Cyberbezpieczeństwo po angielsku: słownictwo zaawansowane

92 słówka

ANGIELSKI	TRANSKRYPCJA	TŁUMACZENIE
threat actor	[θret 'æktə]	sprawca zagrożenia
attack vector	[ə'tæk 'vektə]	wektor ataku
attack surface	[ə'tæk 'sɜːfɪs]	powierzchnia ataku
zero-day	['zɪərəʊ deɪ]	luka zero-day
vulnerability management	[ˌvʌlnərə'bɪlɪti 'mænɪʤmənt]	zarządzanie podatnościami
penetration testing	[ˌpenɪ'treɪʃn 'testɪŋ]	testy penetracyjne
pen test	[pen test]	pentest
red team	[red tiːm]	zespół czerwony
blue team	[bluː tiːm]	zespół niebieski
purple team	['pɜːpl tiːm]	zespół fioletowy
security operations center	[sɪ'kjʊərɪti ˌɒpə'reɪʃnz 'sentə]	centrum operacji bezpieczeństwa
lateral movement	['lætərəl 'muːvmənt]	ruch boczny w sieci
privilege escalation	['prɪvɪlɪʤ ˌeskə'leɪʃn]	eskalacja uprawnień
persistence	[pə'sɪstəns]	utrwalenie dostępu
command and control	[kəˌmɑːnd ən kən'trəʊl]	serwer sterujący
beaconing	['biːkənɪŋ]	okresowe łączenie z serwerem
kill chain	[kɪl ʧeɪn]	łańcuch ataku
threat intelligence	[θret ɪn'telɪʤəns]	wywiad o zagrożeniach
threat hunting	[θret 'hʌntɪŋ]	aktywne poszukiwanie zagrożeń
incident response plan	['ɪnsɪdənt rɪ'spɒns plæn]	plan reagowania na incydenty
forensics	[fə'rensɪks]	informatyka śledcza
digital evidence	['dɪʤɪtl 'evɪdəns]	dowody cyfrowe
chain of custody	[ʧeɪn əv 'kʌstədi]	łańcuch nadzoru nad dowodami

ANGIELSKI	TRANSKRYPCJA	TŁUMACZENIE
root cause analysis	[ruːt kɔːz əˈnælɪsɪs]	analiza przyczyny źródłowej
anomaly detection	[əˈnɒməli dɪˈtekʃn]	wykrywanie anomalii
behavioral analytics	[bɪˈheɪvjərəl ˌænəˈlɪtɪks]	analityka behawioralna
machine learning	[məˈʃiːn ˈlɜːnɪŋ]	uczenie maszynowe
false positive	[fɔːls ˈpɒzɪtɪv]	fałszywy alarm
false negative	[fɔːls ˈnegətɪv]	niewykryty przypadek
risk appetite	[rɪsk ˈæpɪtaɪt]	apetyt na ryzyko
risk mitigation	[rɪsk ˌmɪtɪˈgeɪʃn]	ograniczanie ryzyka
business continuity	[ˈbɪznəs ˌkɒntɪˈnjuːɪti]	ciągłość działania
disaster recovery	[dɪˈzɑːstə rɪˈkʌvəri]	odtwarzanie po awarii
ransomware attack	[ˈrænsəmweə əˈtæk]	atak ransomware
denial of service	[dɪˈnaɪəl əv ˈsɜːvɪs]	odmowa usługi
traffic spike	[ˈtræfɪk spaɪk]	skok ruchu sieciowego
botnet herder	[ˈbɒtnet ˈhɜːdə]	operator botnetu
malware analysis	[ˈmælweə əˈnælɪsɪs]	analiza złośliwego oprogramowania
sandboxing	[ˈsænbɒksɪŋ]	uruchamianie w piaskownicy
reverse engineering	[rɪˈvɜːs ˌendʒɪˈnɪərɪŋ]	inżynieria wsteczna
obfuscation	[ˌɒbfʌsˈkeɪʃn]	zaciemnianie kodu
packer	[ˈpækə]	packer
exploit kit	[ɪkˈsplɔɪt kɪt]	zestaw exploitów
drive-by download	[draɪv baɪ ˈdaʊnləʊd]	infekcja przez odwiedzenie strony
watering hole	[ˈwɔːtərɪŋ həʊl]	atak przez zaufaną stronę
supply chain attack	[səˈplaɪ ʧeɪn əˈtæk]	atak na łańcuch dostaw
insider threat	[ɪnˈsaɪdə θret]	zagrożenie wewnętrzne
data exfiltration	[ˈdeɪtə ˌeksfɪlˈtreɪʃn]	wyprowadzenie danych
lateral movement tool	[ˈlætərəl ˈmuːvmənt tuːl]	narzędzie ruchu bocznego
credential stuffing	[krɪˈdenʃl ˈstʌfɪŋ]	podstawianie wykradzionych danych

ANGIELSKI	TRANSKRYPCJA	TŁUMACZENIE
password spraying	['pɑːswɜːd 'spreɪɪŋ]	rozpylanie haseł
golden ticket	['gəʊldən 'tɪkɪt]	złoty bilet
domain controller	[də'meɪn kən'trəʊlə]	kontroler domeny
certificate pinning	[sə'tɪfɪkət 'pɪnɪŋ]	przypinanie certyfikatu
mutual TLS	['mjuːtʃuəl ˌtiː el 'es]	wzajemny TLS
public key infrastructure	['pʌblɪk kiː 'ɪnfrəˌstrʌkʧə]	infrastruktura klucza publicznego
key management service	[kiː 'mænɪʤmənt 'sɜːvɪs]	usługa zarządzania kluczami
hardware security module	['hɑːdweə sɪ'kjʊərɪti 'mɒdjuːl]	sprzętowy moduł bezpieczeństwa
data classification	['deɪtə ˌklæsɪfɪ'keɪʃn]	klasyfikacja danych
data retention	['deɪtə rɪ'tenʃn]	przechowywanie danych
data minimization	['deɪtə ˌmɪnɪmaɪ'zeɪʃn]	minimalizacja danych
secure by design	[sɪ'kjʊə baɪ dɪ'zaɪn]	bezpieczeństwo od projektu
threat modeling	[θret 'mɒdlɪŋ]	modelowanie zagrożeń
secure coding	[sɪ'kjʊə 'kəʊdɪŋ]	bezpieczne programowanie
code review	[kəʊd rɪ'vjuː]	przegląd kodu
static analysis	['stætɪk ə'nælɪsɪs]	analiza statyczna
dynamic analysis	[daɪ'næmɪk ə'nælɪsɪs]	analiza dynamiczna
vulnerability scanning	[ˌvʌlnərə'bɪlɪti 'skænɪŋ]	skanowanie podatności
patch management	[pæʧ 'mænɪʤmənt]	zarządzanie poprawkami
configuration drift	[kənˌfɪgjə'reɪʃn drɪft]	rozjazd konfiguracji
hardening	['hɑːdənɪŋ]	utwardzanie konfiguracji
secure baseline	[sɪ'kjʊə 'beɪslaɪn]	bezpieczna konfiguracja bazowa
policy enforcement	['pɒlɪsi ɪn'fɔːsmənt]	egzekwowanie polityki
access review	['ækses rɪ'vjuː]	przegląd uprawnień
segregation of duties	[ˌsegrɪ'geɪʃn əv 'djuːtiz]	rozdzielenie obowiązków
logging retention	['lɒgɪŋ rɪ'tenʃn]	przechowywanie logów

ANGIELSKI	TRANSKRYPCJA	TŁUMACZENIE
security telemetry	[sɪˈkjʊərɪti təˈlemətri]	telemetria bezpieczeństwa
endpoint protection	[ˈendpɔɪnt prəˈtekʃn]	ochrona urządzeń końcowych
endpoint detection and response	[ˈendpɔɪnt dɪˈtekʃn ənd rɪ ˈspɒns]	wykrywanie i reagowanie na urządzeniach końcowych
network forensics	[ˈnetwɜːk fəˈrensɪks]	analiza śledcza sieci
memory dump	[ˈmeməri dʌmp]	zrzut pamięci
log correlation	[lɒg ˌkɒrəˈleɪʃn]	korelacja logów
threat scoring	[θret ˈskɔːrɪŋ]	ocena zagrożeń
security posture	[sɪˈkjʊərɪti ˈpɒstʃə]	stan bezpieczeństwa
attack simulation	[əˈtæk ˌsɪmjʊˈleɪʃn]	symulacja ataku
breach notification	[briːtʃ ˌnəʊtɪfɪˈkeɪʃn]	zgłoszenie naruszenia
regulatory compliance	[ˈregjʊlətəri kəmˈplaɪəns]	zgodność regulacyjna
security awareness	[sɪˈkjʊərɪti əˈweənəs]	świadomość bezpieczeństwa
tabletop exercise	[ˈteɪbltɒp ˈeksəsaɪz]	ćwiczenie sztabowe
playbook	[ˈpleɪbʊk]	playbook
post-incident review	[pəʊst ˈɪnsɪdənt rɪˈvjuː]	analiza po incydencie
continuous monitoring	[kənˈtɪnjuəs ˈmɒnɪtərɪŋ]	ciągłe monitorowanie