# \_

|  |  |
| --- | --- |
| \_Default | 5:39, 5:44-45, 5:58-60, 5:63, 5:71-72, 5:135 |
| \_Required | 5:39, 5:44-45, 5:58-60, 5:63, 5:71 |

# A

|  |  |
| --- | --- |
| Access Key | 2:97-100, 3:46, 3:48-50, 3:71, 4:34 |
| accessKeyID | 1:16, 1:18, 3:43, 3:45-46, 3:67, 3:82, 3:117, 3:126, 4:34 |
| accountName | 2:100 |
| Acquire Volatile Memory for Linux (AVML) | 3:153 |
| actAs | 5:24, 5:27 |
| Activity Reports | 4:77 |
| Add-MailboxPermission | 1:71 |
| ADFS | 1:107-108, 1:112, 2:46 |
| Advanced Persistent Threat (APT) | 4:135, 4:151 |
| Amazon Machine Image (AMI) | 3:68, 3:81, 3:147, 3:149, 3:153 |
| Amazon Resource Name (ARN) | 1:18, 3:9, 3:11, 3:34-35, 3:37-40, 3:42-45, 3:67 |
| Analytics Tab | 1:20, 1:22, 1:25 |
| Andromeda | 5:129 |
| anti-malware | 4:134 |
| API Calls | 1:118, 1:127-128, 1:133, 3:13-14, 3:16-20, 3:25-26, 3:29-30, 3:32, 3:47, 3:50-51, 3:53, 3:55, 3:109, 4:77, 5:40 |
| API Key | 1:45, 3:12, 3:22-24, 3:30, 3:40-41, 3:44-51, 3:53, 3:55, 3:67, 3:71, 3:151, 4:12, 5:22, 5:24 |
| Append blobs | 2:94 |
| Application Gateway | 2:80 |
| Application Load Balancer (ALB) | 3:96, 3:98 |
| APT | 4:135, 4:151 |
| Arkime | 5:140 |
| AssumedRole | 3:35, 3:85 |
| Athena | 3:27, 3:57, 3:88, 3:114, 3:123, 3:125-130, 3:149 |
| ATT&CK | 2:95, 2:132, 4:25, 4:30-31, 4:92, 4:96-97, 4:101 |
| AWS Audit Manager | 3:7 |
| AWS Detective | 3:27, 3:55 |
| AWS GuardDuty | 3:32, 3:55, 3:58-59, 3:124, 3:131, 3:133, 3:136, 3:138, 3:142-144 |
| AWS Lambda | 1:41, 3:142 |
| AWS Systems Manager | 3:146, 3:150-152 |
| AWSAccount | 3:35 |
| awsRegion | 1:16-17, 3:34, 3:43, 3:45, 3:68, 3:82, 3:86, 3:117 |
| AWSService | 3:35, 3:40, 3:85 |
| az | 1:46, 1:82, 2:12-13, 2:38, 3:101 |
| AzCopy | 2:94, 2:100, 2:126 |
| Azure Active Directory (AAD) | 1:57, 1:107, 2:4 |
| Azure Defender | 2:128 |
| Azure Functions | 1:41 |
| Azure Kubernetes Service (AKS) | 3:4, 4:3, 4:17-18, 4:20, 4:22 |
| Azure Monitor | 2:106, 4:20, 4:22 |
| Azure Portal | 1:79, 1:108, 2:6, 2:14, 2:18-19, 2:22, 2:24, 2:26, 2:43-45, 2:112, 2:132 |
| Azure Private Link | 2:96 |
| Azure Security Center | 2:49, 2:128 |
| Azure Sentinel | 2:122, 2:128-129 |
| Azure Storage | 2:18, 2:57-58, 2:60, 2:62, 2:92, 2:94, 2:99-100, 2:106, 2:108-109, 2:118 |
| Azure Storage Explorer | 2:18, 2:57-58, 2:60, 2:62, 2:92, 2:94, 2:99-100, 2:108-109, 2:118 |
| AzureActiveDirectory | 1:56-57, 1:69, 1:110-111, 1:131 |
| AzureActivity | 2:54-56 |

# B

|  |  |
| --- | --- |
| Beats | 1:13, 1:15 |
| Billing | 2:4, 2:71, 3:8, 3:100, 4:53, 5:5, 5:44-45, 5:59, 5:105, 5:121-122 |
| Bind | 1:77-81, 1:85-86, 1:133, 5:13, 5:15, 5:30-31 |
| Blob | 1:51, 2:20, 2:58-62, 2:92-95, 2:97-98, 2:100, 2:108, 2:120, 2:126, 5:52 |
| Blob Storage | 1:51, 2:93-94 |
| Block blobs | 2:94 |
| boto | 1:46, 3:51, 3:139 |
| Buckets | 2:34, 3:9, 3:13, 3:16, 3:18-19, 3:27-28, 3:33, 3:99-100, 3:107-109, 3:111-114, 3:117-118, 3:124, 3:128-130, 3:133, 3:138, 4:156, 5:4, 5:14, 5:46, 5:54, 5:58-59, 5:63, 5:71, 5:105, 5:107, 5:109-111, 5:113-115, 5:118, 5:121 |
| Business Email Compromise (BEC) | 1:70, 1:91-92, 4:99, 4:137 |

# C

|  |  |
| --- | --- |
| callerIpAddress | 1:76, 2:23, 2:26, 2:30, 2:32-33, 2:35-36, 2:82, 2:100 |
| Chat | 1:118, 1:124, 4:75, 4:95, 4:120 |
| Chronicle | 1:11 |
| Cloud Flows | 1:39, 1:43, 1:48 |
| Cloud Functions | 1:41, 1:51 |
| Cloud Identity | 5:3-4, 5:9-10 |
| Cloud Pub/Sub | 1:51, 5:58, 5:73-74, 5:77 |
| Cloud Virtual Network | 1:51, 5:127 |
| Cloud-Controller-Manager | 4:12 |
| CloudBerry | 3:31 |
| CloudTrail | 1:15, 1:51, 3:2-4, 3:25-36, 3:41-48, 3:51, 3:55, 3:57-60, 3:62, 3:65, 3:67-70, 3:72, 3:76, 3:82-83, 3:85-87, 3:109, 3:113-114, 3:117, 3:120, 3:124-125, 3:127-130, 3:133, 3:136, 3:138, 3:150, 3:152 |
| CloudTrail Insights | 3:3, 3:32-33, 3:124 |
| CloudWatch | 1:51, 3:25, 3:88, 3:100, 3:103, 3:124, 3:129, 3:138, 4:23 |
| Coldsnap | 3:80 |
| Collection | 1:3, 1:13, 1:20, 1:25, 1:68, 1:92, 1:107, 2:11, 2:132, 3:91, 3:114-115, 3:142-143, 3:154, 4:73, 4:79, 4:85, 4:89-91, 4:97, 5:3, 5:12, 5:37, 5:80, 5:96, 5:105, 5:126 |
| Command line (CLI) | 1:46, 1:117, 2:6, 2:10, 2:13-14, 2:38, 2:44-45, 2:98, 2:132, 3:23, 3:30-31, 3:36, 3:44, 3:47, 3:49, 3:55, 3:79, 3:81, 3:83, 3:117, 3:150, 4:28, 4:31, 4:97, 5:37, 5:66-72, 5:78, 5:88 |
| Compute Engine | 1:51, 5:20, 5:25, 5:83-84, 5:87, 5:89, 5:97, 5:140 |
| Consent | 1:110, 1:112, 1:119, 1:121, 1:124-125, 2:28, 2:131, 4:85, 4:89, 4:95, 4:152 |
| Console | 1:46, 1:108, 1:117, 1:120, 1:122, 2:98, 2:114, 3:18, 3:23-25, 3:27, 3:29-31, 3:36, 3:41-48, 3:51, 3:55, 3:65-66, 3:68, 3:72, 3:103, 3:112, 4:53-54, 4:56-58, 4:61, 4:63, 4:65, 4:69-70, 4:75-77, 4:105-107, 4:110, 4:114-115, 4:117, 4:119, 4:134, 4:140, 4:146, 4:149, 4:157, 4:162, 4:165, 4:173, 4:175, 4:185, 5:6, 5:8, 5:18, 5:40, 5:62, 5:66, 5:97, 5:118 |
| Console Access | 3:36, 3:45, 3:55, 5:40 |
| Console Login | 3:43, 3:47, 5:40 |
| Containers | 1:39, 1:41-42, 2:62, 2:97, 2:108, 3:9, 3:84, 3:149, 4:5-11, 4:13, 4:15-17, 4:24-25, 4:29, 4:39-41 |
| Control Plane | 1:9, 3:26-27, 3:120, 4:11-17, 4:23-24, 4:30-31, 4:34-39 |
| correlationId | 2:23, 2:26, 2:30, 2:32-33, 2:35-37, 2:72, 2:82 |
| createDate | 3:46 |
| CrowdStrike Reporting Tool (CRT) | 1:134 |
| Crypto Mining | 2:21, 2:68, 2:74, 2:76, 2:117, 4:39, 5:86 |
| Customer-managed encryption keys (CMEK) | 5:59 |
| Cyber Duck | 3:31 |

# D

|  |  |
| --- | --- |
| Dashboard | 1:12-13, 1:20-22, 1:25-26, 1:33, 1:35-36, 3:29, 3:52, 3:100, 3:150, 4:136, 5:141 |
| Data Event | 3:26, 3:28, 3:30, 3:33, 3:120 |
| Data Transfer | 1:49-50, 2:71, 3:65, 3:77, 3:100, 4:180 |
| Defender | 2:34, 2:49, 2:128, 4:25, 4:151 |
| Defense Evasion | 4:96 |
| Detective | 3:27, 3:55, 3:123, 3:131-133, 3:142 |
| deviceName | 2:33, 3:76 |
| Discover tab | 1:22 |
| Docker | 1:41-42, 4:29 |

# E

|  |  |
| --- | --- |
| Elastic Block Store (EBS) | 1:51, 3:9, 3:16, 3:62, 3:66, 3:74-77, 3:79, 3:81, 3:83-84, 3:143, 3:148 |
| Elastic Common Schema | 1:11 |
| Elastic Compute Cloud (EC2) | 3:63 |
| Elastic File Store (EFS) | 1:51, 3:62, 3:71, 3:84-87, 3:93 |
| Elastic Kubernetes Service (EKS) | 3:129, 4:3, 4:17, 4:23 |
| Elastic Stack | 1:12-14 |
| Elasticsearch | 1:13, 1:31 |
| Enumeration | 3:51-52, 5:113-114 |
| etcd | 4:12 |
| ETW events | 2:106 |
| Event Hub | 1:51, 1:108, 2:18-19, 2:63-66, 2:93, 2:95, 2:101, 2:106, 4:18 |
| Event logs | 2:106-109, 2:111, 3:25, 3:88, 5:40, 5:44, 5:59, 5:115, 5:134 |
| Event Tracing for Windows (ETW) | 2:106, 2:120 |
| Event Triggers | 3:135, 3:140, 3:142 |
| EventBridge | 3:136, 3:143-144 |
| eventID | 1:17, 2:115, 3:36 |
| eventName | 1:16-17, 3:34, 3:43, 3:45, 3:68, 3:82, 3:86, 3:117 |
| eventSource | 1:16-17, 3:34, 3:43, 3:45, 3:68, 3:82, 3:86, 3:117 |
| eventTime | 2:118, 3:34, 3:42-45, 3:68, 3:82, 3:86, 3:117 |
| eventType | 1:17, 3:36 |
| Exchange | 1:31, 1:53-54, 1:56-57, 1:60-61, 1:69-74, 1:76, 1:78-81, 1:83-91, 1:98, 1:102, 1:107, 1:112, 1:116, 1:133-134, 4:145, 4:147 |
| Exchange Mailbox | 1:72-73, 1:89 |
| Exchange Online | 1:60, 1:90-91, 1:112, 1:116, 1:134 |
| Exclusions | 5:7, 5:57, 5:62 |
| Execution | 1:59, 2:116, 3:52, 3:55, 3:137-138, 3:140-141, 3:151, 4:22, 4:29, 4:96, 5:32 |
| Exfiltration | 2:21, 2:68, 2:95, 2:98-100, 2:102-103, 4:54, 4:68, 4:82, 4:103, 5:121 |
| Exposed API Keys | 3:51 |
| ExpressRoute | 2:78 |

# F

|  |  |
| --- | --- |
| FederatedUser | 3:35 |
| File Storage | 1:51, 2:21, 2:93, 5:107 |
| File Transfer Protocol (FTP) | 2:81 |
| File-based logs | 2:106 |
| FileAccessed | 1:57, 1:95-96, 1:101, 1:103-104 |
| FilePreviewed | 1:95-96 |
| Firewall | 1:45, 2:79-80, 3:16-17, 3:63, 3:91-92, 3:95-96, 3:103, 3:139, 4:37, 5:26, 5:126, 5:128-131, 5:133-139, 5:141 |
| Firewall Rules | 3:91-92, 3:96, 3:103, 5:26, 5:126, 5:128, 5:130-131, 5:134-139 |
| Flow logs | 1:15, 1:27, 1:42, 1:45, 1:48, 2:68, 2:79, 2:84-87, 2:89-90, 2:102, 3:2, 3:4, 3:11, 3:72, 3:87, 3:90, 3:92, 3:94-96, 3:99-100, 3:106, 3:113-114, 3:124, 3:129-130, 3:133, 3:142, 4:37-38, 4:137, 5:62, 5:104, 5:124, 5:126, 5:128, 5:132-134, 5:138, 5:141 |
| Forms | 1:4, 1:13, 1:79, 1:111, 2:5, 2:119, 3:58, 4:12, 4:15, 4:101, 4:103, 4:114, 4:149, 4:184, 5:7, 5:43, 5:58-59, 5:95, 5:140 |
| Functions | 1:41, 1:51, 1:67, 1:119, 3:14, 3:16-17, 3:26, 3:29-30, 3:47, 3:135-137, 3:139, 3:141, 3:144, 4:12, 4:51, 4:56-57, 4:87, 5:11 |

# G

|  |  |
| --- | --- |
| gcloud | 1:46, 5:40, 5:56, 5:58, 5:66-72, 5:88, 5:97 |
| GCPBucketBrute | 5:113-114 |
| Get-AzLog | 2:38, 2:75 |
| GitHub | 1:1, 1:10, 1:112, 1:116-117, 2:74, 2:92, 2:101, 2:109, 3:30, 3:41, 3:52, 3:80, 3:129, 3:153, 4:40, 4:92-93, 4:96-97, 5:27, 5:71, 5:113-114 |
| Globally Unique Identifier (GUID) | 1:76, 1:128-129, 2:9, 2:23, 2:30, 2:35 |
| Glue | 2:78, 3:57, 3:114, 3:123, 3:125-128, 3:130, 4:10 |
| Gmail | 1:133, 1:141, 2:134, 3:1, 3:156, 4:58, 4:106-117, 4:120-121, 4:123-127, 4:129-135, 4:137, 4:150-151, 4:156, 4:180, 4:182, 4:187, 5:12 |
| Gmail Export | 4:129-133 |
| Google Cloud CLI | 5:68-72 |
| Google Cloud Compute | 5:4, 5:81-83 |
| Google Cloud Functions | 1:41 |
| Google Cloud IAM | 5:3, 5:11-15, 5:17-18, 5:20, 5:22, 5:24-35 |
| Google Cloud Identity and Access Management | 5:3-4, 5:9 |
| Google Cloud Logging Platform | 4:24, 5:4, 5:45 |
| Google Cloud Networking | 5:4, 5:129-131 |
| Google Cloud Storage Buckets | 5:4, 5:105, 5:114 |
| Google Docs (GDocs) | 4:150 |
| Google Drive (GDrive) | 4:50, 4:68, 4:77, 4:121, 4:151-152, 4:160, 4:162, 4:164-165, 4:167, 4:169, 4:171-176, 4:182-183, 4:186 |
| Google Group | 4:53, 4:107 |
| Google Groups | 4:53, 4:107 |
| Google Kubernetes Engine (GKE) | 4:17, 4:24, 4:28, 4:30-32, 4:35-36, 5:25, 5:140 |
| Google Ops | 5:95, 5:99-101, 5:103 |
| Google Sheets (GSheets) | 4:171 |
| Google Takeout | 4:54, 4:180 |
| Google Unified Data Model | 1:11 |
| Google Vault | 4:50, 4:54, 4:58, 4:75, 4:99, 4:106, 4:115, 4:118-123, 4:126-127, 4:129, 4:133 |
| Graph API | 1:7-8, 1:12, 1:38-39, 1:46, 1:52-53, 1:76, 1:80, 1:108, 1:114-120, 1:126-129, 1:131-134, 1:136-140, 2:14, 2:18, 2:46, 2:63, 2:66, 2:98, 2:131 |
| Groups | 1:107, 1:135, 2:3-4, 2:7, 2:68, 3:66, 3:91, 3:95, 3:139, 4:44, 4:51, 4:53, 4:58, 4:68-71, 4:82, 4:107, 4:120, 4:156, 4:180, 5:18 |
| gRPC | 1:46 |
| GSheet | 4:79, 4:107, 4:171-172, 4:174 |
| GuardDuty | 3:32, 3:55, 3:58-59, 3:124, 3:131, 3:133, 3:136, 3:138, 3:142-144 |

# H

|  |  |
| --- | --- |
| HardDelete | 1:72 |
| hypervisor | 1:9, 1:47, 3:77, 4:5 |

# I

|  |  |
| --- | --- |
| IAM | 1:9, 1:19, 1:42, 1:45, 1:107, 1:122, 1:139, 2:26, 3:3, 3:5-6, 3:9, 3:11-18, 3:21-24, 3:34-35, 3:38-43, 3:45-46, 3:48-49, 3:51, 3:53, 3:55, 3:63, 3:65, 3:67, 3:71, 3:82, 3:109-110, 3:117, 3:130, 3:150-151, 4:33-34, 5:3, 5:7, 5:9-18, 5:20, 5:22, 5:24-35, 5:68, 5:73, 5:111, 5:114, 5:118 |
| IAM Policy Simulator | 3:21 |
| IAM Roles | 3:13-14, 3:17, 3:23-24, 3:55, 3:63, 3:71, 3:109, 3:150, 4:33-34, 5:24, 5:27 |
| IAMUser | 3:35, 3:82, 3:117 |
| ID Prefixes | 3:49-50 |
| Identity | 1:9, 1:16, 1:18, 1:45, 1:107-110, 1:137, 1:139, 2:4, 2:20, 2:25, 2:36, 2:46-47, 2:60, 2:82, 2:100, 2:113, 3:11, 3:15, 3:34-35, 3:43, 3:45, 3:53, 3:67, 3:71, 3:82, 3:117, 3:126, 4:51, 4:53, 4:83, 4:156, 5:3-4, 5:7, 5:9-12, 5:16, 5:18, 5:40, 5:71-72, 5:110 |
| Identity and Access Management (IAM) | 1:9, 1:42, 1:45, 1:107, 2:4, 3:3, 3:5-6, 3:9, 3:11-18, 3:21-24, 3:34-35, 3:38-43, 3:46, 3:48-49, 3:51, 3:55, 3:63, 3:65, 3:67, 3:71, 3:82, 3:109-110, 3:130, 3:150-151, 4:33-34, 5:3-4, 5:7, 5:9-18, 5:20, 5:22, 5:24-35, 5:40, 5:68, 5:73, 5:111, 5:114 |
| imageId | 3:68 |
| Impact | 1:47, 1:49, 1:83, 2:4, 2:56, 2:69, 2:80, 3:6, 3:22, 3:63, 4:33, 4:54-55, 4:77, 4:110-111 |
| Infrastructure as a Service (IaaS) | 1:40, 4:46, 5:82, 5:95 |
| Initial Access | 4:96 |
| Internet Gateway | 3:90-92, 3:94, 3:98-99 |
| Internet Information Services (IIS) | 2:20-21, 2:105-107, 2:120, 3:88 |
| Internet Message Access Protocol (IMAP) | 1:74, 1:78-79, 1:86 |
| Investigator Tool | 4:114, 4:154, 4:167, 4:169, 4:171 |

# J

|  |  |
| --- | --- |
| JavaScript Object Notation (JSON) | 1:15-16, 1:59, 1:63, 1:65-67, 1:131, 1:134, 2:6, 2:38-39, 2:61-62, 2:85, 2:108, 2:120, 3:14, 3:29, 3:36, 3:87, 3:126, 4:15, 4:77, 4:79, 4:85, 4:92, 4:94-95, 4:137, 4:175-176, 4:186, 5:30, 5:35, 5:72, 5:77, 5:99-100, 5:104, 5:124, 5:141 |

# K

|  |  |
| --- | --- |
| Key Logs | 1:39, 1:45 |
| keyName | 3:68 |
| Kibana | 1:13, 1:20, 1:30, 1:66, 2:62, 2:108, 2:110 |
| Kibana Query Language (KQL) | 1:30 |
| Kroll Artifact Parser and Extractor (KAPE) | 2:124 |
| Kube-APIServer | 4:12, 4:24 |
| Kube-Proxy | 4:11, 4:15 |
| Kube-Scheduler | 4:12, 4:24 |
| Kubelet | 4:11, 4:13, 4:28, 4:30-32, 4:35-36 |
| Kubernetes | 1:4, 1:15, 1:17, 1:27, 1:41-42, 3:129, 4:1, 4:3-18, 4:20, 4:22-26, 4:28-42, 4:44, 4:73, 4:99, 4:138, 4:160, 5:25-26 |
| Kusto Query Language (KQL) | 2:50 |

# L

|  |  |
| --- | --- |
| Lag Time | 3:26, 4:75-76, 4:107, 4:120, 4:163 |
| Lambda | 1:41, 1:51, 3:14, 3:17, 3:26, 3:30, 3:47, 3:114, 3:135-143 |
| Lateral Movement | 2:21, 3:146, 3:155, 4:38, 4:54, 5:25-27, 5:135 |
| Lightsail | 3:53, 3:72-73 |
| Linux Logs | 2:117 |
| Load Balancer | 2:79-80, 3:63, 3:90-91, 3:96-98, 3:113, 3:124, 3:129, 5:129, 5:140 |
| Log Analytics | 1:51, 2:18-19, 2:42-46, 2:48-51, 2:56, 2:58, 2:87, 2:95, 2:101, 2:129, 4:18, 4:22, 5:37, 5:46, 5:54, 5:56, 5:63 |
| Log Buckets | 5:46, 5:54, 5:58-59, 5:63 |
| Log Explorer | 1:51, 4:83, 5:37, 5:46-50, 5:52, 5:56, 5:58, 5:100-101, 5:116 |
| Log Ingestion | 1:56, 3:127, 5:45 |
| Log Lag | 4:75 |
| Log Retention | 1:54, 4:119 |
| Log Storage | 1:42, 3:90, 3:107, 5:45, 5:58, 5:63, 5:65, 5:118 |
| Logstash | 1:12-17, 1:19, 1:27, 1:66, 2:20, 2:35, 2:62, 2:92, 2:108, 2:110, 2:119, 3:36, 5:74 |
| Lucene | 1:30 |

# M

|  |  |
| --- | --- |
| Mail Clients | 1:57, 1:74, 1:79 |
| MailItemsAccessed | 1:56-57, 1:71-72, 1:76-78, 1:80-81, 1:83-86, 1:133 |
| Malware | 4:39, 4:99, 4:106, 4:115, 4:117, 4:134-135, 5:86, 5:110, 5:132 |
| Management Event | 3:26, 3:29-30, 3:33 |
| Management groups | 2:4 |
| Margarita Shotgun | 3:153 |
| MBOX | 4:129, 4:132-133 |
| Metadata Service | 2:113, 3:4, 3:50, 4:33-34 |
| Metrics | 2:106, 2:117, 3:7, 3:88, 3:124 |
| Microsoft 365 | 1:7-8, 1:12, 1:14-15, 1:27, 1:38-40, 1:52-54, 1:56, 1:58-61, 1:65-69, 1:71, 1:74, 1:107, 1:112, 1:114-119, 1:134, 2:66, 2:131, 3:27, 3:34, 3:36 |
| Microsoft Graph API | 1:12, 1:39, 1:53, 1:80, 1:115-119, 1:133, 2:14, 2:46, 2:66 |
| Microsoft Incident Response Playbooks | 2:122, 2:128, 2:131 |
| Microsoft Purview | 1:46, 1:58-59, 1:72, 1:87-89 |
| MITRE ATT&CK | 2:95, 2:132, 4:25, 4:30-31, 4:92, 4:96-97, 4:101 |
| MoveToDeletedItems | 1:71-72 |
| MultiFactor Authentication (MFA) | 1:60, 1:107, 1:125, 2:26-29, 2:33, 3:24, 3:42-43, 4:146, 4:184 |

# N

|  |  |
| --- | --- |
| NetFlow | 1:15, 1:25, 1:27, 1:43, 1:48, 2:102, 3:101, 3:113, 5:140-141 |
| Network Address Translation (NAT) | 2:78, 3:94, 4:13, 5:129 |
| Network Security Group (NSG) | 1:15, 2:60, 2:68, 2:72, 2:78-79, 2:81-87, 2:89-92, 2:96, 3:91-94, 3:100, 3:139, 3:142 |
| NetworkAccessTrafficLogs | 2:46 |
| Nginx | 3:96 |
| Node.js | 2:14, 3:137 |
| Nodes | 4:9-16, 4:30, 4:36-37, 4:40-41 |
| NSG flow logs | 1:15, 2:84-87 |

# O

|  |  |
| --- | --- |
| OAuth | 1:67, 1:116, 1:120, 2:113, 4:50, 4:75, 4:77, 4:83, 4:85-87, 4:89-91, 4:94-95, 4:101, 4:103, 4:138, 4:145, 4:148-159, 5:66, 5:69-72 |
| OAuth Abuse | 4:103, 4:138, 4:150-152, 4:159 |
| OAUTH Token | 1:116, 4:75, 4:95, 4:148-150, 4:152-158 |
| OAuth Token Tracking | 4:148 |
| OneDrive | 1:54, 1:56-57, 1:70-71, 1:95-96, 1:100-101, 1:103, 4:181 |
| operationName | 1:19, 1:122, 1:139, 2:23, 2:26, 2:30, 2:32-33, 2:35-36, 2:54-56, 2:82, 2:84, 2:91, 2:98, 2:100 |
| Ops Agent | 5:80, 5:95-97, 5:99-101, 5:103-104 |
| Organizational Unit | 3:10, 3:15 |
| Outlook | 1:71, 1:74, 1:78-80, 1:82-85 |
| Outlook Web Access (OWA) | 1:71, 1:74, 1:78-79, 1:81, 1:85 |

# P

|  |  |
| --- | --- |
| Packet CAPture (PCAP) | 1:48, 3:92, 5:42, 5:128, 5:140 |
| Packet Mirroring | 5:126, 5:140 |
| Page blobs | 2:94 |
| PageViewed | 1:57, 1:104 |
| Permission Model | 4:69, 5:27 |
| Permissions | 1:45, 1:60-61, 1:67, 1:71, 1:73, 1:107, 1:116, 1:119, 1:123-125, 1:134-136, 1:139-140, 2:5, 2:7, 2:11-12, 3:12, 3:15-16, 3:24, 3:35, 3:55, 3:111-112, 3:130, 3:139, 4:41, 4:44, 4:51, 4:53-55, 4:57, 4:60, 4:65, 4:67-70, 4:76, 4:79, 4:87, 4:95, 4:149, 4:152, 4:174-176, 5:5, 5:7, 5:12-18, 5:20, 5:22, 5:24-25, 5:27-29, 5:31-32, 5:40, 5:67-68, 5:71, 5:105, 5:109-112, 5:114 |
| Persistence | 1:112, 1:116, 3:151, 4:37-38, 4:96 |
| Persistent Disks | 1:51 |
| Phishing | 1:92, 2:131, 3:108, 4:99, 4:103, 4:106-110, 4:112-115, 4:117, 4:124, 4:134-135, 4:150-152 |
| PHP | 1:117, 2:14 |
| Platform as a Service (PaaS) | 1:40, 1:42, 4:46, 5:82 |
| Playbooks | 2:122, 2:128, 2:131, 3:150 |
| Pods | 4:8-16, 4:20, 4:24, 4:34, 4:36, 4:41 |
| Policy Simulator | 3:21 |
| Post Office Protocol (POP3) | 1:74 |
| PowerShell | 1:15, 1:46, 1:53, 1:55, 1:58, 1:60-61, 1:63-69, 1:88, 1:113, 1:117, 1:120, 1:126, 1:134, 1:139, 2:6, 2:10, 2:13-14, 2:38, 2:44-45, 2:74-75, 2:98, 2:109, 2:112-115, 2:132, 3:137, 3:151 |
| Prefixes | 3:49-50 |
| Pricing | 1:39, 1:43, 1:49-50, 2:69-70, 2:130, 3:33, 3:65, 3:78, 3:90, 3:100, 3:113, 3:125, 3:131, 3:137-138, 3:141, 5:39, 5:45 |
| Pricing Calculators | 1:50 |
| privateIpAddress | 3:86-87 |
| Privilege Escalation | 1:115, 1:137-139, 3:51, 4:28, 4:30-32, 4:35-36, 4:96, 4:152, 5:105, 5:113-114 |
| PST | 4:129, 4:132 |
| Purview Compliance Portal | 1:46, 1:53, 1:58-59, 1:63, 1:68-69, 1:72, 1:87-89, 1:107 |
| Python | 1:46, 1:117, 2:14, 2:62, 2:92, 3:30, 3:51-52, 3:83, 3:117, 3:137, 4:93 |

# Q

|  |  |
| --- | --- |
| Quarantine | 1:87-88, 4:58, 4:109, 4:114-117, 4:132, 4:134 |
| Query Builder | 5:47-48, 5:54 |
| Query Logs | 3:102-103 |
| Queue | 1:51, 1:59, 2:93, 2:95, 2:97-98, 4:18, 5:73, 5:75-76 |
| Queue Storage | 2:93 |
| Quicksight | 3:38 |

# R

|  |  |
| --- | --- |
| Regions | 1:50, 2:69, 2:78, 3:30, 3:65-66, 3:77, 3:103, 4:45, 4:129, 5:107, 5:129, 5:131 |
| Relational Database Service (RDS) | 3:26 |
| Remote Desktop Protocol (RDP) | 2:79, 2:81, 2:83, 2:85, 2:110, 3:59, 5:135, 5:139 |
| requestParameters | 1:18, 3:36, 3:43-45, 3:68, 3:83, 3:86, 3:117 |
| Resolver | 3:102-105, 3:129-130 |
| resourceId | 1:19, 1:122, 1:139, 2:26, 2:35-36, 2:82, 2:84, 2:91 |
| responseBodySize | 2:100 |
| responseElements | 3:36, 3:42-44, 3:46, 3:83, 3:87 |
| RESTful | 1:117-118, 2:14 |
| resultSignature | 2:26, 2:36, 2:82 |
| resultType | 2:23, 2:26, 2:36, 2:50, 2:53, 2:82 |
| RFC 1918 | 2:78, 3:92 |
| RiskyServicePrincipals | 2:46 |
| RiskyUsers | 1:109, 2:46 |
| Role Enumeration | 3:51 |
| Role-Based Access Control (RBAC) | 2:6-7, 2:11, 3:24 |
| Root Account | 3:5, 3:7, 3:12, 3:15, 3:23, 3:35, 3:39, 3:43, 3:59 |
| Route 53 | 3:90, 3:102-105, 3:124 |
| Routing | 3:91, 3:93-94, 3:96, 3:144, 4:13, 5:3, 5:37, 5:57-60, 5:80, 5:105, 5:118, 5:126, 5:129, 5:131 |

# S

|  |  |
| --- | --- |
| S3 | 1:51, 1:80, 3:9, 3:13, 3:15-16, 3:18-20, 3:25-27, 3:29-31, 3:33, 3:38, 3:52, 3:57, 3:72, 3:88, 3:92, 3:96, 3:99-100, 3:103, 3:107-121, 3:124-125, 3:127-130, 3:133, 3:138, 3:142-144, 3:153, 4:33, 4:175-178, 5:84 |
| S3 Browser | 3:31 |
| S3 Logging | 3:57, 3:120 |
| s\_request\_id | 5:119-120 |
| SAML | 1:112, 3:53, 4:53, 4:145, 4:147 |
| Secure Shell (SSH) | 2:79, 2:81, 2:118, 3:59, 3:68, 3:95, 3:133, 5:135, 5:139 |
| Security Assertion Markup Language (SAML) | 1:112, 4:53, 4:145, 4:147 |
| Security Information and Event Management (SIEM) | 1:9, 1:11, 1:14, 1:18, 1:40, 1:54, 1:58, 1:65, 1:68-69, 2:19, 2:64, 2:66, 2:74-75, 2:83, 2:85, 2:87, 2:129, 3:27, 3:57-58, 3:131, 3:140, 5:42, 5:73 |
| Security Operations and Forensics ELK (SOF-ELK) | 1:5, 1:9, 1:12, 1:14-15, 1:17, 1:19-21, 1:27, 1:35, 1:37, 1:39, 1:48, 1:53-54, 1:59, 1:65-66, 1:70, 1:115, 2:3, 2:16, 2:20, 2:26, 2:34-35, 2:57, 2:62, 2:72, 2:83, 2:92, 2:105, 2:108-111, 2:118-119, 3:67, 3:104-105, 4:93, 4:95, 4:97, 4:137, 4:159, 4:186, 5:35, 5:47, 5:72-74, 5:104, 5:124, 5:141 |
| Security Orchestration Automated Response (SOAR) | 2:129, 3:140 |
| Security Token Service (STS) | 3:9, 3:15, 3:23-24, 3:34, 3:38, 3:40, 3:48-50, 3:53, 3:71, 3:109-110 |
| SecurityHub | 3:136, 3:143-144 |
| Sentinel | 2:122, 2:128-130 |
| Serverless | 1:39, 1:41, 1:51, 3:14, 3:47, 3:136-137, 3:144 |
| Service Account | 1:45, 1:110-111, 3:23, 3:40, 4:12, 4:32, 4:79-80, 4:85-87, 5:12, 5:16, 5:18, 5:20, 5:22, 5:24-27, 5:34, 5:43, 5:57, 5:66-69, 5:134 |
| ServicePrincipalRiskEvents | 2:46 |
| sessionCredentialFromConsole | 3:36 |
| Set-Mailbox | 1:71 |
| Set-OwaMailboxPolicy | 1:71 |
| Shared Access Signature (SAS) | 2:97-100 |
| Shared Responsibility | 1:39, 1:43-44, 4:44, 4:46 |
| Shared Responsibility Model | 1:39, 1:43-44 |
| SharePoint | 1:53-54, 1:56-57, 1:65, 1:69-71, 1:89, 1:95-97, 1:101, 1:104, 1:111, 1:118 |
| Signin | 1:67, 1:127, 1:131, 2:20, 2:23-24, 2:26, 2:50, 2:52-53, 2:60, 3:43, 3:47, 3:95, 4:51, 4:56, 4:68, 4:96, 5:13, 5:18, 5:40 |
| Simple Queue Service (SQS) | 1:51 |
| Simple Storage Service (S3) | 1:51 |
| Sinks | 5:57-58, 5:60, 5:62, 5:73, 5:96, 5:133 |
| Sites | 1:124, 1:136, 4:120 |
| Snapshot | 1:39, 1:43, 1:47, 1:49, 2:71, 2:75, 2:114, 2:122-126, 3:2, 3:62, 3:68, 3:72, 3:77-83, 3:113, 3:142-144, 3:148, 4:40, 5:80, 5:87-95, 5:107 |
| Snapshotid | 3:79, 3:83 |
| SoftDelete | 1:71-72 |
| Software as a Service (SaaS) | 1:40, 4:46, 4:103 |
| Software Development Kit (SDK) | 1:46, 3:23, 3:36, 3:49, 4:73, 4:77, 4:87, 5:69-70 |
| SolarWinds | 1:115-116, 1:133 |
| source\_ip | 1:93, 1:137, 2:26, 2:76, 2:119, 3:104-105, 5:141 |
| sourceIpaddress | 1:16-17, 3:34, 3:42-45, 3:68, 3:86, 3:117 |
| sourceIPAddress | 1:16-17, 3:34, 3:42-45, 3:68, 3:86, 3:117 |
| Split Entry | 1:19 |
| Splunk Common Information Model | 1:11 |
| Step Functions | 3:135-136, 3:141, 3:144 |
| Storage Explorer | 2:18, 2:57-58, 2:60, 2:62, 2:92, 2:94, 2:99-100, 2:108-110, 2:118 |
| Stream | 2:64, 3:88, 4:15, 4:20, 4:51, 5:101 |
| Subnet | 1:48, 2:78-79, 2:84, 3:17, 3:63, 3:66, 3:85-87, 3:90-96, 3:98-101, 3:142, 5:62, 5:129-132, 5:134, 5:137 |
| Sync | 1:77-79, 1:83-84, 1:95, 1:103, 3:29, 3:31, 3:109, 3:117, 3:144, 4:14 |
| Systems Manager | 3:146, 3:150-152 |

# T

|  |  |
| --- | --- |
| Table Storage | 2:93 |
| Takeout | 4:54, 4:160, 4:179-185 |
| Teams | 1:54, 1:70, 1:95, 4:57-58, 5:5, 5:7, 5:139 |
| Threat Hunting | 1:121, 1:125, 3:55 |
| Throttling | 1:78 |
| Token | 1:31, 1:108, 1:116, 1:119-120, 1:126-127, 1:129, 1:139, 2:27, 2:29, 2:33, 2:100, 2:113, 3:9, 3:15, 3:23-24, 3:34, 3:38, 3:40, 3:48-49, 3:53, 3:71, 3:109-110, 4:32, 4:34, 4:36, 4:75, 4:95, 4:101, 4:138, 4:145, 4:148-150, 4:152-158, 5:25-26 |
| Token Tracking | 4:148 |
| Tracking New API Keys | 3:44 |
| Traffic Analytics | 2:87 |
| Transfer Acceleration | 3:107, 3:114-116 |
| Trusted Platform Module (TPM) | 5:84 |

# U

|  |  |
| --- | --- |
| Unified Audit Log (UAL) | 1:12, 1:15, 1:27, 1:39, 1:53-56, 1:58-59, 1:61-68, 1:70, 1:83, 1:87, 1:108, 1:115, 1:133, 3:36 |
| Unified Data Model | 1:11 |
| Uniform Resource Identifier (URI) | 1:127, 1:133, 2:8-10, 3:118 |
| UpdateCalendarDelegation | 1:73 |
| UpdateFolderPermissions | 1:73 |
| UpdateInboxRules | 1:71, 1:73 |
| Usage Reports | 4:77-78 |
| User Agents | 3:47, 3:133 |
| User Log | 1:33, 1:111, 3:45, 4:76, 4:82, 4:142, 4:144-147 |
| user\_id | 1:31, 1:70, 1:111, 2:15 |
| user\_name | 1:93, 1:103, 1:105, 2:15, 2:26 |
| user\_principal\_name | 1:137, 2:15, 2:26, 2:40, 2:76, 2:102 |
| userAgent | 1:16, 1:18, 1:31, 1:111, 2:26, 2:100, 3:36, 3:42-45, 3:68, 3:83, 3:86, 3:117 |
| userAgentHeader | 2:100 |
| userIdentity | 1:16, 1:18, 3:34-35, 3:43, 3:45, 3:67, 3:82, 3:117, 3:126 |
| UserLoggedIn | 1:33, 1:56-57, 1:64, 1:110-111 |
| UserRiskEvents | 1:109, 2:46 |

# V

|  |  |
| --- | --- |
| Vault | 4:50, 4:54, 4:58, 4:67, 4:70, 4:75, 4:87, 4:99, 4:106, 4:115, 4:117-127, 4:129-133, 4:135, 4:156, 4:162, 4:164, 4:184 |
| Virtual Hard Drive (VHD) | 1:47, 2:94, 2:125 |
| Virtual Network (VNet) | 1:42, 1:48, 1:51, 2:6-7, 2:68, 2:72, 2:78-79, 2:86, 3:17, 3:91, 3:96, 3:100, 4:37-38, 5:26, 5:127, 5:129 |
| Virtual Private Cloud (VPC) | 1:15, 1:51, 3:4, 3:9, 3:11, 3:87, 3:90-94, 3:96, 3:98-103, 3:106, 3:124, 3:129-130, 3:133, 3:142, 4:13, 5:62, 5:126, 5:129-140 |
| Virtual Private Network (VPN) | 2:78, 2:80, 5:129 |
| Virtual router | 2:80 |
| Visualize Library | 1:20, 1:22, 1:24 |
| VNet | 1:51, 2:78, 2:84, 2:86, 2:91 |
| Volumeid | 3:79, 3:83 |
| volumeSize | 3:76, 3:79, 3:83 |
| volumeType | 3:76 |
| VPC Flow Logs | 1:15, 3:11, 3:90, 3:99, 3:106, 3:124, 3:129-130, 3:133, 5:62, 5:126, 5:132-134, 5:138 |
| VPC Subnets | 3:90, 3:93 |
| vpcId | 3:87, 3:139 |
| VPN gateway | 2:78, 2:80 |

# W

|  |  |
| --- | --- |
| WAN optimization appliance | 2:80 |
| Web Application Firewalls (WAFs) | 3:63, 3:91, 3:96 |
| Windows Azure Diagnostics (WAD) | 2:106-108 |

# Z

|  |  |
| --- | --- |
| Zeek | 5:140 |