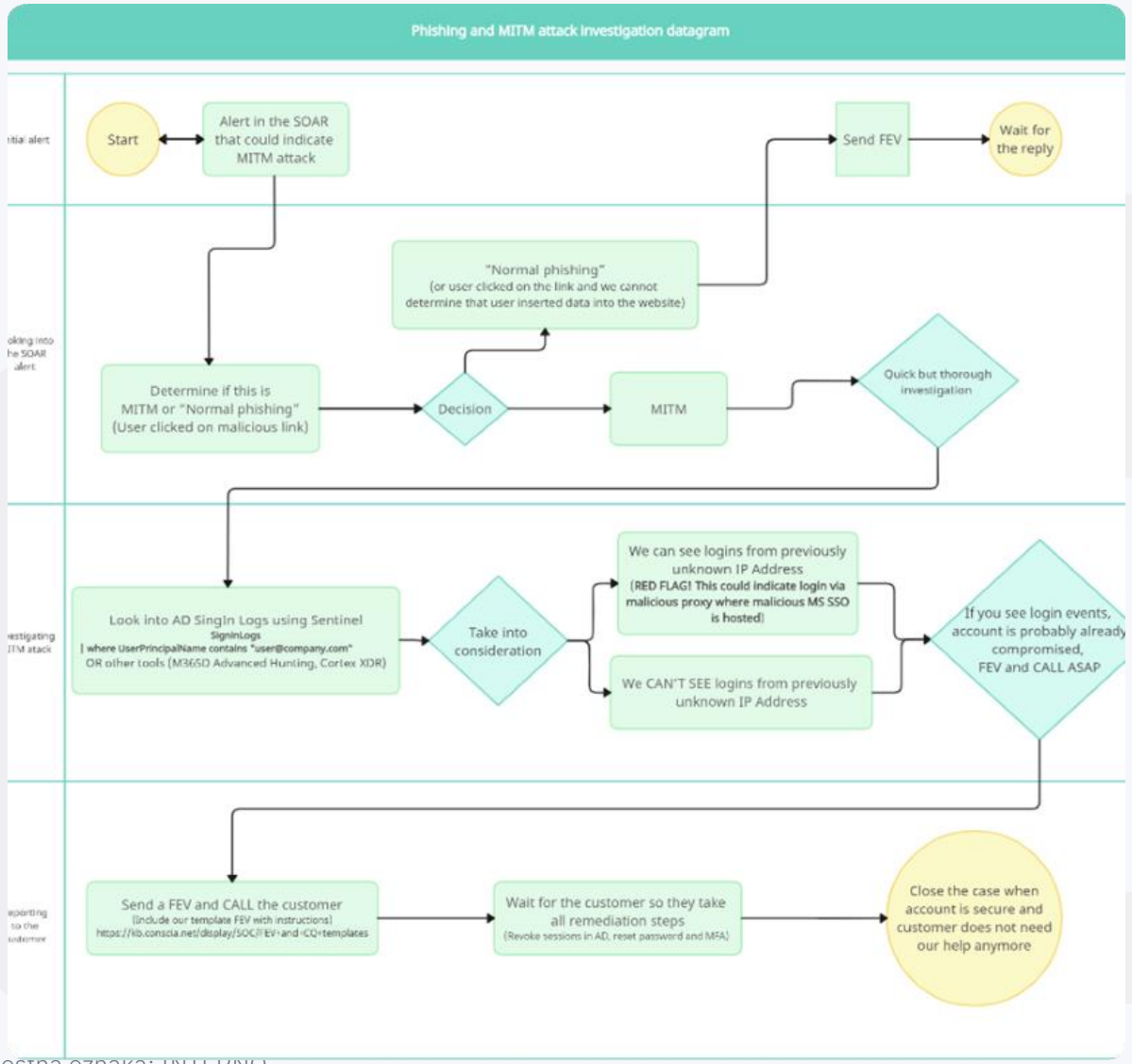
Potek raziskave in mitigacija AiTM napadov brez avtomatizacije

Zaznava do - **48ur**

Ročna detonacija URL ja in preiskovanje le tega -**5min**

Preiskovanje logov in kreiranje baselina – cca **10 min**

Eskalacija, pisanje Incident Reporta in klicanje stranke – cca **10-20min**



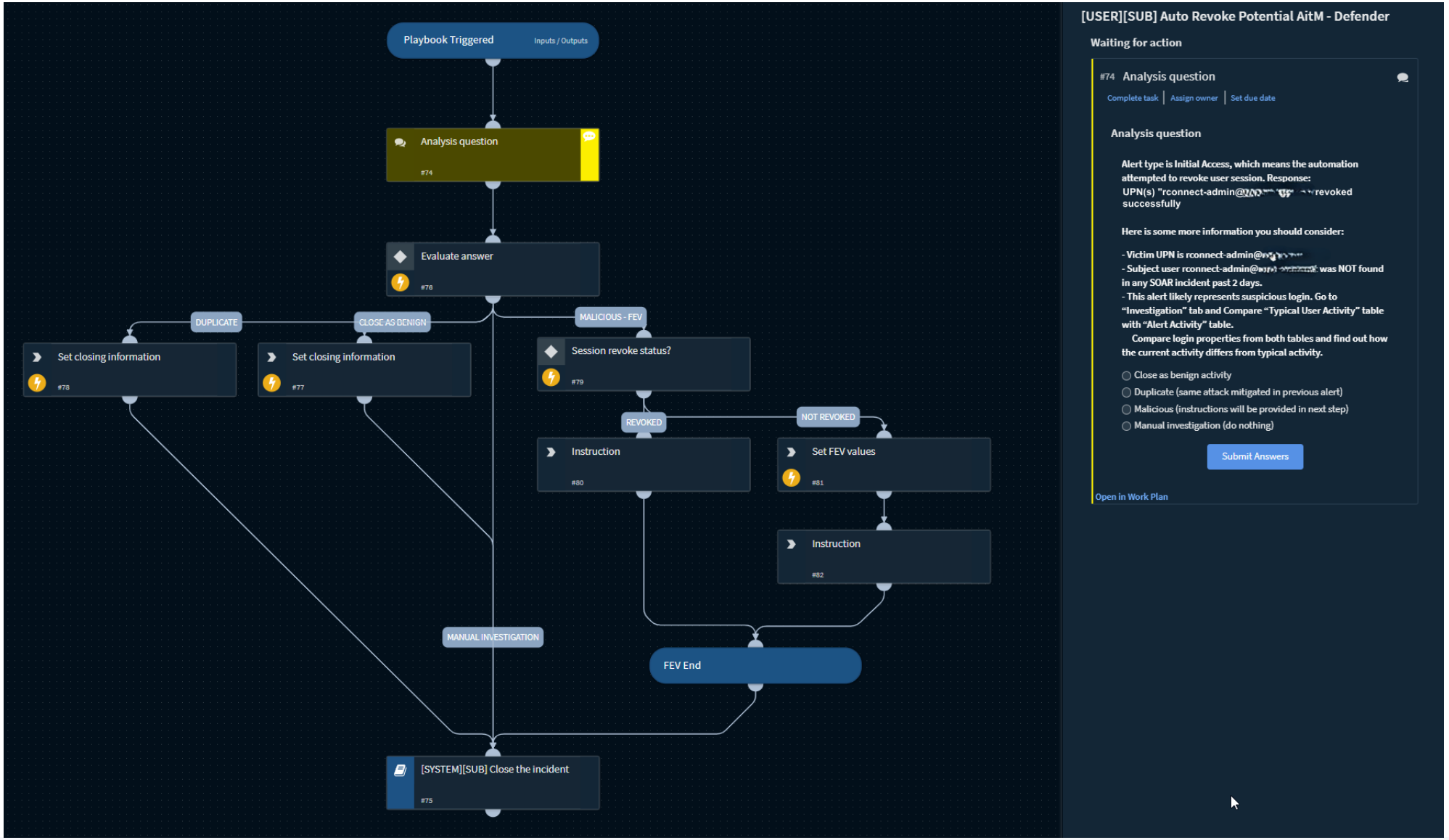
Potek raziskave in mitigacija AiTM napadov z avtomatizacijo

Zaznava od 48ur do **10 min** z WardenGate

Avtomatko brisanje aktivnih sej v Entra ID – **1min**

Avtomatski baseline za uporabnika, predstavitev podatkov analitiku, odločanje/potrjevanje napada. – **do 5 min**

Kreiranje Inciden reporta, obveščanje stranke - **1min**



Razultati avtomatizacije v praksi

Wildfire Malware

- Pred avtomatizacijo 13 min nato 4min
- Število alarmov mesečno: 200
- Prihranek: 26 ur na mesec.

Brand Protection

- Pred avtomatizacijo 3.5 min nato 35 sek.
- Število alarmov mesečno : 300
- Prihranek: 15 ur na mesec.

AiTM napadi

- Pred avtomatizacijo 35 min nato 17min
- Število alarmov mesečno : cca 385
- Prihranek: 115 ur na mesec.

Zaključne misli

Boljša kvaliteta

Hitrejša detekcija in odziv

Napadalci svoje napade avtomatizirajo, kako bomo mi obrambo?

WOMEN 4CYBER
EUROPEAN CYBER SECURITY ORGANISATION
SLOVENIA

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

NIL
part of conscia

IT for a Better Life

nil.com

KIBERNETSKI CUNAMI

Ali smo pripravljeni na spremembe ZInfV?

Ali smo pripravljeni na spremembe ZInfV?

Novi pristopi k testiranju kibernetske varnosti in obvladovanju tveganj

Grega Prešern

CTO, Carbonsec d.o.o.

Novi pristopi k testiranju kibernetske varnosti in obvladovanju tveganj

Grega Prešeren

CARBONSEC
CYBERSECURE YOUR BUSINESS

FORBES > INNOVATION > CYBERSECURITY

It's 2024 And Now Bicycle Hackers Can Shift Your Gears

Davey Winder Senior Contributor

Davey Winder is a veteran cybersecurity writer, hacker and analyst.

Follow

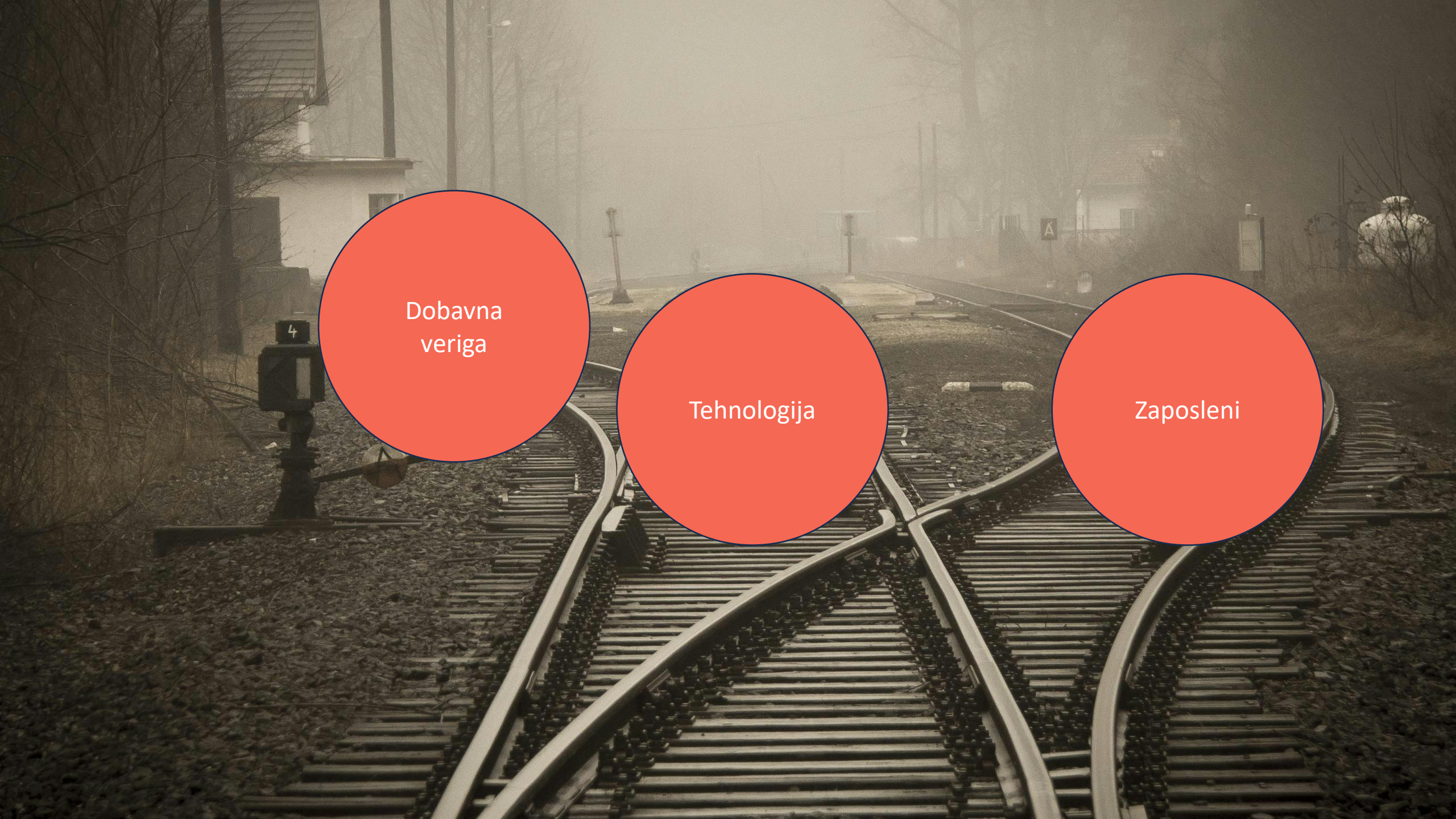
Aug 28, 2024, 10:17am EDT

Updated Aug 29, 2024, 06:58am EDT

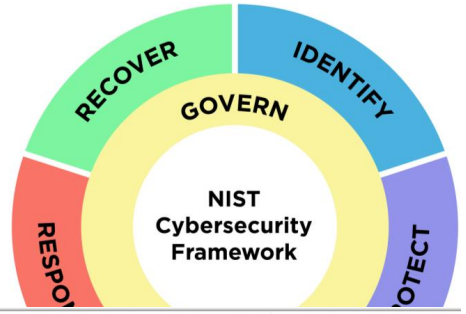
Vir: Forbes

CARBONSEC

Figure 1: Shimano's RF communication.


Dobavna veriga
Tehnologija
Zaposleni

Skladnost s priznanimi ogrodji



	A	B	C	D	E	F	G	H	I	J	K
1	CSF Outcome (Function, Category, or Subcategory)	CSF Outcome Description	Included in Profile?	Rationale	Current Priority	Current Status	Current Policies, Processes, and Procedures	Current Internal Practices	Current Roles and Responsibilities	Current Selected Informative References	Current Artifacts and Evidence
29	GV.SC	Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders									
30	GV.SC-01	A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders									
31	GV.SC-02	Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally									
32	GV.SC-03	Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes									
33	GV.SC-04	Suppliers are known and prioritized by criticality									

Yes
No

CARBONSEC

Vir: NIST

Skladnost s priznanimi ogrodji

	A	B	C	D	E	F	G	H	I	J	K
1	CSF Outcome (Function, Category, or Subcategory)	CSF Outcome Description	Included in Profile?	Rationale	Current Priority	Current Status	Current Policies, Processes, and Procedures	Current Internal Practices	Current Roles and Responsibilities	Current Selected Informative References	Current Artifacts and Evidence
61	ID.IM-01	Improvements are identified from evaluations									
62	ID.IM-02	Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties									
63	ID.IM-03	Improvements are identified from execution of operational processes, procedures, and activities	Yes / No								
64	ID.IM-04	Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved									

CARBONSEC

Vir: NIST

Skladnost s priznanimi ogrodji

PROFILE
CYBER RISK INSTITUTE

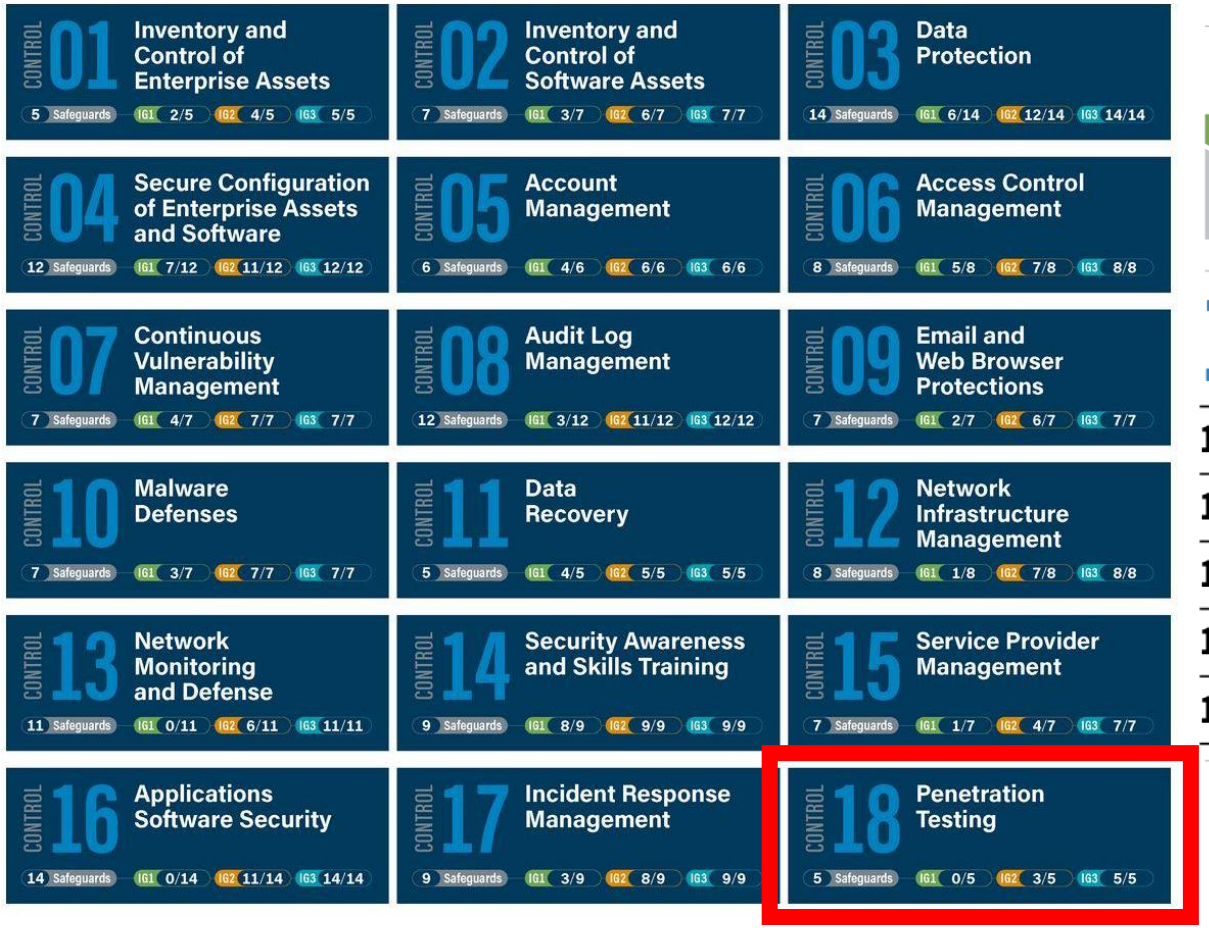
CRI Profile ver. 2.0 Structure View

Outline Id	Level	Profile Id	CRI Profile v2.0 Diagnostic Statement	Tier-1	Tier-2	Tier-3	Tier-4	NIST CSF v2 Mapping	FS References
065.143	DS	ID.IM-02.01	**ID.IM-02.01:** The organization conducts regular, independent penetration testing and red team testing on the organization's network, internet-facing systems, critical applications, and associated controls to identify gaps in cybersecurity defenses.	Yes	Yes	Yes	Yes	ID.IM-02	EBA (1), ECB (13), FFIEC AIO (1), FFIEC CAT (7), JFSA (2), MAS (4), NYDFS (2), OCC (2)
065.144	DS	ID.IM-02.02	**ID.IM-02.02:** The thoroughness and results of independent penetration testing are regularly reviewed to help determine the need to rotate testing vendors to obtain fresh independent perspectives.	Yes	Yes	Yes	No	ID.IM-02	EBA (6), ECB (2), FFIEC CAT (1), JFSA (2), MAS (1)
065.145	DS	ID.IM-02.03	**ID.IM-02.03:** The organization tests and validates the effectiveness of the incident detection, reporting, and communication processes and protocols with internal and external stakeholders.	Yes	Yes	Yes	No	ID.IM-02	EBA (1), ECB (5), FFIEC AIO (2), FFIEC BCM (5), FFIEC CAT (2), JFSA (2), MAS (2), OCC (2)
065.146	DS	ID.IM-02.04	**ID.IM-02.04:** The organization's testing program validates the effectiveness of its resilience strategy and response, disaster recovery, and resumption plans on a regular basis or upon major changes to business or system functions, and includes external stakeholders as required.	Yes	Yes	Yes	Yes	ID.IM-02	EBA (2), ECB (6), FFIEC AIO (3), FFIEC BCM (21), FFIEC CAT (2), JFSA (3), MAS (2), NYDFS (2), OCC (2)
065.147	DS	ID.IM-02.05	**ID.IM-02.05:** The organization establishes testing programs that include a range of scenarios, including severe but plausible scenarios (e.g., disruptive, destructive, corruptive), that could affect the organization's ability to service internal and external stakeholders.	Yes	Yes	Yes	Yes	ID.IM-02	EBA (7), ECB (12), FFIEC AIO (1), FFIEC BCM (14), FFIEC CAT (7), JFSA (7), MAS (5), NYDFS (1), OCC (1)
065.148	DS	ID.IM-02.06	**ID.IM-02.06:** The organization designs and tests its systems and processes, and employs third-party support resources (e.g., Sheltered Harbor), to enable recovery of accurate data (e.g., material financial transactions) sufficient to support defined business recovery time and recovery point objectives.	Yes	Yes	Yes	Yes	ID.IM-02	EBA (8), ECB (10), FFIEC AIO (2), FFIEC BCM (22), FFIEC CAT (4), JFSA (3), MAS (3), NYDFS (4), OCC (2)
065.149	DS	ID.IM-02.07	**ID.IM-02.07:** The organization's governing body (e.g., the Board or one of its committees) and senior management are involved in testing as part of a crisis management team and are informed of test results.	Yes	Yes	No	No	ID.IM-02	EBA (4), ECB (3), FFIEC AIO (1), FFIEC BCM (8), FFIEC CAT (1), JFSA (2), MAS (2)

CARBONSEC

Vir: Cyber Risk Institute (CRI)

Skladnost s priznanimi ogrodji



IG1 is the definition of essential cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.

56
Cyber defense Safeguards

18 Penetration Testing

18.1	Establish and Maintain a Penetration Testing Program	●	●
18.2	Perform Periodic External Penetration Tests	●	●
18.3	Remediate Penetration Test Findings	●	●
18.4	Validate Security Measures		●
18.5	Perform Periodic Internal Penetration Tests		●

Total Safeguards 153

CARBONSEC

Vir: CIS

Regulativa (ne le ZInfV-1)

Tehnologija

ZInfV-1

- **5. člen**
- **(pomen izrazov)**

- 65. Varnostni pregled je postopek, v katerem inšpektor pri zavezancu v postopku inšpekcijskega nadzora izvede identifikacijo in oceno morebitnih ranljivosti v omrežnih in informacijskih sistemih, izvede preizkus učinkovitosti varnostnih ukrepov oziroma mehanizmov in izpostavljenosti kibernetskim grožnjam ter preveri ustreznost izvajanja učinkovitega zaznavanja in obravnavanja kibernetskih incidentov.

Kaj je varnostni pregled?

- Storitve kibernetske varnosti
  - VARNOSTNI PREGLED (SECURITY ASSESSMENT, ETHICAL HACKING)
    - REVIZIJSKI PREGLED (SECURITY AUDIT)
    - PREGLED RANLJIVOSTI, SISTEMSKI VARNOSTNI PREGLED (VULNERABILITY ASSESSMENT, VULNERABILITY SCANNING)
    - PENETRACIJSKO (VDORNO) TESTIRANJE (PENETRATION TESTING)
    - KIBERNETSKA VAJA (RED TEAMING, PURPLE TEAMING)

Vir: GZS

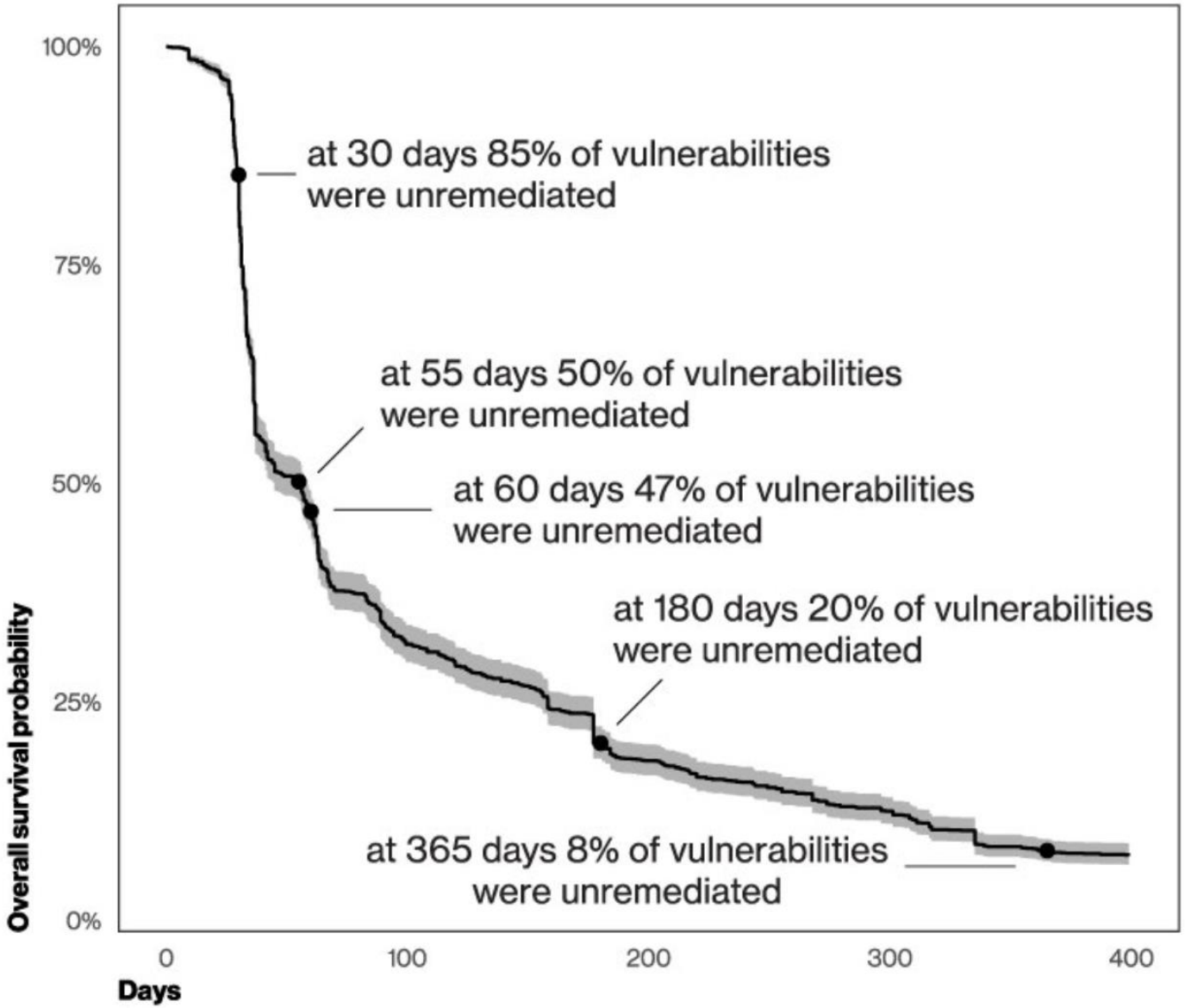


Figure 19. Survival analysis of CISA KEV vulnerabilities

Vir: DBIR

CARBONSEC

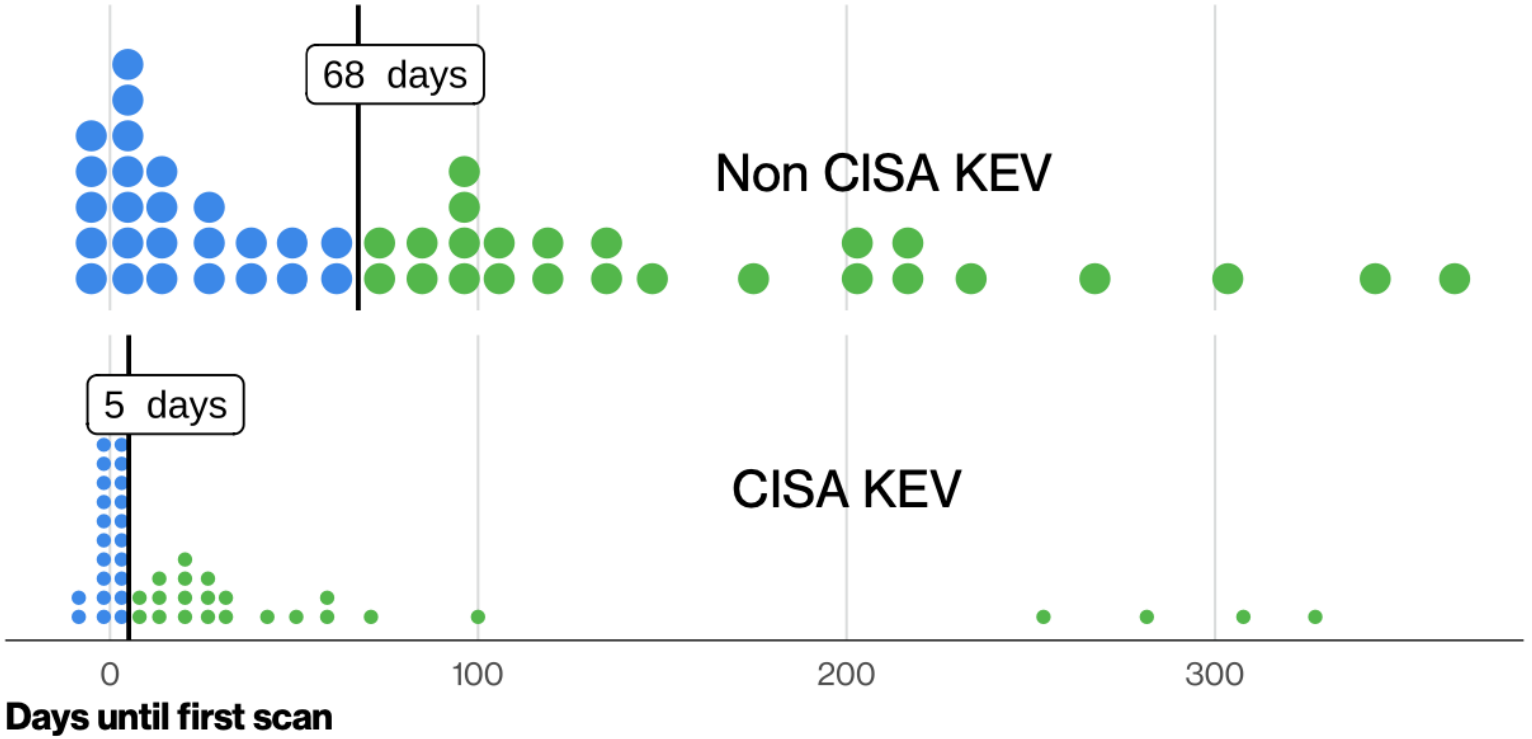
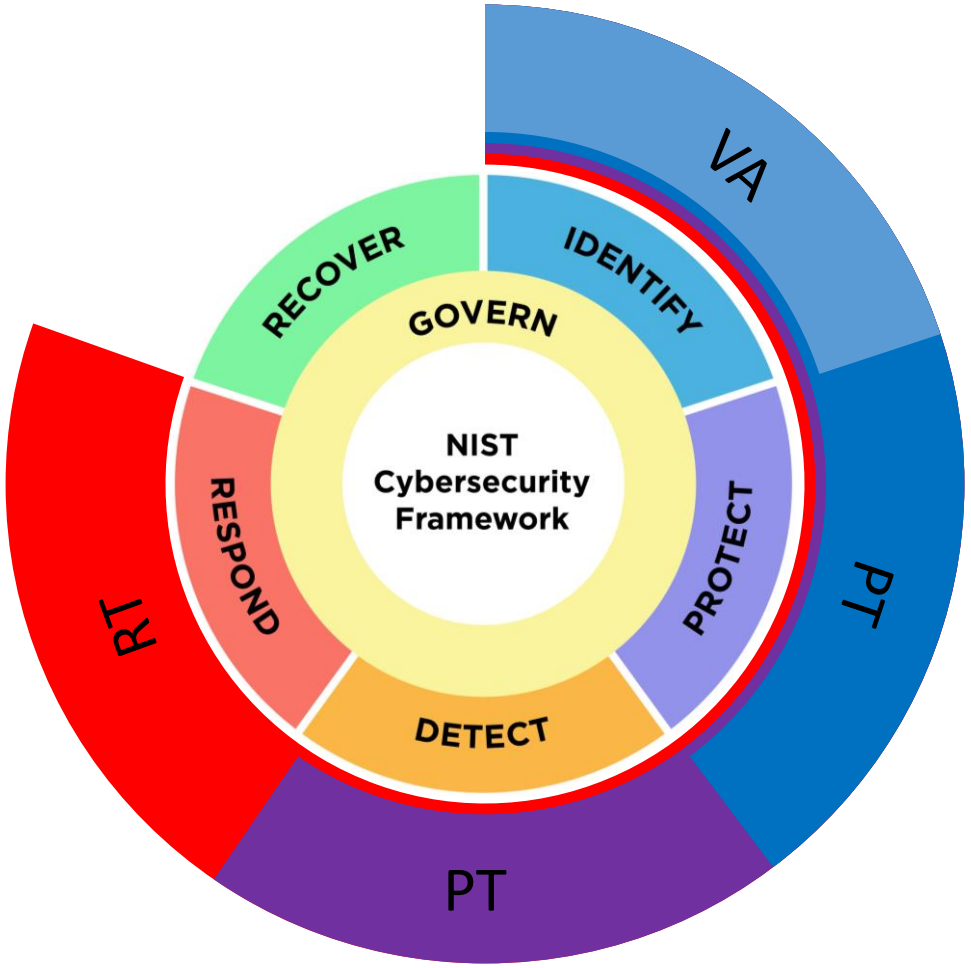


Figure 20. Time from publication of vulnerability to first scan seen (from 2020 onward)

Vir: DBIR

CARBONSEC


VA
PT
PT
RT
RECOVER
IDENTIFY
GOVERN
NIST
Cybersecurity
Framework
RESPOND
PROTECT
DETECT

DORA

- Člen 26
- Napredno testiranje orodij, sistemov in postopkov IKT na podlagi penetracijskega testiranja na podlagi analize groženj
  - 1. Finančni subjekti, ki niso mikropodjetja ter so opredeljeni v skladu z odstavkom 8, tretji pododstavek, tega člena vsaj vsaka tri leta izvedejo napredno penetracijsko testiranje na podlagi analize groženj. Na podlagi profila tveganja finančnega subjekta in ob upoštevanju operativnih okoliščin lahko pristojni organ po potrebi od finančnega subjekta zahteva, da to stori manj ali bolj pogosto.

TLPT

CARBONSEC

Vhodni parametri varnostnega pregleda

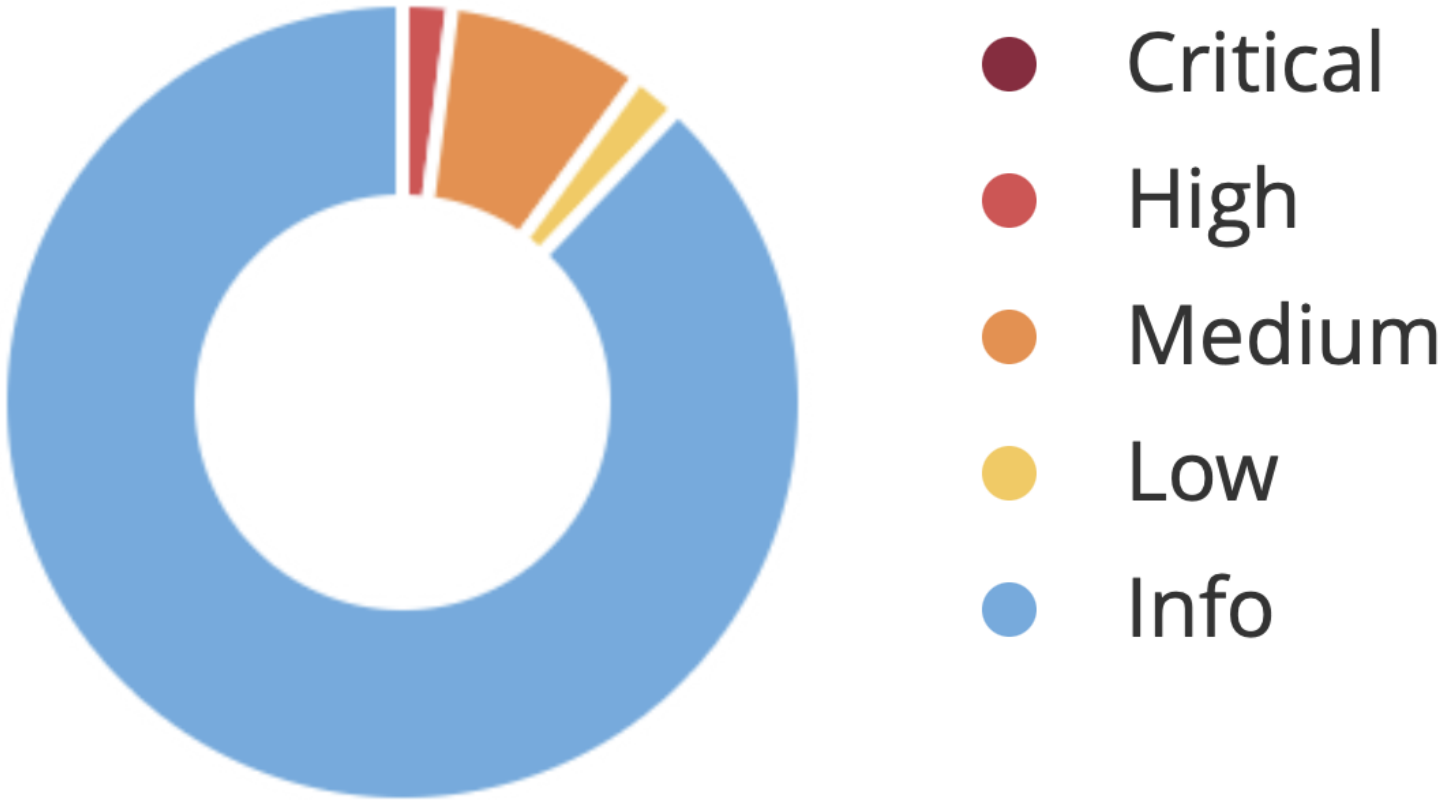
- Obseg
- Metodologija
- Način izvedbe (ročno, avtomatizirano)
- Pristop k testiranju (črna, siva, bela škatla)
- Omejitve
  - Delo v času, ko ni tipičnih aktivnosti
  - Prepoved izrabe odkritih ranljivosti
    - Povišanje privilegijev
    - Bočni, vertikalni premiki

2 HIGH RISKS

- CLEARTEXT SQLITE DATABASE [DAST] [M2] [CWE-312]

- USAGE OF UNENCRYPTED HTTP PROTOCOL [SAST] [M3] [CWE-319]
  - HttpsURLConnection conn = (HttpsURLConnection) url.openConnection();

Vulnerabilities



Zaposleni


TRUST
ACCOUNT
OPERATIVE
PERSONAL
PHISHING
TARGET
SOCIAL
PSYCHOLOGICAL
ACCESS
INFORMATION
STRATEGIC
GATHERING
PEOPLE
ENGINEERING
MANAGE
PLANNING
SECURITY
MANIPULATION
COUNTERMEASURE
ATTACK
FRAUD
CONFIDENTIAL
AUTHENTICATION
SYSTEM

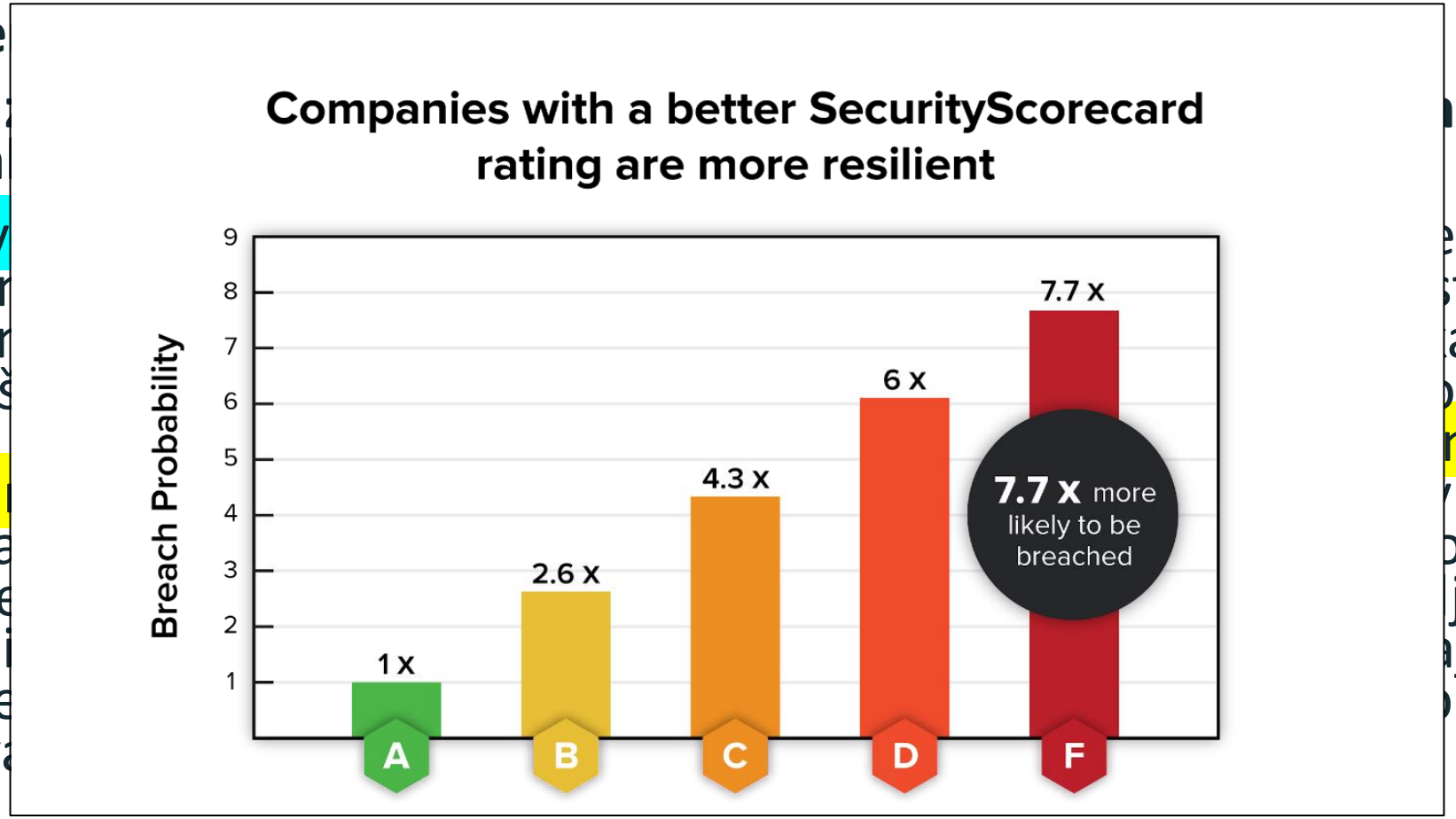
Vir: KnowBe4

CARBONSEC

Dobavna veriga

ZInfV-1

- **21. čle**
- **(ukrepi**
  pomem
- (5) Bistv
  varnostr
  specifičr
  ter splošn
  storitev
  razvojni
  kateri va
  dobavne
  ponudni
  ocen tve
  sodelova

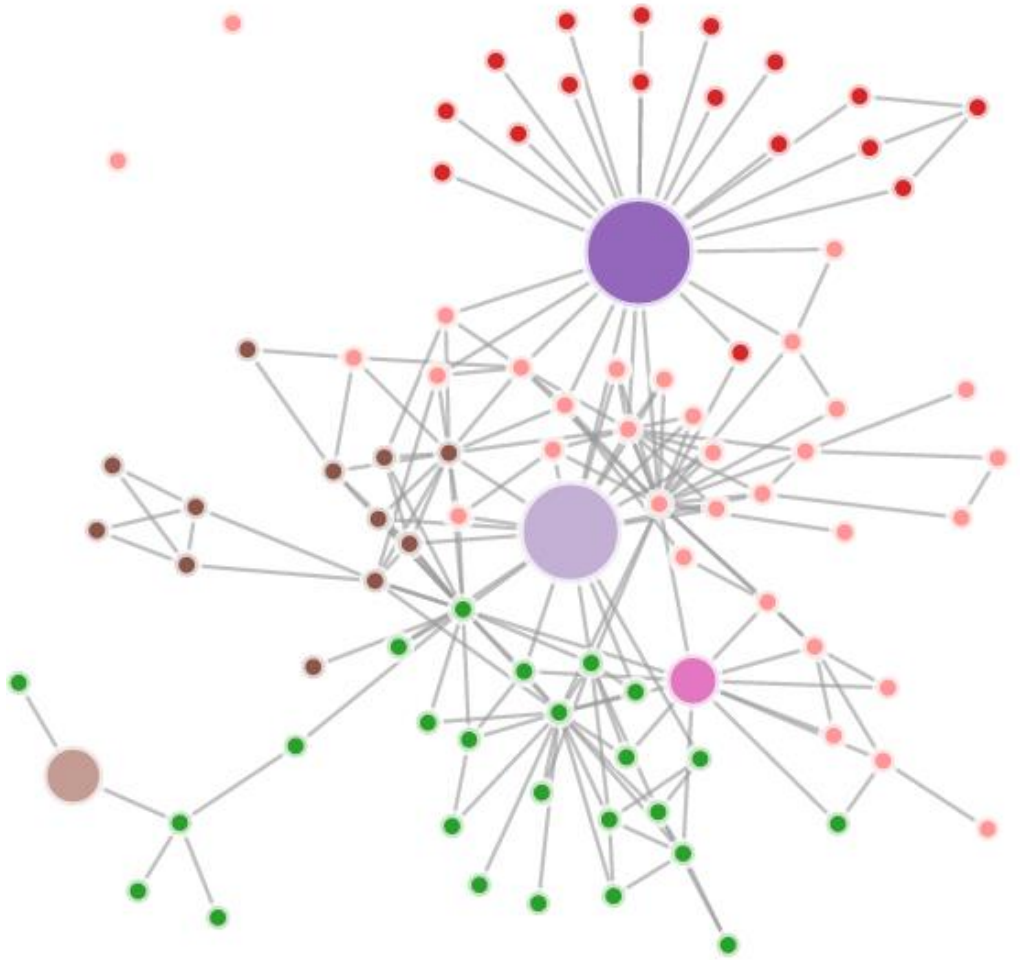


in

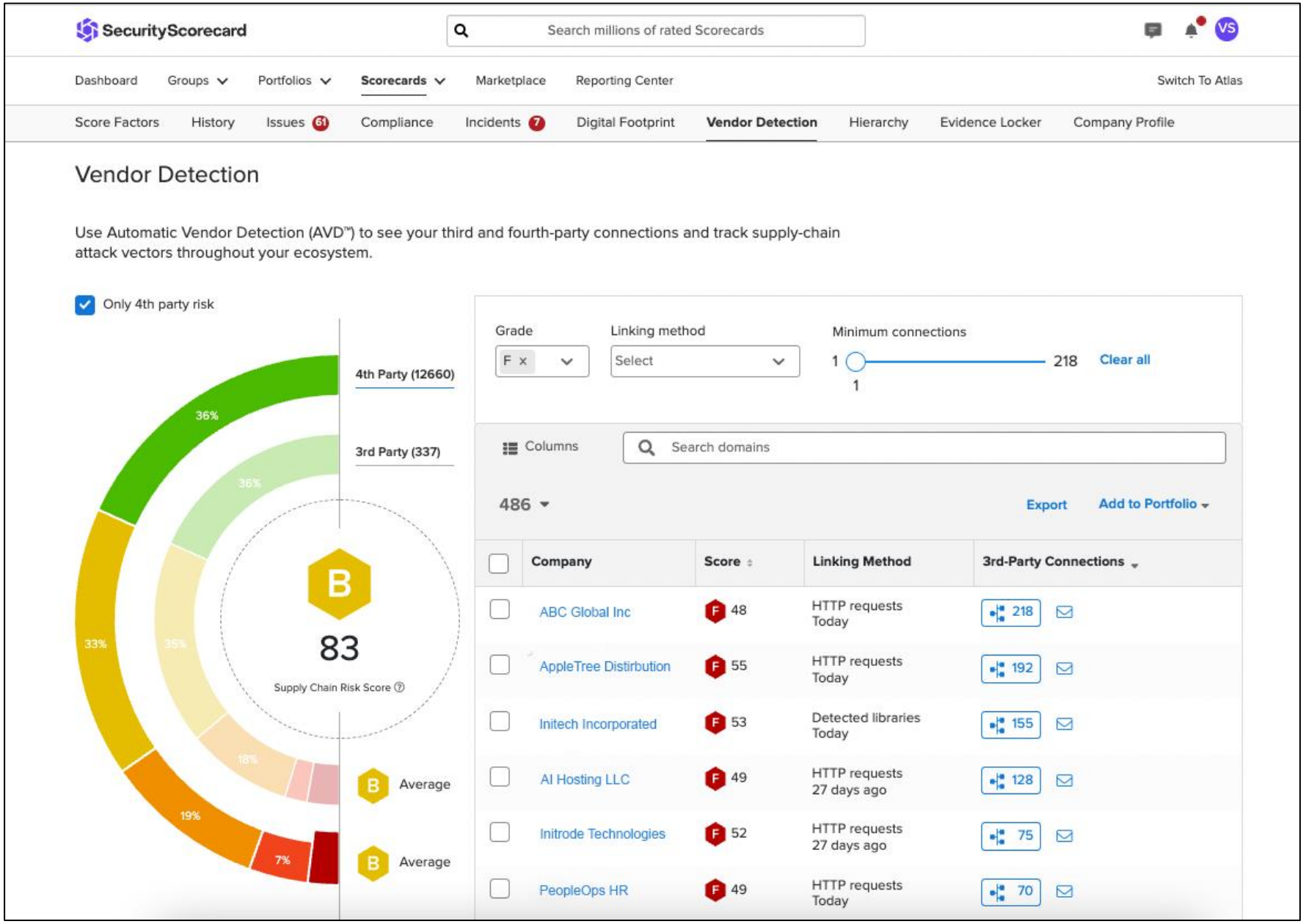
eznih
sti, ki so
a storitev
onudnikov
nimi
vljati
osti
jih in
ajenih
oina za

CARBONSEC

N-ti dobavitelji



CARBONSEC


SecurityScorecard
Search millions of rated Scorecards
VS
Dashboard
Groups
Portfolios
Scorecards
Marketplace
Reporting Center
Switch To Atlas
Score Factors
History
Issues 61
Compliance
Incidents 7
Digital Footprint
Vendor Detection
Hierarchy
Evidence Locker
Company Profile
Vendor Detection
Use Automatic Vendor Detection (AVD™) to see your third and fourth-party connections and track supply-chain attack vectors throughout your ecosystem.
Only 4th party risk
4th Party (12660)
3rd Party (337)
36%
36%
33%
35%
18%
19%
7%
B
83
Supply Chain Risk Score
B Average
B Average
Grade
F ×
Linking method
Select
Minimum connections
1
218
1
Clear all
Columns
Search domains
486
Export
Add to Portfolio
Company
Score
Linking Method
3rd-Party Connections
ABC Global Inc
F 48
HTTP requests Today
218
AppleTree Distirbution
F 55
HTTP requests Today
192
Initech Incorporated
F 53
Detected libraries Today
155
AI Hosting LLC
F 49
HTTP requests 27 days ago
128
Initrode Technologies
F 52
HTTP requests 27 days ago
75
PeopleOps HR
F 49
HTTP requests Today
70

CARBONSEC

Varnost je del odpornosti

Metodološko je objektivno

info@carbonsec.com

CARBONSEC

CYBERSECURE YOUR BUSINESS

KIBERNETSKI CUNAMI

Ali smo pripravljeni na spremembe ZInfV?

Ali smo pripravljeni na spremembe ZInfV?

Odgovor na izzive trga dela: Od Cyber kampa do študijskiega programa

dr. Laura Fink

Gea College – Fakulteta za podjetništvo

geacollege

Odgovor na izzive trga dela:

Od Cyber kampa do študijskega programa

Dr. Laura Fink

IZSTOPAJOČE ŠTEVILKE 2023

si·cert

4.280 obravnavanih incidentov (4% rast v primerjavi z 2022)

več kot **1.600** primerov phishing napadov

na platformi MISP dodanih več kot **35.000** novih dogodkov

okoli **150** kripto-investicijskih prevar

5.158 izdanih certifikatov tečaja Varni v pisarni

162 novinarskih vprašanj

več kot **50** izpeljanih predavanj na različne teme kibernetske varnosti

slovenska policija zabeleži

27,5 milijonov € škode v različnih spletnih goljufijah

največji porast je **v kategoriji investicijskih prevar**

kar 13 milijonov € škode

51 primerov **»BEC« prevar** (vrivanje v poslovno komunikacijo), ki slovenskim podjetjem povzročijo za

7,8 milijonov € škode

2,4 milijona € škode zaradi nedostavljenih izdelkov pri spletnem nakupovanju (večinoma lažne spletne trgovine)

800.000 € škode zaradi ljubezenskih prevar in

3,5 milijona € zaradi **phishing zlorab v elektronskem bančništvu**

INFORMACIJSKI POOBLAŠČENEC

Informacijski pooblaščenec prejme **183 uradnih obvestil o kršitvi varnosti** (Data Breach Notification)

Vir: Nacionalni odzivni center za kibernetsko varnost SI - CERT - Poročilo o kibernetski varnosti 2023

Primanjkljaj usposobljenih strokovnjakov

Vse analize kažejo, da se potrebe po strokovnjakih za kibernetsko varnost povečujejo veliko hitreje kot število usposobljenih kadrov.

V EU bomo kmalu potrebovali **milijon takih strokovnjakov** (v letu 2022 je bilo ocenjeno, da EU potrebuje **883 tisoč strokovnjakov** s področja kibernetske varnosti, po ocenah je primanjkljaj med 260 tisoč in 500 tisoč.

vir: Cybesecurity Skills Academy

Informacijska in kibernetska varnost (IKV)

Dodiplomski študijski program

- **Vrsta programa:** dodiplomski visokošolski strokovni program
- **Trajanje študija:** 3 leta (180 kreditnih točk)
- **Pridobljen strokovni naslov:** diplomiran inženir/diplomirana inženirka informacijske in kibernetske varnosti (VS); okrajšava: dipl. inž. info. varn. (VS)
- **Način študija:** Izredni (klasični študij)

Zakaj študirati IKV?

- Strokovnjaki na tem področju so zaradi velikega povpraševanja **med najbolj iskanimi kadri.**
- Program nudi uporabna in napredna znanja, potrebna za učinkovito **odzivanje na incidente**, kot so vdori v strežnik ali okužbe računalnikov.
- Študij omogoča **razvoj veščin za zaščito sistemov**, sanacijo, odpravo škode in iskanje storilcev.
- Predavanja izvajajo **strokovnjaki z dolgoletnimi izkušnjami** iz različnih področij informacijske in kibernetske varnosti.

CYBER KAMP za dijake

Varnost in hekanje

Poletni Cyber kamp predstavlja izjemno priložnost za mlade, da se ne le podučijo o **zaščiti pred spletnimi napadi**, temveč **spoznajo področje kibernetske varnosti**, ki je trenutno eno izmed najbolj cenjenih na trgu dela.

Udeleženci skozi **interaktivne simulacije, praktične vaje** in **delavnice** pridobijo neprecenljive izkušnje in ob tem stkejo nova prijateljstva.

CYBER KAMP za dijake

Za prihodnost

Osvojiti znanje in biti pripravljen/a na prihodnje izzive v svetu kibernetske varnosti in tehnologije.

Praktične izkušnje

Učenje skozi prakso s simulacijami, vajami in delavnicami.

Zabava in učenje

Spoznati nove prijatelje, ki delijo enake interese, in se zabavati med pridobivanjem novega znanja.

geacollege

Hvala za pozornost

Več o programu:

Informacijska in kibernetska varnost

KIBERNETSKI CUNAMI

Ali smo pripravljeni na spremembe ZInfV?

ZLATI PARTNER

ORGANIZATORJI

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

CyberHubs Slovenia

FutuResilience
Building sustainable futures together

SlovenianCyberResilienceLab
Part of FutuResilience consortium

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101094455.

CyberHubs
Co-funded by the European Union

I FEEL SLOVENIA

SRIP GoDigital

Sofinancira Evropska unija

Naložbo sofinancira Evropska unija iz evropskega sklada za regionalni razvoj

KIBERNETSKI CUNAMI

Ali smo pripravljeni na spremembe ZInfV?