CSIRT UPJS

AGH UNIVERSITY CYBERSECURITY CENTRE

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

SOCCER

13.06.2024

Akademické bezpečnostné tímy Projekt SOCCER

UNINFOS 2024

Pavol Sokol

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH 1795 1861 1959

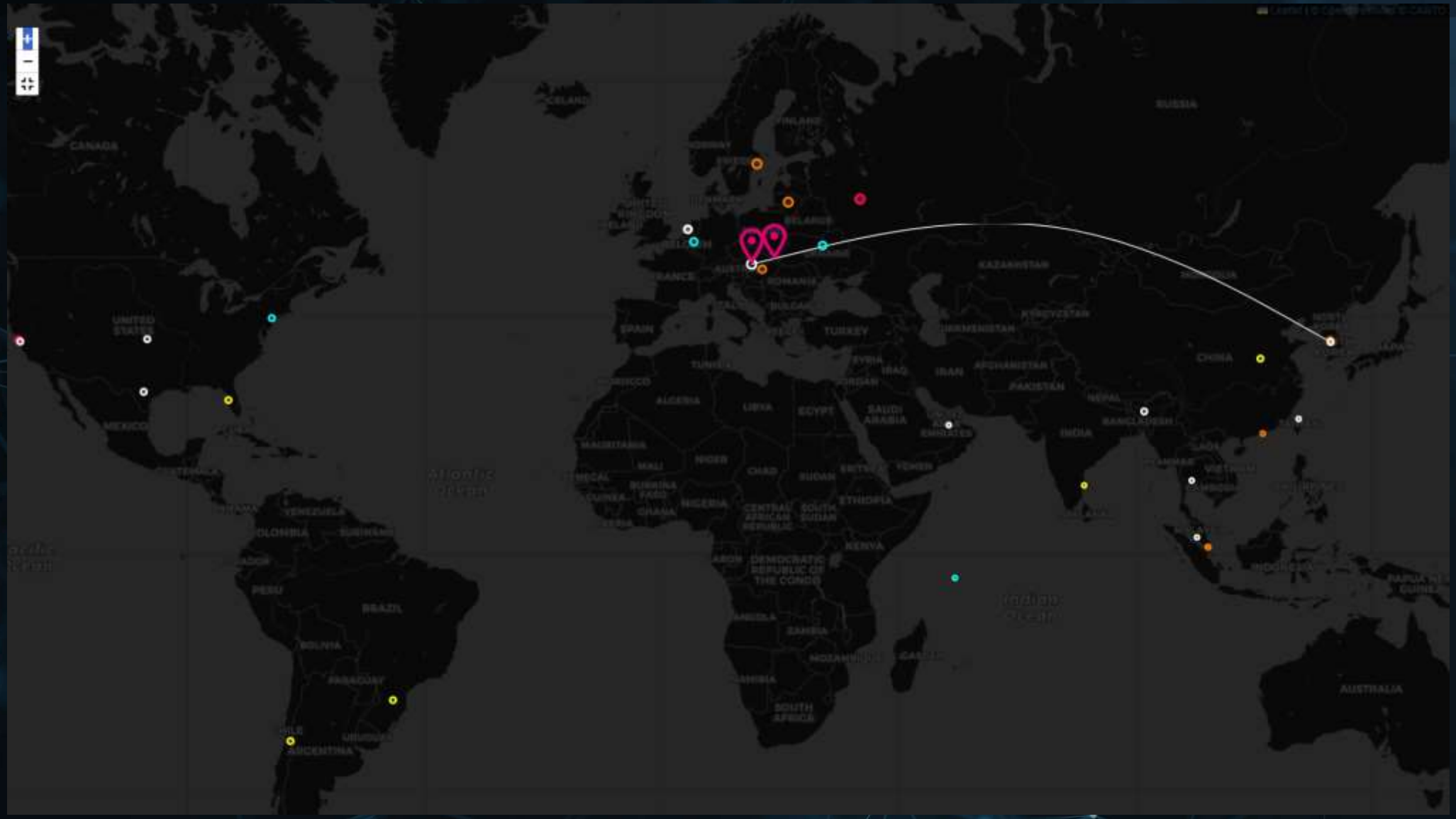
CSIRT UPJS

AGH UNIVERSITY CYBERSECURITY CENTRE

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

SOCCER



Projekt SOCCER (I.)

- Developing and deploying SOC capabilities for the academic sector – a teamwork of Universities and RTOs in the CEE region

- SOC v regióne strednej a východnej Európy (SOCCER)
- Program: Digitálna Európa - DIGITAL-ECCC-2022-CYBER-03-SOC

- 10/2023 – 9/2026

Projects funded under this topic

Found 16 record(s)

Search...

TITLE	ACRONYM	PROJECT ID
Irish Local Government Security Operations Centre	ILG-SOC	101127862
Cyber Threat Intelligence Operations Centre (CTIOC), development & automation of key CTI collection/monitoring/analysis capabilities for National and European financial sector intelligence enrichment.	CTIOC	101128107
Greek Security Operations Centre for Small and Medium Enterprises	GR-SME-SOC	101128028
Establishing Cross-border SOCs	ATHENA	101127968
Developing and deploying SOC capabilities for the academic sector - a teamwork of Universities and RTOs in the CEE region	SOCCER	101128073
Improving SOITRON's SOC capabilities and capacities through building state-of-the-art detection platform SOCulus	SOCulus project	101127851
Enhancing the capacity of the Hellenic Consolidated Security Operation Center	EL-SOC	101127713
Cypriot Sectorial Security Operations Centres	CY-TRUST	101128017

Projekt SOCCER (II.)

- Zameranie: operatívne činnosti, nie výskumná činnosť
- Hlavné ciele projektu:
  - vytvorenie a podpora SOC a iných tímov v akademickom prostredí
  - zdieľanie CTI informácií
  - spolupráca

CSIRT UPJS

AGH UNIVERSITY CYBERSECURITY CENTRE

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

SOCCER

Projektový tím

AGH AGH University of Krakow

JAGIELLONIAN UNIVERSITY IN KRAKÓW

UNIVERSITY OF AGRICULTURE IN KRAKOW

Tomas Bata University in Zlín

MUNI Masaryk University

PAVOL JOZEF ŠAFÁRIK UNIVERSITY IN KOŠICE

MRU Mykolas Romeris University

TARTU ÜLIKOOL 1632 UNIVERSITAS TARTUENSIS

cesnet

. External Expert Advisory Board:

ECS EUROPEAN CYBER SECURITY ORGANISATION

Open CSIRT Foundation

CSIRT.CZ

IstroSec

CSIRT UPJS

AGH UNIVERSITY CYBERSECURITY CENTRE

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

SOCCER

Vytvorenie a podpora SOC / SOC schopností

- SOC / SOC schopností v rámci bezpečnostných tímov (CSIRT)
- tvorba SOC4Academia toolbox
- tvorba materiálov pre SOC pripravenosť
- implementácia SOC alebo schopností SOC na univerzitách a v RTO v strednej a východnej Európe

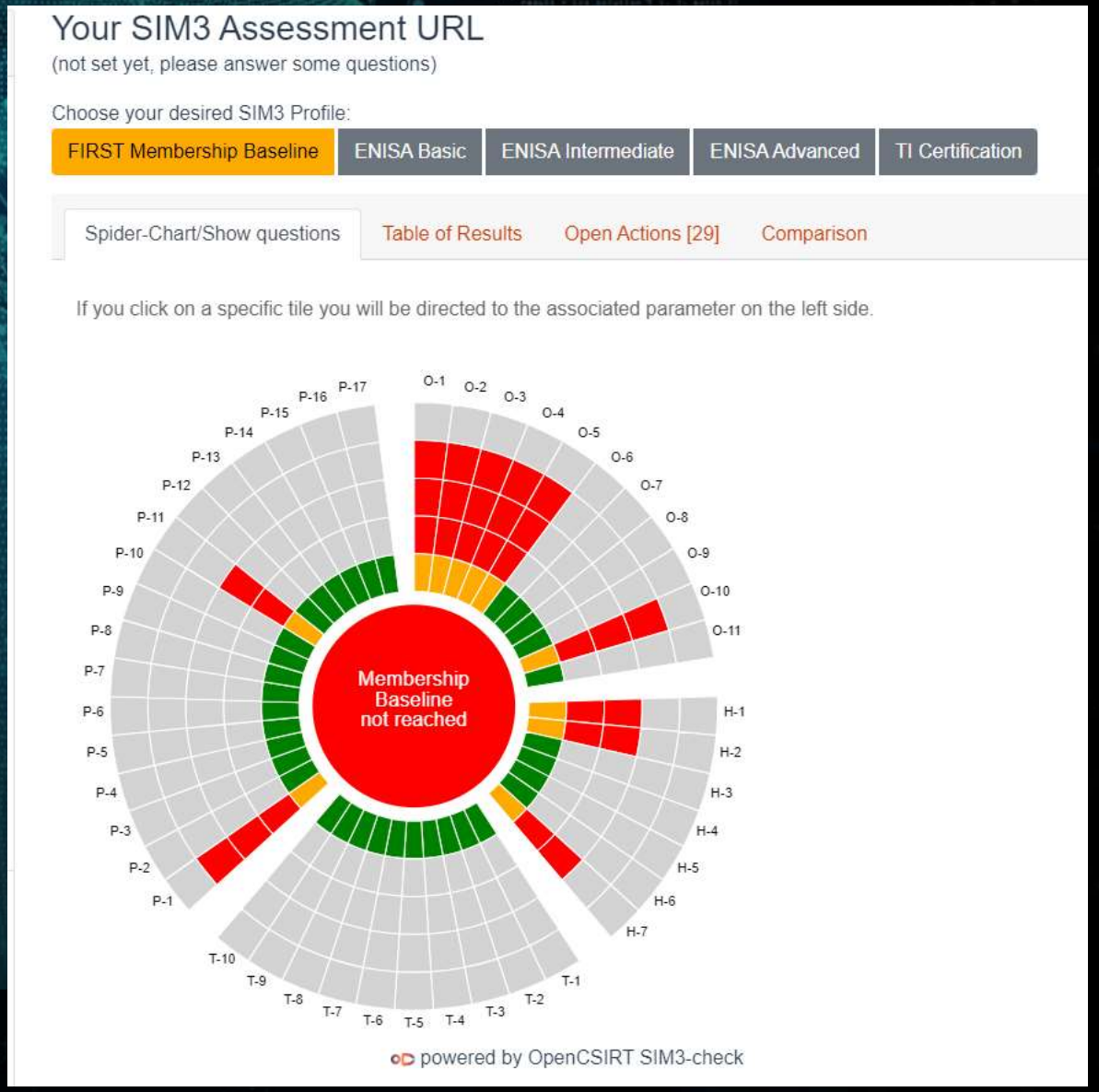
CSIRT UPJS | AGH UNIVERSITY CYBERSECURITY CENTRE | Co-funded by the European Union | ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE | SOCCER

SOC4Academia Toolbox (I.)

- Modely SOC pre akademické prostredie
  - prehodnocovanie existujúcich modelov a architektúr SOC
  - umiestnenie SOC v organizačnej štruktúre
  - možnosti implementácie SOC
- Definovanie požiadaviek (technických, právnych, personálnych) na budovanie SOC4Academia

SOC4Academia Toolbox (II.)

- Modely vyspelosti pre SOC
  - definovanie úrovní schopností a vyspelosti
  - napojenie na model SIM3 pre akademické CSIRT a SOC
  - požiadavky na organizáciu a prostredie SOC pre akademickú oblasť



SOC4Academia Toolbox (III.)

- Tvorba Digital Forensics and Incident Response (DFIR) manuálov
  - metodológia, nástroje, osvedčené postupy
  - šablóny a vzorky politík a postupov
  - prehľad softvérových a hardvérových riešení

- DIFR manuály pre:
  - IR: ransomvér, únik údajov, malvér, sociálne inžinierstvo
  - FA: základná metodológia, zaisťovanie digitálnych stôp, analýza forenzných artefaktov – Windows, Linux, MacOS, Android

SOC4Academia Toolbox (IV.)

Team Logo

Security incident report

CSIRT-2024-BI-001

TLP:AMBER / TLP:RED

University logo

Team Logo

Managerial summary

Security Incident (Title / designation of incident)

This report includes a list of compromise indicators (Appendix A) and several security measures that, as part of proactive organizational activities, could prevent the occurrence of similar security incidents or mitigate the impact of these incidents on the organization.

[Incident description - what happened, when, and what were the consequences]

Security incident response

As part of the security incident response, a security incident response was performed on the compromised device. It included an inspection of the device in question, identification of the method of compromise of the device, as well as the individual actions of the attacker. Further information on the security incident response is provided in the following sections:

- Security incident resolution timeline,
- methodology,
- findings and
- analysis of digital traces and other information.

Timeline of the security incident response

Several important events were identified as part of the security incident response. Within this section (Table 1), we provide a timeline of the security incident, including the activities of the entities relevant to the resolution. Relevant email communications are provided in Appendix B.

KAPE and DFIR

KAPE is an efficient and highly configurable triage program that will target essentially any device or storage location, find forensically valuable artifacts, and parse them within a few minutes. [1] **The key feature of the tool is triage**, whether it is performed on a turned-on or turned-off device. This capability is invaluable in time-sensitive situations or when dealing with large volumes of data. It also works for remote data acquisition if the incident responder has access to the remote computer.

KAPE can be used to seize memory, extract most valuable forensic artifacts, and apply parsers. It can be a valuable tool even if full disk imaging needs to be done, since KAPE can quickly offer an insight into the security incident.

When executing KAPE, it provides a log file, which includes all commands executed, the time of execution and possible errors. This can be used to describe process of evidence collection, ensuring compliance with forensic best practices without the need to manually mark down every step and its timestamp.

Using KAPE

KAPE can be run from command line (kape.exe) with administrator privileges or from GUI (gkape.exe). In this guide, we will focus on the GUI version, which, in the end, provides a complete command that can be executed manually.

Figure X.1 shows gkape.exe window. It contains two main sections - one for configuring targets (left side) and one for modules (right side), and one section on the bottom for displaying final command to be executed.

Figure 1 - Graphical interface of KAPE

[1] https://www.kroll.com/en/insights/publications/cyber/kroll-artifact-parser-extractor-kape

Target options

When "**Use Target options**" is selected, source and destination folders need to be defined (Figure X.2, no. 1.). The **Target source** is the disk partition of a mounted image or a partition of a live system. A specific folder can be selected as well. The **Target destination** is usually an empty disk for data acquisition, or a folder on incident responder's laptop.

In Figure X.2 no. 2. are three options, which can be used based on specific conditions. The "**Flush**" checkbox clears the Target destination before anything else is done. Option "**Add %d**" allows to add a timestamp to the destination folder (for uniqueness) and option "**Add %m**" adds a machine name to the destination folder (when more devices are being examined).

Figure 2 - Main Target options

No. 3 marks a list of all available targets. It is possible to search through them by typing into an "ABC" marked line. After double-clicking on any of the targets, an editor of the target will open. It is possible to choose from several output formats, as seen in Figure X.2, no. 4. The option "None" will copy folders and files as they are in the source file system. Other options require the "**Base name**" to be filled in. It is recommended to use the source machine's name. When creating own targets, it is possible to mark a variable in it. The variable is surrounded by %, e.g., C:\Users\%user%\ has a variable named "user". These variables can be replaced by values in the section "**Target variables**", where key (in our case user) and value (e.g. Default) are added. This way, you can customize the target for each case.

The tool also provides an option for directly transferring seized data using SFTP, S3, AWS S3 or Azure storage (Figure X.3). First, some kind of container must be selected (and base name provided), then the option "Transfer" can be chosen, and transfer options can be filled in.

CSIRT UPJS | AGH UNIVERSITY CYBERSECURITY CENTRE | Co-funded by the European Union | ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE | SOCCER

SOC4Academia Toolbox (V.)

- Prehľad softvérových a hardvérových riešení
  - SIEM, SOAR, EDR, XDR
  - Inventarizácia aktív
  - Monitorovanie sietí
  - Správa bezpečnostných incidentov
  - Zdroje CTI, platformy na zdieľanie CTI
  - Hodnotenie zraniteľností a skenovanie

CSIRT UPJS | AGH UNIVERSITY CYBERSECURITY CENTRE | Co-funded by the European Union | ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE | SOCCER

SOC4Academia Toolbox (VI.)

- cieľom nie je vynájsť koleso
- použitie súčasných osvedčených postupov, existujúcich noriem a materiálov komunity
- široko používané a osvedčené nástroje (s minimálnymi finančními nárokmi)

SOC pripravenosť (I.)

- Príprava organizácií:
  - Výber životaschopných modelov SOC pre akademickú oblasť
  - Posúdenie možnosti externej podpory
  - Riešenie chýbajúcich schopností

SOC pripravenosť (II.)

- Tvorba podporných materiálov a nástrojov:
  - Školenia o bezpečnostnom povedomí a odolnosti (osobne a online)
  - Školenia na rozvoj základných analytických zručností pre schopnosti SOC a DFIR
  - Nástroje na vzdelávací systém pre personalizované vzdelávanie
  - Prípravy osvedčených postupov pre akademické komunity
  - Nástroje na podporu situačného povedomia

CSIRT UPJS | AGH UNIVERSITY CYBERSECURITY CENTRE | Co-funded by the European Union | ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE | SOCCER

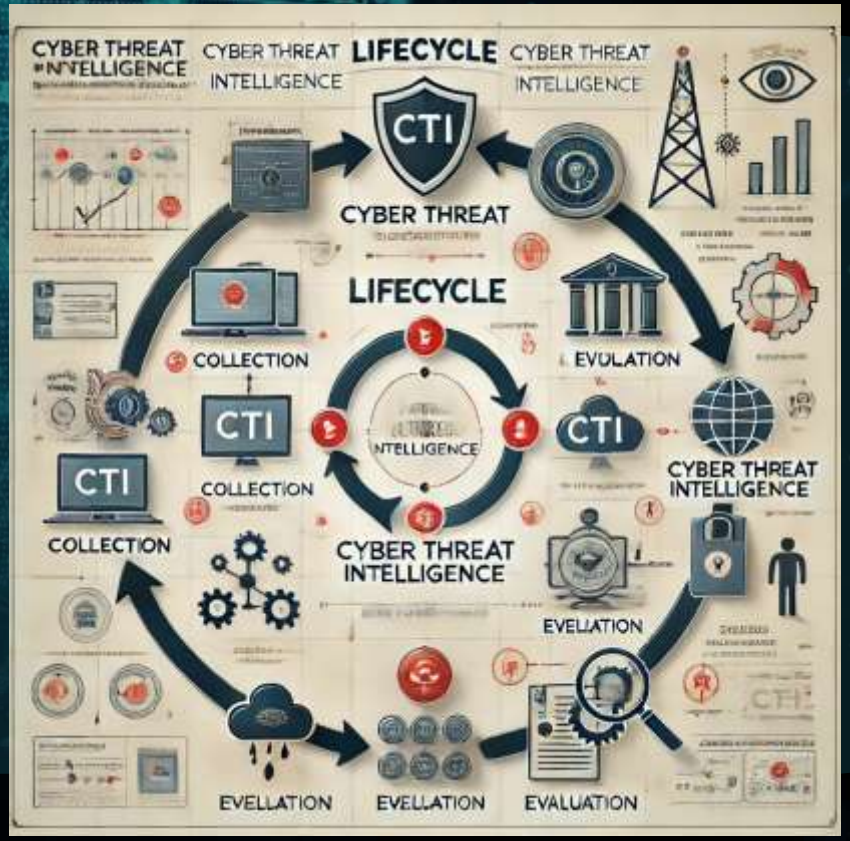
Implementácia SOC / SOC schopností v akademických inštitúciách

- Posúdenie možnej cieľovej úrovne vyspelosti organizácie
- Získanie a implementácia potrebného hardvéru, softvéru a personálu
- Implementácia SOC alebo SOC schopností
- udržateľnosť

CSIRT UPJS | AGH UNIVERSITY CYBERSECURITY CENTRE | Co-funded by the European Union | ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE | SOCCER

Cyber Threat Inteligence

- Definovanie pravidiel pre výmenu CTI
- Implementácia a nasadenie platformy na výmenu CTI
- Vytvorenie medziuniverzitného hubu pre výmenu CTI
- Vytvorenie medziuniverzitnej znalostnej a výskumnej databázy



CSIRT UPJS | AGH UNIVERSITY CYBERSECURITY CENTRE | Co-funded by the European Union | ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE | SOCCER

Integrácia v medzinárodných zoskupeniach

- Integrácia s CSIRT komunitou
  - získavanie a zdieľanie vedomostí
  - budovanie spolupráce
- Príprava pre vstup do komunít bezpečnostných tímov
  - TF-CSIRT a FIRST

FIRST Improving Security Together

TF-CSIRT Trusted Introducer

CSIRT UPJS | AGH UNIVERSITY CYBERSECURITY CENTRE | Co-funded by the European Union | ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE | SOCCER

AGH SOCCER – Cybersecurity for Academic Sector

SOCCER - Security Operation Centre in Central-Eastern Europe Region

SOCCER

. We play for cyber

The SOCCER project is dedicated to fortifying the cybersecurity capabilities and resilience of the EU, with a paramount focus on ensuring a cyber-secure academia sector. Specifically tailored for CEE countries, the initiative aims to support the establishment and advancement of Security Operations Centres (SOCs) within Universities and Research and Technology Organisations (RTOs).

Read more

https://soccer.agh.edu.pl/en

Ďakujem za pozornosť!

soccer.agh.edu.pl

pavol.sokol@upjs.sk

SOCCER projekt je podporený European Cybersecurity Competence Centre - grantovou zmluvou číslo 101128073