onemoreword

Cybersécurité — Avancé

ANGLAIS	TRANSCRIPTION	TRADUCTION
threat actor	[θret ˈæktə]	acteur de la menace
attack vector	[əˈtæk ˈvektə]	vecteur d’attaque
attack surface	[əˈtæk ˈsɜːfɪs]	surface d’attaque
zero-day	[ˈzɪərəʊ deɪ]	zero-day
vulnerability management	[ˌvʌlnərəˈbɪlɪti ˈmænɪʤmənt]	gestion des vulnérabilités
penetration testing	[ˌpenɪˈtreɪʃn ˈtestɪŋ]	tests d’intrusion
pen test	[pen test]	pentest
red team	[red tiːm]	équipe rouge
blue team	[bluː tiːm]	équipe bleue
purple team	[ˈpɜːpl tiːm]	équipe violette
security operations center	[sɪˈkjʊərɪti ˌɒpəˈreɪʃnz ˈsentə]	centre des opérations de sécurité
lateral movement	[ˈlætərəl ˈmuːvmənt]	mouvement latéral
privilege escalation	[ˈprɪvɪlɪʤ ˌeskəˈleɪʃn]	élévation de privilèges
persistence	[pəˈsɪstəns]	persistance
command and control	[kəˌmɑːnd ən kənˈtrəʊl]	commande et contrôle
beaconing	[ˈbiːkənɪŋ]	beaconing
kill chain	[kɪl ʧeɪn]	chaîne d’attaque
threat intelligence	[θret ɪnˈtelɪʤəns]	renseignement sur les menaces
threat hunting	[θret ˈhʌntɪŋ]	threat hunting
incident response plan	[ˈɪnsɪdənt rɪˈspɒns plæn]	plan de réponse aux incidents
forensics	[fəˈrensɪks]	criminalistique numérique

ANGLAIS	TRANSCRIPTION	TRADUCTION
anomaly detection	[əˈnɒməli dɪˈtekʃn]	détection d’anomalies
behavioral analytics	[bɪˈheɪvjərəl ˌænəˈlɪtɪks]	analytique comportementale
machine learning	[məˈʃiːn ˈlɜːnɪŋ]	apprentissage automatique
false positive	[fɔːls ˈpɒzɪtɪv]	faux positif
false negative	[fɔːls ˈnegətɪv]	faux négatif
risk appetite	[rɪsk ˈæpɪtaɪt]	appétit pour le risque
risk mitigation	[rɪsk ˌmɪtɪˈgeɪʃn]	atténuation des risques
business continuity	[ˈbɪznəs ˌkɒntɪˈnjuːɪti]	continuité d’activité
disaster recovery	[dɪˈzɑːstə rɪˈkʌvəri]	reprise après sinistre
ransomware attack	[ˈrænsəmweə əˈtæk]	attaque par rançongiciel
denial of service	[dɪˈnaɪəl əv ˈsɜːvɪs]	déni de service
traffic spike	[ˈtræfɪk spaɪk]	pic de trafic
botnet herder	[ˈbɒtnet ˈhɜːdə]	opérateur de botnet
malware analysis	[ˈmælweə əˈnælɪsɪs]	analyse de malware
sandboxing	[ˈsænbɒksɪŋ]	sandboxing
reverse engineering	[rɪˈvɜːs ˌendʒɪˈnɪərɪŋ]	rétro-ingénierie
obfuscation	[ˌɒbfʌsˈkeɪʃn]	obfuscation
packer	[ˈpækə]	packer
exploit kit	[ɪkˈsplɔɪt kɪt]	kit d’exploits
drive-by download	[draɪv baɪ ˈdaʊnləʊd]	téléchargement furtif
watering hole	[ˈwɔːtərɪŋ həʊl]	attaque watering hole
supply chain attack	[səˈplaɪ ʧeɪn əˈtæk]	attaque de la chaîne d’approvisionnement
insider threat	[ɪnˈsaɪdə θret]	menace interne
data exfiltration	[ˈdeɪtə ˌeksfɪlˈtreɪʃn]	exfiltration de données

ANGLAIS	TRANSCRIPTION	TRADUCTION
golden ticket	[ˈgəʊldən ˈtɪkɪt]	golden ticket
domain controller	[dəˈmeɪn kənˈtrəʊlə]	contrôleur de domaine
certificate pinning	[səˈtɪfɪkət ˈpɪnɪŋ]	pinning de certificat
mutual TLS	[ˈmjuːtʃuəl ˌtiː el ˈes]	TLS mutuel
public key infrastructure	[ˈpʌblɪk kiː ˈɪnfrəˌstrʌktʃə]	infrastructure à clé publique
key management service	[kiː ˈmænɪdʒmənt ˈsɜːvɪs]	service de gestion des clés
hardware security module	[ˈhɑːdweə sɪˈkjʊərɪti ˈmɒdjuːl]	module matériel de sécurité
data classification	[ˈdeɪtə ˌklæsɪfɪˈkeɪʃn]	classification des données
data retention	[ˈdeɪtə rɪˈtenʃn]	conservation des données
data minimization	[ˈdeɪtə ˌmɪnɪmaɪˈzeɪʃn]	minimisation des données
secure by design	[sɪˈkjʊə baɪ dɪˈzaɪn]	sécurité dès la conception
threat modeling	[θret ˈmɒdlɪŋ]	modélisation des menaces
secure coding	[sɪˈkjʊə ˈkəʊdɪŋ]	codage sécurisé
code review	[kəʊd rɪˈvjuː]	revue de code
static analysis	[ˈstætɪk əˈnælɪsɪs]	analyse statique
dynamic analysis	[daɪˈnæmɪk əˈnælɪsɪs]	analyse dynamique
vulnerability scanning	[ˌvʌlnərəˈbɪlɪti ˈskænɪŋ]	analyse de vulnérabilités
patch management	[pætʃ ˈmænɪdʒmənt]	gestion des correctifs
configuration drift	[kənˌfɪgjəˈreɪʃn drɪft]	dérive de configuration
hardening	[ˈhɑːdənɪŋ]	durcissement
secure baseline	[sɪˈkjʊə ˈbeɪslaɪn]	configuration de base sécurisée
policy enforcement	[ˈpɒlɪsi ɪnˈfɔːsmənt]	application des politiques
access review	[ˈækses rɪˈvjuː]	revue des accès
segregation of duties	[ˌsegrɪˈgeɪʃn əv ˈdjuːtiz]	séparation des tâches

ANGLAIS	TRANSCRIPTION	TRADUCTION
endpoint detection and response	[ˈendpɔɪnt dɪˈtekʃn ənd rɪˈspɒns]	détection et réponse endpoints
network forensics	[ˈnetwɜːk fəˈrensɪks]	criminalistique réseau
memory dump	[ˈmeməri dʌmp]	dump mémoire
log correlation	[lɒg ˌkɒrəˈleɪʃn]	corrélation des journaux
threat scoring	[θret ˈskɔːrɪŋ]	score de menace
security posture	[sɪˈkjʊərɪti ˈpɒstʃə]	posture de sécurité
attack simulation	[əˈtæk ˌsɪmjʊˈleɪʃn]	simulation d’attaque
breach notification	[briːtʃ ˌnəʊtɪfɪˈkeɪʃn]	notification de violation
regulatory compliance	[ˈregjʊlətəri kəmˈplaɪəns]	conformité réglementaire
security awareness	[sɪˈkjʊərɪti əˈweənəs]	sensibilisation à la sécurité
tabletop exercise	[ˈteɪbltɒp ˈeksəsaɪz]	exercice sur table
playbook	[ˈpleɪbʊk]	playbook
post-incident review	[pəʊst ˈɪnsɪdənt rɪˈvjuː]	revue post-incident
continuous monitoring	[kənˈtɪnjuəs ˈmɒnɪtərɪŋ]	surveillance continue