2BEAWARE
SECURITY AWARENESS

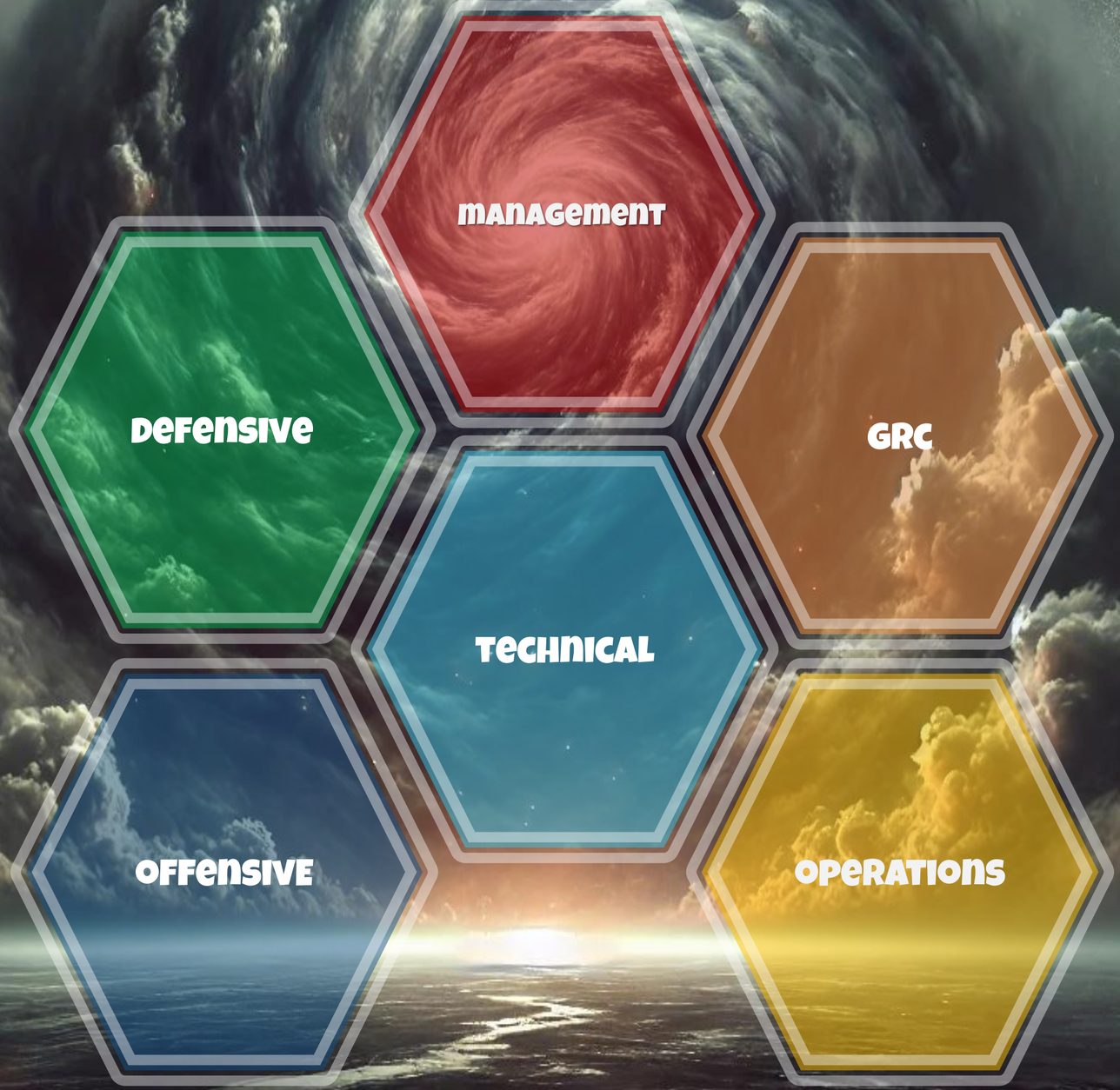
SECURITY DLA LIDERÓW

KTO JEST KIM W SECURITY ?

KRZYSZTOF
BRYŁA

CZĘŚĆ 3

OBSZARY SECURITY



2BEAWARE
SECURITY AWARENESS

Offensive & Defensive Security

Offensive

- Patrzenie na system z perspektywy atakującego
- Testowanie poprzez przeprowadzanie symulowanych ataków
- Wyszukiwanie i usuwanie luk w zabezpieczeniach
- Ulepszona gotowość i reagowanie na incydenty
- Często testowanie określonego systemu lub sieci

DEFENSIVE

- ZAPOBIEGANIE ATAKOM I REAGOWANIE NA NIE
- ŁAGODZENIE SKUTKÓW ATAKÓW W PRZYPADKU ICH WYSTĄPIENIA
- PATRZENIE NA SYSTEM Z PERSPEKTYWY OBROŃCY
- WDRAŻANIE SZEROKIEGO ZAKRESU KONTROLI W CELU OCHRONY PRZED WIELOMA POTENCJALNYMI ZAGROŻENIAMI
- KONCENTROWANIE SIĘ ZWYKLE NA OCHRONIE ZASOBÓW CAŁEJ ORGANIZACJI

OFFENSIVE

Penetration Tester	przeprowadza kontrolowane ataki na systemy komputerowe, aplikacje i sieci w celu identyfikacji i eliminacji potencjalnych słabości. symuluje działania hakerów, aby ocenić skuteczność zabezpieczeń i zaproponować odpowiednie środki ochrony

OFFENSIVE

Penetration Tester	przeprowadza kontrolowane ataki na systemy komputerowe, aplikacje i sieci w celu identyfikacji i eliminacji potencjalnych słabości. symuluje działania hakerów, aby ocenić skuteczność zabezpieczeń i zaproponować odpowiednie środki ochrony
Vulnerability Assesor	identyfikuje, analizuje i ocenia podatności w systemach informatycznych organizacji. systematycznie bada infrastrukturę IT pod kątem potencjalnych luk, które mogłyby zostać wykorzystane przez cyberprzestępców. rekomenduje działania naprawcze

OFFENSIVE

Penetration Tester	przeprowadza kontrolowane ataki na systemy komputerowe, aplikacje i sieci w celu identyfikacji i eliminacji potencjalnych słabości. symuluje działania hakerów, aby ocenić skuteczność zabezpieczeń i zaproponować odpowiednie środki ochrony
Vulnerability Assesor	identyfikuje, analizuje i ocenia podatności w systemach informatycznych organizacji. systematycznie bada infrastrukturę IT pod kątem potencjalnych luk, które mogłyby zostać wykorzystane przez cyberprzestępców. rekomenduje działania naprawcze
Social Engineer Specialist	bada i wykorzystuje ludzkie zachowania w celu uzyskania dostępu do poufnych informacji lub systemów. projektuje i wykonuje strategie manipulacji, które mogą obejmować podszywanie się pod innych, phishing oraz inne techniki wykorzystujące psychologiczne aspekty ludzkiego zachowania

OFFENSIVE

Penetration Tester	przeprowadza kontrolowane ataki na systemy komputerowe, aplikacje i sieci w celu identyfikacji i eliminacji potencjalnych słabości. symuluje działania hakerów, aby ocenić skuteczność zabezpieczeń i zaproponować odpowiednie środki ochrony
Vulnerability Assesor	identyfikuje, analizuje i ocenia podatności w systemach informatycznych organizacji. systematycznie bada infrastrukturę IT pod kątem potencjalnych luk, które mogłyby zostać wykorzystane przez cyberprzestępców. rekomenduje działania naprawcze
Social Engineer Specialist	bada i wykorzystuje ludzkie zachowania w celu uzyskania dostępu do poufnych informacji lub systemów. projektuje i wykonuje strategie manipulacji, które mogą obejmować podszywanie się pod innych, phishing oraz inne techniki wykorzystujące psychologiczne aspekty ludzkiego zachowania
Security Researcher	analizuje systemy i aplikacje w celu identyfikacji nowych podatności i zagrożeń. rozwija metody testowania zabezpieczeń, bada najnowsze technologie, które mogą pomóc w poprawie ogólnego poziomu bezpieczeństwa cyfrowego

OFFENSIVE

Penetration Tester	przeprowadza kontrolowane ataki na systemy komputerowe, aplikacje i sieci w celu identyfikacji i eliminacji potencjalnych słabości. symuluje działania hakerów, aby ocenić skuteczność zabezpieczeń i zaproponować odpowiednie środki ochrony
Vulnerability Assesor	identyfikuje, analizuje i ocenia podatności w systemach informatycznych organizacji. systematycznie bada infrastrukturę IT pod kątem potencjalnych luk, które mogłyby zostać wykorzystane przez cyberprzestępców. rekomenduje działania naprawcze
Social Engineer Specialist	bada i wykorzystuje ludzkie zachowania w celu uzyskania dostępu do poufnych informacji lub systemów. projektuje i wykonuje strategie manipulacji, które mogą obejmować podszywanie się pod innych, phishing oraz inne techniki wykorzystujące psychologiczne aspekty ludzkiego zachowania
Security Researcher	analizuje systemy i aplikacje w celu identyfikacji nowych podatności i zagrożeń. rozwija metody testowania zabezpieczeń, bada najnowsze technologie, które mogą pomóc w poprawie ogólnego poziomu bezpieczeństwa cyfrowego
Security Auditor	przeprowadza audyty systemów informatycznych w celu weryfikacji ich zgodności z obowiązującymi standardami bezpieczeństwa i regulacjami. ocenia procedury, polityki oraz mechanizmy zabezpieczeń, a także formułowanie rekomendacje na podstawie wykrytych słabości

DEFENSIVE

Security Analyst monitoruje systemy informatyczne w organizacji, wykrywa nieprawidłowości i potencjalne zagrożenia. analizuje dane z różnych źródeł, takich jak logi systemowe czy raporty z monitoringu

DEFENSIVE

Security Analyst	monitoruje systemy informatyczne w organizacji, wykrywa nieprawidłowości i potencjalne zagrożenia. analizuje dane z różnych źródeł, takich jak logi systemowe czy raporty z monitoringu
Incident Responder	zarządza sytuacjami kryzysowymi. odpowiada za szybką identyfikację, analizę i neutralizację skutków ataków cybernetycznych, przywracanie normalnego funkcjonowania systemów i minimalizowanie szkód

DEFENSIVE

Security Analyst	monitoruje systemy informatyczne w organizacji, wykrywa nieprawidłowości i potencjalne zagrożenia. analizuje dane z różnych źródeł, takich jak logi systemowe czy raporty z monitoringu
Incident Responder	zarządza sytuacjami kryzysowymi. odpowiada za szybką identyfikację, analizę i neutralizację skutków ataków cybernetycznych, przywracanie normalnego funkcjonowania systemów i minimalizowanie szkód
Threat Intelligence	zbiera, analizuje i interpretuje dane o aktualnych i potencjalnych zagrożeniach cyfrowych. przewiduje i zapobiega atakom

DEFENSIVE

Security Analyst	monitoruje systemy informatyczne w organizacji, wykrywa nieprawidłowości i potencjalne zagrożenia. analizuje dane z różnych źródeł, takich jak logi systemowe czy raporty z monitoringu
Incident Responder	zarządza sytuacjami kryzysowymi. odpowiada za szybką identyfikację, analizę i neutralizację skutków ataków cybernetycznych, przywracanie normalnego funkcjonowania systemów i minimalizowanie szkód
Threat Intelligence	zbiera, analizuje i interpretuje dane o aktualnych i potencjalnych zagrożeniach cyfrowych. przewiduje i zapobiega atakom
Network Security Engineer	projektuje, wdraża i monitoruje zabezpieczenia sieciowe w celu ochrony danych przed nieautoryzowanym dostępem i atakami

DEFENSIVE

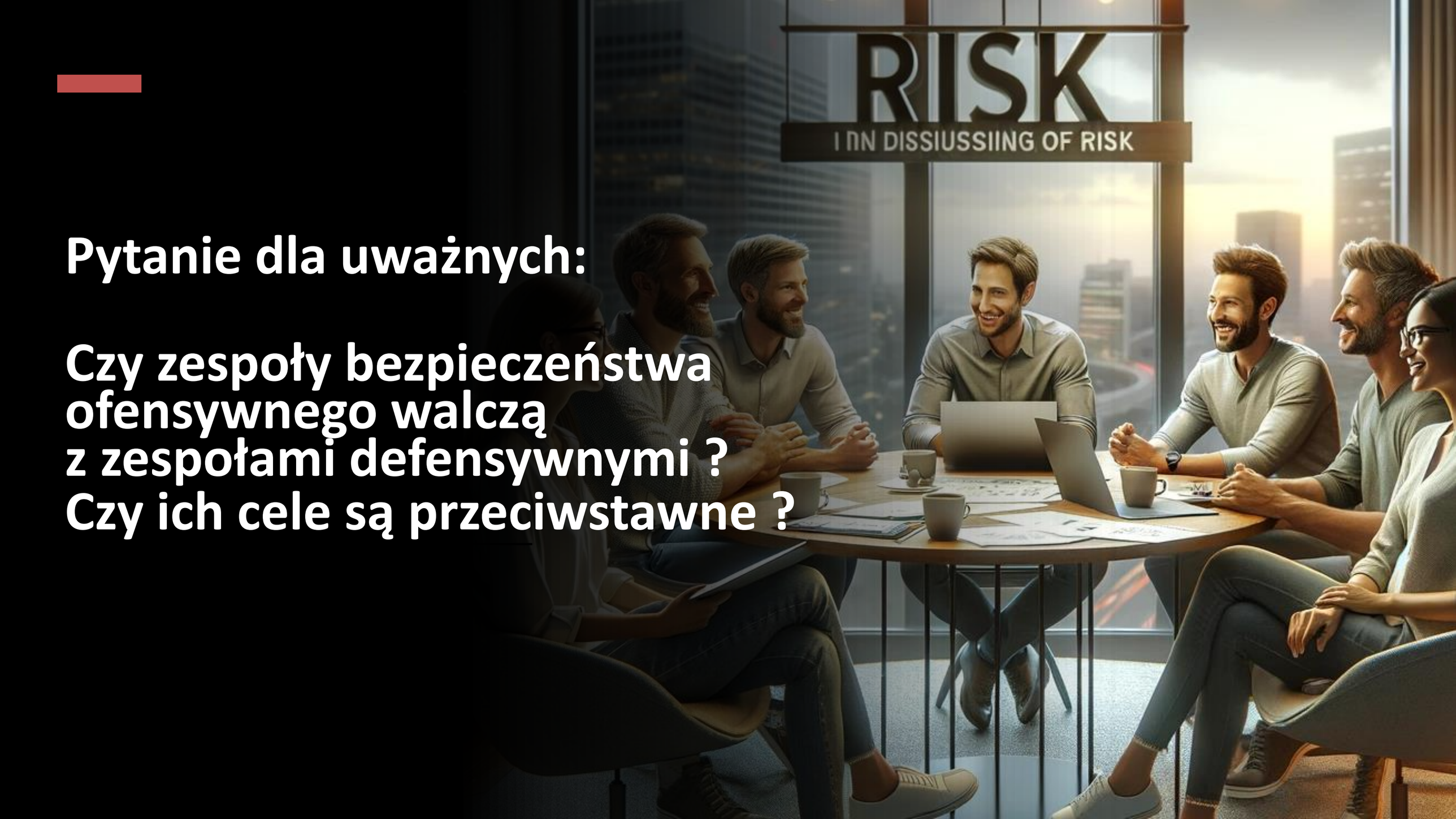
Security Analyst	monitoruje systemy informatyczne w organizacji, wykrywa nieprawidłowości i potencjalne zagrożenia. analizuje dane z różnych źródeł, takich jak logi systemowe czy raporty z monitoringu
Incident Responder	zarządza sytuacjami kryzysowymi. odpowiada za szybką identyfikację, analizę i neutralizację skutków ataków cybernetycznych, przywracanie normalnego funkcjonowania systemów i minimalizowanie szkód
Threat Intelligence	zbiera, analizuje i interpretuje dane o aktualnych i potencjalnych zagrożeniach cyfrowych. przewiduje i zapobiega atakom
Network Security Engineer	projektuje, wdraża i monitoruje zabezpieczenia sieciowe w celu ochrony danych przed nieautoryzowanym dostępem i atakami
Security Architect	tworzy i egzekwuje standardy bezpieczeństwa, przeprowadza regularne oceny bezpieczeństwa, identyfikuje podatności w aplikacjach i współpracuje z developmentem w celu ich naprawy. jest pomostem między bezpieczeństwem a developmentem, zapewniając, że aplikacje są projektowane, rozwijane i wdrażane w bezpieczny sposób

DEFENSIVE

Security Analyst	monitoruje systemy informatyczne w organizacji, wykrywa nieprawidłowości i potencjalne zagrożenia. analizuje dane z różnych źródeł, takich jak logi systemowe czy raporty z monitoringu
Incident Responder	zarządza sytuacjami kryzysowymi. odpowiada za szybką identyfikację, analizę i neutralizację skutków ataków cybernetycznych, przywracanie normalnego funkcjonowania systemów i minimalizowanie szkód
Threat Intelligence	zbiera, analizuje i interpretuje dane o aktualnych i potencjalnych zagrożeniach cyfrowych. przewiduje i zapobiega atakom
Network Security Engineer	projektuje, wdraża i monitoruje zabezpieczenia sieciowe w celu ochrony danych przed nieautoryzowanym dostępem i atakami
Security Architect	tworzy i egzekwuje standardy bezpieczeństwa, przeprowadza regularne oceny bezpieczeństwa, identyfikuje podatności w aplikacjach i współpracuje z developmentem w celu ich naprawy. jest pomostem między bezpieczeństwem a developmentem, zapewniając, że aplikacje są projektowane, rozwijane i wdrażane w bezpieczny sposób
Forensic Expert	bada cyfrowe dowody w celu ustalenia przebiegu i skutków incydentów bezpieczeństwa. analizuje dane z urządzeń komputerowych i sieci, aby zidentyfikować, jak doszło do naruszenia i jak można temu zapobiec w przyszłości

2BEAWARE
SECURITY AWARENESS

CDN ...



Pytanie dla uważnych:

Czy zespoły bezpieczeństwa ofensywnego walczą z zespołami defensywnymi ?
Czy ich cele są przeciwstawne ?

2BEAWARE
SECURITY AWARENESS

KRZYSZTOF BRYŁA

2beaware

2beaware_

office@2beaware.co

krzysztof-bryla