SECURE International Summit – WARSZTATY

3-4 KWIETNIA 2025

	Warsztat nr 1
TYTUŁ:	Building Malware Analysis Capability for CERTs
TERMIN:	3 kwietnia 2025, godz. 9:00 – 17:00, Młyny Rothera piętro 2
CZAS TRWANIA:	8 godzin
LICZBA UCZESTNIKÓW:	20-25

OPIS WARSZTATU:

Szkolenie poprowadzi Daniel Orłowski z CERT Polska.

Celem warsztatu jest kickstart możliwości analizy złośliwego oprogramowania, w szczególności w małych i mniej doświadczonych zespołach. Szkolenie jest techniczne i zawiera wiele aspektów analizy malware dla CSIRT-ów, w tym: ekosystem złośliwego oprogramowania, triage, różne podejścia do analizy, remediacja oraz "polowanie" na nowe zagrożenia. Podczas spotkania omówione zostanie tworzenie odpowiednich wewnętrznych procedur wykorzystując serwisy online oraz narzędzia open source.

Ten jednodniowy warsztat porusza wiele zagadnień związanych z analizą malware na poziomie podstawowym, aby przedstawić uczestnikom temat w ujęciu szerokim. Celem jest ułatwienie osobom biorącym w nim udział podjęcie decyzji, w którym kierunku powinni się specjalizować tak, aby odpowiadało to potrzebom ich organizacji. Warsztat zawiera wiele praktycznych ćwiczeń, dzięki którym uczestnicy nabędą umiejętności używania darmowych narzędzi i serwisów do analizy zagrożeń typu malware.

Informacje dla uczestników:

- szkolenie skierowane jest do personelu technicznego w CSIRT i innych podmiotach odpowiedzialnych za cyberbezpieczeństwo.
- Nie jest wymagana wcześniejsza znajomość analizy złośliwego oprogramowania, jednak uczestnicy powinni znać podstawy cyberbezpieczeństwa.

Rejestracja:

https://forms.office.com/e/tEZQ4tD8xs

SECURE International Summit – WARSZTATY

3-4 KWIETNIA 2025

	Warsztat nr 2
TYTUŁ:	Dostęp do informacji o zagrożeniach przy użyciu platformy n6
TERMIN:	3 kwietnia 2025, godz. 9:30 – 13:00, Młyny Rothera, piętro 2
CZAS TRWANIA:	3,5 godziny
LICZBA UCZESTNIKÓW:	20-25

OPIS WARSZTATU:

Szkolenie poprowadzi Krzysztof Rydz z CERT Polska.

Uczestnicy warsztatu poznają typowe rodzaje zagrożeń bezpieczeństwa dla chronionej infrastruktury teleinformatycznej (m.in. podatności, błędne konfiguracje, złośliwe oprogramowanie), metody pozyskiwania danych o zagrożeniach oraz proaktywne działania, które mogą pomóc zwiększyć bezpieczeństwo sieci w organizacjach. W programie szkolenia zawarte jest również aktywne wykorzystanie usługi n6, wyszukiwanie, analiza i interpretacja danych zawartych w platformie n6, a także wprowadzenie do automatyzacji i integracji n6 innymi systemami.

n6 - Network Security Incident eXchange (https://cert.pl/n6/) to usługa udostępniana przez CERT Polska, dzięki której przedsiębiorstwa i instytucje otrzymują informacje o problemach bezpieczeństwa w ich infrastrukturze. Udostępniane dane dotyczą m.in. infekcji szkodliwym oprogramowaniem, hostowanie szkodliwej treści (np. phishing), czy podatności w aplikacjach dostępnych z internetu.

Informacje dla uczestników:

- Warsztaty są dedykowane dla administratorów i osób odpowiedzialnych za cyberbezpieczeństwo, które chcą podnieść poziom bezpieczeństwa infrastruktury IT w swoich organizacjach.
- Nie jest wymagana specjalistyczna wiedza z obszaru cyberbezpieczeństwa, natomiast uczestnicy powinni znać podstawowe protokoły sieciowe.
- Do wykonania zadań w systemie n6 każdy uczestnik będzie potrzebował własnego laptopa.

Rejestracja:

https://forms.office.com/e/tEZQ4tD8xs

SECURE International Summit – WARSZTATY

3-4 KWIETNIA 2025

	Warsztat nr 3
TYTUŁ:	Ryzyko związane z ransomware
TERMIN:	3 kwietnia 2025, godz. 13:30 – 17:00, Młyny Rothera piętro 2
CZAS TRWANIA:	3,5 godziny
LICZBA UCZESTNIKÓW:	20-25

OPIS WARSZTATU:

Szkolenie poprowadzi Bartosz Trybus z CERT Polska.

Podczas szkolenia przypomnimy, o co należy zadbać, by minimalizować ryzyko incydentu ransomware. Uczestnicy otrzymają praktyczne wskazówki dotyczące zabezpieczenia sieci, a także rady jak działać, jeśli jednak do incydentu doszło. Przedstawimy metody zabezpieczenia materiałów i odtwarzania infrastruktury.

Informacje dla uczestników:

- Szkolenie kierujemy do administratorów.

Rejestracja:

https://forms.office.com/e/tEZQ4tD8xs

SECURE International Summit – WARSZTATY

3-4 KWIETNIA 2025

	Warsztat nr 4
TYTUŁ:	Cyberbezpieczeństwo w jednostkach samorządu terytorialnego. Najpowszechniejsze zagrożenia w sieci, cyberhigiena i komunikacja kryzysowa incydentów cyberbezpieczeństwa.
TERMIN:	4 kwietnia 2025, godz. 9:00 – 12:30
CZAS TRWANIA:	3,5 godziny
LICZBA UCZESTNIKÓW:	50

OPIS WARSZTATU:

Szkolenie poprowadzą Katarzyna Bisialska, Iwona Prószyńska oraz Marcin Napiórkowski z NASK PIB.

Celem szkolenia jest podniesienie poziomu bezpieczeństwa w urzędach dzięki budowaniu i rozwijaniu instytucjonalnej kultury cyberbezpieczeństwa. Świadomość zagrożeń oraz wzmacnianie bezpiecznych nawyków korzystania z sieci wśród pracowników wszystkich szczebli jest niezwykle ważnym elementem tego procesu. W ramach szkolenia omówione zostaną następujące zagadnienia:

- Najpowszechniejsze zagrożenia w sieci
- Skąd przestępcy mają nasze dane i jak dbać o prywatność w sieci
- Cyberhigiena i zgłaszanie incydentów cyberbezpieczeństwa
- Komunikacja kryzysowa incydentów cyberbezpieczeństwa

Informacje dla uczestników:

- Szkolenie skierowane jest do pracowników jednostek samorządu terytorialnego.

Rejestracja:

https://forms.office.com/e/tEZQ4tD8xs