onemoreword

Ciberseguridad — Avanzado

INGLÉS	TRANSCRIPCIÓN	TRADUCCIÓN
threat actor	[θret ˈæktə]	actor de amenazas
attack vector	[əˈtæk ˈvektə]	vector de ataque
attack surface	[əˈtæk ˈsɜːfɪs]	superficie de ataque
zero-day	[ˈzɪərəʊ deɪ]	zero-day
vulnerability management	[ˌvʌlnərəˈbɪlɪti ˈmænɪʤmənt]	gestión de vulnerabilidades
penetration testing	[ˌpenɪˈtreɪʃn ˈtestɪŋ]	pruebas de penetración
pen test	[pen test]	pentest
red team	[red tiːm]	equipo rojo
blue team	[bluː tiːm]	equipo azul
purple team	[ˈpɜːpl tiːm]	equipo púrpura
security operations center	[sɪˈkjʊərɪti ˌɒpəˈreɪʃnz ˈsentə]	centro de operaciones de seguridad
lateral movement	[ˈlætərəl ˈmuːvmənt]	movimiento lateral
privilege escalation	[ˈprɪvɪlɪʤ ˌeskəˈleɪʃn]	escalada de privilegios
persistence	[pəˈsɪstəns]	persistencia
command and control	[kəˌmɑːnd ən kənˈtrəʊl]	mando y control
beaconing	[ˈbiːkənɪŋ]	beaconing
kill chain	[kɪl ʧeɪn]	cadena de ataque
threat intelligence	[θret ɪnˈtelɪʤəns]	inteligencia de amenazas
threat hunting	[θret ˈhʌntɪŋ]	caza de amenazas
incident response plan	[ˈɪnsɪdənt rɪˈspɒns plæn]	plan de respuesta a incidentes
forensics	[fəˈrensɪks]	forense digital

INGLÉS	TRANSCRIPCIÓN	TRADUCCIÓN
anomaly detection	[əˈnɒməli dɪˈtekʃn]	detección de anomalías
behavioral analytics	[bɪˈheɪvjərəl ˌænəˈlɪtɪks]	analítica de comportamiento
machine learning	[məˈʃiːn ˈlɜːnɪŋ]	aprendizaje automático
false positive	[fɔːls ˈpɒzɪtɪv]	falso positivo
false negative	[fɔːls ˈnegətɪv]	falso negativo
risk appetite	[rɪsk ˈæpɪtaɪt]	apetito de riesgo
risk mitigation	[rɪsk ˌmɪtɪˈgeɪʃn]	mitigación de riesgos
business continuity	[ˈbɪznəs ˌkɒntɪˈnjuːɪti]	continuidad del negocio
disaster recovery	[dɪˈzɑːstə rɪˈkʌvəri]	recuperación ante desastres
ransomware attack	[ˈrænsəmweə əˈtæk]	ataque de ransomware
denial of service	[dɪˈnaɪəl əv ˈsɜːvɪs]	denegación de servicio
traffic spike	[ˈtræfɪk spaɪk]	pico de tráfico
botnet herder	[ˈbɒtnet ˈhɜːdə]	operador de botnet
malware analysis	[ˈmælweə əˈnælɪsɪs]	análisis de malware
sandboxing	[ˈsænbɒksɪŋ]	sandboxing
reverse engineering	[rɪˈvɜːs ˌendʒɪˈnɪərɪŋ]	ingeniería inversa
obfuscation	[ˌɒbfʌsˈkeɪʃn]	ofuscación
packer	[ˈpækə]	empaquetador
exploit kit	[ɪkˈsplɔɪt kɪt]	kit de exploits
drive-by download	[draɪv baɪ ˈdaʊnləʊd]	descarga furtiva
watering hole	[ˈwɔːtərɪŋ həʊl]	ataque watering hole
supply chain attack	[səˈplaɪ ʧeɪn əˈtæk]	ataque a la cadena de suministro
insider threat	[ɪnˈsaɪdə θret]	amenaza interna
data exfiltration	[ˈdeɪtə ˌeksfɪlˈtreɪʃn]	exfiltración de datos

INGLÉS	TRANSCRIPCIÓN	TRADUCCIÓN
password spraying	[ˈpɑːswɜːd ˈspreɪɪŋ]	pulverización de contraseñas
golden ticket	[ˈgəʊldən ˈtɪkɪt]	golden ticket
domain controller	[dəˈmeɪn kənˈtrəʊlə]	controlador de dominio
certificate pinning	[səˈtɪfɪkət ˈpɪnɪŋ]	fijación de certificado
mutual TLS	[ˈmjuːtʃuəl ˌtiː el ˈes]	TLS mutuo
public key infrastructure	[ˈpʌblɪk kiː ˈɪnfrəˌstrʌktʃə]	infraestructura de clave pública
key management service	[kiː ˈmænɪdʒmənt ˈsɜːvɪs]	servicio de gestión de claves
hardware security module	[ˈhɑːdweə sɪˈkjʊərɪti ˈmɒdjuːl]	módulo de seguridad hardware
data classification	[ˈdeɪtə ˌklæsɪfɪˈkeɪʃn]	clasificación de datos
data retention	[ˈdeɪtə rɪˈtenʃn]	retención de datos
data minimization	[ˈdeɪtə ˌmɪnɪmaɪˈzeɪʃn]	minimización de datos
secure by design	[sɪˈkjʊə baɪ dɪˈzaɪn]	seguridad desde el diseño
threat modeling	[θret ˈmɒdlɪŋ]	modelado de amenazas
secure coding	[sɪˈkjʊə ˈkəʊdɪŋ]	programación segura
code review	[kəʊd rɪˈvjuː]	revisión de código
static analysis	[ˈstætɪk əˈnælɪsɪs]	análisis estático
dynamic analysis	[daɪˈnæmɪk əˈnælɪsɪs]	análisis dinámico
vulnerability scanning	[ˌvʌlnərəˈbɪlɪti ˈskænɪŋ]	escaneo de vulnerabilidades
patch management	[pætʃ ˈmænɪdʒmənt]	gestión de parches
configuration drift	[kənˌfɪgjəˈreɪʃn drɪft]	deriva de configuración
hardening	[ˈhɑːdənɪŋ]	endurecimiento
secure baseline	[sɪˈkjʊə ˈbeɪslaɪn]	línea base segura
policy enforcement	[ˈpɒlɪsi ɪnˈfɔːsmənt]	aplicación de políticas
access review	[ˈækses rɪˈvjuː]	revisión de accesos

INGLÉS	TRANSCRIPCIÓN	TRADUCCIÓN
endpoint protection	[ˈendpɔɪnt prəˈtekʃn]	protección de endpoints
endpoint detection and response	[ˈendpɔɪnt dɪˈtekʃn ənd rɪ ˈspɒns]	detección y respuesta en endpoints
network forensics	[ˈnetwɜːk fəˈrensɪks]	forense de red
memory dump	[ˈmeməri dʌmp]	volcado de memoria
log correlation	[lɒg ˌkɒrəˈleɪʃn]	correlación de logs
threat scoring	[θret ˈskɔːrɪŋ]	puntuación de amenazas
security posture	[sɪˈkjʊərɪti ˈpɒstʃə]	postura de seguridad
attack simulation	[əˈtæk ˌsɪmjʊˈleɪʃn]	simulación de ataques
breach notification	[briːtʃ ˌnəʊtɪfɪˈkeɪʃn]	notificación de brecha
regulatory compliance	[ˈregjʊlətəri kəmˈplaɪəns]	cumplimiento regulatorio
security awareness	[sɪˈkjʊərɪti əˈweənəs]	concienciación de seguridad
tabletop exercise	[ˈteɪblˌtɒp ˈeksəsaɪz]	ejercicio de mesa
playbook	[ˈpleɪbʊk]	playbook
post-incident review	[pəʊst ˈɪnsɪdənt rɪˈvjuː]	revisión post-incidente
continuous monitoring	[kənˈtɪnjuəs ˈmɒnɪtərɪŋ]	monitoreo continuo