Cyberbezpieczeństwo w przemyśle: Nowe Wyzwania i Możliwości	
26.02.2023	
09:00 – 15:30 Cyberpoligon 2024	
Sesja otwierająca Innowacje w detekcji zagrożeń cybernetycznych z wykorzystaniem sztucznej inteligencji	
13:00 -13:30	Sztuczna Inteligencja a Cyberbezpieczeństwo: Przegląd Nowoczesnych Wyzwań i Rozwiązań *Mariusz Szczęsny, Dyrektor Business Unit Cyber Security, Integrity Partners*
13:30-14:00	Zintegrowane Bezpieczeństwo: Jak Palo Alto Networks Zapewnia Ochronę na Wszystkich Poziomach *Tomasz Pietrzyk, Senior Manager, System Engineering, EEUR, Palo Alto Networks*
14:00 – 14:30	Automatyzacja Procesów Tekniska - Automatyzacja tworzenia i utrzymania usług transmisji danych w oparciu o XTran MPLS-TP
14:30 – 15:00	Tufin – Automatyzacja procesów administracyjnych *Bartosz Krupowski, Network Security Manager, Integrity Partners oraz Łukasz Żurawski, Network Security Engineer, Integrity Partners*
15:00 – 15:30	Ochrona przed atakami Web DDoS Tsunami, *Andrzej Sienkiewicz, Radware*
Monitorowanie sieci przemysłowych w podziemnych zakładach górniczych i wykrywanie cyberzagrożeń	
15:30 – 16:00	System monitorowania i detekcji cyberataków na instalacje podziemnego zakładu górniczego *(Prof. Ewa Niewiadomska-Szynkiewicz, Politechnika Warszawska i GIG-PIB, Rafał Wowra, JSW IT Systems).*
16:00 – 16:15	Metody sztucznej inteligencji do detekcji ataków na sieci IT i IoT *(dr inż. Jędrzej Bieniasz, Politechnika Warszawska)*
16:15 – 16:30	Metody sztucznej inteligencji do detekcji ataków na sieci OT *(dr inż. Sebastian Plamowski, Politechnika Warszawsk*

16:30-17:15	**PANEL DYSKUSYJNY: Wyzwania IT/OT 2024** a) Automatyzacja jakich obszarów i procesów będzie kluczowa w 2024 r. w odniesieniu do IT/OT b) Przemysł kognitywny czyli jaki? O sztucznej inteligencji słów kilka c) Monitorowanie i zarządzanie ryzykiem. Jak sprawić aby analizy i słupki pracowały dla Nas. d) Plastyczność, dostosowywanie się do zmieniających warunków na co położyć nacisk?
27.02.2023	
Sesja poranna I **Budowa świadomości bezpieczeństwa cybernetycznego**	
09:00 – 09:15	Blokowanie i usuwanie treści cyfrowych jako instrument cyberbezpieczeństwa (Dr hab. Katarzyna Chałubińska-Jentkiewicz, Akademia Sztuki Wojennej)
09:15 – 09:30	Świadomość bezpieczeństwa cybernetycznego w podmiocie gospodarczym (Prof. dr hab. inż. Marek Amanowicz, NASK-PIB)
09:30 – 09:45	Dynamiczne zarządzanie ryzykiem w rozległych systemach IT i OT (Dr inż. Piotr Januszewicz, Akademia Górniczo-Hutnicza)
09:45 – 10.00	Czy uczenie ze wzmocnieniem może rzeczywiście wspomagać tworzenie złośliwego oprogramowania? (Dr hab. inż. Mariusz Kamola, Politechnika Warszawska)
10:00 – 10:15	Centra komputerów dużej mocy w Polsce i aktualne inicjatywy europejskie (Jarosław Skomiał, Interdyscyplinarne Centrum Modelowania UW)
Sesja poranna II **Samoorganizacja i autonomia w Przemyśle kognitywnym**	
10:15-10:45	Inteligencja Zagrożeń w Działaniu: Praktyczne Zastosowania Recorded Future w cyberochronie *Maciej Martinek, Recorded Future*
10:45-11:10	Cortex XDR a Nowoczesne Wyzwania Bezpieczeństwa: Perspektywa Użytkownika *Łukasz Żurawski, Network Security Engineer, Integrity Partners*

11:10-11:40	Inteligentne monitorowanie sieci – Greycortex *Tomasz Szymański, Greycortex oraz Konrad Tarsała, Network Security Engineer, Integrity Partners*
11:40-12:05	Dostęp uprzywilejowany w środowiskach przemysłowych *Bartosz Kryński, Solutions Engineering Team Leader, CyberArk*
12:05 – 12:35	Ocena Zagrożeń i Ochrona w Jednym Rozwiązaniu: Imperva Cloud WAF i RASP w Działaniu *Bartosz Chmielewski, Imperva, Bartosz Krupowski, Network Security Manager, Integrity Partners*
12:35 – 13:00	Automatyzacja i Inteligencja w Działaniu: Studium Przypadku z Wykorzystaniem Cortex XSOAR w Przemyśle Kognitywnym *Łukasz Żurawski, Network Security Engineer, Integrity Partners*
13:00 – 13:20	Tekniska – Rozłożymy cyberbezpieczeństwo sieci przemysłowych na czynniki pierwsze! Jak spełnić wymogi nowych legislacji? Konkretne cyberbezpieczne zalecenia
13:20 – 14:20	**Obiad**
28.02.2023	
Sesja poranna **Dostosowywanie się do zmieniających warunków a doskonalenie funkcji**	
09:00-09:30	Widoczność i Kontrola w Zmieniającym Się Środowisku: Jak Cortex XPANSE Ułatwia Monitoring Sieci z Perspektywy Zdalnej *Marcin Szewczuk, Systems Engineer Palo Alto Networks*
09:30-11:00	Jak podejść do bezpieczeństwa aplikacji - od kodu do chmury z wykorzystaniem Prisma Cloud *Ewa Sniechowska, Technical Sales Manager Prisma Cloud, Palo Alto Networks*
11:00 – 12:00	Podsumowanie konferencji

CYBERPOLIGON 2024 KRAKÓW

Cyberpoligon 2024 będzie oparty na zasadach zawodów Capture the Flag (CTF) – są to konkursy związane z cyberbezpieczeństwem, w których uczestnicy rywalizują w rozwiązywaniu problemów związanych z bezpieczeństwem komputerowym w celu zdobycia jak najwyższej liczby punktów. Uczestnicy tych konkursów mają za zadanie "zdobyć flagi", które są zazwyczaj losowymi ciągami znaków

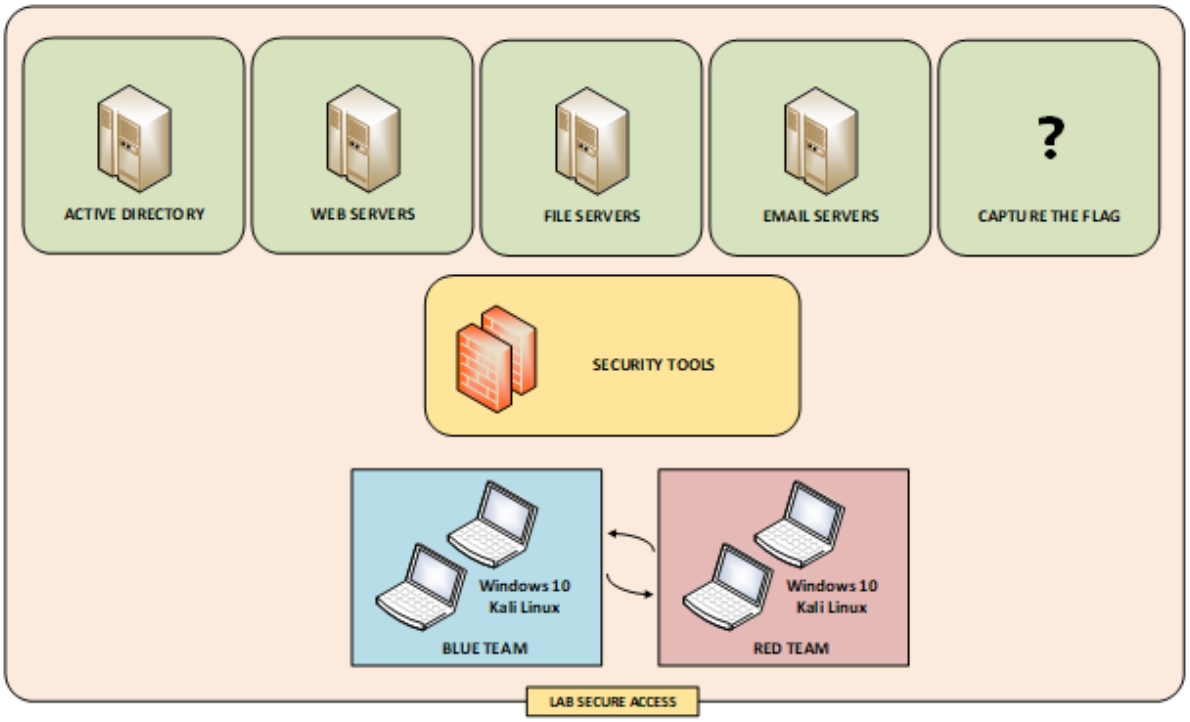
osadzonymi w wyzwaniach. Flagi te są metaforycznymi "trofeami", zdobytymi poprzez rozwiązanie konkretnych problemów lub wyzwań związanych z bezpieczeństwem. CTF są coraz bardziej popularne, ponieważ przyciągają dużą liczbę młodych talentów zainteresowanych karierą w cyberbezpieczeństwie. Zawody te mogą przyjmować różne formy, ale najczęstsze to formaty "Jeopardy" oraz "Attack-Defence". W przypadku formatu "Jeopardy", uczestnicy rozwiązują różne zadania z zakresu bezpieczeństwa, zbierając flagi za każde z nich. Format "Attack-Defence" z kolei polega na tym, że zespoły muszą bronić swoich systemów przed atakami przeciwników, jednocześnie próbując zaatakować systemy przeciwnika. Organizatorzy CTF często rejestrują swoje zawody na platformie CTFtime, co pozwala śledzić pozycję drużyn w czasie i w różnych konkursach. CTF są organizowane zarówno przez społeczności, rządy, jak i korporacje. Przykłady takich konkursów to DEF CON CTF, znany jako jeden z najstarszych konkursów CTF, a także Cybersecurity Awareness Worldwide (CSAW) CTF, czy również Cyberpoligon organizowany w ramach Szkoły Eksploatacji Podziemnej przez ISAC-GIG. Udział w takich konkursach jest doskonałą okazją do nauki i praktykowania umiejętności związanych z cyberbezpieczeństwem w angażujący i praktyczny sposób.

Organizowanie zawodów cyberpoligonu, czyli symulacji cyberataków i reakcji obronnych, obejmuje kilka kluczowych kwestii:

1. **Definicja Celów**: Określenie, co zawody mają na celu, np. testowanie reakcji na określone typy ataków, szkolenie zespołów, czy podnoszenie ogólnej świadomości dotyczącej cyberbezpieczeństwa.
2. **Scenariusze Ataków**: Opracowanie realistycznych scenariuszy symulowanych ataków cybernetycznych, które mogą obejmować różne rodzaje zagrożeń, jak ransomware, ataki DDoS, czy włamania do systemów.
3. **Wybór Platformy i Narzędzi**: Zastosowanie odpowiednich technologii i narzędzi umożliwiających efektywne symulowanie i monitorowanie ataków oraz reakcji obronnych.
4. **Zaangażowanie Zespołów**: Udział różnorodnych zespołów zarówno atakujących, jak i broniących, które mogą reprezentować różne organizacje i branże.
5. **Szkolenie i Przygotowanie Uczestników**: Zapewnienie uczestnikom odpowiedniego przygotowania do uczestnictwa w zawodach, w tym szkolenia z zakresu cyberbezpieczeństwa.
6. **Monitorowanie i Analiza**: Śledzenie przebiegu zawodów, zbieranie danych i analizowanie wyników w celu oceny skuteczności reakcji i identyfikacji obszarów do poprawy.
7. **Aspekty Prawne i Etyczne**: Zapewnienie zgodności z przepisami prawnymi i standardami etycznymi, zwłaszcza w zakresie ochrony danych i prywatności.
8. **Komunikacja i Zarządzanie Incydentami**: Efektywne zarządzanie komunikacją w trakcie i po zawodach, w tym informowanie o incydentach i sposobach reagowania.

9. **Wnioski i Doskonalenie**: Wykorzystanie wyników i doświadczeń z zawodów do doskonalenia strategii obronnych i zwiększenia ogólnej gotowości na cyberataki. Podsumowując, zawody cyberpoligonu są kompleksowym przedsięwzięciem, które wymaga szczegółowego planowania, zaangażowania wielu specjalistów i ciągłej analizy. Celem jest nie tylko testowanie gotowości na cyberataki, ale również nauka, doskonalenie umiejętności i zwiększanie świadomości w zakresie cyberbezpieczeństwa.

Każdy z uczestników warsztatów Cyberpoligonu będzie posiadał swoje maszyny wirtualne, jest to stacja Kali Linux (służąca do przeprowadzania ataków) oraz stacja Windows (służąca do ich analizy). W środowisku znajdują się również serwery, które będą celem ataku. Uproszczona topologia środowiska wygląda następująco:



W ramach cyberpoligonu zostaną przetestowane narzędzia bezpieczeństwa Palo Alto Networks m.in. Firewall oraz system klasy XDR. Zadania będą weryfikowały wiedzę z zakresu bezpieczeństwa sieci, podatności w systemach operacyjnych LINUX oraz WINDOWS, a przede wszystkim sposoby reagowania na incydenty bezpieczeństwa związane z włamaniem do serwerów Windows, zbieraniem poświadczeń, przejęciem kontrolera domeny oraz tzw. „Credential Access".

Cortex XDR od Palo Alto Networks to rozwiązanie z zakresu rozszerzonej detekcji i reakcji (XDR), które integruje różne źródła danych w celu zapewnienia kompleksowej ochrony przed zaawansowanymi zagrożeniami cybernetycznymi. Jest to system bazujący na analizie behawioralnej i uczeniu maszynowym, co pozwala na szybkie wykrywanie anomalii oraz podejrzanych zachowań w sieci. Cortex XDR oferuje pełną widoczność na działania w całym środowisku sieciowym, łącząc dane z endpointów, sieci i chmury. Umożliwia to efektywne zarządzanie incydentami i szybkie reagowanie na potencjalne zagrożenia. Narzędzie to zapewnia także zaawansowane możliwości dochodzeniowe, umożliwiając dokładną analizę i śledzenie źródeł ataków. To sprawia, że Cortex XDR jest skutecznym rozwiązaniem w ochronie przed złożonymi cyberatakami, zapewniającym bezpieczeństwo danych i infrastruktury IT przedsiębiorstw. Natomiast Firewall Palo Alto Networks to zaawansowane rozwiązanie zabezpieczeń sieciowych, które zapewnia kompleksową ochronę przed zagrożeniami cybernetycznymi. Charakteryzuje się następującymi kluczowymi cechami:

1. Inspekcja Ruchu: Wykorzystuje dogłębną inspekcję ruchu sieciowego w celu identyfikacji i blokowania zagrożeń.
2. Zapobieganie Wyciekom Danych: Obejmuje funkcje zapobiegania wyciekom informacji.
3. Zintegrowana Ochrona Przed Zagrożeniami: Oferuje zintegrowaną ochronę przed różnymi rodzajami zagrożeń, w tym wirusami, malware i atakami sieciowymi.
4. Zarządzanie Politykami Bezpieczeństwa: Umożliwia tworzenie i zarządzanie szczegółowymi politykami bezpieczeństwa.
5. Wysoka Wydajność: Zapewnia wysoką wydajność nawet przy głębokiej inspekcji ruchu.
6. Łatwość Zarządzania: Oferuje intuicyjny interfejs użytkownika i narzędzia do zarządzania, ułatwiające monitorowanie i konfigurację zabezpieczeń sieciowych. Firewall Palo Alto jest rozwiązaniem dobrze przyjętym w branży ze względu na swoją skuteczność w ochronie przed złożonymi i zaawansowanymi zagrożeniami cybernetycznymi. Inne rozwiązanie od Palo Alto Networks to ich system zarządzania bezpieczeństwem, czyli Panorama. Panorama umożliwia centralne zarządzanie politykami bezpieczeństwa, logami i raportami dla wielu firewalli Palo Alto Networks, zarówno fizycznych, jak i wirtualnych. Dzięki temu administratorzy mogą efektywnie i spójnie zarządzać zabezpieczeniami w całej organizacji. Panorama zapewnia również szczegółowy wgląd w ruch sieciowy i zagrożenia, co umożliwia szybkie reagowanie na incydenty i skuteczne zarządzanie ryzykiem.