Mariusz Zapalski

SOC-L1

Lublin, gotowość do relokacji do Warszawy i do pracy zmianowej 24/7
Telefon: +48 727 460 550 | E-mail: m.zapalski990@gmail.com
Portfolio: zapalsky.pl | LinkedIn: linkedin.com/in/mariusz-zapalski-9390a530b
GitHub: github.com/Marioo990 | TryHackMe: tryhackme.com/p/Mario990

PROFIL

Magister informatyki Politechniki Lubelskiej. Od 2022 roku odpowiadam za wsparcie IT w firmie ubezpieczeniowej: przeprowadziłem migrację systemu obsługi klienta, skonfigurowałem VPN, napisałem dokumentację i przeszkoliłem pracowników. Na początku 2026 roku zaliczyłem testy wiedzy technicznej w rekrutacji do Centralnego Biura Zwalczania Cyberprzestępczości. Nie wpasowałem się w profil służb, ale wtedy uznałem, że chcę pracować w SOC, i od tamtej pory uczę się pod tę rolę. Dobrze znam sieci, Windows i Linux. Obszary czysto SOC-owe, czyli SIEM, triage i EDR, dopiero poznaję i piszę o tym wprost. Szukam pierwszej pracy w SOC, w zespole, od którego mogę się uczyć.

UMIEJĘTNOŚCI TECHNICZNE

Sieci: model OSI i TCP/IP, IPv4, subnetting, ARP, DNS, DHCP, NAT, VLAN, routing, TCP i UDP, HTTP, HTTPS, TLS, SMTP, SSH, RDP, porty, proxy, VPN, firewall. Podstawy analizy ruchu w Wireshark.

Windows: procesy, usługi, użytkownicy i uprawnienia, rejestr, zadania zaplanowane, PowerShell. Event Viewer: zdarzenia logowania, tworzenie procesów, mechanizmy persistence. Podstawy Sysmon.

Linux: praca w CLI, system plików, prawa dostępu, użytkownicy, procesy, usługi, pakiety, SSH. Narzędzia grep, awk, sed, find, journalctl. Analiza logów auth i syslog.

Programowanie i narzędzia: Dart i Flutter, HTML, CSS, JavaScript, SQL, Git. Podstawy Pythona oraz skryptowania w Bash i PowerShell.

W TRAKCIE NAUKI (ŚCIEŻKA DO SOC)

Uczę się według rozpisanego planu, praktykuję na TryHackMe i w laboratorium domowym. Postępy dokumentuję publicznie na zapalsky.pl.

Web i poczta: request i response, metody oraz kody HTTP, nagłówki, cookies, sesja. Podstawowe ataki webowe. Analiza nagłówków e-mail, SPF, DKIM, DMARC, ocena adresów URL i załączników.

Fundamenty bezpieczeństwa: triada CIA, ryzyko, podatność i exploit, IOC, IOA, TTP. MITRE ATT&CK, Cyber Kill Chain, Pyramid of Pain. Podstawy malware, least privilege, MFA, patching.

Operacje SOC: triage, severity i priority, ustalanie zakresu i osi czasu, zbieranie materiału dowodowego, eskalacja, obsługa zgłoszeń, playbooki, SLA, chain of custody.

SIEM i dane: wyszukiwanie, agregacja, praca z polami i czasem, korelacja, składnia SPL i KQL, schematy logów, dashboardy, alerty, podstawy parsowania.

EDR i SOAR: drzewo procesów, linia poleceń, hash, kontekst użytkownika, hosta i sieci, containment, podstawowe playbooki.

Chmura: shared responsibility, IAM, VPC i VNet, storage, podstawowe logi audytowe i sieciowe.

DOŚWIADCZENIE ZAWODOWE

Wsparcie IT i doradca, Doradztwo Finansowo-Ubezpieczeniowe, Lublin
2022 do teraz
Migracja systemu obsługi klienta: analiza potrzeb, transfer bazy klientów i polis, konfiguracja VPN, dokumentacja powdrożeniowa.
Szkolenia pracowników z nowego systemu, pierwsza linia wsparcia technicznego w biurze.
Prowadzenie firmowych social mediów, kampanie Meta Ads, materiały graficzne.

Specjalista do spraw social media, Spec-ice (branża przemysłowa)
06.2025 do 06.2026
Prowadzenie profilu firmowego: kalendarz publikacji, treści i grafiki, komunikacja z odbiorcami.

Operator kombajnu i ciągnika, gospodarstwo rolne, praca sezonowa
od 2018
Żniwa pod presją czasu, wielogodzinne zmiany, odpowiedzialność za sprzęt wysokiej wartości.

PROJEKTY

NextDrop, aplikacja mobilna (Flutter, Dart), 10.2025
Śledzenie cyklicznych wydarzeń medialnych. Clean architecture, lokalna baza SQLite z systemem migracji, powiadomienia uwzględniające strefy czasowe, wersja polska i angielska. Architekturę i logikę zaprojektowałem samodzielnie. github.com/Marioo990/NextDrop

zapalsky.pl, portfolio, 08.2026
Strona zaprojektowana i zakodowana samodzielnie: HTML, CSS, JavaScript, animacje canvas i

SVG. Hosting Firebase.

Strony komercyjne dla klientów, 2025 do 2026
zaufany-agent.pl: kalkulatory online z kodami QR, formularz kontaktowy, lokalne SEO.
amtrehab.pl: automatyczny status godzin otwarcia, mapa dojazdu, sekcja opinii.
houseofbeautyms.pl: suwaki porównań przed i po, formularz z walidacją, integracja z Booksy.

WYKSZTAŁCENIE

Magister informatyki, Politechnika Lubelska, 2023 do 2025
Architektura i projektowanie systemów, wzorce projektowe, testowanie i jakość kodu. Samodzielny projekt badawczy w ramach pracy magisterskiej, od koncepcji po działającą aplikację.

Inżynier informatyki, Politechnika Lubelska, 2019 do 2022
Algorytmy i struktury danych, programowanie obiektowe, bazy danych, sieci komputerowe, systemy operacyjne.

Liceum Ogólnokształcące im. Mikołaja Reja w Kraśniku, 2016 do 2019
Profil matematyczno-fizyczno-informatyczny.

DODATKOWE

Rekrutacja do Centralnego Biura Zwalczania Cyberprzestępczości, 01.2026 do 03.2026. Testy wiedzy technicznej z cyberbezpieczeństwa zaliczone.
TryHackMe: regularna praktyka na roomach i ścieżkach blue team, tryhackme.com/p/Mario990

JĘZYKI

Polski: język ojczysty.
Angielski: poziom B2.

ZGODA NA PRZETWARZANIE DANYCH

Wyrażam zgodę na przetwarzanie moich danych osobowych zawartych w niniejszym dokumencie w celu realizacji procesu rekrutacyjnego, zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO).