ZDOBYTE CERTYFIKATY

CM)CTA | CySA+, C)CSA & C3SA | CCDA | HTB CDSA | C|SA | PSAP | PSAA | CSOA | CBTeamerX | CBTeamer | CBTP | CM)CFI | GCFE | GCFA | GNFA | CCDFA | C)NFE | C)DFE | eCDFP | CDFEH | ISO/IEC 27037 LI | WCNA | GCED | C|ND | CCD | C)ISSO | CPTA | HTB CPTS | C)PTC | C)PTE | C)PEH | C)VA | RvBCWP | CM)IPS | eCTHP | CRTS | CRTA | CRTeamer | CCMA | C)TIA | CIoTSP | OOSE | CNSP | CNSE | CCC | CCE | CCSE | CCSS

WYDANE PRZEZ

GIAC (w powiązaniu z SANS Institute), Mile2 Cybersecurity Institute, EC-Council, CompTIA, HTB Academy, INE Security, TCM Security, CyberWarFare Labs, CyberDefenders, Cyber5W, The SecOps Group, CertNexus, Hackviser, OPSWAT Academy, Protocol Analysis Institute (program certyfikacyjny WCNA), United States Cybersecurity Institute, Pacific Certifications, Blockchain Council i Global Tech Council.

Michał Sołtysik

✆ +48 796 *** ***
✉ me@michalsoltysik.com
https://michalsoltysik.pl/

Cybersecurity Consultant

Cybersecurity Consulting | Blue Teaming | Purple Teaming | Red Teaming | Informatyka śledcza | Trener SOC | Organizacja działań cyberwojennych | Budowa dojrzałości SOC | Emulacja przeciwnika

Konsultant ds. cyberbezpieczeństwa oraz analityk **Blue Team**, **Purple Team** i **Red Team** z rozległym doświadczeniem oraz dogłębną wiedzą w wielu obszarach cyberbezpieczeństwa.

Ekspert w zakresie informatyki śledczej cyfrowej i sieciowej, **organizator działań z zakresu cyberwojny** oraz **trener SOC**, specjalizujący się w **budowie zdolności operacyjnych i rozwoju dojrzałości SOC**, **profilowaniu ruchu sieciowego na styku sieci** oraz **emulacji przeciwnika w testach systemów EDR**.

DOŚWIADCZENIE

Cybersecurity Consultant | Warszawa | Praca zdalna

Konsulting Security Operations Centre (**SOC**). **Mentoring oraz wsparcie techniczne Tier 1, Tier 2 i Tier 3**. Inżynieria oraz administracja SIEM (Splunk, Elastic SIEM, IBM QRadar). Integracja i optymalizacja rozwiązań bezpieczeństwa (SOAR, SIEM, IDS/IPS, WAF, EDR, NAC, APT, NTA, NIDS, UTM). Organizacja ćwiczeń Blue Team vs. Red Team oraz symulacji cyberwojny. Koordynacja ćwiczeń cyberbezpieczeństwa (w tym Cyber Europe 2024). Rekrutacja SOC oraz techniczna ocena kandydatów. Prowadzenie szkoleń z zakresu SOC i cyberbezpieczeństwa. Reverse engineering malware dla systemów Windows oraz Linux. Tworzenie, administracja oraz zarządzanie środowiskami SOC Lab. Informatyka śledcza cyfrowa oraz sieciowa. Kontrolowane symulacje działań przeciwnika (adversary emulation) oraz analiza malware. Testy penetracyjne oraz oceny bezpieczeństwa. Rekomendacje dotyczące utwardzania infrastruktury bezpieczeństwa. Testowanie oraz walidacja rozwiązań EDR, aplikacyjnych oraz Anti-DDoS. Reagowanie na incydenty (Incident Response) oraz analiza zagrożeń. Obsługa materiału dowodowego oraz reagowanie śledcze (DEFR/DES).

Sektor transformacji cyfrowej i cyberbezpieczeństwa administracji publicznej. Administracja publiczna oraz krajowe platformy usług online. Organizacje związane z cyberbezpieczeństwem, telekomunikacją oraz badaniami naukowymi. Krajowi dostawcy infrastruktury cyfrowej oraz sieci edukacyjnych. Służby bezpieczeństwa, wywiadu oraz kontrwywiadu. Instytucje antykorupcyjne oraz związane z transparentnością życia publicznego. Instytucje administracji finansowej oraz funduszy publicznych. Instytucje sądownicze oraz administracji sądowej. Krajowe instytucje ochrony zdrowia oraz badań medycznych. Operatorzy infrastruktury krytycznej, sektora energetycznego oraz magazynowania gazu. Zarządy portów morskich oraz operatorzy logistyczni. Dostawcy usług ciepłowniczych i komunalnych. Firmy przemysłowe oraz chemiczne. Firmy z branży projektowania wnętrz oraz rozwiązań architektonicznych. Korporacje budowlane oraz infrastrukturalne. Producenci mebli oraz wyposażenia wnętrz. Dostawcy infrastruktury IT oraz usług technologicznych. Szkolnictwo wyższe oraz instytucje akademickie. Producenci motoryzacyjni oraz komponentów przemysłowych. Producenci farmaceutyczni oraz produktów medycznych. Administracja samorządowa oraz lokalna.

Oficjalny list referencyjny od Kierownika SOC, oparty na 5-letnim doświadczeniu pracy jako Konsultant SOC, Analityk i Trener

https://michalsoltysik.pl/referencje/

WIĘCEJ INFORMACJI

Certyfikaty:
https://michalsoltysik.pl/certyfikaty/

Usługi:
https://michalsoltysik.pl/uslugi/

Szkolenia:
https://michalsoltysik.pl/szkolenia/

Umiejętności:
https://michalsoltysik.pl/umiejetnosci/

Referencje:
https://michalsoltysik.pl/referencje/

Treści edukacyjne:
https://michalsoltysik.pl/tresci-edukacyjne/

Własne narzędzia:
https://michalsoltysik.pl/wlasne-narzedzia/

Wydarzenia:
https://michalsoltysik.pl/wydarzenia/

Kontakt:
https://michalsoltysik.pl/kontakt/

SOC Analyst Level 3 | Warszawa | Praca stacjonarna

Operacje Security Operations Centre (**SOC**) **Level 3**. Rozwój, wdrażanie oraz projektowanie zespołów SOC. Wdrażanie oraz integracja rozwiązań bezpieczeństwa. Tworzenie procesów, procedur oraz dokumentacji bezpieczeństwa. Mentoring oraz wsparcie techniczne dla analityków Tier 1 i Tier 2. Administracja IBM QRadar SIEM, tworzenie oraz tuning reguł Flow i Event.

Sektor publiczny oraz komercyjny. Organizacje związane z cyberbezpieczeństwem, telekomunikacją oraz badaniami naukowymi. Krajowi dostawcy infrastruktury cyfrowej oraz sieci edukacyjnych. Operatorzy infrastruktury krytycznej.

SOC Analyst Level 2 | Warszawa | Praca stacjonarna

Operacje Security Operations Centre (**SOC**) **Level 2**. Rozwój oraz wdrażanie Security Operations Centre. Integracja i optymalizacja rozwiązań bezpieczeństwa. Tworzenie procesów, procedur oraz dokumentacji bezpieczeństwa. Mentoring oraz wsparcie techniczne dla analityków Tier 1. Administracja IBM QRadar SIEM, tworzenie oraz tuning reguł. Informatyka śledcza cyfrowa oraz sieciowa.

Rządowe usługi online, portale, strony internetowe oraz aplikacje cyfrowe. Sektor transformacji cyfrowej i cyberbezpieczeństwa administracji publicznej. Dostawcy infrastruktury IT oraz usług informatycznych sektora publicznego.

SOC Analyst | Warszawa | Praca stacjonarna

Operacje bezpieczeństwa Level 1 i Level 2 w ramach Security Operations Centre (**SOC**).

Międzynarodowe środowiska ubezpieczeniowe, finansowe oraz korporacyjne.

Network Specialist | Warszawa | Praca stacjonarna

Wsparcie techniczne 2. linii w ramach Network Operations Centre (**NOC**).

CORP IT Specialist | Warszawa | Praca stacjonarna

Wsparcie Service Desk.

IT Operations associate | Warszawa | Praca stacjonarna

Globalne wsparcie Service Desk.

Helpdesk Agent with English | Warszawa | Praca stacjonarna

Wsparcie IT Helpdesk.

Founder, Owner & Manager - Sick Slaughterhouse

Założenie i zarządzanie wytwórnią muzyki EDM specjalizującą się w produkcji muzycznej, zarządzaniu artystami, dystrybucji muzyki, marketingu, promocji oraz międzynarodowej współpracy biznesowej.

Music Producer, Composer & Audio Engineer - MikeWave

Tworzenie autorskich utworów muzycznych dystrybuowanych na międzynarodowych platformach streamingowych i dystrybucyjnych.

W celu uzyskania rozszerzonej wersji CV zawierającej szczegółowe informacje proszę o bezpośredni kontakt.