Blue Team dla zielonych

OD CZEGO ZACZĄĆ I JAK ZAPLANOWAĆ NAUKĘ?

Beata Zalewa

Not The Hidden Knowledge. 07.01.2025

Agenda

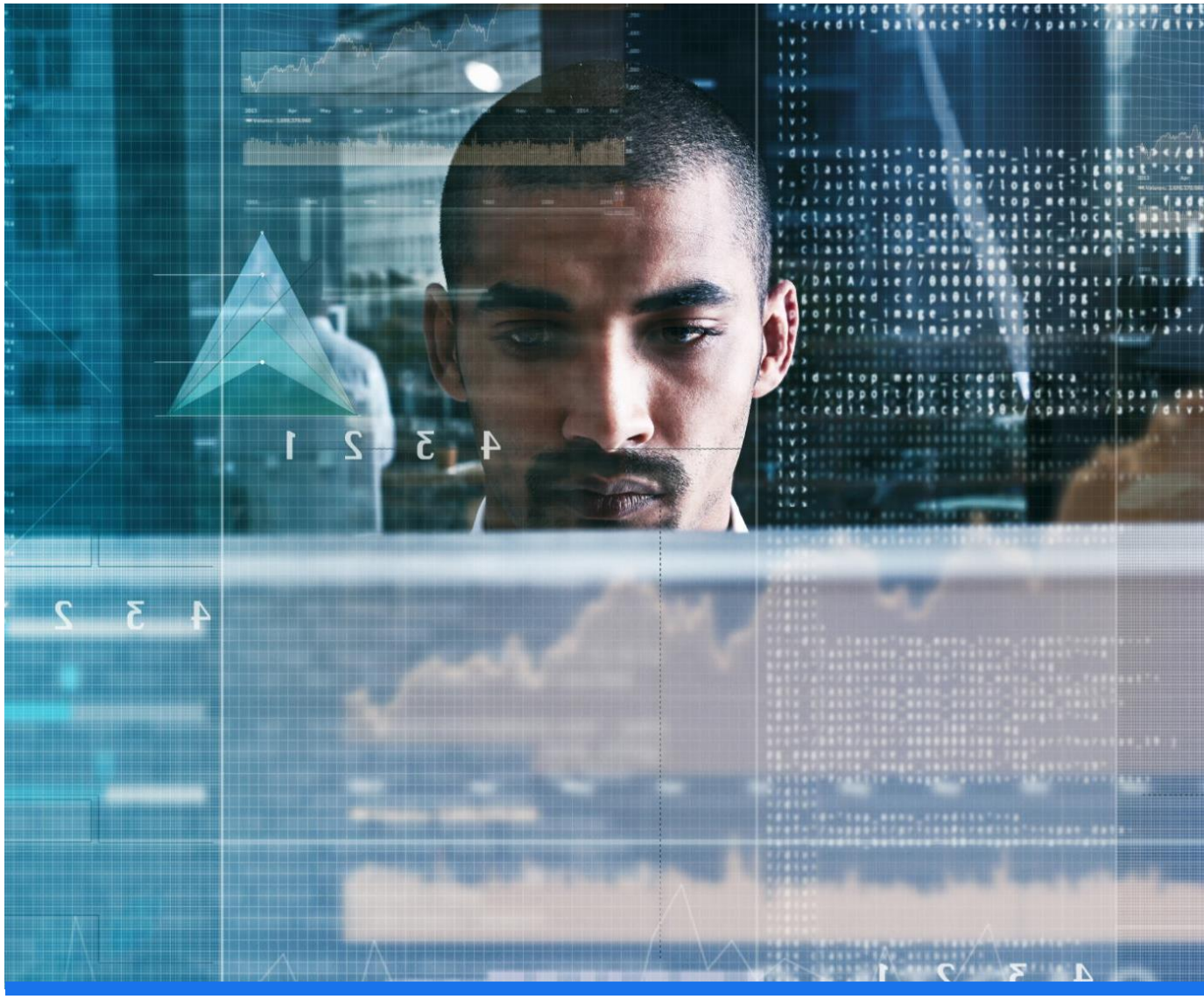
- Wprowadzenie do tematyki Blue Team
- Czym jest Blue Team i jakie ma zadania
- Narzędzia Microsoft używane przez Blue Team
- Codzienna praca analityków SOC
- Praktyczne scenariusze i demonstracje

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

Codzienne obowiązki analityków SOC

- Monitorowanie systemów bezpieczeństwa
- Analiza incydentów bezpieczeństwa

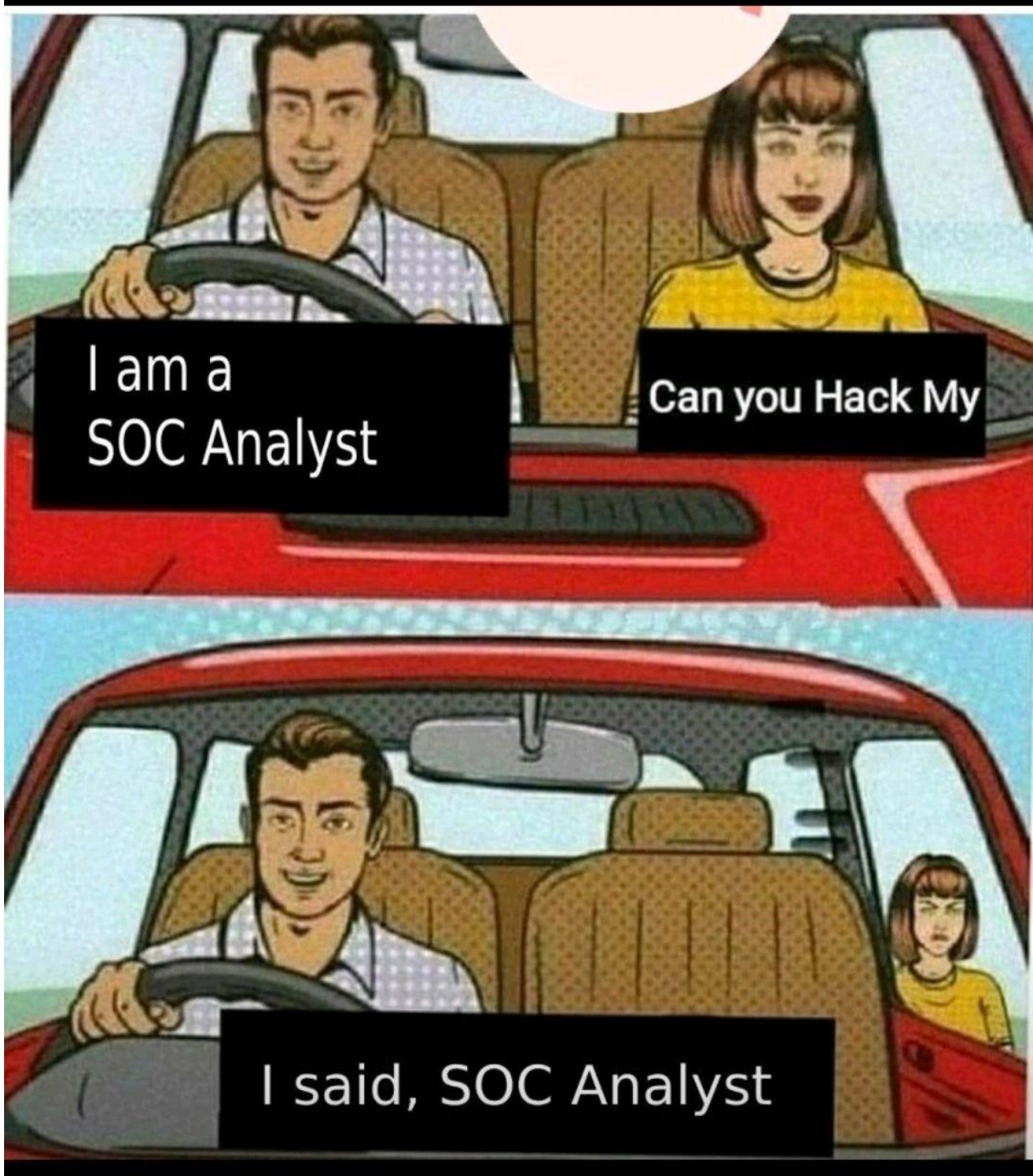
Wymagane umiejętności

- Znajomość narzędzi bezpieczeństwa
- Umiejętność analizy danych

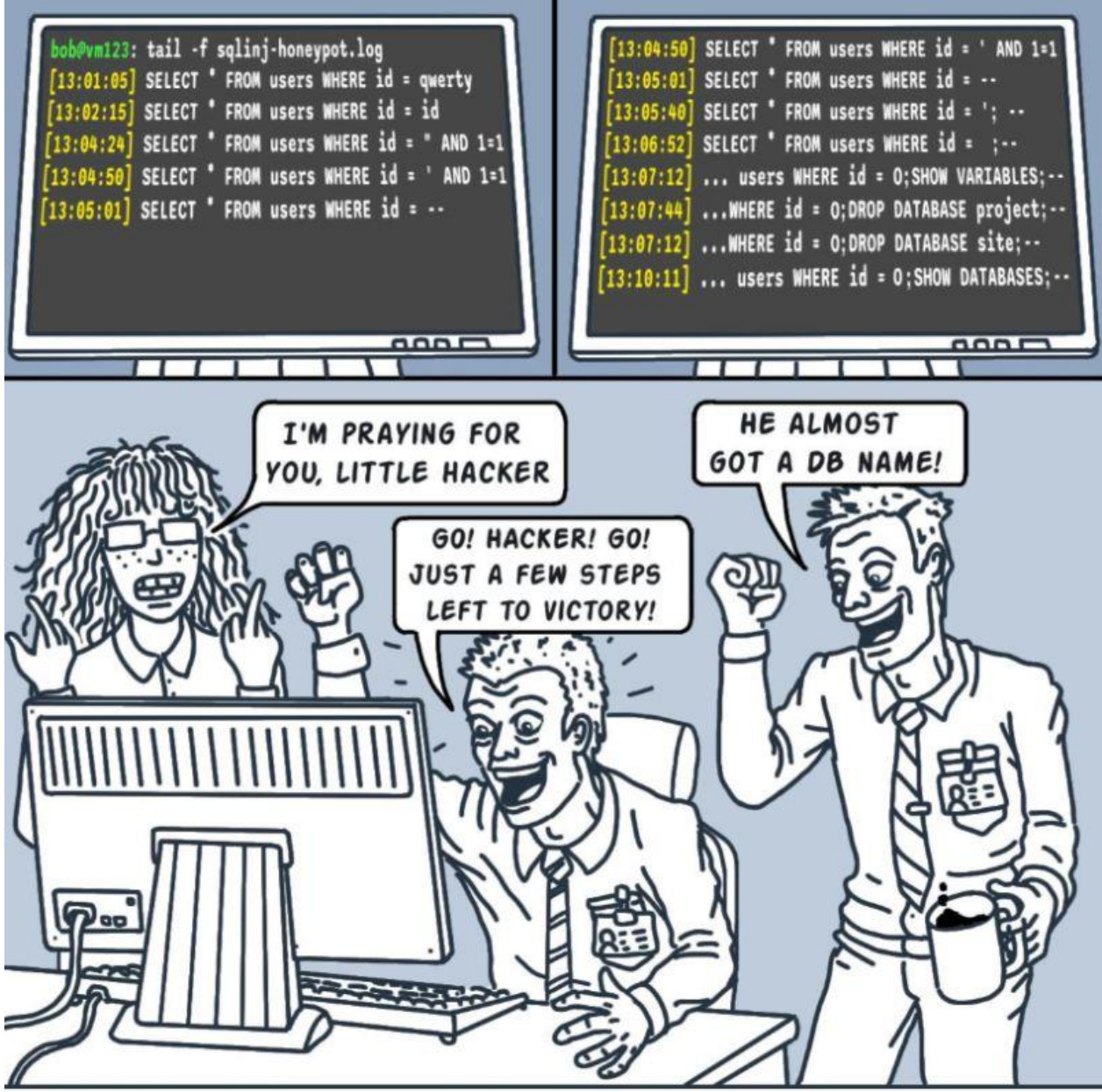
Przyszłe perspektywy

- Rozwój w dziedzinie cyberbezpieczeństwa
- Możliwości awansu

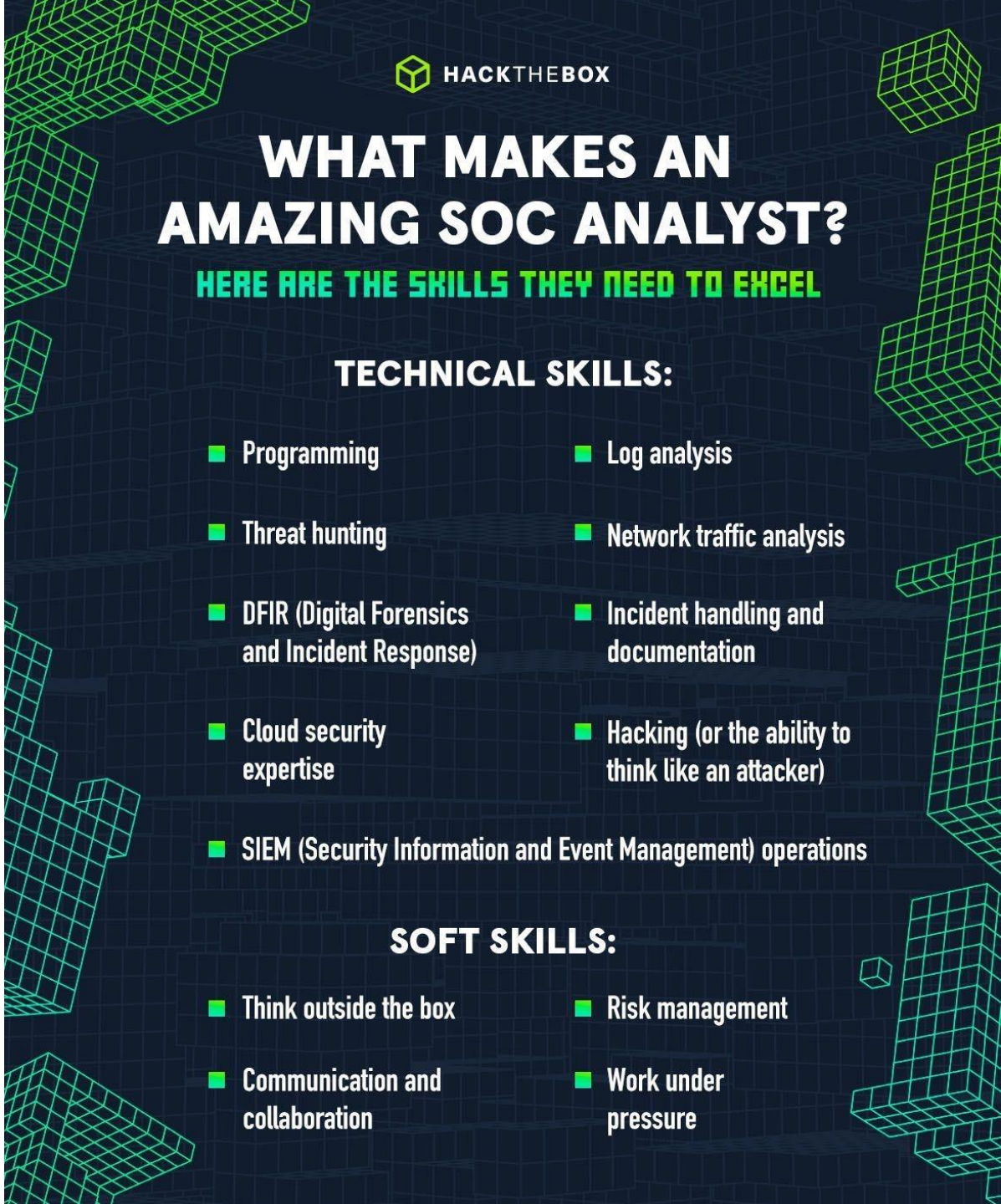
Umiejętności analityków SOC



Haker vs Analityk

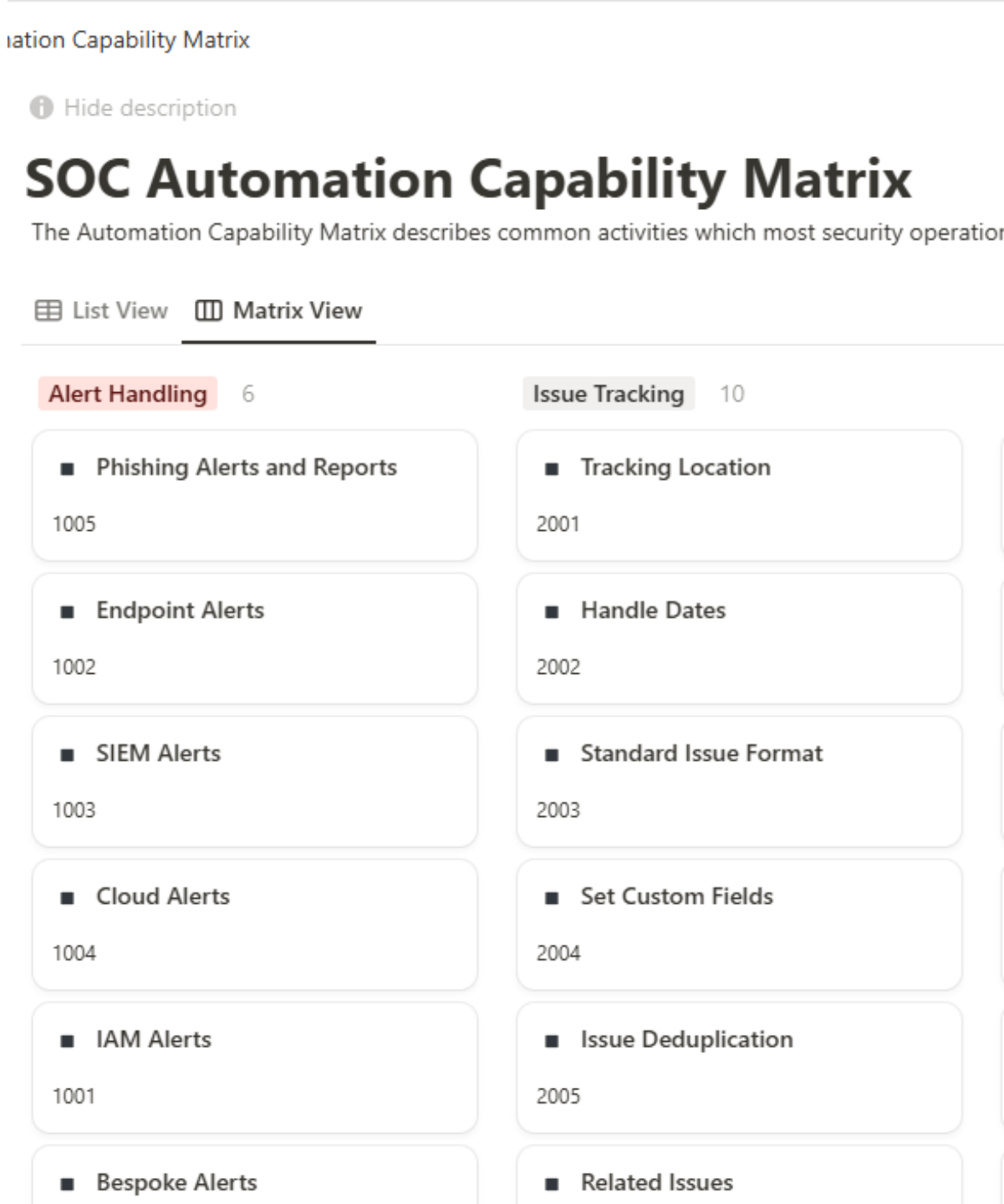


Umiejętności analityków SOC



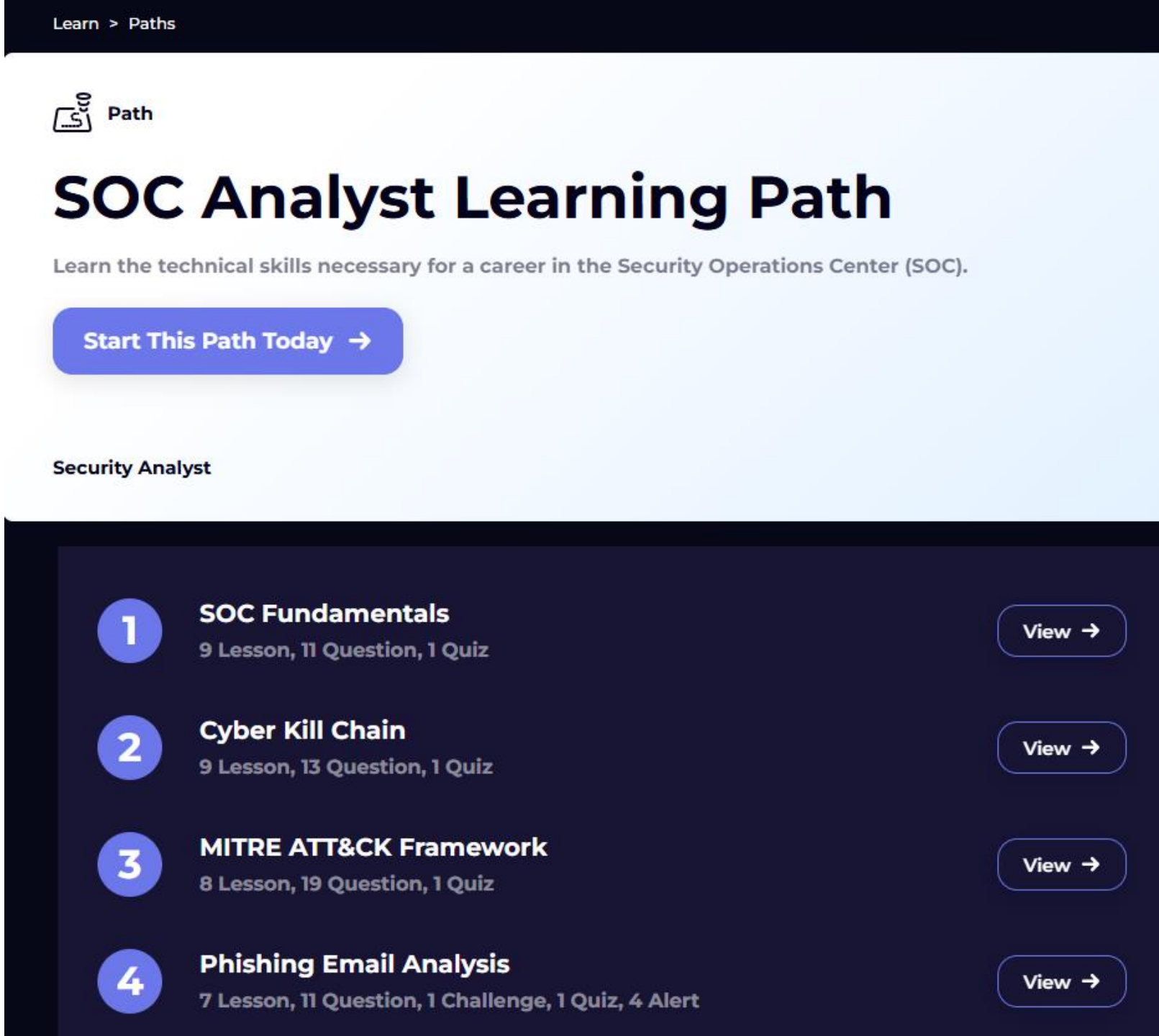
SOC Automation Capability Matrix

https://tinyurl.com/3hxsfz3v



SOC Analyst Learning Path

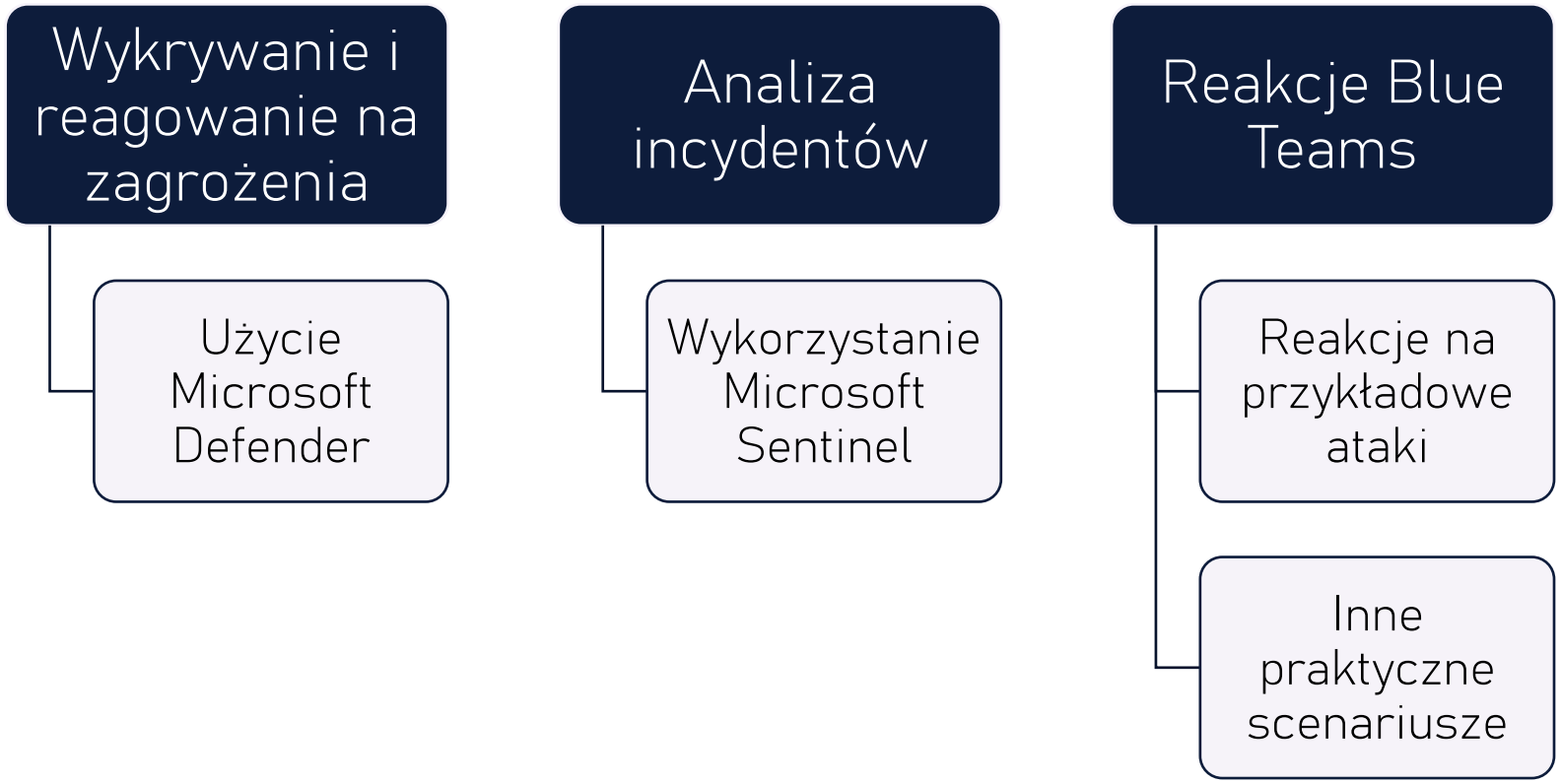
https://app.letsdefend.io/path/soc-analyst-learning-path



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



Demo niespodzianka

AI w służbie Security