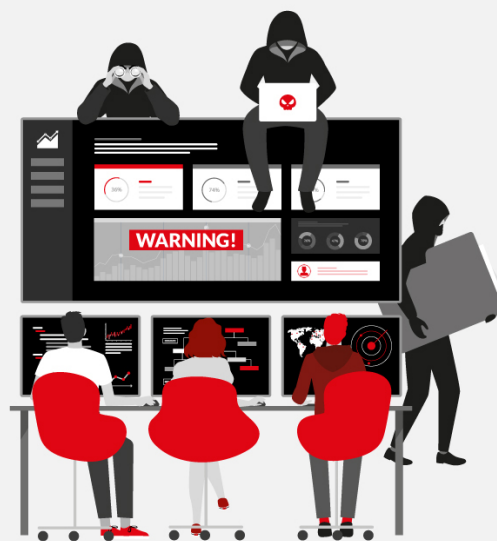


Budowanie świadomości cyberzagrożeń w działach IT



UNIKALNE KORZYŚCI DLA UCZESTNIKÓW SZKOLENIA:

- Większa pewność w codziennej pracy z systemami i danymi
- Lepsze zrozumienie współczesnych wyzwań IT i sposobów reagowania na nie
- Umiejętność identyfikacji ryzyka zanim stanie się problemem
- Wzrost efektywności współpracy między członkami zespołu IT
- Praktyczne wskazówki, jak budować kulturę cyberodpowiedzialności w organizacji

CEL SZKOLENIA:

Celem szkolenia jest rozwinięcie świadomości w zakresie cyberzagrożeń wśród pracowników działów IT oraz wyposażenie ich w wiedzę i narzędzia umożliwiające proaktywne działanie na rzecz bezpieczeństwa cyfrowego organizacji. Uczestnicy nauczą się rozpoznawać potencjalne ryzyka, lepiej rozumieć mechanizmy ataków i współtworzyć kulturę bezpieczeństwa, nie tylko jako specjaliści techniczni, ale także jako świadomi członkowie zespołu IT. Szkolenie ma na celu wzmocnienie czujności, odpowiedzialności i umiejętności reagowania w realnych sytuacjach.

AGENDA

1. Jak wygląda rzeczywiste włamanie do firmy (wiedza z wywiadu cybernetycznego i analiz powłamaniowych)
2. "Grzechy" adminów w polskich firmach (wiedza z testów Red Team)
3. Cyberzagrożenia, których nie wykryjemy skanerami podatności ani nie usuniemy przez poprawki
4. Architektura cyberbezpieczeństwa systemu teleinformatycznego i rola nowych technologii,
m.in. EDR, NDR, SSE, CTEM
5. Przygotowanie zespołów IT w odniesieniu do rosnących cyber zagrożeń i wymagań nowego prawa

Cena szkolenia: 4 000 PLN netto
(Grupa do 10 osób)

atc@clico.pl
www.clico.pl