I know IT by softinet

KNOWLEDGE THAT
EMPOWERS BUSINESS

Administracja rozwiązaniem SentinelOne Singularity

- Weź udział w szkoleniu i poznaj wszystkie funkcje rozwiązania SentinelOne. Podczas praktycznych warsztatów zdobędziesz wiedzę, która pozwoli Ci na:
- Samodzielne zarządzanie rozwiązaniem.
- Zrozumienie mechanizmów, za pomocą których wykrywane są zagrożenia.
- Stworzenie bezpiecznego środowiska pracy w Twojej organizacji.
- Analizę incydentów bezpieczeństwa za pomocą wbudowanych narzędzi.

Czas
2 DNI

Godziny
9:00 - 16:00

Certyfikat
TAK

OPIS SZKOLENIA

Szkolenie dedykowane osobom chcącym zapobiegać nawet najbardziej zaawansowanym cyberatakom. Po jego ukończeniu uczestnicy zdobędą szeroką wiedzę dotyczącą budowy oraz funkcjonalności konsoli SentinelOne - poznają jej strukturę, możliwości oraz zasady działania.

Dzięki praktycznym ćwiczeniom Uczestnicy poznają możliwości SentinelOne pod kątem ochrony swojego środowiska, w tym nauczą się np. zarządzać zadaniami, przeprowadzać skany bezpieczeństwa oraz zidentyfikować i naprawić słabe punkty infrastruktury.

Ukończenie szkolenia pozwoli na zrozumienie mechanizmów, za pomocą których wykrywane są zagrożenia, oraz na analizę przebiegu ataków, a następnie na przeprowadzenie szybkiej i skutecznej remediacji.

CEL SZKOLENIA

Zdobycie umiejętności praktycznych potrzebnych do samodzielnej administracji rozwiązaniem SentinelOne Singularity. Poznanie dobrych praktyk pozwalających na konfigurację bezpiecznego środowiska oraz zdobycie wiedzy pozwalającej na analizę i remediację wykrytych zagrożeń.

FORMA SZKOLENIA

Szkolenie prowadzone jest w formie zdalnego wykładu, połączonego z ćwiczeniami warsztatowymi wykonywanymi zdalnie.

WYMAGANIA

Znajomość podstawowych zagadnień dotyczących administracji infrastrukturą sieciową, Active Directory, serwerami Windows/Unix/Linux. Znajomość podstawowych protokołów sieciowych.

FORTIGATE - kompleksowe bezpieczeństwo sieci komputerowej

Agenda szkolenia:

1. Wprowadzenie
- Co to jest SentinelOne?
- Omówienie architektury

2. Instalacja Agenta
- Łączność sieciowa – wymagania
- Obsługiwane systemy
- Metody instalacji
- Rozwiązywanie problemów

3. Konfiguracja rozwiązania
- Polityki
- Grupy
- Hierarchia i dziedziczenie
- Wykluczenia
- Network Control – Firewall
- Device Control
- Procedura aktualizacji agentów

4. Obsługa incydentów i alarmów
- MITRE ATT&CK
- Storyline
- Metody Remediacji

5. Dodatkowe funkcjonalności
- Inwentaryzacja aplikacji
- Wykrywanie podatności
- Zwiększenie widoczności - moduł Ranger
- Automatyzacja zadań – Remote Ops

6. Threat Hunting – wprowadzenie
- Deep Visibility
- STAR Custom Rules
- Forensic Profile
- Purple AI

7. Dashboard i Raporty

8. Integracje
- Singularity Marketplace
- API - wprowadzenie

TRENERZY

Inżynierowie posiadający certyfikat SentinelOne Paladin (najwyższy stopień certyfikacji technicznej).

TADEUSZ SELBIRAK

www.iknowit.com.pl

AL. JEROZOLIMSKIE 142B, 02-305 WARSZAWA

szkolenia@ iknowit.com.pl

(22) 427 37 54 / +48 728 540 162