

CERTYFIKAT

UCZESTNICTWA W SZKOLENIU

BEZPIECZEŃSTWO IPV6 OD PODSTAW PROTOKOŁU DO HARDENINGU INFRASTRUKTURY

DLA:

Fabian Leśniak

DATA: 21, 22 i 23 KWIETNIA 2026 r.

TRENER: Piotr Wojciechowski

CZAS TRWANIA: 6 godzin

AGENDA

Sesja 1. IPv6 – podstawy:

- Budowa adresu IPv6 – typy adresów: link-local, ULA, GUA
- Różnice względem IPv4: brak broadcastu, obowiązkowy multicast
- Prefix delegation, SLAAC, DHCPv6 stateless i stateful
- Dual-stack i mechanizmy tunelowania: 6in4, 6to4, ISATAP
- Mechanizm DAD (Duplicate Address Detection) – jak działa i dlaczego

Sesja 2. Bezpieczeństwo IPv6 w warstwie drugiej:

- SEND (Secure Neighbor Discovery) – teoria i realia wdrożenia
- DHCPv6: opcje, relay, prefix delegation
- NTP i zarządzanie urządzeniami przez IPv6
- Rekonesans przez skanowanie IPv6
- Wdrożenie RA Guard, DHCPv6 Guard

Sesja 3. Routing i infrastruktura IPv6:

- OSPFv3, EIGRPv6, BGP dla IPv6
- Policy-based routing w dual-stack
- ACL IPv6 na Cisco: różnice vs IPv4 ACL
- Blokowanie tuneli przejściowych (Teredo, ISATAP, 6to4) w środowisku korporacyjnym
- CoPP dla IPv6, filtrowanie ICMPv6 (co blokować, czego nie)

PUNKTY CPE/ECE: 6

SZKOLENIA.SECURITUM.PL

