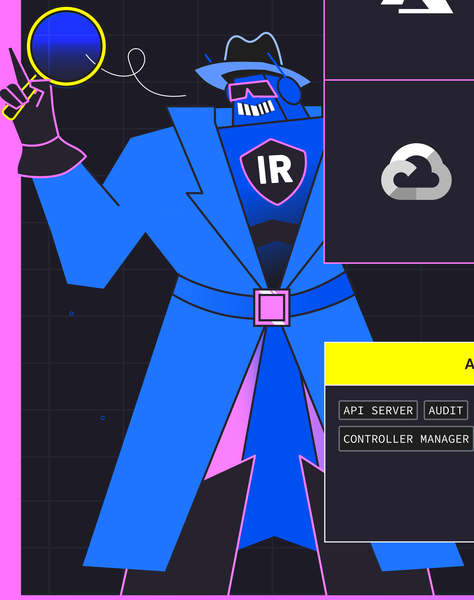
Cloud DFIR



Cloud Service Provider	Log Source	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Exfiltration	Impact
aws	CLOUDTRAIL MANAGEMENT EVENTS CLOUDTRAIL DATA EVENTS*	CONSOLELOGIN GETSIGNINTOKEN PASSWORDRECOVERY REQUESTED	CREATEENVIRONMENT CREATESESSION INVOKE INVOKEMODEL MODIFYINSTANCEATTRIBUTE SENDCOMMAND STARTSESSION	AUTHORIZESECURITYGROUPINGRESS CHANGEPASSWORD CREATEACCESSKEY CREATEFUNCTION20150331 CREATEKEYPAIR CREATELOGINPROFILE CREATEOPENIDCONNECTPROVIDER CREATEROLE CREATESAMLPROVIDER CREATEUSER DELETEBUCKETPOLICY GETFEDERATIONTOKEN IMPORTKEYPAIR UPDATEACCESSKEY UPDATELOGINPROFILE	ADDPERMISSION20150331V2 ADDROLETOINSTANCEPROFILE ADDUSERTOGROUP ASSUMEROLE ASSUMEROLEWITHSAML ATTACHGROUPPOLICY ATTACHROLEPOLICY ATTACHUSERPOLICY CREATEPOLICY GETSESSIONTOKEN PUTROLEPOLICY	CREATEFILTER CREATEIPSET DELETEACCESSKEY DELETEALARMS DELETECONFIGRULE DELETEDETECTOR DELETEFLOWLOGS DELETELOGGROUP DELETENETWORKACLENTRY DELETETRAIL ENABLEREGION PUTEVENTSELECTORS STOPLOGGING UPDATETRAIL	GETPARAMETERS GETPASSWORDDATA GETSECRETVALUE LISTSECRETS	DESCRIBE* GET* HEAD* LIST*	ATTACHVOLUME AUTHORIZEDBSECURITYGROUPINGRESS CREATEDBSECURITYGROUP CREATESNAPSHOT CREATEVOLUME ENABLESERIALCONSOLEACCESS RESUMESESSION SENDSERIALCONSOLESSHPUBLICKEY SENDSSHPUBLICKEY	AUTHORIZESECURITYGROUPEGRESS COPYOBJECT CREATEDBSNAPSHOT CREATEIMAGE GETOBJECT MODIFYDBSNAPSHOTATTRIBUTE MODIFYIMAGEATTRIBUTE SHAREDSNAPSHOTCOPYINITIATED	CREATECLUSTER CREATESERVICE DELETEBUCKET DELETEDBCLUSTER DELETEDBINSTANCE DELETEOBJECT DELETEOBJECTS DELETESNAPSHOT DELETEVOLUME PUTBUCKETLIFECYCLECONFIGURATION PUTBUCKETVERSIONING PUTOBJECT REQUESTSPOTFLEET RUNINSTANCE SENDEMAIL SENDRAWEMAIL STOPINSTANCES TERMINATEINSTANCES
	ENTRA ID AUDIT LOGS ENTRA ID SIGN-IN LOGS AZURE ACTIVITY LOGS AZURE KEY VAULT LOGS* AZURE STORAGE ACCOUNT LOGS*	CONSENT TO APPLICATION SIGN-IN ACTIVITY	MICROSOFT.AUTOMATION/AUTOMATIONACCOUNTS/RUNBOOKS/WRITE MICROSOFT.COMPUTE/VIRTUALMACHINES/RUNCOMMAND/ACTION MICROSOFT.COMPUTE/VIRTUALMACHINES/WRITE (CUSTOMSCRIPT) MICROSOFT.CONTAINERSERVICE/MANAGEDCLUSTERS/RUNCOMMAND/ACTION	ADD SERVICE PRINCIPAL ADD USER ADD VERIFIED DOMAIN MICROSOFT.AUTOMATION/AUTOMATIONACCOUNTS/JOBS/WRITE MICROSOFT.COMPUTE/SSHPUBLICKEYS/WRITE MICROSOFT.NETWORK/NETWORKSECURITYGROUPS/SECURITYRULES/WRITE	ADD APPLICATION ADD MEMBER TO ROLE ADD ROLE DEFINITION MICROSOFT.AUTHORIZATION/ROLEASSIGNMENTS/WRITE MICROSOFT.MANAGEDIDENTITY/USERASSIGNEDIDENTITIES/ASSIGN/ACTION UPDATE ROLE DEFINITION	MICROSOFT.INSIGHTS/DIAGNOSTICSETTINGS/DELETE MICROSOFT.INSIGHTS/DIAGNOSTICSETTINGS/WRITE MICROSOFT.INSIGHTS/METRICALERTS/DELETE MICROSOFT.NETWORK/NETWORKWATCHERS/FLOWLOGS/DELETE MICROSOFT.OPERATIONALINSIGHTS/WORKSPACES/DELETE	MICROSOFT.AUTOMATION/AUTOMATIONACCOUNTS/CREDENTIALS/READ MICROSOFT.KEYVAULT/VAULTS/KEYS/READ MICROSOFT.KEYVAULT/VAULTS/SECRETS/READ MICROSOFT.STORAGE/STORAGEACCOUNTS/LISTKEYS/ACTION VAULTPATCH	*GET* *LIST* *READ	MICROSOFT.COMPUTE/VIRTUALMACHINES/EXTENSIONS/WRITE MICROSOFT.SERIALCONSOLE/SERIALPORTS/CONNECT/ACTION	COPYBLOB GETBLOB MICROSOFT.COMPUTE/DISKS/BEGINGETACCESS/ACTION MICROSOFT.COMPUTE/SNAPSHOTS/BEGINGETACCESS/ACTION MICROSOFT.SQL/SERVERS/DATABASES/EXPORT/ACTION	MICROSOFT.COMPUTE/DISKS/DELETE MICROSOFT.COMPUTE/VIRTUALMACHINES/DELETE MICROSOFT.KEYVAULT/VAULTS/DELETE MICROSOFT.KEYVAULT/VAULTS/SECRETS/DELETE MICROSOFT.RECOVERYSERVICES/VAULTS/BACKUPPROTECTEDITEMS/DELETE MICROSOFT.STORAGE/STORAGEACCOUNTS/DELETE
	ADMIN AUDIT LOGS GOOGLE WORKSPACE AUDIT LOGS DATA ACCESS LOGS*	LOGIN_SUCCESS	CLOUDFUNCTIONS.FUNCTIONS.CALL CLOUDSCHEDULER.JOBS.RUN COMPUTE.INSTANCES.SETMETADATA COMPUTE.PROJECTS.SETCOMMONINSTANCEMETADATA	ADD-IAM-POLICY-BINDING COMPUTE.FIREWALLS.INSERT COMPUTE.FIREWALLS.PATCH CREATESECRET ENABLESERVICEACCOUNT GENERATEACCESSTOKEN GOOGLE.IAM.ADMIN.V1.CREATESERVICEACCOUNT GOOGLE.IAM.ADMIN.V1.CREATESERVICEACCOUNTKEY USERS.IMPORTSSHPUBLICKEY USERS.SSHPUBLICKEYS.PATCH	COMPUTE.DISKS.SETIAMPOLICY CREATEROLE GOOGLE.IAM.ADMIN.V1.SETIAMPOLICY IAM.SERVICEACCOUNTKEYS.CREATE IAM.SERVICEACCOUNTKEYS.IMPLICITDELEGATION SERVICEUSAGE.SERVICES.ENABLE	COMPUTE.FIREWALLS.DELETE LOGGING.PROJECTS.EXCLUSIONS.CREATE LOGGING.SINKS.DELETE LOGGING.SINKS.UPDATE SECURITYCENTER.SETTINGS.UPDATE SECURITYCENTER.SOURCES.DELETE STORAGE.SETIAMPERMISSIONS	SECRETMANAGERSERVICE.ACCESSSECRETVERSION SECRETMANAGERSERVICE.GETSECRET	*GET* *LIST*	GOOGLE.CLOUD.OSLOGIN.DATAPLANE.OSLOGINDATAPLANESERVICE.CHECKPOLICY GOOGLE.SSH-SERIALPORT.V1.CONNECT	BIGQUERY.JOBS.INSERT CLOUDSQL.INSTANCES.EXPORT PUBSUB.TOPICS.PUBLISH STORAGE.OBJECTS.COPY STORAGE.OBJECTS.GET	COMPUTE.INSTANCES.DELETE COMPUTE.INSTANCES.INSERT SECRETMANAGER.SECRETS.DELETE SECRETMANAGERSERVICE.DESTROYSECRETVERSION STORAGE.BUCKETS.DELETE

Managed k8s Control Plane Logs

Amazon EKS	Azure AKS	Google GKE
API SERVER AUDIT AUTHENTICATOR CONTROLLER MANAGER SCHEDULER	API SERVER AUDIT (OR AUDIT ADMIN) CLOUD CONTROLLER MANAGER CLUSTER AUTOSCALER CONTROLLER MANAGER GUARD SCHEDULER	API SERVER CONTROLLER MANAGER HPA DECISION LOGS SCHEDULER

Cloud Native Operating System Logs (Linux and Windows)

Amazon EC2	Azure VM	Google Compute Engine
/VAR/LOG/AMAZON/SSM/* /VAR/LOG/CLOUD-INIT-OUTPUT.LOG /VAR/LOG/CLOUD-INIT.LOG /VAR/LIB/AMAZON/SSM/* /OPT/AWS/AMAZON-CLOUDWATCH-AGENT/LOGS/* %PROGRAMDATA%\AMAZON\SSM\LOGS* %PROGRAMDATA%\AMAZON\AMAZONCLOUDWATCHAGENT\LOGS* %PROGRAMDATA%\AMAZON\EC2-WINDOWS\LAUNCH\LOG*	/VAR/LIB/WAAGENT/* /VAR/LOG/AZURE/* /VAR/LOG/WAAGENT.LOG /VAR/OPT/MICROSOFT/AZUREMONITORAGENT/LOG/ C:\WINDOWSAZURE\LOGS*	/VAR/LOG/GOOGLE-CLOUD-OPS-AGENT/* %PROGRAMDATA%\GOOGLE\CLOUD OPERATIONS\OPS AGENT\LOG*

*Log source is not enabled by default. Bolded events are part of the non-default log sources

WIZ