Below details are just to showcase possible security/operational/compliance monitoring usecases which can automated with appropriate criterias. Usecases are collated based on the technology and not based on vendor. Vendor names are used just to showcase the possible functionality.

Created By: Prasannakumar B Mundas

List of device types considered below for creating use cases

AWS	**Amazon CloudFormation**	**JumpCloud**	**Sophos SG/UTM 9**
Amazon Kinesis	**AWS Lambda**	**Google Workspace**	**Palo Alto Appliance**
Amazon DynamoDB	**AWS Secrets Manager**	**Microsoft Azure**	**Cisco Switch**
Amazon EKS	**AWS Key Management Service (KMS)**	**Linux OS**	**Cisco Wireless Lan Controller**
AWS ELB	**AWS Identity & Access Management (IAM)**	**Crowdstrike Falcon**	**Microsoft IIS**
Amazon EC2	**Amazon CloudWatch**	**Websense WSG**	**Apache**
Amazon EC2 Auto Scaling	**Amazon RDS**	**Cisco IronPort**	**F5 BIG-IP**
Amazon SQS	**AWS Systems Manager**	**Microsoft DNS**	**Microsoft DHCP Server**
Amazon SNS	**Windows Defender**	**Cisco Firepower Threat Defense (FTD)**	**Microsoft Windows Hyper-V**
Amazon S3	**Microsoft Office365**	**FortiGate Firewall**	**Windows Active Directory**

SL. No	Device Type	Product	Device Version	Use case type	Use cases	Description
1	Cloud	AWS	NA	Flex Report	Amazon AWS Login Failed Activity	This report will generate a detailed view of the failed or unauthorized logins to the AWS Management Console
2	Cloud	AWS	NA	Flex Report	Amazon AWS Login Success Activity	This report will generate a detailed view of the successful user login or authentication to the AWS Management Console.
3	Cloud	AWS	NA	Flex Report	Amazon AWS Network Interface Activity	This report will generate a detailed view of the activity related to the network interface created, deleted, reset, modified, detached, attached, etc.
4	Cloud	AWS	NA	Flex Report	Amazon AWS User Management Activity	This report will generate a detailed view of the activities related to the user or group created, deleted, added, removed, etc.
5	Cloud	AWS	NA	Flex Report	Amazon AWS Bucket-Level Activity	This report will generate a detailed view of the activities related to the Amazon S3 bucket. This includes CreateBucket, PutBucketPolicy, ListBuckets, etc.
6	Cloud	AWS	NA	Flex Report	Amazon AWS Policy Activity	This report will generate a detailed view of the activities related to the policies, i.e., AttachUserPolicy, GetPolicy, DetachRolePolicy, CreatePolicy, etc.
7	Cloud	AWS	NA	Flex Report	Amazon AWS Security Group Activity	This report will generate a detailed view of the activities related to the security groups, i.e., CreateSecurityGroup, AuthorizeSecurityGroupIngress, DeleteSecurityGroup, etc.
8	Cloud	AWS	NA	Alert	Amazon AWS: Network Interface Deleted	This alert will be triggered if any activity related to the VPC network interface is deleted.
9	Cloud	AWS	NA	Alert	Amazon AWS:User Deleted	This alert will be triggered if a user gets deleted.
10	Cloud	AWS	NA	Alert	AWS CIS Control: AWS Config configuration changed	This alert will be triggered when the configuration is changed in the AWS Config. It will ensure sustained visibility of the configuration items within the AWS account
11	Cloud	AWS	NA	Alert	AWS CIS Control: AWS Management Console authentication failed	This alert will be triggered in the event of any failed or unauthorized login attempt to the AWS Management Console.
12	Cloud	AWS	NA	Alert	AWS CIS Control: Network Access Control Lists (NACL) changed	This alert will be triggered in the event of any changes to the Network Access Control Lists are detected. Monitoring the changes in the NACLs will ensure that the AWS resources and services are not unintentionally exposed.
13	Cloud	AWS	NA	Alert	AWS CIS Control: Network gateways changed	This alert will be triggered in the event of any changes to the network gateway being detected. Monitoring the changes in the network gateways will ensure all the ingress/egress traffic traverses the VPC border via a controlled path.
14	Cloud	AWS	NA	Alert	AWS CIS Control: CloudTrail configuration changed	This alert will be triggered in the event of any CloudTrail configuration changes. Monitoring these changes in the CloudTrail's configuration will ensure sustained visibility ofthe activities performed in the AWS account.
15	Cloud	AWS	NA	Alert	AWS CIS Control: Disabling or scheduled deletion of customer-created CMKs detected	This alert will be triggered in the event of any disabling or scheduled deletion of customer-created CMKs. Monitoring these changes in the CloudTrail's configuration will ensure sustained visibility of activities performed in the AWS account.

16	Cloud	AWS	NA	Alert	AWS CIS Control: IAM policy changed	This alert will be triggered in the event of any IAM policy changes. Monitoring these changes in the IAM policies will ensure authentication and authorization controls remain intact.
17	Cloud	AWS	NA	Alert	AWS CIS Control: Management console signed-in without MFA	This alert will be triggered in the event of any user signs in without the MFA. Monitoring these single-factor console logins will increase the visibility into the accounts that are not protected by the MFA.
18	Cloud	AWS	NA	Alert	AWS CIS Control: Route table changed	This alert will be triggered in the event of any Route table changes. Monitoring these changes in the route tables will ensure all the VPC traffic flows through an expected path.
19	Cloud	AWS	NA	Alert	AWS CIS Control: S3 bucket policy changed	This alert will be triggered in the event of the S3 bucket policy changes. Monitoring these changes in the S3 bucket policies may reduce the time to detect and correct the permissive policies on sensitive S3 buckets
20	Cloud	AWS	NA	Alert	AWS CIS Control: Security group changed	This alert will be triggered in the event of the S3 bucket policy changes. Monitoring these changes in the security group will ensure that the resources and services are not unintentionally exposed.
21	Cloud	AWS	NA	Alert	AWS CIS Control: Unauthorized API calls detected	This alert is triggered in the event of unauthorized API calls being detected. Monitoring these unauthorized API calls will reveal the application errors and may reduce the time to detect the malicious activity.
22	Cloud	AWS	NA	Alert	AWS CIS Control: Usage of root account detected	This alert will be triggered in the event of root account usage detection. Monitoring the root account logins will provide visibility into the use of a fully privileged account and an opportunity to reduce its use.
23	Cloud	AWS	NA	Alert	AWS CIS Control: VPC changes detected	This alert will be triggered in the event of the VPC changes. Monitoring these changes in the IAM policies will help ensure authentication and authorization controls remain intact.
24	Cloud	AWS	NA	Dashboard	Amazon AWS Login Success Activity By the User Type	
25	Cloud	AWS	NA	Dashboard	Amazon AWS Login Failed Activity By Failed Reason	
26	Cloud	AWS	NA	Dashboard	Amazon AWS Policy Activity By the Source IP Address	
27	Cloud	AWS	NA	Dashboard	Amazon AWS Policy Activity By the User Type	
28	Cloud	AWS	NA	Dashboard	Amazon AWS Login Failed Activity By the User-Agent	
29	Cloud	AWS	NA	Dashboard	Amazon AWS All Operations Activity By the Event Name	
30	Cloud	AWS	NA	Dashboard	Amazon AWS Login Failed Activity By City	
31	Cloud	AWS	NA	Dashboard	Amazon AWS User Management Activity By the User Added	
32	Cloud	AWS	NA	Dashboard	Amazon AWS User Management Activity By the User Deleted	
33	Cloud	AWS	NA	Dashboard	Amazon AWS Policy Activity By the Service Name	
34	Cloud	AWS	NA	Dashboard	Amazon AWS Bucket and Object Activity By the Error Codes	
35	Cloud	AWS	NA	Dashboard	Amazon AWS Critical Security Activity By the Source IP Address	
36	Cloud	AWS	NA	Dashboard	Amazon AWS VM Instances Activity By the User Type	
37	Cloud	Amazon Kinesis	NA	Flex Report	Amazon Kinesis - Analytics application modifications	This report gives the details of all the actions carried out in relation to the Kinesis analytics service. It gives information about the action name, the time it was initiated, and by whom, among some other details related to the application and the user.
38	Cloud	Amazon Kinesis	NA	Flex Report	Amazon Kinesis - Data stream activities	This report gives the details of all the actions related to the data streams in Kinesis, which includes information like the stream name, the action initiated against it, the timestamp for the action, and the user information for the same.

39	Cloud	Amazon Kinesis	NA	Alert	Amazon Kinesis: Data preprocessor deleted	This alert is triggered when a data pre-processing function is removed from the configuration settings of a Kinesis analytics application.
40	Cloud	Amazon Kinesis	NA	Alert	Amazon Kinesis: SQL I/O configuration deletion	This alert is triggered when an output stream or a reference output data source is deleted.
41	Cloud	Amazon Kinesis	NA	Alert	Amazon Kinesis: Application stopped	This alert is triggered when a Kinesis Analytics application is stopped.
42	Cloud	Amazon Kinesis	NA	Alert	Amazon Kinesis: Stream enhanced metrics disabled	This alert is triggered when the enhanced monitoring for a Kinesis stream is disabled.
43	Cloud	Amazon Kinesis	NA	Alert	Amazon Kinesis: Stream shard count updated	This alert is triggered when the shard count for a particular Kinesis data stream is updated.
44	Cloud	Amazon Kinesis	NA	Dashboard	Amazon Kinesis – Application activity	
45	Cloud	Amazon Kinesis	NA	Dashboard	Amazon Kinesis – Activity by IP Address	
46	Cloud	Amazon Kinesis	NA	Dashboard	Amazon Kinesis – User activity	
47	Cloud	Amazon Kinesis	NA	Dashboard	Amazon Kinesis - Data streams activities overview	
48	Cloud	Amazon Kinesis	NA	Dashboard	Amazon Kinesis - Data stream critical activities	
49	Cloud	Amazon DynamoDB	NA	Flex Report	Amazon DynamoDB - Database activity	This report will give a detailed overview of all the activities related to the DynamoDB service.
50	Cloud	Amazon DynamoDB	NA	Flex Report	Amazon DynamoDB - DAX cluster activity	This report will give the details of all the activity related specifically to the DAX cluster in the DynamoDB.
51	Cloud	Amazon DynamoDB	NA	Alert	Amazon DynamoDB: Table deletion attempt	This alert is triggered when an attempt is made to delete a DynamoDB table in the AWS.
52	Cloud	Amazon DynamoDB	NA	Alert	Amazon DynamoDB: Backup deletion attempt	This alert is triggered when an attempt is made to delete a manual on-demand backup.
53	Cloud	Amazon DynamoDB	NA	Alert	Amazon DynamoDB: DAX cluster deletion attempt	This alert is triggered when an attempt is made to delete a DAX cluster.
54	Cloud	Amazon DynamoDB	NA	Alert	Amazon DynamoDB: Parameter group deletion attempt	This alert is triggered when an attempt is made to delete a parameter group of a DAX cluster in the DynamoDB.
55	Cloud	Amazon DynamoDB	NA	Alert	Amazon DynamoDB: DAX subnet deletion attempt	This alert is triggered when an attempt is made to delete a subnet in a DAX cluster in the DynamoDB.
56	Cloud	Amazon DynamoDB	NA	Dashboard	Amazon DynamoDB - Database activities	
57	Cloud	Amazon DynamoDB	NA	Dashboard	Amazon DynamoDB - DAX activity	
58	Cloud	Amazon DynamoDB	NA	Dashboard	Amazon DynamoDB - Activity overview	
59	Cloud	Amazon DynamoDB	NA	Dashboard	Amazon DynamoDB - User activity	
60	Cloud	Amazon EKS	NA	Flex Reports	Amazon EKS - Cluster activity	This report will give a detailed overview of the actions that are being triggered in all the AWS EKS instances. It gives information about the action, the time in which the action was triggered, user information related to it, and other cluster-related information.
61	Cloud	Amazon EKS	NA	Alert	Amazon EKS: Addon deletion attempt	This will trigger an alert if an attempt to delete an add-on to the EKS cluster is detected.
62	Cloud	Amazon EKS	NA	Alert	Amazon EKS: Cluster deletion attempt	This will trigger an alert if an attempt to delete an EKS cluster is made.
63	Cloud	Amazon EKS	NA	Alert	Amazon EKS: Fargate profile deletion attempt	This will trigger an alert if an attempt to delete a Fargate profile is made in an EKS cluster.
64	Cloud	Amazon EKS	NA	Alert	Amazon EKS: Nodegroup deletion attempt	This will trigger an alert if an attempt is made to delete a node group in an EKS cluster.
65	Cloud	Amazon EKS	NA	Dashboard	Amazon EKS - User activity	
66	Cloud	Amazon EKS	NA	Dashboard	Amazon EKS - Cluster activity	
67	Cloud	Amazon EKS	NA	Dashboard	Amazon EKS - Activity overview	
68	Cloud	AWS ELB	NA	Flex Report	AWS ELB - Elastic load balancer activities	This report will give a detailed overview of the actions triggered as part of the AWS ELB service. It gives information about the action, the time in which the action was triggered, user information related to it, among some other details related to the configured load balancers.

69	Cloud	AWS ELB	NA	Alert	AWS ELB: Load balancer listener deleted	This alert is triggered when a listener is deleted from a particular load balancer.
70	Cloud	AWS ELB	NA	Alert	AWS ELB: Instance deregistered	This alert is triggered when an instance is removed from the list of the associated instances in a load balancer.
71	Cloud	AWS ELB	NA	Alert	AWS ELB: Load balancer subnet/AZ removed	This alert is triggered when a subnet or Availability Zone (AZ) is removed from the configuration settings of a load balancer.
72	Cloud	AWS ELB	NA	Alert	AWS ELB: Target group deleted	This alert is triggered when a target group is deleted from the load balancer configuration.
73	Cloud	AWS ELB	NA	Alert	AWS ELB: Load balancer deleted	This alert is triggered when a load balancer is purged and removed from the ELB service.
74	Cloud	AWS ELB	NA	Dashboard	AWS ELB - User activity	
75	Cloud	AWS ELB	NA	Dashboard	AWS ELB - Load balancer activities	
76	Cloud	AWS ELB	NA	Dashboard	AWS ELB - Load balancer critical activities	
77	Cloud	AWS ELB	NA	Dashboard	AWS ELB - Activity by IP Address	
78	Cloud	Amazon EC2	NA	Flex Report	Amazon EC2 - Activity overview	This report will contain relevant information related to all activities for instance in Amazon EC2.
79	Cloud	Amazon EC2	NA	Flex Report	Amazon EC2 - VPC changes	This report will contain relevant information related about modifications in VPC configuration in Amazon EC2.
80	Cloud	Amazon EC2	NA	Flex Report	Amazon EC2 - Security group modifications	This report will contain relevant information related about changes security group configuration in Amazon EC2.
81	Cloud	Amazon EC2	NA	Alert	Amazon EC2: Security group rules changed to unrestricted	This alert is triggered when a change is detected in the security group configuration.
82	Cloud	Amazon EC2	NA	Alert	Amazon EC2: Snapshot deletion attempt	This alert is triggered when an attempt is made to delete a snapshot for a specified account and region.
83	Cloud	Amazon EC2	NA	Alert	Amazon EC2: Sensitive VPC settings modification attempt	This alert is triggered when an attempt is made to change the VPC configuration.
84	Cloud	Amazon EC2	NA	Alert	Amazon EC2: Instance termination attempt	This alert is triggered when an attempt is made to shut down the specified instances.
85	Cloud	Amazon EC2	NA	Dashboard	Amazon EC2 – Activity overview	
86	Cloud	Amazon EC2	NA	Dashboard	Amazon EC2 – Critical activity	
87	Cloud	Amazon EC2	NA	Dashboard	Amazon EC2 – Security group changes	
88	Cloud	Amazon EC2	NA	Dashboard	Amazon EC2 – Instance termination	
89	Cloud	Amazon EC2	NA	Dashboard	Amazon EC2 – VPC configuration	
90	Cloud	Amazon EC2 Auto Scaling	NA	Flex Report	Amazon EC2 Auto Scaling - Activity overview	This report will contain relevant information related to all the activities for the configuration of instances in Amazon EC2 Auto Scaling.
91	Cloud	Amazon EC2 Auto Scaling	NA	Dashboard	Amazon EC2 Auto Scaling - Activity overview	
92	Cloud	Amazon EC2 Auto Scaling	NA	Dashboard	Amazon EC2 Auto Scaling - Critical activity	
93	Cloud	Amazon EC2 Auto Scaling	NA	Dashboard	Amazon EC2 Auto Scaling -Instance protection	
94	Cloud	Amazon EC2 Auto Scaling	NA	Dashboard	Amazon EC2 Auto Scaling - Scaling policies	
95	Cloud	Amazon SQS	NA	Flex Report	Amazon SQS - Activity overview	This report will contain relevant information related to all activities for configuration changes in the SQS service.
96	Cloud	Amazon SQS	NA	Dashboard	Amazon SQS - Activity overview	
97	Cloud	Amazon SQS	NA	Dashboard	Amazon SQS – Createqueue with user detail	
98	Cloud	Amazon SQS	NA	Dashboard	Amazon SQS – SetQueueAttributes with user information	
99	Cloud	Amazon SNS	NA	Flex Report	Amazon SNS - Activity overview	This report will contain relevant information related to all activities for configuration in the SNS service.
100	Cloud	Amazon SNS	NA	Dashboard	Amazon SNS – Activity overview	

101	Cloud	Amazon SNS	NA	Dashboard	Amazon SNS – Subscriptions	
102	Cloud	Amazon SNS	NA	Dashboard	Amazon SNS – Topic created user details	
103	Cloud	Amazon S3	NA	Flex Report	Amazon S3 - Bucket level activity	This report gives the details of all actions carried out into the S3 service. It gives information about the action name, the time it was initiated, and by whom, among some other details related to the application and the user.
104	Cloud	Amazon S3	NA	Flex Report	Amazon S3 -Unauthorized user activities	This report gives details of the specific actions that were carried out related to the S3 service which failed due to one or more errors related access management and/or data misconfiguration.
105	Cloud	Amazon S3	NA	Flex Report	Amazon S3 - Activity overview	This report gives the details of all the actions carried out in relation to S3. It gives information about the action name, the time it was initiated, and by whom, among some other details related to the application and the user.
106	Cloud	Amazon S3	NA	Alert	Amazon S3: Bucket encryption disabled	This alert is triggered when an attempt is made to disable server-side encryption on an S3 bucket.
107	Cloud	Amazon S3	NA	Alert	Amazon S3: Inventory configuration changes detected	This alert is triggered when an attempt is made to add-edit or delete an S3 inventory configuration.
108	Cloud	Amazon S3	NA	Alert	Amazon S3: Bucket ownership settings changed	This alert is triggered when an attempt is made to edit or delete an S3 bucket ownership setting.
109	Cloud	Amazon S3	NA	Alert	Amazon S3: Public access block settings changed	This alert is triggered when an attempt is made to the public access settings of an S3 bucket.
110	Cloud	Amazon S3	NA	Alert	Amazon S3: Bucket replication detected	This alert is triggered when an attempt is made to change the bucket replication settings for S3.
111	Cloud	Amazon S3	NA	Alert	Amazon S3: Access points modified	This alert is triggered when an attempt is made to modify the access point settings for an S3 bucket.
112	Cloud	Amazon S3	NA	Alert	Amazon S3: Unauthorized bucket configuration access	This alert is triggered when multiple API calls are detected to access the details of an S3 bucket, which failed due to one or more errors.
113	Cloud	Amazon S3	NA	Alert	Amazon S3: New lifecycle policy added	This alert is triggered when a new life cycle policy is added for an S3 bucket which has a limited object expiration period and may supersede existing policies.
114	Cloud	Amazon S3	NA	Alert	Amazon S3: Bucket policy changed	This alert is triggered when events related to changes in the S3 bucket policy are detected, based on the request of a privileged user.
115	Cloud	Amazon S3	NA	Dashboard	Amazon S3 – Critical activities	
116	Cloud	Amazon S3	NA	Dashboard	Amazon S3 - Configuration changes by IP address	
117	Cloud	Amazon S3	NA	Dashboard	Amazon S3 – Failed API calls	
118	Cloud	Amazon CloudFormation	NA	Flex Report	AWS CloudFormation - Activity overview	This report will contain relevant information related to all the activities for stacks in AWS CloudFormation.
119	Cloud	Amazon CloudFormation	NA	Flex Report	AWS CloudFormation - Critical configuration changes	This report will contain relevant information about delete actions and help to detect the configuration changesin AWS CloudFormation.
120	Cloud	Amazon CloudFormation	NA	Alert	AWS CloudFormation: Stack drift detected	This alert is triggered when a change is detected in the stack's actual configuration.
121	Cloud	Amazon CloudFormation	NA	Alert	AWS CloudFormation: Stack instance deleted	This alert is triggered when an attempt is made to delete a stack for a specified account and region.
122	Cloud	Amazon CloudFormation	NA	Alert	AWS CloudFormation: Stack resource drift detected	This alert is triggered when a change is detected in the resources for the stack's actual configuration.
123	Cloud	Amazon CloudFormation	NA	Alert	AWS CloudFormation: Stackset operation stopped	This alert is triggered when an attempt is made to stop an in-progress operation on a stack set and its associated stack instances.
124	Cloud	Amazon CloudFormation	NA	Dashboard	AWS CloudFormation – Activity overview	
125	Cloud	Amazon CloudFormation	NA	Dashboard	AWS CloudFormation – Critical activity	
126	Cloud	Amazon CloudFormation	NA	Dashboard	AWS CloudFormation – User activity by IP address	
127	Cloud	Amazon CloudFormation	NA	Dashboard	AWS CloudFormation – User activity	
128	Cloud	AWS Lambda	NA	Flex Report	AWS Lambda - Activity overview	This will give the details of all the actions and API calls related to the different Lambda functions present in the AWS instance.

129	Cloud	AWS Lambda	NA	Alert	AWS Lambda: Codesign configuration change	This alert is triggered when changes are detected on the codesign configuration which helps to ensure that only trusted code runs on the Lambda functions.
130	Cloud	AWS Lambda	NA	Alert	AWS Lambda: Function configuration change	This alert is triggered when an attempt is made to change or update the configuration of a Lambda function
131	Cloud	AWS Lambda	NA	Alert	AWS Lambda: Layer version permission change	This alert is triggered when an attempt is made to change the codesign configuration of a Lambda function.
132	Cloud	AWS Lambda	NA	Dashboard	AWS Lambda -Activity overview	
133	Cloud	AWS Lambda	NA	Dashboard	AWS Lambda -Error details	
134	Cloud	AWS Lambda	NA	Dashboard	AWS Lambda -User activity by IP address	
135	Cloud	AWS Secrets Manager	NA	Flex Report	AWS Secrets Manager - Secrets read-write level activity	This report will provide information related to the actions that are based on viewing and modifying secret keys in AWS Secrets Manager.
136	Cloud	AWS Secrets Manager	NA	Flex Report	AWS Secrets Manager - Resource policy changes	This report will provide information related to the policy changes related to AWS Secrets Manager.
137	Cloud	AWS Secrets Manager	NA	Alert	AWS Secrets Manager: Secrets enumeration detected	This alert is triggered when multiple attempts related to read, list, or describe actions for different secrets stored are detected within a very short timeframe.
138	Cloud	AWS Secrets Manager	NA	Alert	AWS Secrets Manager: Secrets policy changes detected	This alert is triggered if the resource policy related to a secret key has been modified.
139	Cloud	AWS Secrets Manager	NA	Alert	AWS Secrets Manager: Secrets restored	This alert is triggered if a secret key has been restored which was otherwise scheduled for disposal.
140	Cloud	AWS Secrets Manager	NA	Alert	AWS Secrets Manager: Secrets value modifications detected	This alert is triggered if the secret key or its related settings have been modified.
141	Cloud	AWS Secrets Manager	NA	Dashboard	AWS Secrets Manager -Activity overview	
142	Cloud	AWS Secrets Manager	NA	Dashboard	AWS Secrets Manager - Settings and permission changes	
143	Cloud	AWS Secrets Manager	NA	Dashboard	AWS Secrets Manager - User activity by IP address	
144	Cloud	AWS Secrets Manager	NA	Dashboard	AWS Secrets Manager - Error details	
145	Cloud	AWS Key Management Service (KMS)	NA	Flex Report	AWS KMS - Permission management related activity	This report gives the details of all actions carried out related to permission management in the AWS KMS.
146	Cloud	AWS Key Management Service (KMS)	NA	Flex Report	AWS KMS - Read-write access level activity	This report gives details of the actions that were carried out which are related to viewing and updating the configuration settings in KMS.
147	Cloud	AWS Key Management Service (KMS)	NA	Alert	AWS KMS: High privileged key created	This alert is triggered when an attempt is made to create a customer-managed key that has sensitive permissions like delete and/or updates and/or revokes for all resources as part of KMS.
148	Cloud	AWS Key Management Service (KMS)	NA	Alert	AWS KMS: Key deletion cancelled	This alert is triggered when an attempt is made to cancel the scheduled deletion of a customer-managed key.
149	Cloud	AWS Key Management Service (KMS)	NA	Alert	AWS KMS: Key rotation disabled	This alert is triggered when the setting for an auto change of the cryptographic material of a key has been disabled as part of KMS.
150	Cloud	AWS Key Management Service (KMS)	NA	Alert	AWS KMS: Short window key deletion scheduled	This alert is triggered when a key deletion is scheduled for a customer-managed key in KMS, where the timeframe of the deletion is too short
151	Cloud	AWS Key Management Service (KMS)	NA	Dashboard	AWS KMS - Activity overview	
152	Cloud	AWS Key Management Service (KMS)	NA	Dashboard	AWS KMS -User activity by IP address	
153	Cloud	AWS Key Management Service (KMS)	NA	Dashboard	AWS KMS - Permission management level activity	
154	Cloud	AWS Identity & Access Management (IAM)	NA	Flex Report	AWS IAM - Activity overview	This report will contain relevant information related to all activities in AWS IAM.
155	Cloud	AWS Identity & Access Management (IAM)	NA	Alert	AWS IAM: Add policy and roles	This alert is triggered when a new policy created is detected in the Identity and Access Management (IAM) service

156	Cloud	AWS Identity & Access Management (IAM)	NA	Alert	AWS IAM: Create new user and group	This alert is triggered when an attempt is made to create a new user or new group in Identity and Access Management (IAM) console
157	Cloud	AWS Identity & Access Management (IAM)	NA	Alert	AWS IAM: Delete group and user	This alert is triggered when an attempt is made to delete or remove a user or group from the IAM console.
158	Cloud	AWS Identity & Access Management (IAM)	NA	Alert	AWS IAM: Delete policy and role	This alert is triggered when the AWS service policies or role has been deleted by the user from the Identity and Access Management (IAM) console.
159	Cloud	AWS Identity & Access Management (IAM)	NA	Alert	AWS IAM: Create and delete access key	This alert is triggered when the credentials have been deleted or newly created by the user in the Identity and Access Management (IAM) console.
160	Cloud	AWS Identity & Access Management (IAM)	NA	Dashboard	AWS IAM – Activity overview	
161	Cloud	AWS Identity & Access Management (IAM)	NA	Dashboard	AWS IAM – Critical activity	
162	Cloud	AWS Identity & Access Management (IAM)	NA	Dashboard	AWS IAM – IAM users	
163	Cloud	AWS Identity & Access Management (IAM)	NA	Dashboard	AWS IAM – User group	
164	Cloud	AWS Identity & Access Management (IAM)	NA	Dashboard	AWS IAM – User policies	
165	Cloud	AWS Identity & Access Management (IAM)	NA	Dashboard	AWS IAM – User roles list	
166	Cloud	Amazon CloudWatch	NA	Flex Report	Amazon CloudWatch - Activity overview	This report will contain relevant information related to any changes in the CloudWatch activities in the Amazon CloudWatch service.
167	Cloud	Amazon CloudWatch	NA	Alert	Amazon CloudWatch: Create export task	This alert is triggered when there is a new export file has been created and sentto the database or S3 storage in the CloudWatch service
168	Cloud	Amazon CloudWatch	NA	Alert	Amazon CloudWatch: Delete and disable alarms	This alert is triggered when an attempt is made to delete the specified alarms and disables the actions for the specified alarms.
169	Cloud	Amazon CloudWatch	NA	Alert	Amazon CloudWatch: Create and delete log groups	This alert is triggered when an attempt is made to delete or remove the log group and create a new log group in CloudWatch.
170	Cloud	Amazon CloudWatch	NA	Alert	Amazon CloudWatch: Delete filters	This alert is triggered when the matric filter and subscription filter have been deleted by the user from the log group in the CloudWatch service.
171	Cloud	Amazon CloudWatch	NA	Dashboard	Amazon CloudWatch – Activity overview	
172	Cloud	Amazon CloudWatch	NA	Dashboard	Amazon CloudWatch – Critical activity	
173	Cloud	Amazon CloudWatch	NA	Dashboard	Amazon CloudWatch – New filters created	
174	Cloud	Amazon CloudWatch	NA	Dashboard	Amazon CloudWatch – New log group created	
175	Cloud	Amazon RDS	NA	Flex Report	Amazon RDS - Activity overview	This report will contain relevant information related to all the activities in Amazon Relational Database Service (RDS).
176	Cloud	Amazon RDS	NA	Alert	Amazon RDS: Backup deletion attempt	This alert is triggered when there are databases backups that have been deleted and is detected in Amazon Relational Database Service (RDS)service.
177	Cloud	Amazon RDS	NA	Alert	Amazon RDS: Database deletion attempt	This alert is triggered when an attempt is made to delete or remove a database from Amazon Relational Database Service (RDS) console.
178	Cloud	Amazon RDS	NA	Alert	Amazon RDS: Backup export attempted	This alert is triggered when an attempt is made to export data or copy data to a simple storage service(s3) from the RDS console.
179	Cloud	Amazon RDS	NA	Dashboard	Amazon RDS – Activity overview	
180	Cloud	Amazon RDS	NA	Dashboard	Amazon RDS – Critical activity	
181	Cloud	Amazon RDS	NA	Dashboard	Amazon RDS – Data exported by user	
182	Cloud	AWS Systems Manager	NA	Flex Report	AWS Systems Manager - Activity overview	This report will contain relevant information related to any changes in the automation of Systems Manager activities in the AWS System Manager service.
183	Cloud	AWS Systems Manager	NA	Dashboard	AWS Systems Manager – Activity overview	
184	Cloud	AWS Systems Manager	NA	Dashboard	AWS Systems Manager – Critical activity	
185	Cloud	AWS Systems Manager	NA	Dashboard	AWS Systems Manager – Node Management	

186	Cloud	AWS Systems Manager	NA	Dashboard	AWS Systems Manager – Task update information	
187	AV	Windows Defender	NA	Flex Report	Windows Defender – Configuration changed	This report provides information related to changes happened on Windows Defender features like enabling/disabling of real-time protection, changes in the configuration of the defender.
188	AV	Windows Defender	NA	Flex Report	Windows Defender – Threat detected	This report provides information related to threat detected in windows machine. It provides information about the threat name, it's category, what action was taken by the defender on that threat.
189	AV	Windows Defender	NA	Flex Report	Windows Defender – Suspicious behavior detected	This report provides information when the defender has detected some suspicious behavior in windows machine like usage of malicious macro, changes in the registry which can compromise the system.
190	AV	Windows Defender	NA	Flex Report	Windows Defender – Action taken on threats	This report provides information related to the action taken by the Windows Defender on the threats detected on the system. If action has failed, then this report will provide the detail of reason.
191	AV	Windows Defender	NA	Alert	Windows Defender – Malware detected	This alert is generated when the anti-malware engine finds malware or other potentially unwanted software.
192	AV	Windows Defender	NA	Alert	Windows Defender – Action taken on threats	This event will be triggered when action is taken on the threat.
193	AV	Windows Defender	NA	Alert	Windows Defender – Suspicious behavior detected	This alert is generated when Windows Defender antivirus has detected suspicious behavior.
194	AV	Windows Defender	NA	Alert	Windows Defender–Definition update failed	This alert is generated when Windows Defender antivirus has encountered an error trying to use Dynamic Signature Service or update, load signatures and attempt reverting to a known-good set of signatures.
195	AV	Windows Defender	NA	Alert	Windows Defender – Signature update failed	This alert will be triggered when the signature update fails on Windows Defender.
196	AV	Windows Defender	NA	Alert	Windows Defender - Action taken on malware failed	This alert is generated when Windows Defender antivirus has encountered a non-critical error when acting on malware or other potentially unwanted software.
197	AV	Windows Defender	NA	Alert	Windows Defender - Engine update failed	This alert is generated when Windows Defender antivirus has encountered an error while trying to update the engine, could not load anti-malware engine and update the platform.
198	Cloud	Microsoft Office365	NA	Alert	Microsoft 365 - Spam Mail Detected	This alert will trigger whenever spam mail is detected in Microsoft 365 Exchange.
199	Cloud	Microsoft Office365	NA	Alert	Microsoft 365 - Threat Detected	This alert will trigger whenever Microsoft 365 ATP module detects malicious/suspicious activity in Exchange.
200	Cloud	Microsoft Office365	NA	Alert	Microsoft 365 - Malicious Email Detected	This alert will trigger whenever some malicious mail is detected in Microsoft 365 Exchange.
201	Cloud	Microsoft Office365	NA	Alert	Microsoft 365 - Security & compliance alerts	This alert will trigger when security & compliance alert policies detect suspicious activities in the office environment.
202	Cloud	Microsoft Office365	NA	Alert	Microsoft 365 - A potentially malicious URL click was detected	This alert will trigger when a user is protected by Safe Links clicks a malicious link. This event is triggered when URL verdict changes are identified by Microsoft Defender for Microsoft 365 or when users override the Safe Links pages.
203	Cloud	Microsoft Office365	NA	Alert	Microsoft 365 - Creation of forwarding/redirect rule	This alert will trigger when someone in your organization creates an inbox rule for their mailbox that forwards or redirects messages to another email account. This policy only tracks inbox rules that are created using Outlook on the web (formerly known as Outlook Web App) or Exchange Online PowerShell.
204	Cloud	Microsoft Office365	NA	Alert	Microsoft 365 - eDiscovery search started or exported	This alert will trigger when someone uses the content search tool in the security and compliance center. An alert is triggered when the following content search activities are performed: A content search is started. The results of a content search are exported. A content search report is exported. Alerts are also triggered when the previous content search activities are performed in association with an eDiscovery case.
205	Cloud	Microsoft Office365	NA	Alert	Microsoft 365 - Elevation of Exchange admin privilege	This alert will trigger when someone is assigned administrative permissions in your Exchange Online organization. For example, when a user is added to the organization management role group in Exchange Online.

206	Cloud	Microsoft Office365	NA	Alert	Microsoft 365 - Email messages containing malware removed after delivery	This alert will trigger when any messages containing malware are delivered to mailboxes in your organization. If this event occurs, Microsoft removes the infected messages from Exchange Online mailboxes using zero-hour auto-purge.
207	Cloud	Microsoft Office365	NA	Alert	Microsoft 365 - Email messages containing phish URLs removed after delivery	This alert will trigger when any phishing messages are delivered to mailboxes in your organization. If this event occurs, Microsoft removes the infected messages from Exchange Online mailboxes using zero-hour auto-purge.
208	Cloud	Microsoft Office365	NA	Alert	Microsoft 365 - Email reported by the user as malware or phish	This alert will trigger when users in your organization report messages as phishing emails using the report message add-in.
209	Cloud	Microsoft Office365	NA	Alert	Microsoft 365 - Malware campaign detected after delivery	This alert will trigger when an unusually large number of messages containing malware are delivered to mailboxes in your organization. If this event occurs, Microsoft removes the infected messages from Exchange Online mailboxes.
210	Cloud	Microsoft Office365	NA	Alert	Microsoft 365 - Malware campaign detected and blocked	This alert will trigger when someone attempts to send an unusually large number of email messages containing a certain type of malware to users in your organization. If this event occurs, the infected messages are blocked by Microsoft and not delivered to the mailboxes.
211	Cloud	Microsoft Office365	NA	Alert	Microsoft 365 - Malware campaign detected in SharePoint and OneDrive	This alert will trigger when an unusually high volume of malware or viruses are detected in the files located in the SharePoint sites or OneDrive accounts in your organization.
212	Cloud	Microsoft Office365	NA	Alert	Microsoft 365 - Messages have been delayed	This alert will trigger when Microsoft cannot deliver email messages to your on-premises organization or a partner server by using a connector. When this happens, the message is queued in Microsoft 365. This alert is triggered when there are 2,000 messages or more that have been queued for more than an hour.
213	Cloud	Microsoft Office365	NA	Alert	Microsoft 365 - Phish delivered due to tenant or user override	This alert will trigger when Microsoft detects an admin or user override allows the delivery of a phishing message to a mailbox. Examples of overrides include an inbox or mail flow rule that allows messages from a specific sender or domain or an anti-spam policy that allows messages from specific senders or domains.
214	Cloud	Microsoft Office365	NA	Alert	Microsoft 365 - Suspicious email sending patterns detected	This alert will trigger when someone in your organization has sent a suspicious email and is at risk of being restricted from sending an email. This is an early warning for behavior that may indicate that the account is compromised, but not severe enough to restrict the user.
215	Cloud	Microsoft Office365	NA	Alert	Microsoft 365 - Tenant restricted from sending an email	This alert will trigger when most of the email traffic from your organization has been detected as suspicious and Microsoft has restricted your organization from sending an email. Investigate any potentially compromised user and admin accounts, new connectors, or open relays, and then contact Microsoft support to unblock your organization.
216	Cloud	Microsoft Office365	NA	Alert	Microsoft 365 - Unusual external user file activity	This alert will trigger when an unusually large number of activities are performed on files in SharePoint or OneDrive by the users outside of your organization. This includes activities such as accessing files, downloading files, and deleting files.
217	Cloud	Microsoft Office365	NA	Alert	Microsoft 365 - Unusual increase in an email reported as phish	This alert will trigger when there is a significant increase in the number of people in your organization using the report message add-in in Outlook to report messages as phishing mail.
218	Cloud	Microsoft Office365	NA	Alert	Microsoft 365 - Unusual volume of external file sharing	This alert will trigger when an unusually large number of files in SharePoint or OneDrive are shared with the users outside of your organization.
219	Cloud	Microsoft Office365	NA	Alert	Microsoft 365 - Unusual volume of file deletion	This alert will trigger when an unusually large number of files are deleted in SharePoint or OneDrive within a short time frame.
220	Cloud	Microsoft Office365	NA	Alert	Microsoft 365 - User impersonation phish delivered to inbox/folder	This alert will trigger when Microsoft detects that an admin or user override has allowed the delivery of a user impersonation phishing message to the inbox (or another user-accessible folder) of a mailbox. Examples of overrides include an inbox or mail flow rule that allows the messages from a specific sender or domain or an anti-spam policy that allows messages from specific senders or domains.
221	Cloud	Microsoft Office365	NA	Alert	Microsoft 365 - User restricted from sending an email	This alert will trigger when someone in your organization is restricted from sending the outbound mail. This typically results when an account is compromised, and the user is listed on the restricted users page in the security & compliance center.
222	Cloud	Microsoft Office365	NA	Alert	Microsoft 365: User login failed due to MFA	This alert is triggered when the user fails to satisfy the strong authentication requirement to login into Microsoft 365.
223	Cloud	Microsoft Office365	NA	Alert	Microsoft 365: User MFA disabled	This alert is triggered when MFA is disabled to a user.

224	Cloud	Microsoft Office365	NA	Alert	Microsoft 365: CAS alerts have been triggered	This alert is triggered when Cloud App Security generates alerts like unusual addition of credentials to an OAuth app, block downloads on non-domain joined devices, etc.
225	Cloud	Microsoft Office365	NA	Alert	Microsoft 365 - Azure active directory login failure	This alert will trigger whenever an Azure AD user tries to login but fails.
226	Cloud	Microsoft Office365	NA	Alert	Microsoft 365 - Exchange Mailbox login failure	This alert will trigger whenever a mailbox user tries to login but fails.
227	Cloud	Microsoft Office365	NA	Alert	Microsoft 365 - Sensitive information detected in Mail	This alert is triggered when sensitive information matches with DLP Rule in Exchange.
228	Cloud	Microsoft Office365	NA	Alert	Microsoft 365 - Sensitive information detected in SharePoint	This alert is triggered when sensitive information matches with DLP Rule in SharePoint.
229	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - Exchange Spam Mail Traffic Details	This report will provide detailed information on spam mail received by the Exchange user.
230	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - Exchange Malware Traffic Details	This report will provide detailed information related to the threats detected by the Microsoft 365 ATP/Defender.
231	Cloud	Microsoft Office365	NA	Flex Report	Microsoft365 - User login failed due to MFA activities	This report will provide information related to user failure to satisfy strong authentication requirement to login which contains information about Username, application, and Source IP address, etc.
232	Cloud	Microsoft Office365	NA	Flex Report	Microsoft365 - User MFA activities	This report will provide information related to MFA enable and Disable activities for the user which contains information about Username, Target Username, and Action, etc.
233	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - CAS alert triggered	This report will provide information related to the Cloud App Security (CAS) alert activities like unusual addition of credential to an OAuth app, block downloads on non-domain joined devices, etc. It will contain filed information username, reason, category, log type, message, etc.
234	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - Activated user detail	This report will provide information related to the Microsoft 365 activated user and Operating System (OS) in use.
235	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - Activation counts	This report will provide an overall summary of the Microsoft 365 activated license and Operating System (OS) in use.
236	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - Active user counts	This report will provide an overall summary of users active on Exchange, OneDrive, SharePoint, Teams, and Yammer.
237	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - Email activity user counts	This report will provide an overall summary of email activities in the Microsoft 365 Exchange server. (receive, send, read)
238	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - Email app usage user counts	This report will provide an overall summary of the application and user using mail for sending/receiving. (Outlook, IMAP, POP3, etc.)
239	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - Email app usage user detail	This report will provide information related to the user using the application for sending/receiving the mail.
240	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - Email app usage version user counts	This report will provide an overall summary for version usage of email clients by the user. (Outlook 2016, Outlook 2013, etc.)
241	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - Exchange Mail Traffic Details	This report will provide an overall summary related to mail matching transport rules (BCL0, BCL1, bad mail, good mail, spam mail, etc.) of Exchange.
242	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - Exchange Message Trace Details	This report will provide detailed information on receiving/sending mail by Exchange users. If mails fail, then this report will provide a reason for failure.
243	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - Mailbox storage usage	This report will provide an overall summary of storage used by the Microsoft 365 Exchange mailbox.
244	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - Mailbox usage detail	This report will provide information for storage used by Microsoft 365 Exchange mailbox for each user.
245	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - Mailbox usage mailbox counts	This report will provide information for active mailbox count.
246	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - Mailbox usage quota status mailbox counts	This report will provide an overall summary for the mailbox when they reach the usage quota
247	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 –Microsoft 365 activation user counts	This report will provide a summary of Microsoft 365 license usage.
248	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - OneDrive activity file counts	This report will provide a count of OneDrive activities (viewed or edited, shared externally, synced, shared internally) done on files.
249	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - OneDrive activity user counts	This report will provide a count of OneDrive activities (viewed or edited, shared externally, synced, shared internally) done by the user.

250	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - OneDrive usage account counts	This report will provide a summary of users actively using OneDrive.
251	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - OneDrive usage account detail	This report will provide a summary of users using OneDrive and a count of activities.
252	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - OneDrive usage file counts	This report will provide the total file used by the user on OneDrive.
253	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - OneDrive usage storage	This report will provide a summary of storage used by OneDrive.
254	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - SharePoint activity user details	This report will provide user activity count in Microsoft 365 SharePoint.
255	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - SharePoint site storage usage	This report will provide a summary of storage used by SharePoint sites.
256	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - Azure active directory admin activities	This report will provide information related to Azure active directory admin activities like user management, group management, permission assigning, etc.
257	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - Azure active directory login activities	This report will provide information for user login activities from various Microsoft 365 applications using the Azure active directory as an authentication server.
258	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - Exchange admin activities	This report will provide detailed information about admin activities for Microsoft 365 Exchange like permission changes on the mailbox, mailbox creation, deletion, or modification, etc.
259	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - Exchange Mailbox login activities	This report will provide detailed information related to the mailbox login activities.
260	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - SharePoint site operations	This report will provide detailed information on activities on Microsoft 365 SharePoint.
261	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - OneDrive file operations	This report will provide detailed information of activities on OneDrive like file uploaded, downloaded, edited, accessed, shared, etc.
262	Cloud	Microsoft Office365	NA	Flex Report	Microsoft 365 - DLP activities	This report will provide information related to DLP activities which contains information about rule name, application, and severity, etc.
263	Cloud	JumpCloud	NA	Alert	JumpCloud - Login Failure Events	This alert is generated when any login failure is detected on JumpCloud user portal, LDAP directory server, SSO application, system (Mac, Linux, Windows), RADIUS server.
264	Cloud	JumpCloud	NA	Alert	JumpCloud - User Granted Admin Privilege	This alert is generated when any user is granted admin sudo privileges on devices by admin. This action will give the user access to create accounts and amend system settings.
265	Cloud	JumpCloud	NA	Alert	JumpCloud - Active Directory Deleted	This alert is generated when an active directory is deleted.
266	Cloud	JumpCloud	NA	Alert	JumpCloud - Admin Created	This alert is generated when an admin is created. Admin account has privilege to amend setting affecting the whole organization and should be monitoring closely.
267	Cloud	JumpCloud	NA	Alert	JumpCloud - System Deleted	This alert is generated when any system is deleted.
268	Cloud	JumpCloud	NA	Alert	JumpCloud - User Account Deleted	This alert is generated when any user is deleted.
269	Cloud	JumpCloud	NA	Alert	JumpCloud - User Account Locked or Suspended	This alert is generated when any user account is locked or suspended. Lockout or account suspension should be monitored as it can be a result of brute force attack.
270	Cloud	JumpCloud	NA	Flex Report	JumpCloud - Login Failure Detected Report	This report gives information about all the login failure events to user portal, systems (Mac, OS, Linux), RADIUS server, LDAP and SSO application. Reports contain IP address, username, event_type, auth method, user_agent, information regarding user location, organization id and other useful information.
271	Cloud	JumpCloud	NA	Flex Report	JumpCloud - Directory Command and Policy Event Report	This report gives the information about command management events, policy management events, file management events, IP list management events.
272	Cloud	JumpCloud	NA	Flex Report	JumpCloud - Directory Object Event Report	This report gives information about directory application, group, translation rule, system, organization, notification and RADIUS server management events.
273	Cloud	JumpCloud	NA	Flex Report	JumpCloud - Directory Integration Event Report	This report gives information about active directory events, ids resource events, samba domain events, workday, and integration events.
274	Cloud	JumpCloud	NA	Flex Report	JumpCloud - Directory User and Admin Event Report	This report provides information related to all user and admin management events such as user/admin create update, delete create. password change, password reset, user account lockout etc.
275	Cloud	JumpCloud	NA	Flex Report	JumpCloud - System Event Report	This category provides information related to user lockout, password change and other system (Mac, Linux, Windows) events.
276	Cloud	JumpCloud	NA	Flex Report	JumpCloud - LDAP and MDM Events Report	This report gives information about LDAP search events and MDM command result. Report contains username who initiated the event, organization, changes, search result and other relevant information.

277	Cloud	JumpCloud	NA	Flex Report	JumpCloud: Login Success Detected Report	This report gives information about all the successful login events to user portal, systems (Mac, OS, Linux), RADIUS server, LDAP and SSO application. Report contains IP address, username, event_type, auth method, user_agent, info regarding user location, organization id and other useful information.
278	Cloud	Google Workspace	NA	Alert	Google Workspace - Login failed	This alert is generated when user fails to login.
279	Cloud	Google Workspace	NA	Alert	Google Workspace - Suspicious login	This alert is generated when any suspicious login is detected.
280	Cloud	Google Workspace	NA	Flex Report	Google Workspace - Admin Activities	This report gives the information about the admin activities performed such as user creation, email log search, google chrome, hangout activities, etc. Reports contains IP address, username, customer id, log type and other fields which will be helpful for further investigation.
281	Cloud	Google Workspace	NA	Flex Report	Google Workspace - Mobile Activities	This report gives the information about all the mobile activities such as device application change, OS update, device compliance status, device action, device ownership, device settings change etc. Reports contains user email, device ID, device type, device events, etc. which can be used for further investigation.
282	Cloud	Google Workspace	NA	Flex Report	Google Workspace - Token Activities	This report gives information about all the OAuth token audit activity events like authorize and revoke. Reports contains IP address, application name which used the token, action as authorize or revoke and other useful details for further investigation.
283	Cloud	Microsoft Azure	NA	Alert	Azure Monitor: Azure service authentication failed	This alert is triggered when the EventTracker receives a failed authentication for an Azure service.
284	Cloud	Microsoft Azure	NA	Alert	Azure Monitor: Threat has been blocked	This alert is triggered when the Azure Security blocks a malicious activity in Azure services.
285	Cloud	Microsoft Azure	NA	Alert	Azure Monitor: Threat has been detected	This alert is triggered when the Azure Security detects a malicious activity in Azure services.
286	Cloud	Microsoft Azure	NA	Alert	Azure Monitor: Azure resources alerts	This alert is triggered when a custom defined alert is generated by Azure. For e.g. CPU exceeding the assigned threshold value.
287	Cloud	Microsoft Azure	NA	Alert	Azure CIS: New policy assignment created	This alert is triggered by EventTracker when it receives an event which contains information on new policy assignment being created.
288	Cloud	Microsoft Azure	NA	Alert	Azure CIS: Network security group created/updated	This alert is triggered by EventTracker when it receives an event which contains information on a network security group being created or updated.
289	Cloud	Microsoft Azure	NA	Alert	Azure CIS: Network security group deleted	This alert is triggered by EventTracker when it receives an event which contains information on deletion of a network security group.
290	Cloud	Microsoft Azure	NA	Alert	Azure CIS: A Network security group rule has been created/updated	This alert is triggered by EventTracker when it receives an event which contains information related to creation or update of a network security group rule.
291	Cloud	Microsoft Azure	NA	Alert	Azure CIS: A network Security group rule has been deleted	This alert is triggered by EventTracker when it receives an event which contains information related to deletion of a network security group rule.
292	Cloud	Microsoft Azure	NA	Alert	Azure CIS: A Security solution has been created or updated	This alert is triggered by EventTracker when it receives an event which contains information on changes on the active security solutions such as, create or update.
293	Cloud	Microsoft Azure	NA	Alert	Azure CIS: A Security solution has been deleted	This alert is triggered by EventTracker when it receives an event which contains information on changes on the active security solutions such as, delete.
294	Cloud	Microsoft Azure	NA	Alert	Azure CIS: An SQL Server Firewall rule has been created/updated	This alert is triggered by EventTracker when it receives an event which contains information on creation or update of a SQL server firewall rule.
295	Cloud	Microsoft Azure	NA	Alert	Azure CIS: An SQL Server Firewall rule has been deleted	This alert is triggered by EventTracker when it receives an event which contains information on deletion of a SQL server firewall rule.
296	Cloud	Microsoft Azure	NA	Alert	Azure CIS: Security Policy has been updated	This alert is triggered by EventTracker when it receives an event which contains information on update of an Azure security policy.
297	Cloud	Microsoft Azure	NA	Flex Reports	Azure Monitor - Security Event Operations	This report generates the summary of security related events such as, antimalware actions taken by Azure security or detections of double extension file execution, etc.
298	Cloud	Microsoft Azure	NA	Flex Reports	Azure Monitor - Virtual machine operations	This report provides a summary of events generated by virtual machines and virtual machine scale sets. Such as, restart VM. This report does not include any administrative actions.
299	Cloud	Microsoft Azure	NA	Flex Reports	Azure Monitor - Virtual machine administrative operations	This report generates the summary of all the administrative actions performed in virtual machine, or virtual machine scale sets such as, restore point create, delete, etc.

300	Cloud	Microsoft Azure	NA	Flex Reports	Azure Monitor - Alerts generated by Azure resources	This report generates, detailed information on custom alerts that are configured in the Azure services and is triggered. It includes, the alert description, alert name, and alert severity.
301	Cloud	Microsoft Azure	NA	Flex Reports	Azure Monitor - Audit Event authorization operations	This report generates a summary of events related to audit activities, such as, SecretGet, Authentication, etc. This includes, values such as operations status, Source Ip address, requested URI, etc
302	Operating System	Linux OS	NA	Alert	Linux - A user or group has been deleted	This alert is triggered when a user or a group is removed or deleted from Linux system.
303	Operating System	Linux OS	NA	Alert	Linux - A user password has been changed or modified	This alert is triggered when password is changed for any user.
304	Operating System	Linux OS	NA	Alert	Linux - Console login failed	This alert is triggered when a user fails to successfully login into Linux system.
305	Operating System	Linux OS	NA	Alert	Linux - Sudoers configuration file has been changed or modified	This alert is triggered when someone tries to change or modify the configuration of sudoers file.
306	Operating System	Linux OS	NA	Flex Report	Linux - Console login failed	This report contains a detailed overview of events associated to failed login by users into Linux system. This includes, current user, parent user, event datetime, terminal and operation status.
307	Operating System	Linux OS	NA	Flex Report	Linux - User command execution activities	This report contains a detailed overview of commands that were executed in user shell. This includes, executed command, shell user, parent user, log datetime, and operation status.
308	Operating System	Linux OS	NA	Flex Report	Linux - Console login and logout activities	This report contains a detailed overview of user login and logout activities. This includes, shell user, parent user, log datetime, and operation status.
309	Operating System	Linux OS	NA	Flex Report	Linux - Mount and Unmount activities	This report contains a detailed overview of device/drive mount or unmount activities into Linux system. This includes, shell user, parent user, log datetime, and operation status.
310	Operating System	Linux OS	NA	Flex Report	Linux - Root Shell Command Execution activities	This report contains a detailed overview of commands executed in root shell. This includes, executed command, shell user, parent user, log datetime, and operation status.
311	Operating System	Linux OS	NA	Flex Report	Linux - Sudo commands execution activities	This report contains a detailed overview of commands executed by elevating user privilege, i.e. ‘sudo’. This includes, executed command, shell user, parent user, and log datetime.
312	Operating System	Linux OS	NA	Flex Report	Linux – File Monitoring	This report contains a detailed overview of activities associated with file monitoring such as, file read, file delete, file create, etc. This includes, username, event datetime, filepath, filename, status, etc.
313	Operating System	Linux OS	NA	Flex Report	Linux - User Management	This report contains a detailed overview of activities performed by any user, such as, user add, user delete, user password change, etc. This includes, shell user, parent user, and log datetime, and operation status.
314	Operating System	Linux OS	NA	Flex Report	Linux - Group Management	This report contains a detailed overview of activities performed by any user, such as, group add, group delete, etc. This includes, shell user, parent user, and log datetime, and operation status.
315	Operating System	Linux OS	NA	Flex Report	Linux - Package Management	This report contains a detailed overview of activities related to software/package install, remove, or update. This includes, shell user, parent user, and log datetime, application/package name, and operation status.
316	EDR	Crowdstrike Falcon	NA	Alert	CrowdStrike Falcon - File Quarantined	This alert is triggered when any suspicious file is quarantined by CrowdStrike Falcon.
317	EDR	Crowdstrike Falcon	NA	Alert	CrowdStrike Falcon - Detection Summary Event	This alert is triggered when any suspicious activity is detected by CrowdStrike Falco or malware-related event triggers in CrowdStike Falcon.
318	EDR	Crowdstrike Falcon	NA	Flex Report	CrowdStrike Falcon – Threat detected	This report gives information regarding the various threat detection in the CrowdStrike Falcon. Reports contain computer name, destination hostname, destination username, parent file name, parent pathname, message, the action is taken and other useful information for further analysis to drill down the incidents.
319	EDR	Crowdstrike Falcon	NA	Flex Report	CrowdStrike Falcon - File Quarantined	This report provides detailed information on the quarantined files by CrowdStrike Falcon. The report contains information about action, parent file path, parent file name, destination username, destination hostname, quarantine file hash value, quarantined filename, quarantined file path, and other useful information for further analysis to drill down the incidents.

320	EDR	Crowdstrike Falcon	NA	Flex Report	CrowdStrike Falcon – Authentication details	This report gives information about the CrowdStrike Falcon AV authentication-related events. Reports contain a destination hostname, destination username, authentication types, destination IP addresses, usernames, and other details that can be used for further investigation.
321	EDR	Crowdstrike Falcon	NA	Flex Report	CrowdStrike Falcon – Document Access	This report gives information about the document accessed by the user in CrowdStrike Falcon. The report contains a destination username, hostname, accessed filename, accessed file path, and other useful information.
322	EDR	Crowdstrike Falcon	NA	Flex Report	CrowdStrike Falcon – AV Scan Results	This report gives information about the CrowdStrike Falcon AV scan results details. Reports contain a destination hostname, destination username, filename, file pathname, file hash, results and scan engine name, and other details that can be used for further investigation.
323	Proxy/Content Filter	Websense WSG	Websense Web Security Gateway (WSG) v7.7 and later	Alert	Websense WSG: Productivity web category access blocked	This alert is generated when any productivity web category access is blocked from Websense WSG.
324	Proxy/Content Filter	Websense WSG	Websense Web Security Gateway (WSG) v7.7 and later	Alert	Websense WSG: Security web category access blocked	This alert is generated when any Security web category access is blocked from Websense WSG.
325	Proxy/Content Filter	Websense WSG	Websense Web Security Gateway (WSG) v7.7 and later	Alert	Websense WSG: Bandwidth web category access blocked	This alert is generated when any Bandwidth web category access is blocked from Websense WSG.
326	Proxy/Content Filter	Websense WSG	Websense Web Security Gateway (WSG) v7.7 and later	Alert	Websense WSG: Baseline web category access blocked	This alert is generated when any Baseline web category access is blocked from Websense WSG
327	Proxy/Content Filter	Websense WSG	Websense Web Security Gateway (WSG) v7.7 and later	Alert	Websense WSG: Social networking web category access blocked	This alert is generated when any Social networking web category access is permitted from Websense WSG.
328	Proxy/Content Filter	Websense WSG	Websense Web Security Gateway (WSG) v7.7 and later	Flex Report	Websense WSG: Security web category access blocked	This report provides information related to security web category which have been blocked.
329	Proxy/Content Filter	Websense WSG	Websense Web Security Gateway (WSG) v7.7 and later	Flex Report	Websense WSG: Security web category access permitted	This report provides information related to security web category which have been given access permit.
330	Proxy/Content Filter	Websense WSG	Websense Web Security Gateway (WSG) v7.7 and later	Flex Report	Websense WSG: Social networking web category access blocked	This report provides information related to social networking web category which have been blocked.
331	Proxy/Content Filter	Websense WSG	Websense Web Security Gateway (WSG) v7.7 and later	Flex Report	Websense WSG: Social networking web category access permitted	This report provides information related to social networking web category which have been given access permit.
332	Proxy/Content Filter	Websense WSG	Websense Web Security Gateway (WSG) v7.7 and later	Flex Report	Websense WSG: Bandwidth web category access blocked	This report provides information related to bandwidth web category that have been blocked.
333	Proxy/Content Filter	Websense WSG	Websense Web Security Gateway (WSG) v7.7 and later	Flex Report	Websense WSG: Bandwidth web category access permitted	This report provides information related to bandwidth web category that have been given access permit.
334	Proxy/Content Filter	Websense WSG	Websense Web Security Gateway (WSG) v7.7 and later	Flex Report	Websense WSG: Baseline web category access blocked	This report provides information related to baseline web category that have been blocked.
335	Proxy/Content Filter	Websense WSG	Websense Web Security Gateway (WSG) v7.7 and later	Flex Report	Websense WSG: Baseline web category access permitted	This report provides information related to baseline web category that have been given access permit.
336	Proxy/Content Filter	Websense WSG	Websense Web Security Gateway (WSG) v7.7 and later	Flex Report	Websense WSG: Productivity web category access blocked	This report provides information related to productivity web category which have been blocked.
337	Proxy/Content Filter	Websense WSG	Websense Web Security Gateway (WSG) v7.7 and later	Flex Report	Websense WSG: Productivity web category access permitted	This report provides information related to productivity web category which have been given access permit.

338	Email Security Gateway	Cisco IronPort	Any version which supports REST API	Alert	Cisco ESA - DLP Event has been detected	This alert is triggered when a message/email content is flagged under DLP.
339	Email Security Gateway	Cisco IronPort	Any version which supports REST API	Alert	Cisco ESA - Message has been dropped by AMP	This alert is triggered when a message/email content is flagged under AMP.
340	Email Security Gateway	Cisco IronPort	Any version which supports REST API	Alert	Cisco ESA - Message has been dropped by Content Filters	This alert is triggered when a message/email content is flagged under Content Filters.
341	Email Security Gateway	Cisco IronPort	Any version which supports REST API	Alert	Cisco ESA- Email quarantined by AntiSpam/Graymail	This alert is triggered when a spam mail/graymail has been quarantined by Cisco ESA.
342	Email Security Gateway	Cisco IronPort	Any version which supports REST API	Flex Report	Cisco ESA – AMP Messages	This report will provide the summary of advanced malware protection (AMP) messages as detected in Cisco ESA. It will include details such as, Event log Time, Email direction, sender/recipient address, AMP details, etc.
343	Email Security Gateway	Cisco IronPort	Any version which supports REST API	Flex Report	Cisco ESA – DLP Messages	This report will provide the summary of Data Loss and Prevention (DLP) messages as detected in Cisco ESA. It includes details such as Event Log Time, Sender/recipient address, types of attachments with the specific email, DLP details, and so on.
344	Email Security Gateway	Cisco IronPort	Any version which supports REST API	Flex Report	Cisco ESA - Emails Quarantined by Anti-Spam Graymail	This report outlines the summary of spam email/ graymail activity that includes, source/recipient address, email direction, SBRS score, and so on.
345	Email Security Gateway	Cisco IronPort	Any version which supports REST API	Flex Report	Cisco ESA - Emails Quarantined by Content Filters	This report generates a details summary of emails that has been flagged/quarantined by content filters. This includes, email direction, sender/recipient address, SBRS score, and so on.
346	Email Security Gateway	Cisco IronPort	Any version which supports REST API	Flex Report	Cisco ESA - Emails Delivered	Thisreport generates a summary of all the inbound and outbound emails that has been successfully delivered. It includes, email direction, sender/recipient address, SBRS score, and so on.
347	Email Security Gateway	Cisco IronPort	Any version which supports REST API	Dashboard	Cisco ESA Events by email direction	
348	Email Security Gateway	Cisco IronPort	Any version which supports REST API	Dashboard	Cisco ESA Events by Message Status	
349	Email Security Gateway	Cisco IronPort	Any version which supports REST API	Dashboard	Cisco ESA incoming email by Source IP address	
350	Email Security Gateway	Cisco IronPort	Any version which supports REST API	Dashboard	Cisco ESA Events by Message Timeline	
351	Email Security Gateway	Cisco IronPort	Any version which supports REST API	Dashboard	Cisco ESA Events by Sender Group	
352	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Alert	Microsoft DNS: Service down	This alert is generated when DNS service is down in Microsoft DNS Server.
353	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Alert	Microsoft DNS: Configuration changes	This alert is generated when configuration changes in scope, zone, or resource record in Microsoft DNS Server.
354	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Alert	Microsoft DNS: Object deletion in zone	This alert is generated when zone or resource record is deleted from any scope in Microsoft DNS Server.
355	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Alert	Microsoft DNS: Name resolution failed	This alert is generated when resolution of FQDN name is failed by Microsoft DNS Server.
356	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Alert	DNS: Malformed domain detected	This alert is generated when EventTracker detect malformed (typosquatted) domains from queries in the DNS logs.
357	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Alert	DNS: Snort high priority alert generated	This alert is generated when Snort detects high priority alerts for DNS.
358	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Alert	DNS: DGA domain detected	This alert is generated when EventTracker detects DGA (Domain generated algorithm) domains from DNS logs.
359	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Alert	DNS: Suspicious DNS settings detected	This alert is generated when DNS setting of clients differs from the recommended settings.
360	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Alert	DNS: Malicious domain detected	This alert is generated when malicious domain is detected from DNS logs.
361	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Alert	DNS: High DNS server latency detected	This alert is generated when latency of DNS server is greater than threshold value.

362	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Alert	DNS: High error query count detected for domain	This alert is generated when error query count is greater than domain threshold.
363	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Alert	DNS: High error query count detected for type	This alert is generated when error query count is greater than record type threshold.
364	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Alert	DNS: High error query count detected from client	This alert is generated when error query count is greater than client threshold.
365	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Alert	DNS: High query count detected for record type	This alert is generated when successful query count is greater than record type threshold.
366	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Alert	DNS: High query count detected from client	This alert is generated when successful query count is greater than client threshold.
367	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Alert	DNS: High query count detected from domain	This alert is generated when successful query count isgreater than domain threshold.
368	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Flex Report	Microsoft DNS-Zone creation, deletion and updating	This report provides information related to zone creation, deletion, and updates in scope and by whom it was made.
369	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Flex Report	Microsoft DNS-Resource record creation and deletion	This report provides information related toresource record creation and deletion in zone and by whom it was made.
370	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Flex Report	Microsoft DNS-Configuration changes	This report provides information related to configuration name changes and by whom it was made.
371	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Flex Report	Microsoft DNS-Query resolution successfully	This report provides information related to FQDN or IP address, query type (forward lookup or reverse), query status, when query successfully resolve from DNS Server.
372	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Flex Report	Microsoft DNS-Query resolution failed	This report provides information related to FQDN or IP address, query type (forward lookup or reverse), query status, when query fails to resolve from DNS Server.
373	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Flex Report	DNS- Error type count details	This report provides information about error queries count for an error type and details of error type.
374	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Flex Report	DNS- Error client count details	This report provides information about error queries count for a client. and details of client IP address.
375	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Flex Report	DNS- Summary client count details	This report provides information about successful query count for a client and details of client IP address.
376	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Flex Report	DNS- Summary query count details	This report provides information about successful query for a FQDN resolution request and details of its count.
377	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Flex Report	DNS- Error query count details	This report provides information about error query for a FQDN resolution request and details of its count.
378	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Flex Report	DNS- Traffic details	This report provides information about the query request to DNS server. It gives details of query request (FQDN, record type) and client details (IP address).
379	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Flex Report	DNS- Summary record type details	This report provides information about successful query for a record type. It gives details of record type requested and count of queries.
380	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Flex Report	DNS-Malicious domain detection details	This report provides information related to detection of malicious domain from DNS logs. It gives information about malicious domain, client trying to access, its record type and when the client is trying to access it.
381	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Flex Report	DNS-Malformed domain detection details	This report provides information related to detection of malformed domain from DNS logs. It gives information about malformed domain, method of creation (typo-squatted methods), client trying to access such domain and its geological details.
382	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Flex Report	DNS-Suspicious DNS settings detection details	This report provides information about suspicious client DNS setting.
383	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Flex Report	DNS-DGA domain detection details	This report provides information on DGA domains detection details (FQDN and its IP) and client details from DNS logs.
384	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Flex Report	DNS-Least resolved domain details	This report provides information about least resolved domain in a network. It gives information on least domains resolved by DNS server and client details.
385	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Flex Report	DNS-Server latency details	This report provides information about the provided DNS server (private and public DNS) and its latency.
386	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Dashboard	Microsoft DNS: Top URL usage	This dashboard gives information about usage of URL in the network.

387	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Dashboard	Microsoft DNS: Resource record operations	This dashboard gives information about the created and deleted resource record in a DNS zone.
388	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Dashboard	Microsoft DNS: Zone operations	This dashboard gives information about the creation, deletion, and the updates of DNS zone.
389	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Dashboard	DNS: Error pattern	This dashboard gives information about query count for an error type.
390	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Dashboard	DNS: Top queried domains	This dashboard gives information about query count for a domain.
391	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Dashboard	DNS: Top queried domains with errors	This dashboard gives information about error query count for a domain.
392	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Dashboard	DNS: Top querying clients	This dashboard gives information about query count for a client.
393	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Dashboard	DNS: Top querying clients with errors	This dashboard gives information about error query count for a client.
394	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Dashboard	DNS: Record type pattern	This dashboard gives information about the query count for a record type.
395	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Dashboard	DNS: Suspicious domains detected	This dashboard gives information on malware domain access from a client.
396	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Dashboard	DNS: Received traffic	This dashboard gives information on received traffic in DNS server.
397	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Dashboard	DNS: Send traffic	This dashboard gives information on send traffic from DNS server.
398	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Dashboard	DNS: Malformed domains detected	This dashboard gives information on typo-squatted domains access from a client.
399	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Dashboard	DNS: Server latency	This dashboard gives information about latency of a public and internal DNS server.
400	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Dashboard	DNS: DGA domain detected	This dashboard gives information on DGA domains access by a client
401	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Dashboard	DNS: Suspicious DNS settings detected	This dashboard gives information about the client having suspicious DNS settings.
402	DNS	Microsoft DNS	n Windows Server 2012 R2 and later	Dashboard	DNS: Least resolved domains	This dashboard gives information about the least resolved domains over the network.
403	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Alert	Cisco FTD: NGIPS has blocked a suspicious connection	This alert is triggered when the Cisco Firepower NGIPS detects a suspicious connection event.
404	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Alert	Cisco FTD: NGIPS has detected a Malware	This alert is triggered when the Cisco Firepower NGIPS detects a File Malware Event.
405	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Alert	Cisco FTD: NGIPS has blocked an intrusion event	This alert is triggered when Cisco Firepower NGIPs detects an intrusion event and blocks it.
406	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Alert	Cisco FTD: Authorization fail detected for admin user	This alert is triggered when Cisco FTD login fails for the admin user.
407	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Alert	Cisco FTD: Authorization fail detected for network user	This alert is triggered when Cisco FTD detects a login failure for network user.
408	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Alert	Cisco FTD: Device console 'enable' password incorrect	This alert is triggered when Cisco FTD receives incorrect credentials for device console that is “enable”.
409	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Alert	Cisco FTD: Device console login failed	This alert is triggered when there is an incorrect login attempt or a failed login to FTD to the console.
410	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Alert	Cisco FTD: Intrusion detection event has been detected	This alert is triggered when the IDS engine discovers a potential attack/scanning on the network.
411	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Alert	Cisco FTD: SSL-VPN invalid client tried to login	This alert is triggered when an invalid/ unknown SSL VPN Client/ AnyConnect client tries to login.
412	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Alert	Cisco FTD: SSL-VPN login fail detected	This alert is triggered when the SSL handshake with remote device fails.

413	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Alert	Cisco FTD: User session request with IP options has been discarded	This alert is triggered when an IP packet is seen with IP options. Because IP options are considered as security risk, the incoming packet is discarded.
414	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Alert	Cisco FTD: User session with possible ARP poisoning in progress	This alert is triggered when the FTD device receives an ARP packet, and the MAC address in the packet differs from the ARP cache entry.
415	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Alert	Cisco FTD: User session with possible footprint/port scanning in progress	This alert is triggered when a real IP packet is denied by ACL. When this event is reoccurring, it becomes suspicious for port scanning/ footprint attempt.
416	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Alert	Cisco FTD: User session with possible IP address spoof detected	This alert is triggered when there is an attack in progress where an adversary is attempting to spoof an IP address on an inbound connection.
417	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Alert	Cisco FTD: user session with possible spoofing attack in progress	This alert is triggered when either FTD device receives a packet with the same IP, but a different MAC address from one of its uauth entries, Or, FTD device receives a packet with exempt MAC address, but a different IP address from the corresponding uauth entry.
418	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Alert	Cisco FTD: User session with teardrop signature detected	This alert is triggered when FTD device discards a packet with a teardrop signature containing either a small offset or fragment overlapping.
419	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Alert	Cisco FTD: VPN session failed	This alert is triggered when a VPN client authentication fails.
420	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Alert	Cisco FTD: WebVPN/AnyConnect session login failed	This alert is triggered when a WebVPN/ AnyConnect authentication is rejected.
421	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Alert	Cisco FTD: WebVPN/AnyConnect session file access denied	This alert is triggered when a file access via a WebVPN/ AnyConnect session is denied for any user.
422	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Alert	Cisco FTD: High memory utilization detected on FTD device	This alert is triggered when the FTD system reports high memory utilization.
423	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Alert	Cisco FTD: Device configuration erased	This alert is triggered when the device configuration is erased by any user.
424	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Alert	Cisco FTD: SSL-VPN unsupported client has been rejected	This alert is triggered when an unsupported AnyConnect client connection is rejected.
425	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Flex Report	Cisco FTD - NGIPS (Intrusion Events)	This report generates a summary of intrusion events as detected by Cisco Firepower NGIPS. It includes, date, time, the type of exploit, and contextual information about the source of the attack and its target.
426	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Flex Report	Cisco FTD - IDS scanning report	This report contains a summary of IDS events when a host is being targeted/ attacked. It includes the destination subnet, or endpoint IP address with action that is being performed on the target system.
427	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Flex Report	Cisco FTD - SSLVPN failed connections	This report has a summary of failed SSLVPN handshakes. This includes source IP/ Source port, destination IP/ destination port, and type of peer type i.e. ‘client’ or ‘server’.
428	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Flex Report	Cisco FTD - VPN client failed connections	This report consists summary of failed VPN client connections. It includes source Ip address and username.
429	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Flex Report	Cisco FTD - WebVPN failed connections	This report is generated when there is a failed login attempt from WebVPN/ AnyConnect client. This includes, the user group name, username, and session type, e.g. ‘WebVPN’ or ‘admin’.
430	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Flex Report	Cisco FTD - SSLVPN successful connections	This report generates a detailed summary of successful SSLVPN handshake with client. This includes, the protocol version used to establish connection, along with peer type, source IP/ source port, and destination Ip/ destination port.
431	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Flex Report	Cisco FTD - VPN client successful connections	This report is generated for successful VPN client connections. It includes, username and source IP address.
432	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Flex Report	Cisco FTD - WebVPN successful connections	This report includes a summary of successful WebVPN/AnyConnect client connections/ sessions. This includes the username, user group name, and source IP address.
433	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Flex Report	Cisco FTD - Device configuration changes	This report is generated for the configuration changes on the FTD device by any user. This includes, username, time of command execution, and the actual command that was executed to make any changes in device configuration.
434	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Flex Report	Cisco FTD – User privilege changed	This report is generated when there is a user privilege change. It includes, username, old privilege level, new privilege level and event timestamp.

435	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Flex Report	Cisco FTD – User management	This report generates a detailed summary of event which includes new user creation in FTD database, and user deletion from FTD database. It includes, username and privilege level assigned to that user.
436	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Flex Report	Cisco FTD – System login failed	This report generates a detailed summary of failed login attempt in Cisco FTD device. It includes, username, source IP/ source port, destination IP/ destination port, and event timestamp.
437	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Flex Report	Cisco FTD – Traffic activity (TCP denied)	This report generates a detailed summary of failed TCP connections. It includes, source IP/ source port, destination IP/ destination port, and event timestamp.
438	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Flex Report	Cisco FTD – Traffic activity (UDP denied)	This report generates a detailed summary of failed UDP connections. It includes, source IP/ source port, destination IP/ destination port, and event timestamp.
439	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Flex Report	Cisco FTD - NGIPS (Network connection)	This report outlines a summary of network connections at the beginning and at the end of a session. This includes SSL flow status, access control rule action, URL accessed, etc.
440	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Flex Report	Cisco FTD - User command execution	This report provides a detailed summary of commands executed by the user, like show config, or run diagnostics.
441	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Flex Report	Cisco FTD – System login success	This report generates a detailed summary of successful login by a user to FTD device. It includes, username, source IP/ source port, destination IP/ destination port, and event timestamp.
442	IPS/IDS	Cisco Firepower Threat Defense (FTD)	Release 6.3 and later	Flex Report	Cisco FTD – Allowed traffic activities	This report generates a detailed summary of allowed traffic connection, like TCP, UDP, or ICMP. It includes, protocol type, source IP/ source port, destination IP/ destination port, and event timestamp.
443	Firewall/UTM	FortiGate Firewall	version 4.0-6.0	Alert	Fortinet: Attack detected	This alert is generated when any IPS alert detected by Fortinet firewall.
444	Firewall/UTM	FortiGate Firewall	version 4.0-6.0	Alert	Fortinet: Virus detected	This alert is generated when any virus is detected by the Fortinet firewall.
445	Firewall/UTM	FortiGate Firewall	version 4.0-6.0	Alert	Fortinet: Data leak protection	This alert is generated when any DLP event is occurred.
446	Firewall/UTM	FortiGate Firewall	version 4.0-6.0	Alert	Fortinet: Configuration changed	This alert is generated when any configuration changes is done in the Fortinet firewall.
447	Firewall/UTM	FortiGate Firewall	version 4.0-6.0	Alert	Fortinet: Administrator logon failed	This alert is generated when there is an administrator does a login failure.
448	Firewall/UTM	FortiGate Firewall	version 4.0-6.0	Flex Report	Fortinet- Attack detected	This report provides details about all the IPS and IDS attacks that is detected by the Fortinet firewall.
449	Firewall/UTM	FortiGate Firewall	version 4.0-6.0	Flex Report	Fortinet- Suspicious web content detected	This report provides details about all the suspicious web traffic content that is detected by the Fortinet firewall.
450	Firewall/UTM	FortiGate Firewall	version 4.0-6.0	Flex Report	Fortinet- Suspicious email content detected	This report provides details about all the suspicious email traffic content that is detected by the Fortinet firewall.
451	Firewall/UTM	FortiGate Firewall	version 4.0-6.0	Flex Report	Fortinet- Data leak detected	This report provides details about all the DLP event that is detected by the Fortinet firewall.
452	Firewall/UTM	FortiGate Firewall	version 4.0-6.0	Flex Report	Fortinet- Virus detected	This report provides details about all the virus that is detected by the Fortinet firewall.
453	Firewall/UTM	FortiGate Firewall	version 4.0-6.0	Flex Report	Fortinet- Configuration changes	This report provides details about all the configuration changes that is done in the Fortinet firewall.
454	Firewall/UTM	FortiGate Firewall	version 4.0-6.0	Flex Report	Fortinet- Traffic allowed details	This report provides details about all the traffic that is allowed by the Fortinet firewall.
455	Firewall/UTM	FortiGate Firewall	version 4.0-6.0	Flex Report	Fortinet- Traffic denied details	This report provides details about all the traffic that is denied by the Fortinet firewall.
456	Firewall/UTM	FortiGate Firewall	version 4.0-6.0	Flex Report	Fortinet- Application control	This report provides details about all the application control policies and rules that is defined by the Fortinet firewall.
457	Firewall/UTM	FortiGate Firewall	version 4.0-6.0	Flex Report	Fortinet- VPN logon details	This report provides details about all the vpn logon details.
458	Firewall/UTM	FortiGate Firewall	version 4.0-6.0	Flex Report	Fortinet- User authentication details	This report provides details about all the user authentication details.
459	Firewall/UTM	FortiGate Firewall	version 4.0-6.0	Flex Report	Fortinet- Administrator logon details	This report provides details about all the admin login and logout activities.
460	Firewall/UTM	Sophos SG/UTM 9	version 15.01.0 - 17.1.2.	Alert	Sophos Firewall - IPS Attacks Detected on System	This alert is generated when a threat is detected by the Sophos Firewall.
461	Firewall/UTM	Sophos SG/UTM 9	version 15.01.0 - 17.1.2.	Alert	Sophos Firewall - Virus or Spam Detected on System	This alert is generated when any virus or spam is detected by the Sophos Firewall.
462	Firewall/UTM	Sophos SG/UTM 9	version 15.01.0 - 17.1.2.	Alert	ophos Firewall - Advance Threat Protection	This alert is generated when any vulnerability is detected in the traffic by the Sophos Firewall.
463	Firewall/UTM	Sophos SG/UTM 9	version 15.01.0 - 17.1.2.	Alert	Sophos Firewall- Firewall Configuration Changed	This alert is generated when any configuration changes are done in Sophos Firewall.

464	Firewall/UTM	Sophos SG/UTM 9	version 15.01.0 - 17.1.2.	Alert	Sophos Firewall - User Logon Failed	This alert is generated when any firewall login failure is attempted.
465	Firewall/UTM	Sophos SG/UTM 9	version 15.01.0 - 17.1.2.	Alert	Sophos Firewall - VPN User Logon Failed	This alert is generated when any VPN login failure is attempted.
466	Firewall/UTM	Sophos SG/UTM 9	version 15.01.0 - 17.1.2.	Alert	Sophos Firewall - VPN Login and Logout	This alert is generated when any VPN login and logout event is detected.
467	Firewall/UTM	Sophos SG/UTM 9	version 15.01.0 - 17.1.2.	Alert	Sophos Firewall - User Login Activities	This alert is generated when any firewall login and logout activity is detected.
468	Firewall/UTM	Sophos SG/UTM 9	version 15.01.0 - 17.1.2.	Flex Report	Sophos Firewall - Security Policy Activity Report	This report provides information related to all the security policy events.
469	Firewall/UTM	Sophos SG/UTM 9	version 15.01.0 - 17.1.2.	Flex Report	Sophos Firewall- Suspicious E-mail Activity Report	This report provides information related to all the email traffic.
470	Firewall/UTM	Sophos SG/UTM 9	version 15.01.0 - 17.1.2.	Flex Report	Sophos Firewall - Content Filter Activity Report	This report provides information related to all the content filtering that is done by the Sophos Firewall.
471	Firewall/UTM	Sophos SG/UTM 9	version 15.01.0 - 17.1.2.	Flex Report	Sophos Firewall - Spam Detected on System Report	This report provides information related to all the spam that is detected by the Sophos Firewall.
472	Firewall/UTM	Sophos SG/UTM 9	version 15.01.0 - 17.1.2.	Flex Report	Sophos Firewall - Intrusion Detected on System Report	This report provides information related to all the IPS attack that is detected by the Sophos Firewall.
473	Firewall/UTM	Sophos SG/UTM 9	version 15.01.0 - 17.1.2.	Flex Report	Sophos Firewall - Virus Detected on System Report	This report provides information related to all the virus that is detected by the Sophos Firewall.
474	Firewall/UTM	Sophos SG/UTM 9	version 15.01.0 - 17.1.2.	Flex Report	Sophos Firewall - Advanced Threat Protection Management Report	This report provides information related to all the threat that is detected by the Sophos Firewall.
475	Firewall/UTM	Sophos SG/UTM 9	version 15.01.0 - 17.1.2.	Flex Report	Sophos Firewall - Administrative Activity Report	This report provides information related to all admin activities.
476	Firewall/UTM	Sophos SG/UTM 9	version 15.01.0 - 17.1.2.	Flex Report	Sophos Firewall - Traffic Accepted or Denied Report	This report provides information related to all the traffic that is allowed and denied by the Sophos Firewall.
477	Firewall/UTM	Sophos SG/UTM 9	version 15.01.0 - 17.1.2.	Flex Report	Sophos Firewall - WAF Traffic Accepted or Denied Report	This report provides information related to all the traffic that is allowed and denied by the Sophos Firewall.
478	Firewall/UTM	Sophos SG/UTM 9	version 15.01.0 - 17.1.2.	Flex Report	Sophos Firewall - Sandbox Activity Report	This report provides information related to all the sandbox activities.
479	Firewall/UTM	Sophos SG/UTM 9	version 15.01.0 - 17.1.2.	Flex Report	Sophos Firewall - System Health Status Report	This report provides information related to all the system health status.
480	Firewall/UTM	Sophos SG/UTM 9	version 15.01.0 - 17.1.2.	Flex Report	Sophos Firewall - Firewall Configuration Change Report	This report provides information related to configuration changes done in Sophos Firewall.
481	Firewall/UTM	Sophos SG/UTM 9	version 15.01.0 - 17.1.2.	Flex Report	Sophos Firewall - FTP File Blocked Report	This report provides information about FTP activities detected by Sophos Firewall.
482	Firewall/UTM	Sophos SG/UTM 9	version 15.01.0 - 17.1.2.	Flex Report	Sophos Firewall - VPN Connection Status Report	This report provides information about VPN activities detected.
483	Firewall/UTM	Sophos SG/UTM 9	version 15.01.0 - 17.1.2.	Flex Report	Sophos Firewall - Administrator Logon or Logoff Report	This report provides information related to all the admin login and logout activity.
484	Firewall/UTM	Sophos SG/UTM 9	version 15.01.0 - 17.1.2.	Flex Report	Sophos Firewall - User Authentication Success Report	This report provides information related to all the firewall login and logout activity.
485	Firewall/UTM	Sophos SG/UTM 9	version 15.01.0 - 17.1.2.	Flex Report	Sophos Firewall - User Authentication Failed Report	This report provides information related to all the firewall login failures that is done.
486	Firewall/UTM	Sophos SG/UTM 9	version 15.01.0 - 17.1.2.	Flex Report	Sophos Firewall - VPN User Logon or Logoff Success Report	This report provides information related to all the VPN login and logout activity.
487	Firewall/UTM	Sophos SG/UTM 9	version 15.01.0 - 17.1.2.	Flex Report	Sophos Firewall - VPN User Logon Failed Report	This report provides information related to all the VPN login failures that is done.
488	Firewall/UTM	Palo Alto Appliance	PanOS version (2.0-8.1)	Alert	Palo Alto Firewall: Virus detected	This alert is generated when any virus is detected in the traffic by the Palo Alto Firewall.
489	Firewall/UTM	Palo Alto Appliance	PanOS version (2.0-8.1)	Alert	Palo Alto Firewall: Vulnerability detected	This alert is generated when any vulnerability is detected in the traffic by the Palo Alto Firewall.
490	Firewall/UTM	Palo Alto Appliance	PanOS version (2.0-8.1)	Alert	Palo Alto Firewall: Configuration success and failure	This alert is generated when any configuration success or failure is done in the Palo Alto Firewall.
491	Firewall/UTM	Palo Alto Appliance	PanOS version (2.0-8.1)	Alert	Palo Alto Firewall: VPN configuration changes	This alert is generated when any vpn configuration changes is done in the Palo Alto Firewall.
492	Firewall/UTM	Palo Alto Appliance	PanOS version (2.0-8.1)	Alert	Palo Alto Firewall: Logon failure	This alert is generated when any logon failure is attempted in the Palo Alto Firewall.
493	Firewall/UTM	Palo Alto Appliance	PanOS version (2.0-8.1)	Alert	Palo Alto Firewall: VPN login failures	This alert is generated when any vpn login failure is attempted in the Palo Alto Firewall.
494	Firewall/UTM	Palo Alto Appliance	PanOS version (2.0-8.1)	Flex Report	Palo Alto Firewall- Threat details	This report provides information related to threat detection which includes threat id, protocol type, action taken, source address, source port, source location, destination address, destination port and destination location.

495	Firewall/UTM	Palo Alto Appliance	PanOS version (2.0-8.1)	Flex Report	Palo Alto Firewall- Traffic details	This report provides information related to traffic flow which includes session id, source address, source port, source location, destination address, destination port, destination location, protocol type, total bytes, bytes sent, bytes received, total packets, packets sent and packets received.
496	Firewall/UTM	Palo Alto Appliance	PanOS version (2.0-8.1)	Flex Report	Palo Alto Firewall- Configuration success or failure	This provides information related to changes that happens in configuration of Palo Alto firewall which includes user, source IP, console type, and configuration path.
497	Firewall/UTM	Palo Alto Appliance	PanOS version (2.0-8.1)	Flex Report	Palo Alto Firewall- VPN configuration changes	This report provides information related to vpn configuration changes that is done in Palo Alto firewall which includes user, source IP, console type, and configuration path.
498	Firewall/UTM	Palo Alto Appliance	PanOS version (2.0-8.1)	Flex Report	Palo Alto Firewall- Logon failure	This report provides information related to user logon failure in Palo Alto firewall which includes source IP, user and reason.
499	Firewall/UTM	Palo Alto Appliance	PanOS version (2.0-8.1)	Flex Report	Palo Alto Firewall- Logon success	This report provides information related to user login success in Palo Alto firewall which includes source IP and user.
500	Firewall/UTM	Palo Alto Appliance	PanOS version (2.0-8.1)	Flex Report	Palo Alto Firewall- VPN login and logout activity	This report provides information related to VPN user login and logout activity which include user name, source IP, status and reason.
501	Firewall/UTM	Palo Alto Appliance	PanOS version (2.0-8.1)	Flex Report	Palo Alto Firewall- VPN login failures	This report provides information related to vpn logon failure in Palo Alto firewall which includes source IP, user and reason.
502	Switch	Cisco Switch	series 2600, 2800, 1900, 2900, 3900, 4500, 6500 with IOS 12.x and 15.x	Alert	Cisco Switch : Interface down or detached	This alert is generated when interface down or detached event occurs.
503	Switch	Cisco Switch	series 2600, 2800, 1900, 2900, 3900, 4500, 6500 with IOS 12.x and 15.x	Alert	Cisco Switch : Internal software error	This alert is generated when internal software error occurs.
504	Switch	Cisco Switch	series 2600, 2800, 1900, 2900, 3900, 4500, 6500 with IOS 12.x and 15.x	Alert	Cisco Switch : Line protocol down	This alert is generated when line protocol is down.
505	Switch	Cisco Switch	series 2600, 2800, 1900, 2900, 3900, 4500, 6500 with IOS 12.x and 15.x	Alert	Cisco Switch : Runaway processes	This alert is generated when runaway processes occur.
506	Switch	Cisco Switch	series 2600, 2800, 1900, 2900, 3900, 4500, 6500 with IOS 12.x and 15.x	Alert	Cisco Switch : Configuration changed	This alert is generated when any configuration change event occurs.
507	Switch	Cisco Switch	series 2600, 2800, 1900, 2900, 3900, 4500, 6500 with IOS 12.x and 15.x	Flex Report	Cisco Switch -Access denied	This report provides information related to connection denial events occurring on router or switch which includes Source address, Source Port, Destination Address, Destination port and Packets Transferred fields.
508	Switch	Cisco Switch	series 2600, 2800, 1900, 2900, 3900, 4500, 6500 with IOS 12.x and 15.x	Flex Report	Cisco Switch-VLAN management	This report provides information related to activities that occurs within the VLAN.
509	Switch	Cisco Switch	series 2600, 2800, 1900, 2900, 3900, 4500, 6500 with IOS 12.x and 15.x	Flex Report	Cisco Switch -Administrative account activity	This report provides information related to account activities that is done by the administrator.
510	Switch	Cisco Switch	series 2600, 2800, 1900, 2900, 3900, 4500, 6500 with IOS 12.x and 15.x	Flex Report	Cisco Router-VTP management	This report provides information related to activities that occurs with the VTP.
511	Switch	Cisco Switch	series 2600, 2800, 1900, 2900, 3900, 4500, 6500 with IOS 12.x and 15.x	Flex Report	Cisco Switch -Port status change	This report provides information related to port status changed from UP to DOWN or vice-versa which includes Device Address, Interface Name and Port Status fields.
512	Switch	Cisco Switch	series 2600, 2800, 1900, 2900, 3900, 4500, 6500 with IOS 12.x and 15.x	Flex Report	Cisco Switch -Authentication failure	This report provides information related to authentication failure that is whenever the user tries to login into one of the Cisco Switch .
513	Switch	Cisco Switch	series 2600, 2800, 1900, 2900, 3900, 4500, 6500 with IOS 12.x and 15.x	Flex Report	Cisco Switch -User logon success	This report provides information related to user logon success which includes User Name, Source Address and Source Port fields.

514	Switch	Cisco Switch	series 2600, 2800, 1900, 2900, 3900, 4500, 6500 with IOS 12.x and 15.x	Flex Report	Cisco Switch -User logon failure	This report provides information related to user logon failure which includes User Name, Source Address, Source Port and Reason fields.
515	Switch	Cisco Switch	series 2600, 2800, 1900, 2900, 3900, 4500, 6500 with IOS 12.x and 15.x	Flex Report	Cisco Switch -Configuration changed	This report provides information related to configuration changes which include Device Address, User Name, and Command Issued fields.
516	Switch	Cisco Switch	series 2600, 2800, 1900, 2900, 3900, 4500, 6500 with IOS 12.x and 15.x	Flex Report	Cisco Router-Port security	This report provides information related to port security violation.
517	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Alert	Cisco NAC: Access-point addition failed	This alert is generated when access-point addition failed.
518	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Alert	Cisco NAC: Admin login failed	This alert is generated when admin login failed.
519	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Alert	Cisco NAC: CAS disconnected	This alert is generated when CAS disconnected.
520	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Alert	Cisco NAC: Guest login failed	This alert is generated when guest login failed.
521	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Alert	Cisco NAC: IPSec error	This alert is generated when IPSec error.
522	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Alert	Cisco NAC: Remote login failed	This alert is generated when remote login failed.
523	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Alert	Cisco NAC: Rogue AP report error	This alert is generated when rogue AP report error.
524	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Alert	Cisco NAC: Unknown/Blocked WLC found	This alert is generated when unknown/Blocked WLC found.
525	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Alert	Cisco NAC: User login failed	This alert is generated when user login failed
526	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Alert	Cisco NAC: User session timeout	This alert is generated when user session timeout.
527	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Alert	Cisco NAC: Wireless user login failed	This alert is generated when wireless user login failed.
528	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: Access-point addition failed	This category based report provides information related to access-point addition failed.
529	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: Admin login failed	This category based report provides information related to admin login failed.
530	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: Admin session expired	This category based report provides information related to admin session expired.
531	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: Admin user setup failed	This category based report provides information related to admin user setup failed.

532	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: Agent update failed	This category based report provides information related to agent update failed.
533	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: Automatic user logoff	This category based report provides information related to automatic user logoff.
534	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: CAS disconnected	This category based report provides information related to CAS disconnected.
535	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: CAS-CAM sync error	This category based report provides information related to CAS-CAM sync error.
536	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: Device added to MAC list	This category based report provides information related to device added to MAC list.
537	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: Guest login failed	This category based report provides information related to guest login failed.
538	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: IPSec error	This category based report provides information related to IPSec error.
539	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: License check failed	This category based report provides information related to license check failed.
540	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: Logout failed	This category based report provides information related to logout failed.
541	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: NAT mapping error	This category based report provides information related to NAT mapping error.
542	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: New admin group setup failed	This category based report provides information related to new admin group setup failed.
543	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: Policy update failed	This category based report provides information related to policy update failed.
544	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: RADIUS authentication failed	This category based report provides information related to RADIUS authentication failed.
545	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: Remote login failed	This category based report provides information related to remote login failed.
546	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: Rogue AP report error	This category based report provides information related to rogue AP report error.
547	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: Server update failed	This category based report provides information related to server update failed.
548	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: SNMP trap setup failed	This category based report provides information related to SNMP trap setup failed.
549	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: Unable to add device	This category based report provides information related to unable to add device.

550	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: Unable to add temp user	This category based report provides information related to unable to add temp user.
551	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: Unable to set VLAN for wireless user	This category based report provides information related to unable to set VLAN for wireless user.
552	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: Unknown/Blocked WLC found	This category based report provides information related to unknown/Blocked WLC found.
553	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: User account deletion failed	This category based report provides information related to user account deletion failed.
554	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: User account modification failed	This category based report provides information related to user account modification faile
555	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: User account setup failed	This category based report provides information related to user account setup fail
556	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: User login failed	This category based report provides information related to user login failed.
557	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: User session timeout	This category based report provides information related to user session timeout.
558	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: Wireless user deletion failed	This category based report provides information related to wireless user deletion failed.
559	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	3300 Series and later.	Flex Report	Cisco NAC: Wireless user login failed	This category based report provides information related to wireless user login failed.
560	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	5500 Series, IOS version 8.0.140 and later.	Alert	Cisco Wlc-Attack detection	This alert is generated when any Attack is detected in the Wireless Controller.
561	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	5500 Series, IOS version 8.0.140 and later.	Alert	Cisco Wlc-Port status changed	This alert is generated when any Port status is changed.
562	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	5500 Series, IOS version 8.0.140 and later.	Alert	Cisco Wlc-ACL configuration failed	This alert is generated when any Access list configuration fails.
563	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	5500 Series, IOS version 8.0.140 and later.	Alert	Cisco Wlc-System failures	This alert is generated when any System failure occurs
564	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	5500 Series, IOS version 8.0.140 and later.	Alert	Cisco Wlc-AP login success	This alert is generated when any Access Point successfully logs in.
565	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	5500 Series, IOS version 8.0.140 and later.	Alert	Cisco Wlc-AP login failure	This alert is generated when any Access Point login fails.
566	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	5500 Series, IOS version 8.0.140 and later.	Alert	Cisco Wlc-AP registration failures	This alert is generated when any Access Point registration fails.
567	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	5500 Series, IOS version 8.0.140 and later.	Flex Report	Cisco Wlc-Attack detection	This report provides details about any Attack that is attempted to compromise the Wlc.

568	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	5500 Series, IOS version 8.0.140 and later.	Flex Report	Cisco Wlc-Port status changed	This report provides details on the Port status associated with the Wlc.
569	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	5500 Series, IOS version 8.0.140 and later.	Flex Report	Cisco Wlc-Rogue AP activities	This report provides details about all the Rogue Access Point that is detected in the network.
570	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	5500 Series, IOS version 8.0.140 and later.	Flex Report	Cisco Wlc-ACL configuration failed	This report provides details about any Access List configuration failures that occurs in Cisco Wlc.
571	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	5500 Series, IOS version 8.0.140 and later.	Flex Report	Cisco Wlc-System failures	This report provides details about all the System failures, hardware failures and memory allocation failures in the Wlc.
572	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	5500 Series, IOS version 8.0.140 and later.	Flex Report	Cisco Wlc-User account management	This report provides details about all the User account management that is done in Wlc.
573	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	5500 Series, IOS version 8.0.140 and later.	Flex Report	Cisco Wlc-DHCP activities	This report provides details on all the DHCP activities that is done on the Wlc.
574	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	5500 Series, IOS version 8.0.140 and later.	Flex Report	Cisco Wlc-AP login success	This report provides details on all successful Access Point logon that is done.
575	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	5500 Series, IOS version 8.0.140 and later.	Flex Report	Cisco Wlc-AP login failure	This report provides details on Access Point logon failure attempts.
576	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	5500 Series, IOS version 8.0.140 and later.	Flex Report	Cisco Wlc-AP registration failures	This report provides details about all the Access Point registration failures that is done.
577	Wireless Lan Controller (WLC)/Network Access Control (NAC)	Cisco Wireless Lan Controller	5500 Series, IOS version 8.0.140 and later.	Flex Report	Cisco Wlc-Successful AP registrations	This report provides details about all the successful Access Point registration or association with Wlc.
578	Web Server	Microsoft IIS	8.5 and later	Flex Report	Microsoft IIS – Directory traversal	This report provides information related to restricted directories.
579	Web Server	Microsoft IIS	8.5 and later	Flex Report	Microsoft IIS – Backup finder	This report provides information related to suspicious commands running by the client for data backup.
580	Web Server	Microsoft IIS	8.5 and later	Flex Report	Microsoft IIS – Cross site scripting	This report provides information about suspicious cross site scripting queries run by the client.
581	Web Server	Microsoft IIS	8.5 and later	Flex Report	Microsoft IIS – Malicious SQL injection	This report provides information about suspicious SQL queries run by the client which we can be compared with the MSSQL-Extended error details report for investigating SQL injection
582	Web Server	Microsoft IIS	8.5 and later	Flex Report	Microsoft IIS - Web traffic details	This report provides information of all HTTP request and responses sent and received by IIS server.
583	Web Server	Microsoft IIS	8.5 and later	Flex Report	Microsoft IIS - Site with errors	This report provides count and error codes for requested URI’s.
584	Web Server	Microsoft IIS	8.5 and later	Flex Report	Microsoft IIS - Referral report	This report provides information about the client accessed URI’s.
585	Web Server	Apache	2.4.43 and later.	Alert	Apache-Request Forbidden	This alert is generated when resources or data stored is moved or removed from the database.
586	Web Server	Apache	2.4.43 and later.	Alert	Apache-Moved Permanently	This alert is generated when access is not allowed to the server due to several authentication criteria.
587	Web Server	Apache	2.4.43 and later.	Alert	Apache-Access Denied	This alert is generated when user logon is failed (e.g. http 401, 403).
588	Web Server	Apache	2.4.43 and later.	Flex Report	Apache-Backup Finder	This report provides the Web traffic details of the user traversal when accessing an Apache web page
589	Web Server	Apache	2.4.43 and later.	Flex Report	Apache-Directory Traversal	This report provides information of ways in which an HTTP exploit takes place which allows attackers to access restricted directories and execute commands outside of the web server's root directory.

590	Web Server	Apache	2.4.43 and later.	Flex Report	Apache-Sql Injection	This report provides information related to flex master user login successful from specified IP address. It consists of columns LogTime, Device Name, User Name and Source IP.This report provides information about the attackers who are trying to do sql injection on apache web server. It also provides information about the uri on which attacker is trying to execute suspicious sql queries which we can correlate with sql syntax error to confirm whether it is a possible sql injection or not.
591	Web Server	Apache	2.4.43 and later.	Flex Report	Apache-URI Error	This report provides information related to users using incorrect uri to access the server which is not recognized or rejected by apache.
592	Web Server	Apache	2.4.43 and later.	Flex Report	Apache-Page Views	This report provides us the information about the browser pages accessed by the user.
593	Web Server	Apache	2.4.43 and later.	Flex Report	Apache-Traffic Details	This report provides the Web traffic details of the user traversal when accessing an Apache web page
594	Web Server	Apache	2.4.43 and later.	Flex Report	Apache-Client Access Error	This report provides information regarding the various errors on the server when any request is given by the client.
595	Web Server	Apache	2.4.43 and later.	Flex Report	Apache-Server Error	This report provides the different Server side and database errors when trying to access the Apache Server.
596	Load Balancer/Local Traffic Manager (LTM)	F5 BIG-IP	Firmware version 9.x to 14.x	Alert	F5 BIG IP LTM Login Failed	This alert will be generated when there is a failed or unauthorized login attempt by the user.
597	Load Balancer/Local Traffic Manager (LTM)	F5 BIG-IP	Firmware version 9.x to 14.x	Flex Report	F5 BIG IP LTM Login Failed	This report will generate a detailed view on failed or unauthorized login attempts.
598	Load Balancer/Local Traffic Manager (LTM)	F5 BIG-IP	Firmware version 9.x to 14.x	Flex Report	F5 BIG IP LTM Login and Logout activity	This report will provide a detailed view of user access management.
599	Load Balancer/Local Traffic Manager (LTM)	F5 BIG-IP	Firmware version 9.x to 14.x	Flex Report	F5 BIG IP LTM Traffic Management Activity	This report will generate detailed view on local traffic activities as discovered by the F5 appliance. This report also includes activities related configuration changes on F5 BIG IP LTM.
600	Load Balancer/Local Traffic Manager (LTM)	F5 BIG-IP	Firmware version 9.x to 14.x	Flex Report	F5 BIG IP GTM Activity	This report will generate detailed view on global traffic activities as discovered by the F5 appliance.
601	Load Balancer/Local Traffic Manager (LTM)	F5 BIG-IP	Firmware version 9.x to 14.x	Flex Report	F5 BIG IP LTM SSL Activity	This report will generate a detailed view of all the SSL related activities.
602	DHCP	Microsoft DHCP Server	Server 2003 and later.	Alert	Microsoft DHCP Server-Lease expired	This alert is generated when DHCP lease is expired.
603	DHCP	Microsoft DHCP Server	Server 2003 and later.	Alert	Microsoft DHCP Server-Database migration	This alert is generated when DHCP database migration occurs.
604	DHCP	Microsoft DHCP Server	Server 2003 and later.	Alert	Microsoft DHCP Server-Lease deleted	This alert is generated when lease deleted by DHCP Server.
605	DHCP	Microsoft DHCP Server	Server 2003 and later.	Alert	Microsoft DHCP Server-Authorization failure	This alert is created when a DHCP Server authorization fails.
606	DHCP	Microsoft DHCP Server	Server 2003 and later.	Flex Report	Microsoft DHCP Server-Lease renewed by client	This report provides information related to lease renewed by client, when a client already has lease and needs to renew that lease with the DHCP server. It consists of columns EventDate, EventTime, Computer, Client Host Name, Client IP Address and Client MAC Address.
607	DHCP	Microsoft DHCP Server	Server 2003 and later.	Flex Report	Microsoft DHCP Server-DNS update request	This report provides the information related to DNS update request, where DHCP sends request to DNS to dynamically update resource records to DNS. It consists of columns EventDate, EventTime, Computer, Client Host Name and Client IP Address.
608	DHCP	Microsoft DHCP Server	Server 2003 and later.	Flex Report	Microsoft DHCP Server-DNS update successful	This report provides the information about DNS update successful, when DNS registers the resource records successfully upon receiving DNS update request by DHCP. It consists of columns EventDate, EventTime, Computer, Client Host Name and Client IP Address.
609	DHCP	Microsoft DHCP Server	Server 2003 and later.	Flex Report	Microsoft DHCP Server-Lease denied	This report provides the information related to lease denied, where client lease requests might be denied by the DHCP server for invalid (out of pool) or duplicate IP addresses to avoid IP addresses conflicts. It consists of columns EventDate, EventTime, Computer, Client Host Name, Client IP Address and Client MAC Address.
610	Hyper-V	Microsoft Windows Hyper-V	Server 2008 and later.	Alert	Microsoft Windows Hyper V: Configuration error	This alert is generated when a configuration error has occurred in the system
611	Hyper-V	Microsoft Windows Hyper-V	Server 2008 and later.	Alert	Microsoft Windows Hyper V: Network adapter create failed	This alert is generated when a network had failed to create a network adapter.
612	Hyper-V	Microsoft Windows Hyper-V	Server 2008 and later.	Alert	Microsoft Windows Hyper V: Network conflict	This alert is generated when a network conflict has occurred at another adapter.

613	Hyper-V	Microsoft Windows Hyper-V	Server 2008 and later.	Alert	Microsoft Windows Hyper V: Network resource error	This alert is generated when certain type of network resource error has occurred.
614	Hyper-V	Microsoft Windows Hyper-V	Server 2008 and later.	Alert	Microsoft Windows Hyper V: System create failed	This alert is generated when a system fails to create the given path.
615	Hyper-V	Microsoft Windows Hyper-V	Server 2008 and later.	Alert	Microsoft Windows Hyper V: Virtual machine shut down	This alert is generated when virtual machine is shut down.
616	Hyper-V	Microsoft Windows Hyper-V	Server 2008 and later.	Flex Report	Microsoft Windows Hyper V-Virtual switch created	This report provides information related to switch created where it explains about which switch is created along with their port name and the fields are Computer, Switch Name and Port Name.
617	Hyper-V	Microsoft Windows Hyper-V	Server 2008 and later.	Flex Report	Microsoft Windows Hyper V-Image management service status	This report provides information related to image management service that is whether the service has been started or stopped along with the fields Computer and Status.
618	Hyper-V	Microsoft Windows Hyper-V	Server 2008 and later.	Flex Report	Microsoft Windows Hyper V-Virtual hard disk partition management	This report provides information related to hard disk management that explains about hard disk partition and the value of partition with the fields Computer, Partition Status and Partition Number.
619	Hyper-V	Microsoft Windows Hyper-V	Server 2008 and later.	Flex Report	Microsoft Windows Hyper V-Virtual SAN management	This report provides information related to SAN management that is whether the storage area network has been created or deleted with the fields Computer, Storage Area Network Name and Status.
620	Hyper-V	Microsoft Windows Hyper-V	Server 2008 and later.	Flex Report	Microsoft Windows Hyper V-VM failed to unregister	This report provides information related to un-registered virtual machine that explains regarding the configuration of the machine where an error occurs to be failed with the fields Machine Name and Status.
621	Hyper-V	Microsoft Windows Hyper-V	Server 2008 and later.	Flex Report	Microsoft Windows Hyper V-Virtual machine create	This report provides information related to virtual machine that is, it explains whether the virtual machine has been created along with path of hard disk location and the fields Computer, Machine Name and Status.
622	Hyper-V	Microsoft Windows Hyper-V	Server 2008 and later.	Flex Report	Microsoft Windows Hyper V-Virtual machine operational message	This report provides information related to virtual machine operational messages which explains whether the machine was restored, started, saved, paused, resumed, reset and reset by the guest operating system with the fields Computer, Machine Name and Operation Message.
623	Hyper-V	Microsoft Windows Hyper-V	Server 2008 and later.	Flex Report	Microsoft Windows Hyper V-Virtual disk image management	This report provides information related to virtual disk image management which explains about different managements like create, convert, expand, compact, or failed to create etc along with their fields Computer, File Path and Status.
624	Hyper-V	Microsoft Windows Hyper-V	Server 2008 and later.	Flex Report	Microsoft Windows Hyper V-Virtual Switch management	This report provides information related to virtual switch management that explains whether the virtual switch has been created or deleted or set up along with their fields Computer, Machine Name and Status.
625	Identity and Access Management	Windows Active Directory		Alert	Possible Pass the Ticket attack detected	This alert triggeres when there is match for Event ID 4769 and the status code is 0x1F
626	Identity and Access Management	Windows Active Directory		Alert	Malformed anomalous Kerberos activity detected	This alert triggers if there are logon attempts for blank usernames (Event ID 4624 or 4672 or 4634 and username blank)
627	Identity and Access Management	Windows Active Directory		Alert	Kerberoasting Detected	Accounts making numerous requests, Event ID 4769, within a small time frame, especially if they also request RC4 encryption [Type 0x17]
628	Identity and Access Management	Windows Active Directory		Alert	AS-REP Roasting Detected	Accounts making numerous requests, Event ID 4768 and 4769, within a small time frame, especially if they also request RC4 encryption [Type 0x17], pre-authentication not required [Type: 0x0]).
629	Identity and Access Management	Windows Active Directory		Alert	Non-Business hours Account logon detected	Account logon detected outside office hours
630	Identity and Access Management	Windows Active Directory		Alert	Unusual account activity detected	Track and match non-active accounts, disabled account or guest accounts on logon events
631	Identity and Access Management	Windows Active Directory		Alert	Non-comply account activity detected	Your organization might have specific naming conventions for account names. Monitor “User ID” for names that don’t comply with naming conventions.(Ex: Contoso-user1, contoso-user2 - Try looking for accounts without contose)
632	Identity and Access Management	Windows Active Directory		Alert	Simultaneous logon activity Detected	One account loging into various machines in certain time period

633	Identity and Access Management	Windows Active Directory		Alert	Pass the hash attack detected	NTLM LogonType 3 authentications that are not associated to a domain login and are not anonymous logins are suspicious. 4624 events on your workstations with: Logon Type = 9 Authentication Package = Negotiate Logon Process = seclogo
634	Identity and Access Management	Windows Active Directory		Alert	AD Group Policy Discovery Detected	Monitor for abnormal LDAP queries with filters for groupPolicyContainer and high volumes of LDAP traffic to domain controllers. Windows Event ID 4661 can also be used to detect when a directory service has been accessed.
635						Monitor for suspicious use of gpresult. Monitor for the use of PowerShell functions such as Get-DomainGPO and Get-DomainGPOLocalGroup and processes spawning with command-line arguments containing GPOLocalGroup.
636	Identity and Access Management	Windows Active Directory		Alert	Credential Dumping Detected	Monitor activit related to "system32/config/SAM"
637	Identity and Access Management	Windows Active Directory		Alert	Account Manipulation Detected	Monitor for usage of command arguments or parameters authorized_keys or /etc/ssh/sshd_config or Add-MailboxPermission or localgroup
638	Identity and Access Management	Windows Active Directory		Alert	Domain or Group Policy modification detected	Monitor for newly constructed active directory objects, such as Windows EID 5137.
639	Identity and Access Management	Windows Active Directory		Alert	Domain or Group Policy deletion detected	Monitor for unexpected deletion of an active directory object, such as Windows EID 5141.
640	Identity and Access Management	Windows Active Directory		Alert	Access Token Manipulation Detected	Monitor for runas commad
641						Monitor for API calls, loaded by a payload, for token manipulation only through careful analysis of user network activity, examination of running processes, and correlation with other endpoint and network behavior. There are many Windows API calls a payload can take advantage of to manipulate access tokens (e.g., LogonUser, DuplicateTokenEx, and ImpersonateLoggedOnUser).
642	Identity and Access Management	Windows Active Directory		Alert	SID-History Injection detected	Monitor event ID 4766 or 4765
643	Identity and Access Management	Windows Active Directory		Alert	Account access removed activity	Event ID 4726 - A user account was deleted, Event ID 4725 - A user account was disabled
644						Net utility, Set-LocalUser and Set-ADAccountPassword PowerShell cmdlets may be used by adversaries to modify user accounts.
645	Identity and Access Management	Windows Active Directory		Alert	AD User Privilege Escalation Detected	4728(S) : A member was added to a security-enabled global group. 4729(S) : A member was removed from a security-enabled global group. 4732(S) : A member was added to a security-enabled local group. 4733(S) : A member was removed from a security-enabled local group. 4746(S) : A member was added to a security-disabled local group. 4747(S) : A member was removed from a security-disabled local group. 4751(S) : A member was added to a security-disabled global group. 4752(S) : A member was removed from a security-disabled global group. 4756(S) : A member was added to a security-enabled universal group. 4757(S) : A member was removed from a security-enabled universal group. 4761(S) : A member was added to a security-disabled universal group. 4762(S) : A member was removed from a security-disabled universal group.
646	Identity and Access Management	Windows Active Directory		Alert	Domain Trust Modification Detected	Monitor for PowerShell commands such as: Update-MSOLFederatedDomain –DomainName: "Federated Domain Name", or Update-MSOLFederatedDomain –DomainName: "Federated Domain Name" –supportmultipledomain
647	Identity and Access Management	Windows Active Directory		Alert	File and Directory Permission Modification detected	Monitor for newly constructed processes and/or command-lines that can interact with the DACLs using built-in Windows commands, such as icacls, cacls, takeown, and attrib, which can grant adversaries higher permissions on specific files and folders.
648	Identity and Access Management	Windows Active Directory		Alert	Modify Authentication Process: Reversible Encryption Detected	Monitor property changes in Group Policy: Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Store passwords using reversible encryption. By default, the property should be set to Disabled.
649						Monitor command-line usage for -AllowReversiblePasswordEncryption $true or other actions that could be related to malicious tampering of user settings (i.e. Group Policy Modification).

References
https://attack.mitre.org/techniques/enterprise/
https://www.netsurion.com/knowledge-packs