

Blue Team dla zielonych

OD CZEGO ZACZAĆ I JAK
ZAPLANOWAĆ NAUKĘ?

Beata Zalewa, Not The Hidden Knowledge, 07.01.2025

0 mnie



Security Architect



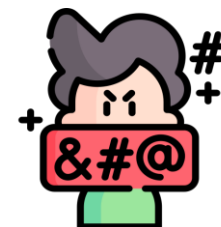
Consultant



Microsoft Certified Trainer



AI & Cybersecurity Practitioner



Developer



Freelancer



Azure @ ❤️



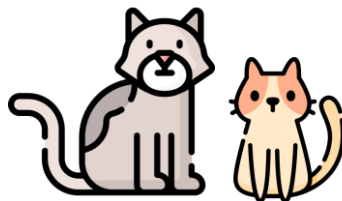
Google Cloud



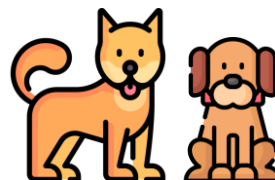
1 Mąż



1 Córka



2 Koty



2 Psy



Kryminały



Fotografia

Agenda

Wprowadzenie do tematyki Blue Team

Czym jest Blue Team i jakie ma zadania

Narzędzia Microsoft używane przez Blue Team

Codzienna praca analityków SOC

Praktyczne scenariusze i demonstracje

Wprowadzenie do Blue Team

- Rola Blue Team w organizacjach
- Produkty Microsoft dla Cyberbezpieczeństwa
 - Microsoft Defender for Endpoint
 - Microsoft Sentinel
 - Microsoft Entra ID
 - Microsoft Intune



Czym jest Blue Team i jakie ma zadania

- Ochrona organizacji przed cyberzagrożeniami:
 - Zabezpieczanie dostępu do usługi wewnątrz firmy
 - Utrzymywanie aktualności systemów i edukacja z zakresu bezpiecznego korzystania z nich
 - Monitorowanie incydentów bezpieczeństwa
 - Reagowanie na incydenty bezpieczeństwa



Narzędzia Microsoft używane przez Blue Teams

Microsoft Defender XDR

- Rodzina produktów do ochrony przed zagrożeniami

Microsoft Sentinel

- Tworzenie instancji do monitorowania i analizy zagrożeń

Microsoft Intune

- Zarządzanie urządzeniami i aplikacjami

Microsoft Entra ID

- Identyfikacja i zarządzanie dostępami

Microsoft Defender XDR

- Microsoft Defender XDR to ujednolicony pakiet ochrony przed i po naruszeniu zabezpieczeń przedsiębiorstwa, który natywnie koordynuje wykrywanie, zapobieganie, badanie i reagowanie między punktami końcowymi, tożsamościami, pocztą e-mail i aplikacjami w celu zapewnienia zintegrowanej ochrony przed zaawansowanymi atakami.
- Microsoft Defender XDR pomaga zespołom ds. zabezpieczeń chronić i wykrywać swoje organizacje przy użyciu informacji z innych produktów zabezpieczających firmy Microsoft.

Źródło: <https://learn.microsoft.com/pl-pl/defender-xdr/microsoft-365-defender>

Microsoft Defender XDR

- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps
- Microsoft Defender Vulnerability Management
- Microsoft Defender for Cloud
- Microsoft Entra ID Protection
- Microsoft Data Loss Prevention
- App Governance

Źródło: <https://learn.microsoft.com/pl-pl/defender-xdr/microsoft-365-defender>

Codzienna praca analityków SOC

Codziennie obowiązki analityków SOC

- Monitorowanie systemów bezpieczeństwa
- Analiza incydentów bezpieczeństwa

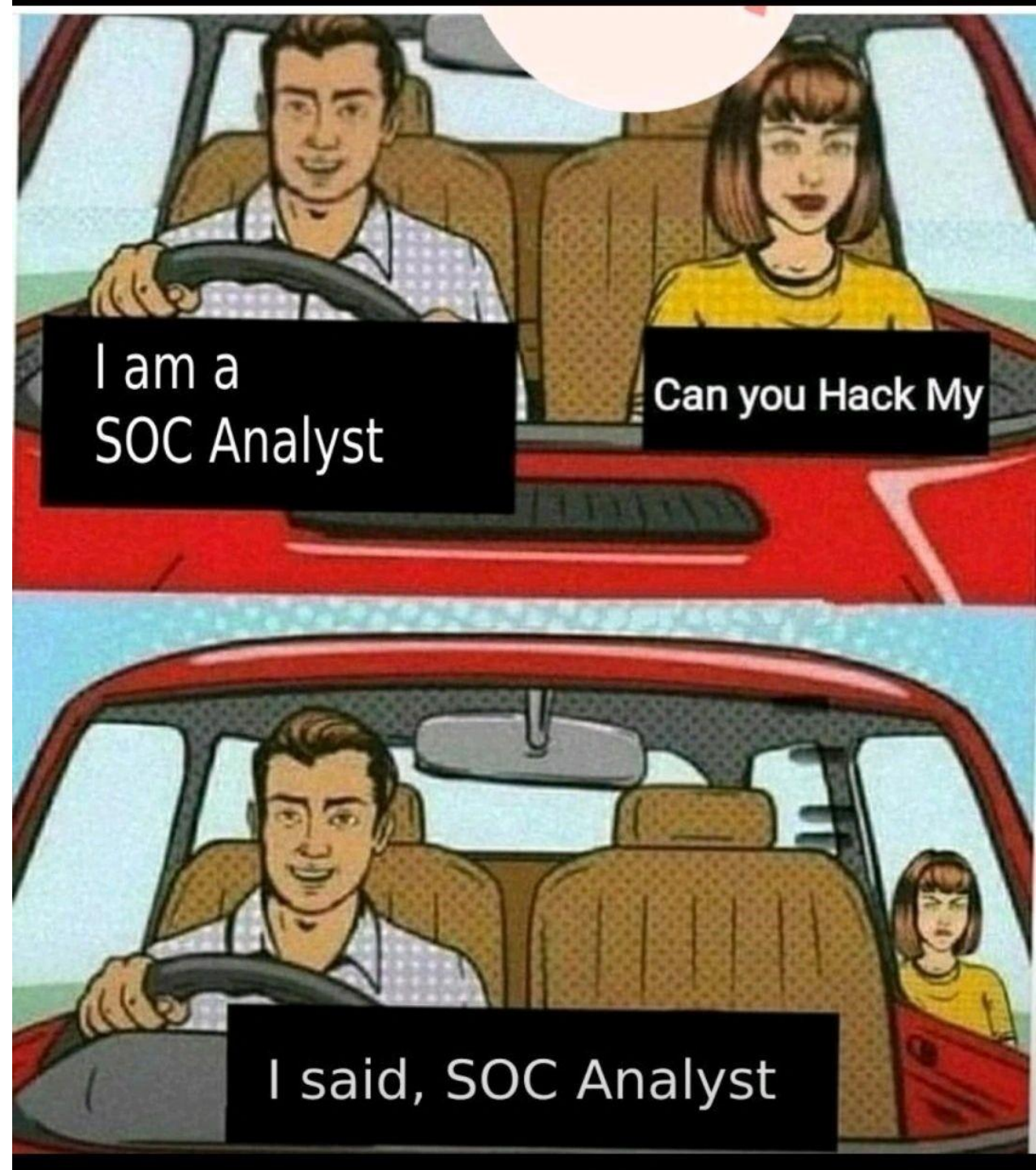
Wymagane umiejętności

- Znajomość narzędzi bezpieczeństwa
- Umiejętność analizy danych

Przyszłe perspektywy

- Rozwój w dziedzinie cyberbezpieczeństwa
- Możliwości awansu

Umiejętności analitików SOC



Haker vs Analytyk



ONE OF THE FUNNIEST THINGS IN OUR OFFICE IS WATCHING IN REAL TIME SOME RANDOM "HACKER" TRY TO USE SQL INJECTION ON A HONEYPOT IN OUR PRODUCT

Umiejętności analityków SOC

WHAT MAKES AN AMAZING SOC ANALYST?

HERE ARE THE SKILLS THEY NEED TO EXCEL

TECHNICAL SKILLS:

- Programming
- Threat hunting
- DFIR (Digital Forensics and Incident Response)
- Cloud security expertise
- SIEM (Security Information and Event Management) operations
- Log analysis
- Network traffic analysis
- Incident handling and documentation
- Hacking (or the ability to think like an attacker)

SOFT SKILLS:

- Think outside the box
- Communication and collaboration
- Risk management
- Work under pressure

SOC Automation Capability Matrix

<https://tinyurl.com/3hxsfz3v>

Automation Capability Matrix

 Hide description

SOC Automation Capability Matrix

The Automation Capability Matrix describes common activities which most security operations centers perform.

 List View  Matrix View

Alert Handling 6

■ Phishing Alerts and Reports

1005

■ Endpoint Alerts

1002

■ SIEM Alerts

1003

■ Cloud Alerts

1004

■ IAM Alerts

1001

■ Bespoke Alerts

Issue Tracking 10

■ Tracking Location

2001

■ Handle Dates

2002

■ Standard Issue Format

2003

■ Set Custom Fields

2004

■ Issue Deduplication

2005

■ Related Issues

SOC Analyst Learning Path

<https://app.letsdefend.io/path/soc-analyst-learning-path>

Learn > Paths



Path

SOC Analyst Learning Path

Learn the technical skills necessary for a career in the Security Operations Center (SOC).

Start This Path Today →

Security Analyst

1

SOC Fundamentals

9 Lesson, 11 Question, 1 Quiz

View →

2

Cyber Kill Chain

9 Lesson, 13 Question, 1 Quiz

View →

3

MITRE ATT&CK Framework

8 Lesson, 19 Question, 1 Quiz

View →

4

Phishing Email Analysis

7 Lesson, 11 Question, 1 Challenge, 1 Quiz, 4 Alert

View →

Certyfikacja

- AZ-900 Microsoft Certified: Azure Fundamentals
 - <https://learn.microsoft.com/en-us/credentials/certifications/azure-fundamentals/?practice-assessment-type=certification>
 - <https://learn.microsoft.com/en-us/training/courses/az-900t00>
- SC-900 Microsoft Certified: Security, Compliance, and Identity Fundamentals
 - <https://learn.microsoft.com/en-us/credentials/certifications/security-compliance-and-identity-fundamentals/?practice-assessment-type=certification>
 - <https://learn.microsoft.com/en-us/training/courses/sc-900t00>

Praktyczne scenariusze i demonstracje

Wykrywanie i reagowanie na zagrożenia

Użycie Microsoft Defender

Analiza incydentów

Wykorzystanie Microsoft Sentinel

Reakcje Blue Teams

Reakcje na przykładowe ataki

Inne praktyczne scenariusze

Demo niespodzianka

AI w służbie Security



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

Email: beata@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/>

