Szkolenie HoneyINT: OSINT + Honeypoty w praktyce obronnej

Opis szkolenia: HoneyINT to szkolenie, które łączy OSINT i honeypoty w jeden spójny system wczesnego wykrywania aktywności ofensywnej w infrastrukturze IT. Zamiast reagować na incydenty, uczysz się wykrywać rekonesans i próby ataku zanim dojdzie do włamania. To szkolenie o analizie danych, korelacji sygnałów i podejmowaniu decyzji operacyjnych - nie o instalacji narzędzi.

Czas trwania: 15 godzin (5 spotkań x 3 godziny, 18:00 – 21:00)

Kategoria: OSINT, Blue Team

Język wykładowy: język polski

Materiały i narzędzia: w języku polskim

Czym jest szkolenie o HoneyINT?

HoneyINT to moje autorskie podejście do bezpieczeństwa, które łączy OSINT i honeypoty w jeden proces:

- **Honeypoty** – do aktywnego ujawniania intencji atakującego
- **OSINT** – identyfikacja powierzchni ataku
- **Korelacja** – interpretacja intencji

Dopiero ich połączenie pozwala wykryć atak zanim faktycznie nastąpi. Zamiast reagować na incydent, uczysz się **przewidywać ataki, zanim te się zaczną**.

Zamiast omawiać ogólne koncepcje, pracujemy na rzeczywistych scenariuszach:

- jak atakujący zbiera informacje o Twojej infrastrukturze,
- jak wykryć rekonesans, zanim przejdzie w atak,
- jak wykorzystać honeypoty do identyfikacji i profilowania przeciwnika,
- jak interpretować dane i podejmować decyzje operacyjne.

To nie jest kolejne szkolenie o narzędziach. To nie jest szkolenie tylko o tym jak zainstalować honeypota lub narzędzie do białego wywiadu. Takich szkoleń, jak i książek, jest dużo na rynku. Większość takich kursów wykracza tylko delikatnie poza dokumentację. To szkolenie to pójście o kilka kroków dalej: to szkolenie o **interpretacji danych, korelacji sygnałów i podejmowaniu decyzji**.

Dlaczego miód i OSINT?

Od ponad 9 lat jestem współwłaścicielką Pasieki na Roztoczu i z miodem i pułapkami mam do czynienia na co dzień. My zakładamy „pułapki", zwalczając choroby pszczół, wystawiamy stare ule, aby wyłapywać roje pszczele. Pszczoły zakładają pułapki na intruzów i konkurencję.

W praktyce:

- pszczoły nie reagują dopiero na atak – **monitorują otoczenie** cały czas,
- potrafią **rozpoznać intruza**, zanim wyrządzi szkody, w końcu miód jak rzadko który produkt przyciąga intruzów oraz nieproszonych gości
- dla pszczół nie każdy, kto się pojawia, jest zagrożeniem – liczy się **wzorzec zachowania**
- działają na podstawie **zbioru sygnałów**, nie pojedynczych zdarzeń,
- bronią zasobów (miodu) poprzez organizację i **wczesne ostrzeganie**
- najważniejsze dla nich jest wczesne wykrycie intruza, nie późniejsza reakcja

To dokładnie ten sam model, który działa w bezpieczeństwie IT:

- OSINT to odpowiednik obserwacji otoczenia ula,
- honeypoty to kontrolowane „wabiki", które pozwalają wykryć intruza, zanim dotknie właściwych zasobów,
- analiza logów to odpowiednik interpretacji zachowania kolonii.

Dla kogo jest to szkolenie?

Szkolenie jest przeznaczone dla osób, które:

- zarządzają serwerami i infrastrukturą (Linux / Windows / infrastruktura webowa / WordPress / chmura)
- analizują logi
- pracują jako DevSecOps / SysAdmin / specjalista Security
- odpowiadają za bezpieczeństwo aplikacji lub sieci
- chcą przejść z podejścia reaktywnego na wyprzedzające
- chcą zrozumieć realne techniki rekonesansu i wykrywania ataków

Dla kogo NIE jest przeznaczone to szkolenie?

- dla początkujących bez podstaw IT (zakładana jest znajomość podstaw sieci, HTTP oraz pracy z systemami)
- osób szukających tylko checklist i gotowców
- osób oczekujesz szkolenia typu tool-driven learning
- osób liczących na to, że po 15 godzinach szkolenia, bez dodatkowych ćwiczeń, zostaną ekspertami od honeypotów i OSINT

Uczestnicy otrzymają zestaw instrukcji, jak stworzyć środowisko testowe.

Szkolenie kończy się certyfikatem uczestnictwa.

Szczegółowy program szkolenia

Spotkanie 1 – 17 czerwca 2026 – OSINT (recon & attack surface mapping)

Identyfikacja powierzchni ataku i analiza rekonesansu

W tym module dowiesz się, jak realnie wygląda rekonesans widziany „z zewnątrz", jak go wykrywać oraz jak mapować powierzchnię ataku (*attack surface*) organizacji na podstawie danych publicznych.

Zakres:

- identyfikacja subdomen, usług i ekspozycji infrastruktury
- analiza technologii backend / CMS / frameworków
- wykrywanie śladów automatycznego skanowania

Przykładowe narzędzia:

- **amass** – enumeracja subdomen i relacji DNS
- **theHarvester** – email, domeny, metadane
- **Shodan** – ekspozycja usług i portów
- **SpiderFoot** – integruje wiele źródeł (Shodan, WHOIS, DNS, wycieki danych (*leaks*))
- **Recon-ng** – automatyzacja OSINT
- **Photon** – crawler aplikacji web, pasuje pod WordPress + honeypoty HTTP

Efekt dnia:
po tym module będziesz potrafił(a) zbudować mapę powierzchni ataku, która później będzie determinowała rozmieszczenie honeypotów.

Spotkanie 2 – 24 czerwca 2026 – Honeypoty jako kontrolowany wabik (OSINT-driven deception layer)

Projektowanie honeypotów w oparciu o dane OSINT

Ten moduł skupia się na budowie warstwy obserwacyjnej opartej na rzeczywistej powierzchni ataku, a nie losowych usługach.

Zakres:

- typy honeypotów i ich zastosowanie

- gdzie i jak je umieszczać w infrastrukturze
- jak nie ujawnić honeypota
- jakie dane są wartościowe, a jakie są szumem
- wzorce zachowań atakujących
- kiedy użycie honeypota traci sens

Typy honeypotów omawiane na szkoleniu:

- SSH / Telnet honeypoty
- HTTP/HTTPS honeypoty (fake login panels)
- API honeypoty (REST endpoints)
- Honeypoty na WordPressa
- Honeypoty typu credential harvesting traps

Przykładowe narzędzia:

- Cowrie – symulacja SSH i logowanie ataków brute-force
- Dionaea – przechwytywanie exploitów i malware
- Honeytrap - nasłuchuje na portach i loguje próby połączeń
- Wordpot - symuluje WordPressa i zbiera próby logowania i exploitów
- OpenCanary – służy do wczesnego wykrywania intruzów i cyberataków wewnątrz sieci firmowej

Efekt dnia:
po tym module będziesz rozumiał(a), co honeypot realnie wykrywa i potrafił(a) zaprojektować honeypoty na podstawie zebranych danych z OSINT, dopasowanie rozwiązanie do realnych wymagań infrastruktury i minimalizować szum i fałszywie pozytywne sygnały.

Spotkanie 3 – 01 lipca 2026 – WordPress i aplikacje internetowe (real-world attack surface monitoring)

Wykrywanie botów, skanowania i prób exploitacji

Moduł skupia się na jednym z najczęstszych wektorów ataku w internecie: WordPressie, a także na aplikacjach internetowych.

Zakres:

- najczęstsze ataki na WordPress

- honeypoty jako fałszywe punkty wejścia
- wykrywanie brute-force i botów
- analiza prób exploitacji pluginów i wersji CMS (RCE, upload plików, LFI)
- fingerprinting narzędzi atakujących
- których honeypotów na Wordpresie osobiście, a z których zrezygnowałam i dlaczego

Przykładowe narzędzia:

- Wordfence – detekcja i firewall aplikacyjny
- WPScan – analiza podatności WordPress
- Fail2ban – blokowanie brute-force
- ModSecurity – reguły WAF dla HTTP
- Nginx – analiza logów i reverse proxy security

Przykładowe testy honeypotów na WordPressie:

- fałszywe panele logowania /wp-admin
- fałszywe plugin endpoints
- atrapy endpointów REST API i stron uploadu plików

Efekt:
po tym module będziesz potrafił(a) rozpoznać automatyczne skanowanie i oddzielić je od realnego targetowania.

Spotkanie 4 – 08 lipca 2026 – Korelacja danych (OSINT + honeypoty = detekcja)

Łączenie sygnałów i identyfikacja wzorców ataków

Najważniejszy moduł operacyjny.

Zakres:

- przejście od danych do działania
- korelacja IP, user-agentów i fingerprintów
- połączenie OSINT + honeypoty + logi
- identyfikacja botnetów i narzędzi skanujących
- analiza timingów i sekwencji ataków
- budowa reguł detekcji

- priorytetyzacja zagrożeń, co ignorować, co eskalować
- wprowadzenie do automatyzacji reakcji

Przykładowe narzędzia:

- **Elastic Stack (Elasticsearch, Kibana, Logstash)** – korelacja logów
- **Wazuh** – SIEM + HIDS
- **Grafana Loki** – dashboardy metryk
- **Graylog (wersja Open Source)** – scentralizowany system zarządzania logami z wbudowanymi mechanizmami alertów i korelacji
- **Zeek** – analiza ruchu sieciowego

Efekt dnia:
po tym module będziesz potrafił(a) korelować dane z OSINT i honeypotów w celu identyfikacji wzorców ataków, rozróżniać przypadkowy ruch od ukierunkowanej aktywności oraz określać moment wymagający reakcji operacyjnej.

Spotkanie 5 – 15 czerwca 2026 – Q&A (architektura i scenariusze)

Analiza przypadków uczestników i konsultacje architektury

Moduł praktyczny oparty o realne środowiska uczestników.

Zakres:

- dopasowanie wiedzy do Twojego środowiska
- pytania techniczne uczestników
- analiza konkretnych przypadków z podwórka uczestników
- konsultacja architektury i podejścia
- omówienie problemów z wdrożeń

To nie jest „luźna sesja pytań" – to **praktyczna walidacja podejścia HoneyINT w Twoim środowisku**.

Wymagania techniczne przed szkoleniem:

- do udziału w szkoleniu wymagany jest komputer, na którym można uruchomić maszynę wirtualną lub dostęp do serwera VPS, na którym będzie można przygotować środowiska wg instrukcji i zainstalować honeypoty i narzędzia OSINT
- instancja WordPress (testowa)
- dostęp do wygenerowanych przez honeypoty i aplikacje logów (web / systemowych)

Jak pracujemy

- brak instalacji narzędzi podczas zajęć, to spokojnie możesz sama zrobić wcześniej na podstawie instrukcji, które otrzymasz odpowiednio wcześniej
- szkolenie opiera się w większości na narzędziach open-source, aby na proponowane rozwiązania mogły pozwolić sobie nawet nieduże firmy i organizacje
- analizujemy realne logi i scenariusze
- identyfikujemy wzorce ataków
- podejmujemy decyzje na podstawie danych, a nie na podstawie hipotez

To szkolenie to **praca na realnych maszynach i danych, nie na slajdach**.

Czego to szkolenie nie obejmuje

- instalacji narzędzi krok po kroku „na żywo”
- podstaw cyberbezpieczeństwa
- teorii bez zastosowania.

Zasada całego szkolenia:

OSINT definiuje *gdzie patrzeć*

Honeypoty definiują *na co reagować*

Korelacja definiuje *kiedy działać*

HoneyINT to podejście, które pozwala:

- widzieć więcej niż standardowe zabezpieczenia
- rozumieć zachowanie atakującego
- reagować zanim dojdzie do incydentu

Bez uproszczeń.
Bez marketingu.
Tylko dane, logi i decyzje.

Co dostajesz?

- materiały techniczne (checklisty, scenariusze, przykłady logów)
- instrukcje konfiguracji środowiska (do wykonania przed szkoleniem)
- dostęp do nagrań
- sesje Q&A
- certyfikat na zakończenie szkolenia
- dostęp do zamkniętej grupy na Discordzie
- trenerkę, która zawsze ma wiele do przekazania i chętnie dzieli się wiedzą

Dowiedz się więcej: https://honeynint.pl

Kup szkolenie: https://cart.easy.tools/checkout/zalnet/honeyint-osint-honeypoty-w-praktyce-obronnej

ZALNET
Beata Zalewa

+48 600 926 031
info@zalnet.pl
www.zalnet.pl

Wola Radzięcka 62
23-440 Frampol
NIP 717 111 99 64