Możliwość dofinansowania

Dagma sp. z o.o.

4,5 / 5

454 oceny

BLUE TEAM - Poziom 3: Detekcja, Reagowanie i Automatyzacja w SOC L1

Numer usługi 2026/01/19/17164/3268074

Usługa szkoleniowa

zdalna w czasie rzeczywistym

07:00 h

19.06.2026 do 19.06.2026

2 447,70 PLN brutto

1 990,00 PLN netto

349,67 PLN brutto/h

284,29 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	**Szkolenie Blue Team Poziom 3 to najbardziej zaawansowany moduł w cyklu edukacyjnym Blue Team. Skierowane jest do specjalistów, którzy opanowali już fundamenty cyberbezpieczeństwa (Poziom 0), logowanie i monitoring (Poziom 1) oraz ochronę infrastruktury (Poziom 2), i chcą wejść na wyższy poziom analizy incydentów, automatyzacji reakcji oraz integracji systemów SOC.** Szkolenie opiera się na realistycznych scenariuszach ataków: brute-force, phishing, ransomware oraz APT. Uczestnicy analizują prawdziwe logi z Windows, Linux, firewalli i EDR, wykorzystując narzędzia takie jak **Elastic Stack**, **Shuffle**, **MISP**, **VirusTotal** i inne.
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	08-06-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	7
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Uczestnicy nauczą się wykorzystywać zaawansowane systemy SIEM i SOAR, analizować alerty bezpieczeństwa w czasie rzeczywistym oraz automatyzować triage i eskalację incydentów. Szczególny nacisk położony jest na korelację logów, detekcję złośliwej aktywności, analizę wskaźników kompromitacji (IoC) oraz integrację Threat Intelligence z systemami detekcji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Poznanie zaawansowanych funkcji SIEM i korelacji logów.	Uczestnik poprawnie analizuje i koreluje logi z różnych źródeł w systemie SIEM oraz identyfikuje incydenty na podstawie reguł detekcji i filtrów.	Obserwacja w warunkach symulowanych
Automatyzacja triage alertów i reakcji z wykorzystaniem SOAR.	Uczestnik konfiguruje i uruchamia playbooki SOAR automatyzujące triage alertów oraz potrafi uzasadnić zastosowane mechanizmy automatycznej reakcji.	Obserwacja w warunkach symulowanych
Detekcja zaawansowanych zagrożeń (ransomware, phishing, C2).	Uczestnik rozpoznaje wzorce zaawansowanych zagrożeń w logach i alertach oraz stosuje odpowiednie techniki detekcji do ich identyfikacji.	Obserwacja w warunkach symulowanych
Praktyczne wykorzystanie Threat Intelligence w SOC.	Uczestnik wykorzystuje dane Threat Intelligence do wzbogacania alertów i oceny zagrożeń oraz poprawnie interpretuje wskaźniki kompromitacji (IOC).	Obserwacja w warunkach symulowanych
Eskalacja i tworzenie dokumentacji incydentów zgodnie z dobrymi praktykami.	Uczestnik poprawnie eskaluje incydenty oraz tworzy dokumentację zgodną z przyjętymi standardami i procedurami SOC.	Obserwacja w warunkach symulowanych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

TAK

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Moduł 1: SIEM – Analiza logów i alertów

- Wprowadzenie do funkcji SIEM i jego architektury
- Rola SIEM w SOC L1.
- Źródła logów: Windows Event Logs, Sysmon, firewall.
- Ćwiczenia: analiza i korelacja zdarzeń z logów na przykładzie ataków.

Moduł 2: Frameworki detekcji – MITRE ATT&CK, Sigma, YARA

- Rola frameworków w detekcji zagrożeń.
- Łączenie frameworków w SOC L1.
- Proces detekcja zagrożeń.

Moduł 3: Eskalacja alertów i triage, Incident Response (IR)

- 5-punktowa checklista L1 do oceny alertu.
- Tworzenie raportu eskalacyjnego do L2/L3.
- Automatyzacja: auto-close, auto-escalate, tagging, playbooki.
- Etapy reagowania na incydent (wg NIST).
- Ćwiczenia: reakcja na incydent oraz dopasowanie reguł i tworzenie raportu

Moduł 4: SOAR – Automatyzacja reakcji

- Architektura SOAR (Shuffle): webhooki, playbooki, konektory.
- Scenariusze automatyzacji: phishing, ransomware, hash checking.
- Integracja z Elastic, VirusTotal, HybridAnalysis.

Moduł 5: Threat Intelligence – analiza IoC

- TI jako źródło kontekstu: hash, IP, domena, sandbox.
- Narzędzia: VirusTotal, OTX, HybridAnalysis, Any.Run, MISP.
- Korelacja IoC w SIEM (Indicator Match), feedy TI w SOAR.

Harmonogram

Liczba pozycji harmonogramu: 0

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 447,70 PLN
Koszt przypadający na 1 uczestnika netto	1 990,00 PLN
Koszt osobogodziny brutto	349,67 PLN
Koszt osobogodziny netto	284,29 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Mariusz Wilczyński

...

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- materiały dydaktyczne w formie elektronicznej (prezentacja, do której dostęp zostanie udostępniony na adres e-mail uczestnika)

Warunki uczestnictwa

Prosimy o zapisanie się na szkolenie przez naszą stronę internetową **https://szkolenia.dagma.eu/pl** w celu rezerwacji miejsca.

Informacje dodatkowe

- Jedna godzina lekcyjna to 45 minut
- W cenę szkolenia nie wchodzą koszta związane z dojazdem, wyżywieniem oraz noclegiem.
- Szkolenie nie zawiera egzaminu.
- Uczestnik otrzyma zaświadczenie DAGMA Szkolenia IT o ukończeniu szkolenia
- Uczestnik ma możliwość złożenia reklamacji po zrealizowanej usłudze, sporządzając ją w formie pisemnej (na wniosku reklamacyjnym) i odsyłając na adres szkolenia@dagma.pl. Reklamacja zostaje rozpatrzona do 30 dni od dnia otrzymania dokumentu przez DAGMA SZKOLENIA IT.

Warunki techniczne

a) platforma/rodzaj komunikatora, za pośrednictwem którego prowadzona będzie usługa:

- **ZOOM i/lub MS Teams**
- w przypadku kilku uczestników przebywających w jednym pomieszczeniu, istnieją dwie możliwości udziału w szkoleniu:

1) każda osoba bierze udział w szkoleniu osobno (korzystając z oddzielnych komputerów), wówczas należy wyciszyć dźwięki z otoczenia by uniknąć sprzężeń;

2) otrzymujecie jedno zaproszenie, wówczas kilka osób uczestniczy w szkoleniu za pośrednictwem jednego komputera

- Można łatwo udostępniać sobie ekran, oglądać pliki, bazę handlową, XLS itd.

b) minimalne wymagania sprzętowe, jakie musi spełniać komputer Uczestnika lub inne urządzenie do zdalnej komunikacji:

- Uczestnik potrzebuje komputer z przeglądarką Chrome lub Edge (NIE firefox), mikrofon, głośniki.

c) minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik:

- łącze internetowe o przepustowości minimum 10Mbit,

d) niezbędne oprogramowanie umożliwiające Uczestnikom dostęp do prezentowanych treści i materiałów:

- uczestnik na tydzień przed szkoleniem otrzyma maila organizacyjnego, ze szczegółową instrukcją pobrania darmowej platformy ZOOM.
- Z platformy MS Teams można korzystać za pośrednictwem przeglądarki, nie trzeba nic instalować.

e) okres ważności linku:

- link będzie aktywny od pierwszego dnia rozpoczęcia się szkolenia do ostatniego dnia trwania usługi

Szczegóły, związane z prowadzonymi przez nas szkoleniami online, znajdziesz na naszej stronie: https://szkolenia.dagma.eu/pl/training-list

Kontakt

Michalina Krzyszkowska

E-mail krzyszkowska.m@dagma.pl
Telefon (+48) 327 931 015