securitum

Akademia NIS2/KSC2
od sekuraka

32 SZKOLENIA ONLINE | 2 SESJE Q&A | NAGRANIA DO 31.12.2027

Praktyczny cykl szkoleń dla osób przygotowujących organizację do spełnienia wymagań NIS2/KSC2

COMPLIANCE (10 SZKOLEŃ)
obowiązki | dokumentacja | incydenty | sankcje | kontrole | NIS2 a RODO

CYBERSEC (17 SZKOLEŃ)
SOC | SIEM | Wazuh | podatności | pentesty | OT/ICS | MFA | DLP | XDR | incydenty

CYBER AWARENESS (5 SZKOLEŃ)
zagrożenia | phishing | socjotechnika | metody obrony | dostawcy

MATERIAŁY SZKOLENIOWE

- nagrania szkoleń
- słowniczek pojęć
- skrócone prezentacje
- quizy
- certyfikat uczestnictwa (PDF)
- przykładowe dokumentacje
- dostęp do społeczności projektu (1000+ osób!)

PO AKADEMII BĘDZIESZ WIEDZIEĆ

- czego realnie wymaga NIS2/KSC2
- jak przygotować organizację do nowych obowiązków
- jak ograniczyć ryzyko kar i odpowiedzialności kadry zarządzającej
- jak oceniać bezpieczeństwo dostawców
- jak podejść do incydentów, SOC, audytów, podatności i testowania zabezpieczeń
- jak budować kulturę cyberbezpieczeństwa w organizacji

INFO LOGISTYCZNE

ROZPOCZĘCIE KURSU
19.10.2026, godz. 10:00

SZKOLENIA
- 2-3 razy w tygodniu
- od 10:00 do 11:30
- Szkolenia na żywo
- Dostęp do nagrań

POTRZEBUJESZ POMOCY?

pomoc@securitum.pl
tel.: +48 (12) 352 33 82
Discord Projektu

DOSTĘP DO DISCORDA

- Wsparcie społeczności na żywo
- Komunikacja z ekipą sekuraka
- Forum pomocowe

NIE MASZ DOSTĘPU?
Pisz na: pomoc@securitum.pl

SEKURAK.PL

NIS2.SEKURAK.PL

securitum

Lista szkoleń w ramach Akademii NIS2/KSC2 od sekuraka

SESJA	MODUŁ	DATA	TYTUŁ SZKOLENIA	TRENER	BILET
Sesja 1	Compliance	19.10.2026	Wprowadzenie. Przegląd najważniejszych wymogów NIS2/KSC2	Marcin Serafin	Standard / Compliance
Sesja 2	Cybersec	23.10.2026	Błyskawiczne sposoby na podniesienie bezpieczeństwa organizacji	Marek Rzepecki	Standard
Sesja 3	Compliance	2.11.2026	NIS2 a RODO – jeden incydent, dwa reżimy, dwie instytucje	Paula Skrzypecka	Standard / Compliance
Sesja 4	Cybersec	4.11.2026	Nie tylko SIEM i EDR – jak zbudować warsztat analityka Incident Response	Maciej Szymczak	Standard
Sesja 5	Compliance	10.11.2026	NIS2 przy małym zespole i ograniczonym budżecie – co naprawdę trzeba zrobić?	Paula Skrzypecka	Standard / Compliance
Sesja 6	Cybersec	12.11.2026	W audycie 100% zgodność. W praktyce 100% fail. Case studies	Maciej Szymczak	Standard
Sesja 7	Cyber Awareness	18.11.2026	SOC/IDS/XDR/SIEM/DLP/MFA – jak się połapać w tym wszystkim?	Tomasz Turba	Standard / Compliance
Sesja 8	Cybersec	20.11.2026	Czym jest SOC i po co nam jest potrzebny? Pro tipy #1	Marek Rzepecki	Standard
Sesja 9	Cyber Awareness	25.11.2026	Dlaczego bezpieczeństwo dostawców jest istotne? Case studies incydentów	Marek Rzepecki	Standard / Compliance
Sesja 10	Cybersec	27.11.2026	Wykonaj praktyczny rekonesans zasobów IT organizacji	Marek Rzepecki	Standard
Sesja 11	Compliance	1.12.2026	Bezpieczeństwo łańcucha dostaw – jak napisać i ocenić umowę z dostawcą ICT pod NIS2?	Paula Skrzypecka	Standard / Compliance
Sesja 12	Cybersec	3.12.2026	Wiem, że mam w swoich systemach podatności. Ale co z tym zrobić? [praktyczne zarządzanie podatnościami]	Maciej Szymczak	Standard
Sesja 13	Compliance	8.12.2026	Nadzór i sankcje – jak wygląda kontrola organu i jak się do niej przygotować?	Paula Skrzypecka	Standard / Compliance
Sesja 14	Cybersec	10.12.2026	Top 3 bezpłatnych narzędzi, które pomogą Ci we wdrożeniu NIS2	Tomasz Turba	Standard
Sesja 15	Compliance	15.12.2026	Osobista odpowiedzialność zarządu i jak się przed nią obronić?	Marcin Serafin	Standard / Compliance
Sesja 16	Cybersec	17.12.2026	Zegar tyka: 24h na zgłoszenie. Praktyczny pokaz obsługi incydentu (IR) od detekcji po raport do CSIRT	Tomasz Turba	Standard
Sesja 17	Compliance	22.12.2026	Artykuł 21 NIS2 od środka – co naprawdę oznaczają „odpowiednie środki techniczne i organizacyjne”? [Dowody operacyjne zgodności z dwóch perspektyw #1]	Paula Skrzypecka	Standard / Compliance

LEGENDA: Compliance Cybersec Cyber Awareness

securITum

Lista szkoleń w ramach Akademii NIS2/KSC2 od sekuraka

SESJA	MODUŁ	DATA	TYTUŁ SZKOLENIA	TRENER	BILET
Sesja 18	Cybersec	28.12.2026	Wprowadzenie do bezpieczeństwa OT/ICS i IIoT	Roland Kulanek	Standard
Sesja 19	Compliance	11.01.2027	Dokumentacja operacyjna, ENISA Technical Guidelines i zdrowy rozsądek [Dowody operacyjne zgodności z dwóch perspektyw #2]	Marcin Serafin i Wojciech Piszewski	Standard / Compliance
Sesja 20	Cybersec	13.01.2027	Jak w praktyce testować realną odporność organizacji na incydent, a nie tylko gotowość dokumentacji BCP?	Joanna Jakubowska	Standard
Sesja 21	Compliance	15.01.2027	Współpraca z dostawcami SOC, pentesterami i innymi dostawcami usług cyberbezpieczeństwa	Marcin Serafin i Wojciech Piszewski	Standard / Compliance
Sesja 22	Cybersec	18.01.2027	SOC w praktyce: jak zacząć? Pro tipy #2	Maciej Szymczak	Standard
Sesja 23	Compliance	20.01.2027	Obowiązek zgłaszania incydentów a tajemnica przedsiębiorstwa – napięcia prawne	Paula Skrzypecka	Standard / Compliance
Sesja 24	Cybersec	22.01.2027	Jak wdrożyć SOC na bazie bezpłatnego WAZUH? Wprowadzenie	Tomasz Turba	Standard
Sesja 25	Cyber Awareness	26.01.2027	Jak obecnie hackerzy przenikają do organizacji?	Michał Sajdak	Standard / Compliance
Sesja 26	Cybersec	28.01.2027	Praktyczny wstęp do modelowania zagrożeń	Kamil Jarosiński	Standard
Sesja 27	Cyber Awareness	2.02.2027	Aktualne cyberataki na pracowników firm. Case studies. Pokazy praktyczne, prewencja	Katarzyna Szczypiń	Standard / Compliance
Sesja 28	Cybersec	4.02.2027	Najczęstsze podatności w systemach IT polskich firm oraz instytucji [case studies]	Marcin Piosek	Standard
Sesja 29	Cybersec	9.02.2027	Zarządzanie ryzykiem w NIS2 – praktyczne wykorzystanie NIST CSF	Joanna Jakubowska	Standard
Sesja 30	Cyber Awareness	11.02.2027	Jak zbudować program szkoleń / kulturę cyberbezpieczeństwa w organizacji?	Michał Sajdak	Standard / Compliance
Sesja 31	Cybersec	16.02.2027	Jak testować wdrożone przez organizację zabezpieczenia? [testy penetracyjne]	Maciej Szymczak	Standard
Sesja 32	Cybersec	18.02.2027	Case study wdrożenia SOC w realiach samorządu (JST)	Sławomir Świder	Standard
Q&A	Compliance	23.02.2027	Dedykowana sesja pytań i odpowiedzi (około 1.5h)	Marcin Serafin, Wojciech Piszewski, Paula Skrzypecka	Standard / Compliance
Q&A	Cybersec	25.02.2027	Dedykowana sesja pytań i odpowiedzi (około 1.5h)	Tomasz Turba, Michał Sajdak, Marek Rzepecki, Maciej Szymczak	Standard

LEGENDA: Compliance Cybersec Cyber Awareness

Trenerzy Akademii NIS2/KSC2

Michał Sajdak

Założyciel sekuraka, ekspert ds. ofensywnego bezpieczeństwa IT, współautor i redaktor branżowych bestsellerów. Od lat szkoli, audytuje i pokazuje, jak wyglądają realne ataki na organizacje.

Tomasz Turba

Konsultant ds. bezpieczeństwa IT w Securitum, praktyk z doświadczeniem administratora, pentestera, SOC i RODO. Specjalizuje się m.in. w AI, Wazuhu, automatyzacji i praktycznym podnoszeniu bezpieczeństwa organizacji.

Maciej Szymczak

CISO i konsultant ds. cyberbezpieczeństwa w Securitum, etyczny hacker i trener. Łączy doświadczenie pentesterskie z perspektywą zarządzania bezpieczeństwem w organizacji.

Marek Rzepecki

Etyczny hacker i konsultant ds. bezpieczeństwa w Securitum. Specjalizuje się w testach bezpieczeństwa aplikacji, infrastruktury, rekonesansie i praktycznych case studies z cyberbezpieczeństwa.

Paula Skrzypecka

Doktor nauk prawnych, ekspertka ds. prawa nowych technologii, AI, chmury, RODO i cyberbezpieczeństwa. Wspiera organizacje w obszarze zgodności, danych, regulacji i umów technologicznych.

Marcin Serafin

Partner w kancelarii Sterberg, ekspert ds. ochrony danych, AI i cyberbezpieczeństwa z 20-letnim doświadczeniem w projektach technologicznych i regulacyjnych. Doradza przy incydentach, strategii odporności cyfrowej i wdrożeniach wymogów prawnych.

Wojciech Piszewski

Partner w kancelarii Sterberg, ekspert ds. AI, cyberbezpieczeństwa, ochrony danych, compliance i e-commerce. Wspiera organizacje w audytach zgodności, analizie ryzyk i wdrażaniu systemów compliance.

Joanna Jakubowska

Ekspertka ds. cyberbezpieczeństwa i GRC, specjalizująca się w NIS2, DORA, AI Act, RODO, NIST, ISO 27001 i ISO 22301. Pomaga przekładać wymagania regulacyjne na konkretne procesy i działania operacyjne.

Trenerzy Akademii NIS2/KSC2

Kamil Jarosiński

Konsultant ds. bezpieczeństwa w Securitum, pentester i trener. Specjalizuje się w bezpieczeństwie aplikacji WWW, API, chmury i testach środowisk technicznych.

Marcin Piosek

Ekspert ds. bezpieczeństwa IT i Team Leader w Securitum. Koordynuje zespoły pentesterskie, testuje systemy w sektorze finansowym i usługowym oraz publikuje materiały z zakresu bezpieczeństwa IT.

Roland Kulanek

Specjalista cyberbezpieczeństwa OT/ICS i IT. Zajmuje się architekturą bezpieczeństwa przemysłowego, ochroną systemów produkcyjnych i standardami dla środowisk OT/ICS.

Sławomir Świder

Zastępca dyrektora Biura Obsługi Informatycznej i Telekomunikacyjnej Urzędu Miasta Rzeszowa. Praktyk wdrożeń IT i cyberbezpieczeństwa w samorządzie, związany m.in. z miejską siecią teleinformatyczną i projektem SOC.

Katarzyna Szczypiń

Doświadczona trenerka cyberbezpieczeństwa z ponad 7-letnim stażem, specjalizująca się w cyberhigienie, socjotechnice i pogłębianiu świadomości użytkowników w tym zakresie. Prowadzi szkolenia po polsku i angielsku oraz webinary dla sektora bankowego (między innymi Standard Chartered, BNP Paribas). Poza pracą jest aktywną kolarką torową i ratownikiem medycznym.