Możliwość dofinansowania

Dagma sp. z o.o.

★★★★½

Informatyka śledcza Pozyskiwanie i analiza elektronicznych dowodów przestępstw

Numer usługi 2024/07/04/17164/2209326

zdalna w czasie rzeczywistym
Usługa szkoleniowa
21 h
10.09.2024 do 12.09.2024

3 677,70 PLN brutto
2 990,00 PLN netto
175,13 PLN brutto/h
142,38 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Szkolenie przeznaczone jest dla osób pracujących w sektorze IT, chcących rozpocząć swoją przygodę z informatyką śledczą.
Minimalna liczba uczestników	4
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	03-09-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	21
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

Celem szkolenia jest dostarczenie kompetencji z zakresu Informatyki śledczej, dzięki którym uczestnik będzie samodzielnie wykorzystywał możliwości sprzętu i oprogramowania oraz stosował nawyki w prowadzeniu analiz śledczych. Uczestnik nabędzie kompetencje społeczne, takie jak samokształcenie, współpraca w zespole, rozstrzyganie dylematów związanych z codzienną pracą.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik wie, jak działają procesy analizy śledczej, wie jak tworzyć kopie binarne komputerów pple; przeprowadzać fizyczną ekstrakcję urządzeń mobilnych	samodzielna praca i wykonywanie zadań w środowisku wirtualnym podczas szkolenia	Obserwacja w warunkach rzeczywistych
Uczestnik nabędzie umiejętności: zabezpieczania dysków, poczty elektronicznej, stron internetowych oraz innych nośników; zabezpieczania informacji ulotnych wykonuje kopie binarne w środowisku sieciowym i lokalnym; Wyszukiwania i ukrywania plików w Alternatywnych strumieniach danych	samodzielna praca i wykonywanie zadań w środowisku wirtualnym podczas szkolenia	Obserwacja w warunkach rzeczywistych
Uczestnik nabędzie kompetencje społeczne, takie jak samokształcenie, rozwiązywanie problemów, kreatywność w działaniu.	samodzielna praca i wykonywanie zadań w środowisku wirtualnym podczas szkolenia	Obserwacja w warunkach rzeczywistych

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 Informatyka śledcza - definicja, znaczenie - zajęcia teoretyczne (wykład)

- Cele informatyki śledczej
- Dowód elektroniczny

- Co nam wolno, a na co powinniśmy uważać
- Założenia informatyki śledczej

Moduł 2 Polskie i światowe praktyki wykorzystywane w informatyce śledczej - zajęcia teoretyczne (wykład)

- Procesy analizy śledczej
- Sposób zabezpieczania i gromadzenia danych
- Reguły i zasady przeprowadzania analizy śledczej
- Opis i przedstawienie narzędzi wykorzystywanych przez śledczych
- Opis i przedstawienie programów wykorzystywanych przez śledczych
- Co to jest kopia binarna i po co jest nam w ogóle potrzebna
- Proces zabezpieczenia materiału jako dowodu
- Kopie binarne komputerów pple
- Proces zabezpieczenia materiału dowodowego zaszyfrowanych nośników
- Proces zabezpieczenia materiału dowodowego – Live Forensics

Moduł 3 Logiczna ekstrakcja urządzeń mobilnych - zajęcia praktyczne (ćwiczenia)

- Logiczna ekstrakcja – system plików urządzeń mobilnych
- Fizyczna ekstrakcja urządzeń mobilnych
- Różnice między logiczną a fizyczną ekstrakcja urządzeń mobilnych
- Przedstawienie materiału dowodowego z wykorzystaniem interaktywnych raportów
- Cloud Forensics - mechanizmy zabezpieczania danych z chmury
- Suma kontrolna - czy warto ją robić
- Jak przechowywać dowód elektroniczny
- Zabezpieczanie dysków, poczty elektronicznej, strony internetowej, innych nośników
- Zabezpieczanie informacji ulotnych

Moduł 4 Przekazanie materiału dowodowego - zajęcia praktyczne (ćwiczenia)

- Wykonywane kopii binarnych w środowisku lokalnym
- Wykonywane kopii binarnych w środowisku sieciowym
- Analiza i zabezpieczanie danych z Volume Shadow Copy
- Różnice w analizie koszta systemowego w systemach operacyjnych
- Analiza zawartości pagefile.sys oraz hiberfile
- Analiza zawartości bufora wydruku

Moduł 5 Ukrywanie danych w Alternatywnych strumieniach danych - zajęcia praktyczne (ćwiczenia)

- Wyszukiwanie plików w Alternatywnych strumieniach danych
- Informacje zawarte w listach szybkiego dostępu
- Zabezpieczanie informacji ulotnych - TRIGE
- Analiza Prefetch

Moduł 6 Zabezpieczanie obrazu pamięci RAM - zajęcia praktyczne (ćwiczenia)

- Analiza zawartości pamięci RAM
- Wyszukiwanie plików po sygnaturach czasowych
- Automatyzacja pracy - budowa własnego narzędzia

Moduł 7 Na czym polega logiczna i fizyczna ekstrakcja - zajęcia teoretyczne (wykład)

- Klonowanie kart SIM
- Dlaczego karta SIM po klonowaniu zawiera niekompletne dane
- Logiczna ekstrakcja kart SIM
- Zakładanie nowej sprawy
- Analiza danych

Moduł 8 Tagowanie i zaawansowanie wyszukiwanie informacji - zajęcia teoretyczne (wykład)

- Listy kontrolne
- Filtrowanie danych
- Analiza osi czasu
- Praktyczne analizy urządzeń mobilnych
- Jakie dane można wyodrębnić podczas fizycznej ekstrakcji
- Fizyczna ekstrakcja urządzeń mobilnych

- Praca w programie Physical Phone Analyzer
- Zakładanie nowej sprawy
- Analiza danych
- Analiza systemu plików
- Analiza systemu w kodzie HEX
- Analiza danych z wykorzystaniem wyrażeń regularnych

Moduł 9 Data Carving - zajęcia praktyczne (ćwiczenia)

- Tagowanie i zaawansowane wyszukiwanie informacji
- Listy kontrolne
- Filtrowanie danych
- Analiza osi czasu
- Wyszukiwanie i analiza złośliwego oprogramowania
- Wyszukiwanie artefaktów JailBreak w iPhone
- Pomijanie zabezpieczeń KOD PIN lub „wężyk” w urządzeniach mobilnych
- UFED Reader

Godzinowy harmonogram usługi ma charakter orientacyjny - trener, w zależności od potrzeb uczestników, może zmienić długość poszczególnych modułów (przy zachowaniu łącznego wymiaru 21 godz. lekcyjnych). Podczas szkolenia, w zależności od potrzeb uczestników, będą robione krótkie przerwy. Trener ustali z uczestnikami konkretne godziny przerw

Harmonogram

Liczba przedmiotów/zajęć: 0

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

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 677,70 PLN
Koszt przypadający na 1 uczestnika netto	2 990,00 PLN
Koszt osobogodziny brutto	175,13 PLN
Koszt osobogodziny netto	142,38 PLN

Prowadzący

Liczba prowadzących: 3

1 z 3

Maciej Karmoliński

Absolwent kierunku Zarządzanie na Akademii Ekonomicznej w Katowicach oraz studiów MBA Akademii Leona Koźmińskiego w Warszawie. W branży informatyki śledczej od 12 lat, w tym od 8 lat na stanowiskach kierowniczych. Specjalizuje się w procesach zarządzania bezpieczeństwem informacji. Współtwórca wielu prestiżowych projektów z zakresu bezpieczeństwa IT i informatyki śledczej w kraju i zagranicą. Prowadzący zna teoretyczne aspekty zagadnień i posiada minimum trzyletnie doświadczenie dydaktyczne oraz praktyczne w dziedzinie.

2 z 3

Daniel Suchocki

Doświadczenie zawodowe: Posiada 15-letnie doświadczenie w bezpieczeństwie systemów i sieci informatycznych oraz 9 letnie doświadczenie w informatyce śledczej. Trener IT w autoryzowanym centrum szkoleniowym Dagma od 2017 roku.
Wieloletnie doświadczenie w prowadzeniu szkoleń, wykładów i konsultacji w dziedzinie technik hackingu, informatyki śledczej, technik cyberprzestępczości, przeciwdziałaniu atakom na strony, aplikacje webowe, systemy i rozwiązania chmurowe. Zna teoretyczne aspekty zagadnień i posiada minimum trzyletnie doświadczenie dydaktyczne oraz praktyczne w dziedzinie. Certyfikowany trener CEH.
Wykształcenie wyższe.

3 z 3

Wojciech Chyb

Specjalista do spraw informatyki śledczej – w branży informatyki śledczej działa od 5 lat. Odbył liczne szkolenia zarówno w kraju jak i za granicą, swoją znajomość narzędzi AccessData FTK pogłębiał m.in. na autoryzowanych kursach w Londynie. Specjalizuje się w zabezpieczeniach danych ze szczególnym uwzględnieniem urządzeń mobilnych oraz złożonych, wielowątkowych analizach danych z różnych źródeł. Prowadzący zna teoretyczne aspekty zagadnień i posiada minimum trzyletnie doświadczenie dydaktyczne oraz praktyczne w dziedzinie.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- materiały dydaktyczne w formie elektronicznej (e-book, lub dostęp do materiałów autorskich, przygotowanych przez trenera) przesłane na e-mail uczestnika
- dostęp do przygotowanego środowiska wirtualnego (dane dostępowe przesłane na wskazany przez uczestnika adres e-mail)

Warunki uczestnictwa

Prosimy o zapisanie się na szkolenie przez naszą stronę internetową **www.acsdagma.com.pl** w celu rezerwacji miejsca.

- Laptopy muszą mieć zainstalowany Virtual Box wraz z dodatkami (extension pack) oraz posiadać około 50 GB wolnej przestrzeni dyskowej i minimum 4 GB RAM.

Informacje dodatkowe

Informacje organizacyjne:

- 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 ACS 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 Autoryzowane Centrum Szkoleniowe DAGMA.

Warunki techniczne

WARUNKITECHNICZNE:

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 (czyt. od 30 maja do 1 czerwca)

Szczegóły, związane z prowadzonymi przez nas szkoleniami online, znajdziesz na naszej stronie:
https://www.acsdagma.com/pl/szkolenia-online

Kontakt

Agnieszka Palenga

E-mail palenga.a@dagma.pl

Telefon (+48) 32 7931 139