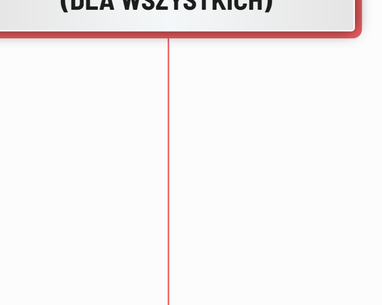
SEKURAK.PL

32 szkolenia on-line, ~1,5 godz. każde

AKADEMIA NIS2/KSC2 OD SEKURAKA



SZKOLENIA CYBER AWARENESS (DLA WSZYSTKICH)

- Aktualne cyberataki na pracowników firm. Case studies. Pokazy praktyczne, prewencja
- Jak zbudować program szkoleń/kulturę cyberbezpieczeństwa w organizacji?
- Dlaczego bezpieczeństwo dostawców jest istotne? Case studies incydentów
- Jak obecnie hackerzy przenikają do organizacji?
- SOC/IDS/XDR/SIEM/DLP/MFA – jak się połapać w tym wszystkim?

SZKOLENIA CYBERSEC (DLA IT)

Podstawy oraz narzędzia

- Błyskawiczne sposoby na zwiększenie bezpieczeństwa organizacji
- W audycie 100-proc. zgodność, w praktyce 100-proc. fail. Case studies
- Wykonaj praktyczny rekonesans zasobów IT organizacji
- Top 3 bezpłatne narzędzia, które pomogą Ci we wdrożeniu NIS2
- Praktyczny wstęp do modelowania zagrożeń
- Wprowadzenie do bezpieczeństwa OT/ICS i IIoT
- Jak w praktyce testować realną odporność organizacji na incydent, a nie tylko gotowość dokumentacji BCP
- Zarządzanie ryzykiem w NIS2 – praktyczne wykorzystanie NIST CSF

Incydenty/SOC

- Zegar tyka: 24 godz. na zgłoszenie. Praktyczny pokaz obsługi incydentu (IR) od detekcji po raport do CSIRT
- Nie tylko SIEM i EDR – jak zbudować warsztat analityka Incident Response
- Jak wdrożyć SOC na bazie bezpłatnego Wazuha? Wprowadzenie
- Czym jest SOC i po co nam jest potrzebny? pro tipy #1
- Jak w praktyce działa SOC i na co uważać? pro tipy #2
- Case study wdrożenia SOC w realiach samorządu (JST)

Podatności

- Najczęstsze podatności w systemach IT polskich firm oraz instytucji [case studies]
- Jak testować wdrożone przez organizację zabezpieczenia? [testy penetracyjne]
- Wiem, że mam w swoich systemach podatności. Ale co z tym zrobić? [praktyczne zarządzanie podatnościami]

SZKOLENIA PRAWNE (DLA WSZYSTKICH)

- Wprowadzenie. Przegląd najważniejszych wymogów NIS2/KSC2
- Osobista odpowiedzialność zarządu i jak się przed nią obronić?
- NIS2 light. Jak wdrożyć NIS2 w mniejszej organizacji i w sektorze publicznym?
- Współpraca z dostawcami SOC, pentesterami i innymi dostawcami usług cyberbezpieczeństwa
- Obowiązek zgłaszania incydentów a tajemnica przedsiębiorstwa – napięcia prawne
- NIS2 a RODO – jeden incydent, dwa reżimy, dwie instytucje
- Nadzór i sankcje – jak wygląda kontrola organu i jak się do niej przygotować?
- Bezpieczeństwo łańcucha dostaw – jak napisać i ocenić umowę z dostawcą ICT pod NIS2?

Dowody operacyjne zgodności z dwóch perspektyw

- Artykuł 21 NIS2 od środka – co naprawdę oznaczają „odpowiednie środki techniczne i organizacyjne"?
- Dokumentacja operacyjna, ENISA Technical Guidelines i zdrowy rozsądek

SESJE PYTAŃ I ODPOWIEDZI

- Sesja cybersec
- Sesja prawna

MATERIAŁY

- Certyfikat potwierdzający spełnienie obowiązku szkoleniowego opisanego w KSC2
- Przykładowa dokumentacja – reagowanie na incydenty bezpieczeństwa
- Społeczność związana z wdrażaniem NIS2 — Dostęp do serwera Discord
- Regularne quizy sprawdzające Twoją wiedzę
- Dodatkowy dostęp do zapisu filmowego każdego ze szkoleń

KAŻDE ZAGADNIENIE TO JEDNO SZKOLENIE TRWAJĄCE OKOŁO 1,5 GODZ.

securITum

NIS2.SEKURAK.PL