

序号	英文	中文
1	0day attack	0day攻击
2	AAA: Authentication, authorization, accounting	认证、授权、记录
3	access and authentication	访问和认证
4	Access Control	访问控制
5	Access Control Service	访问控制服务
6	access governance	访问管理
7	Access Matrix	访问矩阵
8	Access Method	访问方式
9	Accessibility Features	易用性函数
10	Account collision attack	撞库攻击
11	Account Harvesting	帐户收集
12	accountability	可追溯性
13	ACK Piggybacking	ACK捎带确认机制
14	ACL: Access Control List	访问控制列表
15	active attack	主动攻击
16	Active Content	动态内容
17	Active Data Dictionary	主动数据字典
18	Active Directory	活动目录
19	Activity Monitors	活动监视器、活动监控器
20	actuator	促进器【物联网设备中常用来指触发器或触发机制】
21	ADM: Application Data Management	应用数据管理
22	Administrative Templates	管理模板
23	Advanced Analytics	高级分析
24	Advanced Fraud Detection and Analysis Technologies	高级的欺诈检测与分析技术
25	Advanced targeted attacks	高级定向攻击

26	Advanced Threat Detection (ATD) Appliances	高级威胁检测设备
27	Advanced Web Services	高级网络服务
28	adversary	攻击者、敌方
29	AES: Advanced Encryption Standard	高级加密标准
30	aggregation	聚合
31	AI: Artificial Intelligence	人工智能
32	AIOps: Artificial Intelligence for IT Operations	智能化运维
33	Air-gapped	完全与互联网无连接的物理主机
34	alert	警报; 警告
35	Algorithm	算法
36	Algorithmic Business	算法业务
37	All-in-One (AIO) PCs	一体式电脑、一体机
38	ambiguous risk	未知风险
39	AMG: Access Media Gateways	媒体接入网关
40	ANSI: American National Standards Institute	美国国家标准学会
41	anti-evasion technologies	防绕过技术
42	anti-malware	防恶意软件
43	anti-virus	杀毒、防病毒
44	antivirus software	杀毒软件
45	AP: Access Point	接入点
46	APA: Applications Portfolio Analysis	应用组合分析
47	aPaaS: Application Platform as a Service	应用平台即服务
48	API Management	API 管理
49	API: Application programming interface	应用程序编程接口
50	APIs for automated provisioning	用于自动资源调配的API
51	Applet	小应用程序
52	application architects	应用架构师

53	Application Architecture	应用体系结构
54	Application Control	应用控制
55	Application Infrastructure	应用基础架构
56	Application Integration	应用集成
57	Application Obfuscation	应用加固
58	Application Outsourcing	应用外包
59	Application Performance Monitoring	应用性能监控
60	Application Program	应用程序
61	Application Release Automation	应用发布自动化
62	Application Server	应用服务器
63	Application Sharing	应用共享
64	Application Software Services	应用软件服务
65	application stack	应用程序栈
66	application-aware	应用感知
67	approval policy	允许策略
68	APT: Advanced Persistent Threat	高级持续性威胁
69	Architected Rapid Application Development	架构化快速应用程序开发
70	ARP: Address Resolution Protocol	地址解析协议
71	ARPANET: Advanced Research Projects Agency Network	高级研究计划局网络，简称阿帕网
72	ASCII: American Standard Code For Information Interchange	美国信息交换标准代码
73	Asset Performance Management	资产绩效管理
74	Asymmetric Warfare	不对称对抗
75	asynchronous procedure call	异步过程调用
76	Asynchronous Transmission	异步传输
77	ATM: Asynchronous Transfer Mode	异步传输模式

78	attack entry point	侵入点、攻击点
79	attack path	攻击路径
80	attack pattern	攻击模式
81	attack signature	攻击特征
82	attack surface	攻击面
83	Attack Surface Reduction	缩小攻击面
84	Attack vector	攻击向量
85	Audio Mining/speech Analytics	音频挖掘/语音分析
86	Auditing	审计
87	Augmented Analytics	增强分析
88	Augmented Intelligence	增强智能
89	Authentication	身份认证
90	Authentication Service	身份认证服务
91	Authentication Technologies	身份认证技术
92	Authenticity	真实性
93	Authorization	授权
94	autoElevate	自动提权
95	Automated Backup	自动备份
96	Automatic Restart	自动重启
97	Automatically programmed tool	自动编程工具
98	automatically updated	自动更新
99	Autonomous System	自治系统
100	Auto-Tiering: Automatic Storage Tiering	自动存储分层
101	Availability	可用性
102	Backbone Network	骨干网
103	Backbone Router	骨干路由器
104	Backdoor	后门

105	Background Task	后台任务
106	Backhaul	回传
107	backup	备份
108	Backup Server	备份服务器
109	Backup/recovery Software	备份/恢复软件
110	BAPI: Business Application Programming Interface	业务应用程序接口
111	baseline/benchmark	基线/基准
112	Basic Authentication	基本认证
113	BCMP: Business Continuity Management Planning	业务延续性管理计划（灾难重建计划【disaster recovery plan】中的一部分）
114	BCP: Business Continuity Planning	业务延续性计划
115	BEC: Business Email Compromise	商务电邮攻击；企业电子邮件攻击
116	behavior analytic techniques	行为分析技术
117	behavior data	行为数据
118	behavior monitoring	行为监控
119	Beta Testing	Beta测试
120	BGP: Border Gateway Protocol	边界网关协议
121	BIA: Business Impact Analysis	业务影响分析
122	Big Data	大数据
123	Bi-modal approach	IT交付的双模平衡（创新和系统稳定性的平衡）【Gartner有Definition】
124	Binary Code	二进制代码
125	binary copies	二进制副本
126	BIND: Berkeley Internet Name Domain	伯克利互联网域名
127	Biometric Authentication	生物特征身份认证
128	Biometric Characteristic	生物特征
129	Biometrics	生物认证信息（指纹、视网膜、人脸识别等）

130	BIOS: Basic Input/Output System	基本输入输出系统
131	Bit	比特、位
132	blacklist	黑名单
133	BLE: Behavior Learning Engines	行为学习引擎
134	Block Cipher	块状密码
135	Blockchain	区块链
136	Blue Team	蓝队（攻防演练中的防守方）
137	BOM: Bill of Materials	BOM清单
138	bot herder	僵尸网络操纵者
139	bot master	僵尸主人，僵尸网络操纵者的另一种称呼
140	Botnet	僵尸网络
141	BPA: Business Process Automation	业务流程自动化
142	BPM: Business Process Management	业务流程管理
143	BPO: Business Process Outsourcing	业务流程外包
144	BPR: Business Process Re-engineering	业务流程重组
145	BRE: Business Rule Engines	业务规则引擎
146	breach	失陷
147	Broadcast Address	广播地址
148	Browser	浏览器
149	Brute force	暴力破解
150	Buffer	缓冲区
151	Buffer Overflow	缓冲区溢出
152	build	构建
153	Business Analytics	商业分析
154	Business Intelligence (BI) Platforms	商业信息平台
155	Business Intelligence (BI) Services	商业信息服务
156	Business Process	业务流程

157	Business Process Analysis Tools	业务流程分析工具
158	Business Process As A Service	业务流程即服务
159	Business Process Management (BPM) Standards	业务流程管理标准
160	Business Process Modeling	业务流程建模
161	business process	业务流程
162	business unit	业务部门
163	BYOD: bring your own device	自带设备
164	Byte	字节
165	Cache	缓存
166	Cache Cramming	缓存填满
167	Cache Poisoning	缓存投毒、缓存中毒
168	Caching Server	缓存服务器
169	CARTA: Continuous Adaptive Risk and Trust Assessment	持续自适应风险与信任评估
170	CASB: cloud access security brokers	云访问安全代理
171	Cascading Faults	连锁故障
172	Case Management Solutions	场景管理解决方案
173	Certificate pinning	证书锁定
174	Certificate-Based Authentication	基于证书的身份认证
175	CGI: Common Gateway Interface	通用网关接口
176	Chain of Custody	监管链
177	Change Management	变更管理
178	CHAP: Challenge-Handshake Authentication Protocol	质询握手认证协议
179	Chatbot	聊天机器人
180	Check Digit	校验码

181	Checksum	校验和
182	CIA: confidentiality, integrity, availability	(数据的) 保密性、完整性、可用性
183	CIAM: Customer Identity and Access Management	客户身份与访问管理
184	CIFS: Common Internet File System	通用互联网文件系统
185	CIRP: Cyber Incident Response Plan	网络空间事件响应计划
186	CIRT: Cyber Incident Response Team	网络空间事件响应团队
187	CIS: Center for Internet Security	互联网安全中心
188	CISSP: Certified Information Systems Security Professional	信息系统安全认证专业人员
189	CKO: Chief Knowledge Officer	首席知识官
190	CLI: Common Language Infrastructure	公共语言基础设施
191	clickjacking	点击劫持
192	Clicks And Bricks	线上线下 (同时使用线上和实体店铺进行销售的销售模式)
193	Client	客户端
194	Client/server	客户端/服务端
195	Cloud Communications Service Provider	云通信服务提供商
196	Cloud Computing	云计算
197	Cloud Email	云电子邮件
198	Cloud Encryption Gateways	云加密网关
199	Cloud File Sharing	云文件共享
200	Cloud Security	云安全
201	Cloud Security Gateways	云安全网关
202	Cloud Service Elasticity	云服务弹性
203	Cloud sprawl	云端蔓延
204	Cloud Strategy	云战略
205	cloud users	云端用户

206	Cloud-based Grid Computing	基于云的网格计算
207	Cloudbursting	云爆发，公有云和私有云的一种协同机制，当私有云资源占用率为100%时将剩余的处理任务转移至公有云进行处理
208	Cluster Controller	集群控制器
209	Clustered System	集群系统
210	Clustering	聚类
211	CM: Content Management	内容管理
212	CM: Configuration Management	配置管理
213	CMP: cloud management platform	云管理平台
214	code injection	代码注入
215	coin miner software	挖矿软件
216	collection management system	采集管理系统
217	COM: Component Object Model	组件对象模型
218	Command and Control	命令与控制
219	Command and Control traffic	命令与控制流量
220	Command Line Transformation Utility	命令行转换实用程序
221	Common Information Model	通用信息模型
222	Common Vulnerability Enumeration	通用漏洞枚举
223	Community Cloud	社区云
224	compensating controls	补偿性控制，检查是否有能够替代弱点的其他的措施
225	Competitive Intelligence	竞争情报
226	compromise	入侵，通过攻击手段使某系统失陷
227	computer network defense	计算机网络防御
228	Computer-Integrated Manufacturing	计算机集成制造
229	Configuration Auditing	配置审计
230	Configuration Management	配置管理

231	console	控制台
232	Content Delivery Networks	内容分发网络
233	Content Management Systems	内容管理系统
234	Content-aware Data Loss Prevention (DLP)	基于内容感知数据防泄密
235	Context	上下文
236	Context Management Engine	上下文管理引擎
237	Context-aware Computing	上下文感知计算
238	Context-aware Security	上下文感知安全
239	Context-enriched Content	上下文内容丰富
240	Continuous Improvement	持续改进
241	Continuous Integration	持续集成
242	Continuous Operations	持续运营
243	Continuous Production	持续生产
244	correlating anomalies	异常关联
245	Corruption	损坏
246	Cost Benefit Analysis	投入产出分析
247	Course Of Action	行动方案
248	Covert Channels	隐蔽信道
249	CPE: Customer Premises Equipment	用户驻地设备（包括电话机、开关、电缆以及在顾客地点的其它硬件）
250	CPU: central processing unit	中央处理器
251	crawling file system	爬取文件系统
252	Credential Dumping	凭据转储
253	credentials	凭据
254	Crimeware	涉及犯罪的软件
255	Crisis/incident Management (C/IM) Software	危机/事件管理软件
256	critical infrastructure	关键基础设施
257	Cryptanalysis	密码分析

258	cryptographic algorithm	密码算法
259	cryptographic isolation	加密隔离
260	CSB: Cloud Services Brokerage	云服务代理
261	CSP: cloud service provider	云服务供应商
262	CSPM: cloud security posture management	云安全态势管理
263	CTI: cyber threat intelligence	网络威胁情报
264	CTO: Chief Technology Officer	首席技术官
265	Customer Information Management	客户信息管理
266	Customized Network Management	自定义网络管理
267	CVE: Common Vulnerabilities and Exposures	常见漏洞披露（一个平台和命名标准）
268	CWPP: cloud workload protection platforms	云工作负载保护平台
269	cyber ecosystem	网络生态系统
270	cyber incident	网络事件
271	cyber incident response plan	网络事件响应计划
272	cyber range	网络靶场
273	cyber teams	网络团队
274	cyberattack	网络攻击
275	cyberespionage	网络间谍行为
276	Cybersecurity	网络空间安全
277	Cybersecurity Policies	网络安全策略
278	cyberspace	网络空间
279	Cycle Time	周期时间
280	Daemon	守护进程
281	DAP: Directory Access Protocol	目录访问协议
282	DAST: Dynamic Application Security Testing	动态应用安全测试
283	Data Administration	数据管理
284	Data Aggregation	数据聚合

285	Data And Analytics	数据与分析
286	data at rest	静态数据
287	data breach	数据泄露
288	Data Broker	数据代理商
289	Data Center	数据中心
290	Data Center Storage Encryption	数据中心存储加密
291	data confidentiality	数据机密性
292	Data Custodian	数据管理员
293	Data Deduplication	重复数据删除
294	Data Dependency Mapping	数据依赖关系映射
295	Data Execution Prevention	数据执行保护, Windows XP之后的Windows版本中用于防止缓冲区溢出的一种保护机制
296	data exfiltration	数据泄露、数据渗出
297	Data Governance	数据治理
298	data in motion	动态数据
299	Data Integration	数据集成
300	data integrity	数据完整性
301	Data Lake	数据湖
302	data leakage	数据泄露
303	data loss	数据丢失
304	Data Mining	数据挖掘
305	Data Monetization	数据货币化
306	Data Ops	数据运维
307	Data Owner	数据拥有者
308	Data Profiling	数据剖析、数据概要分析
309	Data Quality Tools	数据质量工具
310	Data Replication	数据复制
311	Data Synchronization	数据同步

312	data theft	数据窃取
313	Data Warehouse	数据仓库
314	Data Wiping	数据擦除
315	Datagram	数据报
316	DBMS Management	DBMS管理
317	DBMS: Database Management System	数据库管理系统
318	DCB: Data Center Bridging	数据中心桥接
319	DCIM: Data Center Infrastructure Management	数据中心基础设施管理
320	DCO: Data Center Outsourcing	数据中心外包
321	DDoS Mitigation Services	DDoS缓解服务
322	DDoS: Distributed Denial of Service	分布式拒绝服务攻击
323	Decapsulation	解封装
324	Decision Intelligence	决策信息
325	Decryption	解密
326	Defacement	外观破坏（例如网站显示界面被替换）
327	defense in depth	纵深防御
328	Demand Forecasting	需求预测
329	Demand Pattern Analysis	需求模式分析
330	Denial of Service	拒绝服务攻击
331	Deployment	部署
332	DES: Data Encryption Standard	数据加密标准（一种对称性密码）
333	deviation	偏差
334	DevOps: development and operations	开发运维
335	DevOps-washing	DevOps洗白；旧瓶装新酒；生搬硬套组成新品
336	Dictionary Attack	字典遍历攻击
337	Diffie-Hellman	Diffie-Hellman密钥交换算法
338	Digest Authentication	摘要式身份验证

339	digital business	电子商务；数字化业务
340	Digital Certificate	数字证书
341	Digital Envelope	数字信封
342	Digital Forensics	数字取证
343	Digital Network	数字网络
344	Digital Security	数字化安全
345	Digital Signature	数字签名
346	Directory Services	目录服务
347	Discretionary Access Control	自主访问控制
348	Discretionary Access Control List	自由访问控制列表
349	Distance Vector	距离向量
350	Distributed Computing	分布式计算
351	Distributed Data Management	分布式数据管理
352	Distributed Database	分布式数据库
353	distributed digital technology	分布式数字技术
354	Distributed File Systems	分布式文件系统
355	Distributed Scans	分布式扫描
356	distributed sensor	分布式传感器
357	diverting attackers by using commercial honeypots	使用商业蜜罐让攻击者找不到目标
358	DLL: Dynamic Linkable Library	动态链接库
359	DLP: Data leakage prevention	数据防泄漏
360	DLP: data loss prevention	数据防泄密
361	DM: Data Management	数据管理
362	DMP: Data Management Platform	数据管理平台
363	DMZ: demilitarized zone	隔离区（提供外网服务，安全性较低）
364	DNS: domain name server	域名服务器

365	DNS: Domain Name System	域名系统
366	Domain Controller	域控制器
367	Domain fronting	域前置攻击
368	Domain Generation Algorithms	域生成算法
369	Domain Hijacking	域劫持攻击
370	Domain Name	域名
371	downstream function	下游功能
372	DPI: deep package inspection	深度数据包检测
373	DR: data recovery	数据恢复
374	DR: Disaster Recovery	灾难恢复
375	Drive-by Compromise	网站挂马攻击
376	drive-by pharming	偷渡式域欺骗
377	DRM: digital rights management	数字版权管理
378	DRP: Disaster Recovery Planning	灾难恢复计划
379	DSA: Digital Signature Algorithm	数字签名算法
380	DSS: Digital Signature Standard	数字签名标准
381	Dumpster Diving	垃圾搜索，去垃圾堆中搜索有用信息，属于社工的一种
382	Dynamic Business Process Management (BPM)	动态业务流程管理
383	Dynamic Content	动态内容
384	Dynamic Routing	动态路由
385	Dynamic Routing Protocol	动态路由协议
386	Dynamic Web Application Tools	动态Web应用工具
387	EA: Enterprise Architecture	企业体系架构
388	EAP: Extensible Authentication Protocol	可扩展认证协议
389	Eavesdropping	窃听
390	Edge	边缘
391	Edge Computing	边缘计算

392	EDR: endpoint detection and response	终端检测与响应
393	Egress Filtering	出站过滤
394	Elastic Multitenancy	弹性多租户
395	Electronic Signature (e-Signature)	电子签名
396	Electronic Waste (e-Waste)	电子垃圾
397	Embedded Analytics	嵌入式分析
398	Emotion Detection	情绪检测
399	Encapsulation	封装
400	Encryption	加密
401	encryption and tokenization	加密和令牌化
402	end-user organization	终端客户企业
403	end-user-facing desktops and laptops	终端台式机和笔记本
404	Enhanced Data Rate	增强数据传输速率
405	Enhanced Parallel Port	增强型并行端口
406	Enterprise Architecture (EA) Assurance	企业体系架构保障
407	Enterprise Architecture (EA) Tools	企业体系架构工具
408	enterprise information security charter	企业信息安全纲领/章程
409	Enterprise Network	企业网络
410	Ephemeral Port	临时端口
411	EPP: Endpoint protection platform	端点保护平台
412	escalate privileges	提权
413	Escrow Passwords	第三方保管的密码
414	ESI: Enterprise Security Intelligence	企业安全情报
415	Event, Fault And Log Management	事件、故障和日志管理
416	Exploit kit	漏洞利用工具包
417	exploit prevention	漏洞利用防御
418	Exploit Target	攻击目标

419	Exploitation	渗透攻击
420	Exploited in the Wild	在野攻击
421	Exterior Gateway Protocol	外部网关协议
422	External Audit	外部审计
423	false negative	漏报
424	false positive	误报
425	False Rejects	拒识
426	Fast File System	快速文件系统
427	fast flux	快速流量
428	Fast-packet Switching	快速分组交换
429	Fault Detection And Isolation	故障检测与隔离
430	Fault Line Attacks	故障线路攻击
431	file hash	文件哈希
432	File Server	文件服务器
433	FIM: file integrity monitoring	文件完整性监控
434	Firewall	防火墙
435	firewall and anti-virus	防火墙及杀毒
436	FMEA: Failure Modes Effects Analysis	失效模式和效果分析
437	footprinting	踩点
438	force multiplier	力量倍增器、效力增强系统
439	Forensic Analysis	取证分析
440	Forensic Software	取证软件
441	forensics	取证
442	Fork Bomb	fork炸弹攻击
443	Form-Based Authentication	基于表单的验证
444	Forward Lookup	正向搜索
445	forward proxy	正向代理

446	Fragment Offset	分片偏移
447	Fragment Overlap Attack	碎片交错攻击
448	Fragmentation	碎片化
449	Fraud Detection	欺诈检测
450	free during beta, fee-based at general availability	测试版免费，之后依据使用的功能收费
451	free full-volume encryption	免费全盘加密
452	full-packet capture solutions	全包捕捉解决方案，它是一种网络审计方法。
453	Fuzzing	模糊测试
454	Fuzzy Logic	模糊逻辑
455	FWaaS: Firewall as a Service	防火墙即服务
456	Gateway	网关
457	Gateway (Transcoding) Server	网关（转码）服务器
458	Gateway Server	网关服务器
459	GDPR: General Data Protection Regulation	通用数据保护条例（欧盟的一项条例）
460	go to a console	登录控制台
461	Golden Ticket	黄金票据
462	graphic display interface	图形显示界面
463	GRC: Governance, Risk and Compliance	治理、风险与合规
464	Grid Computing	网格计算
465	Grid Computing Without Using Public Cloud Computers	不使用公有云计算机的网格计算
466	Group Managed Service Accounts	组托管服务帐户
467	GUI: Graphical User Interface	图形化用户界面
468	hacker	黑客
469	Hardening	加固
470	Hardware And Software Maintenance Services	软硬件维保服务
471	HDD: Hard-Disk Drive	硬盘驱动器

472	Headless system	无外设设备（显示器、鼠标、键盘等）的主机
473	heterogeneous cloud environments	异构云环境 / 异构云平台
474	Hierarchical Storage	分层存储管理 (HSM) 系统
475	Hijack Attack	劫持攻击
476	HIPS: hosted intrusion prevention system	主机入侵防御系统
477	Honey pot	蜜罐
478	hopping attack	跳跃攻击
479	HSM: hardware security module	硬件安全模块
480	HTTP Public Key Pinning	HTTP 公钥固定/锁定
481	Human Augmentation	人工增强
482	human element	人为因素
483	Human Intelligence	人工情报
484	human middleware	人工介入、人工中介软件
485	hunting	狩猎
486	Hybrid Attack	混合攻击
487	Hybrid cloud	混合云
488	Hybrid Cloud Computing	混合云计算
489	Hybrid Encryption	混合加密
490	Hybrid Modeling	混合建模
491	Hype Cycle	炒作曲线（Gartner报告的一种）
492	Hyperlink	超链接
493	Hypertext	超文本
494	hypervisor	虚拟机监控器
495	I/O Bound	I/O 绑定
496	I/O Channel	I/O 通道
497	I/O: Input/Output	输入/输出
498	IaaS: Infrastructure as a service	基础设施即服务

499	IAM: Identity and Access Management	身份和访问管理
500	IAMS: identity access management system	身份验证与访问管理系统
501	ICMP: Internet Control Message Protocol	互联网控制消息协议
502	IDARS: Integrated Document Archive and Retrieval System	集成的文档存档和检索系统
503	IDC: Internet Data Center	网络数据中心
504	IDE: Integrated Development Environment	集成开发环境
505	identity cloning	身份克隆
506	identity fraud	身份欺诈
507	Identity Management	身份管理
508	identity services	身份验证服务
509	IDoT: Identity of Things	万物皆有身份，万物互联时代设备的身份信息
510	IDS: Intrusion Detection System	入侵检测系统
511	IETF: Internet Engineering Task Force	互联网工程任务组
512	ILM: Information Life Cycle Management	信息生命周期管理
513	image	镜像
514	IMAP: Internet Message Access Protocol	互联网邮件访问协议
515	immediately actionable intelligence	可操作情报
516	incident response	事件响应
517	incident response plan	事件响应计划
518	Incremental Backups	增量备份
519	Industrial Control System	工控系统
520	infected	感染病毒
521	Inference Attack	推理攻击
522	inflection point	拐点、转折点
523	Infocentric	能够将信息充分利用和掌控并当做一项重要资产的企业【Gartner有definition】
524	information and communication(s) technology	信息通信技术

525	Information Governance	信息治理
526	information security policy	信息安全策略
527	Information Warfare	信息战
528	infrastructural cloud	云基础设施
529	Ingress Filtering	入口过滤
530	initial access	(攻击过程中的) 初始访问
531	Input Validation Attacks	输入验证攻击
532	insider threat	内部威胁
533	instance-to-instance network connectivity	实例网络连接
534	integrated sensor	集成传感器
535	Integration as a Service	集成即服务
536	Integrity Star Property	完整性等级属性
537	intelligence-driven	以情报为驱动
538	intelligent electronic devices	智能电子设备
539	Internet Protocol Security	互联网协议安全
540	Intrusion Detection	入侵检测
541	intrusion protection system	入侵防御系统
542	IOCs: indicators of compromise	入侵迹象; 入侵指标; 失陷指标
543	IoE: Internet of Everything	万物互联或者万联网
544	IoT: Internet of things	物联网
545	IP: Internet Protocol	互联网协议
546	IPS: Intrusion Prevention System	入侵防御系统
547	IR: incident response	事件响应
548	IRM: Identity Relationship Management	身份关系管理
549	ISOC: intelligence-based security operation center	基于情报的安全运营中心
550	isolated point solutions	单点解决方案

551	ISP: internet service provider	网络服务供应商
552	ISV: independent software vendor	独立软件供应商
553	IT/OT Integration	IT/OT 集成
554	ITG: IT Governance	IT 治理
555	Job Scheduling	作业调度
556	Jump Lists	跳转列表
557	key management	密钥管理
558	key pair	密钥对
559	keylogger	键盘记录器
560	kill chain	杀伤链
561	Knowledge Assets	知识资产
562	Knowledge Base	知识库
563	known bad/ known good	黑白名单
564	LAN Bridging	局域网桥接
565	LAN: Local-Area Network	局域网
566	Latency	延迟
567	Lateral Movement	横向移动
568	LDAP: Lightweight Directory Access Protocol	轻量目录访问协议
569	Least Privilege	最小权限
570	legitimate traffic	正常的网络流量
571	licensing models	授权模式
572	link jacking	链接劫持
573	Link-Local Multicast Name Resolution	链路本地多播名称解析
574	live triage	实时分类
575	LM: log management	日志管理
576	Load Balancing	负载均衡
577	Loadable kernel module	可加载内核模块

578	log normalization	日志标准化
579	Logic bombs	逻辑炸弹
580	Logic Gate	逻辑门
581	M&A: Mergers and Acquisitions	并购
582	MAC: Mandatory Access Control	强制访问控制
583	MAC: Moves, Adds and Changes	移动、增加和更改
584	Machine Learning	机器学习
585	Magic Quadrant	魔力象限，一种Gartner报告
586	malicious files	恶意文件
587	malicious operations	恶意操作
588	Malware	恶意软件
589	Man in the Browser	浏览器中间人攻击
590	Managed Network Services	托管网络服务
591	Managed Object	托管对象
592	Masquerade	伪装
593	Masquerade Attack	伪装攻击
594	md5	单向加密哈希函数
595	memory scraping	内存刮取
596	memory	内存
597	Mesh Network	网状网络
598	Message Authentication	消息认证
599	Message Authentication Code	消息认证码
600	Metadata	元数据
601	metadata analysis	元数据分析
602	Metadata And Data Modeling Tools	元数据与数据建模工具
603	MFA: multi-factor authentication	多因素认证
604	Microsegmentation	微隔离

605	Microservice	微服务
606	microvisor	具有虚拟化功能的微核
607	Middleware	中间件
608	mitigation	缓解
609	modem	调制调解器
610	monitoring	监控
611	Morris Worm	莫里斯蠕虫病毒
612	moving target defense	移动目标防御
613	MRTI: machine-readable threat intelligence	可机读的威胁情报
614	MSP: Managed Service Provider	托管服务提供商
615	MSS: Managed security services	安全托管服务
616	MSSP: managed security service provider	安全托管服务提供商
617	MTTD: Mean Time to Detect	平均检测时间
618	MTTR: Mean Time to Respond	平均响应时间
619	Multiplexing	多路复用
620	multi-staged dropper	多阶段病毒
621	Multitenancy	多租户
622	Multithreading	多线程
623	mundane work	日常工作
624	NAC: Network Access Control	网络访问控制
625	named pipe	命名管道
626	name-space	命名空间
627	NAP: Network Access Point	网络接入点
628	NAS: Network-Attached Storage	接入网络的存储
629	Native encryption	本机加密
630	native integration	原生集成
631	native management console	原生控制面板

632	navigation workflow	导航流程
633	Network and System Management	网络与系统管理
634	Network Computing	网络计算
635	Network Configuration and Change Management (NCCM) Tools	网络配置和变更管理工具
636	Network Database	网络数据库
637	Network Fault Monitoring Tools	网络错误监控工具
638	network forensics	网络取证
639	Network Intelligence	网络情报
640	Network Interface Card	网卡
641	Network Inventory	网络资产
642	Network Management	网络管理
643	Network Management Center	网络管理中心
644	Network Operating System	网络操作系统
645	network protocol analysis	网络协议分析
646	Network Redundancy	网络冗余性
647	network resilience	网络弹性
648	Network Security	网络安全
649	network segmentation	网络分段
650	Network Sharing	网络共享
651	network tap	网络分流器
652	Network Topology	网络拓扑
653	network traffic	网络流量
654	Network Virtual Terminal	网络虚拟终端
655	Network Virtualization	网络虚拟化
656	Network/Host Artifacts	网络/主机工件
657	network-connected/power-on	联网或者开机状态

658	Neural Network	神经网络
659	new mindset	新观念
660	Next-generation Network	下一代网络
661	Nexus of forces	众力聚合。Gartner提出的概念，指的是社交网络+移动终端+云计算+信息 (social + mobile + cloud + information)之间大融合，成为数字业务的统一平台。
662	NFC: Near Field Communication	近场通信
663	NGFW: Next-generation Firewalls	下一代防火墙
664	NIST: National Institute of Standards and Technology	美国国家标准与技术研究所，原名为美国国家标准局
665	NLP: Natural-Language Processing	自然语言处理
666	NTA: network traffic analysis	网络流量分析
667	Object Data Model	对象数据模型
668	Object Instance	对象实例
669	Object Linking and Embedding	对象链接与嵌入
670	Object Request Broker	对象请求代理
671	Object Role Modeling	对象角色建模
672	OLAP: On-line analytical processing	联机分析处理技术
673	on-premise	本地
674	Open Architecture	开放式体系结构
675	Open Compute Project	开放计算项目
676	Open Source	开源
677	Open source intelligence	公源情报
678	Operating System	操作系统
679	operation hygiene	运维规范
680	Operational Data Store	操作数据存储
681	Operations Services	运营服务

682	operations staff	运维人员
683	Operations Support System	运维支持系统
684	orchestration	编排
685	origin server	原始服务器
686	OSA: Open Scripting Architecture	开放脚本框架
687	OSS: open-source software	开源软件
688	OT: Operational technology	工业控制技术
689	outsider threat	外部威胁
690	OWASP: Open Web Application Security Project	开源Web应用安全项目
691	PaaS: Platform as a service	平台即服务
692	packet capture	数据包捕获
693	packet sniffing	数据包嗅听、数据包监测
694	Packet Switching	报文分组交换
695	Packet-switched Network	包交换网络
696	PAD: Packet Assembler/Disassembler	封包组合及拆解器
697	PAM: Pulse Amplitude Modulation	脉幅调制
698	Pass the Hash	哈希传递攻击
699	Pass the Ticket	票据传递攻击
700	passive attack	被动攻击
701	Passive Data Dictionary	被动数据字典
702	Password Cracking	密码破解
703	Password Management Tools	秘钥管理工具
704	Password Sniffing	密码嗅探
705	password spraying	密码喷洒
706	payload analysis	载荷分析
707	payload	有效载荷
708	payment card skimmers	支付卡信息窃取工具（除了程序之外还有实体的磁条复制器）

709	PCI DSS: Payment card industry data security standard	支付卡行业数据安全标准
710	PCU: Packet Control Unit	分组控制单元
711	PDM: Product Data Management	产品数据管理
712	pen testing (penetration testing)	渗透测试
713	penetration	渗透
714	Performance Management	性能管理
715	perimeter	边界
716	perimeter defense	边界防御
717	perimeter firewall	边界防火墙
718	periphery	外围
719	persistence	持久化
720	Personal Cloud	个人云
721	Personalization Engines	个性化引擎
722	Pharming	域欺骗
723	Phishing	钓鱼攻击
724	phishing activity	钓鱼行为
725	physical control	实物管制、实地控制
726	physical firewall	物理防火墙
727	Physical Security	实体安全
728	PKI: Public-key Infrastructure	公钥基础设施
729	PLM: Product Life Cycle Management	产品生命周期管理
730	PMO: Project Management Office	项目管理办公室
731	PNFS: Parallel Network File System	并行网络文件系统
732	POC: proof of concept	概念验证
733	point product	终端产品、单点产品
734	Poison Reverse	毒性逆转

735	POP: Point of Presence	入网点
736	populate automatically	自动填写
737	port forwarding	端口转发
738	Port Knocking	端口碰撞
739	Portable Executable	可移植性可执行文件
740	Portal	门户
741	Portfolio Management	组合管理
742	post-compromise	失陷后的
743	posture	态势
744	power user	高权限用户
745	precision	精度
746	pre-compromised	失陷前的
747	pre-filtering	预过滤技术
748	Private Cloud Computing	私有云计算
749	Private Key	私钥
750	privilege escalation	提权
751	process kill	杀死进程、终止进程
752	process	进程
753	Product Support Services	产品支持服务
754	profile	配置文件
755	Program Compatibility Assistant	程序兼容性助手
756	Programmable Infrastructure	可编程的基础设施
757	Protected Process Light	受保护轻进程，一种从Windows 8开始引入的进程保护机制
758	Protocol	协议
759	Protocol Conversion	协议转换
760	Protocol Stack	协议栈
761	Proxy Agent	代理客户端

762	Proxy Server	代理服务器
763	proxy	代理
764	Public Cloud Computing	公有云计算
765	Public Key	公钥
766	Public-key Cryptography	公钥密码学
767	Publish/Subscribe Architecture	发布/订阅体系架构
768	pull or push information	提取或推送信息
769	purple team	紫队
770	Push Technology	推送技术
771	Pyramid of Pain	痛苦金字塔
772	QA: Quality Assurance	质量保证
773	QAM: Quadrature Amplitude Modulation	QAM正交振幅调制
774	QoS: Quality of Service	服务质量
775	Quantum Computing	量子计算
776	Ransomware	勒索软件
777	RASP: Runtime Application Self-protection	运行时应用自我保护机制
778	RAT: Remote access trojan	远程访问木马
779	raw socket	原始套接字
780	Real-time Analytics	实时分析
781	Reconnaissance	侦察、侦测
782	Red Team	红队
783	Registry	注册表
784	registry modifications	注册表修改
785	regression analysis	回归分析
786	Relational DBMS	关系型数据库管理系统
787	Remote Access	远程访问
788	Remote Control	远程控制

789	Remote Desktop Protocol	远程桌面协议
790	Remote Diagnostics	远程诊断
791	Remote Work	远程办公
792	Removable Media	可移动媒体
793	replication	副本
794	repository	仓库、存储库、资源库
795	reputation-based intelligence	信誉库
796	Resource Exhaustion	资源枯竭、资源耗尽
797	Response Time	响应时间
798	Reverse Engineering	逆向工程
799	Reverse Lookup	反向搜索
800	Reverse Proxy	反向代理
801	RFP: Request for proposal	招标书、征求建议书
802	Risk appetite	风险偏好
803	risk assessment	风险评估
804	Risk Averse	风险规避
805	Risk Management	风险管理
806	Risk Management And Compliance Consulting Services	风险管理与合规咨询服务
807	risk mitigation	风险缓解
808	risk modeling	风险建模
809	risk tolerance	风险容忍度
810	Role Based Access Control	基于角色的访问控制
811	RSA: Rivest-Shamir-Adleman	不对称密码算法
812	SaaS: Software as a Service	软件即服务
813	SAE: System Architecture Evolution	系统架构演进
814	SAM: Software Asset Management	软件资产管理

815	SAN: Storage Area Network	存储区域网络
816	sandbox	沙箱
817	SAST: Static Application Security Testing	静态应用安全测试
818	Scalability	可扩展性
819	Scanner	扫描器
820	SCCM: Software Change and Configuration Management	软件变更与配置管理
821	SCM: Software Configuration Management	软件配置管理
822	Scrambler	扰频器
823	Screen Sharing	屏幕共享
824	SDA: Software-Defined Architecture	软件定义的架构
825	SDK: Software Development Kit	软件开发包
826	SDN: Software Defined Network	软件定义的网络
827	SDP: Software Defined Protection	软件定义的防护
828	SD-WAN: Software-Defined WAN	软件定义的广域网
829	Search Engine	搜索引擎
830	secondary distribution network	二级网络
831	Secret Key	密钥
832	Secret-key Cryptography	私有秘钥密码学
833	secure boot	安全启动
834	Secure Web Gateway	Web安全网关
835	security control	安全管控
836	Security descriptors	安全描述符
837	Security Governance	安全治理
838	security perimeter	安全边界
839	security telemetry data	安全遥测数据
840	SEG: Secure email gateway	邮件安全网关

841	selection guidelines	选型原则
842	Self-defending network	自防御网络
843	Semantic analysis	语义分析
844	Semantic Data Model	语义数据模型
845	Semantic Nets	语义网络
846	Separation of Duties	职责分离
847	server workload	服务器工作负载
848	Service Inventory	服务清单
849	Service Mesh	服务网格
850	Service pack	服务包、补丁包
851	Session	会话
852	Session Hijacking	会话劫持
853	Session Key	会话密钥
854	severity and confidence	严重程度及可信度
855	shadow cloud	影子云
856	Shadow IT	影子IT
857	shared-service	共享服务
858	shipping soon	即将发售
859	shortlist	列入候选名单；确定名单
860	shoulder surfing	肩窥
861	S-HTTP: Secure Hypertext Transport Protocol	安全超文本传输协议
862	SI: system integrators	系统集成商
863	Side-Loading	侧加载
864	SIEM: security information and event management	安全信息和事件管理
865	signalling systems	信令系统
866	Signature	签名

867	Signature Verification	签名验证
868	signature-based anti-malware	基于特征码的反恶意软件程序
869	Silver Tickets	白银票据
870	situational awareness	态势感知
871	SLA: Service-level agreements	服务等级协议
872	Sliding Scale of Cyber Security	网络安全滑动标尺
873	Sniffer	嗅探器
874	SNMP: Simple Network Management Protocol	简单网络管理协议
875	SOA Governance Technologies	SOA治理技术, Gartner定义为一套用于执行治理 条例和政策的工具和技术
876	SOA: Service-oriented Architecture	面向服务的体系结构
877	SOAR: Security Orchestration, Automation and Response	安全编排、自动化和响应
878	SOC: Security operation center	安全运营中心
879	Social Engineering	社工
880	socket	套接字
881	Software Development	软件开发
882	Software Maintenance	软件维护
883	Software Restriction Policies	软件限制策略
884	Software-defined Networks	软件定义的网络
885	software-defined security mechanism	软件定义的安全机制
886	spam	垃圾邮件
887	spear phishing	鱼叉式网络钓鱼
888	SPI: stateful packet inspection	全状态数据包检查机制
889	Spider	爬虫
890	Spoofing	电子欺骗
891	spyware	间谍软件

892	SQL Injection: structured query language injection	SQL 注入攻击
893	SSH: Secure Shell	安全壳协议（用于远程管理UNIX计算机的一个网络协议）
894	SSL: Secure Sockets Layer	安全套接层
895	SSN: Switched Service Network	交换服务网络
896	SSO: Single Sign-on	单点登录
897	SSP: Storage Service Provider	存储服务供应商
898	Stack Mashing	栈溢出攻击
899	startup folders, drivers and bootloader	启动目录、驱动和引导装载程序
900	Stateful Inspection	状态检测
901	steering committee	指导委员会
902	sticky keys	粘滞键
903	strategic reach	战略影响
904	strong authentication	强认证机制
905	Strong Star Property	强星属性安全规则
906	Subnet	子网
907	Subnet Mask	子网掩码
908	Subnet Number	子网号
909	subscription-based pricing model	订阅收费模式
910	supply chain	供应链
911	Supply chain management	供应链管理
912	SWG: secure Web gateways	安全门户
913	Switched Line	交换线路
914	Switched Network	交换网络
915	Switching Center	交换中心
916	Symmetric Cryptography	对称加密算法
917	SYN Flood	SYN 泛洪攻击

918	Synchronous Communications	同步通信
919	Synchronous Network	同步网络
920	Synchronous Transmission	同步传输
921	Syntax	语法
922	system design philosophy	系统设计原则
923	System Integration	系统集成
924	System Management	系统管理
925	tab nabbing	标签钓鱼攻击
926	targeted attack	定点攻击
927	TCO: Total Cost of Ownership	总持有成本
928	technology steward	技术管理员
929	templates and scripts	模板和脚本
930	test for vulnerabilities	脆弱性测试
931	Text Mining	文本挖掘
932	Text Retrieval	文本检索
933	TGT: Ticket Granting Ticket	票据授予票据
934	Thread Execution	线程执行
935	Thread Local Storage	线程本地存储（线程局部存储）
936	Threat Actor	威胁主体
937	Threat Assessment	威胁评估
938	threat detection capabilities	威胁检测能力
939	Threat hunter	威胁猎人
940	Threat hunting	威胁狩猎
941	Threat Model	威胁模型
942	Threat Modeling	威胁建模
943	Threat Vector	威胁向量
944	threshold	阈值

945	TI: threat intelligence	威胁情报
946	ticketing system	工单系统
947	Time to Live	存活时间
948	timeline	时间线
949	TIP: Threat Intelligence Platform	威胁情报平台
950	TLS: Transport Layer Security	传输层安全
951	token	令牌
952	Tokenization	令牌化
953	tooling integration	工具集成
954	toolkit	工具包
955	Track And Trace	追溯
956	tracking	追踪
957	triage	(威胁) 分级、分类
958	Trojan Horse	特洛伊木马
959	Trunking	链路聚集
960	TSP technical specification	技术参数
961	TTPs: Tactics, Techniques & Procedures	战术、技术 & 步骤
962	TVM: threat and vulnerability managment	威胁和漏洞管理
963	Typosquatting	误植域名 (URL劫持) 攻击
964	UEBA: User and entity behavior analytics	用户和实体行为分析
965	unifying taxonomy	统一分类法
966	Universal Naming Convention	通用命名规则
967	USB ports	USB端口
968	use case	用例
969	User Authentication Technologies	用户身份验证技术
970	User Provisioning	用户开通
971	utility	实用程序

972	UTM: Unified Threat Management	统一威胁管理
973	UXP: User Experience Platforms	用户体验平台
974	VDI: virtual desktop infrastructure	虚拟桌面基础设施
975	virtual machine	虚拟机
976	virtual memory	虚拟内存; 虚拟存储器
977	visibility gap	可视化差距
978	Visualization	可视化
979	Volume Boot Record	卷引导记录
980	VPN concentrators	VPN 集中器
981	VPN: Virtual Private Network	虚拟专用网络
982	vulnerability management tools	漏洞管理工具
983	vulnerability scoring	漏洞评级
984	WAF: Web application firewall	Web应用防火墙
985	watchlists	监视列表
986	watering hole attack	水坑式攻击
987	Weakness	缺陷/弱点
988	Web Crawler	网络爬虫
989	web gateway	网关
990	Web Server	网络服务器
991	Web Services	网络服务
992	Web Services Software	网络服务软件
993	White Team	白队
994	whitelist	白名单
995	Windows Event Forwarding	Windows事件转发
996	workflow	workflow
997	Worm	蠕虫
998	Zombies	僵尸

999 ZTNA: Zero Trust Network Access

零信任网络访问