Alerts

name	status	severity	compromisedEntity	alertDisplayName	description
2517420867506866060_0d6abe87-9e4a-497b-8339-0bba07a71386	Active	High	Sample-App	[SAMPLE ALERT] Suspicious WordPress theme invocation detected	THIS IS A SAMPLE ALERT: The Azure App Service activity log indicates a possible code injection activity on your App Service resource.Đ The suspicious activity detected resembles that of a manipulation of WordPress theme to support server side execution of code, followed by a direct web request to invoke the manipulated theme file.Đ This type of activity was seen in the past as part of an attack campaign over WordPress.
2517420867526866060_6f6cd458-355b-4fdc-b30d-5d65acd961dc	Active	High	Sample-App	[SAMPLE ALERT] Phishing content hosted on Azure Webapps	THIS IS A SAMPLE ALERT: URL used for phishing attack found on the Azure AppServices website. This URL was part of a phishing attack sent to O365 customers. The content typically lure visitors into entering their corporate credentials or financial information into a legitimate looking website.
2517420867546709806_139c0ce3-e078-4a0f-aae2-1286f6d470b9	Active	Medium	Sample-KV	[SAMPLE ALERT] User accessed high volume of Key Vaults	THIS IS A SAMPLE ALERT: While may be benign it could also indicate that a larger volume of Key Vault operations has been performed compared to past historical data. Key Vaults typical exhibit the same behavior over time. This may be a legitimate change in activity but may also indicate that your Key Vault infrastructure has been compromised warranting further investigation.
2517420867566709806_087d4a68-7429-4f20-a6a2-6114e5fc0112	Active	Medium	Sample-KV	[SAMPLE ALERT] High volume of operations in a Key Vault	THIS IS A SAMPLE ALERT: While may be benign it could also indicate that the number of vaults that a user or application accesses has changed compared to past historical data. Key Vault activity typically exhibits the same behavior over time. This may be a legitimate change in activity but may also indicate that your Key Vault infrastructure has been compromised warranting further investigation.

name	status	severity	compromisedEntity	alertDisplayName	description
2517420867586709806_55b80856-ed6b-47ec-b8c3-09064d912512	Active	Medium	Sample-KV	[SAMPLE ALERT] Suspicious secret listing and query in a Key Vault	THIS IS A SAMPLE ALERT: While may be benign it could also indicate that a Secret List operation was followed by numerous Secret Get operations. In addition, this operation pattern is not normally performed by the user on this vault. This is likely indicative th at /someone /is /dumping /the This is sample alert: secrets stored in the Key Vault for potentially malicious purposes.
2517420867606709806_f4cb425c-c23d-4abe-ac2b-44ee7f629b4a	Active	Medium	Sample-KV	[SAMPLE ALERT] Suspicious policy change and secret query in a Key Vault	THIS IS A SAMPLE ALERT: While may be benign it could also indicate that a Key Vault policy change has been made and operations to list and/or get secrets occurred shortly thereafter. In addition, this operation pattern is not normally performed by the user on this vault. This is highly indicative that the Key Vault has been compromised and the secrets within have been /stolen /by a malicious actor.
2517420867626709806_bebe5278-9463-449a-afa4-eaea921b1083	Active	Medium	Sample-KV	[SAMPLE ALERT] Access from a TOR exit node to a Key Vault	THIS IS A SAMPLE ALERT: While may be benign it could also indicate that the Key Vault has been accessed by someone using the TOR IP anonymization system to hide their true source location. This is suspicious because malicious actors will often try to mask their source location when attempting to gain unauthorized access to internet-connected resources.
2517420867646553556_2bb7dfae-b4ff-4458-bb0c-8bafbce67c7c	Active	Medium	Sample-KubernetesService	[SAMPLE ALERT] Container with a sensitive volume mount detected	THIS IS A SAMPLE ALERT: Kubernetes audit log analysis detected a new container with a sensitive volume mount. The volume that was detected is a hostPath type which mounts a sensitive file or folder from the node to the container. If the container gets compromised, the attacker can use this mount for gaining access to the node.

name	status	severity	compromisedEntity	alertDisplayName	description
2517420867666553556_0c07464b-25f5-4d11-80fe-d729763b0138	Active	Medium	Sample-KubernetesService	[SAMPLE ALERT] Exposed Kubernetes service detected	THIS IS A SAMPLE ALERT: The Kubernetes audit log analysis detected exposure of a service by a load balancer. This service is related to a sensitive application that allows high impact operations in the cluster such as running processes on the node or creating new containers. In some cases, this service doesn't require authentication. If the service doesn't require authentication, exposing it to the internet poses a security risk.
2517420867706553556_decf709b-0a94-4ebc-8d76-39d068d53bfa	Active	High	Sample-SQL	[SAMPLE ALERT] Potential SQL Brute Force attempt	THIS IS A SAMPLE ALERT: Someone is attempting to brute force credentials to your SQL server 'Sample-SQL'.
2517420867726553556_c7f8472b-510f-4760-924c-15eb1a724343	Active	High	Sample-SQL	[SAMPLE ALERT] Attempted logon by a potentially harmful application	THIS IS A SAMPLE ALERT: A potentially harmful application attempted to access SQL server 'Sample-SQL'.
2517420867746553556_c8d04487-2653-45ed-9252-4a65854d0c43	Active	High	Sample-SQL	[SAMPLE ALERT] Potential SQL Injection	THIS IS A SAMPLE ALERT: Potential SQL Injection was detected on your database elitronix-com on server Sample-SQL
2517420867766553556_503ee315-5a55-41ae-ad80-0dedb7c5a54e	Active	Medium	Sample-SQL	[SAMPLE ALERT] Logon from an unusual location	THIS IS A SAMPLE ALERT: Someone logged on to your SQL server Sample-SQL from an unusual location.
2517420867786553556_f4449b87-74f1-48e1-a870-cce1b043145a	Active	High	Sample-SQL	[SAMPLE ALERT] Unusual export location	THIS IS A SAMPLE ALERT: Someone has extracted a massive amount of data from your SQL Server 'Sample-SQL' to an unusual location.
2517420867885615984_721501e0-48cc-4035-bdd7-bcee82b8b2e6	Active	Medium	Sample-VM	[SAMPLE ALERT] Executable found running from a suspicious location	THIS IS A SAMPLE ALERT: Analysis of host data detected an executable file on Sample-VM that is running from a location in common with known suspicious files. This executable could either be legitimate activity, or an indication of a compromised host.
2517420867905615984_f9df6bb5-c486-4e17-8065-60aa00ddfaf0	Active	High	Sample-VM	[SAMPLE ALERT] Digital currency mining related behavior detected	THIS IS A SAMPLE ALERT: Analysis of host data on Sample-VM detected the execution of a process or command normally associated with digital currency mining.

name	status	severity	compromisedEntity	alertDisplayName	description
2517420867925615984_3e345129-e16b-4d8d-957f-f43cbcc32590	Active	Medium	Sample-VM	[SAMPLE ALERT] Suspicious PHP execution detected	THIS IS A SAMPLE ALERT: Machine logs indicate a that a suspicious PHP process is running. The action included an attempt to run OS commands or PHP code from the command line using the PHP process.Ð While this behavior can be legitimate, in web applications this behavior is also observed in malicious activities such as attempts to infect websites with web shells.
2517420867945615984_44609b2f-324e-4428-8cdd-1df3b5634463	Active	High	Sample-VM	[SAMPLE ALERT] Detected suspicious file cleanup commands	THIS IS A SAMPLE ALERT: Analysis of host data on Sample-VM detected a combination of systeminfo commands that has previously been associated with one of activity group GOLD's methods of performing post-compromise self-cleanup activity. While 'systeminfo.exe' is a legitimate Windows tool, executing it twice in succession, followed by a delete command in the way that has occurred here is rare.
2517420867965615984_bb60ed6b-012d-471a-83d5-edba54257b3f	Active	High	Sample-VM	[SAMPLE ALERT] Detected Petya ransomware indicators	THIS IS A SAMPLE ALERT: Analysis of host data on OMS-AGENT-2 detected indicators associated with Petya ransomware. See https://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/ for more information. Review the command line associated in this alert and escalate this alert to your security team.
2517420868005147240_ede7fd70-8038-43a4-a9fb-6f362edbf9ac	Active	High	2f69bcc6-e7d1-4de5-9006-d8ede4c4c6d5	[SAMPLE ALERT] MicroBurst exploitation toolkit used to extract keys to your storage accounts (Preview)	THIS IS A SAMPLE ALERT: MicroBurst's exploitation toolkit was used to extract keys to your storage accounts. This was detected by analyzing Azure Activity logs and resource management operations in your subscription.

name	status	severity	compromisedEntity	alertDisplayName	description
2517420868025147240_34e9ec9b-f349-4832-8fa3-637456422386	Active	Medium	Sample-VM	[SAMPLE ALERT] Antimalware real-time protection was disabled in your virtual machine (Preview)	THIS IS A SAMPLE ALERT: Real-time protection disablement of the antimalware extension was detected in your virtual machine by analyzing the Azure Resource Manager operations in your subscription. Attackers might disable real-time protection from the antimalware scan on your virtual machine to avoid detection while running arbitrary code or infecting the machine with malware.
2517420868045147240_76d49958-d48f-4a19-9f7b-4c49c237add3	Active	Medium	Sample-VM	[SAMPLE ALERT] Custom script extension with suspicious command in your virtual machine (Preview)	THIS IS A SAMPLE ALERT: Custom script extension with suspicious command was detected in your virtual machine by analyzing the Azure Resource Manager operations in your subscription. Attackers may use custom script extension to execute a malicious code on your virtual machine via the Azure Resource Manager.
2517420868065303496_48eaf679-2fc5-4b32-9618-f095e7f21ef8	Active	Low	Sample-VM	[SAMPLE ALERT] Anonymity network activity (Preview)	THIS IS A SAMPLE ALERT: Analysis of DNS transactions detected anonymity network activity. Such activity, while possibly legitimate user behaviour, is frequently employed by attackers to evade tracking and fingerprinting of network communications. Typical related attacker activity is likely to include the download and execution of malicious software or remote administration tools.
2517420868085303496_b2335c09-c1f0-4c2d-9602-26db00891977	Active	Low	Sample-VM	[SAMPLE ALERT] Possible data exfiltration via DNS tunnel (Preview)	THIS IS A SAMPLE ALERT: Analysis of DNS transactions detected a possible DNS tunnel. Such activity, while possibly legitimate user behaviour, is frequently performed by attackers to evade network monitoring and filtering. Typical related attacker activity is likely to include the download and execution of malicious software or remote administration tools.

name	status	severity	compromisedEntity	alertDisplayName	description
2517420868105303496_89dd8bf9-89de-4fdd-90da-7b0a7b57d883	Active	Low	Sample-VM	[SAMPLE ALERT] Communication with possible phishing domain (Preview)	THIS IS A SAMPLE ALERT: Analysis of DNS transactions detected a request for a possible phishing domain. Such activity, while possibly benign, is frequently performed by attackers to harvest credentials to remote services. Typical related attacker activity is likely to include the exploitation of any credentials on the legitimate service.
2517420868125303496_079a4d70-5610-4ec1-8d87-1fd8d9823295	Active	Medium	Sample-VM	[SAMPLE ALERT] Attempted communication with suspicious sinkholed domain (Preview)	THIS IS A SAMPLE ALERT: Analysis of DNS transactions detected request for sinkholed domain. Such activity, while possibly legitimate user behaviour, is frequently an indication of the download or execution of malicious software. Typical related attacker activity is likely to include the download and execution of further malicious software or remote administration tools.
2517420868146866060_6cb85caa-5b80-4168-b7e1-72141e86d2ee	Active	Medium	Sample-VM	[SAMPLE ALERT] Attempt to run high privilege command detected	THIS IS A SAMPLE ALERT: Analysis of App Service processes detected an attempt to run a command that requires high privileges.
2517420868166866060_8bbd22e5-6188-4e51-9517-6511a3a76540	Active	High	Sample-App	[SAMPLE ALERT] Dangling DNS record for an App Service resource detected	THIS IS A SAMPLE ALERT: A DNS record that points to a recently deleted App Service resource (also known as "dangling DNS" entry) has been detected. This leaves you susceptible to a subdomain takeover. Subdomain takeovers enable malicious actors to redirect traffic intended for an organization’s domain to a site performing malicious activity.
2517420868186553556_fd3e887f-252f-4382-ab1e-ee9c5b22b3b1	Active	Low	Sample-ConnectedCluster	[SAMPLE ALERT] AKS API requests from proxy IP address detected (Preview)	THIS IS A SAMPLE ALERT: Kubernetes audit log analysis detected API requests to your cluster from an IP address that is associated with proxy services, such as TOR.Ð While this behavior can be legitimate, it's often seen in malicious activities, when attackers try to hide their source IP.

name	status	severity	compromisedEntity	alertDisplayName	description
2517420868206553556_67828b8e-f261-446e-8e4b-550b12318f17	Active	Medium	Sample-ConnectedCluster	[SAMPLE ALERT] Kubernetes events deleted (Preview)	THIS IS A SAMPLE ALERT: Security Center detected that some Kubernetes events have been deleted. Kubernetes events are objects in Kubernetes which contain information about changes in the cluster. Attackers might delete those events for hiding their operations in the cluster.
2517420868226553556_42b1585c-d333-489b-9ac0-48a6e0133432	Active	High	Sample-ConnectedCluster	[SAMPLE ALERT] Digital currency mining container detected (Preview)	THIS IS A SAMPLE ALERT: Kubernetes audit log analysis detected a container that has an image associated with a digital currency mining tool.
2517420868246553556_86c5f8f3-b750-4062-93e9-6b16297661bf	Active	Low	Sample-KubernetesService	[SAMPLE ALERT] CoreDNS modification in Kubernetes detected	THIS IS A SAMPLE ALERT: Kubernetes audit log analysis detected a modification of the CoreDNS configuration. The configuration of CoreDNS can be modified by overriding its configmap. While this activity can be legitimate, if attackers have permissions to modify the configmap, they can change the behavior of the clusterâ€™s DNS server and poison it.
2517420868265147240_1b008d4c-2dc3-44ff-82df-e2e8bf3faa44	Active	High	Sample-VM	[SAMPLE ALERT] Suspected successful brute force attack	THIS IS A SAMPLE ALERT: A successful login occurred after an apparent brute force attack on your resource
2517420868285147240_3e215b5d-2fa5-4d72-8f00-0b3a62ef800b	Active	High	Sample-VM	[SAMPLE ALERT] Potential SQL Injection	THIS IS A SAMPLE ALERT: Potential SQL Injection was detected on your database Sample-DB on server Sample-VM
2517420868305147240_2134e927-2c89-40b6-9089-5fd3c1c04b0b	Active	High	Sample-VM	[SAMPLE ALERT] Attempted logon by a potentially harmful application	THIS IS A SAMPLE ALERT: A potentially harmful application attempted to access your resource.
2517420868325147240_745da96c-0f0f-4d89-ae71-b8de0cac861a	Active	Medium	Sample-VM	[SAMPLE ALERT] Login from a suspicious IP	THIS IS A SAMPLE ALERT: Your resource has been accessed successfully from an IP address that Microsoft Threat Intelligence has associated with suspicious activity.

name	status	severity	compromisedEntity	alertDisplayName	description
2517420868345147240_10b9f6c1-e254-492b-ac2f-fc20e66f184f	Active	Medium	2f69bcc6-e7d1-4de5-9006-d8ede4c4c6d5	[SAMPLE ALERT] Permissions granted for an RBAC role in an unusual way for your Azure environment (Preview)	THIS IS A SAMPLE ALERT: Azure Defender for Resource Manager detected an RBAC role assignment that's unusual when compared with other assignments, performed by the same assigner. The following components were anomalous: -Assigner Authentication Method This operation might have been performed by a legitimate user in your organization. Alternatively, it might indicate that an account in your organization was breached, and that the threat actor is trying to grant permissions to an additional user account they own.
2517420868365147240_dc7d4dd7-4f08-4268-84fc-09b3bf4aab94	Active	Low	2f69bcc6-e7d1-4de5-9006-d8ede4c4c6d5	[SAMPLE ALERT] Privileged custom role created for your subscription in a suspicious way (Preview)	THIS IS A SAMPLE ALERT: Azure Defender for Resource Manager detected a suspicious creation of privileged custom role definition in your subscription. This operation might have been performed by a legitimate user in your organization. Alternatively, it might indicate that an account in your organization was breached, and that the threat actor is trying to create a privileged role to use in the future to evade detection.
2517420868425147240_283e11a2-3e79-4a48-b527-36232b5c71a0	Active	Medium	2f69bcc6-e7d1-4de5-9006-d8ede4c4c6d5	[SAMPLE ALERT] Permissions granted for a classic role in an unusual way for your Azure environment (Preview)	THIS IS A SAMPLE ALERT: Microsoft Defender for Resource Manager detected a role assignment that's unusual when compared with other assignments performed by the same assigner / performed for the same assignee / in the tenant due to the following anomalies: assignment time, assigner location, assigner, authentication method, assigned entities, client software used, assignment extent. This operation might have been performed by a legitimate user in your organization. Alternatively, it might indicate that an account in your organization was breached, and that the threat actor is trying to escalate privileges to a different user account.

name	status	severity	compromisedEntity	alertDisplayName	description
2517420868466396780_dbdc9d34-d75d-40d2-9327-1e4464db8c32	Active	High	Sample-Storage	[SAMPLE ALERT] Access from a Tor exit node to a storage file share	THIS IS A SAMPLE ALERT: An IP that is a known Tor exit node accessed Storage file share 'Sample-fileShare' in storage account 'Sample-Storage'.
2517420868486396780_7a348ef8-8cb7-4b79-9a03-60996e354310	Active	High	Sample-Storage	[SAMPLE ALERT] Access from a suspicious IP to a storage file share	THIS IS A SAMPLE ALERT: Someone has accessed your Azure storage account 'Sample-Storage' from a suspicious IP address.
2517420868506396780_31465ab6-279c-454a-8af1-1a68f06bab5d	Active	Medium	Sample-Storage	[SAMPLE ALERT] Unusual overwrite of .exe in a storage file share	THIS IS A SAMPLE ALERT: Someone has performed an unusual overwrite of an executable file in your Azure storage account 'Sample-Storage'.
2517420868526396780_0590bd2b-447b-49ab-a0b9-d1d708c490dc	Active	Medium	Sample-Storage	[SAMPLE ALERT] Unusual change of access permissions in a storage file share	THIS IS A SAMPLE ALERT: Someone has performed an unusual change of access permissions of a directory or a file in your Azure storage account 'Sample-Storage'.
2517420868546396780_655b1a3a-6cab-4fac-9489-a524a1f63c38	Active	High	Sample-Storage	[SAMPLE ALERT] Potential malware uploaded to a storage file share	THIS IS A SAMPLE ALERT: Someone has uploaded potential malware to your Azure storage account 'Sample-Storage'.
2517420868566396780_6101f5c8-887b-45be-bfc6-7564991560fb	Active	Medium	Sample-Storage	[SAMPLE ALERT] Access from an unusual location to a storage file share	THIS IS A SAMPLE ALERT: Someone has accessed your Azure storage account 'Sample-Storage' from an unusual location.
2517420868586396780_b18ce191-f7b9-4743-b2d0-b8e025c9e76f	Active	Medium	Sample-Storage	[SAMPLE ALERT] Unusual upload of .exe to a storage file share	THIS IS A SAMPLE ALERT: Someone has performed an unusual upload of an executable file to your Azure storage account 'Sample-Storage'.
2517420868606396780_70da6f07-0415-4aea-af58-8508625a20e5	Active	Medium	Sample-Storage	[SAMPLE ALERT] Unusual deletion in a storage file share	THIS IS A SAMPLE ALERT: Someone has performed an unusual deletion in your Azure storage account 'Sample-Storage'.
2517420868626396780_ce75798d-98f2-45fd-91c7-0fda5e41030b	Active	Medium	Sample-Storage	[SAMPLE ALERT] Unusual data exploration in a storage file share	THIS IS A SAMPLE ALERT: Someone has performed an unusual data exploration operation in your Azure storage account 'Sample-Storage'.
2517420868646396780_e4cf001c-d232-4b45-b235-ce3c173ce09c	Active	High	Sample-Storage	[SAMPLE ALERT] Unusual number of files extracted from a storage file share	THIS IS A SAMPLE ALERT: Someone has extracted an unusual number of files from your Azure storage account 'Sample-Storage'.
2517420868666396780_28bea8f6-8573-48aa-bcfc-048305df4c77	Active	High	Sample-Storage	[SAMPLE ALERT] Unusual amount of data extracted from a storage file share	THIS IS A SAMPLE ALERT: Someone has extracted an unusual amount of data from your Azure storage account 'Sample-Storage'.

name	status	severity	compromisedEntity	alertDisplayName	description
2517420868686396780_7504b6fc-7d91-4af2-a801-396ada73da80	Active	Medium	Sample-Storage	[SAMPLE ALERT] Unusual application accessed a storage file share	THIS IS A SAMPLE ALERT: Someone has accessed your Azure storage account 'Sample-Storage' using an unexpected application.
2517420868706396780_1c244f81-d1df-425b-86da-d0f3ab81a220	Active	Medium	Sample-Storage	[SAMPLE ALERT] Unusual access inspection in a storage file share	THIS IS A SAMPLE ALERT: Someone has performed an unusual access inspection in your Azure storage account 'Sample-Storage'.
2517420868726396780_596e34f7-7e39-4134-a40e-a0d38e968a1d	Active	Medium	Sample-Storage	[SAMPLE ALERT] Access from a Tor exit node to a storage blob container	THIS IS A SAMPLE ALERT: An IP that is a known Tor exit node accessed Storage container 'Sample-Container' in storage account 'Sample-Storage'. This alert was triggered by an ADLS Gen2 transaction.
2517420868746396780_b43743a6-0c24-4ea1-aff3-06ce7888e9f5	Active	Low	Sample-Storage	[SAMPLE ALERT] Access from a suspicious IP to a storage blob container	THIS IS A SAMPLE ALERT: Someone has accessed your Azure storage account 'Sample-Storage' from a suspicious IP address.
2517420868766396780_ed5a83fb-2c45-49bd-820f-ee7af2ead22f	Active	High	Sample-Storage	[SAMPLE ALERT] PREVIEW - Access from a suspicious application	THIS IS A SAMPLE ALERT: There was a failed attempt to anonymously access the blob container `Sample-Container` in your storage account `Sample-Storage`. This might indicate that an attacker is trying to exploit a vulnerability or access data in your storage account, or it could be the result of a penetration test carried out in your organization. The suspicious application detected was `eicarDummyApp`. For more details, please see the user-agent string in the alert fields. In many cases, attackers might successfully access data after a series of failed attempts. It’s therefore important to act on this alert.
2517420868786396780_ee3f9dd9-0410-4546-b255-f51992e8de5f	Active	High	Sample-Storage	[SAMPLE ALERT] PREVIEW - Phishing content hosted on a storage account	THIS IS A SAMPLE ALERT: A URL used in a phishing attack points to your Azure Storage account. This URL was part of a phishing attack affecting users of Microsoft 365. Typically, content hosted on such pages is designed to trick visitors into entering their corporate credentials or financial information into a web form that looks legitimate.

name	status	severity	compromisedEntity	alertDisplayName	description
2517420868806396780_2d882170-6296-4f40-8518-086a981c4ca1	Active	Medium	Sample-Storage	[SAMPLE ALERT] Unusual change of access permissions in a storage blob container	THIS IS A SAMPLE ALERT: Someone has performed an unusual change of access permissions of a directory or a file in your Azure storage account 'Sample-Storage'. This alert was triggered by an ADLS Gen2 transaction.
2517420868826396780_d7e12db6-753a-4f4b-ab35-99dbd01cc8f8	Active	High	Sample-Storage	[SAMPLE ALERT] Publicly accessible storage containers successfully discovered	THIS IS A SAMPLE ALERT: A successful discovery of 3 publicly open storage containers in storage account 'Sample-Storage' was performed in the last hour by a scanning script or tool.Ð Ð Scanned containers include: static, images, backups.Ð Ð This usually indicates a reconnaissance attack, where the threat actor tries to list blobs by guessing container names, in the hope of finding misconfigured open storagecontainers with sensitive data in them.Ð The threat actor may use their own script or use known scanning tools like Microburst to scan for publicly open containers.Ð Ð After a threat actor successfully discovers a container, they usually continue by reading and exfiltrating the data.
2517420868846396780_2e7ebc97-1709-41ab-8a14-1e09655f8a53	Active	High	Sample-Storage	[SAMPLE ALERT] Publicly accessible storage containers unsuccessfully scanned	THIS IS A SAMPLE ALERT: 1232 failed attempts to scan for publicly open storage containers in storage account 'Sample-Storage' were performed in the last hour.Ð Ð Scanned containers include: erp, exe, export, exports, file.Ð Ð This usually indicates a reconnaissance attack, where the threat actor tries to list blobs by guessing container names, in the hope of finding misconfigured open storage containers with sensitive data in them.Ð The threat actor may use their own script or use known scanning tools like Microburst to scan for publicly open containers.

name	status	severity	compromisedEntity	alertDisplayName	description
2517420868866396780_0bd73f5d-8bc5-480b-9dae-56c9ac1f6c2c	Active	Medium	Sample-Storage	[SAMPLE ALERT] Storage account with potentially sensitive data has been detected with a publicly exposed container	THIS IS A SAMPLE ALERT: The access policy of a container in your storage account was modified to allow anonymous access. This might lead to a data breach if the container holds any sensitive data. This alert is based on analysis of Azure activity log.
2517420868886396780_8bdfa611-a272-48b1-adf9-5969e340ddaa	Active	High	Sample-Storage	[SAMPLE ALERT] Potential malware uploaded to a storage blob container	THIS IS A SAMPLE ALERT: Someone has uploaded potential malware to your Azure storage account 'Sample-Storage'.
2517420868906396780_149c12ed-f8b2-437b-badf-aee5add8372b	Active	Medium	Sample-Storage	[SAMPLE ALERT] Access from an unusual location to a storage blob container	THIS IS A SAMPLE ALERT: Someone has accessed your Azure storage account 'Sample-Storage' from an unusual location.
2517420868926396780_fee157d3-cac8-4744-bbcd-869e5b0788b5	Active	Medium	Sample-Storage	[SAMPLE ALERT] Unusual upload of .exe to a storage blob container	THIS IS A SAMPLE ALERT: Someone has performed an unusual upload of an executable file to your Azure storage account 'Sample-Storage'. This alert was triggered by an ADLS Gen2 transaction.
2517420868946396780_cfefbedb-57e8-4b45-8dcb-66c25fc5cda3	Active	Medium	Sample-Storage	[SAMPLE ALERT] Unusual deletion in a storage blob container	THIS IS A SAMPLE ALERT: Someone has performed an unusual deletion in your Azure storage account 'Sample-Storage'. This alert was triggered by an ADLS Gen2 transaction.
2517420868966396780_9a417e69-7c66-4d7f-9dd0-665969b18ac1	Active	Medium	Sample-Storage	[SAMPLE ALERT] Unusual data exploration in a storage blob container	THIS IS A SAMPLE ALERT: Someone has performed an unusual data exploration operation in your Azure storage account 'Sample-Storage'.
2517420868986396780_aaeba517-411a-4d69-b61f-f46730f5ec2b	Active	Low	Sample-Storage	[SAMPLE ALERT] Unusual number of blobs extracted from a storage blob container	THIS IS A SAMPLE ALERT: Someone has extracted an unusual number of blobs from your Azure storage account 'Sample-Storage'.
2517420869006396780_d5d3b844-e875-45fc-a695-6e1b6e796c42	Active	Low	Sample-Storage	[SAMPLE ALERT] Unusual amount of data extracted from a storage blob container	THIS IS A SAMPLE ALERT: Someone has extracted an unusual amount of data from your Azure storage account 'Sample-Storage'.
2517420869026396780_29d0f0e3-0563-4d93-9c71-fdc62ae8e2b0	Active	Medium	Sample-Storage	[SAMPLE ALERT] Unusual upload of .cspkg to a storage blob container	THIS IS A SAMPLE ALERT: Someone has performed an unusual upload of a Cloud Service deployment package to your Azure storage account 'Sample-Storage'.

name	status	severity	compromisedEntity	alertDisplayName	description
2517420869046396780_9c6b8664-a553-41e7-bc90-7c406e296653	Active	Medium	Sample-Storage	[SAMPLE ALERT] Unusual application accessed a storage blob container	THIS IS A SAMPLE ALERT: Someone has accessed your Azure storage account 'Sample-Storage' using an unexpected application.
2517420869066396780_fd2dc4c7-d8f0-4232-a62a-f44f550b4a71	Active	Medium	Sample-Storage	[SAMPLE ALERT] Unauthenticated access to a storage blob container	THIS IS A SAMPLE ALERT: Container 'Sample-Container' in storage account 'Sample-Storage' from an IP address located in Azure Data Center: Central Us.Đ Đ There may have been additional unauthenticated access to this storage account.
2517420869086396780_6a223ba4-2709-40f9-96ab-ad4cf3d6423a	Active	Medium	Sample-Storage	[SAMPLE ALERT] Unusual access inspection in a storage blob container	THIS IS A SAMPLE ALERT: Someone has performed an unusual access inspection in your Azure storage account 'Sample-Storage'.
2517420869106396780_02e415d3-f639-4f73-9983-523dae479a8f	Active	High	Sample-Storage	[SAMPLE ALERT] Malicious file uploaded to storage account	THIS IS A SAMPLE ALERT: A malicious file was uploaded to your storage account 'Sample-Storage'.Đ The malware detection is based on Microsoft antimalware scanning.Đ Potential causes may include an intentional upload of malware by a threat actor, or an unintentional upload of a malicious file by a legitimate user.
2517420869144990988_a8e6594f-0905-4efb-9746-519b094815fa	Active	High	Sample-AzureCosmosDb	[SAMPLE ALERT] Access from a Tor exit node	THIS IS A SAMPLE ALERT: Azure Cosmos DB account 'Sample-AzureCosmosDBAccount' was successfully accessed from an IP address known to be an active exit node of Tor, an anonymizing proxy.Đ The threat actor's access was authenticated using Aad.Đ Authenticated access from a Tor exit node is a likely indication that a threat actor is trying to hide their identity.
2517420869164990988_bc3717f2-66f6-46d6-9a3c-e540ea803b9d	Active	High	Sample-AzureCosmosDb	[SAMPLE ALERT] Access from a suspicious IP	THIS IS A SAMPLE ALERT: Azure Cosmos DB account 'Sample-AzureCosmosDBAccount' was successfully accessed from an IP address that was identified as a threat by Microsoft Threat Intelligence.Đ The threat actor's access was authenticated using Aad.

name	status	severity	compromisedEntity	alertDisplayName	description
2517420869184990988_7ae142fb-78ab-40a8-8788-39bb02602196	Active	Medium	Sample-AzureCosmosDb	[SAMPLE ALERT] SQL injection: failed fuzzing attempt	THIS IS A SAMPLE ALERT: A suspicious SQL statement was used to query container 'Sample-Container' in Azure Cosmos DB account 'Sample-AzureCosmosDBAccount'.Ð Like other well-known SQL injection attacks, this statement won’t succeed in Azure Cosmos DB. Nevertheless, it’s an indication that a threat actor is trying to attack the resources in this account.Ð Some SQL injection attacks can succeed and be used to exfiltrate data. This means that if the attacker continues performing SQL injection attempts, they may be able to compromise your Azure Cosmos DB account and exfiltrate data.Ð You can prevent this threat by using parameterized queries (for more information, see the remediation steps).
2517420869204990988_527a7505-aa60-492e-bc0f-66860a57c426	Active	Medium	Sample-AzureCosmosDb	[SAMPLE ALERT] SQL injection: potential data exfiltration	THIS IS A SAMPLE ALERT: A suspicious SQL statement was used to query container 'Sample-Container' in Azure Cosmos DB account 'Sample-AzureCosmosDBAccount'.Ð The injected statement might have succeeded in exfiltrating data the user wasn’t authorized to access.Ð Due to the structure and capabilities of Azure Cosmos DB queries, many known SQL injection attacks on Azure Cosmos DB accounts cannot work. However, the variation used in this attack may work and threat actors can exfiltrate data.
2517420869224990988_efeb98cc-aa7a-4d5f-bc98-97bb76444f42	Active	Medium	Sample-AzureCosmosDb	[SAMPLE ALERT] Access from an unusual location	THIS IS A SAMPLE ALERT: One or more containers in Azure Cosmos DB account 'Sample-AzureCosmosDBAccount' were accessed from a location considered unfamiliar, based on the usual access pattern.Ð Either a threat actor has gained access to the account, or a legitimate user has connected from a new or unusual geographic location.

name	status	severity	compromisedEntity	alertDisplayName	description
2517420869244990988_98697588-3578-4a74-9161-b29e3bd99074	Active	High	Sample-AzureCosmosDb	[SAMPLE ALERT] Unusual volume of data extracted	THIS IS A SAMPLE ALERT: An unusually large amount of data has been extracted from container 'Sample-Container' in Azure Cosmos DB account 'Sample-AzureCosmosDBAccount'. This might indicate that a threat actor exfiltrated data.
2517420869264990988_b4724463-4455-46ad-a23a-88338e6bd465	Active	Medium	Sample-AzureCosmosDb	[SAMPLE ALERT] Preview - Suspicious extraction of Azure Cosmos DB account keys was detected	THIS IS A SAMPLE ALERT: A suspicious source extracted Azure Cosmos DB account access keys from your subscription. If this source is not a legitimate source, this may be a high impact issue. The access key that was extracted provides full control over the associated databases and the data stored within.Ð The key extraction is suspicious for the following reasons:Ð - Key listing operations are rarely invoked by this principal on Azure Cosmos DB accounts in this subscription.Ð Ð This can indicate that the identity performed this operation is compromised and is being used with malicious intent.
2517420869284990988_9f57bb43-7d6f-4ab4-a0ec-c930cea22cad	Active	High	Sample-AzureCosmosDb	[SAMPLE ALERT] Extraction of Azure Cosmos DB accounts keys via a potentially malicious script	THIS IS A SAMPLE ALERT: A Powershell script was run in your subscription and performed a suspicious pattern of key-listing operations to get the keys of Azure Cosmos DB accounts in your subscription.Ð Threat actors use automated scripts, like Microburst, to list keys and find Azure Cosmos DB accounts they can access.Ð Ð This operation might indicate that an identity in your organization was breached, and that the threat actor is trying to compromise Azure Cosmos DB accounts in your environment for malicious intentions.Ð Alternatively, a malicious insider could be trying to access sensitive data and perform lateral movement.