

JAKUB SKRZYNECKI

Junior Cybersecurity Analyst | SOC Trainee | Blue Team

Rzeszów, Polska

sjakubskrzynecki@gmail.com | +48 662 516 512

LinkedIn: jakub-skrzynecki | Portfolio: jakubsx01.github.io | TryHackMe: CyberhelperJS

PROFIL ZAWODOWY

Ambitny student studiów magisterskich na kierunku Cyberbezpieczeństwo z solidnymi podstawami w zakresie obrony sieci, bezpieczeństwa aplikacji webowych i technologii chmurowych. Praktyczne doświadczenie zdobyte poprzez projekty akademickie i symulacje laboratoryjne (TryHackMe, Home Lab). Biegłość w ocenie podatności (OWASP ZAP, OpenVAS), wdrażaniu IAM (Authentik, Azure AD) oraz podstawach reagowania na incydenty. Pasjonat Blue Teaming, dążący do rozwoju w roli analityka SOC lub inżyniera bezpieczeństwa.

DOŚWIADCZENIE ZAWODOWE

Praktykant IT/Sieć

ELTEL NETWORKS ENERGETYKA S.A.

Lipiec 2023 – Sierpień 2023

Wielka, Polska

- Wsparcie bezpieczeństwa sieci:** Asystowałem przy bezpiecznej konfiguracji infrastruktury sieciowej (routery, switchy, AP), zapewniając zgodność z politykami bezpieczeństwa.
- Zarządzanie zasobami:** Przeprowadziłem inwentaryzację i enumerację zasobów IT, wspierając procesy oceny ryzyka i zarządzania podatnościami.
- Ciągłość działania:** Weryfikowałem systemy UPS i zasilania awaryjnego, gwarantując niezawodność infrastruktury krytycznej.
- Wsparcie techniczne:** Rozwiązywałem problemy sprzętowe i programowe użytkowników końcowych, utrzymując wysoką dostępność stacji roboczych.

KLUCZOWE PROJEKTY

Wdrożenie Identity & Access Management

Authentik, Microsoft Azure, Docker

Projekt Akademicki

- Wdrożenie SSO:** Skonfigurowałem Authentik jako dostawcę tożsamości (IdP) w Azure, umożliwiając Single Sign-On (SSO) dla wielu aplikacji poprzez **OIDC** i **SAML 2.0**.
- Integracja:** Zintegrowałem usługi z Active Directory (LDAP), centralizując zarządzanie użytkownikami dla symulowanej organizacji (3 grupy, 18 użytkowników).
- Wzmocnienie bezpieczeństwa:** Zaimplementowałem MFA i ścisłe polityki dostępu, chroniąc przed nieautoryzowanym dostępem.

Audyt Bezpieczeństwa Aplikacji Webowej (PlantCare)

OWASP ZAP, Burp Suite, Python

Projekt Akademicki

- Ocena podatności:** Przeprowadziłem kompleksowy audyt bezpieczeństwa w oparciu o OWASP Top 10, identyfikując krytyczne luki, w tym **Unrestricted File Upload** i **XSS**.
- Automatyczne skanowanie:** Wykorzystałem OWASP ZAP do skanowania automatycznego oraz GitHub Dependabot do analizy zależności (SCA).
- Remediacja:** Opracowałem szczegółowe raporty naprawcze i naprawiłem zidentyfikowane podatności CVE w kodzie.

Analiza Biometryczna Dynamiki Pisania

Python, Machine Learning, Scikit-learn

Projekt Badawczy

- Uwierzytelnianie behawioralne:** Opracowałem model uczenia maszynowego do uwierzytelniania użytkowników na podstawie wzorców pisania (czas lotu, czas nacisku).
- Detekcja anomalii:** Osiągnąłem wynik **AUC ~0.81** w odróżnianiu użytkowników uprawnionych od intruzów przy użyciu klasyfikatorów Random Forest.
- Zastosowanie:** Zademonstrowałem skuteczność biometrii behawioralnej jako warstwy ciągłego uwierzytelniania.

Bettercap, Wireshark, Snort, ffuf

- **Analiza ruchu:** Symulowałem ataki MitM (ARP Spoofing, DNS Spoofing), aby zrozumieć wektory ataku i sygnatury detekcji.
- **Fuzzing aplikacji:** Przeprowadziłem rozległe testy fuzzingowe przy użyciu **ffuf**, odkrywając ukryte endpointy i pliki konfiguracyjne.
- **Detekcja:** Skonfigurowałem reguły IDS (Snort) do wykrywania i alarmowania o podejrzanych wzorcach sieciowych.

UMIEJĘTNOŚCI TECHNICZNE

Security Operations: SIEM (ELK Stack), Zarządzanie Podatnościami (OpenVAS, Nessus), IDS/IPS (Snort), Honeypots (T-Pot).

Web Security: OWASP Top 10, Burp Suite, OWASP ZAP, Security Headers, koncepcje WAF, Bezpieczeństwo Uploadu Plików.

Sieci: TCP/IP, Model OSI, Wireshark, Nmap, VPN, DNS, DHCP, Routing (podstawy BGP).

Chmura i IAM: Microsoft Azure, Active Directory, Authentik, OIDC, SAML, Docker, Linux (Kali, Ubuntu).

Programowanie: Python (Skrypty, Automatyzacja), SQL, Bash, JavaScript (Podstawy).

JĘZYKI OBCE

- **Angielski:** C1 (Zaawansowany) – Pełna biegłość zawodowa
- **Polski:** Ojczysty

WYKSZTAŁCENIE

Magister Informatyki (Cyberbezpieczeństwo)

Politechnika Rzeszowska

2025 – Obecnie

Specjalizacja: Cyberbezpieczeństwo i Technologie Chmurowe

Inżynier Elektroniki i Telekomunikacji

Politechnika Rzeszowska

2019 – 2025

Specjalizacja: Systemy Telekomunikacyjne

CERTYFIKATY I SZKOLENIA

- **CompTIA Security+** (SY0-701) – *W trakcie/Ukończone*
- **Google Cloud Digital Leader** – Google Cloud Skills Boost
- **Ścieżki TryHackMe:** Pre-Security, Web Fundamentals, Jr. Penetration Tester, SOC Level 1
- **Bezpieczeństwo Sieci** – Certyfikat ukończenia kursu