

Noworoczne postanowienia dla przyszłych Analityków SOC

PRZYGOTOWANIE DO
KARIERY W
CYBERBEZPIECZEŃSTWIE



0 mnie



Security Architect



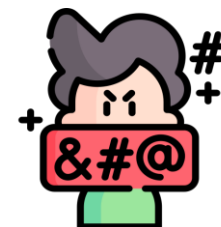
Consultant



Microsoft Certified Trainer



AI & Cybersecurity Practitioner



Developer



Freelancer



Azure @ ❤️



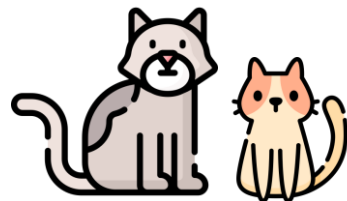
Google Cloud



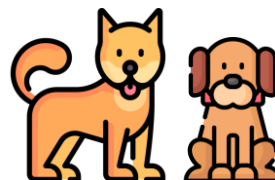
1 Mąż



1 Córka



2 Koty



2 Psy



Kryminały



Fotografia

Dziękuję



Krystian Kaczmarek

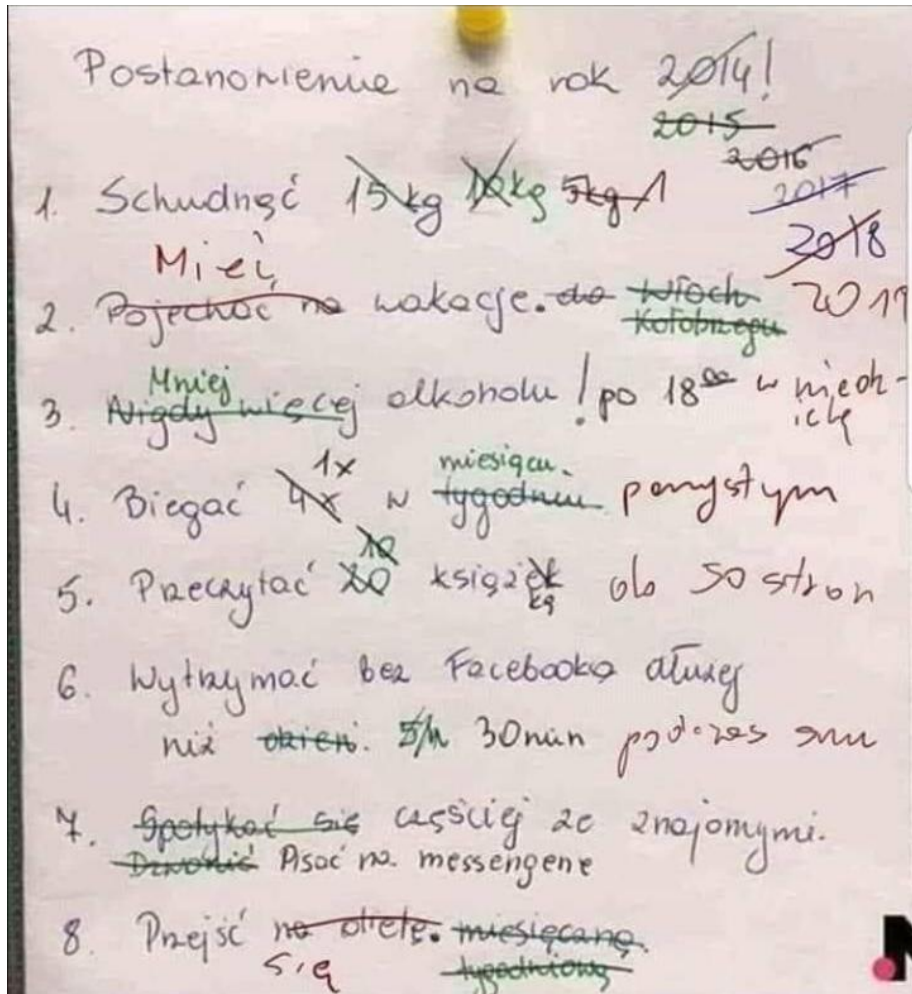


Michał Błaszczak



Wprowadzenie





Znaczenie postanowień noworocznych

Wyznaczanie nowych celów

Postanowienia noworoczne pomagają w wyznaczaniu nowych, ambitnych celów zarówno w życiu osobistym, jak i zawodowym.

Motywacja do działania

Postanowienia noworoczne są doskonałym źródłem motywacji, które może pchnąć nas do działania i dążenia do lepszej wersji siebie.

Rozwój osobisty i zawodowy

Postanowienia noworoczne wspierają świadome podejście do rozwoju osobistego i zawodowego, umożliwiając nam ciągłe doskonalenie.

Postanowienie 1 - Zdobycie certyfikacji



Znaczenie certyfikacji

Rola certyfikatów

- Budują wiarygodność.
- Potwierdzają umiejętności.
- Systematyzują wiedzę.

Znaczenie dla analityków SOC

Certyfikaty są kluczowe dla analityków SOC, ponieważ potwierdzają ich umiejętności i wiedzę w dziedzinie cyberbezpieczeństwa.



Przykładowe certyfikaty: CompTIA Security+, CISSP, CEH

Certyfikat CompTIA Security+

CompTIA Security+ to podstawowy certyfikat w dziedzinie bezpieczeństwa IT, uznawany przez wielu pracodawców w branży.

Certyfikat CISSP

CISSP to zaawansowany certyfikat, który potwierdza umiejętności w zakresie bezpieczeństwa informacji i zarządzania ryzykiem.

Certyfikat CEH

CEH, czyli Certified Ethical Hacker, potwierdza umiejętności z zakresu etycznego hakowania i oceny bezpieczeństwa systemów.

Jak wybrać odpowiednią certyfikację

Dostosowanie do poziomu doświadczenia

Wybór certyfikacji powinien być zgodny z aktualnym poziomem doświadczenia, aby maksymalizować korzyści z nauki.

Cele kariery

Określenie celów kariery jest kluczowe dla wyboru odpowiedniej certyfikacji, która pomoże osiągnąć zamierzone cele.

Ważne czynniki

Warto zwrócić uwagę na czynniki takie jak renoma certyfikacji oraz jej przydatność w branży.



Postanowienie 2 - Rozwój umiejętności technicznych

Kluczowe umiejętności techniczne dla analityków SOC

Analiza logów / danych

Analitycy SOC powinni mieć doświadczenie w analizie danych, aby skutecznie identyfikować zagrożenia i anomalie.

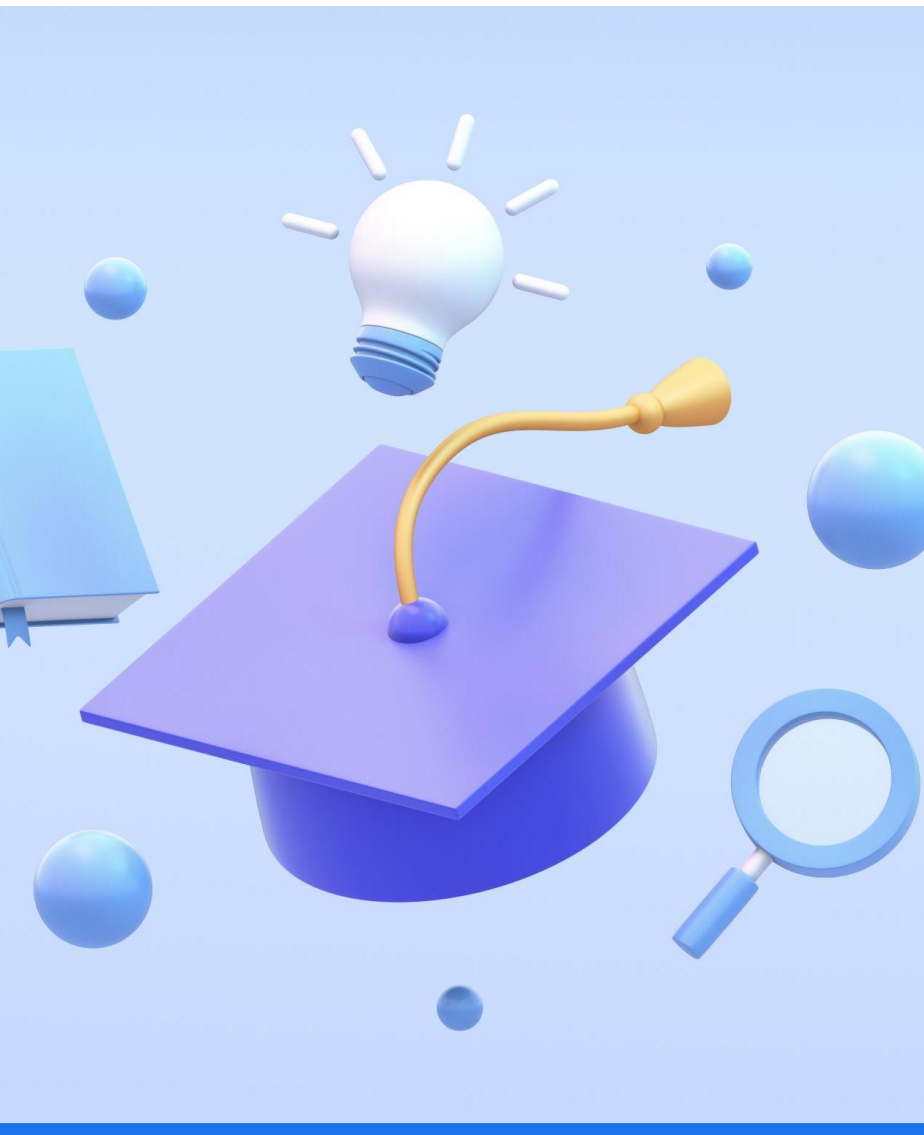
Znajomość systemów bezpieczeństwa

Wiedza na temat systemów bezpieczeństwa jest kluczowa dla analityków SOC w celu ochrony sieci i danych organizacji.

Umiejętności programistyczne

Umiejętności programistyczne pozwalają analitykom SOC na automatyzację zadań i rozwijanie narzędzi do monitorowania.





Najlepsze źródła do nauki: kursy online, książki, szkolenia

Kursy online

Kursy online oferują elastyczne podejście do nauki, pozwalając na zdobywanie wiedzy w dogodnym czasie i tempie.

Książki

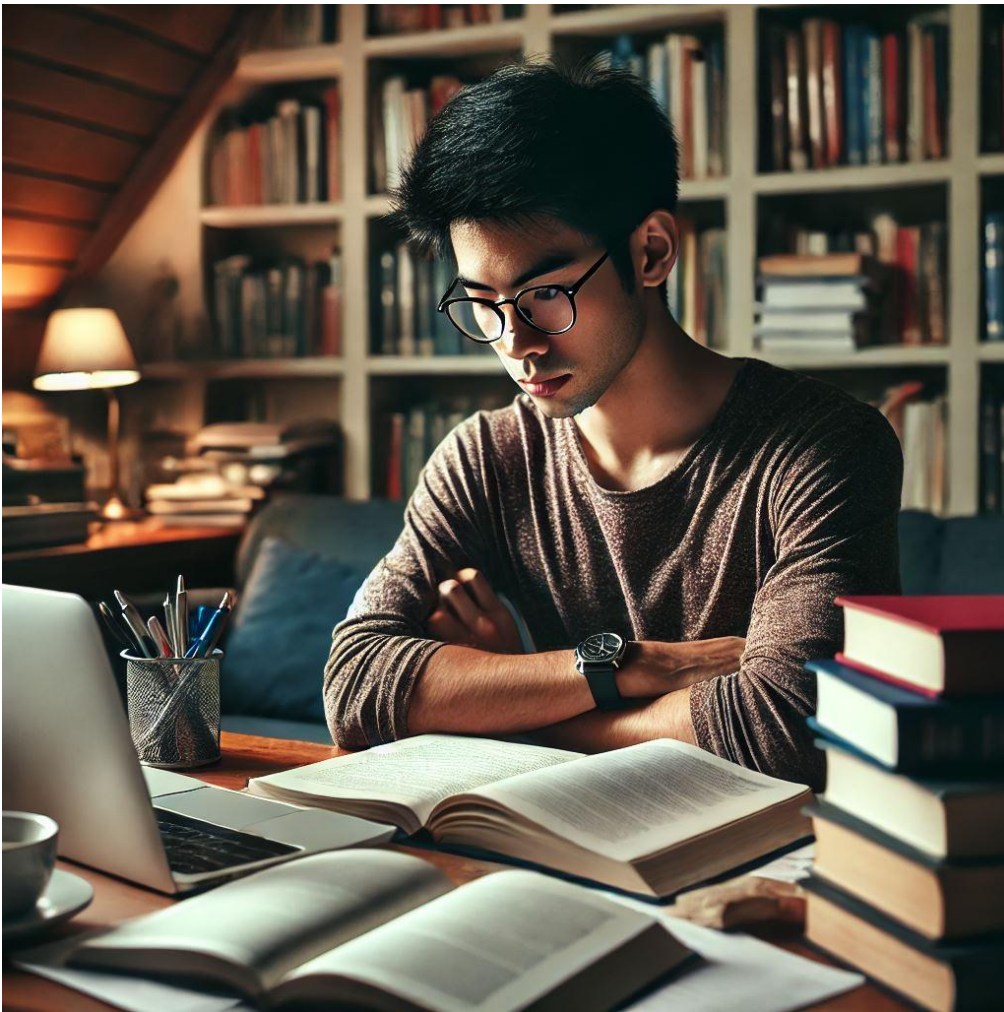
Książki pozostają nieocenionym źródłem wiedzy, dostarczając głębokiego zrozumienia tematów i umiejętności.

Szkolenia

Szkolenia oferują praktyczne doświadczenie i interakcję z ekspertami, co jest kluczowe dla efektywnej nauki.

Praktyka

Praktyka, praktyka i jeszcze raz praktyka.



Nauka samodzielna czy profesjonalny kurs?

Zalety nauki samodzielnej:

- Elastyczność czasowa.
- Możliwość dostosowania materiałów do własnych potrzeb.
- Oszczędność kosztów.

Wady:

- Potrzeba samodyscypliny: Wymaga dużej motywacji i organizacji.
- Brak struktury: Może prowadzić do chaotycznego przyswajania wiedzy.
- Ograniczony dostęp do mentora: Trudności w uzyskaniu feedbacku.



Nauka samodzielna czy profesjonalny kurs?

Zalety kursów i szkoleń:

- Struktura i plan nauki.
- Dostęp do specjalistycznej wiedzy i doświadczenia wykładowców.
- Networking i możliwość wymiany doświadczeń z innymi uczestnikami.

Wady:

- Koszt: Często wyższe koszty niż nauka samodzielna.
- Mniej elastyczności: Ustalane terminy i harmonogramy zajęć.
- Możliwość ograniczonego dostosowania materiału do indywidualnych potrzeb.

Postanowienie 3 – Praktyczne doświadczenie





Praktyczne projekty i ćwiczenia

Znaczenie praktyki w nauce

Praktyczne doświadczenie jest niezbędne do skutecznego przyswajania wiedzy teoretycznej i jej zastosowania w realnym świecie.

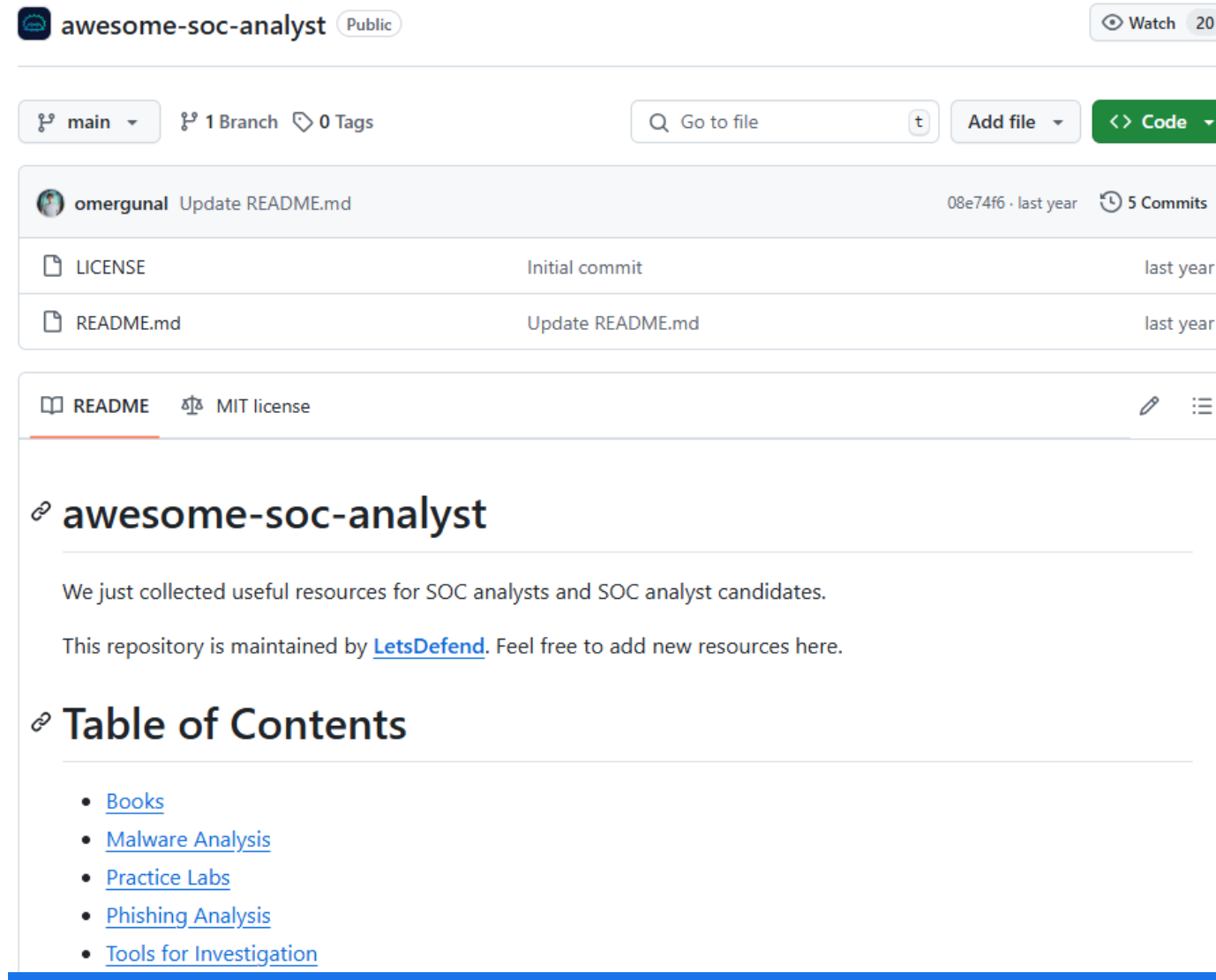
Jak zdobyć doświadczenie?

- Staże
- Wolontariat
- Projekty open source

Praktyczne projekty i ćwiczenia

LetsDefend – Awesome SOC analyst

- Useful resources for SOC Analyst and SOC Analyst candidates.
- <https://github.com/LetsDefend/awesome-soc-analyst>



The screenshot shows the GitHub repository page for 'awesome-soc-analyst', which is a public repository. The repository has 1 branch (main) and 0 tags. It was last updated by user 'omergunal' with the commit 'Update README.md' (08e74f6) last year, with 5 commits in total. The file list shows 'LICENSE' (Initial commit, last year) and 'README.md' (Update README.md, last year). The 'README' file is selected, showing the repository's description: 'We just collected useful resources for SOC analysts and SOC analyst candidates. This repository is maintained by LetsDefend. Feel free to add new resources here.' Below the description is a 'Table of Contents' with links to 'Books', 'Malware Analysis', 'Practice Labs', 'Phishing Analysis', and 'Tools for Investigation'.

awesome-soc-analyst Public

main 1 Branch 0 Tags

Go to file t Add file <> Code

omergunal Update README.md 08e74f6 · last year 5 Commits

LICENSE Initial commit last year

README.md Update README.md last year

README MIT license

awesome-soc-analyst

We just collected useful resources for SOC analysts and SOC analyst candidates.

This repository is maintained by [LetsDefend](#). Feel free to add new resources here.

Table of Contents

- [Books](#)
- [Malware Analysis](#)
- [Practice Labs](#)
- [Phishing Analysis](#)
- [Tools for Investigation](#)

Postanowienie 4 – Budowanie sieci kontaktów w branży

Znaczenie networkingu



Otwarte drzwi w karierze

Networking może prowadzić do nowych możliwości zawodowych i pomóc w awansie w karierze.



Cenne informacje

Dzięki networkingowi można uzyskać cenne informacje o ofertach pracy i trendach w branży.



Wspólne projekty

Networking sprzyja nawiązywaniu współpracy i realizacji wspólnych projektów z innymi profesjonalistami.



Jak budować i utrzymywać profesjonalne relacje

Czas i zaangażowanie

Budowanie trwałych relacji wymaga inwestycji czasu i zaangażowania w rozwijanie kontaktów zawodowych.

Najlepsze praktyki

Warto osiąść najlepsze praktyki dotyczące skutecznego nawiązywania kontaktów, które pomagają w budowaniu relacji.

Utrzymywanie kontaktów

Regularne utrzymywanie kontaktów jest kluczowe dla długoterminowych relacji zawodowych i osobistych.



Platformy i wydarzenia branżowe

Konferencje branżowe

Konferencje branżowe są doskonałą okazją do nawiązywania kontaktów z innymi profesjonalistami w dziedzinie bezpieczeństwa cybernetycznego.

Grupy online

Grupy online oferują platformy do dzielenia się wiedzą oraz doświadczeniami, co jest szczególnie cenne dla analityków SOC.

Spotkania lokalne

Spotkania lokalne umożliwiają bezpośrednie interakcje z innymi specjalistami, co może prowadzić do owocnej współpracy.

Postanowienie 5 - Ciągłe uczenie się i śledzenie trendów





Dlaczego warto być na bieżąco

Szybkie zmiany w cyberbezpieczeństwie

Branża cyberbezpieczeństwa zmienia się w dynamicznym tempie, co wymaga stałej uwagi i edukacji.

Znaczenie aktualnych informacji

Bycie na bieżąco z nowinkami i trendami jest kluczowe dla zrozumienia zagrożeń i ochrony danych.

Unikanie pozostawania w tyle

Brak aktualnych informacji może prowadzić do poważnych luk w zabezpieczeniach i zagrożeń.



Źródła informacji: blogi, fora, konferencje

Popularne blogi

Istnieje wiele blogów, które dostarczają cennych informacji na temat trendów i nowości w branży cyberbezpieczeństwa.

Fora dyskusyjne

Fora dyskusyjne są doskonałym miejscem do wymiany informacji oraz doświadczeń w dziedzinie cyberbezpieczeństwa.

Konferencje branżowe

Uczestnictwo w konferencjach branżowych pozwala na nawiązanie kontaktów oraz zapoznanie się z najnowszymi osiągnięciami w cyberbezpieczeństwie.

Techniki efektywnego uczenia się

Techniki zapamiętywania

Użycie technik zapamiętywania, takich jak mnemotechniki, może znacząco poprawić zdolność do przyswajania informacji.


Notowanie i organizacja

Skuteczne notowanie i organizacja materiałów edukacyjnych są kluczowe dla efektywnego uczenia się i zapamiętywania.

Grupy studyjne

Udział w grupach studyjnych sprzyja wymianie wiedzy i lepszemu zrozumieniu trudnych zagadnień poprzez dyskusję.





Postanowienie 6 – Rozwój umiejętności miękkich



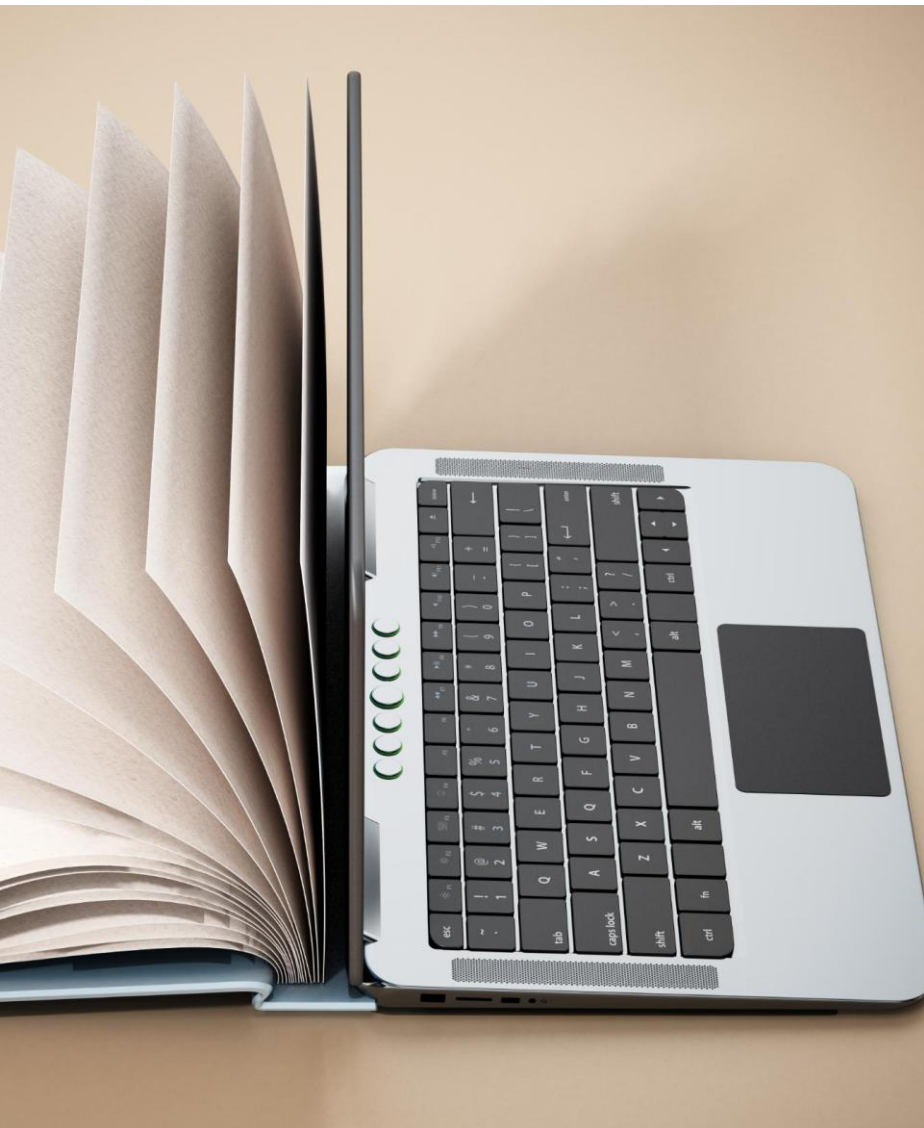
Kluczowe umiejętności miękkie

Co to są umiejętności miękkie?

Zestaw umiejętności interpersonalnych, które wpływają na sposób, w jaki komunikujemy się i współpracujemy z innymi.

Najważniejsze umiejętności miękkie dla Analityków SOC

- **Komunikacja:** Umiejętność jasnego przekazywania informacji i słuchania innych.
- **Praca zespołowa:** Współpraca z innymi członkami zespołu w celu rozwiązywania problemów i osiągnięcia celów.



Dlaczego umiejętności miękkie są ważne?

Znaczenie w pracy SOC Analyst:

- Współpraca z różnymi działami (IT, zarządzanie ryzykiem, zarządzanie incydentami).
- Efektywne przekazywanie informacji o zagrożeniach i incydentach.

Korzyści z rozwijania umiejętności miękkich:

- Lepsza atmosfera w zespole.
- Zwiększona efektywność w rozwiązywaniu problemów.
- Wyższa satysfakcja z pracy.

Podsumowanie i tworzenie własnej listy



POSTANOWIENIA NOWOROCZNE NA ~~2013~~ ~~2014~~ 2015

- 1) ^{znowu}schudnąć ~~10 kg~~ ^{co najmniej} 3 kg
- 2) zacząć ~~biegać~~ ^{chodzić na spacer} ^{kupić sobie} psa
- 3) ^{znowu}powiedzieć szefowi co o nim ~~myśle~~ ^{znaleźć pracę}
- 4) posprzątać w ~~szafie~~ ^{życiu}
- 5) ^{postarać się} być miłym dla mojej ^{byłej} dziewczyny
- 6) ~~nie jeść~~ ^{mniej słodczy} słodczy i ~~chipsów~~

DEMOTYWATORY.PL

Z cyklu: jak sumiennie realizować
postanowienia noworoczne

Tworzenie realistycznych i osiągalnych celów

Znaczenie realistycznych celów

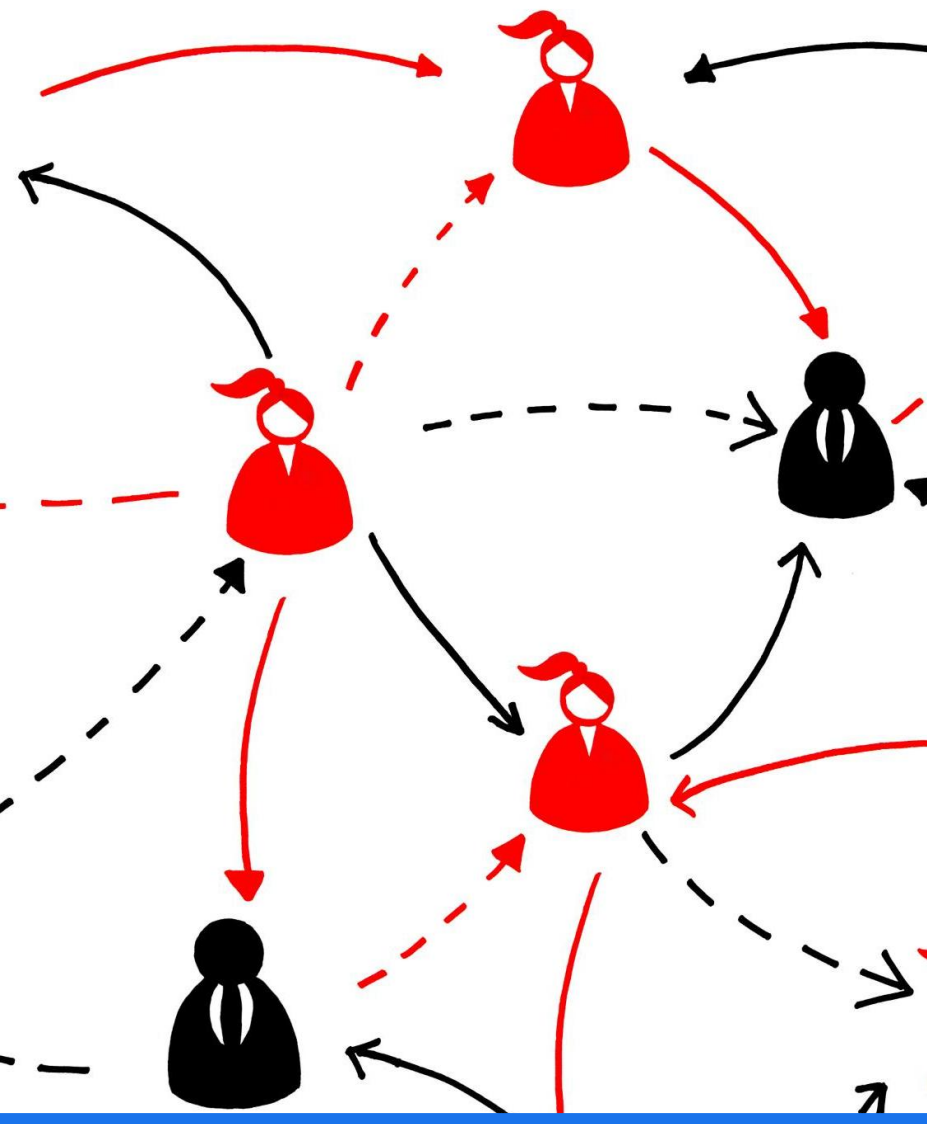
Ustalenie realistycznych celów pomaga w uniknięciu frustracji i zwiększa szanse na sukces. Kluczowe jest, aby cel był wykonalny.

Formułowanie celów

Cele powinny być sformułowane w sposób jasny i konkretny, aby można je było łatwo zrozumieć i osiągnąć w określonym czasie.

Planowanie czasowe

Określenie ram czasowych dla celów jest niezwykle istotne. Pomaga to w monitorowaniu postępów i dostosowywaniu działań.



Podsumowanie kluczowych punktów sesji

Certyfikacja

Uzyskanie odpowiednich certyfikatów jest kluczowe dla rozwoju kariery analityków SOC, potwierdzając ich umiejętności i wiedzę.

Budowanie sieci kontaktów

Budowanie silnej sieci kontaktów może znacząco wpłynąć na rozwój kariery analityków SOC, umożliwiając wymianę wiedzy i możliwości zawodowe.

Rozwój umiejętności

Ciągłe doskonalenie umiejętności jest niezbędne, aby analitycy SOC mogli dostosować się do zmieniającego się krajobrazu technologicznego.

Jak monitorować postępy i utrzymać motywację

Znaczenie monitorowania postępów

Regularne śledzenie postępów pozwala na ocenę osiągnięć i dostosowanie strategii działania w celu osiągnięcia celów.

Metody utrzymania motywacji

Wykorzystanie technik takich jak wizualizacja celów oraz afirmacje może znacząco wpłynąć na naszą motywację do działania.





Jak stworzyć własną listę postanowień

Zdefiniowanie celów

Pierwszym krokiem jest jasne określenie, jakie cele chcesz osiągnąć. Spisanie celów pomoże w ich realizacji.

Ustalanie priorytetów

Ustal priorytety swoich celów, aby skupić się na tych najważniejszych. To pomoże w efektywnym planowaniu działań.

Regularne przeglądy

Regularnie przeglądaj swoją listę postanowień, aby dostosować cele do zmieniających się okoliczności. Pomaga to utrzymać motywację i kierunek.



6 grzechów głównych osób chcących wejść do branży IT

- **Brak solidnych podstaw teoretycznych:** Wiele osób pomija naukę podstawowych koncepcji związanych z bezpieczeństwem IT, takich jak protokoły sieciowe, architektura systemów czy zasady działania systemów operacyjnych. Zrozumienie tych elementów jest kluczowe dla skutecznego działania w obszarze cybersecurity.
- **Niedostateczne praktyczne doświadczenie:** Skupianie się wyłącznie na teorii bez praktycznego zastosowania wiedzy może prowadzić do braku przygotowania na rzeczywiste wyzwania. Praktyczne umiejętności są niezwykle ważne w tej dziedzinie.



6 grzechów głównych osób chcących wejść do branży IT

- **Nieprzywiązywanie wagi do etyki:** W branży cybersecurity niezwykle istotne jest przestrzeganie zasad etyki zawodowej. Osoby, które nie rozumieją znaczenia odpowiedzialności za swoje działania, mogą narazić siebie i swoją firmę na poważne konsekwencje.
- **Brak umiejętności komunikacyjnych:** Efektywne komunikowanie się z innymi członkami zespołu oraz z osobami nietechnicznymi jest kluczowe w branży cybersecurity. Niedostateczne umiejętności interpersonalne mogą prowadzić do nieporozumień i problemów w pracy zespołowej.



6 grzechów głównych osób chcących wejść do branży IT

- **Zaniedbywanie ciągłego kształcenia:** Cybersecurity to dynamiczna dziedzina, w której nowe zagrożenia i technologie pojawiają się nieustannie. Osoby uczące się muszą być gotowe na ciągłe doskonalenie swoich umiejętności i śledzenie trendów w branży.
- **Zbyt wczesne lub zbyt późne poszukiwanie pracy:** Niektórzy mogą zacząć szukać pracy w branży cybersecurity zanim zdobędą wystarczającą wiedzę i umiejętności, co prowadzi do frustracji i niepowodzeń. Z kolei inni mogą odkładać poszukiwania pracy na zbyt długi czas, co skutkuje utratą okazji oraz trudnościami w wejściu na rynek pracy.

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/>

