Szkolenie autoryzowane

ESET Secure Authentication

Strona szkolenia | Terminy szkolenia | Rejestracja na szkolenie | Promocje

Opis szkolenia

ESET Secure Authentication pozwala chronić poufne dane firmowe przed nieautoryzowanym dostępem i wzmacnia uwierzytelnienie pracowników podczas zdalnego korzystania z zasobów firmowych.

To zaawansowane narzędzie dwuetapowej autoryzacji z wykorzystaniem haseł jednorazowych generowanych np. poprzez urządzenie mobilne. Szkolenie kompleksowo wprowadza w temat ochrony, instalacji, konfiguracji i metod uwierzytelniania rozwiązania.

Szkolenie i materiały w języku polskim.

Korzyści po szkoleniu

- Dowiesz się czym jest uwierzytelnianie wieloskładnikowe
- Poznasz w pełni rozwiązanie ESA
- Wykorzystasz pełnię możliwości rozwiązania ESA

Wymagania

- podstawowa znajomość konfiguracji sieci komputerowych,
- podstawowa znajomość zagadnień związanych z TCP/IP,
- podstawowa wiedza na temat wirtualizacji,

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
szkolenia.dagma.eu

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
Numer KRS: 0000130206, kapitał zakładowy: 75 000 zł
Numer NIP: 634-012-60-68, numer REGON: 008173852

- telefon komórkowy z kartą SIM, dostępem do Internetu (Apple - iOS 12+ lub Android z usługami Google).

Harmonogram szkolenia

1. Wprowadzenie do tematu dwuskładnikowego uwierzytelniania.
2. ESET PROTECT Hub – licencjonowanie (ćwiczenie).
3. Instalacja serwera ESET Secure Authentication On-prem (ćwiczenie).
4. Omówienie funkcji serwera ESET Secure Authentication On-prem.
5. Konfiguracja serwera ESET Secure Authentication On-prem (ćwiczenia):
    1. dodanie licencji,
    2. konfiguracja użytkownika,
    3. wdrożenie i konfiguracja aplikacji mobilnej.
6. Omówienie możliwości ochrony zasobów firmowych przy użyciu ESET Secure Authentication On-prem.
7. Wdrożenie klienta ESET Secure Authentication On-prem (ćwiczenie):
    1. konfiguracja klienta,
    2. metody uwierzytelniania
8. Instalacja systemu raportowania (ćwiczenie).
9. Instalacja ochrony połączenia VPN (ćwiczenie).
10. Konfiguracja ochrony połączeń VPN (ćwiczenie).
11. Rozwiązywanie problemów.

Tagi: