Szkolenie autoryzowane

SC 200T00 Microsoft Security Operations Analyst

Strona szkolenia | Terminy szkolenia | Rejestracja na szkolenie | Promocje

Opis szkolenia

Szkolenie podejmuje tematykę zagrożeń w kontekście usługi Microsoft Sentinel, Microsoft Defender for Cloud i Microsoft 365 Defender. Podczas szkolenia, omówione zostaną sposoby ograniczania zagrożenia cybernetycznego za pomocą tych technologii, a w szczególności konfiguracja i korzystanie z usługi Microsoft Sentinel oraz z języka KQL (Kusto Query Language) do wykrywania, analizowania i raportowania.

Po ukończeniu szkolenia, uczestnik będzie potrafił:

- Wyjaśnić, w jaki sposób program Microsoft Defender for Endpoint i Microsoft Defender for Identity mogą zapobiegać zagrożeniom w danym środowisku,
- Administrować środowisko Microsoft Defender for Endpoint,
- Konfigurować reguły Attack Surface Reduction na urządzeniach z systemem Windows,
- Badać domeny i adresy IP oraz konta użytkowników w usłudze Microsoft Defender for Endpoint,
- Konfigurować ustawienia alertów w usłudze Microsoft 365 Defender,
- Wyjaśnić, jak rozwijają się zagrożenia, monitorować je w czasie za pomocą podglądu i używać zapytań do ich neutralizacji,
- Zarządzać zdarzeniami w usłudze Microsoft 365 Defende,
- Badać alerty DLP w usłudze Microsoft Defender for Cloud Apps,
- Wyjaśnić różne rodzaje działań, które można podjąć w przypadku zarządzania ryzykiem wewnętrznym,
- Konfigurować automatyczną zdalną konfigurację w usłudze Microsoft Defender for Cloud Apps,

- Korygować alerty w usłudze Microsoft Defender for Cloud Apps,
- Tworzyć instrukcje KQL,
- Filtrować wyszukiwanie na podstawie czasu zdarzenia, priorytetu, domeny i innych istotnych danych przy użyciu funkcji KQL,
- Wyodrębniać dane z nieustrukturyzowanych pól typu string przy użyciu KQL,
- Zarządzać obszarem roboczym usługi Microsoft Sentinel,
- Konfigurować dostęp do listy obserwowanych (watchlist) w usłudze Microsoft Sentinel za pomocą KQL,
- Zarządzać wskaźnikami zagrożeń w usłudze Microsoft Sentinel,
- Wyjaśnić różnice w CEF (Common Event Format) i łączniku Syslog w usłudze Microsoft Sentinel,
- Łączyć maszyny wirtualne systemu Azure z usługą Microsoft Sentinel,
- Konfigurować agenta usługi Log Analytics do zbierania zdarzeń Sysmon,
- Tworzyć nowe reguły i zapytania analityczne za pomocą kreatora reguł analizy,
- Tworzyć podręczniki z regułami działania (playbooki) w celu automatyzacji reagowania na zdarzenia.

Wymagania:

- Podstawowa wiedza o usłudze Microsoft 365,
- Podstawowe rozumienie zabezpieczeń, zgodności i tożsamości produktów firmy Microsoft,
- Średniozaawansowana znajomość systemu Windows 10,
- Znajomość usług platformy Azure, w szczególności usługi Azure SQL Database i usługi Azure Storage,
- Znajomość maszyn wirtualnych platformy Azure i sieci wirtualnych,
- Podstawowa wiedza na temat pojęć skryptów.

SZKOLENIE PROWADZONE JEST W JĘZYKU POLSKIM, MATERIAŁY W JĘZYKU ANGIELSKIM.

Program szkolenia

Moduł 1: Ograniczanie zagrożeń przy użyciu usługi Microsoft 365 Defender

- Wprowadzenie do ochrony przed zagrożeniami dzięki usłudze Microsoft 365
- Ograniczanie zdarzeń przy użyciu usługi Microsoft 365 Defender
- Usuwanie ryzyka przy użyciu usługi Microsoft Defender dla usługi Office 365
- Ochrona środowiska dzięki usłudze Microsoft Defender for Identity
- Ochrona tożsamości przy użyciu usługi Azure AD Identity Protection
- Ochrona przy użyciu usługi Microsoft Defender for Cloud Apps

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

- Reagowanie na alerty dotyczące zapobiegania utracie danych przy użyciu usługi Microsoft 365
- Zarządzenie ryzykiem wewnętrznym przy użyciu usługi Microsoft 365

Laboratorium: Ograniczanie zagrożeń przy użyciu usługi Microsoft 365 Defender

- Zapoznanie się z Microsoft 365 Defender

Moduł 2: Ograniczanie zagrożeń przy użyciu usługi Microsoft Defender for Endpoint

- Ochrona przed zagrożeniami za pomocą programu Microsoft Defender for Endpoint
- Wdrażanie środowiska usługi Microsoft Defender for Endpoint
- Wdrażanie ulepszeń zabezpieczeń systemu Windows
- Wykonywanie badań dotyczących urządzeń
- Wykonywanie akcji na urządzeniu
- Wykonywanie badań dotyczących zdarzeń i encji
- Konfigurowanie i zarządzanie automatyzacji
- Konfigurowanie alertów i wykrywania
- Wykorzystanie zarządzania zagrożeniami i lukami

Laboratorium: Ograniczanie zagrożeń przy użyciu usługi Microsoft 365 Defender for Endpoint

- Wdrażanie usługi Microsoft Defender for Endpoint
- Ograniczanie zagrożeń przy pomocy usługi Defender for Endpoint

Moduł 3: Ograniczanie zagrożeń przy użyciu usługi Microsoft Defender for Cloud

- Planowanie zabezpieczeń obciążeń w chmurze przy użyciu usługi Microsoft Defender for Cloud
- Zabezpieczanie obciążeń przy użyciu usługi Microsoft Defender for Cloud
- Łączenie zasobów platformy Azure z usługą Microsoft Defender for Cloud
- Łączenie zasobów niekorzystających z Azure z usługą Microsoft Defender for Cloud
- Korygowanie alertów zabezpieczeń przy użyciu usługi Microsoft Defender for Cloud

Laboratorium: Ograniczanie zagrożeń przy użyciu usługi Microsoft Defender for Cloud

- Wdrażanie usługi Microsoft Defender for Cloud
- Ograniczanie zagrożeń przy pomocy usługi Microsoft Defender for Cloud

Moduł 4: Tworzenie zapytań dla usługi Microsoft Sentinel przy użyciu języka KQL (Kusto Query Language)

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

- Konstruowanie instrukcji KQL dla Microsoft Sentinel
- Analizowanie wyników kwerend przy użyciu KQL
- Tworzenie instrukcji dla wielu tabel przy użyciu KQL
- Praca z danymi typu string przy użyciu instrukcji KQL

Laboratorium: Tworzenie zapytań dla usługi Microsoft Sentinel przy użyciu języka KQL (Kusto Query Language)

- Tworzenie zapytań dla usługi Microsoft Sentinel przy użyciu języka KQL (Kusto Query Language)

Moduł 5: Konfiguracja środowiska Microsoft Sentinel

- Tworzenie obszarów roboczych usługi Microsoft Sentinel i zarządzanie nimi
- Logi zapytań w usłudze Microsoft Sentinel
- Używanie list obserwowanych (watchlist) w usłudze Microsoft Sentinel
- Korzystanie z analizy zagrożeń (threat intelligence) w usłudze Microsoft Sentinel

Laboratorium: Konfiguracja środowiska Microsoft Sentinel

- Konfiguracja środowiska Microsoft Sentinel

Moduł 6: Łączenie logów z usługą Microsoft Sentinel

- Łączenie danych z usługą Microsoft Sentinel przy użyciu łączników danych
- Łączenie usług firmy Microsoft z usługą Microsoft Sentinel
- Łączenie usługi Microsoft 365 Defender z usługą Microsoft Sentinel
- Łączenie hostów systemu Windows z usługą Microsoft Sentinel
- Łączenie dzienników w CEF z usługą Microsoft Sentinel
- Łączenie źródeł danych syslogu z usługą Microsoft Sentinel
- Łączenie wskaźników zagrożeń z usługą Microsoft Sentinel

Laboratorium: Dołączanie logów do Microsoft Sentinel

- Łączenie danych z usługą Microsoft Sentinel przy użyciu łączników danych
- Łączenie urządzeń z systemem Windows do Microsoft Sentinel przy użyciu łączników danych
- Łączenie hostów w systemie Linux z Microsoft Sentinel przy użyciu łączników danych
- Łączenie analizy zagrożeń (threat intelligence) z Microsoft Sentinel przy użyciu łączników danych

Moduł 7: Wykrywanie i badanie zagrożeń przy użyciu usługi Microsoft Sentinel

- Wykrywanie zagrożeń za pomocą analizy Microsoft Sentinel
- Zarządzanie zdarzeniami bezpieczeństwa w usłudze Microsoft Sentinel
- Reagowanie na zagrożenia za pomocą playbooków Microsoft Sentinel

- Analiza zachowania użytkowników i jednostek (User and Entity Behavior Analytics) w usłudze Microsoft Sentinel
- Zapytania, wizualizacja i monitorowanie danych w Microsoft Sentinel

Laboratorium: Wykrywanie i badanie zagrożeń przy użyciu usługi Microsoft Sentinel

- Aktywacja reguły Microsoft Security
- Tworzenie playbooków
- Tworzenie zaplanowanych zapytań (Scheduled Query)
- Zrozumienie modelowania wykrywania
- Przeprowadzanie ataków
- Wykrywanie
- Badanie zdarzeń
- Tworzenie skoroszytów

Moduł 8: Neutralizacja zagrożeń w usłudze Microsoft Sentinel

Uczestnicy dowiedzą się jak proaktywnie identyfikować zagrożenia za pomocą zapytań Azure Sentinel.

- Koncepcje dotyczące wyszukiwania zagrożeń w programie Microsoft Sentinel
- Wyszukiwanie zagrożeń za pomocą programu Microsoft Sentinel
- Szukanie zagrożeń przy użyciu notatników w programie Microsoft Sentinel

Laboratorium: Wyszukiwanie zagrożeń w programie Microsoft Sentinel

- Neutralizacja zagrożeń w usłudze Microsoft Sentinel
- Wyszukiwanie zagrożeń przy użyciu notatników z programem Microsoft Sentinel

---

Tagi:

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