Słownictwo Cybersecurity	
Cyberthreats **English**: "Cyberthreats are becoming more sophisticated, requiring companies to invest in advanced cybersecurity measures." **Polish**: "Cyberzagrożenia stają się coraz bardziej zaawansowane, co zmusza firmy do inwestowania w zaawansowane środki cyberbezpieczeństwa."	Cyberzagrożenia Termin **"cyberthreats"** odnosi się do zagrożeń związanych z cyberbezpieczeństwem. Obejmuje wszelkie działania, które mogą prowadzić do naruszenia poufności, integralności lub dostępności systemów informatycznych, danych lub sieci. Cyberzagrożenia mogą pochodzić od złośliwego oprogramowania (np. wirusy, ransomware), hakerów, phishingu, ataków DDoS (Distributed Denial-of-Service) czy wewnętrznych naruszeń bezpieczeństwa.
Phishing **English**: "Phishing attacks often involve emails that mimic well-known companies to steal personal data." **Polish**: "Ataki phishingowe często polegają na wysyłaniu e-maili, które naśladują znane firmy, aby wyłudzić dane osobowe."	Wyłudzanie informacji **Phishing** to rodzaj cyberataku, w którym oszuści podszywają się pod zaufane osoby lub instytucje w celu wyłudzenia poufnych informacji, takich jak hasła, dane logowania, numery kart kredytowych lub inne wrażliwe dane. Najczęściej odbywa się to poprzez fałszywe e-maile, wiadomości tekstowe lub strony internetowe, które wyglądają na autentyczne. Celem phishingu jest oszukanie ofiary i nakłonienie jej do podania informacji lub kliknięcia w zainfekowany link.
White paper **English**: "The company published a white paper to explain the benefits of its new blockchain technology." **Polish**: "Firma opublikowała white paper, aby wyjaśnić korzyści płynące z jej nowej technologii blockchain."	Biała księga **White paper** to oficjalny dokument lub raport, który szczegółowo opisuje dany temat, problem, technologię, produkt, usługę lub rozwiązanie, zazwyczaj w kontekście biznesowym lub technologicznym. White papers są często wykorzystywane jako narzędzie marketingowe i edukacyjne, aby dostarczyć wartościowe informacje i przekonać odbiorców do określonego rozwiązania, podejścia lub produktu. Dokumenty te cechują się rzeczowym i eksperckim tonem, często opartym na danych i analizach.
Security Operations Center (SOC) **English**: "The Security Operations Center (SOC) detected an unusual spike in	Centrum operacji cyberbezpieczeństwa **Security Operations Center (SOC)** to dedykowane centrum operacyjne, w

network activity and prevented a potential cyberattack." **Polish**: "Centrum Operacyjne Bezpieczeństwa (SOC) wykryło nietypowy wzrost aktywności w sieci i zapobiegło potencjalnemu cyberatakowi."	którym specjaliści ds. bezpieczeństwa monitorują, analizują i reagują na zagrożenia cybernetyczne w czasie rzeczywistym. SOC jest centralnym punktem zarządzania cyberbezpieczeństwem organizacji, zapewniającym ochronę przed atakami i naruszeniami bezpieczeństwa poprzez stały nadzór nad systemami informatycznymi, sieciami, aplikacjami oraz danymi. SOC działa 24/7, aby zapewnić szybkie wykrywanie i neutralizowanie zagrożeń.
Rampant Password Reuse **English**: "Rampant password reuse is one of the primary reasons for the success of credential-stuffing attacks." **Polish**: "Powszechne używanie tych samych haseł jest jednym z głównych powodów skuteczności ataków typu credential-stuffing."	Powszechne nadużywanie haseł **Rampant Password Reuse** oznacza powszechne i niebezpieczne praktyki używania tego samego hasła w różnych kontach, serwisach lub aplikacjach. Jest to duże zagrożenie dla cyberbezpieczeństwa, ponieważ jeśli jedno z kont zostanie naruszone, pozostałe, korzystające z tego samego hasła, również mogą być łatwo przejęte przez hakerów. Tego rodzaju praktyka zwiększa ryzyko ataków, takich jak credential stuffing, gdzie cyberprzestępcy wykorzystują wyciekłe dane logowania w celu uzyskania dostępu do innych systemów.
Infostealer **English**: "The cybersecurity team discovered an infostealer that had compromised several employee accounts." **Polish**: "Zespół ds. cyberbezpieczeństwa wykrył infostealera, który naruszył kilka kont pracowników."	Złodziej informacji **Infostealer** to rodzaj złośliwego oprogramowania (malware) zaprojektowanego do kradzieży poufnych informacji z urządzeń ofiar. Infostealery zbierają dane takie jak loginy, hasła, dane bankowe, informacje o kartach kredytowych, dane przeglądarek (np. zapisane hasła, pliki cookie) czy nawet klucze dostępu do aplikacji. Zebrane informacje są następnie przesyłane do cyberprzestępców, którzy mogą je wykorzystać do ataków, oszustw finansowych lub sprzedać na czarnym rynku. Infostealery są często dostarczane za pośrednictwem phishingu, zainfekowanych załączników, złośliwych

	reklam lub niebezpiecznych stron internetowych.
Full Disclosure **English**: "The researcher opted for full disclosure and published the details of the vulnerability online." **Polish**: "Badacz zdecydował się na pełne ujawnienie i opublikował szczegóły podatności w sieci."	Pełne ujawnienie **Full Disclosure** to termin, który może mieć różne znaczenia w zależności od kontekstu, ale najczęściej odnosi się do praktyki ujawniania wszystkich istotnych informacji w sposób pełny i przejrzysty. W kontekście cyberbezpieczeństwa i technologii, **Full Disclosure** oznacza publiczne ujawnienie szczegółowych informacji o wykrytej podatności (vulnerability) lub zagrożeniu bezpieczeństwa, często zanim producent oprogramowania zdąży wypuścić poprawkę (patch). Celem takiego podejścia może być: 1. **Uświadomienie użytkowników** o istniejącym zagrożeniu, aby mogli podjąć środki zaradcze. 2. **Wymuszenie szybkiej reakcji na producentów** oprogramowania, którzy mogą zwlekać z naprawą podatności. Choć praktyka ta bywa kontrowersyjna, zwolennicy twierdzą, że motywuje firmy do poprawy bezpieczeństwa, natomiast krytycy wskazują, że może narazić użytkowników na ataki, zanim rozwiązanie zostanie udostępnione.