

Analiza ruchu sieciowego w modelu TCP/IP

[Dyrektywa NIS2](#) Unijne przepisy rozszerzają zakres przepisów dotyczących cyberbezpieczeństwa. Przedsiębiorcy objęci regulacją NIS2, wynikającą z ustawy o krajowym systemie bezpieczeństwa, będą objęci obowiązkiem stosowania produktów, usług bądź procesów, objętych tymi schematami certyfikacyjnymi. [Sprawdź, czy Twoja firma będzie objęta dyrektywą NIS2](#)



Przeznaczenie szkolenia

Szkolenie skierowane do pracowników niższego szczebla działów IT, analityków sieci, administratorów systemów informatycznych, administratorów sieci oraz osób rozpoczynających pracę związaną z infrastrukturą sieciową.



Korzyści wynikające z ukończenia szkolenia

Uzyskanie wiedzy i praktycznych umiejętności posługiwania się narzędziami do analizy ruchu w sieciach teleinformatycznych. Poznasz podstawy użycia narzędzia Wireshark, będziesz potrafić zbierać, filtrować i analizować różnorodną komunikację sieciową. Na szkoleniu przekażemy Ci również wiedzę dotyczącą wykrywania typowych anomalii i zagrożeń w ruchu sieciowym



Oczekiwane przygotowanie słuchaczy

Wymagana wiedza związana z teorią sieci opartych na TCP/IP oraz doświadczenie i umiejętności z zakresu konfiguracji sieci. Mile widziany wcześniejszy udział w szkoleniu „Podstawy działania sieci opartych na modelu TCP/IP”.



Język szkolenia

- Szkolenie: polski
- Materiały: angielski / polski



Szkolenie obejmuje

* materiały w formie elektronicznej dostępne na platformie: <https://www.altkomakademia.pl/>

* dostęp do portalu słuchacza Altkom Akademii

Metoda szkolenia:

wykład + warsztaty



Czas trwania

2 dni / 14 godzin

Agenda szkolenia

1. Komunikacja sieciowa
 - Warstwowy model sieci TCP/IP
 - Typowe rodzaje komunikacji w sieci TCP/IP
2. Przegląd narzędzi przydatnych do analizy ruchu sieciowego
 - Przykładowe narzędzia Microsoft
 - Przykładowe aplikacje i rozwiązania firm trzecich

LAB: Narzędzia do analizy ruchu w sieci
3. Użycie programu Wireshark
 - Podstawy korzystania z Wireshark
 - Podstawy monitorowania ruchu sieciowego
 - Filtry w Wireshark

LAB: Korzystanie z Wireshark
4. Analiza ruchu ARP, TCP i UDP
 - Analiza ruchu ARP
 - Analiza ruchu TCP
 - Analiza ruchu UDP

LAB: Analiza ruchu ARP, TCP i UDP

5. Analiza ruchu DHCP i DNS

- Analiza ruchu DHCP
- Analiza ruchu DNS

LAB: Analiza ruchu DHCP i DNS

6. Analiza ruchu SMB, HTTP i HTTPS

- Analiza ruchu SMB
- Analiza ruchu HTTP
- Analiza ruchu HTTPS

LAB: Analiza ruchu SMB, HTTP i HTTPS

7. Wykrywanie przykładowych anomalii i zagrożeń w sieci

- Analiza obciążenia sieci
- Wykrywanie nieautoryzowanego serwera DHCP
- Zduplikowane adresy IP
- Zduplikowane adresy MAC
- Wykrywanie przykładowych zagrożeń

LAB: Wykrywanie anomalii i zagrożeń w sieci

8. Laboratorium podsumowujące