Ministerstwo Aktywów Państwowych

Ministerstwo Cyfryzacji

ISACGIG

59 Silesian CYBER hackathon 2023 – pierwsze starcie na Śląsku

67 III CYBER poligon ISAC-GIG w murach Politechniki Śląskiej

54 Członkowie ISAC GIG budują „Centrum monitorowania instalacji przemysłowych w podziemnych zakładach górniczych i wykrywania cyberzagrożeń”

84 Program Cyfrowy, Bezpieczny Śląsk 2030 - podsumowanie

89 CyberSecurity Hub - nowa inicjatywa ISAC GIG

CYBERPOLIGON BIULETYN

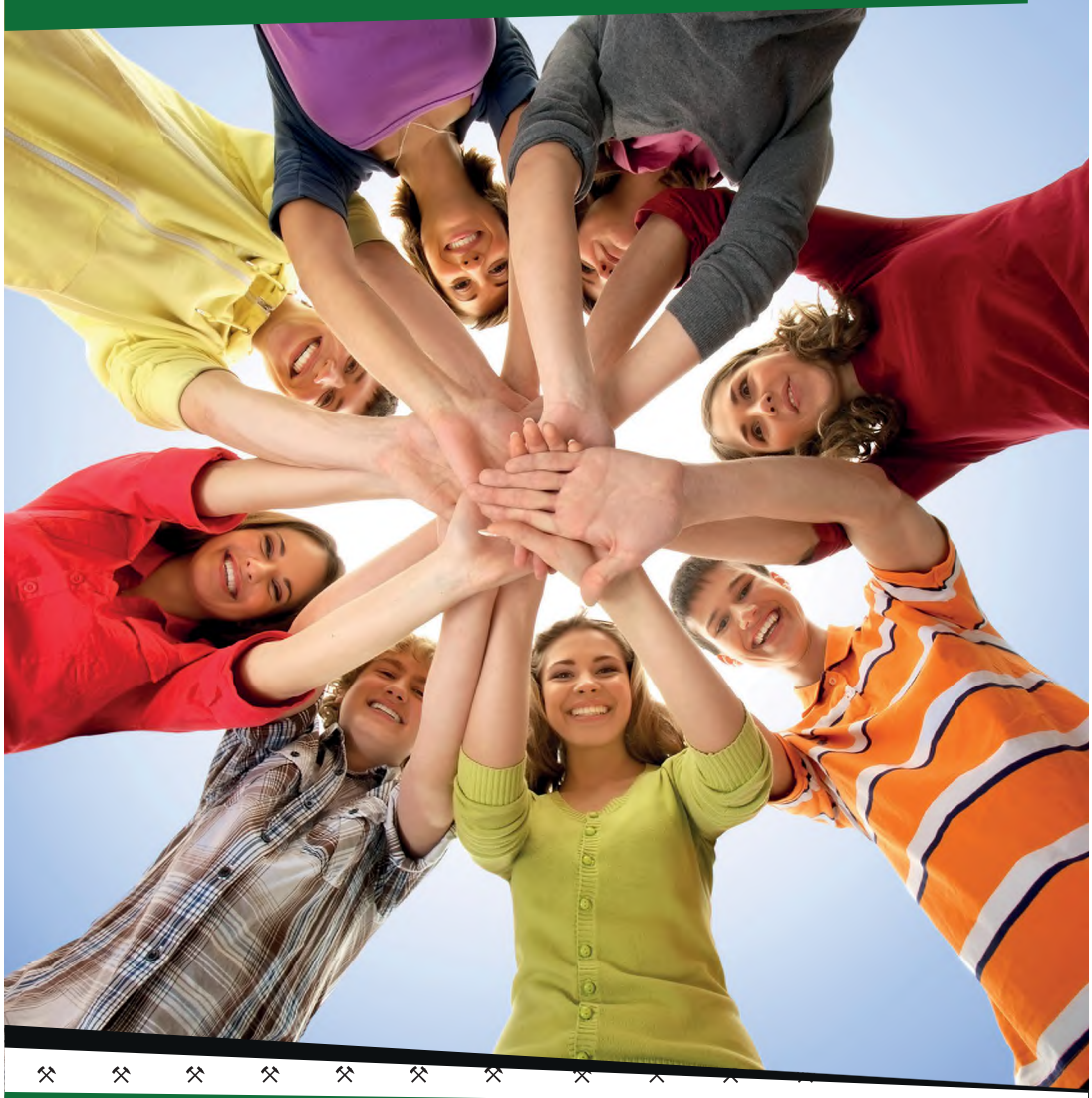
ISAC-GIG

GLIWICE 21-23.06.2023

Politechnika Śląska

UCZELNIA BADAWCZA
INICJATYWA DOSKONAŁOŚCI

FUNDACJA DLA WYDZIAŁU GÓRNICTWA, INŻYNIERII BEZPIECZEŃSTWA I AUTOMATYKI PRZEMYSŁOWEJ POLITECHNIKI ŚLĄSKIEJ



WYDAWCA BIULETYNU

Fundacja dla Wydziału Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej
44-100 Gliwice, ul. Akademicka 2
tel. + 48 (32) 237-11-91, fax: + 48 (32) 237-18-19
e-mail: fundacjawgig@polsl.pl
REGON: 366787120, NIP: 6312668917, KRS: 0000668313

Spis treści

5 Franciszek Plewa
Dziekan Wydziału Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej

7 Stanisław Prusek
Dyrektor Głównego Instytutu Górnictwa

9 Dariusz Prostański
Dyrektor Instytutu Techniki Górniczej KOMAG

11 Piotr Toś
Przewodniczący Komitetu Zarządzającego ISAC GIG, Prezes JSW IT Systems Sp. z o.o.

13 Silesian CYBERhackathon 2023

14 ISAC-GIG minął rok od inauguracji – Jaki był, przeżyjmy to jeszcze raz

19 NASK i Główny Instytut Górnictwa razem dla cyberbezpieczeństwa i cyfryzacji – styczeń 2022

21 Organizacja przez ISAC-GIG sesji Cyberbezpieczeństwo 4.0 w trakcie obrad XXXI Szkoła Eksploatacji Podziemnej – kwiecień 2022 rok

26 Współpraca w czasach zagrożenia atakami w cyberprzestrzeni. KGHM Polska Miedź SA organizatorem pierwszego Cyberpoligon ISAC GIG dla spółek skarbu państwa – 28 września 2022

28 Wydział Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej i ITG KOMAG w ISAC-GIG inaugurują studia podyplomowe Cyberbezpieczeństwo systemów przemysłowych – listopad 2022

34 Organizacja przez ISAC GIG sesji: Cyber(nie)bezpieczeństwo: geneza, istota i rozwój podczas XXIX Międzynarodowej Konferencji Naukowo-Techniczna Górnicze Zagrożenia Naturalne – 08 listopada 2022

36 ISAC-GIG warsztaty o stosowaniu sztucznej inteligencji i Internecie Rzeczy w cyberbezpieczeństwie – 24 listopada 2022

38 Sojusze cyberodporności w sektorze górniczym i energetycznym – czerwiec 2022

42 Organizacja przez ISAC-GIG warsztatów CYBERpoligon ISAC-GIG oraz sesji szkoleniowej pt. „Cyberbezpieczeństwo w przemyśle 4.0" podczas XXXII Szkoły Eksploatacji Podziemnej – luty 2023

50 ISAC-GIG zaproszony przez Krajową Izbę Gospodarczą na 15 Economic Forum TIME – nasz głos w dyskusji o optymalnym scenariuszu cyfryzacji energetyki – marzec 2023

54 Członkowie ISAC GIG: JSW IT Systems Sp. z o.o., Główny Instytut Górnictwa oraz Politechnika Warszawska uzyskali finansowanie projektu „Centrum monitorowania instalacji przemysłowych w podziemnych zakładach górniczych i wykrywania cyberzagrożeń" – kwiecień 2023

56 ISAC GIG ISAC na Warsaw Cyber Summit 2023 prezentowaliśmy podejmowane działania na rzecz budowania świadomości cyberzagrożeń i współpracy w sektorze wydobywczo-energetycznym – kwiecień 2023

59 Wydział Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej wspólnie z ISAC GIG zorganizowali „Silesian CYBERhackathon" – 21 czerwca 2023

67 Za nami III Cyberpoligon ISAC-GIG, praktyczne warsztaty dla sektora wydobywczego i energetycznego – 22 czerwca 2023

77 Cyfrowa transformacja to nasze DNA – wywiad z dziekanem Franciszkiem Plewą gospodarzem i pomysłodawcą CYBER poligonu ISAC-GIG

84 Organizacja przez ISAC-GIG konferencji „Cyfrowy, Bezpieczny Śląsk 2030 – strategia zarządzania cyberbezpieczeństwem w dobie transformacji cywilizacyjnej" – 22-23 czerwca 2023 rok

89 Silesian CyberSecurity Hub – nowy sposób ISAC GIG na budowanie świadomości cyfrowej oraz rozwój kompetencji w zakresie cyberbezpieczeństwa

94 Szczegółowy Program konferencji „Cyfrowy, Bezpieczny Śląsk 2030 – strategia zarządzania cyberbezpieczeństwem w dobie transformacji cywilizacyjnej"

102 KSC FORUM 2023, najważniejsze spotkanie praktyków realizujących wymogi Ustawy o Krajowym Systemie Cyberbezpieczeństwa – 23-25 sierpnia 2023

106 Raport ISAC-GIG: Cyberbezpieczeństwo systemów przemysłowych dla sektora wydobywczo-energetycznego

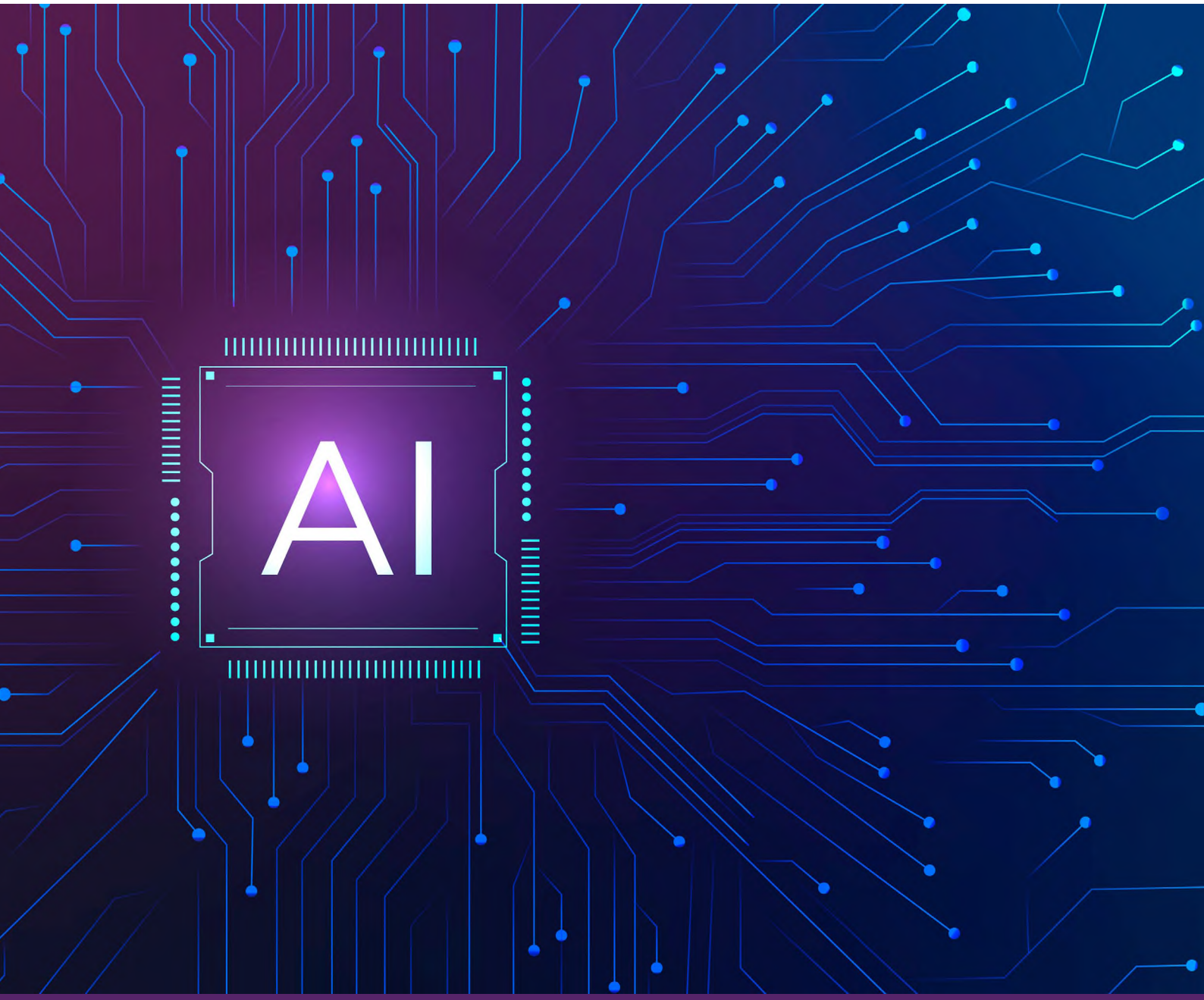
© Fundacja dla Wydziału Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej

Konferencję Cyfrowy, Bezpieczny Śląsk 2030 – strategia zarządzania cyberbezpieczeństwem w dobie transformacji cywilizacyjnej, trzeci CYBERpoligonu ISAC-GIG oraz Silesian CYBERhackathon 2023

HONOROWYM PATRONATEM OBJĘLI

Ministerstwo
Aktywów Państwowych

Ministerstwo
Cyfryzacji



ISAC-GIG Centrum Wymiany i Analizy Informacji dla sektora wydobywczo-energetycznego

Biuro ISAC-GIG:
Główny Instytut Górnictwa
ul. plac Gwarków 1
40-166 Katowice
Telefon
+48-32-259-26-01
+48-32-259-27-60
Internet:
https://isac.gig.eu/kontakt/
e-mail: isac@gig.eu

Organizator trzeciego „CYBERpoligonu ISAC-GIG" w murach Politechniki Śląskiej w Gliwicach:

FUNDACJA DLA WYDZIAŁU GÓRNICTWA, INŻYNIERII BEZPIECZEŃSTWA I AUTOMATYKI PRZEMYSŁOWEJ POLITECHNIKI ŚLĄSKIEJ
Biuro
ul. AKADEMICKA 2
44-100 GLIWICE
Telefon
tel.: +48 (32) 237-11-91
fax: +48 (32) 237-18-19
e-mail: fundacjawgig@polsl.pl
REGON: 366787120
NIP: 631-266-89-17
ING Bank Śląski S.A. Nr rachunku: 58 1050 1298 1000 0090 8015 4447

Franciszek Plewa
Dziekan Wydziału Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej

Szanowni Państwo,

rozwój innowacji i technologii wymaga sprawnie funkcjonującego szkolnictwa wyższego zarówno w kwestii proponowanych kierunków kształcenia, np. zamawianych kierunków, jak również podniesienia jakości bazy i infrastruktury szkół wyższych, która zapewni możliwość kształcenia na najwyższym poziomie. Tak jest właśnie na kierowanym przez mnie Wydziale Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej.

Strategia najstarszego Wydziału Politechniki Śląskiej prestiżowej, europejskiej uczelni badawczej, kreującej rozwój naukowy i postęp techniczny, kształcącej wysoko wykwalifikowane kadry, a także aktywnie wpływającej na rozwój regionu i społeczności lokalnych nie tylko Śląska zakłada, że staniemy się fundamentem bezpieczeństwa transformacji polskiej gospodarki.

Jest dla nas dużym wyróżnieniem uczestnictwo w ISAC-GIG, swoistym sojuszu największych spółek skarbu państwa z sektora wydobywczo-surowcowego na rzecz budowy spójnej polityki w dziedzinie cyberobronności, a zwłaszcza kształcenia wysokokwalifikowanych specjalistów w tym zakresie.

Idea utworzenia ISAC-GIG zrodziła się z potrzeby wymiany wiedzy, informacji, doświadczeń oraz dobrych praktyk w zakresie stosowania zabezpieczeń systemów teleinformatycznych i zapewnienia ciągłości działania infrastruktury krytycznej w przypadku cyberataku. ISAC GIG już dziś opracowuje i promuje własne standardy komunikacji i rekomendacje dla sektora wydobywczo-energetycznego, a także współpracuje przy obsłudze incydentów bezpieczeństwa i cyberataków dotykających jednostki całego sektora.

Stąd nasz inicjatywa kształcenie kadr wchodzących w skład ISAC-GIG spółek skarbu państwa, wychowywanie młodzieży w świadomości szans ale i zagrożeń cyberbezpieczeństwa, Big Data, Internetu rzeczy, biometrii i sztucznej inteligencji, które mają pozwolić wyjść naprzeciw oczekiwaniom młodego pokolenia przyszłych studentów Politechniki. Mają umożliwić naszym absolwentom ciągłe kształcenie i podnoszenie kwalifikacji.

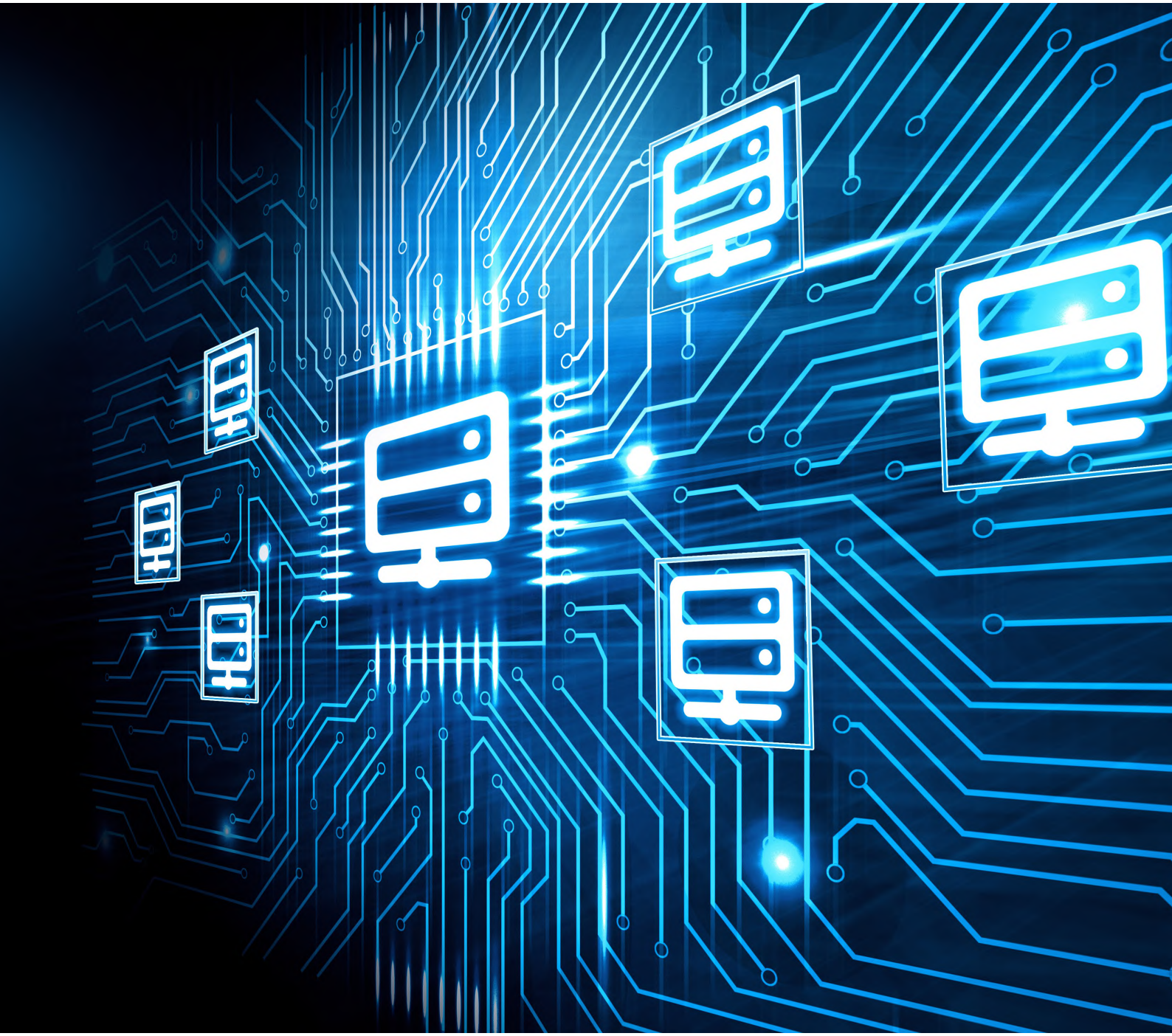
Uruchamiane przez nas dla ISAC-GIG studia podyplomowe: „Cyberbezpieczeństwo systemów przemysłowych" zgodnie z misją Politechniki Śląskiej i mają zapewnić rozwój kadr na najwyższym poziomie. Są to pierwsze studia swoim zakresem obejmujące nie tylko IT ale również OT oraz elementy certyfikacji produktów i usług w zakresie cyberbezpieczeństwa. Już dziś realizujemy projekty inżynierskie, które wspierają rozwiązania w zakresie zagadnień technicznych oraz organizacyjnych związanych z funkcjonowaniem w obszarze cyberbezpieczeństwa. sektora wydobycie surowców i energetyka.

Szanowni Państwo, możliwość organizacji na naszym Wydziale w murach Politechniki Śląskiej trzeciej edycji „CYBERpoligon ISAC-GIG" jest dla nas wyróżnieniem ale i swoistym zobowiązaniem związanym z podnoszeniem świadomości cyfrowej oraz rozwojem kompetencji w zakresie cyberbezpieczeństwa zwłaszcza wśród młodzieży, dlatego postanowiliśmy wydarzeniem towarzyszącym „CYBERpoligonu ISAC-GIG" uczynić „Silesian CYBERhackathon 2023" kierowany do uczniów śląskich szkół średnich oraz prowadzoną niejako równolegle do części praktycznej CYBERpoligonu dyskusję w sesjach szkoleniowych konferencji pod hasłem: „Cyfrowy, Bezpieczny Śląsk 2030 – strategia zarządzania cyberbezpieczeństwem w dobie transformacji cywilizacyjnej".

Życząc wszystkim Państwu niezapomnianych wrażeń płynących z serca najstarszego Wydziału Politechniki Śląskiej, zapraszam do współpracy w kształceniu wysoko wykwalifikowanej kadry dla przemysłu, samorządów i jednostek badawczych. Pamiętajcie jesteście zawsze mile widziani na Wydziale Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej fundamencie bezpieczeństwa transformacji polskiej gospodarki.

Zapraszam do współpracy – naprawdę warto.

Franciszek Plewa – Dziekan



Stanisław Prusek
Dyrektor Głównego Instytutu Górnictwa

Szanowni Państwo,

w lutym br. w trakcie obrad XXXII Szkoły Eksploatacji Podziemnej w Krakowie podczas oficjalnego posiedzenia Komitetu Zarządzającego Centrum Wymiany i Analizy Informacji w Zakresie Cyberbezpieczeństwa dla sektora wydobywczego (ISAC-GIG) podjęto decyzję o przyznaniu Wydziałowi Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej organizacji warsztatów „CYBERpoligon ISAC-GIG", które odbędą się w dniach 21-23 czerwca 2023 w murach Politechniki Śląskiej w Gliwicach.

Doceniając wagę problematyki cyberbezpieczeństwa w sektorze przemysłowym oraz chcąc popularyzować wiedzę z tego obszaru u jak najszerszego grona słuchaczy, nasze obrady swoim patronatem objęło Ministerstwo Aktywów Państwowych, Ministerstwo Cyfryzacji oraz Jego Magnificencja Rektor Politechniki Śląskiej Prof. Arkadiusz Mężyk.

Szanowni Państwo, ISAC-GIG utworzono przy Głównym Instytucie Górnictwa w styczniu, a jego prace inaugurowano uroczyście w czerwcu 2022 roku w Warszawie w Ministerstwie Aktywów Państwowych. Mija więc rok naszej współpracy, tym bardziej cieszy mnie fakt, że w trakcie bieżącego „CYBERpoligonu ISAC-GIG" do naszego grona dołączą PGE Górnictwo i Energetyka Konwencjonalna oraz Tauron Wydobycie SA, które obok ITG KOMAG, Wydziału Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej, KGHM Polska Miedź SA, Polskiej Grupy Górniczej SA, JSW SA, LW Bogdanka SA, Tauron SA i Węglokoks Kraj SA. uzupełnią ostatecznie grono podmiotów pełniących kluczową rolę dla polskiego sektora wydobywczego.

Współpraca pomiędzy największymi spółkami skarbu państwa w zakresie stanowienia wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych, w tak trudnym czasie jakim jest wojna w Ukrainie oraz niedoborze specjalistów z zakresu cyberbezpieczeństwa jest szczególnie cenna i winna wskazywać w mojej ocenie kierunek dla innych podmiotów. Budujmy nadal wspólnie świadomość lepszego zrozumienia kluczowych problemów związanych z zapewnieniem bezpieczeństwa informatycznego we współczesnym społeczeństwie. Wymieniajmy się wiedzą, informacjami, doświadczeniami oraz dobrymi praktykami w zakresie stosowania zabezpieczeń systemów teleinformatycznych zapewniających ciągłość działania infrastruktury krytycznej w przypadku cyberataku.

Aktualna sytuacja na świecie w Europie, a zwłaszcza za naszą wschodnia granicą zmusza nas wszystkich do stałego podnoszenia poziomu bezpieczeństwa nie tylko w stosowanych rozwiązaniach teleinformatycznych. Dziś stoimy przed technologicznymi, środowiskowymi, ale także społecznymi wyzwaniami związanymi z zaopatrzeniem w surowce i energię, co stanowi o naszym bezpieczeństwie i rozwoju gospodarki. Bez współdziałania w tak ważnym obszarze, jakim jest cyberbezpieczeństwo, bez sprawnej wymiany informacji oraz dostępu do nowych rozwiązań i technologii w zakresie ochrony przed zagrożeniami cybernetycznymi, nie można już bezpiecznie funkcjonować, szczególnie w tak ważnych sektorach gospodarki jak wydobycie surowców i energetyka.

Życząc Państwu owocnych spotkań, ciekawych dyskusji i emocjonujących zmagań cyberinformatycznych, zachęcam do dalszego zacieśniania współpracy w ramach ISAC-GIG, do budowania świadomości i odpowiedzialności cyfrowej sektora surowcowego będącego fundamentem nowego oblicza przemysłu wydobywczego w naszym kraju.

Z górniczym pozdrowieniem Szczęść Boże.

Stanisław Prusek

Dariusz Prostański
Dyrektor Instytutu Techniki Górniczej KOMAG

Szanowni Państwo,

Instytut Techniki Górniczej KOMAG jako aktywny członek ISAC-GIG wspólnie z Wydziałem Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej buduje relacje z czołowymi partnerami technologicznymi w zakresie opracowania rozwiązań podnoszących poziom świadomości i kompetencje cyberbezpieczeństwa, tak abyśmy mogli jako Polska bezpiecznie się rozwijać, bogacić i spokojnie żyć.

Ostatnimi czasy głośno jest o zaangażowaniu ITG KOMAG w budowę Śląskiego Systemu Magazynów energii, który to projekt prowadzimy we współpracy z samorządami pięciu wielkich miast Śląska tj.: Bytomia, Zabrza, Gliwic, Piekar, Dąbrowy Górniczej i Katowic. Tak, widzimy olbrzymią szansę w kreowaniu rozwoju energetyki rozproszonej w naszym kraju. Więcej uważamy, że magazyny energii tak jak my je projektujemy stanowią odpowiedź na potrzebę systemowej regionalizacji bezpieczeństwa energetycznego, i mogą – a naszym zdaniem wręcz obowiązkowo powinny – być istotnym elementem procesu planowanej transformacji energetycznej Polski. Nasze magazyny energii już dziś tak projektujemy w KOMAG-u, aby ich budowa tu wokół nas na Śląsku stanowiła tak formą jaki i funkcją atrakcyjną szansę rozwoju całej społeczności lokalnej, jak swego rodzaju dania drugiego życia obiektom obecnie często zdegradowanym. Zdecydowanie mówmy nie bezmyślnej likwidacji i burzeniu, chcemy przekształcać zachowując cały czas regionalny charakter tej ziemi.

Nie możemy jednak zapominać, że transformacja polskiej energetyki, której magazyny energii są pewnym wg nas istotnym elementem tworzącej się na naszych oczach energetyki rozproszonej to przede wszystkim transformacja cywilizacyjna całego kraju. To wszechogarniająca nas cyfryzacja, digitalizacji i automatyzacja całego sektora wytwarzania i przesyłu energii. To wreszcie zarządzanie inteligentnymi podatnymi na cyberataki systemami nadzoru i monitorowania sieci. Wiemy wszak, że jeżeli potrafimy zarządzać inteligentnymi systemami rozproszonymi, zabezpieczać je i monitorować to jesteśmy w stanie również dbać o ich bezpieczeństwo jak i bezpieczeństwo całego krajowego systemu energetycznego.

W mojej ocenie Cyberbezpieczeństwo dzisiaj w kontekście infrastruktury energetycznej, powiem więcej infrastruktury krytycznej jest absolutnie podstawowym zagadnieniem nad którym musimy się wszyscy pochylić i które musimy rozwijać, stąd pomysł na budowę w naszym Instytucie ultranowoczesnego laboratorium testowania i kształtowania bezpieczeństwa cybernetycznego systemów przemysłowych. Stąd inicjatywa uruchomienia w oparciu o najlepszych fachowców zrzeszonych w ISAC-GIG specjalnych studiów podyplomowych realizowanych z Wydziałem Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej. Stąd wreszcie nowa strategia IT KOMAG mająca docelowo stymulować transformację branży energetycznej, w której centralną rolę odgrywać będzie cyfryzacja, informatyzacja, gromadzenie i racjonalne olbrzymiej ilości danych, które nie tylko w przypadku energetyki rozproszonej odgrywają krytyczną rolę.

Szanowni Państwo, życząc nam wszystkim owocnych obrad i ciekawych innowacyjnych pomysłów w trakcie trzeciego „CYBERpoligonu ISAC-GIG", chciałem bardzo podziękować wszystkim naszym partnerom zrzeszonym w ISAC-GIG za otwartość i wsparcie w budowaniu świadomości nie tylko w obszarze cyberbespieczeństwa ale także we wdrażaniu czwartej rewolucji przemysłowej w mechanizacji, elektryfikacji, informatyzacji oraz automatyzacji GOSPODARKI 4.0.

Pozdrawiam
Dariusz Prostański

cyber
security

Piotr Toś
Przewodniczący Komitetu Zarządzającego ISAC GIG, Prezes JSW IT Systems Sp. z o.o.

Szanowni Państwo,

ochrona cyberprzestrzeni stała się jednym z najczęściej poruszanych tematów związanych z bezpieczeństwem. Państwa, organizacje międzynarodowe i inne podmioty niepaństwowe rozumieją, że stabilne funkcjonowanie i rozwój globalnego społeczeństwa informacyjnego zależy od otwartej, niezawodnej i przede wszystkim bezpiecznej cyberprzestrzeni. Rosnąca świadomość w tym zakresie idzie w parze z gwałtownym wzrostem liczby incydentów komputerowych i pojawianiem się nowych rodzajów zagrożeń.

Mija właśnie rok od powołania do życia Centrum Wymiany i Analizy Informacji w Zakresie Cyberbezpieczeństwa ISAC-GIG. Dla mnie osobiście był to okres wytężonej pracy i olbrzymiej satysfakcji z wspólnie realizowanych inicjatyw mających na celu ni mniej ni więcej jak podniesienie poziomu cyberbezpieczeństwa naszego kraju między innymi poprzez budowanie potencjału i zdolności w obszarze cyberbezpieczeństwa oraz przekazywanie informacji dotyczących incydentów, podatności i ryzyk podmiotom krajowego systemu cyberbezpieczeństwa.

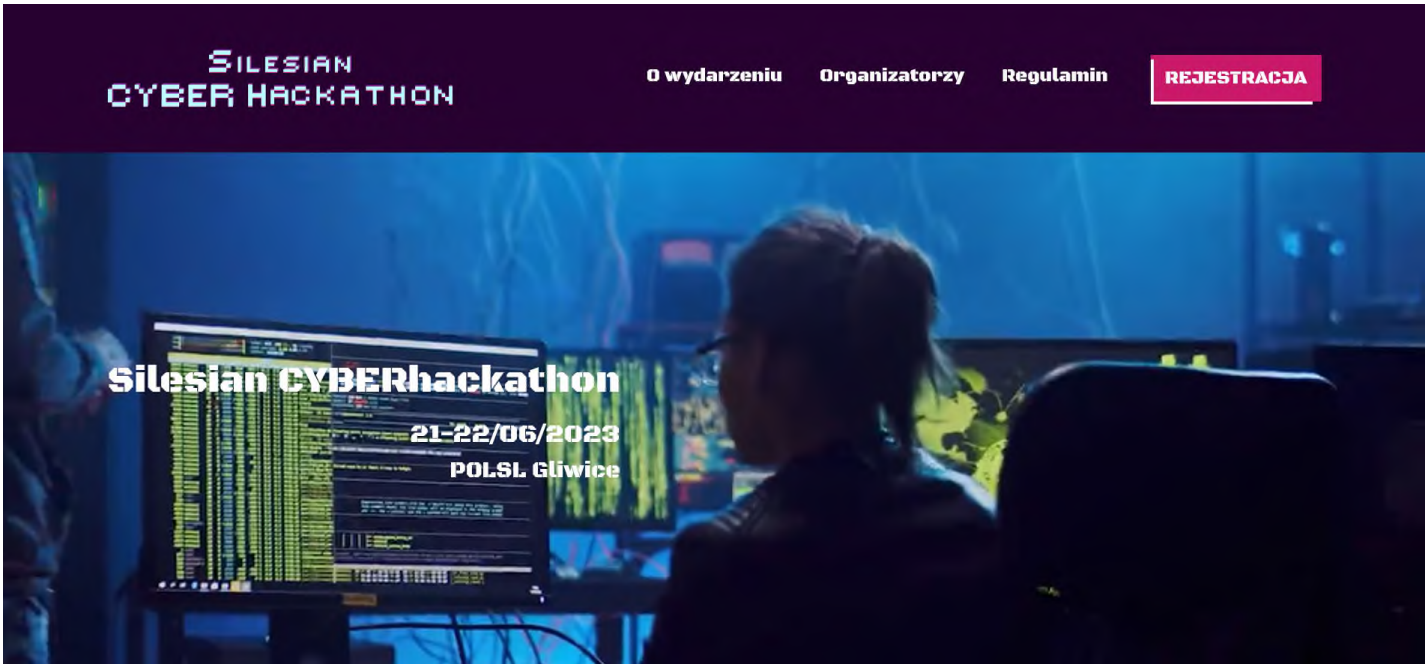
Regularne spotkania Komitetu Zarządzającego, trzy „CYBERpoligon ISAC-GIG", uruchomione na Wydziale Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej studia podyplomowe „Cyberbezpieczeństwo systemów przemysłowych", wreszcie opublikowany właśnie RAPORT pt.: „Cyberbezpieczeństwo systemów przemysłowych dla sektora wydobywczego za rok 2022" autorstwa wykładowców firmowanych przez ISAC-GIG studiów podyplomowych to tylko mały wycinek realizowanych przez nas inicjatyw. Na pewno cieszy fakt, że grono podmiotów zrzeszonych w ramach Centrum ISAC-GIG obejmuje już wszystkie podmioty tak ważnych sektorów gospodarki polski jak wydobycie surowców i energetyka.

Wierze, że przyszłość pozwoli nam skutecznie przygotować się na zwiększoną dynamikę procesów zachodzących w obszarze cyberbezpieczeństwa tak w jednostkach samorządu terytorialnego, przedsiębiorstw jak i instytucji naukowo-badawczych. Chciałbym, aby nasze działania pozwoliły na zwiększenie liczby podmiotów funkcjonujących w obszarze nowych technologii oraz podniesie poziom cyberbezpieczeństwa w kraju. Wierzę że uruchomienie struktur integracji danych związanych z procesem restrukturyzacji spółek górniczych, umożliwi w przyszłości budowę mechanizmów monitoringu transformacji całych regionów kraju. Cieszę się że nasze działania dają kłam powszechnie panującym w społeczeństwie stereotypom jakoby polskie górnictwo było technicznie i organizacyjnie zacofane i nie było w stanie udźwignąć nowych technologii informatycznych.

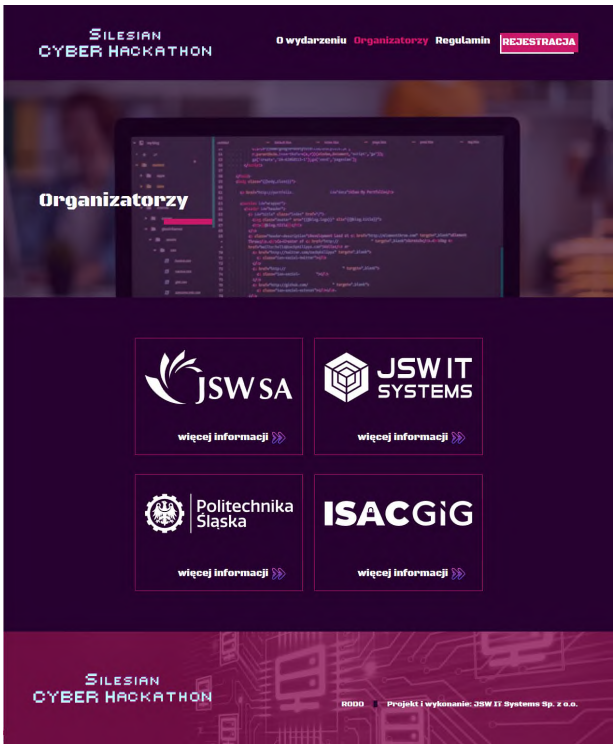
Polska stoi przed technologicznymi, środowiskowymi, ale także społecznymi wyzwaniami związanymi z zaopatrzeniem w surowce, które leżą u podstaw naszej przemysłowej działalności. Transformacja cywilizacyjna naszej gospodarki nie może dokonać się bez zapewnienia monitoringu i bezpieczeństwa procesów przemysłowych, procesów tych nie da się nadzorować bez sprawnej wymiany informacji oraz dostępu do najnowszych technologii, systemów teleinformatyki, automatyki i sterowania których budowa i funkcjonowanie jest już przedmiotem naszych rutynowych działań.

Organizowany przez nas już po raz trzeci „CYBERpoligon" to praktyczne warsztaty dla przedstawicieli podmiotów tworzących ISAC-GIG, podczas których uczestnicy przechodzą szkolenie w realistycznym środowisku w zakresie wykrywania i reagowania na symulowane cyberataki. Celem wydarzenia jest wymiana wiedzy i doświadczeń, upowszechnianie dobrych praktyk oraz podnoszenie świadomości i zgłębianie zagadnień dotyczących cyberbezpieczeństwa. W trakcie bieżących warsztatów kilkuosobowe zespoły będą rywalizowały w odpieraniu cybernetycznych ataków na powierzone ich ochronie systemy informatyczne Linux i SCADA. Jednocześnie w trakcie obrad w sesjach szkoleniowych obejmujących swoją tematyką: budowanie strategii zarządzania ryzykiem cybernetycznym, elementy informatyki śledczej (CHFI – Computer Hacking Forensic) oraz bezpieczeństwo informacji uczestnicy naszego spotkania dyskutować będą mogli z czołowymi ekspertami o blaskach i cieniach powszechnie obecnie wdrażanych rozwiązaniach czwartej rewolucji przemysłowej w mechanizacji, elektryfikacji, informatyzacji oraz automatyzacji GOSPODARKI 4.0.

Piotr Toś


SILESIAN
CYBER HACKATHON
O wydarzeniu
Organizatorzy
Regulamin
REJESTRACJA
Silesian CYBERhackathon
21-22/06/2023
POLSL Gliwice

SILESIAN
CYBER HACKATHON
O wydarzeniu
Organizatorzy
Regulamin
REJESTRACJA
Silesian CYBERhackathon
21-22/06/2023
POLSL Gliwice
Organizatorzy
JSW SA
JSW IT SYSTEMS
Politechnika Śląska
ISACGiG
O wydarzeniu
Hackathon odbędzie się stacjonarnie na Wydziale Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej w Gliwicach przy ul. Akademickiej 2 w dniach 21-22 czerwca 2023 r.
Honorowy Patronat nad wydarzeniem:
Wicepremier Jacek Sasin, Minister Aktywów Państwowych
Minister Cyfryzacji Janusz Cieszyński
Rektor Politechniki Śląskiej prof. dr hab. inż. Arkadiusz Mężyk
NAGRODY:
I miejsce - 8 000 PLN
II miejsce - 6 000 PLN
III miejsce - 4 000 PLN
Partnerzy


SILESIAN
CYBER HACKATHON
O wydarzeniu
Organizatorzy
Regulamin
REJESTRACJA
Organizatorzy
JSW SA
więcej informacji
JSW IT SYSTEMS
więcej informacji
Politechnika Śląska
więcej informacji
ISACGiG
więcej informacji
SILESIAN
CYBER HACKATHON
ROOD
Projekt i wykonanie: JSW IT Systems Sp. z o.o.

Silesian CYBERhackathon 2023

Silesian CYBERhackathon 2023 jest pierwszym tego typu wydarzeniem na Śląsku, jego celem jest zwiększanie świadomości społecznej na temat wpływu technologii cyfrowych na życie codzienne i zawodowe, w tym na zwiększanie bezpieczeństwa fizycznego i cyfrowego oraz ochronę klimatu, a także zachęcenie do tworzenia rozwiązań wspomagających te działania.

Uważamy, że to idealna okazja dla wszystkich zainteresowanych programowaniem, projektowaniem i nowymi technologiami, młodych ludzi aby spotkać się i wspólnie stworzyć innowacyjne, cyfrowe rozwiązania zadań przegotowanych przez organizatorów wywodzących się z ISAC-GIG.

Jak napisaliśmy na specjalnie przygotowanym na tą okazję plakacie „...Niezależnie od tego, czy jesteś początkującym programistą czy doświadczonym hackerem, hackathon oferuje moc wrażeń, inspirujące wyzwania oraz naukę nowych technologii. Na najlepsze zespoły czekają cenne nagrody!”. Dodatkową atrakcją będzie możliwość udziału młodych uczestników hackathonu w CYBERpoligonie ISAC-GIG – warsztatach, na których doświadczeni pracownicy spółek skarbu państwa z sektora wydobywczego będą w realistycznym środowisku wykrywali i reagowali na cyberataki i inne prawdziwe zagrożenia związane z systemami operacyjnymi Linux oraz SCADA.

Pierwszy „Silesian CYBERhackathon 2023” jest organizowany przez Wydział Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej wspólnie z JSW IT Systems Sp. z o.o. pod auspicjami Centrum Wymiany i Analizy Informacji dla sektora wydobywczo-energetycznego ISAC-GIG.

Na potrzeby hackathonu przygotowano REGULAMIN zmagań oraz specjalną stronę internetową dostępną pod adresem:

https://silesiancyberhackathon.pl/

ISAC-GIG minął rok od inauguracji – Jaki był, przeżyjmy to jeszcze raz

Information Sharing and Analysis Center (ISAC) to organizacje non-profit które zapewniają możliwość wymiany informacji o zagrożeniach w obszarze cyber. Umożliwiają wymianę informacji na temat zagrożeń i podatności systemów informatycznych oraz automatyki pomiędzy przedsiębiorstwami, instytutami naukowymi czy też jednostkami samorządowymi. Jest to szczególnie ważne teraz, gdy za granicami naszego kraju trwa konflikt zbrojny, a w przedsiębiorstwach i urzędach w wyniku pandemii COVID-19 znacząco zwiększyło się wykorzystanie systemów informatycznych i internetu. To właśnie większe wykorzystanie informatyki w prowadzeniu działalności przedsiębiorstw przemysłowych przełożyło się na bardzo duży wzrost zagrożeń z tym związanych.

W przeciwdziałaniu cyber zagrożeniom kluczową kwestią jest dostęp do wiedzy eksperckiej. Dlatego też umożliwienie wymiany doświadczeń pomiędzy osobami zajmującymi się cyberbezpieczeństwem w różnych przedsiębiorstwach jest szczególnie ważne i cenne, zwłaszcza dziś, gdy tak bardzo brakuje specjalistów w tej dziedzinie. Współdziałanie w ramach ISAC daje tą możliwość oraz umożliwia kształcenie nowych specjalistów przyczyniając się do podniesienia odporności na wszelkiego rodzaju zagrożenia związane z systemami informatyki i automatyki.

Zespoły ISAC to nie jest nowa inicjatywa – w Europie oraz Stanach Zjednoczonych istnieje wiele tego typu ośrodków, a najstarsze działają od lat dziewięćdziesiątych XX wieku. W Polsce pierwszym tego typu przedsięwzięciem było powołanie 2 października 2020 r. w Warszawie, ISAC-Kolej, a następnie 5 listopada 2021 Centrum Reputacyjne Komunikacji Elektronicznej będącego ISACiem Urzędu Komunikacji Elektronicznej w sektorze telekomunikacyjnym.

MINISTERSTWO
AKTYWÓW
PAŃSTWOWYCH

MINISTERSTWO

www.itss.pl

iTSS

IT SYSTEMS & SOLUTIONS

BEZPIECZEŃSTWO W IT I BIZNESIE

IT Systems and Solutions sp. z o.o. jako jedna z wiodących firm na polskim rynku IT, dostarcza kompleksowe rozwiązania podnoszące konkurencyjność, produktywność i bezpieczeństwo środowisk informatycznych.

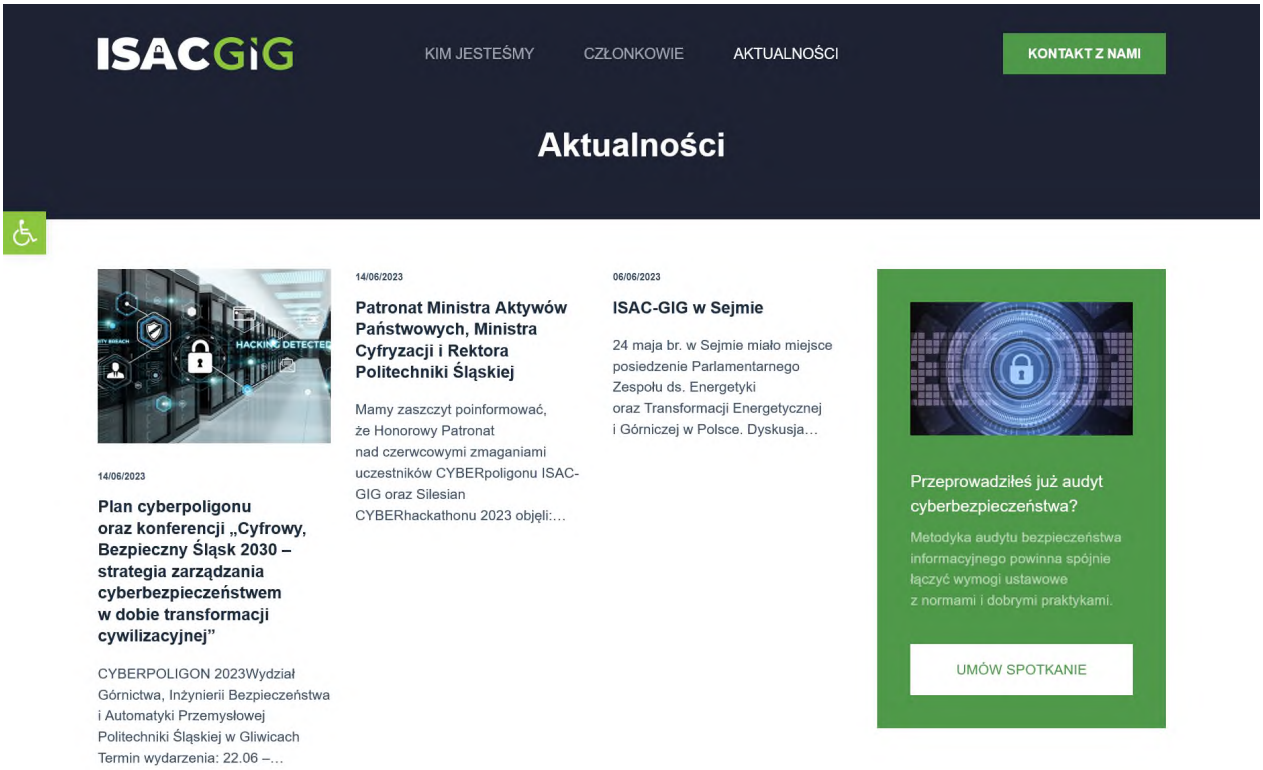
Zajmuje się projektowaniem oraz budowaniem wysokowydajnych i bezpiecznych środowisk IT na rzecz średnich i dużych przedsiębiorstw z sektora energetycznego, bankowego, komercyjnego i publicznego. Połączenie najnowocześniejszych technologii dostępnych na rynku oraz wysokich kompetencji inżynierów posiadających najwyższe poziomy certyfikacji w wielu obszarach technologicznych pozwala realizować spółce duże i skomplikowane projekty informatyczne.

- BEZPIECZEŃSTWO
- INFRASTRUKTURA
- MANAGED SERVICES - enterCLOUD
- SYSTEMY I DEDYKOWANE APLIKACJE
- INTEGRACJA SYSTEMÓW I BAZ DANYCH

Diament Miesięcznika Forbes 2021

POLSKA NAGRODA INTELIGENTNEGO ROZWOJU

Dowiedz się więcej na



ISAC-GIG powstał w styczniu 2022 roku w Głównym Instytucie Górnictwa (GIG), na mocy podpisanych wcześniej przez Instytut porozumień ze spółkami sektora wydobywczo-energetycznego. Uroczyste podpisanie deklaracji uruchomienia ISAC-GIG nastąpiło 3 czerwca 2022 roku w Ministerstwie Aktywów Państwowych w Warszawie i nadal jest jednym z pierwszych tego typu przedsięwzięć w kraju, a zapewne pierwszym skupiającym wszystkie spółki skarbu państwa pełniące kluczową rolę w zakresie bezpieczeństwa energetycznego.

Uważamy, iż cyberbezpieczeństwo budowane jako partnerstwo podmiotów będących operatorami usług kluczowych stanowi fundament bezpieczeństwa państwa, minimalizując ryzyka związane z cyberatakami, których liczba stale rośnie. Obecnie utworzono z inicjatywy Ministerstwa Aktywów Państwowych ISAC-GIG, skupia wszystkie spółki skarbu państwa pełniące kluczową rolę dla sektora wydobywczego kraju tj.: KGHM Polska Miedź SA, Polską Grupę Górniczą SA, Jastrzębską Spółkę Węglową SA, Polską Grupę Energetyczną Górnictwo i Energetyka Konwencjonalna SA, LW Bogdanka SA, Tauron SA, Tauron Wydobycie SA i Węglokoks Kraj SA.

Wierzymy, że powołanie ISAC-GIG będzie jednym z pierwszych elementów opracowania „Polityki współpracy w zakresie informatyki i telekomunikacji spółek pełniących kluczową rolę dla sektora wydobywczego kraju” i jest krokiem w kierunku budowy surowcowego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego – CSIRT.

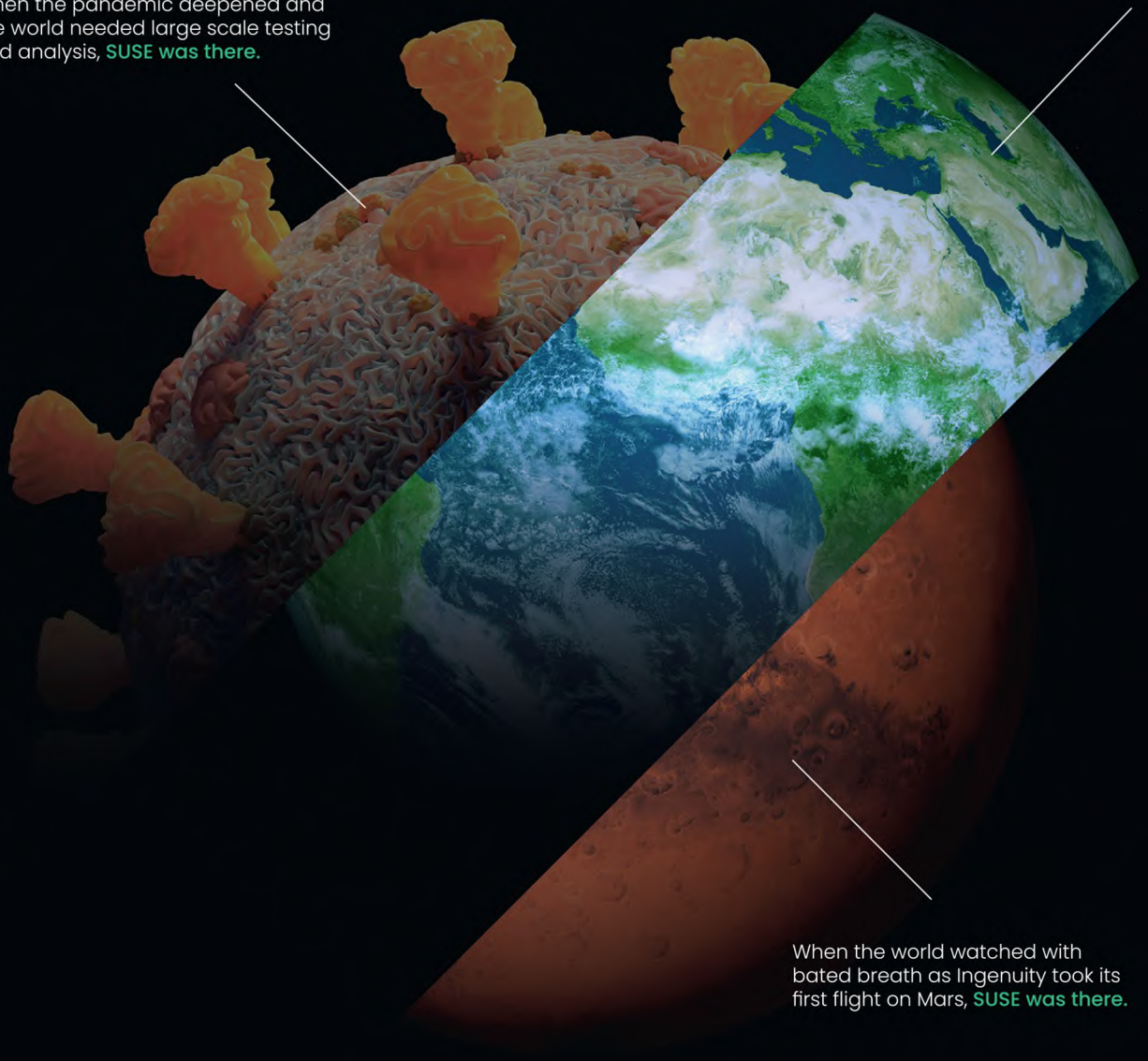
Jednym z celów polityki będzie konieczność standaryzacji oraz ustanowienia wspólnych zasad zarządzania obszarem cyberbezpieczeństwa w górnictwie oraz ochrona wszystkich jego aspektów cyberprzestrzeni, a także aktywne wsparcie budowy Krajowego Systemu Cyberbezpieczeństwa.

Piotr Toś
Przewodniczący Komitetu
Zarządzającego ISAC GIG

SUSE

When manufacturers came together and said, "It's time to reduce our carbon footprint", SUSE was there.

When the pandemic deepened and the world needed large scale testing and analysis, SUSE was there.



When the world watched with bated breath as Ingenuity took its first flight on Mars, SUSE was there.

Trust Open. Trust SUSE.

Discover how SUSE solves the world's most pressing challenges with the power of open.

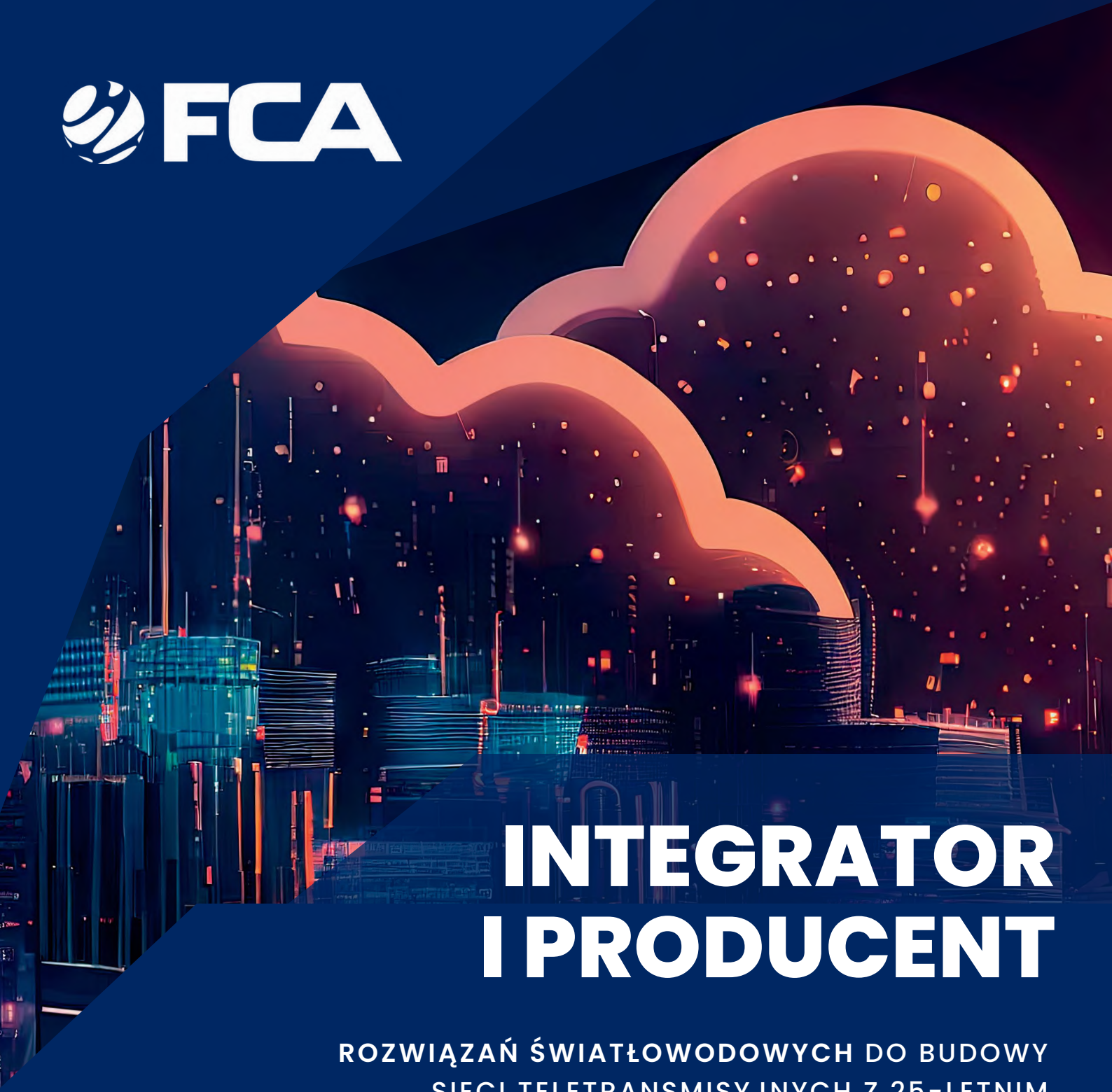
NASK i Główny Instytut Górnictwa razem dla cyberbezpieczeństwa i cyfryzacji – styczeń 2022

27 stycznia 2022 r. w siedzibie NASK w Warszawie Główny Instytut Górnictwa i Państwowy Instytut Badawczy NASK podpisały porozumienie o współpracy w zakresie rozwoju cyfrowej administracji, bezpieczeństwa nowoczesnych instalacji przemysłowych oraz budowy Data Center „Silesian CyberSecurity Hub" w części Kopalni Doświadczalnej „Barbara" – to najważniejsze plany, które zamierzają zrealizować razem.

Jak podkreślono w trakcie uroczystości Przemysł 4.0 staje się faktem, robotyzacja i automatyzacja instalacji postępuje, coraz więcej urządzeń łączy się z Internetem. To czyni przemysł nowocześniejszym i bardziej wydajnym, ale naraża go też na nowe zagrożenia, np. cyberataki. Profesor Stanisław Prusek, który uruchomił właśnie w Instytucie Centrum Wymiany Informacji i Analiz ISAC GIG (z ang. ISAC – Information Sharing and Analysis Center), którego celem jest stała wymiana wiedzy oraz doświadczeń w zakresie cyberbezpieczeństwa pomiędzy najważniejszymi przedsiębiorstwami sektora wydobywczego zwrócił uwagę na fakt, iż jednym z głównych zadań zawartego sojuszu jest zbudowanie wspólnych usług z zakresu cyberbezpieczeństwa dla jednostek samorządu terytorialnego, przedsiębiorstw i ośrodków naukowych ze szczególnym uwzględnieniem bezpieczeństwa systemów automatyki przemysłowej (OT) oraz Internetu Rzeczy (IoT). Istotnym elementem współpracy winny być również wspólne działania w obszarze edukacji i szkoleń, m.in. utworzenie ośrodka szkolenia specjalistów w zakresie cyberbezpieczeństwa.

Porozumienie podpisali uroczyście: prof. dr hab. inż. Ewa Niewiadomska-Szynkiewicz – Zastępca Dyrektora NASK PIB, Dyrektor ds. Naukowych i prof. dr hab. inż. Stanisław Prusek - Dyrektor Głównego Instytutu Górnictwa.

FCA



INTEGRATOR I PRODUCENT

ROZWIĄZAŃ ŚWIATŁOWODOWYCH DO BUDOWY SIECI TELETRANSMISYJNYCH Z 25-LETNIM DOŚWIADCZENIEM NA RYNKU ICT.

Oferta FCA zawiera całą gamę specjalistycznych systemów i usług między innymi do budowy sieci **LAN**, **WLAN**, kompleksowego **zarządzania siecią z poziomu chmury** oraz rozwiązania dedykowane dla obszaru **bezpieczeństwa sieci**.

Zeskanuj kod QR i dowiedz się więcej!

PRODUKTY | ROZWIĄZANIA | USŁUGI

| FCA S.A.

www.fca.com.pl

Organizacja przez ISAC-GIG sesji Cyberbezpieczeństwo 4.0 w trakcie obrad XXXI Szkoła Eksploatacji Podziemnej – kwiecień 2022 rok

Szkoła Eksploatacji Podziemnej od lat uznawana jest za największe spotkanie kadry inżynierskiej i środowiska naukowego działającego w obszarze górnictwa podziemnego. Od ponad 30 lat gromadzi każdego roku blisko 500 uczestników związanych z szeroko rozumianym przemysłem surowcowym w Polsce, a także na świecie.

W roku 2022 swoje pierwsze spotkanie na tej konferencji mieli również członkowie ISAC-GIG prezentując wśród głównych tematów obrad konferencji zagadnienia z obszaru cyberbezpieczeństwa dotyczące min.:

- Standaryzacji w cyberbezpieczeństwie.
- Wyzwań przed którymi stoi branża górnicza w związku funkcjonowaniem Operatorów Usług Kluczowych (OUK).
- Bezpieczeństwa i monitorowania w sieciach przemysłowych.
- Sposobów zabezpieczania środowisk cyfrowych w dobie wzmożonych ataków na infrastrukturę OT/IT.

W czasie Sesji Cyberbezpieczeństwo 4.0 Przemysław Jaroszewski przedstawił raport nt. zagrożeń w obszarze cyberbezpieczeństwa w roku 2022. Ciekawym nawiązaniem do procedowanej nowelizacji Ustawy o Krajowym Systemie Cyberbezpieczeństwa była prezentacja Pawła Kostkiewicza nt. standaryzacji w cyberbezpieczeństwie, w trakcie której szczegółowo omówiona została norma Conunon Criteria oraz inne standardy pozwalające weryfikować bezpieczeństwo systemów teleinformatycznych.

W trakcie panelu dyskusyjnego „Wyzwania Cyberbezpieczeństwa w 2022 roku w kontekście Operatorów Usług Kluczowych" omówione zostały kluczowe elementy wpływające na działania Operatorów Usług Kluczowych (OUK) w obszarze cyberbezpieczeństwa w kontekście wprowadzonego stopnia alarmowego CRP.

Spotkanie miało również wymiar techniczny, przedstawione referaty omawiały takie tematy jak bezpieczeństwa i monitorowanie w sieciach przemysłowych, czy też sposoby zabezpieczania środowisk cyfrowych w dobie wzmożonych ataków na infrastrukturę IT/OT.

Ramowy program spotkania ISAC-GIG podczas XXXI Szkoły Eksploatacji Podziemnej obejmował wystąpienia:

- Przemysław Jaroszewski – Cyber Threar Response Manager Standard Chartered Bank: Cyberthreats to watch out for in 2022,
- Paweł Kostkiewicz – Research Department NASK PIB: Standaryzacja w cyberbezpieczeństwie

W panelu dyskusyjnym pt.: „Wyzwania Cyberbezpieczeństwa 2022 w kontekście OUK" moderatorem którego był EY Polska dyskutowali:

- Marek Pawlik – Instytut Kolejnictwa: Współdziałanie w ramach ISAC-Kolej
- Jacek Skrzydło – Microsoft: Bezpieczeństwo i monitorowanie w sieciach przemysłowych
- Paweł Łakomski – Microsoft: Sposoby zabezpieczania środowisk cyfrowych w dobie wzmożonych ataków na infrastrukturę IT
- Jarosław Chodkiewicz – Mediarecovery: Zwiększenie widoczności danych oraz filtracja i optymalizacja ruchu w sieciach OT
- Robert Ługowski – Mediarecovery: Automatyzacja i orkiestracja procesu obsługi incydentów wsparciem dla SOC
- Marcin Paciorkowski – Mediarecovery: Ochrona tożsamości jako klucz do bezpieczeństwa organizacji
- Jan Kąkol – ABB: Cyberbezpieczeństwo podstawą sprawnego funkcjonowania przedsiębiorstwa w kontekście obecnych zagrożeń

Zebrani podkreślili w podsumowaniu dyskusji, iż podjęta przez GIG inicjatywa powołania dla sektora wydobywczego ISAC-GIG wpisuje się idealnie w procedowane w Ustawodawstwie europejskim, dyrektywę NIS oraz nowelizowaną Ustawa o Krajowym Systemie Cyberbezpieczeństwa wspierającą tworzenie sektorowych Centrów Wymiany i Analizy Informacji (z ang. Information Sharing and Analysis Centers – ISAC) i należy dążyć do tego by Centrum swoim działaniem objęło wszystkie podmioty sektora wydobywczego w Polsce.

Ransomware
Maersk - NotPetya (2017)
Atak dotknął ~45k stacji roboczych i ~4k serwerów
Czas paraliżu: 8-10 dni
Czas do pełnego przywrócenia systemów i sieci: 4 tygodnie
Bezpośrednie koszty przywrócenia oszacowano na $300m
Colonial Pipeline - DarkSide (2021)
Sześciodniowa przerwa w transporcie ropy ze względu na brak możliwości rozliczania
75BTC ($5m) okupu

ABB

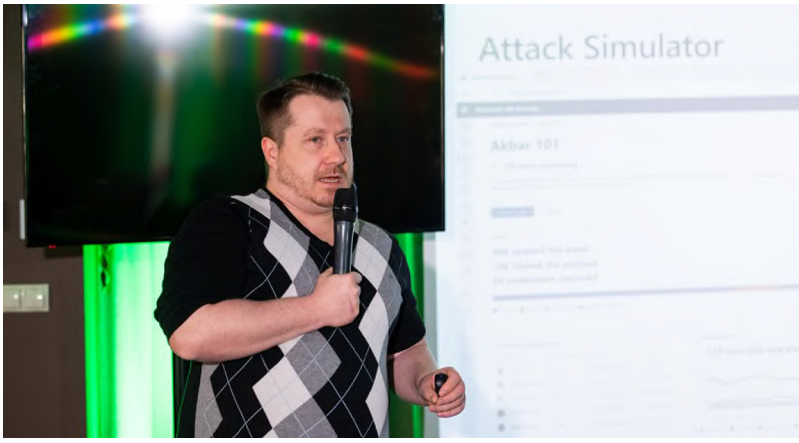
Bezpieczeństwo
uszkodzony-bezpieczny / poziomy SIL
SIL

Cyberbezpieczeństwo 4.0
Instytut Badawczy

Kraków, 11 –13 kwietnia 2022
Cyberbezpieczeństwo 4.0
GiG Instytut Badawczy

XXXI Szkoła Eksploatacji Podziemnej
Kraków, 11 –13 kwietnia 2022
PARTNER
ABB

Defender for I
urządzeń nieza
Wykrywanie zasobów IoT/OT


Attack Simulator

XXXI SZKOŁA EKSPLOATACJI PODZIEMNEJ
11-13.04.2022 Kraków
KOMATS
P&H
PATRON

do pakietów

mine master

CYBER
SECURITY

Współpraca w czasach zagrożenia atakami w cyberprzestrzeni. KGHM Polska Miedź SA organizatorem pierwszego Cyberpoligon ISAC GIG dla spółek skarbu państwa – 28 września 2022

W środę, 28 września, 2022 roku w KGHM Polska Miedź SA w Lubinie przeprowadzono pierwszy Cyberpoligon dla spółek Skarbu Państwa zrzeszonych w Centrum Wymiany i Analizy Informacji dla sektora wydobywczego ISAC GIG.

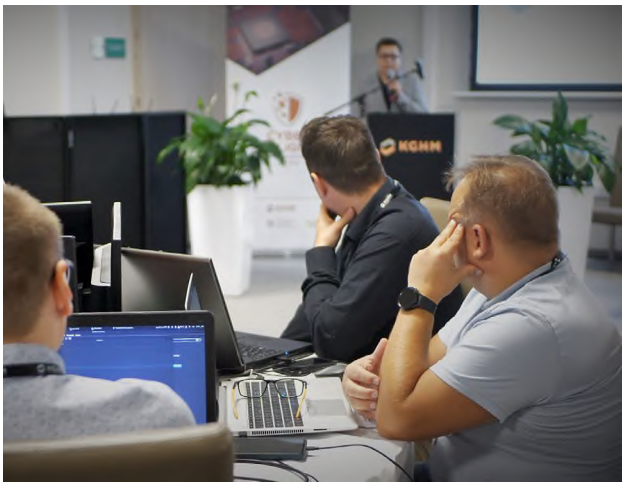
Wirtualne scenariusze rzeczywistych zagrożeń, ochrona przed cyberatakami oraz wymiana doświadczeń składały się na pierwsze warsztaty dla zespołów odpowiadających za cyberbezpieczeństwo w spółkach skarbu państwa należących do ISAC-GIG oraz z sektora energetycznego.

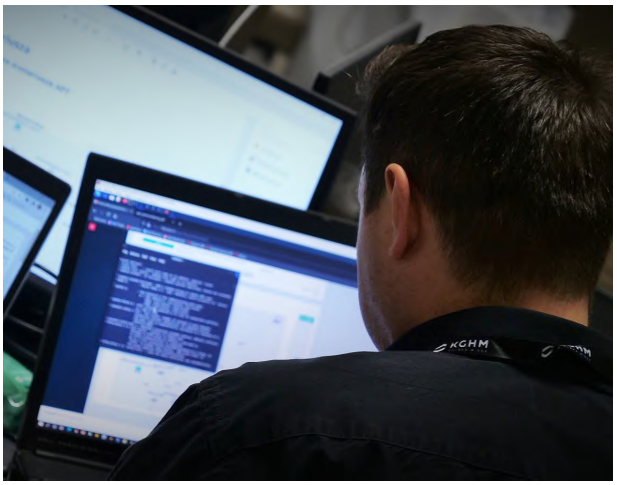
– Cieszę się, że jako KGHM zorganizowaliśmy pierwsze tego typu warsztaty – pierwszy cyberpoligon dedykowany spółkom działającym w kluczowych sektorach gospodarki. Taka forma doskonalenia zdolności pozwala na współzawodnictwo pomiędzy zespołami, stanowiąc jednocześnie ciekawą formę aktywnego ćwiczenia, a także przyczyniając się do wzmocnienia integracji środowiska cyberbezpieczeństwa, co ułatwia następnie niezbędne w tej sferze współdziałanie. To szczególnie ważne, kiedy za naszą wschodnią granicą trwa wojna. Od zagrożeń w wirtualnej przestrzeni nie uciekniemy i musimy być przygotowani. Musimy działać razem – powiedział Tomasz Zdzikot, wiceprezes ds. rozwoju KGHM Polska Miedź S.A.

Cyberpoligon to warsztaty, które służyły przygotowaniu zespołów z poszczególnych firm i spółek na zagrożenia w cyberprzestrzeni. Dla uczestników przygotowane zostały scenariusze ataków, które wymagały szybkich działań i podejmowania decyzji kluczowych dla danych organizacji. Szkolenie dało możliwość wykorzystania swoich doświadczeń i nauki nowych rozwiązań.

W wydarzeniu wzięli udział przedstawiciele ośmiu największych spółek z sektora energetycznego i branży wydobywczej. Patronat honorowy nad wydarzeniem objęło Ministerstwo Aktywów Państwowych oraz Główny Instytut Górniczy – Instytut Badawczy.

CYBER
POLIGON
2022





CYBER
POLIGON

KGHM
POLSKA MIEDŹ

Wydział Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej i ITG KOMAG w ISAC-GIG inaugurują studia podyplomowe Cyberbezpieczeństwo systemów przemysłowych – listopad 2022

26 sierpnia 2022 roku w murach Politechniki Śląskiej Wydział Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej wraz z Instytutem Techniki Górniczej KOMAG podpisali oficjalnie porozumienie o przystąpieniu do ISAC-GIG w celu uruchomienia od listopada elitarnych studiów podyplomowych pt.: „Cyberbezpieczeństwo systemów przemysłowych".

Podpisy pod porozumieniem złożyli: Prorektor ds. Ogólnych Politechniki Śląskiej prof. dr hab. inż. Bogusław Łazarz, dziekan Wydziału Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej prof. dr hab. inż. Franciszek PLEWA, a w imieniu ITG KOMAG dr hab. inż. Dariusz Prostański, ISAC GiG reprezentowała dyrektor Aleksandra Mraczek-Krzak oraz Przewodniczący Komitetu Zarządzającego Centrum Wymiany i Analizy Informacji ISAC-GIG Pan Piotr Toś.

26 sierpnia 2022 roku wstąpienie KOMAGu I PŚ do ISACA

Przystąpienie do ISAC-GIG poprzedziło podpisanie 20 maja 2022 roku porozumienia między JSW S.A., Politechniką Śląską a ITG KOMAG, którego celem było promowanie i rozwijanie współpracy w zakresie cyberbezpieczeństwa pomiędzy nauką a biznesem, współpraca w zakresie realizacji innowacyjnych projektów i programów badawczych, a także upowszechnianie ich rezultatów.

Porozumienie podpisali: Dziekan Wydziału Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej prof. Franciszek Plewa, prezes JSW S.A. Tomasz Cudny, dyrektor ITG KOMAG dr hab. inż. Dariusz Prostański. Przy podpisaniu obecny był wiceminister aktywów państwowych Piotr Pyzik.

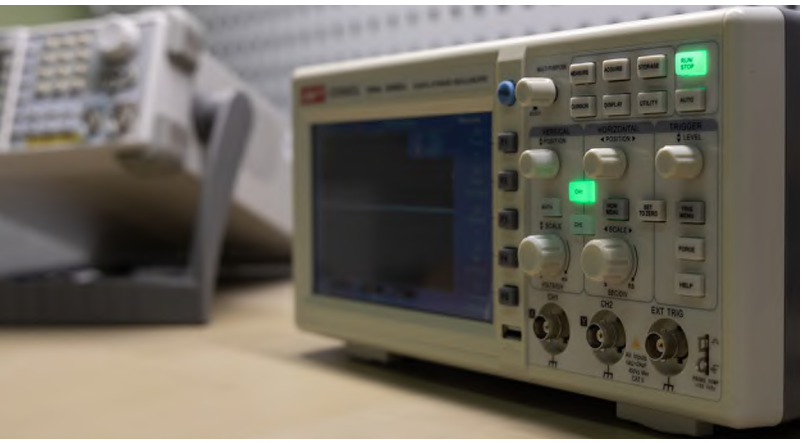
Sygnatariusze porozumienia wyrazili nadzieję, iż studia staną się płaszczyzną umożliwiającą budowanie i rozwijanie kompetencji z zakresu cyberbezpieczeństwa oraz rozwoju kadr, niezbędnych do zapewnienia ciągłości produkcji w odniesieniu do infrastruktury krytycznej naszego kraju.

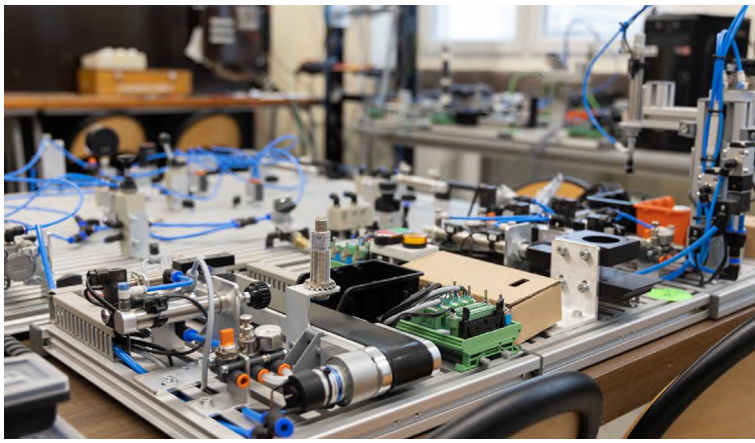
Ostatecznie 5 listopada 2022 roku na Wydziale Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej odbyła się uroczysta inauguracja roku akademickiego studiów podyplomowych „Cyberbezpieczeństwo systemów przemysłowych". Słuchaczami pierwszej edycji studiów podyplomowych zostali pracownicy Spółek Wydobywczych Skarbu Państwa, będących uczestnikami Centrum Wymiany i Analizy Informacji dla sektora wydobywczo-energetycznego (#ISACGIG).

W uroczystości inauguracji roku akademickiego udział wzięli: Podsekretarz stanu, Pełnomocnik Rządu do spraw transformacji spółek energetycznych i górnictwa węglowego, Piotr Pyzik, Prorektor ds. Infrastruktury i Promocji dr hab. inż. Tomasz Trawiński, prof. PŚ, Dziekan Wydziału Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej prof. dr hab. inż. Franciszek Plewa, Przewodniczący Centrum Wymiany i Analizy Informacji dla sektora wydobywczo-energetycznego (#ISACGIG), Piotr Toś, Dyrektor Główny Instytut Górnictwa prof. dr hab. inż. Stanisław Prusek, Dyrektor Instytut Techniki Górniczej KOMAG, dr hab. inż. Dariusz Prostański, prof. Instytutu oraz Dyrektor ds. Projektów Strategicznych CISCO Systems Poland Sp. z o.o., Piotr Skirski.

Jak zaznaczył w swoim wystąpieniu Pan Dziekan Wydziału Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej prof. dr hab. inż. Franciszek Plewa program studiów stworzono tak aby jego słu-

20 maja 2022 roku porozumienie między JSW S.A., Politechniką Śląską a ITG KOMAG





Inauguracja studiów podyplomowych
„Cyberbezpieczeństwo systemów przemysłowych”,
5 listopada 2022 roku

chacze zdawali sobie sprawę z ciążącej na nich odpowiedzialności zapewnienia ciągłości działania infrastruktury krytycznej, co jak wiemy obecnie zależy głównie od szybkich i trafnych decyzji podejmowanych w nieustannie zmieniających się warunkach.

Studia rozwijają wszechstronną wiedzę o zabezpieczeniu systemów teleinformatycznych IT&OT realizowanych procesów biznesowych, dając całościowe spojrzenie na funkcjonowanie sektora wydobywczo-energetycznego, jednocześnie dostarczając słuchaczom wyjątkowej satysfakcji i pewności działania wynikającej z ukończenia prestiżowego, wymagającego programu studiów potwierdzającego posiadanie najwyższych kompetencji zarządczych, kierowniczych i przywódczych w zakresie cyberbezpieczeństwa sektora wydobywczo-energetycznego Polski. Zakres tematyczny studiów objął m. in.:

- Zasady funkcjonowania krajowego systemu cyberbezpieczeństwa.
- Zasady działania sterowników przemysłowych.
- Krajowy system cyberbezpieczeństwa oraz inne regulacje.
- Sposoby modelowania zagrożeń oraz projektowania zabezpieczeń.
- Sposoby testowania bezpieczeństwa aplikacji i sieci komputerowych.
- Zasady gromadzenia materiału dowodowego.

Studenci w trakcie studiów podyplomowych zapoznali się z zagadnieniami związanymi z europejskim i krajowymi systemami cyberbezpieczeństwa, a także standaryzacją i certyfikacją rozwiązań teleinformatycznych w zakresie cyberbezpieczeństwa, oraz modelowaniem zagrożeń. Zapoznali się również z zagadnienia z zakresu sterowników i sieci przemysłowych oraz układów automatycznego sterowania, w tym robotów.

Dużo miejsca w trakcie studiów poświęcono zasadom budowy architektury bezpieczeństwa w przedsiębiorstwie produkcyjnym, modelowaniu zachowań oraz określaniu indywidualnych cech grup APT (Advanced Persistent Threats), bezpieczeństwu aplikacji webowych, infrastruktury sieciowej i systemów przemysłowych.

Odrębnym tematem szeroko omawianym w trakcie zajęć było zabezpieczanie środowiska chmurowego, a zwłaszcza zabezpieczanie chmury obliczeniowej przed atakami wykorzystując Standardy Cyberbezpieczeństwa Chmur Obliczeniowych. Zajęcia zakończyły zajęcia z zakresu informatyki śledczej a zwłaszcza sposobów gromadzenia materiału dowodowego. Co istotne i wielokrotnie podnoszone było w trakcie zajęć dziedzina dostarczania elektronicznych środków dowodowych wybiega znacznie poza przestępstwa komputerowe i ma zastosowanie przy każdym przestępstwie czy nadużyciu, gdzie urządzenia elektroniczne miały zastosowanie jako nośnik danych.

Studia kończą się w lipcu 2023 roku obronami prac.

SAFE PROJECT

Rozwijasz swój arsenał środków ochrony przed cyberzagrożeniami?
Pomożemy Ci dokonać wyboru!

Oferujemy rozwiązania z poniższych obszarów:

- **Kompleksowa ochrona sieci i interfejsów API**
- **Zarządzalne usługi bezpieczeństwa** (*ang. Managed Security Services*)
- **Systemy SIEM / SOAR**
- **Zautomatyzowana weryfikacja skuteczności wdrożonych zabezpieczeń** (*ang. Automated Security Validation*)
- **Automatyzacja SOC (ang. Security Operations Center)**
- **Skanowanie podatności aplikacji WEB'owych**
- **Testy bezpieczeństwa kodu źródłowego aplikacji**
- **Centralne zarządzanie konfiguracją i politykami bezpieczeństwa na zaporach i urządzeniach sieciowych**
- **Zarządzanie dostępami uprzywilejowanymi i nagrywanie sesji**
- **Ochrona stacji roboczych (EDR / XDR)**
- **Ochrona przed wyciekiem danych (DLP)**
- **Ochrona poczty elektronicznej**
- **Budowanie świadomości na temat bezpieczeństwa wśród pracowników**
- **Weryfikacja skuteczności środków ochrony przed atakami DDoS**
- **Wykonywanie kopii zapasowych i odtwarzanie danych po awarii**
- **Testowanie bezpieczeństwa firmware'u**
- **Zabezpieczenie środowiska IT z wykorzystaniem tzw. „deception technology"**
- **Konteneryzacja, zarządzanie klastrami i bezpieczeństwo środowiska Kubernetes**

Jesteśmy jedynym dystrybutorem na rynku polskim oferującym rozwiązania renomowanych firm:

BALASYS BlueVoyant

SAFE PROJECT P.S.A.
ul. Łączyny 4, 02-820 Warszawa
NIP: 9512533431, KRS: 0000946893
biuro@safeproject.pl
www.safeproject.pl

Organizacja przez ISAC GIG sesji: Cyber(nie)bezpieczeństwo: geneza, istota i rozwój podczas XXIX Międzynarodowej Konferencji Naukowo-Techniczna Górnicze Zagrożenia Naturalne – 08 listopada 2022

W ramach XXIX konferencji ,,Górnicze Zagrożenia Naturalne" ISAC GIG zorganizował, pierwszą w historii tej konferencji, sesję wprowadzającą uczestników w problematykę cyberbezpieczeństwa, Naukowcy z Politechniki Warszawskiej i Głównego Instytutu Górnictwa wygłosili dwa wykłady.

Zwrócono uwagę, że cyberprzestrzeń jest rozumiana jako zbiór technik cyfrowych służących do wymiany informacji, ale także jako nowego typu przestrzeń społeczna częściowo wirtualna, która może być bytem całkowicie odseparowanym od fizycznego. Przytoczono genezę nazwy: w latach 1968-1970 duńska artystka Susanne Ussing we współpracy z duńskim architektem Karstenem Hoffem stworzyła serię kolaży pod tytułem "CYBERSPACE". Dekadę później termin pojawił się w literaturze (William Gibson). Jako cezurę powstania cyberprzestrzeni można podać rok 1968, w którym pojawił się routing w sieci ARPANET, a także pierwszy programowalny sterownik logiczny (PLC). Natomiast dla cyberbezpieczeństwa jest to rok 1976 – opublikowanie algorytmu uzgadniania klucza przez Witfielda Diffiego oraz Martina Hellmana. W ramach wygłoszonych wykładów przedstawiono cyfryzację mowy oraz wybrane ataki (podsłuch, modyfikacja, podszycie się i wyparcie). Określono podstawowe związki pomiędzy podstawowymi usługami cyberbezpieczeństwa: poufnością, integralnością, uwierzytelnieniem i niezaprzeczalnością. Przedstawiono związki pomiędzy zagrożeniem, podatnością, zasobami i ryzykiem, a następnie zaprezentowano generycznie projektowanie zabezpieczeń jako iteracyjny proces zawierający analizę ryzyka, projekt polityki bezpieczeństwa i oszacowanie kosztów.

Omówiono są podstawowe klasy złośliwego oprogramowania oraz typowe ataki i techniki ochrony. Uwaga koncentrowała się na krajobrazie cyberbezpieczeństwa kraju w ostatnich latach, w tym atakach na kluczowe sektory gospodarki, tj. ochrona zdrowia, finanse, energetyka, transport i telekomunikacja oraz urzędy państwowe. Zaprezentowano statystyki incy-

„Cyber(nie)bezpieczeństwo: geneza, istota i rozwój”,
dr hab. inż. Krzysztof Szczypiorski (PW)

dentów odnotowywane przez zespoły zajmujące się monitorowaniem sytuacji w sieci.

W dalszej części przedstawiono zagadnienia rozpoznawania znanych ataków i anomalii tłumacząc złożoność tworzenia modeli zachowania w cyberprzestrzeni, które przeważnie nie odzwierciedlają wszystkich cech i ich dynamizmu. Omówiono koncepcję ISAC, rolę i ulokowanie w systemach cyberbezpieczeństwa i związane z tym zadania.

„ Zagrożenia w sieciach komputerowych oraz metody ochrony”, prof. dr hab. inż. Ewa Niewiadomska-Szynkiewicz (PW i GIG)

ISAC-GIG warsztaty o stosowaniu sztucznej inteligencji i Internecie Rzeczy w cyberbezpieczeństwie – 24 listopada 2022

24 listopada 2022 roku w siedzibie Głównego Instytutu Górnictwa odbyły się warsztaty ISAC-GIG dotyczące problematyki cyberbezpieczeństwa, w tym nowoczesnych metod ochrony. Pracownicy naukowi Politechniki Warszawskiej, Wojskowej Akademii Technicznej oraz państwowego instytutu badawczego NASK PIB wygłosili następujące wykłady.

Uwaga była zwrócona na dwa aspekty, tj. wykrywanie podatności oraz metody sztucznej inteligencji, i ich zastosowanie w systemach wykrywania incydentów bezpieczeństwa i ataków komputerowych.

Internet Rzeczy przestał być jedynie teoretyczną koncepcją ewolucji globalnej sieci, a powoli staje się faktem. „Inteligentne" przedmioty, mające możliwość komunikacji z siecią są wszechobecne, jednakże problemy bezpieczeństwa z tym związane, mimo że dostrzegane znacznie wcześniej, nadal nie są rozwiązane. Oprócz aspektów technicznych, także dojrzałość metod zarządzania bezpieczeństwem w Internecie Rzeczy, jest znacząco niższa niż w przypadku tradycyjnego świata IT, co wynika z krótszej historii IoT, ale także z potencjalnie większego skomplikowania i nierzadko całkowicie innych problemów. Dostarczenie rzetelnych informacji użytecznych (ang. actionable information) dotyczących podatności i eksploitów, może być przynajmniej częściowym, rozwiązaniem niektórych problemów związanych z bezpieczeństwem IoT. W trakcie prezentacji szczególną uwagę poświęcono bazie podatności i eksploitów IoT, do tworzenia której wykorzystano różnorodne mechanizmy agregacji, korelacji, analizy i automatycznej oceny rzetelności informacji, oparte m.in. na metodach sztucznej inteligencji oraz ocenie zaufania.

W ostatnich latach metody sztucznej inteligencji, w tym techniki muczenia maszynowego znajdują coraz częściej zastosowanie w cyberbezpieczeństwie. Wspierają analizę danych o zagrożeniach i budowanie świadomości sytuacyjnej, są wykorzystywane do klasyfikacji zagrożeń i wykrywania cyberataków oraz złośliwych kampanii. W ramach warsztatów omówiono różne metody uczenia maszynowego, w tym warianty sztucznych sieci neuronowych. Szczególna uwaga była zwrócona na najbardziej popularne rozwiązania – sieci głębokie, w tym sieci splotowe. Zaprezentowano wady i zalety różnych rozwiązań, podane przykłady ich zastosowań. Następnie omówio-

no możliwości zastosowania uczenia maszynowego do detekcji anomalii i wykrywania ataków cybernetycznych. Przedstawiono przykłady zastosowania klasycznych klasyfikatorów i metod głębokiego uczenia do wykrywania złośliwych aplikacji mobilnych zainstalowanych na urządzeniu użytkownika.

Przyszłe konflikty zbrojne to również w dużym stopniu wojny maszyn (wojny na algorytmy i to już nie tylko z obszaru kryptologii). Szczególnie ciekawym spostrzeżeniem jest jednak fakt, że jak się okazuje niekiedy nawet niezwykle złożone systemy wykorzystujące elementy sztucznej inteligencji można dość łatwo „oszukać". Stąd w ostatnich latach zrodził się obszar antagonistycznego uczenia maszynowego AML (ang. Adversarial Machine Learning). Wydaje się, że AML to początek bardzo poważnych badań nad wojnami maszyn, obszar niezwykle ciekawy i dynamicznie rozwijający się, ale również obszar niełatwy ze względu choćby na trudności związane z możliwością interpretacji/wyjaśnienia sposobu działania "inteligentnych" maszyn. Celem wykładu było zasygnalizowanie wyzwań związanych z nowym poziomem możliwości hakowania rozwiązań operatach o sztuczną inteligencje.

Sojusze cyberodporności w sektorze górniczym i energetycznym – czerwiec 2022

28 czerwca 2022 roku Instytut Techniki Górniczej KOMAG podpisał z Microsoft strategiczne porozumienie w zakresie zwiększenia poziomu zabezpieczeń cyfrowych systemów przemysłowych. Współpraca ta ma zapewnić zwiększoną ochronę rozwiązań z zakresu Internetu Rzeczy, gospodarki obiegu zamkniętego oraz Przemysłu 4.0.

Przedmiotem współpracy ITG KOMAG z Microsoft jest m.in. współdziałanie w obszarze rozwoju kompetencji, a także współpraca zespołów eksperckich obu organizacji w zakresie wykorzystania i rozwoju narzędzi do monitoringu, analizy oraz zapewnienia cyberbezpieczeństwa dla przemysłu. Microsoft zobowiązał się również do wsparcia ITG KOMAG w zakresie budowy i prowadzenia Laboratorium Badania Systemów Teleinformatycznych. Porozumienie przewiduje działania zwiększające zdolności operacyjne ITG KOMAG, zapewniając dostęp do wiedzy i rozwiązań sprzętowo-programowych wspierających realizację badań i prac rozwojowych związanych z cyberbezpieczeństwem przemysłowym.

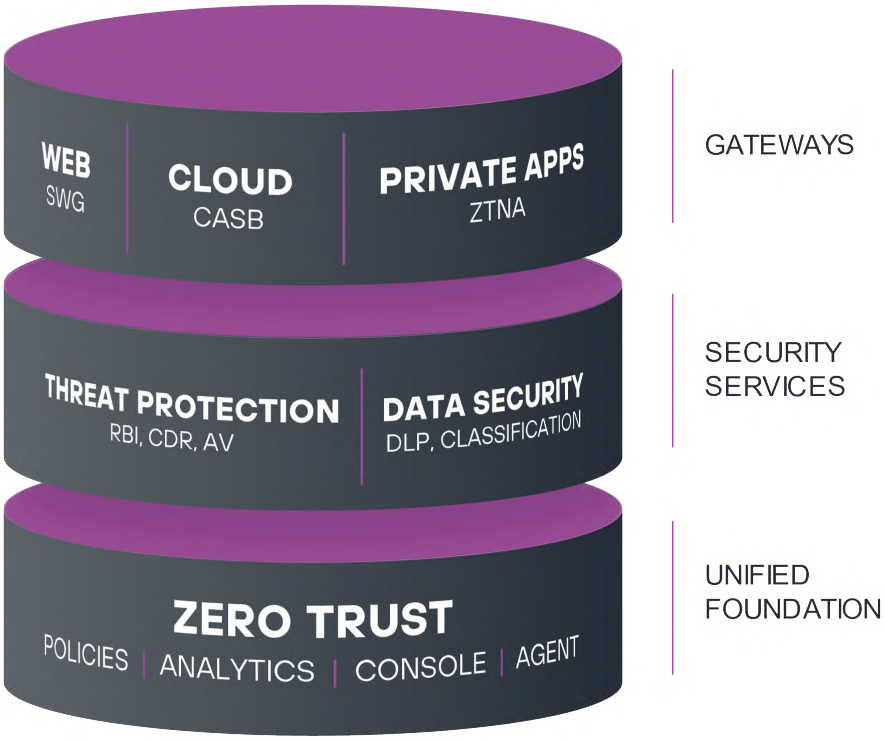
Podczas podpisywania porozumienia strony kilkukrotnie podkreślały konieczność poszerzenia współpracy w związku z odbywającą się na naszych oczach cyfrową transformacją życia codziennego obejmującą praktycznie każdy obszar gospodarki, a zwłaszcza funkcjonowanie przedsiębiorstw przemysłowych.

Piotr Toś Przewodniczący Komitetu Zarządzającego ISAC GIG przedstawił zebranym cele i strategię działania Centrum Wymiany i Analizy Informacji w Zakresie Cyberbezpieczeństwa (ISAC-GIG) podkreślając znaczenie budowania w społeczeństwie świadomości cyberbezpieczeństwa wykorzystywanych systemów informatycznych oraz automatyki przemysłowej. Jak zauważono w podsumowaniu dyskusji mechanizacja, automatyzacja i cyfryzacja górnictwa w obecnych czasach nieodłącznie związana jest z procesami wdrażania przemysłu 4.0 i Internetem rzeczy. Mimo, że przemysł wydobywczy napotyka wiele barier we wdrażaniu innowacyjnych rozwiązań, związanych ze specyfiką sektora to od lat przygotowuje się i wdraża rozwiązania, które znajdują zastosowanie również w innych gałęziach przemysłu.

Strony poinformowały o planowanej na 26 sierpnia 2022 roku uroczystości przystąpieniu Wydziału Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej oraz Instytutu Techniki Górniczej KOMAG do ISAC-GIG.

W podpisywaniu porozumienia uczestniczyli dyrektor Dariusz Prostański z Instytutu Techniki Górniczej KOMAG, Tomasz Niebylski, dyrektor ds. sektora energetycznego, telekomunikacji i produkcji, Microsoft w Polsce, Dziekan Wydziału Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej prof. dr hab. Inż. Franciszek Plewa i Piotr Toś Przewodniczący Komitetu Zarządzającego ISAC-GIG.

Forcepoint ONE



Forcepoint ONE to wszechstronna platforma chmurowa, która sprawia, że bezpieczeństwo jest proste. Umożliwia szybkie wdrożenie Zero Trust i Security Service Edge (SSE, komponent bezpieczeństwa SASE), dzięki ujednoliceniu kluczowych usługi bezpieczeństwa, w tym Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) i Zero Trust Network Access (ZTNA). Forcepoint One to jedna platforma z jedną konsolą i jednym agentem z wieloma rozwiązaniami. Zyskaj widoczność, kontroluj dostęp i chroń dane w zarządzanych i niezarządzanych aplikacjach oraz na wszystkich urządzeniach za pomocą jednego zestawu zasad bezpieczeństwa.

Więcej informacji: **www.forcepoint.com/product/forcepoint-one**

Możliwości Forcepoint ONE natywne dla chmury, Zero Trust obejmują:

- Ujednolicone bramy dostępu do aplikacji internetowych, chmurowych i prywatnych.
- Bezagentowe zabezpieczenia BYOD dla aplikacji w chmurze i prywatnych.
- Zintegrowana zaawansowana ochrona przed zagrożeniami i bezpieczeństwo danych we wszystkich środowiskach zapobiegają utracie lub eksfiltracji danych oraz uniemożliwiają hakerom dostanie się do środka.
- Dynamiczna skalowalność z globalnym dostępem – 300 punktów PoP zbudowanych w oparciu o AWS zapewnia szybką łączność z niskimi opóźnieniami i 99,99% czasu pracy niezależnie od miejsca pracy.

Ujednolicone zabezpieczenia aplikacji internetowych, chmurowych i prywatnych:

- Sieć: SWG monitoruje i kontroluje interakcje z dowolną witryną internetową w oparciu o ryzyko i kategorię, blokując pobieranie złośliwego oprogramowania lub przesyłanie poufnych danych na osobiste udostępnianie plików i konta e-mail.
- Chmura: CASB wymusza szczegółowy dostęp do korporacyjnych aplikacji SaaS i danych z dowolnego urządzenia. CASB blokuje pobieranie wrażliwych danych i blokuje przesyłanie złośliwego oprogramowania w czasie rzeczywistym. Skanuje dane w spoczynku w popularnych SaaS i IaaS w poszukiwaniu złośliwego oprogramowania i wrażliwych danych oraz w razie potrzeby dokonuje działań naprawczych. CASB wykrywa ukryte aplikacje IT i kontroluje dostęp z dowolnego zarządzanego urządzenia.
- Prywatne aplikacje: ZTNA zabezpiecza i upraszcza dostęp do prywatnych aplikacji bez komplikacji i ryzyka związanego z VPN.

ZAPRASZAMY DO KONTAKTU Z PRZEDSTWICIELEM W POLSCE:
piotr.kulik@forcepoint.com, mob. 691 490 024

*Updated May 2023

Hewlett Packard Enterprise

The Edge-to-Cloud Company

Delivering Exceptional Experiences with a Differentiated Portfolio

HPE delivers unique, open and intelligent technology solutions as a service – spanning Cloud Services, Compute, High Performance Computing & AI, Intelligent Edge, Software, and Storage – with a consistent experience across all clouds and edges, helping customers develop new business models, engage in new ways, and increase operational performance.

Strategic partner to accelerate digital transformations

HPE helps organizations drive outcomes by unlocking value from all of their data, everywhere, with businesses aligned to customer needs

Compute: Offers both general purpose servers for multi-workload computing and workload optimized servers to deliver the best performance and value for demanding applications.

Storage: Transforms the customer experience with storage as-a-service and cloud data services with portfolio offerings like primary storage, hyper-converged infrastructure, disaster and ransomware recovery, big data solutions, management offerings, and storage for unstructured data and analytics workloads, plus traditional tape, storage networking, and disk products.

HPE Services: Advises on digital transformation, designs IT solutions and helps businesses consume IT as-a-service.

HPC & AI: Delivers standard and custom hardware, software, and data-management solutions designed to support supercomputers, high-performance compute, converged edge systems, and data-intensive workloads like data analytics and artificial intelligence applications.

Intelligent Edge: Operates platforms and services at network edges, connecting devices and applications via Aruba solutions such as wired and wireless local area network, campus and data center switching, software-defined wide area networking, and network security.

HPE GreenLake Cloud Services: Provides customers with a consistent cloud experience for all applications and data wherever they live: at the edge, data center, colocation facility or across public clouds.

HPE Financial Services: Serves as the financial engine behind HPE's offerings to provide financial solutions including leasing offers, asset management, and asset upcycling.

Organizacja przez ISAC-GIG warsztatów CYBERpoligon ISAC-GIG oraz sesji szkoleniowej pt. „Cyberbezpieczeństwo w przemyśle 4.0" podczas XXXII Szkoły Eksploatacji Podziemnej – luty 2023

W trakcie XXXII Szkoły Eksploatacji Podziemnej aktywność członków ISAC GIG doprowadziła do uruchomienia prowadzonych równolegle do obrad Szkoły warsztatów „CYBERpoligon ISAC-GIG" orasz sesji szkoleniowej pt. „Cyberbezpieczeństwo w przemyśle 4.0". Przedsięwzięcie organizowane przez ISAC-GIG oraz Instytut Gospodarki Surowcami Mineralnymi PAN przy udziale Politechniki Śląskiej trwało trzy dni i zgromadziło ponad 100 osób. Z uwagi na charakter poruszanej w trakcie szkoleń problematyki zarówno sesja jak i „CYBERpoligon ISAC-GIG" były przedsięwzięciami zamkniętymi, w których udział brali jedynie członkowie ISAC GIG i zaproszeni goście.

W pierwszym dniu obrad (27.02.2023) odbył się drugi „CYBERpoligon ISAC-GIG", w których udział wzieli inżynierowie odpowiedzialni za bezpieczeństwo w firmach górniczych i energetycznych. W ramach „CYBERpoligon ISAC-GIG" zebrani mieli możliwość „walki" w realistycznym środowisku w zakresie wykrywania i reagowania na prawdziwe zagrożenia związane z usługami chmurowymi Microsoft. W zmaganiach udział wzięło 10 zespołów po 4-5 osób, którym udostępniono specjalnie przygotowane środowisko informatyczne.

Równolegle do warsztatów, w sąsiedniej sali wykładowej trwały obrady sesji szkoleniowej pt. „Cyberbezpieczeństwo w przemyśle 4-0". Wykłady i prezentacje prowadzone były przez specjalistów i ekspertów branżowych (m.in.: ISAC-GIG, Operator Chmury Krajowej, Microsoft, CISCO, Integrated Solutions) oraz uczelnie i instytuty naukowo-badawcze.

W następnym dniu, tj. 28.02.2023 r. odbyło się Zamknięte Spotkanie Komitetu Zarządzającego ISAC-GIG dla sektora wydobywczo-energetycznego.

W godzinach popołudniowych uczestnicy „CYBERpoligon ISAC-GIG" i sesji szkoleniowej wzieli udział w obradach Szkoły Eksploatacji Podziemnej w teatrze im. Juliusza Słowackiego m.in. w Gali konkursowej, podczas której przedstawiony został RAPORT „Cyberbezpieczeństwo systemów przemysłowych dla sektora wydobywczego za rok 2022" przygotowany przez Politechnikę Śląską. Ogłoszono również wyniki drugiego „CYBERpoligon ISAC-GIG". Bardzo wysoki poziom zmagań oraz wyrównana stawka ostatecznie wyłoniły zwycięzcę „CYBERpoligon ISAC-GIG – „CloudWARS", którym został Centralny Ośrodek Przetwarzania Informacji KGHM Polska Miedź SA zdobywając 1. miejsce w ćwiczeniach, drugie miejsce zajęły służby informatyczne Polskiej Grupy Górniczej SA a trzecie Tauron Polska Energia SA.

W trzecim dniu (1.03.2023 r.) zorganizowana została wizyta uczestników konferencji w krakowskim Security Operations Center (SOC) firmy CISCO, gdzie można było zapoznać się z wykorzystywanymi przez światowego potentata rozwiązaniami security oraz porozmawiać nt. sposobu organizacji i działania tego typu jednostek.

Ramowy program spotkania ISAC-GIG podczas XXXI Szkoły Eksploatacji Podziemnej obejmował wystąpienia:

- Łukasz Ciukaj – CISCO: Czy i jak wdrażać model Zero Trust w sieciach OT?
- Bartosz Krupowski - Integrity Partners: Chroń należycie swoje dane
- Janusz Małgorzaciak, Jacek Skrzydło – Microsoft: Wyzwania organizacji w budowaniu odporności w wymiarze współczesnych zagrożeń
- Adam Milczarek – Palo Alto: Pierwsza rozszerzona platforma do zarządzania i reagowania na zagrożenia
- Robert Przychodzień - Szef bezpieczeństwa OChK: Bezpieczeństwo Platformy OChK i monitoring bezpieczeństwa środowisk IT/OT w platformie Microsoft Defender i Microsoft Sentinel
- Dr inż. Sebastian Plamowski - Zespół Technik Sterowania, Instytut Automatyki i Informatyki Stosowanej, Politechnika Warszawska: Metody sztucznej inteligencji w systemach ochrony sieci przemysłowych przed cyberzagrożeniami
- Dr inż. Adam Kozakiewicz - Zespół Złożonych Systemów, Instytut Automatyki i Informatyki Stosowanej, Politechnika Warszawska: Czy bać się komputerów kwantowych - nadchodzące zagrożenie dla zabezpieczeń kryptograficznych
- Dr inż. Jędrzej Bieniasz - Zakład Cyberbezpieczeństwa, Instytut Telekomunikacji, Politechnika Warszawska: Metody ukrywania informacji w sieciach i nie tylko, czyli dwie natury technik oszukiwania zmysłów w cyberprzestrzeni
- Dr Sylwia Jarosławska-Sobór: Cyberbezpieczeństwo w dobie fake newsów
- Robert Przychodzień - Szef bezpieczeństwa OCHK: Monitoring i platforma bezpieczeństwa w oparciu o chmurę MSFT (Sentinel, defender, automatyzacja obsługi incydentów bezpieczeństwa)
- Michał Bugowski - Capgemini Poland: Budowa SOC IT/OT– Pryncypia SOC dla obszaru OT

W podsumowaniu dyskusji, uczestnicy drugiego „CYBERpoligon ISAC-GIG" podkreślali konieczność zacieśnienia współpracy pomiędzy członkami Centrum oraz potrzebę stworzenie ośrodka umożliwiającego budowanie i rozwijanie kompetencji z zakresu cyberbezpieczeństwa przekwalifikowywanych pracowników, wymianę informacji oraz zapewnienie odpowiedniej reakcji na pojawiające się zagrożenia.

Budżet
Wysoko wykwalifikowana kadra
Zaawansowane narzędzia i technologie
Współpraca z innymi podmiotami
Świadomość i edukacja
Procesy i procedury / ISO 27001, NIST, SANS
Ciągłość działania – 24/7
Monitoring i raportowanie
Skuteczność
Analityk bezpieczeństwa
Inżynier bezpieczeństwa
Manager Zespołu SOC
Architekt bezpieczeństwa
Specjalista ds. reagowania na incydenty
Specjalista do spraw zagrożeń
KOMUNIKACJA
(SOAI) Kierownik dostarczania usług

Ministerstwo
Aktywów Państwowych

XXXII Szkoła Eksploatacji Podziemnej
AGH
Honorowy patronat
Ministra Aktywów Państwowych
Ministerstwo
Aktywów Państwowych
platforma
ochk

Honorowy patronat
Ministra Aktywów Państwowych
Ministerstwo
Aktywów Państwowych
XXXII Szkoła Eksploatacji Podziemnej
JSW IT
SYSTEMS
PATRON SESJI WYKŁADOWEJ

JSW IT
chmura
krajowa
integrity
Microsoft
Poniedziałek 27.02.2023
9:00 – 17:30 Hotel Galaxy

Cyberpoligon – CloudWars
ISACGiG
JSW IT
chmura
krajowa
CISCO
integrity
Microsoft
Poniedziałek 27.02.2023
9:00 – 17:30 Hotel Galaxy

paloalto
NETWORKS
Cyberpoligon – CloudWars
FCA

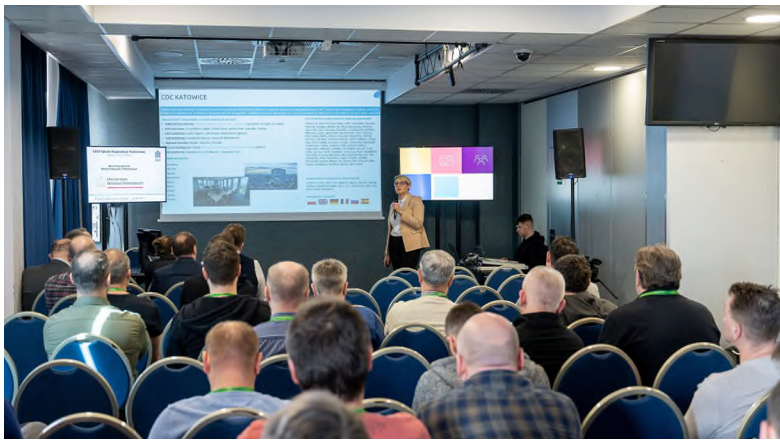
Ministra Aktywów Państwowych
Ministerstwo
Aktywów Państwowych
Cyberbezpieczeństwo cz. I
FCA

tywów Państwowych

ISACGiG
Nowi Cztonkowie ISAC-GIG
W ubiegłym roku w obecności podsekretarza stanu w Ministerstwie Aktywów Państwowych Pana Ministra Piotra PYZIKA, Wydział Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej oraz ITG KOMAG uroczyście podpisały porozumienie o wstąpieniu do Centrum Wymiany i Analizy Informacji w zakresie CYBERBEZPIECZEŃSTWA dla sektora wydobywczo-energetycznego ISAC GiG (ang. Information Sharing and Analysis Center).

ISACGiG

Budowa SOC IT/OT –
Pryncypia SOC dla obszaru OT
Michał Bugowski
Magdalena Sipek
Radosław Dusiło
Paweł Zięba
1 marca 2023



ISAC-GIG zaproszony przez Krajową Izbę Gospodarczą na 15 Economic Forum TIME – nasz głos w dyskusji o optymalnym scenariuszu cyfryzacji energetyki – marzec 2023

14 marca 2023 przedstawiciele ISAC-GIG uczestniczyli w 15 Economic Forum TIME organizowanym przez Krajową Izbę Gospodarc (KIGEiT). Uwaga Forum koncentrowała się na transformacji cyfrowej. Prof. Ewa Niewiadomska-Szynkiewicz z ISAC-GIG była moderatorem panelu ,,Optymalny scenariusz cyfryzacji energetyki".

Gośćmi Panelu byli prezesi i dyrektorzy spółek sektora energetycznego i teleinformatycznego: Grzegorz Bojar (PSE), Jarosław Tworóg (KIGEiT), Piotr Toś (ISAC-GIG), Marcin Petrykowski (Atende), Wiesław Łodzikowski (Grupa Orlen).

Problem transformacji cyfrowej jest kluczowy dla działania państwa i konkurencyjności polskiej gospodarki, szczególnie w kontekście obecnej sytuacji energetycznej na świecie. Cyfryzacja energetyki obejmuje niezwykle szerokie spektrum zagadnień, od prawnych, przez rozwiązania technologiczne, po problemy społeczne. Uwaga uczestników panelu skoncentrowała się na aspektach technologicznych, planach unowocześniania infrastruktury i wdrażaniu innowacyjnych usług cyfrowych. Dokonano oceny obecnego stanu zaawansowania procesów transformacji cyfrowej, zwracając uwagę na stopień wykorzystywania innowacyjnych technologii teleinfor-

matycznych w sektorze wydobywczym, konkretnie w podziemnych zakładach górniczych, sektorze wytwarzania i dystrybucji paliw oraz sieciach energetycznych. Następnie uwaga skoncentrowała się na obecnie realizowanych, planowanych i koniecznych do podjęcia działaniach na rzecz budowania inteligentnej energetyki przyszłości, w tym technologiach cyfrowych. Ważnym osiągnięciem, na które zwrócono uwagę jest postrzeganie infrastruktury technicznej i otoczenia jako jednego ekosystemu obejmującego wydobycie, produkcję i dystrybucję. Istotną rolę w tym ekosystemie pełni użytkownik. Sukces cyfryzacji wymaga, aby podejmowane działania były transparentne dla otoczenia sektora, efektywne dla biznesu, ale jednocześnie korzystne dla końcowego użytkownika.

Systemy energetyki to klasyczne rozproszone systemy wielkiej skali. W miarę ich rozwoju pojawiają się nowe wyzwania – jak optymalnie zarządzać tak złożoną infrastrukturą? Nie da się tego problemu rozwiązać bez zaawansowanych platform cyfrowych. Bez usług cyfrowych nie ma energetyki obywatelskiej, która włącza OZE, magazyny energii, w sposób naturalny ma strukturę systemu rozproszonego.

Uczestnicy panelu wskazali również na podstawowe problemy i ograniczenia, które spowalniają proces cyfrowej transformacji reprezentowanych przez nie branż. W przypadku podziemnych zakładów górniczych widać wyraźną potrzebę opracowania spójnej strategii i wytycznych, wskazania głównych kierunków działań oraz ustalenia standardów, które obowiązywałyby w całym sektorze. Obecnie aktywność w zakresie cyfryzacji zakładów jest rozproszona, brakuje synergii i koordynacji działań. Wyzwaniem najbliższych lat będzie również integracja, dotychczas separowanych ze względów bezpieczeństwa, systemów OT, IoT i IT. Pozwoli ona na lepszy wgląd w systemy, sprawniejsze sterowanie. Niemniej, w sytuacji wzrastającego poziomu cyberzagrożeń, realizacja tego procesu będzie wymagała ogromnej uwagi.

Uczestnicy panelu zgodnie stwierdzili, ze sektory wydobywczy i energetyczny ambitnie wkraczają w erę zaawansowanej cyfryzacji. Należy mieć tylko nadzieję, że uda się zrealizować wszystkie nowe pomysły i idee.

HPE at a glance

$28.5B FY2022 net revenue

170+ Countries with HPE Customers

35 of the top 100 supercomputers

As of 2022 Entire portfolio is offered as-a-service

99% of Fortune 500 companies are HPE customers

85,000 Channel partners around the world

Investing in innovation

Through R&D, acquisitions and partnerships to help customers today and reimagine tomorrow

Completed 18 acquisitions since 2018 including Cray, Determined AI, Axis Security, and OpsRamp

Approximately 800 patents in 2022

Hewlett Packard **Labs**

Solves complex problems in collaboration with HPE businesses to deliver differentiated IP that advances the state of the art to benefit customers

Hewlett Packard Pathfinder

Brings startup innovations to the enterprise by investing in startup companies and creating solutions combining portfolio companies' technologies with HPE products

Making a global impact as a force for good

2023 WORLD'S MOST ETHICAL COMPANIES ETHISPHERE 5-TIME HONOREE

Named one of the Ethisphere Institute World's Most Ethical Companies (2023)

seramount part of EAB

HPE earns a spot on Seramounts 2022 list of Inclusion Index Organizations

Member of the DJ Sustainability Index for nine consecutive years (2022)

HPE received S&P Global's 2022 Sustainability Award for commitment to corporate sustainability and ESG

HPE recognized as one of Fortune's Most Admired Companies for 2022 for innovation, social responsibility and leadership

HPE earns the #29 spot on Seramounts 2022 Best Companies list

Great Place To Work.

HPE is proud to be recognized, for the second year in a row, on Fortune's 100 Best Companies to Work For®

Bloomberg Gender-Equality Index 2023 Member

HPE named a member in Bloomberg's 2023 Gender-Equality Index for commitment to inclusion and ESG

Established in 2015
Following separation from HP, Inc.

Headquarters
Houston, TX

NYSE
HPE

Known As
Hewlett Packard Enterprise or HPE

CEO
Antonio Neri

For more information: https://www.hpe.com/us/en/newsroom.html

© Copyright 2023 Hewlett Packard Enterprise Development LP. May 2023.

Już w listopadzie!
W otwartym dostępie!

Doceniona w organizowanym przez Ministerstwo Edukacji i Nauki programie „Doskonała Nauka" promującym wydawnictwa o wysokim poziomie naukowym i istotnym znaczeniu dla rozwoju polskiej gospodarki!

Bogato ilustrowana, ponad pięćset stronicowa - przygotowana w dwóch wersjach językowych monografia:

Automatyzacja i monitorowanie procesu produkcyjnego w kopalniach podziemnych – polskie doświadczenia we wdrażaniu paradygmatu PRZEMYSŁU 4.0

Dedykowana jest szerokiemu gronu odbiorców zainteresowanych transformacją cyfrową tradycyjnych gałęzi gospodarki w organizacje uczące się, a więc takie które w usystematyzowany i aktywny sposób korzystając z własnych doświadczeń i dostępnych zasobów informacyjnych, optymalizują swój model biznesowy w zgodzie z paradygmatem przemysłu 4.0, zachowując konkurencyjność na zmieniającym się dynamicznie rynku.

Książka prezentuje polskie doświadczenia całych Zespołów inżynierów: informatyków, automatyków, górników, geologów i ekonomistów transformujących tradycyjną gałęź gospodarki jaką jest górnictwo w europejski koncern surowcowy z ambicjami.

Chcesz wiedzieć:

- Jak budować strategię zarządzania i nadzoru nad obszarem produkcyjnym nowoczesnego przedsiębiorstwa surowcowego?
- Jak projektować integrację i automatyzację całych procesów produkcyjnych oraz innowacyjnych rozwiązań IT/OT w cyklu produkcyjnym i handlowym w zakresie infrastruktury technicznej, łączności, aplikacji wspierających obszary bezpieczeństwa oraz przetwarzanie danych?
- Jak monitorować obszar cyberbezpieczeństwa, zabezpieczeń systemów i urządzeń automatyki wykorzystywanych w produkcji?
- Jak kreować planowanie pożądanej przyszłości, bazując na analizie doświadczeń z przeszłości oraz funkcjonowania w teraźniejszości i przyszłości?

Sięgnij i PRZECZYTAJ! Naprawdę warto!

Członkowie ISAC GIG: JSW IT Systems Sp. z o.o., Główny Instytut Górnictwa oraz Politechnika Warszawska uzyskali finansowanie projektu „Centrum monitorowania instalacji przemysłowych w podziemnych zakładach górniczych i wykrywania cyberzagrożeń” – kwiecień 2023

Program Operacyjny Inteligentny Rozwój (POIR) to największy w Unii Europejskiej program finansujący badania, rozwój i innowacje ze środków funduszy strukturalnych oraz drugi pod względem budżetu krajowy program na lata 2014-2020

Celem projektu jest podniesienie bezpieczeństwa IT/OT w podziemnych wyrobiskach górniczych. Bazując na posiadanej wiedzy i pracach B+R w projekcie wnioskodawcy zbudują centrum monitorowania cyberbezpieczeństwa i wykrywania cyberzagrożeń w podziemnych zakładach górniczych. Zweryfikowane w środowisku badawczym Kopalni Doświadczalnej ,,Barbara" centrum zostanie uruchomione i włączone do pracy operacyjnej w wybranym zakładzie górniczym Grupy Kapitałowej JSW S.A. Będzie ono wyposażone w trzy nowe rozwiązania, które przyjmą postać ostatecznej formy technologii (TRL IX): System Monitorowania Cyberzagrożeń w Górnictwie (SMCG), Sonda IDS dla OT zintegrowana z SCADA oraz dedykowany Koncentrator Danych Telemechaniki Obiektowej.

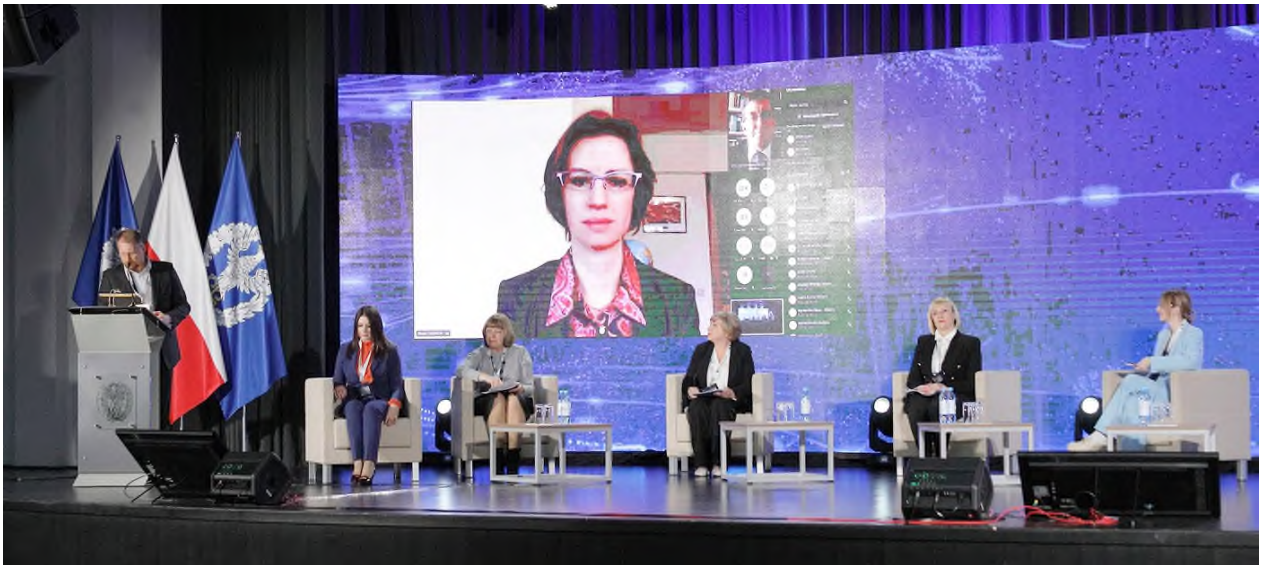
Zostaną wykonane narzędzia do pełnej integracji wymienionych narzędzi z systemami funkcjonującymi obecnie w polskich kopalniach. Dodatkowo będą opracowane, wykonane i zweryfikowane w środowisku badawczym biblioteki algorytmów wykrywania anomalii i cyberzagrożeń w sieciach OT i IoT. Będą to nowe narzędzia do detekcji zagrożeń wykorzystujące m.in. metody sztucznej inteligencji. Zbudowane w ramach projektu centrum umożliwi stałe, zautomatyzowane monitorowanie instalacji górniczych, wizualizację stanu urządzeń i procesów oraz wykrywanie anomalii i incydentów bezpieczeństwa. Dedykowane algorytmy wykrywania incydentów bezpieczeństwa pozwolą na szybką detekcję cyberataków oraz prób nieautoryzowanego dostępu a także bezpiecznego zarządzania procesami.

ISAC GIG ISAC na Warsaw Cyber Summit 2023 prezentowaliśmy podejmowane działania na rzecz budowania świadomości cyberzagrożeń i współpracy w sektorze wydobywczo-energetycznym – kwiecień 2023

W dniach 12-13 kwietnia 2023 roku w Warszawie miała miejsce międzynarodowa konferencja poświęcona tematyce cyberbezpieczeństwa ,,2023 Warsaw Cyber Summit". Organizatorem konferencji było Akademickie Centrum Polityki Cyberbezpieczeństwa (ACPC), Akademii Sztuki Wojennej w Warszawie. Wydarzenie jest kierowane do krajowego oraz międzynarodowego grona specjalistów, profesjonalistów zajmujących się cyberbezpieczeństwem na całym świecie. W ramach konferencji poruszane są różne zagadnienia, w tym istotnym tematem są aspekty prawne cyberbezpieczeństwa. Są to m.in. problemy funkcjonowania środowiska cyber w Polsce i na świecie, operacje wojskowe w środowisku cyber, współpraca na polu cyber oraz nowoczesnych technologii pomiędzy środowiskami akademickim, cywilnym, handlowym i militarnym, możliwości rozwoju i wyzwania, stojące przed środowiskiem cyberbezpieczeństwa w Polsce i na świecie.

Jednym z paneli organizowanych w ramach tegorocznej edycji konferencji był ,, Polish Experts – Round Table; Science & Business & Cybersecurity – experiences & challenges". Moderatorem dyskusji była dyrektor ACPC profesor Katarzyna Chałubińska-Jentkiewicz. Dyskusja koncentrowała się na kwestiach partnerstwa publiczno-prywatnego w zakresie odpowiedzialności za infrastrukturę krytyczną państw oraz problematykę prawodawstwa w zakresie cyberbezpieczeństwa na poziomie krajowym i międzynarodowym. Prof. Ewa Niewiadomska-Szynkiewicz z ISAC-GIG prezentowała koncepcję ISAC, rolę i ulokowanie w systemach cyberbezpieczeństwa i związane z tym zadania. Przedstawiła również działania podejmowane przez ISAC-GIG na rzecz budowania świadomości cyberzagrożeń i potrzeby współpracy na rzecz cyberbezpieczeństwa w sektorze wydobywczo-energetycznym.

ACADEMIC CENTER
FOR CYBERSECURITY POLICY
2023
WARSAW
CYBER
SUMMIT
12-13 TH APRIL 2023
WAR STUDIES
UNIVERSITY
WARSAW - REMBERTÓW
MICROSOFT TEAMS PLATFORM



12 April 2023
CYBER – LEGAL ASPECTS /
I. War & Cyberwar in Ukra
II. National cybersecurity stra
- Artificial Intelligence &
global challenges –

AP3000, najmniejszy i najbardziej energooszczędny punkt dostępowy Wi-Fi 6E na rynku, to najnowsza propozycja w portfolio produktów ExtremeWireless, która zapewnia wysokiej klasy, nową generację Wi-Fi nawet w bardzo trudnych i wymagających warunkach, takich jak np. chłodnie, hale produkcyjne i magazyny wysokiego składowania czy wypełnione uczniami klasy w szkołach. To małe lecz potężne urządzenie cechuje wyjątkowa wydajność przy jednoczesnym poborze mocy na poziomie zaledwie 13,9 W.

Nowe przełączniki rdzeniowe i agregacyjne 7520 oraz 7720 należą do grupy tzw. Uniwersalnych Platform Extreme, w przypadku których w dowolnym momencie możliwa jest zmiana systemu operacyjnego i związanych z nim funkcji, co z kolei znacząco wydłuża cykl życia sprzętu i ułatwia amortyzację inwestycji. Dzięki przystosowanej do silnie zagęszczonych środowisk, skalowalnej wszerz architekturze, wysokiej wydajności oraz opcjom wentylacji, 7720 i 7520 stanowią efektywne ekonomicznie, optymalne pod względem poboru mocy, chłodzenia i zajmowanej przestrzeni rozwiązanie dla każdego centrum operacji sieciowych!

PRZEŁĄCZNIK
7520

PRZEŁĄCZNIK
7720

PUNKT DOSTĘPOWY
AP3000X

Extreme Networks to lider w dziedzinie korporacyjnej klasy rozwiązań sieciowych dla firm oraz organizacji sektora publicznego. Extreme specjalizuje się w nowoczesnych technologiach chmurowych, a także w rozwiązaniach dla sieci typu fabric. Korzystając z zaawansowanych funkcjonalności z obszaru sztucznej inteligencji, machine learning, analityki i automatyzacji, Extreme tworzy nowe, innowacyjne sposoby łączenia ze sobą urządzeń, aplikacji i użytkowników. Wysoką jakość dostarczanych rozwiązań, usług oraz wsparcia technicznego potwierdza ponad 50 000 klientów firmy na całym świecie.

Wydział Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej wspólnie z ISAC GIG zorganizowali „Silesian CYBERhackathon" – 21 czerwca 2023

21 czerwca 2023 na Wydziale Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej odbyły się pierwszy Silesian CYBERhackathon – jego celem było zwiększanie wśród młodzieży szkół średnich świadomości społecznej na temat wpływu technologii cyfrowych na życie codzienne i zawodowe, w tym na zwiększanie bezpieczeństwa fizycznego i cyfrowego oraz ochronę klimatu, a także zachęcenie do tworzenia rozwiązań wspomagających te działania.

Patronat nad wydarzeniami objęli:

- Minister Aktywów Państwowych JACEK SASIN,
- Minister Cyfryzacji JANUSZ CIESZYŃSKI,
- JM Rektor Politechniki Śląskiej prof. dr hab. inż. ARKADIUSZ MĘŻYK,

Uważam, że to idealna okazja dla wszystkich zainteresowanych programowaniem, projektowaniem i nowymi technologiami, młodych ludzi aby spotkać się i wspólnie stworzyć innowacyjne, cyfrowe rozwiązania zadań przegotowanych przez organizatorów wywodzących się spośród Centrum Wymiany i Analizy Informacji dla sektora wydobywczo-energetycznego ISAC-GIG – powiedział prof. dr hab. Inż. Franciszek PLEWA Dziekan Wydziału Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej.

Jak informowali na specjalnie przygotowanym na tą okazję plakacie Organizatorzy wydarzenia „... Niezależnie od tego, czy jesteś początkującym programistą czy doświadczonym hackerem, hackathon oferuje moc wrażeń, inspirujące wyzwania oraz naukę nowych technologii. Na najlepsze zespoły czekają cenne nagrody!" Dodatkową atrakcją będzie możliwość udziału młodych uczestników hackathonu w CYBERpoligonie ISAC-GIG – warsztatach, na których doświadczeni pracownicy spółek skarbu państwa z sektora wydobywczego będą w realistycznym środowisku wykrywali i reagowali na cyberataki i inne prawdziwe zagrożenia związane z systemami operacyjnymi Linux oraz SCADA.

Motywem przewodni Silesian CYBERhackathon 2023 był wpływ technologii cyfrowych na życie codzienne oraz zawodowe, w tym na zwiększanie bezpieczeństwa fizycznego i cyfrowego oraz ochronę klimatu. Uczestnicy w ramach zmagań turniejowych mogli przygotować dowolne rozwiązania w formie cyfrowej: aplikacja, gra, prezentacja, symulacja, strona www, które promowałaby lub wyjaśniały zagadnienia związane z wykorzystaniem cyfrowych technologii. Dodatkowo punktowane były scenariusze zwierające wątki związane z cyberbezpieczęństwem, ochroną klimatu i pracą ludzi. Główna tematyka CYBERhackathon obejmowała:

- Bezpieczeństwo pracowników w zakładach przemysłowych
- Wydajność i efektywność w zakładach przemysłowych
- Ochrona środowiska
- Edukacja i świadomość społeczna
- Zarządzanie infrastrukturą
- Cyberbezpieczeństwo w branży wydobywczo-energetycznej
- Zastosowanie technologii cyfrowych w życiu codziennym i pracy zawodowej

AOC

Politechnika
Śląska
Silesian
University
of Technology
WYDZIAŁ GÓRNICTWA
INŻYNIERII BEZPIECZEŃSTWA
I AUTOMATYKI PRZEMYSŁOWEJ
FACULTY OF MINING , SAFETY ENGINEERING
AND INDUSTRIAL AUTOMATION

JSW IT SYSTEMS SP. Z O.O.
INFORMATYKA DLA BIZNESU
Dedykowane rozwiązani IT dopasowane do indywidualnych wymagań Klientów, oparte o najnowocześniejsze i sprawdzone produkty, pochodzące od liderów światowego rynku nowych technologii.
ul. Armii Krajowej 56, 44-330 Jastrzębie-Zdrój
JSW IT SYSTEMS
www.jswits.pl

Silesian
CyberHackatho
3 NAC

Silesian CyberHackathon
2023
2 NAGRODA
6000zł
PLATER

Silesian CyberHackathon
2023
3 NAGRODA
4000zł
DZAYLOPMENT
JSWIT
JSWSA
ISACGiG
Politechnika Śląska

Silesian CyberHackathon
2023
1 NAGRODA
8000zł
SKOPCA

Silesian CyberHackathon
2023
WYRÓŻNIENIE
2000zł
CZECHOTEAM
DYPLOM

Blisko 60 uczestników podzielonych na 11 drużyn rywalizowało o nagrody których łączna pula wyniosła 20 tys. zł.

Ostatecznie wyniki rywalizacji wyglądały następująco:

- **I miejsce** – SKOPCA z Zespołu Szkół nr 6 im. Króla Jana III Sobieskiego w Jastrzębiu-Zdroju za projekt pn. „EvaquAR".
- **II miejsce** – PLATER z II Liceum Ogólnokształcącego z Oddziałami Dwujęzycznymi im. Emilii Plater w Sosnowcu za projekt pn. „Wydział Bezpieczeństwa".
- **III miejsce** – DZAJLOPMENT z Technikum nr 1 z Zespołu Szkół Techniczno-Informatycznych w Gliwicach za projekt pn. „Safety Shield".

Dodatkowo wyróżnienie Jury otrzymała drużyna CZECHOTEAM z Liceum Ogólnokształcącego im. Marii Skłodowskiej-Curie w Czechowicach-Dziedzicach za projekt pn. „BHP game".

Pierwszy „Silesian CYBERhackathon 2023" był organizowany przez Wydział Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej wspólnie z JSW IT Systems Sp. z o.o. pod auspicjami Centrum Wymiany i Analizy Informacji dla sektora wydobywczo-energetycznego ISAC-GIG.

Wręczając młodzieży nagrody i podsumowują zmagania konkursowe, gospodarz CYBERhackathonu Pan Dziekan Franciszek Plewa podkreślił, iż na Wydziale Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej kształci się aktualnie na kierunku Automatyka i Informatyka Przemysłowa wysokokwalifikowane kadry dla przemysłu 4.0 a jego absolwenci są poszukiwani na rynku pracy, co znalazło potwierdzenie w rankingu Ogólnopolskiego systemu monitorowania Ekonomicznych Losów Absolwentów szkół wyższych, gdzie kierunek Automatyka i Informatyka Przemysłowa Wydziału Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej uplasował się na drugiej pozycji spośród wszystkich kierunków I stopnia stacjonarnych prowadzonych na Politechnice Śląskiej. Ranking ten dotyczy pierwszych absolwentów kierunku, którzy studia ukończyli w roku 2021.

Szczegółowe informacje na temat zmagań młodych informatyków znaleźć można pod adresem internetowym silesiancyberhackathon.pl.

Następny Silesian CYBERhackathon już w marcu 2024 roku – w imieniu organizatorów zapraszamy do udziału, naprawdę warto.

Za nami III Cyberpoligon ISAC-GIG, praktyczne warsztaty dla sektora wydobywczego i energetycznego – 22 czerwca 2023

22 czerwca o godzinie 08:30 rozpoczął się w murach Politechniki Śląskiej czwarty już CYBERpoligon ISAC-GIG, w trakcie którego kilkuosobowe drużyny złożone z pracowników KGHM, JSW, PGE GiEK, PGG, Bogdanki, KOMAG, Tauron Wydobycie i Węglokoks Kraj rywalizowały w odpieraniu ataków cybernetycznych na powierzone ich ochronie systemy informatyczne tym razem Linux i SCADA.

W pierwszej części poligonu siedem drużyn ISAC GIG musiało wykazać się wiedzą na temat warunków bezpieczeństwa funkcjonowania serwerów Linux. Jury oceniało znajomość konfiguracji zapory sieciowej, serwera FTP, certyfikatów SSL/TLS, uprawnień w systemie GNU/Linux, mechanizmów konteneryzacji oraz konfiguracji serwerów www.

Ciekawym i nieszablonowym problemem z którym musieli zmierzyć się uczestnicy III Cyberpoligon ISAC-GIG w murach Politechniki Śląskiej było Bezpieczeństwo środowiska Kubernetes, popularnej platformy open source do orkiestracji kontenerów - czyli do zarządzania aplikacjami zbudowanymi z wielu, w dużej mierze samodzielnych runtime'ów zwanych kontenerami. W tej części zmagań uczestnicy CYBERpoligon ISAC-GIG musieli min. utworzyć użytkowników o różnym typie uprawnień, zbudować klaster produkcyjny z przypisanymi zasadami bezpieczeństwa (Pod Security Policy, lub Pod Security Admission) i stworzyć nowego właściciela (Owner) i użytkownika: NeuVector oraz zablokować możliwości uruchamiania aplikacji klienckich we wszystkich namespace poza default i nowo utworzonymi.

Odrębnym zagadnieniem analizowanym w tym bloku zadań było wykazanie się znajomością oprogramowania open source NeuVector wykorzystywanego obecnie powszechnie do zarządzania Kubernetesem dzięki Rancher 2.6 platformie rozwijanej przez SUSE.

W drugiej części poligonu uczestnicy mieli do rozwiązania zadania dotyczące bezpieczeństwa cybernetycznego systemów klasy Supervisory Control and Data Acquisition (SCADA). Uczestnicy musieli wykazać się wiedzą na temat przepisów NIS2, identyfikacji luk w symulowanym systemie SCADA – między innymi poprzez włamanie się do niego w ciągu 40 minut.

iTSS
IT SYSTEMS & SOLUTIONS
BEZPIECZEŃST
W IT I BIZNES

BALASYS
CYBER DEFENSE
ALLIANCE

ISACGiG
KGHM
JSW SA

PoliGon*3 | PoliGon*4
SCADA:
DONT MODIFY THE
FIRMWARE

Politech
Śląska

BALASYS
ITSS

BALASYS

BALASYS
CYBER DEFENSE
ALLIANCE
BALASYS

STOWARZYSZENIE WYCHOWANKÓW
POLITECHNIKI ŚLĄSKIEJ

Roland

I miejsce
CyberPoligon
Politechnika Śląska
Gliwice 2023
II miejsce
CyberPoligon
Politechnika Śląska
Gliwice 2023
III miejsce
CyberPoligon
Politechnika Śląska
Gliwice 2023

Roland

Zadaniem tej części ćwiczeń było wykorzystanie słabych punktów w zabezpieczeniach systemu w celu uzyskania do niego nieautoryzowanego dostępu i zademonstrowania zdolności do naruszenia bezpieczeństwa infrastruktury krytycznej. Nad prawidłowością tej części zmagań czuwał Balasys twórca pierwszej na świecie modułowej zapory proxy opartej na zasadach Zero Trust.

W powszechnej opinii jury poziom zmagań IV edycji CYBERpoligonu ISAC-GIG był bardzo wysoki i wyrównany, ostatecznie najlepszymi zespołami gliwickiej rywalizacji, okazały się:

- I miejsce – JSW IT Systems Sp. z o.o.
- II miejsce – Instytut Techniki Górniczej KOMAG
- III miejsce – KGHM Polska Miedź

IV edycja CYBERpoligonu ISAC-GIG zgromadziła blisko 60 uczestników wywodzących się spośród spółek skarbu państwa pełniących kluczową rolę dla sektora wydobywczego i energetycznego w naszym kraju tj.: KGHM Polska Miedź SA, Polskiej Grupy Górniczej SA, JSW SA, Polskiej Grupy Energetycznej Górnictwo i Energetyka Konwencjonalna SA , LW Bogdanka SA, Tauron SA, Tauron Wydobycie SA i Węglokoks Kraj SA oraz Instytutu Techniki Górniczej KOMAG.

Minister Piotr PYZIK reprezentujący Ministerstwo Aktywów Państwa otwierając 22 czerwca IV edycję CYBERpoligonu ISAC-GIG powiedział: „... wierzę, że powołanie ISAC-GIG jest jednym z pierwszych elementów opracowania polityki współpracy w zakresie informatyki i telekomunikacji spółek pełniących kluczową rolę dla sektora wydobywczego kraju. W mojej ocenie jest również milowym krokiem w kierunku budowy surowcowego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego – CSIRT. Dziękując wam z zaangażowanie i zapał z jakim bronicie nas wszystkich przed zagrożeniami gospodarki 4.0 zachęcam do dalszego zacieśniania współpracy w ramach ISAC-GIG, do podnoszenia świadomości i odpowiedzialności cyfrowej sektora surowcowego będącego fundamentem nowego oblicza wolnego przemysłu wydobywczego w naszym kraju...”

Więcej informacji na temat działań ISAC GIG znaleźć można pod adresem internetowym isac.gig.eu.

Następny V CYBERpoligon ISAC-GIG odbędzie się w dniach 14-16 listopada 2023 r. w Hotel Crystal -Mountain w Wiśle podczas XXX JUBILEUSZOWAEJ MIĘDZYNARODOWEJ KONFERENCJA NAUKOWO -TECHNICZNEJ GÓRNICZE ZAGROŻENIA NATURALNE - w imieniu organizatorów zapraszamy do udziału, naprawdę warto.

I miejsce – JSW IT Systems Sp. z o.o.

II miejsce – Instytut Techniki Górniczej KOMAG

III miejsce – KGHM Polska Miedź

Cyfrowa transformacja to nasze DNA

– wywiad z dziekanem Franciszkiem Plewą gospodarzem CYBER poligonu ISAC-GIG" i pomysłodawcą Silesian CYBER hackathon 2023

Panie Dziekanie 3 kwietnia podczas już piątej edycji Akademii Bezpieczeństwa organizowanej przez Wydawnictwo Gospodarcze pod hasłem „BO NAJWAŻNIEJSZY JEST CZŁOWIEK" dyskutowano o problemach zatrudnieniowych w polskim górnictwie, dużo miejsca poświęcając zwłaszcza edukacji. Jak Pan jako Dziekan Wydziału Górniczego Politechniki Śląskiej postrzega wyzwania przed którymi nie tylko tu na Śląsku stoi obecnie cały sektor surowcowy?

Po pierwsze jestem Dziekanem Wydziału Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej i jeżeli Pan pozwoli w naszej rozmowie będę starał się być pryncypialny i precyzyjny bo w mojej ocenie to jedyny oręż w walce z kłamstwem, hipokryzją i otaczającą nas głupotą!

Po drugie gratuluję udanej konferencji! Cieszę się że Wydawnictwo Gospodarcze nie poddaje się powszechnej histerii dekarbonizacyjnej – tak trzymać! Tłumaczcie i zmuszajcie ludzi do myślenia, mimo tego, że jak mówię często moim studentom cytując Henry'ego Forda - myślenie to najcięższa praca z możliwych i pewnie dlatego tak niewielu ją podejmuje.

Pyta mnie Pan Redaktor o kierunki rozwoju zatrudnienia w przemyśle górniczym, o szkolnictwo wyższe – cały czas podkreślam nie zapominajmy o szkolnictwie zawodowym – generalnie o możliwości rozwoju zawodowego branży.

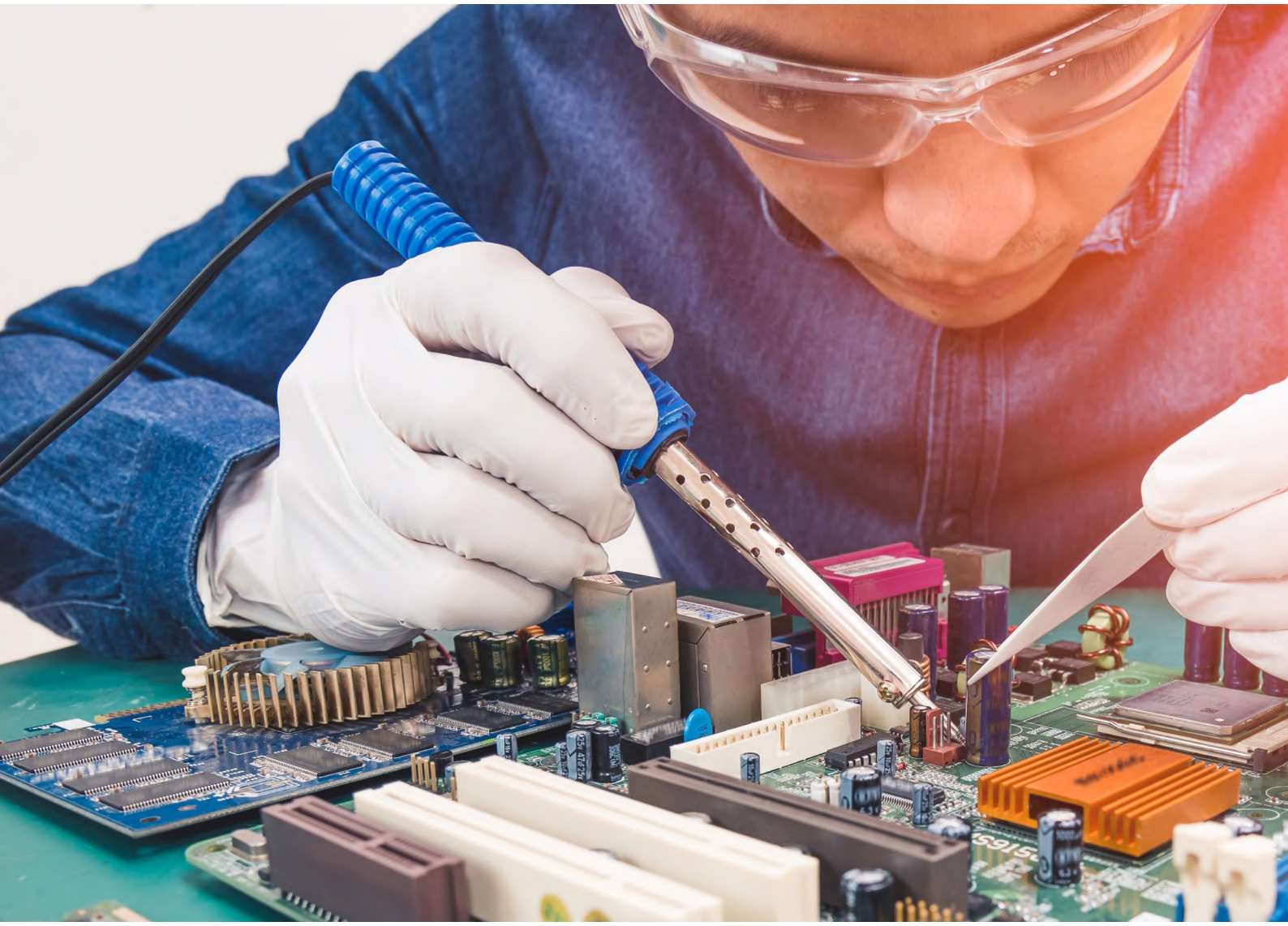
W mojej ocenie odpowiedzią na te wszystkie pytania jest: KSZTAŁCIĆ i jeszcze raz KSZTAŁCIĆ! Wychowywać młode pokolenia nowoczesnych techników i inżynierów górników. Rozwijać kierunki górnicze na uczelniach wyższych i finansować projekty badawcze górniczych instytutów naukowych. Na pewno nie likwidować Wydziałów Górniczych i nie zmieniać młodych inżynierów na siłę choćby w budowlańców.

No tak ale młodzież nie garnie się do górnictwa. Jak uczynić aby zmienić ten niepokojący trend? Jak pokazać przyszłość branży?

Często zarzuca mi się, że jestem konserwatystą, to wychodząc naprzeciw tym opiniom odpowiem na Pana pytanie parafrazując stare hasło konserwatystów, które mówi, że wszystko się musi zmienić by mogło zostać po staremu. TAK! w pierwszej kolejności my sami musimy przestać się biczować i wstydzić mówić dobrze o branży. Musimy być pryncypialni i precyzyjni w mówieniu o polskim górnictwie, pisaniu o branży, pokazywaniu młodemu pokoleniu szansy rozwoju i perspektyw ciekawego zawodu. Musimy wyzbyć się tej maniery deprecjonowania ciężkiej pracy całych pokoleń górników przez szukających taniej sensacji medialnej pseudodziennikarzy. Musimy wrócić do korzeni etosu górniczej pracy, jednocześnie rozwijając sposoby kształcenia nowych pokoleń inżynierów w zgodzie z INDUSTRY 4.0.

Musimy wreszcie przełamywać polski stereotypy postrzegania górnictwa, zbudować nasze GÓRNICTWO 4.0.!

Mało kto o tym wie ale to właśnie polscy górnicy wydobywają surowce mineralne zalegające w najtrudniejszych warunkach górniczo-geologicznych na świecie! To na śląsku zlokalizowana jest najgłębsza kopalnia węgla koksowego na świecie! Tak KWK Budryk wydobywa węgiel z głębokości 1290 m pod ziemią. To na dolnym śląsku w Lubinie KGHM planuje wydobywać rudę miedzi z blisko 2000 metrów pod ziemią tu w środku Europy nie na jakiejś pustyni w Afryce



czy Ameryce Południowej. To na Lubelszczyźnie LW Bogdanka wydobywa węgiel kamienny uzyskując wydajności plasujące ją w czołówce światowej będąc niedoścignionym wzorem dla wielu kopalń chińskich, amerykańskich i australijskich – o czym to świadczy?

O tym że potrafimy kształcić inżynierów którzy swoją wiedzą i doświadczeniem byli, są i będą elitą i będą w przyszłości podbijać nie tylko krajowy ale i światowy przemysł surowcowy. Już kształcimy młodzież która swoją kreatywnością, samodzielnością i wiedzą podbija rynek pracy. Ale kto o tym wie u nas? Czytaliście Państwo gdzieś o tym? Uważam, że nie mamy się czego wstydzić!

Czas zacząć mówić głośno że nowoczesne górnictwo nie ma nic wspólnego z łopatą i kilofem! W nadchodzących latach jeszcze bardziej ograniczony zostanie popyt na siłę roboczą wykonującą proste, powtarzalne prace nie tylko w Polsce ale całej Europie, a na znaczeniu bardzo zyskają zawody wymagające wyższych, bardziej specjalistycznych umiejętności, charakteryzujące się wysokim stopniem kreatywności – tak dziś wygląda sylwetka absolwenta na moim Wydziale Politechniki Śląskiej.

Ale czy szybka dekarbonizacja europejskiej gospodarki nie pokrzyżuje Waszych planów?

Panie Redaktorze konserwatyzm, o który jestem podejrzewany zupełnie niesłusznie w mojej ocenie będący bardziej postawą niż zbiorem twardych przekonań i raczej pewnym postrzeganiem człowieka niż spójną ideologią, każe mi nie bez pewnej nostalgii dostrzec fakt, że branża górnicza się zmienia, zresztą zawsze się zmieniała i nikt tego procesu nie zatrzyma. Niektórzy mówią, że górnictwo się likwiduje ja wierzę że mimo tendencyjnej wieloletniej nagonki różnej maści dekarbonizatorów po prostu się transformuje. Proces jest ciągły i nie należy z nim walczyć, mieliśmy już czasy ZRÓWNOWAŻONEGO ROZWOJU, GOSPODARKI O OBIEGU ZAMKNIĘTYM, a teraz mamy ZIELONY ŁAD którego elementem jest szeroko dyskutowane aktual-

nie w Polsce rozporządzenie dotyczące emisji przez polskie kopalnie metanu do atmosfery.

Czy faktycznie Komisja Europejska zasłaniając się metanem, chce szybko zlikwidować polskie górnictwo postaramy się odpowiedzieć w maju na konferencji pt.: „Klimat i energia - konsekwencje europejskiej polityki klimatycznej dla polskiej gospodarki. Globalne wyzwania i regionalne działania" już dziś wszystkich zapraszam do uczestnictwa. Wierzę że w atmosferze akademickiej dyskusji uda nam się na nowo przybliżyć i przypomnieć mieszkańcom Śląska paradygmaty europejskiego „rozwoju" – gdzie jak nie na Wydziale Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej może się odbyć dyskusja na argumenty - zawsze pryncypialnie, zawsze precyzyjnie i zawsze merytorycznie!! Tym razem o dekarbonizacji, czy likwidacji a może jak ja uważam transformacji górnictwa na rzecz gospodarki neutralnej dla klimatu. Na Śląsku doskonale wiemy, że nie można poddawać się wszechobecnej histerii klimatycznej i partykularnym interesom bogatych państw europejskich stawiających nad suwerenność energetyczną Unii Europejskiej własny interes gospodarczy i krótkowzroczność geopolityczną!

Dlatego zachowując czujność i spokój z wielką atencją obserwujemy ten proces i w sposób ciągły dostosowujemy nasz program kształcenia do aktualnych potrzeb będąc cały czas w kontakcie z naszymi przedsiębiorcami.

Wszystko po to aby jeszcze lepiej móc kształcić elity!

Czyli nie boi się Pan Dziekan, że nie będzie kogo kształcić? Jak widzi Pan transformację polskiego górnictwa?

Panie Redaktorze ja niczego się nie boję! Wydział którym kieruję transformuje się wraz z branżą już od lat, i nigdy się nie poddawaliśmy przeciwnościom losu wręcz przeciwnie zawsze wykorzystujemy je jako szansę na rozwój - zmiana jest wpisana w nasze DNA!

A teraz FAKTY - jako matematyk z wykształcenia kocham liczby, one nie kłamią i pozwalają inżynierom na fascynującą podróż po zakamarkach nauki parafrazując tytuł świetnej książki Vaclava Smili.

GÓRNICTWO dziś to nasz węgiel, ale i miedź, siarka, sól, pierwiastki ziem rzadkich oraz kopaliny pospolite - kruszywa, piasek i żwir. Mamy obecnie w Polsce ok. 7.5 tys. zakładów górniczych: podziemnych, otworowych i odkrywkowych zatrudniających bezpośrednio blisko 170 tys. pracowników, w tym ponad 75 tys. w kopalniach węgla kamiennego – w których przypomnijmy, że w roku 1990 zatrudnionych było jeszcze 388 tys. pracowników, w 2015 r. 98 tys. osób, a obecnie rzeczone 75 tys. z czego 77 proc. pracuje pod ziemią.

Dołóżmy teraz do tego fakt, że niestety czas działa na naszą niekorzyść branża się starzeje obecnie w górnictwie w regionie śląskim pracują przede wszystkim osoby w wieku 18-39 lat (49 proc. zatrudnionych). 33 proc. stanowią osoby w wieku 40-49 lat, a 50-59 lat (16 proc.), a 60 i więcej – dwa procent. W 2019 roku, biorąc pod uwagę dane dotyczące zatrudnienia w Zagłębiu Górnośląskim, średnia wieku pracownika dołowego wynosiła 36 lat, a pracownika powierzchni 48 lat. Pracujący pod ziemią robotnicy mieli średnio 36 lat, a dozoru 40 lat. Jednocześnie wśród zatrudnionych dominuje wykształcenie średnie. 48 proc. pracowników, 29 proc. posiada wykształcenie zasadnicze zawodowe, 16 proc. wyższe, a trzy procent – podstawowe.

Sytuacja jest poważna, bo nie pomaga nam również demografia. Zgodnie z prognozami GUS do 2050 roku liczba ludności w województwie śląskim względem roku 2018 zmniejszy się o 18,8%, czyli o ponad 850 tys. osób. Wielkość ta analizowana w wartościach bezwzględnych jest najwyższa w kraju.

Transformacja o którą Pan Redaktor pyta dokonuje się na naszych oczach tylko jeszcze nie wszyscy zdajemy sobie z tego sprawę! Proszę mi wierzyć środowisko naukowe odczuwa ten proces w ostatnim okresie niezwykle mocno, często podejmując radykalne działania włącznie ze zmianą dotychczasowego profilu naukowo-badawczego.

Czy zatem czekają nas jakieś radykalne zmiany na Wydziale Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej

Proszę się nie martwić ja w tym zakresie żadnych pochopnych i nieprzemyślanych działań nie zamierzam podejmować. Pragnę aby kierowany przeze mnie Wydział dzięki swej aktywności i kreatywności stał się fundamentem realizowanej transformacji dla całego sektora wydobywczo-energetycznego naszym kraju.

Musimy zrozumieć, że transformacja przemysłu w kierunku Górnictwa 4.0. i jej efekty wymagają wdrożenia w praktyce nowoczesnej górniczej edukacji inżynierskiej, przezwyciężając wynikające z niej wyzwania i wykorzystując pojawiające się szanse.

Uważam, że kluczowym elementem zachodzącej transformacji cywilizacyjnej naszego kraju, jest konkurencyjność polskiej gospodarki! Dlatego też proces transformacji musi być odpowiednio zaplanowany, monitorowany i wdrażany. Zmiany tej nie da się przeprowadzić bez odpowiedzialnych, pracowitych, oddanych tej ziemi i dobrze wykształconych młodych ludzi, musimy dbać o to aby wychowywać całe rzesze specjalistów charakteryzujących się wysokim stopniem kreatywności i zaangażowania.

To jak zaprojektować i wdrożyć atrakcyjne programy nauczania dla przyszłych inżynierów górnictwa żeby dostrzegli potencjał tej branży?

Oczywiście nie jest to proste, zważywszy jak negatywnie wielu z komentatorów naszego życia społeczno-gospodarczego postrzega GÓRNICTWO już od lat.

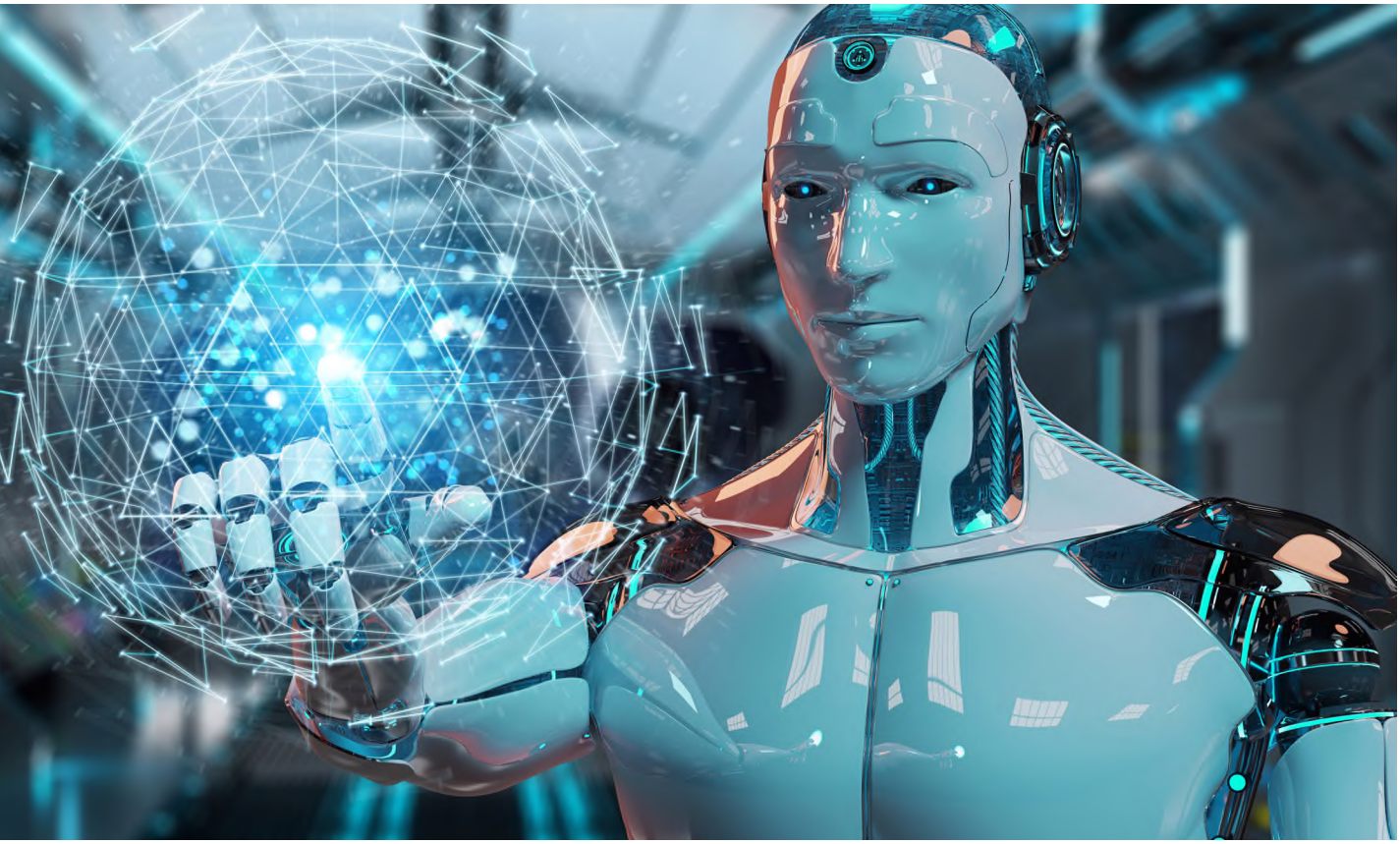
W swoich działaniach postawiłem na współpracę i zaufanie, ktoś kiedyś powiedział że Zespół nie jest grupą ludzi, którzy pracują razem. Zespół to grupa ludzi, którzy sobie ufają – takie podejście idealnie oddaje moją filozofię działania na Wydziale. Przykładem tego sposobu myślenia jest choćby nasz współpraca z Instytutem Techniki Górniczej KOMAG z którym w zeszłym roku uruchomiliśmy studia podyplomowe z zakresu Cyberbezpieczeństwa Systemów Przemysłowych czy Głównym Instytutem Górnictwa gdzie dzięki zaangażowaniu Pan Profesora Stanisława Pruska Wydział Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej stał się aktywnym członkiem powołanego w 2022 roku w Ministerstwie Aktywów Państwa przez największe spółki skarbu państwa z sektora wydobywczego Centrum Wymiany i Analizy Informacji (ISAC-GIG). Z tego miejsca chciałem podziękować prezesom PGG, KGHM, JSW, Bogdanka, Tauron i Węglokoks za zaufanie jakim nas obdarzyli przyjmując w lutym br. podczas XXXII Szkoły Eksploatacji Podziemnej w Krakowie organizowane przez Wydział studia podyplomowe z zakresu Cyberbezpieczeństwa Systemów Przemysłowych jako dedykowane dla ISAC-GIG!.

Cieszy mnie to, że to właśnie u nas Prezes Tomasz Rogala i profesor Stanisław Prusek dostrzegli potencjał wspólnego zgłębiania wiedzy w zakresie zasad funkcjonowania Krajowego Systemu Cyberbezpieczeństwa tym samym budując nowy potencjał Wydziału na przyszłość - nie szukali poza Śląskiem na wielkich uniwersytetach ale zdecydowali się postawić na nasze górnicze zasoby! Jest to o tyle ważne, że musimy mieć

świadomość, tego że rozwój innowacji i technologii w regionie wymaga sprawnie funkcjonującego szkolnictwa wyższego zarówno w kwestii proponowanych kierunków kształcenia, np. zamawianych kierunków, jak również podniesienia jakości bazy i infrastruktury szkół wyższych, która zapewni możliwość kształcenia na najwyższym światowym poziomie.

Czyli wg Dziekana Franciszka Plewy kluczem do pokonania obecnej stagnacji w edukacji górniczej jest skupienie się na rozwoju umiejętności i osobowości przyszłych inżynierów?

Rozwój indywidualnych umiejętności i osobowości przyszłych inżynierów zawsze był, jest i zapewne będzie w przyszłości podstawą nowoczesnej edukacji. W mojej ocenie nic tego nie zmieni. Wie Pan tyle się nasłuchałem na różnych konferencjach jak to źle jest w branży, że nawet Pan nie wie jak się ucieszyłem jak po uruchomieniu na Wydziale studiów podyplomowych z zakresu Cyberbezpieczeństwa Systemów Przemysłowych przyszli do mnie studenci koła naukowego z propozycją organizacji na Wydziale równolegle z „CYBERpoligonem ISAC GIG" który planujemy przeprowadzić w naszych salach laboratoryjnych w dniach 21-23 czerwca bieżącego roku dla członków Centrum Wymiany i Analizy Informacji sektora wydobywczo-energetycznego ISAC-GIG, również HACKATHONU dla licealistów śląskich szkół średnich. Młodzież uznała że nic bez nich na ich uczelni się odbywać nie może no i organizujemy „Silesian-HACKATHON 2023" – już dziś zapraszam wszystkich chętnych do udziału.



Czyli jednak odchodzimy od klasycznego górnictwa w kierunku cyfrowej rzeczywistości?

Panie Redaktorze często sobie nie zdajemy sprawy z tego, że wszystkie rewolucje przemysłowe zasadniczo zmieniły sposób pojmowania górnictwa. Mechanizacja, elektryfikacja, informatyzacja oraz systemy cyber-fizyczne to słowa klucze rewolucji 4.0.

Kto z nas pamięta, że w okresie powojennym w Polsce wybudowano dwadzieścia dwie duże nowoczesne kopalnie węgla kamiennego, pięć dużych ultranowoczesnych kopalń węgla brunatnego, osiemnaście kopalń rudy żelaza, sześć kopalń rudy miedzi, cztery kopalnie rudy cynku i ołowiu oraz szereg innych odkrywkowych i podziemnych kopalń surowców chemicznych, skalnych, drogowych i budowlanych. Wyobraża Pan sobie rozwój jakiejkolwiek gospodarki bez tych surowców nawet teraz? A przecież ktoś tych inżynierów przygotował do tego by mogli zabezpieczyć bezpieczeństwo surowcowe państwa.

Innowacje wspierane przez czwartą rewolucję przemysłową muszą znaleźć swoje miejsce w górniczej edukacji inżynierskiej. Oprócz technologii, dwa inne główne czynniki wpływające na systemy edukacji: to społeczeństwo i gospodarka. Obydwa zmieniają się również wraz z cyfryzacją, prowadząc do konieczności zmian w edukacji.

Pan i Pana czytelnicy muszą zrozumieć, że efektywne kształcenie inżynierów górniczych musi mieć na celu kształcenie studentów w taki sposób, aby byli jak najlepiej przygotowani do życia zawodowego tak w świecie sztucznej inteligencji jak i górniczej eksploatacji pierwiastków ziem rzadkich bez których nie ma sztucznej inteligencji .

Panie Dziekanie skąd tyle optymizmu, jak na konserwatystę?

Tylko pragmatyzm Panie Redaktorze. Tylko pragmatyzm!

Ktoś kiedyś powiedział, że nie jest prawdą, że moglibyśmy rozwiązać wszystkie problemy za pomocą większej ilości zasobów. Tym, czego tak naprawdę potrzebujemy jest większa wiedza. Wierzę w to, że przyszli absolwenci Wydziału Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej będą pracowali w branży kojarzącej się z nowymi technologiami które będą potrafili rozwijać. Aby tak się stało muszą myśleć procesowo, muszą potrafić działać odpowiedzialnie w swoim otoczeniu posiadając szeroką znajomością branży i głęboką wiedzę inżynierską w swojej dziedzinie.

Oznacza to, że edukacja której ich będziemy poddawać musi koncentrować się na umiejętnościach znalezienia rozwiązania nawet nieoczywistego problemu – oznacza to w praktyce że nic się nie zmienia i nadal będziemy naszą młodzież uczyli myśleć – bo myślenie w mojej ocenie ma przyszłość.

STINET

Dbamy **o bezpieczeństwo biznesów w sieci!**

DLACZEGO STINET?

Stinet od 1996 roku specjalizuje się w dostarczaniu technologii z zakresu bezpieczeństwa IT we wszystkich sektorach gospodarki. Firma powstała w oparciu o wspólną wizję – sukces naszych Klientów poprzez zapewnienie ciągłości działania w obliczu zwiększonego ryzyka cyberataków. Dlatego starannie dobieramy technologie należące do światowych liderów z zakresu cyberbezpieczeństwa. Oferujemy rozwiązania nowej generacji zapewniające ochronę przed atakami i zagrożeniami, od punktu końcowego do brzegu sieci i chmury.

NASZE ATUTY

- Zespół inżynierów z wieloletnim doświadczeniem
- Ugruntowana pozycja na rynku, liczne nagrody i wyróżnienia
- Wysokie kompetencje w zakresie projektowania, dostawy i implementacji
- Wsparcie techniczne oraz dedykowane szkolenia i warsztaty
- Znakomita znajomość procesów biznesowych
- Umowy partnerskie z wiodącymi producentami rynku cyberbezpieczeństwa

Solec 18, lok. U61
00-410 Warszawa

+48 22 740 42 20

biuro@stinet.pl

www.stinet.pl

Organizacja przez ISAC-GIG konferencji „Cyfrowy, Bezpieczny Śląsk 2030 – strategia zarządzania cyberbezpieczeństwem w dobie transformacji cywilizacyjnej" – 22-23 czerwca 2023 rok

22 czerwca od godzinie 14:00 Jego Magnificencja Rektor Politechniki Śląskiej Prof. dr hab. inż. Arkadiusz MĘŻYK wspólnie z Dyrektorem Głównego Instytutu Górnictwa Prof. dr hab. inż. Stanisławem PRUSKIEM w obecności ministra Piotra PYZIKA otworzyli konferencję „Cyfrowy, Bezpieczny Śląsk 2030 – strategia zarządzania cyberbezpieczeństwem w dobie transformacji cywilizacyjnej."

Zakres tematyczny konferencji objął :

- Bezpieczeństwo Informacji jako kluczowy element transformacji cyfrowej Śląska.
- Konsolidacja w cyberbezpieczeństwie – przyjaciel, czy wróg?
- Strategia zarządzania cyberbezpieczeństwem.
- Szkolenia w obszarze cyberbezpieczeństwa w ramach OUK wraz elementami ryzyka i forensic w bezpieczeństwie

W trakcie konferencji przyjęto do ISAC-GIG kolejnych dwóch członków: Polską Grupę Energetyczną Górnictwo i Energetyka Konwencjonalna oraz Tauron Wydobycie.

Podczas uroczystego podpisywania porozumień o współpracy Wydziału Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej z partnerami przemysłowymi Prof. dr hab. inż. Franciszek PLEWA Dziekan Wydziału powiedział: „… Szanowni Państwo możliwość organizacji na naszym Wydziale w murach Politechniki Śląskiej trzeciej edycji CYBERpoligonu ISAC-GIG jest dla nas wyróżnieniem ale i swoistym zobowiązaniem związanym z podnoszeniem świadomości cyfrowej oraz rozwojem kompetencji w zakresie cyberbezpieczeństwa. To Uczestnictwo w swoistym sojuszu największych Spółek Skarbu Państwa z sektora wydobywczego na rzecz budowy spójnej polityki w dziedzinie cyberobronności, pozwala nam kształcić wysokokwalifikowanych specjalistów w tym zakresie, Cyfrowa transformacja wpisana jest w nasze DNA …"

Jako pierwsze porozumienie o współpracy podpisano list intencyjny z SUSE Polska Sp. z o.o. to w zakresie kształcenia cyberbezpieczeństwa systemów

Politechnika
Śląska

Politechnika
Śląska

iTSS
FCA
JSWSA

Politechnika
Śląska
POLIGON
apex.it

CYBERPOLIGON
SUSE
SUSE

ISACGiG
KGHM
JSWSA
JSWIT
GiG
KOMAG

atman
BALASYS
Extreme networks
FCA
Forcepoint
TREND
STINET
SUSE
SAFE PROJECT
TEKNISKA
JSW SA
ISACGiG
Politechnika Śląska

Politechnika Śląska

Politechnika Śląska

Moment uroczystego przyjęcia do ISAC-GIG kolejnych dwóch członków: Polskiej Grupy Energetycznej Górnictwo i Energetyka Konwencjonalna oraz Tauron Wydobycie

Podpisanie porozumienia o współpracy Wydziału Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej z SUSE Polska Sp. z o.o. w zakresie kształcenia cyberbezpieczeństwa systemów przemysłowych i zarządzania środowiskiem skonteneryzowanym

Podpisanie porozumienia o współpracy Wydziału Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej z BALASYS IT Zrt w zakresie kształcenia studentów w obszarze cyberbezpieczeństwa systemów teleinformatycznych ze szczególnym uwzględnieniem systemów przemysłowych

Podpisanie porozumienia o współpracy Wydziału Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej z firmą Hewlett Packard Enterprise Polska Sp. z o.o.

Wręczenie nagród i wyróżnień dla zwycięzców Silesian CYBERhackathon 2023

przemysłowych i zarządzania środowiskiem skonteneryzowanym

Drugie porozumie o współpracy pomiędzy Wydziałem Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej a BALASYS IT Zrt. Podpisano w zakresie kształcenia studentów w obszarze cyberbezpieczeństwa systemów teleinformatycznych ze szczególnym uwzględnieniem systemów przemysłowych.

Trzecie porozumienie o współpracy Wydział Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej zawarł z firmą Hewlett Packard Enterprise Polska Sp. z o.o. w zakresie wzajemnego prezentowania i propagowania osiągnięć w zakresie nowych technologii i wymiany doświadczeń w zakresie praktycznych elementów kształcenia.

Szczególnie miłym punktem inauguracji konferencji „Cyfrowy, Bezpieczny Śląsk 2030 – strategia zarządzania cyberbezpieczeństwem w dobie transformacji cywilizacyjnej" było wręczenie w trakcie jej otwarcia nagród i wyróżnień dla zwycięzców odbywającego się dzień wcześniej jako wydarzenia towarzyszącego CEBERpoligonowi ISAC GIG tj.: Silesian CYBERhackathon 2023 – pierwszych na Śląsku zawodów skierowanych do młodzieży szkół średnich zainteresowanej informatyką i automatyką przemysłową w tym rozwojem programowania.

Silesian CyberSecurity Hub to ważny element strategii zarządzania cyberbezpieczeństwem w dobie transformacji cywilizacyjnej

– rozmowa z Dyrektorem Naczelnym Głównego Instytutu Górnictwa – Państwowego Instytutu Badawczego Prof. dr hab. inż. Stanisławem PRUSKIEM

Panie Profesorze, podczas trzeciej edycji CYBERpoligonu ISAC GIG organizowanego w dniach 21-23 czerwca 2023 na Wydziale Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej, który otwierał Pan wspólnie z Jego Magnificencją Rektorem Politechniki Śląskiej Prof. dr hab. inż. Arkadiuszem MĘŻYKIEM zorganizowano również konferencję „Cyfrowy, Bezpieczny Śląsk 2030 – strategia zarządzania cyberbezpieczeństwem w dobie transformacji cywilizacyjnej", w czasie której po raz pierwszy szerokiemu gronu zaprezentowana została idea Programu Bezpieczny Cyfrowy Śląsk 2030. Czy może nam Pan zdradzić skąd się wziął ten pomysł i jak wygląda jego realizacja?

W kwietniu 2021 roku w Głównym Instytucie Górnictwa rozpoczęto prace koncepcyjne związane z uruchomieniem strategicznego programu badawczego pt.: Bezpieczny Cyfrowy Śląsk 2030. W mojej ocenie niezwykle ambitnej inicjatywy, która ma na celu zwiększenie świadomości i zapewnienie bezpieczeństwa cyfrowego mieszkańcom Śląska w dobie transformacji cywilizacyjnej.

Całość koncepcji oparta została na założeniu, że nadrzędnym celem programu Bezpieczny Cyfrowy Śląsk 2030 będzie budowa w należącej do GIG-PIB Kopalni Doświadczalnej „Barbara" w Mikołowie, Ośrodka Rozwoju Innowacyjnych Kompetencji Cyfrowych, którego zadaniem w perspektywie najbliższych lat będzie:

- utworzenie Centrum Wymiany i Analizy Informacji na temat podatności, zagrożeń i incydentów w celu wspierania podmiotów krajowego systemu cyberbezpieczeństwa obecnie jest to ISAC GIG,
- rozwój kompetencji cyfrowych, zwłaszcza w zakresie cyberbezpieczeństwa jednostek samorządu terytorialnego, dużych, małych i średnich przedsiębiorstw, budowa bazy szkoleniowej w zakresie cyberbezpieczeństwa, wraz z uruchomieniem programu wyszukiwania i szkolenia najzdolniejszych studentów Cybersecurity Talent Identification and Assessment Program – CTIAP
- tworzenie zabezpieczeń technologicznych zapewniających ciągłość działania systemów przemysłowych IT/OT, umożliwiających koordynowanie i aktywne reagowanie na incydenty w cyberprzestrzeni, stworzenie Centrum Monitoringu Transformacji Regionu bazującego na pozyskaniu źródłowych danych produkcyjnych i środowiskowych z kopalń objętych procesem transformacji.

ISACGiG
Centrum Wymiany i Analizy Informacji

FILARY PROGRAMU: CYFROWY BEZPIECZNY ŚLĄSK 2030

Taki pomysł zrodził się na przełomie roku 2021/2022, a wszystko po to, aby dzięki systematycznie orgaznizowanym Cyberpoligonom i szkoleniom, przygotowywaniu raportów oraz analiz, stać się liderem opinii i twórcą ekosystemów podnoszących odporność na cyberataki.

Innowacyjny pomysł, dobrze przygotowany, szczególnie pod kątem realnych kosztów, został przedstawiony w Urzędzie Marszałkowskim który po zapoznaniu się z naszą koncepcją włączył ją do Terytorialnego Planu Sprawiedliwej Transformacji Województwa Śląskiego do roku 2030, wspierającego działania ukierunkowane na podnoszenie poziomu innowacyjności gospodarki, rozwój nowych kompetencji związanych z koniecznością dostosowania zatrudnionych w branży górniczej i okołogórniczej do zachodzących zmian oraz efektywny i społecznie odpowiedzialny system zarządzania transformacją.

Ostatecznie przygotowane przez nas projekty składające się na program badawczy „Bezpieczny Cyfrowy Śląsk 2030" prezentują trzy filary tj.:

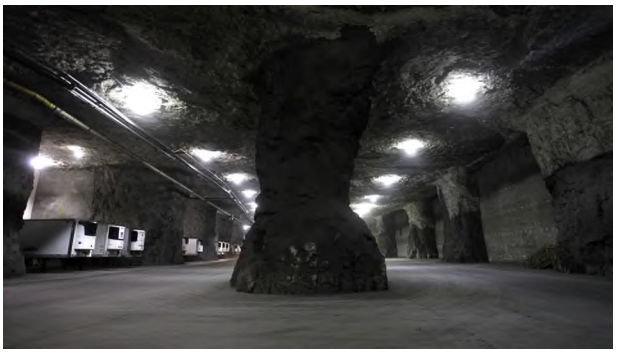
> Ośrodek kompetencji cyfrowych - Silesian CyberSecurity Knowledge Center
> Ośrodek monitoringu transformacji regionu - Mining Transformation Monitoring Center
> Ośrodek zabezpieczenia technologicznego - Silesian CyberSecurity Data Center

Wierzę, że już niebawem będziemy mogli rozpocząć przekształcać Kopalnię Doświadczalną „Barbara", która - przypomnijmy - w przeszłości prowadziła normalną działalność wydobywczą, w nowoczesny ośrodek informatyczny ze zlokalizowanym pod ziemią nowoczesnym Data Center, który stanie się dobrym przykładem transformacji cyfrowej, nie tylko Śląska, ale całej branży surowcowej.

Podziemna serwerownia zlokalizowana w wyrobiskach Kopalni Doświadczalnej „Barbara", czy to w ogóle możliwe?

O utworzeniu nowoczesnego centrum przetwarzania danych (Data Center) na Śląsku mówi się od lat - my posiadamy idealną lokalizację oraz warunki do stworzenia takiego miejsca. Podstawową zaletą lokalizacji naszego Data Center w wyrobiskach podziemnych jest utrzymanie dużego stopnia bezpieczeństwa przechowywanych danych w łatwiejszy sposób niż przy korzystaniu z tradycyjnych serwerowni. Klienci centrów przetwarzania danych wymagają niezawodności serwerów i pełnej dostępności. Wszelkie urządzenia IT oraz wspomagające zlokali-

Najbardziej energooszczędna serwerownia w Europie znajduje się w norweskiej kopalni oliwinu Lefdal 150 m pod ziemią. Źródło www.datasenterindustrien.no.



W amerykańskim Springfield w stanie Missouri w starej podziemnej kopalni wapienia około 25 m pod ziemią zlokalizowano centrum przetwarzania danych o powierzchni ponad 7,5 tys. m^2.
Źródła: missouripartnership.com i eu.news-leader.com.

zowane pod ziemią nie są narażone na złe warunki atmosferyczne oraz inne sytuacje losowe, że o wojnie nie wspomnę.

Na świecie dostawcy usług internetowych od lat współpracują z wieloma zlokalizowanymi pod ziemią centrami przetwarzania danych. Najbardziej energooszczędna serwerownia w Europie znajduje się w norweskim Lefdal. Jest ona zlokalizowana 150 m pod ziemią w wyrobiskach dawnej kopalni oliwinu i działa od 2017 r.

W amerykańskim Springfield w stanie Missouri w starej podziemnej kopalni wapienia około 25 m pod ziemią, zlokalizowano centrum przetwarzania danych o powierzchni ponad 7,5 tys. m^2. Podobne serwerownie podziemne funkcjonują w Pensylwanii i Kansas City. Centrum w Kansas City zlokalizowane jest 34 m pod powierzchnią terenu, a centrum w Pensylwanii znajduje się około godziny drogi od miasta Pittsburgh, 70 m pod ziemią.

Nasze Data Center poprzez wykorzystanie istniejących wyrobisk podziemnych pozwala ograniczyć koszty związane z inwestycją w takie centrum przetwarzania danych, ponieważ nie jest wymagane budowanie całego budynku serwerowni czy wynajmowanie drogich powierzchni. Obniża się również koszty związane z chłodzeniem urządzeń – pod ziemią panuje stała temperatura, a także nie ma bezpośredniego wpływu światła słonecznego. Co więcej, zabezpieczenie terenu takiej lokalizacji jest łatwiejsze niż przy korzystaniu z tradycyjnych serwerowni.

Silesian CyberSecurity Hub będzie Śląską Chmurą Obliczeniową zbudowaną w oparciu o Data Center KD „Barbara" i w mojej ocenie winien stać się ważnym elementem Rządowej Chmury Obliczeniowej w obszarze monitoringu transformacji polskiej energetyki.

Mówiąc o programie „Cyfrowy, Bezpieczny Śląsk 2030" myślami jesteśmy w niedalekiej - ale jednak przyszłości, widzimy główne filary projektu koncentrujące się wokół idei budowy Silesian CyberSecurity Hub. Jaka jest szansa na realizację tej idei w zaprezentowanej formule?

Myślę, że przygotowany przez nas w 2021 roku program nie stracił nic na swojej atrakcyjności oraz aktualności, a wojna w Ukrainie tylko potwierdziła zasadność formułowanych przez nas rok przed jej wybuchem tez, nadając im dodatkowego znaczenia.

Ktoś kiedyś powiedział, że przeszłość jest w naszych głowach, a przyszłość w naszych rękach, słowa te potwierdził dobitnie miniony rok. Rok funkcjonowania Centrum Wymiany i Analizy Informacji dla sektora wydobywczo-energetycznego (ISAC GIG). Intensywność realizowanych w tej formule inicjatyw zaskoczyła wielu, ale nie nas, udowadniając że nie czekamy z założonymi rękami na to, że pieniądze spadną nam z nieba! Pracujemy integrując całe środowisko Polskiego Sektora Wydobywczego do podnoszenia świadomości i odpowiedzialności cyfrowej będącej fundamentem nowego oblicza przemysłu wydobywczo-energetycznego w naszym kraju.

Gdyby ktoś dwa lata temu zapytał czym jest Silesian CyberSecurity Hub usłyszałby odpowiedź, że Ośrodkiem Rozwoju Innowacyjnych Kompetencji Cyfrowych zbudowanym w Kopalni Doświadczalnej „Barbara" z jedyną w Polsce nowoczesną serwerownią ulokowaną w wyrobiskach podziemnych. Dziś po roku funkcjonowania ISAC GIG, Silesian CyberSecurity Hub to przede wszystkim porozumienie i współpraca Głównego Instytutu Górnictwa - Państwowego Instytutu Górnictwa, Wydziału Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej i Instytutu Techniki Górniczej KOMAG na rzecz Spółek Skarbu Państwa pełniących kluczową rolę dla polskiego sektora wydobywczo-energetycznego.

Silesian CyberSecurity Hub to również a może przede wszystkim porozumienie świata nauki i przemysłu - branży wyjątkowo ważnej dla bezpieczeństwa funkcjonowania naszego państwa - na rzecz trwałego zabezpieczenia na wielu polach elementarnego węzła koncentracji głównych strumieni danych naszej infrastruktury krytycznej.

Proces przekształcania Kopalni Doświadczalnej "Barbara", prowadzącej w przeszłości normalną działalność wydobywczą, w nowoczesny ośrodek informatyczny ze zlokalizowanym pod ziemią nowoczesnym centrum przetwarzania danych może być wzorcowym przykładem transformacji cyfrowej nie tylko Śląska

Chciałbym, aby Silesian CyberSecurity Hub stał się bazą szkoleniową dla wszystkich funkcjonujących i powstających ISAC'ów w całej Polsce. Posiadamy doświadczenie oraz osiągniecia w budowaniu sprawnie działających Centrów Wymiany i Analizy Informacji w zakresie cyberbezpieczeństwa. Chcemy stać się ważnym elementem Rządowej Chmury Obliczeniowej w obszarze monitoringu transformacji polskiej energetyki, chcemy wspólnie z Politechniką Śląską uruchomić program wyszukiwania i szkolenia najzdolniejszych studentów Cybersecurity Talent Identification and Assessment Program – CTIAP, chcemy wreszcie wspólnie z Instytutem KOMAG zbudować szybką ścieżkę certyfikacji w zakresie cyberbezpieczeństwa produktów IT/OT, które będą uznawane w Europie.

Czyli nadzieja w młodzieży, a siła w sojuszach? Czy Silesian CyberSecurity Hub to nowa jakość na naukowej mapie polski?

Bardzo bym chciał, aby nasza współpraca na Śląsku dała nową jakość. Bez wątpienia gramy w jednej drużynie, a nasz zespół nie jest grupą ludzi, którzy tylko pracują razem. Nasz zespół to grupa ludzi, którzy sobie ufają tak w kontekście nauki, nowych i innowacyjnych pomysłów jak i projektów badawczych i inicjatyw, które mają na celu rozwijanie i unowocześnianie polskiego sektora naukowego.

Porozumienie Głównego Instytutu Górnictwa, Wydziału Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej oraz Instytutu Techniki Górniczej KOMAG umożliwia poprzez organizowane studia podyplomowe, szkolenia i wymianę informacji oraz zapewnienie odpowiedniej reakcji na pojawiające się zagrożenia - budowanie i rozwijanie kompetencji z zakresu cyberbezpieczeństwa tak na rzecz Spółek Skarbu Państwa, Jednostek Samorządu Terytorialnego jak i innych uczestników Krajowego Systemu Cyberbezpieczeństwa.

Zrobiliśmy wszyscy jako ISAC GIG w pierwszym roku funkcjonowania Centrum bardzo dużo, aby pokazać nasza determinację i kreatywność, przed nami długa droga i dużo, bardzo dużo pracy, ale wierzę, że osiągniemy stawiane sobie cele stając się ostatecznie ważnym element strategii zarządzania bezpieczeństwem w dobie transformacji cywilizacyjnej. Czego sobie i państwu życzę.

Rozmowę przeprowadzono podczas 3 CYBERpoligonu ISAC GIG organizowanego w dniach 21-23 czerwca 2023 na Wydziale Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej, Politechniki Śląskiej w Gliwicach

Politechnika
Śląska
CYBERPOLIGON
TREND

Politechnika
Śląska
CYBERPOLIGON
TREND

TREND

Szczegółowy Program konferencji "Cyfrowy, Bezpieczny Śląsk 2030 – strategia zarządzania cyberbezpieczeństwem w dobie transformacji cywilizacyjnej"

Dzień I: 23.06.2023

13:00 – 13:10 Przywitanie zaproszonych gości i uczestników konferencji Prof. dr hab. inż. Franciszek Plewa – Dziekan Wydziału Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej

13:10 – 13:20 Uroczyste otwarcie obrad konferencji Prof. dr hab. inż. Arkadiusz Mężyk – Rektor Politechniki Śląskiej Prof. dr hab. inż. Stanisław Prusek – Dyrektor Instytutu GIG

13:20 – 13:40 Centrum Wymiany i Analizy Informacji ISAC GIG rok działania w zakresie zarządzania cyberbezpieczeństwem w spółkach sektora wydobywczoenergetycznego Piotr Toś – Prezes JSW IT Systems Sp. z o.o., Przewodniczący Komitetu Zarządzającego ISAC GIG

13:40 – 14:00 Cyfrowy, Bezpieczny Śląsk 2030 – strategia zarządzania cyberbezpieczeństwem w dobie transformacji cywilizacyjnej Prof. dr hab. inż. Stanisław Prusek – Dyrektor Instytutu GIG, Piotr Toś – Prezes JSW IT Systems Sp. z o.o., Przewodniczący Komitetu Zarządzającego ISAC GIG

14:00 – 14:20 Cyberbezpieczeństwo systemów przemysłowych dla sektora wydobywczego za rok 2022" – prezentacja głównych tez RAPORTU ISAC GIG i Politechniki Śląskiej - dr inż. Artur Dylong, Wydział Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej

Panel I – Bezpieczeństwo Informacji jako kluczowy element transformacji cyfrowej Śląska

15:00 – 15:20 HPE – Wielopoziomowe bezpieczeństwo infrastruktury IT od serwera aż po sieć
Maciej Kalisiak – HPE Compute and Data Services Sales Manager

15:20 – 15:40 Extreme Networks – Bezpieczeństwo i automatyzacja dostępu do sieci
Adam Minowski – Senior Systems Engineer Extreme Networks

15:40 – 16:00 FCA, Forcepoint: DLP anywhere – jak chronić dane swojej organizacji w dobie pracy zdalnej
Julian Kujawski – FCA S.A., Dyrektor Rynku, Dział Sprzedaży Krajowej
Aleksander Raczyński – Forcepoint, Sales Engineering EEUR – EMEA,
Łukasz Leszkiewicz – FCA S.A., Product Manager

Politechnika Śląska
CYBERPOLIGON
Hewlett Packard Enterprise
apex it

Problemy zarządzania regułami bezpieczeństwa systemów informatycznych
Urządzenia od różnych producentów, różne systemy monitorowania i konfiguracji.
Setki/tysiące reguł i zapisów w obszarze polityk bezpieczeństwa.
Skomplikowanie konfiguracji reguł w czasie.
Czynnik ludzki, ograniczone zasoby, brak know-how, czasu i budżetu.
Migracje technologii, kompatybilność.
Proceduralne i audytowe wymagania zgodności.
Policies
Standards
Guidelines
Procedures
FIREMON

ENDPOINTS
AILS
HIGH PRIORIT
ALERTS WI

Panel II – Konsolidacja w cyberbezpieczeństwie. Przyjaciel, czy wróg?

16:00 – 16:20 SUSE: Bezpieczeństwo w środowiskach Open Source
Marcin Madey, Prezes Zarządu SUSE Polska

16:20 – 16:40 SafeProject, Zarządzanie politykami bezpieczeństwa na firewallach i urządzeniach sieciowych na przykładzie rozwiązania Firemon oraz Cyberbezpieczeństwo IT i OT. Rozwiązania: Logsign, LiveAction.
Jarosław Paszke – Wiceprezes Safe Project P.S.A.
Adam Książek – Prianto Polska
Aleksander Turewicz, Business Development Manager – Poland

16:40 – 17:00 Balasys: From Zero Trust to NIS2 and CER
Patrik SZALAI – lider Zespołu Przedsprzedażowego (ang. Pre-sales Team Leader), firma Balasys

Panel III – Strategia zarządzania cyberbezpieczeństwem

17:00 – 17:20 Trend Micro: Automatyzacja procesów w cyber bezpieczeństwie – Platforma Trend Micro Vision One
Joanna Dąbrowska – Trend Micro

17:20 – 17:40 ITSS: Praktyczne podejście do całościowej ochrony przed zagrożeniami na przykładzie produktów Trend Micro i doświadczenia integratora – firmy IT Systems and Solutions Sp. z o.o.
Łukasz Miązek/Grzegorz Łazęcki – IT Systems and Solutions Sp. z o.o.

17:40 – 18:00 TXOne i ITSS: Ochrona środowisk ICS za pomocą systemu zabezpieczeń klasy przemysłowej TXOne
Sebastian Mazurczyk – TXOne Networks

Dzień ii: 24.06.2023

08:30 – 09:00 Przywitanie uczestników CYBERpoligonu

09:00 – 12:00 Rozpoczęcie warsztatów CYBERpoligon część I

12:00 – 13:00 Lunch

13:00 – 17:00 Rozpoczęcie warsztatów CYBERpoligon część II

17:00 – 17:30 Rozstrzygnięcie - wyniki CYBERpoligonu

Panel IV – Szkolenia w obszarze cyberbezpieczeństwa w ramach OUK wraz elementami ryzyka i forensic w bezpieczeństwie

10:00 – 10:25	ITSS: Zarządzanie podatnościami, a Bezpieczeństwo Informacji Łukasz Miązek – IT Systems and Solutions Sp. z o.o
10:25 – 10:45	TrendMicro: Zabezpieczenie materiału dowodowego Joanna Dąbrowska – Trend Micro
10:45 – 11:05	TrendMicro, ITSS: Czy muszę budować Security Operations Center? Sławomir Dec – Trend Micro
11:05 – 11:25	Extreme Networks: Bezpieczeństwo sieci bezprzewodowych Adam Minowski Senior – Systems Engineer Extreme Networks
11:25 – 11:45	Stinet sp. z o.o., Arrow ECS: Cyberbezpieczeństwo systemów sterowania przemysłowego Marcin Filipiak – Presales Engineer w Arrow ECS
11:45 – 12:05	Stinet sp. z o.o., GRC Advisory: Integracja informacji o bezpieczeństwie i podatnościach w kontekście ryzyka Maciej Wieliczko – Archer Engineer w GRC Advisory

LASYS
Extreme networks
FCA
Forcepoint
STINET
SUS
SAFE PROJECT
TEKNISKA
JSW IT SYSTEMS
SACGiG

HPE Aruba Networking
Zarządzanie usługami sieciowymi od brzegu do chmury

SOFTPROM
VALUE ADDED DISTRIBUTOR
SAFE PROJECT
2023

FROM ZERO TRUST TO NIS2 AND CER
ESTABLISHING CYBER RESILIENCY WHERE IT MATTERS THE MOST
KOMAG

XDR Data Lake
Detection and Activity Logs At Cloud Storage
Endpoint Detection & Response
E-mail Detection & Response
Cloud Detection & Response
Network Traffic Analytics
Activity data detections
Threat Intel Collaboration
Triage & Workbench
Detections – MITRE mapping
SIEM & SOC Analyst

Praktyczne podejście do całościowej o
przed zagrożeniami na przykładzie pro
Trend Micro i doświadczenia integrato
– firmy IT Systems and Solutions Sp. z

ISACGIG

Minister Piotr Pyzik reprezentujący Ministerstwo Aktywów Państwa

Konferencja „Cyfrowy, Bezpieczny Śląsk 2030 – strategia zarządzania cyberbezpieczeństwem w dobie transformacji cywilizacyjnej" zgromadziła blisko 160 uczestników wywodzących się spośród spółek skarbu państwa pełniących kluczową rolę dla sektora wydobywczego i energetycznego w naszym kraju tj.: KGHM Polska Miedź SA, Polskiej Grupy Górniczej SA, JSW SA, Polskiej Grupy Energetycznej Górnictwo i Energetyka Konwencjonalna SA , LW Bogdanka SA, Tauron SA, Tauron Wydobycie SA i Węglokoks Kraj SA oraz Instytutu Techniki Górniczej KOMAG.

Minister Piotr PYZIK reprezentujący Ministerstwo Aktywów Państwa kończąc konferencje powiedział: „... Wierzę, że nasze dyskusje wokół idei budowy Cyfrowego, Bezpiecznego Śląska jako strategii zarządzania cyberbezpieczeństwem w dobie transformacji cywilizacyjnej, przyczynią się do skutecznego budowania świadomości cyfrowej wśród mieszkańców Śląska oraz lepszego zrozumienia kluczowych problemów związanych z zapewnieniem bezpieczeństwa informatycznego we współczesnym społeczeństwie, a Wydział Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej teraz i w przyszłości będzie fundamentem tych zmian nie tylko na Śląsku..."

Więcej informacji na temat działań ISAC GIG znaleźć można pod adresem internetowym **isac.gig.eu**.

Następna konferencja towarzysząca tym razem IV CYBERpoligonowi ISAC-GIG odbędzie się w dniach 14-16 listopada 2023 r. w Hotel Crystal-Mountain w Wiśle podczas XXX JUBILEUSZOWAEJ MIĘDZYNARODOWEJ KONFERENCJA NAUKOWO-TECHNICZNEJ GÓRNICZE ZAGROŻENIA NATURALNE – w imieniu organizatorów zapraszamy do udziału, naprawdę warto.

KSC FORUM 2023, najważniejsze spotkanie praktyków realizujących wymogi Ustawy o Krajowym Systemie Cyberbezpieczeństwa – 23-25 sierpnia 2023

W dniach 23-25.08 2023 r. w Zakopanem odbyła się 5 edycja konferencji KSC FORUM 2023 czyli najważniejszego spotkania praktyków realizujących wymogi Ustawy o Krajowym Systemie Cyberbezpieczeństwa.

KSC Forum to wyjątkowe wydarzenie, które zgromadziło w jednym miejscu ekspertów cyberbezpieczeństwa z podmiotów objętych Ustawą o Krajowym Systemie Cyberbezpieczeństwa z różnych sektorów gospodarki. Podczas konferencji swoje wystąpienia mieli przedstawicieli podmiotów tworzących przepisy, firmy prezentujące swoje rozwiązania z zakresu cyberbezpieczeństwa oraz odbyły się interesujące panele dyskusyjne.

Dyskusja panelowa: **KSC po dobrej stronie mocy**

W panelu wzięli udział:

- Jakub Jagielak - Technology Leader - Security, Atende
- Krzysztof Nierodka - Major Account Manager, Check Point
- Marek Wach - Dyrektor ds. cyberbezpieczeństwa, Poczta Polska
- Piotr Toś - Prezes Zarządu, JSW IT Systems, Przewodniczący Komitetu Zarządzającego ISAC-GIG

A całość poprowadził Przemysław Gamdzyk - CEO & Meeting Designer, CSO Council/Evention

Co dobrego przyniosła ta kluczowa regulacja dla objętych nią podmiotów, w szczególności Operatorów Usług Kluczowych i podmiotów Infrastruktury Krytycznej, oraz całego rynku i państwa – analiza po 5 latach.

W jaki sposób wdrożenie ustawy dotyczącej Operatorów Usług Kluczowych (OUK) i podmiotów Infrastruktury Krytycznej (IK) wpłynęło na sposób myślenia i działania w tych sektorach? Czy udało się zwiększyć świadomość i zmianę kultury bezpieczeństwa cybernetycznego? Czy powstały nowe mechanizmy współpracy i wymiany informacji w celu lepszej ochrony infrastruktury krytycznej? Czy regulacje KSC miały wpływ na inwestycje w infrastrukturę krytyczną i rozwój nowych technologii?

To tylko niektóre z pytań pojawiających się w dyskusji.

Wypełnienie wymogów ustawy o Krajowym Systemie Cyberbezpieczeństwa to niebanalne wyzwanie dla wielu podmiotów – przedsiębiorstw i instytucji, dla tych, którzy są operatorami usług kluczowych i podlegają wymogom Ustawy. Wyzwanie zarówno organizacyjne, technologiczne, regulacyjne, jak i ludzkie. Większość podmiotów podlegających wymogom ustawy podjęła już szereg działań i projektów wdrożeniowych, ale to jest nadal trudna droga, którą trzeba dalej podążać. Zwłaszcza, że liczba tych podmiotów rośnie.

KSC Forum jest miejscem spotkania i rozmowy wszystkich interesariuszy Ustawy o KSC. To ważny i potrzebny dialog, bo kluczowa jest tutaj współpraca pomiędzy różnymi podmiotami - w ramach danych branż, jak i pomiędzy branżami. Poprzednie edycje konferencji znakomicie spełniły tutaj swoje zadanie – wzmocnienia tego dialogu i budowy relacji osób odpowiedzialnych za cyberbezpieczeństwo swoich organizacji.

Centra Wymiany i Analizy Informacji (ISAC, z ang. Information Sharing and Analysis Centers) odgrywają kluczową rolę w zapewnianiu bezpieczeństwa cybernetycznego, szczególnie w dziedzinie ochrony przed zagrożeniami związanymi z cyberprzestępczością i cyberatakami. Oto kilka powodów, dla których ISAC są ważne:

1. Wymiana informacji: ISAC umożliwiają organizacjom prywatnym i publicznym wymianę ważnych informacji na temat incydentów bezpieczeństwa, zagrożeń i sposobów obrony. Dzięki temu organizacje mogą dowiedzieć się o nowych atakach i technikach cyberprzestępców oraz szybko reagować na potencjalne zagrożenia.

2. Wzajemne wsparcie: ISAC dostarczają platformę do współpracy między organizacjami, co pozwala na wzajemne wsparcie w przypadku incydentów. Organizacje mogą dzielić się wiedzą, doświadczeniem i narzędziami, aby lepiej radzić sobie z trudnościami związanymi z cyberatakami.

3. Szybka reakcja: Dzięki dostępowi do bieżących informacji i analizy zagrożeń, organizacje mogą szybciej reagować na ataki i podejmować działania w celu zminimalizowania szkód oraz przywrócenia normalnego funkcjonowania.

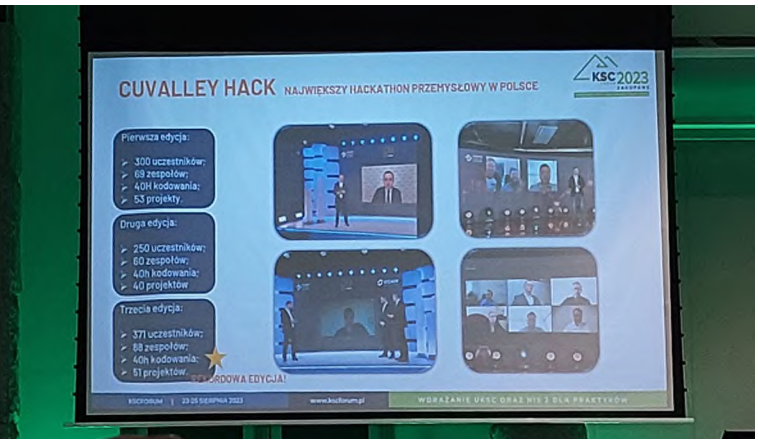
4. Wzmacnianie świadomości: Działalność ISAC pomaga w podnoszeniu świadomości wśród organizacji członkowskich na temat nowych zagrożeń i najlepszych praktyk w zakresie cyberbezpieczeństwa. To z kolei pozwala organizacjom lepiej się przygotować i chronić przed potencjalnymi atakami.

5. Współpraca na szczeblu krajowym: Wiele ISAC ma partnerstwa lub współpracuje z instytucjami rządowymi zajmującymi się cyberbezpieczeństwem, co pozwala na lepszą koordynację działań i wymianę informacji na poziomie krajowym i międzynarodowym.

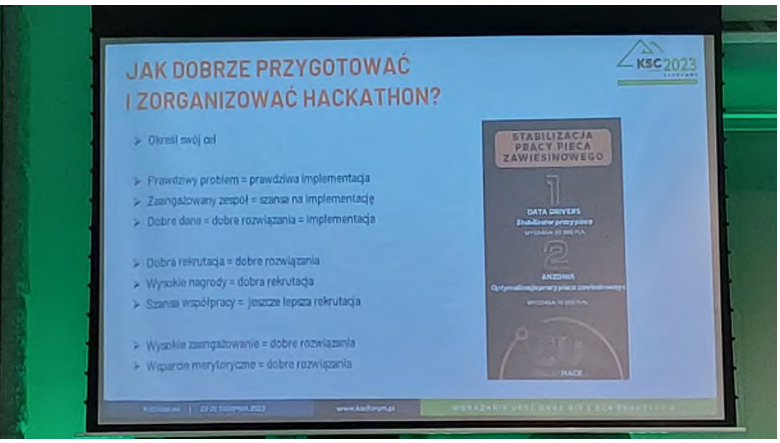
6. Ciągłe doskonalenie: Dzięki analizie incydentów i zbieraniu danych, ISAC pomagają organizacjom doskonalić swoje strategie obronne i dostosowywać się do ewoluujących zagrożeń.

Warto podkreślić, że ISAC mogą różnić się w zależności od branży lub regionu – przykładem jest ISAC-GIG powstały na bazie kooperacji spółek z sektora energetyczno-wydobywczego, a co pozwala na dostosowanie działań do konkretnych potrzeb i zagrożeń. Ogólnie rzecz biorąc, centra wymiany i analizy informacji ISAC pełnią kluczową rolę w zwiększaniu cyberbezpieczeństwa, pomagając organizacjom lepiej się chronić przed atakami i reagować na nie w sposób skuteczny.

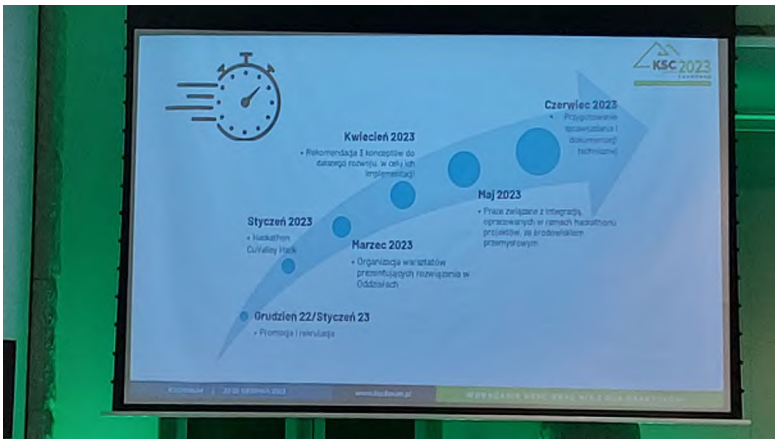
KSC 2023
ZAKOPANE
DYSKUSJA PANELOWA
KSC PO DOBREJ STRONIE MOCY


CUVALLEY HACK
NAJWIĘKSZY HACKATHON PRZEMYSŁOWY W POLSCE
KSC 2023
ZAKOPANE
Pierwsza edycja:
300 uczestników;
69 zespołów;
40H kodowania;
53 projekty.
Druga edycja:
250 uczestników;
60 zespołów;
40h kodowania;
40 projektów
Trzecia edycja:
371 uczestników;
88 zespołów;
40h kodowania;
51 projektów
REKORDOWA EDYCJA!
KSCFORUM | 23-25 SIERPNIA 2023
www.kscforum.pl
WDRAŻANIE UKSC ORAZ NIS 2 DLA PRAKTYKÓW

KSC 2023
ZAKOPANE
DYSKUSJA PANELOWA
KSC PO DOBREJ STRONIE MOCY
Moderator:
Panelisci:
Komentarz do dyskusji:
KSC


JAK DOBRZE PRZYGOTOWAĆ
I ZORGANIZOWAĆ HACKATHON?
KSC 2023
Określ swój cel
Prawdziwy problem = prawdziwa implementacja
Zaangażowany zespół = szansa na implementację
Dobre dane = dobre rozwiązania = implementacja
Dobra rekrutacja = dobre rozwiązania
Wysokie nagrody = dobra rekrutacja
Szansa współpracy = jeszcze lepsza rekrutacja
Wysokie zaangażowanie = dobre rozwiązania
Wsparcie merytoryczne = dobre rozwiązania
STABILIZACJA PRACY PIECA ZAWIESINOWEGO
DATA DRIVERS
ANZONIA

KSC


KSC 2023
Czerwiec 2023
Kwiecień 2023
Maj 2023
Styczeń 2023
Marzec 2023
Grudzień 22/Styczeń 23

Raport ISAC-GIG: Cyberbezpieczeństwo systemów przemysłowych dla sektora wydobywczo-energetycznego

Szanowni Państwo,

Raport „Cyberbezpieczeństwo systemów przemysłowych dla sektora wydobywczo-energetycznego za rok 2022" stanowi element większej strategii grupy ludzi związanych z prowadzeniem elitarnych studiów podyplomowych pt.: „Cyberbezpieczeństwo systemów przemysłowych" w murach Politechniki Śląskiej przez Wydział Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej wraz z Instytutem Techniki Górniczej KOMAG. Stanowić ma on ważny element działań ISAC-GIG w zakresie promowania i rozwijania współpracy w obszarze cyberbezpieczeństwa pomiędzy nauką, a biznesem będąc swoistym SOJUSZEM realizacji innowacyjnych projektów i programów badawczych, a także źródłem upowszechniania ich rezultatów w celu podnoszenia świadomości zarządzania całym ekosystemem cyberbezpieczeństwa dla sektora wydobywczo-energetycznego.

Rozwój technologii oraz wykorzystanie narzędzi teleinformatycznych w każdym aspekcie codziennego życia nie ominęły sektora surowcowego. W krajobrazie polskiego przemysłu wydobywczego, który obejmuje zarówno surowce energetyczne jak i rudy metali, bardzo istotna jest cyberprzestrzeń.

Wierzymy, że ten raport będzie dla Państwa dużą wartością. Wyniki badania i obserwacji wskazują na znaczący wzrost incydentów i podatności pokazuje jednak również, że rośnie świadomość tych zagrożeń i wiedza jak sobie z nimi radzić.

Postęp technologiczny oraz idąca wraz z nim konieczność minimalizacji ryzyka związanego z zagrożeniem atakami sprawiły, że cyberbezpieczeństwo jest jednym z największych wyzwań dzisiejszych czasów, a co za tym idzie jest jednym z kluczowych elementów strategii bezpieczeństwa IT oraz OT dla sektora wydobywczo-energetycznego.

Szanowni Państwo, Raport, przedstawiający zrealizowane cele oraz udoskonalenia, jakie zostały wypracowane w ramach rozwijania wyższego poziomu dojrzałości i odporności cyberbezpieczeństwa w sektorze wydobywczo-energetycznym zawiera również skutki nowelizacji ustawy o KSC, a także propozycje Dyrektywy NIS2 wprowadzające szereg wyzwań dla podmiotów krajowego systemu cyberbezpieczeństwa we wszystkich sektorach. Naszym zdaniem warto zawczasu przygotować się na nadchodzące zmiany poprzez ocenę aktualnego poziomu dojrzałości organizacji w obszarze cyberbezpieczeństwa.

Składamy go w Państwa ręce z nadzieją, że zawarte w nim dane oraz zalecenia przyczynią się do ułatwienia wdrażania najlepszych praktyk w zakresie bezpieczeństwa, które są zgodne z obowiązującymi standardami i wytycznymi.

Zapraszamy do lektury i współpracy przy tworzeniu następnych raportów.

NASZ RAPORT DOSTĘPNY JUŻ NA STRONIE ISAC.GIG.EU

Postęp technologiczny oraz idąca wraz z nim konieczność minimalizacji ryzyka związanego z zagrożeniem atakami sprawiły, że cyberbezpieczeństwo jest jednym z największych wyzwań dzisiejszych czasów, a co za tym idzie jest jednym z kluczowych elementów strategii bezpieczeństwa IT oraz OT dla sektora wydobywczo-energetycznego.

R A P O R T „Cyberbezpieczeństwo systemów przemysłowych dla sektora wydobywczo-energetycznego za rok 2022" jest elementem większej strategii grupy ludzi związanych z prowadzeniem elitarnych studiów podyplomowych pt.: „Cyberbezpieczeństwo systemów przemysłowych" w murach Politechniki Śląskiej przez Wydział Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej wraz z Instytutem Techniki Górniczej KOMAG i ISAC-GIG. Stanowić ma on ważny element działań ISAC-GIG w zakresie promowania i rozwijania współpracy w obszarze cyberbezpieczeństwa pomiędzy nauką, a biznesem będąc swoistym SOJUSZEM realizacji innowacyjnych projektów i programów badawczych, a także źródłem upowszechniania ich rezultatów w celu podnoszenia świadomości zarządzania całym ekosystemem cyberbezpieczeństwa dla sektora wydobywczo-energetycznego.

Branża wydobywcza i energetyczna, jako obszar wyjątkowo ważny dla funkcjonowania państwa, w sposób szczególny zwraca uwagę na zabezpieczenie systemów i urządzeń automatyki wykorzystywanych w produkcji. Chcielibyśmy bardzo, aby nasz R A P O R T był dla Państwa dużą wartością, przedstawiając zrealizowane cele oraz udoskonalenia, jakie zostały wypracowane w ramach rozwijanego przez ISAC-GIG wyższego poziomu dojrzałości i odporności cyberbezpieczeństwa.

Zachęcamy do dalszego zacieśniania współpracy w ramach ISAC-GIG, do podnoszenia świadomości i odpowiedzialności cyfrowej sektora surowcowego będącego fundamentem nowego oblicza przemysłu wydobywczego w naszym kraju.

Zapraszamy do lektury
Wejdź na stronę isac.gig.eu

Silesian Cyber Hackathon

21-22/06/2023
Wydział Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej Politechniki Śląskiej w Gliwicach

Honorowy Patronat nad wydarzeniem:
Wicepremier Jacek Sasin, Minister Aktywów Państwowych
Rektor Politechniki Śląskiej prof. dr hab. inż. Arkadiusz Mężyk

Tematyka:

I Bezpieczeństwo pracowników w zakładach przemysłowych
II Wydajność i efektywność w zakładach przemysłowych
III Ochrona środowiska
IV Edukacja i świadomość społeczna
V Zarządzanie infrastrukturą
VI Cyberbezpieczeństwo w branży wydobywczo-energetycznej
VII Zastosowanie technologii cyfrowych w życiu codziennym i pracy zawodowej

Nagrody:

I miejsce - 8000 PLN
II miejsce - 6000 PLN
III miejsce - 4000 PLN

silesiancyberhackathon.pl

JSW SA ISACGiG JSW IT SYSTEMS Politechnika Śląska

ZŁOTY SPONSOR
Hewlett Packard Enterprise apex.it

SREBRNY SPONSOR
iTSS IT SYSTEMS & SOLUTIONS

FCA BALASYS STINET Extreme networks frse Fundacja Rozwoju Systemu Edukacji TEKNISKA
Forcepoint atman TREND MICRO SUSE SAFE PROJECT

CYBERBEZPIECZEŃSTWO SYSTEMÓW PRZEMYSŁOWYCH

Studia podyplomowe na Wydziale Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej

Sylwetka Absolwenta:

- Uczestnik po zakończeniu studiów podyplomowych będzie znał i rozumiał zagadnienia związanie z europejskim i krajowym systemem cyberbezpieczeństwa, a także standaryzacją i certyfikacją rozwiązań teleinformatycznych w zakresie cyberbezpieczeństwa, oraz modelowaniem zagrożeń.
- Będzie znał wybrane zagadnienia z zakresu sterowników i sieci przemysłowych oraz układów automatycznego sterowania, w tym robotów.
- Absolwent studiów będzie miał wiedzę w zakresie: budowy architektury bezpieczeństwa w przedsiębiorstwie produkcyjnym, modelu zachowań oraz określania indywidualnych cech grup APT (Advanced Persistent Threats), bezpieczeństwa aplikacji webowych, infrastruktury sieciowej i systemów przemysłowych.
- Absolwent będzie znał sposoby zabezpieczania środowiska chmurowego, a także będzie umieć wdrażać zabezpieczenia chmury obliczeniowej, znając Standardy Cyberbezpieczeństwa Chmur Obliczeniowych.
- Absolwent będzie również miał wiedzę z zakresu gromadzenia materiału dowodowego, znając zasady informatyki śledczej.

Kontakt w sprawie rekrutacji:

Anna Kukla
tel. 32 237 21 79
anna.kukla@polsl.pl

Politechnika Śląska

ISACGiG

CYBERBEZPIECZEŃSTWO SYSTEMÓW PRZEMYSŁOWYCH

Studia podyplomowe na Wydziale Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej

Kontakt w sprawie rekrutacji:
Anna Kukla
tel. 32 237 21 79
anna.kukla@polsl.pl

Politechnika Śląska

ISACGiG