

AI w praktyce  
Red Teamingu  
i Blue Teamingu



zalnet

# O mnie



Security  
Architect



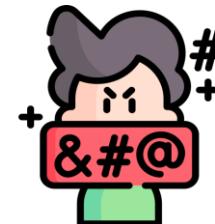
Consultant



Microsoft Certified  
Trainer



AI & Cybersecurity  
Practitioner



Developer



Freelancer



Azure @ ❤️



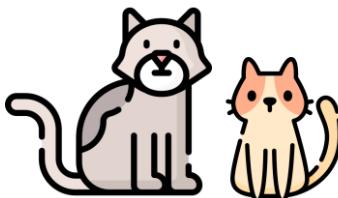
Google Cloud



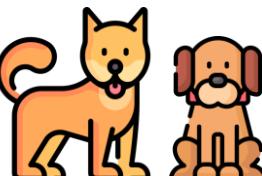
1 Mąż



1 Córka



2 Koty



2 Psy



Kryminały



Fotografia

# Wprowadzenie do Blue Teamingu i sztucznej inteligencji

# Rola Blue Teamu w cyberbezpieczeństwie

## Ochrona infrastruktury IT

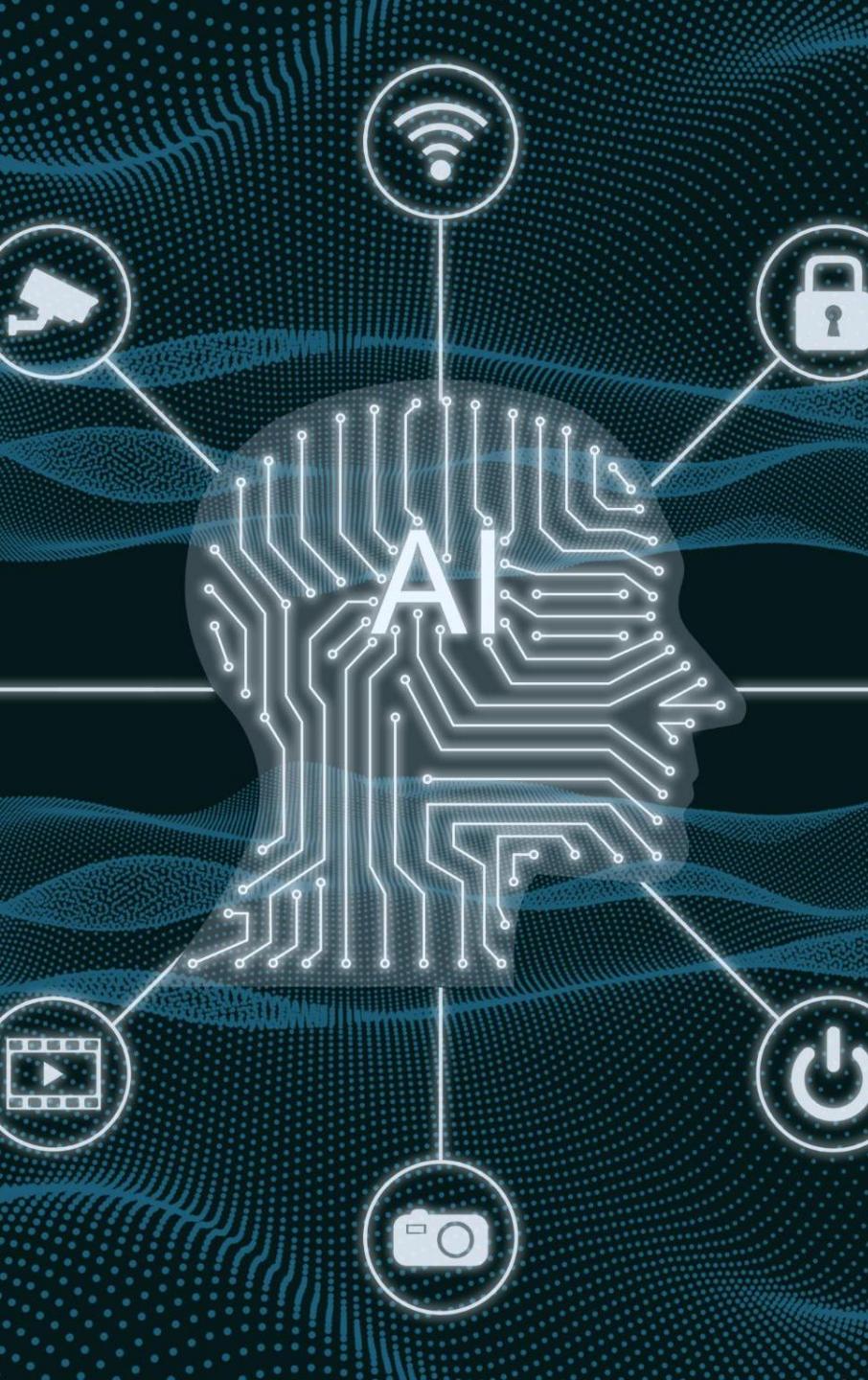
Blue Team odpowiada za ochronę systemów IT, dbając o bezpieczeństwo sieci oraz wszystkich zasobów organizacji. Działa proaktywnie, aby zapobiegać atakom i utrzymać stabilność środowiska informatycznego.

## Monitorowanie zagrożeń

Dzięki ciągłemu monitorowaniu systemów Blue Team szybko wykrywa podejrzane działania oraz potencjalne ataki, co pozwala na natychmiastowe podjęcie odpowiednich działań obronnych.

## Reagowanie na incydenty

Zespół sprawnie reaguje na wszelkie incydenty bezpieczeństwa, ograniczając szkody i zapewniając szybkie przywrócenie normalnego funkcjonowania systemów, co minimalizuje wpływ zagrożeń na działalność organizacji.



# Podstawy sztucznej inteligencji w kontekście bezpieczeństwa

## Uczenie maszynowe

Uczenie maszynowe pozwala systemom na samodzielne uczenie się i doskonalenie w wykrywaniu zagrożeń bez konieczności ręcznego programowania, co zwiększa skuteczność ochrony.

## Analiza danych

Analiza dużych zbiorów danych umożliwia identyfikację wzorców oraz anomalii, które mogą wskazywać na występowanie potencjalnych zagrożeń w środowisku IT.

## Automatyczne wykrywanie zagrożeń

Sztuczna inteligencja automatycznie wykrywa nieprawidłowości i podejrzane zachowania, co znaczco podnosi poziom bezpieczeństwa systemów informatycznych i skraca czas reakcji na ataki.

# Dlaczego AI zmienia praktyki obronne

## Szybsze wykrywanie zagrożeń

Sztuczna inteligencja pozwala na szybkie i precyzyjne wykrywanie zagrożeń, co zmniejsza ryzyko udanych ataków i zwiększa poziom bezpieczeństwa systemów..

## Automatyzacja rutynowych zadań

Dzięki automatyzacji rutynowych czynności zespoły mogą skoncentrować się na bardziej skomplikowanych problemach, co podnosi ich efektywność i skraca czas reakcji.

## Wsparcie w podejmowaniu decyzji

AI dostarcza szczegółowe analizy i rekomendacje, które wspierają zespoły Blue Team w podejmowaniu szybkich i trafnych decyzji podczas reagowania na incydenty bezpieczeństwa.



# Zastosowania AI w wykrywaniu zagrożeń

# Automatyczna analiza logów i anomalie

## Szybkie przetwarzanie logów

Sztuczna inteligencja pozwala na szybkie i efektywne analizowanie dużych ilości danych z logów, co znacznie zwiększa wydajność i dokładność wykrywania zagrożeń.

## Wykrywanie nietypowych wzorców

AI skutecznie identyfikuje nietypowe wzorce i anomalie, które mogą sygnalizować obecność potencjalnych zagrożeń w systemie.

## Zapobieganie zagrożeniom bezpieczeństwa

Dzięki wykrywaniu anomalii możliwe jest szybkie reagowanie na próby ataku lub naruszenia bezpieczeństwa, co pomaga zapobiegać poważnym incydentom.

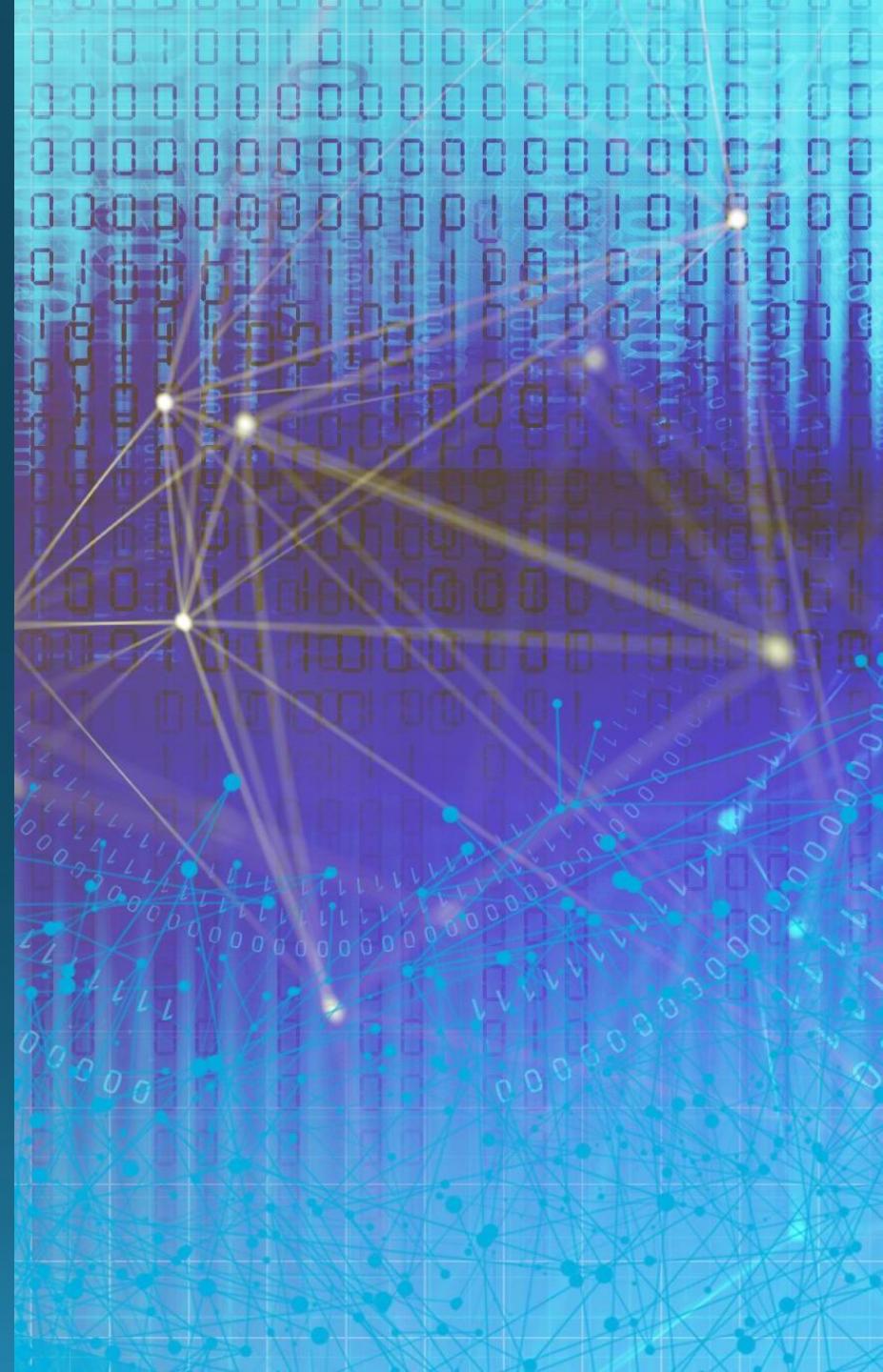
# Wykorzystanie uczenia maszynowego w identyfikacji ataków

## Modelowanie ataków

Uczenie maszynowe umożliwia tworzenie modeli, które rozpoznają różne typy ataków na podstawie analizy danych historycznych, co pozwala lepiej przewidywać zagrożenia.

## Skuteczność wykrywania

Dzięki tym modelom wykrywanie zagrożeń staje się szybsze i bardziej precyzyjne, co zwiększa efektywność ochrony systemów w czasie rzeczywistym.



# Systemy wczesnego ostrzegania o incydentach

## Sztuczna inteligencja w monitoringu

Systemy wykorzystują AI do ciągłej analizy i monitorowania środowiska IT w czasie rzeczywistym, co zwiększa skuteczność wykrywania zagrożeń.

## Natychmiastowe alerty bezpieczeństwa

Dzięki AI system natychmiast informuje zespół Blue Team o potencjalnych zagrożeniach, umożliwiając szybką reakcję.

## Szybka reakcja na zagrożenia

Wczesne ostrzeżenia pozwalają na natychmiastowe przeciwdziałanie incydentom, minimalizując ryzyko poważnych skutków ataków.



AI w monitoringu i  
reagowaniu na  
incydenty

# Inteligentne systemy monitoringu sieciowego

## Analiza ruchu sieciowego

AI umożliwia monitorowanie i analizowanie ruchu sieciowego w czasie rzeczywistym, co pozwala na szybką identyfikację i reakcję na zagrożenia.

## Wykrywanie podejrzanych zachowań

Systemy oparte na AI wykrywają anomalie i potencjalnie niebezpieczne działania w sieci, co zwiększa poziom bezpieczeństwa.

## Zwiększoną skuteczność monitoringu

Dzięki zastosowaniu AI monitoring sieci jest bardziej precyzyjny i efektywny, co minimalizuje ryzyko nieautoryzowanych działań i naruszeń.

# Automatyzacja procesu triage incydentów

## Szybsza klasyfikacja incydentów

AI przyspiesza proces klasyfikowania incydentów, co pozwala na szybką identyfikację i ocenę zagrożeń.

## Precyjna priorytetyzacja zagrożeń

Sztuczna inteligencja precyjnie ustala priorytety incydentów, umożliwiając skupienie się na najpoważniejszych zagrożeniach.

## Wsparcie zespołów bezpieczeństwa

Automatyzacja wspiera zespoły bezpieczeństwa, pozwalając im skoncentrować się na kluczowych zadaniach i skuteczniej reagować na incydenty.





# Wsparcie AI w podejmowaniu decyzji podczas incydentu

## Rekomendacje AI dla ekspertów

Systemy AI generują precyzyjne rekomendacje, które wspierają ekspertów Blue Teamu w podejmowaniu trafnych decyzji podczas obsługi incydentów bezpieczeństwa.

## Analizy wspierające reakcję

Dzięki szybkim i dokładnym analizom AI pomaga zespołom efektywnie reagować na incydenty, zmniejszając ryzyko popełnienia błędów i ograniczając potencjalne szkody.

# Wyzwania i przyszłość AI w Blue Teamingu

# Ograniczenia i zagrożenia wynikające ze stosowania AI

## Fałszywe alarmy AI

Sztuczna inteligencja czasami generuje błędne lub fałszywe ostrzeżenia, co może powodować niepotrzebne działania i nieefektywne wykorzystanie zasobów.

## Podatność na manipulacje

Systemy AI mogą być narażone na ataki i manipulacje, co zagraża ich dokładności oraz bezpieczeństwu całej infrastruktury.

## Wysokie wymagania zasobów

AI wymaga dużej ilości danych i sporej mocy obliczeniowej, co może ograniczać możliwość jej efektywnego wdrożenia, zwłaszcza w mniejszych organizacjach.

# Integracja AI z istniejącymi narzędziami i zespołami

## Integracja z narzędziami bezpieczeństwa

Sztuczna inteligencja powinna bezproblemowo współpracować z istniejącymi narzędziami bezpieczeństwa, aby maksymalnie zwiększyć skuteczność ochrony i ułatwić zarządzanie ryzykiem.

## Szkolenie zespołów

Odpowiednie szkolenia zespołów są niezbędne, by wykorzystać pełen potencjał AI, zapewniając, że stanie się ona realnym wsparciem w codziennej pracy, a nie dodatkowymi utrudnieniami.





# Możliwe trendy rozwojowe i możliwości

## Autonomiczne systemy obronne

Sztuczna inteligencja napędza rozwój autonomicznych systemów obronnych, które samodzielnie wykrywają i neutralizują zagrożenia, zwiększając szybkość i skuteczność ochrony.

## Analiza behawioralna

Głębsza integracja AI z analizą behawioralną umożliwia precyzyjne wykrywanie anomalii i podejrzanych działań w sieci, co pomaga wcześnie identyfikować nietypowe wzorce zachowań.

## Prognozowanie zagrożeń

AI pozwala prognozować przyszłe zagrożenia, co umożliwia organizacjom proaktywne przeciwdziałanie atakom i zwiększa odporność na nowe formy cyberzagrożeń.

# Przegląd aplikacji

# Blueteam.AI od ChatGPT

https://chatgpt.com/g/g-Ewq6VIJ7b-blueteam-ai

Blueteam.AI 5

Upgrade your plan

New chat

Search chats

Library

Sora

GPTs

Blueteam.AI

DORA Regulation AI

Projects NEW

Chats

Beata Zalewa Free

Blueteam.AI

By Ryan Gao

Cyber Security Analyst, Specialized in Threat Intels and Attack Analysis.

"Hey Mr. Blue, analyze this cyber threat scenario:"

"Hey Mr. Blue, provide a visual analysis of this..."

"Hey Mr. Blue, what are the best practices for this..."

"Hey Mr. Blue, correlate this incident with..."

+ Ask anything

# Scrut

[https://marketing.scrut.io/landing-page/soc\\_2\\_compliance](https://marketing.scrut.io/landing-page/soc_2_compliance)



Schedule a Demo

# Get SOC 2 compliant in < 6 weeks

Strengthen your SOC 2 security compliance posture with pre-built controls and 24/7 compliance monitoring

- ✓ 75+ integrations for evidence collection
- ✓ Reduce SOC 2 audit efforts by 70%

## See Scrut in action

First name\*

Last name\*

Business email\*

Phone number\*

Company name

Headquarters Country



Company size\*

### What frameworks do you need

ISO 27001

SOC 2

GDPR

HIPAA

PCI DSS

Others

Hello! Welcome to Scrut Automation, and thanks for visiting. How can I help you today?



# ai-soc-automation

<https://github.com/ai-soc-automation/>

The screenshot shows the GitHub organization page for 'ai-soc-automation'. At the top, there's a navigation bar with links for Platform, Solutions, Resources, Open Source, Enterprise, Pricing, and a search bar. To the right are 'Sign in' and 'Sign up' buttons. Below the header is the organization's logo, a blue-toned image of a futuristic control room with multiple screens. The main navigation menu includes Overview, Repositories (6), Projects, Packages, and People. The 'Overview' tab is currently selected. On the left, the README.md file is displayed, featuring a lock icon and the title 'AI-SOC-Automation'. It also lists 'Advancing AI-Driven Security Operations' and 'Where Cybersecurity meets LLMs, Automation, and Open Research'. Below this is a section titled 'About the Organization' with a pin icon. The right sidebar shows a 'People' section stating 'This organization has no public members. You must be a member to see who's a part of this organization.' and a 'Top languages' section showing 'HTML' and 'Jupyter Notebook'.

https://github.com/ai-soc-automation/

Platform Solutions Resources Open Source Enterprise Pricing

Search or jump to... / Sign in Sign up

ai-soc-automation

Overview Repositories 6 Projects Packages People

README.md

## AI-SOC-Automation

Advancing AI-Driven Security Operations  
Where Cybersecurity meets LLMs, Automation, and Open Research

### About the Organization

AI-SOC-Automation is an open research and development initiative focused on designing intelligent agents for Security Operations Centers (SOCs) using Large Language Models (LLMs), data-centric pipelines, and automation tools.

People

This organization has no public members. You must be a member to see who's a part of this organization.

Top languages

HTML Jupyter Notebook

# Unveiling LLM-SOC-Agent

<https://elbazhazem.github.io/projects/>

The screenshot shows a web browser displaying a personal website. The URL in the address bar is <https://elbazhazem.github.io/projects/>. The page header includes a lock icon, the URL, and various browser controls like A, star, and profile. Below the header, the navigation menu has items: HOME, ABOUT, PROJECTS (which is highlighted in orange), BLOGS, PUBLICATIONS, and SUPERVISION. The main content area is titled "Projects" and "My Active Projects". It lists three projects: "AI-Driven SOC Automation" (with a folder icon), "Log Analyzer LLM" (with a magnifying glass icon), and "Anomaly Detection from Logs" (with a bar chart icon). Each project entry includes a bulleted list of details.

## Projects

### My Active Projects

- AI-Driven SOC Automation**
  - Goal: Research, projects, and public work documenting my specialization in LLM-driven security automation.
  - Details: [Visit the project page](#)
  - Repo: [ai-soc-automation](#)
- Log Analyzer LLM**
  - Goal: Analyze `.log` files using LLMs (ChatGPT/OpenAI APIs).
  - Repo: [log-analyzer-LLM](#)
- Anomaly Detection from Logs**
  - Goal: Accurately classify normal vs. anomalous traffic in network logs.
  - Repo: [log-anomaly-detection](#)

# Podsumowanie i pytania

## Rola AI w obronie cyberszybkiej

Sztuczna inteligencja jest kluczowa dla nowoczesnej ochrony, umożliwiając szybkie wykrywanie zagrożeń.

## Wsparcie zespołów Blue Team

AI pomaga zespołom reagować efektywnie na zagrożenia, zwiększając skuteczność ochrony.

## Wyzwania i przyszłość AI

Świadome podejście do wyzwań pozwoli na dalsze innowacje i wzmacnianie bezpieczeństwa.

Stale poszukuję nowych możliwości i ekscytujących wyzwań. Jeśli chcesz się ze mną skontaktować, proszę, skorzystaj z poniższych kanałów:

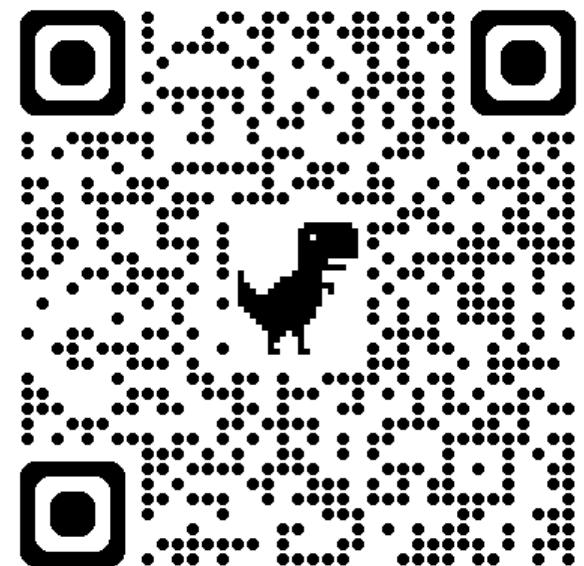
Email: [info@zalnet.pl](mailto:info@zalnet.pl)

LinkedIn: <https://www.linkedin.com/in/beatazalewa/>

Blog: <https://zalnet.pl/blog/>

X: <https://x.com/beatazalewa>

GitHub: <https://github.com/beatazalewa/Conferences/>



# Ciekawe artykuły

- [BlueTeamGPT: The AI Defender Every Security Team Needs | by Ekene Joseph | Medium](#)
- [SOC 3.0 - The Evolution of the SOC and How AI is Empowering Human Talent](#)
- [AI SOC, Explained: Definition, Use Cases & Benefits | Torq](#)
- [What is AI-Native SOC? | CrowdStrike](#)
- [Top 5 AI SOC Analyst Platforms to Watch out for in 2025 - IT Security Guru](#)
- [Boost SOC automation with AI: Speed up incident triage with Security Copilot and Microsoft Sentinel | Microsoft Community Hub](#)