Enhanced Cyber Resilience Solution by Threat Detection using IBM Cloud Object Storage System and IBM QRadar
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive summary</td>
<td>1</td>
</tr>
<tr>
<td>Target audience</td>
<td>1</td>
</tr>
<tr>
<td>Scope</td>
<td>1</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>2</td>
</tr>
<tr>
<td>IBM Cloud Object Storage System introduction</td>
<td>2</td>
</tr>
<tr>
<td>IBM QRadar SIEM introduction</td>
<td>3</td>
</tr>
<tr>
<td>IBM QRadar on Cloud</td>
<td>5</td>
</tr>
<tr>
<td>Identifying threats to data and taking action on potential incidents</td>
<td>6</td>
</tr>
<tr>
<td>Solution overview</td>
<td>7</td>
</tr>
<tr>
<td>Configuring IBM Cloud Object Storage System</td>
<td>9</td>
</tr>
<tr>
<td>Environment setup</td>
<td>9</td>
</tr>
<tr>
<td>Understanding access logs in IBM Cloud Object Storage System</td>
<td>10</td>
</tr>
<tr>
<td>Sending IBM Cloud Object Storage System accessor logs to IBM QRadar SIEM</td>
<td>13</td>
</tr>
<tr>
<td>IBM QRadar SIEM configuration</td>
<td>14</td>
</tr>
<tr>
<td>Configuring IBM QRadar SIEM to process IBM Cloud Object Storage accessor logs</td>
<td>14</td>
</tr>
<tr>
<td>Configuring Custom Extract Properties in IBM QRadar SIEM</td>
<td>18</td>
</tr>
<tr>
<td>Configuring QRadar Identifiers in IBM QRadar SIEM</td>
<td>22</td>
</tr>
<tr>
<td>Configuring log source in IBM QRadar SIEM</td>
<td>24</td>
</tr>
<tr>
<td>Mapping IBM Cloud Object Storage events to QRadar Identifiers</td>
<td>26</td>
</tr>
<tr>
<td>IBM QRadar SIEM custom script</td>
<td>28</td>
</tr>
<tr>
<td>Testing custom action scripts</td>
<td>31</td>
</tr>
<tr>
<td>Creating rules in IBM QRadar SIEM</td>
<td>32</td>
</tr>
<tr>
<td>Sample Rule 1</td>
<td>32</td>
</tr>
<tr>
<td>Sample Rule 2</td>
<td>35</td>
</tr>
<tr>
<td>Sample Rule 3</td>
<td>38</td>
</tr>
<tr>
<td>Conclusion</td>
<td>42</td>
</tr>
<tr>
<td>Notice</td>
<td>42</td>
</tr>
<tr>
<td>Appendix</td>
<td>43</td>
</tr>
<tr>
<td>Related resources</td>
<td>44</td>
</tr>
<tr>
<td>Acknowledgments</td>
<td>45</td>
</tr>
</tbody>
</table>

**Notices**

- Trademarks                                                              | 48   |
- Terms and conditions for product documentation                          | 49   |
  - Applicability                                                          | 49   |
  - Commercial use                                                         | 49   |
  - Rights                                                                 | 49   |
  - Privacy policy considerations                                          | 49   |
Executive summary

Having suitable storage for hosting business-critical data and advance security Information and event management software for deep inspection, detection, and prioritization of threats is a necessity of any business.

This IBM® Redpaper™ publication explains how the storage features of IBM Cloud® Object Storage System reduces the effect of incidents on the business data when combined with the log analysis, deep inspection, and detection of threats that is provided by IBM QRadar SIEM. Such integration provides an excellent platform for hosting unstructured business data that are subject to regulatory compliances.

In this paper, we also demonstrate how IBM Cloud Object Storage’s access logs can be integrated with IBM QRadar SIEM where an administrator can monitor, inspect, detect, and derive insights for identifying potential threats to the data that is stored on IBM Cloud Object Storage. An administrator also can take action on these threats quickly to mitigate or reduce the effect of such incidents. We also demonstrate how the threat detection by IBM QRadar SIEM can proactively trigger cyber resiliency workflow in IBM Cloud Object Storage remotely to protect the data during threat.

Target audience

This publication is intended for chief technology officers, solution and security architects, and systems administrators.

Scope

This publication provides a solutions architecture and related solution configuration workflows, with the following essential software components:

- IBM Cloud Object Storage System or IBM ICOS
- IBM QRadar SIEM
- Detailed technical configuration steps for building an end-to-end solution

This paper does not:

- Provide scalability and performance analysis from a user perspective
- Replace any official manuals and documents that were issued by IBM
Prerequisites

This technical paper assumes basic knowledge of the following prerequisites:

• IBM Cloud Object Storage System
• IBM Cloud Object Storage System installation and configuration
• IBM QRadar SIEM installation and configuration

IBM Cloud Object Storage System introduction

IBM Cloud Object Storage System is the primary storage solution that is used in the cloud and on-premises solutions as a central storage platform for unstructured data. IBM Cloud Object Storage System is growing more popular for the following reasons:

• It is designed for exabyte scale.
• It is easy to manage and yet meets the growing demands of enterprises for a broad set of applications and workloads.
• It allows users to balance storage cost, location, and compliance control requirements across data sets and essential applications.

IBM Cloud Object Storage System (see Figure 1) provides industry-leading flexibility that enables your organization to handle unpredictable but always changing needs of business and evolving workloads. IBM Cloud Object Storage System is a software-defined storage solution that is hardware aware. This awareness allows IBM Cloud Object Storage System to be an enterprise-grade storage solution that is highly available and reliable and uses commodity x86 servers. IBM Cloud Object Storage System takes full advantage of this hardware awareness by ensuring that the server performs optimally from a monitoring, management, and performance perspective.

Figure 1  IBM Cloud Object Storage System overview
Typical application use cases for IBM Cloud Object Storage System across industries include the following examples:

- Analytics, artificial intelligence, and machine learning data repository; for example, sensor data collection for autonomous driving.
- Storage for cloud native applications.
- Secondary storage for Active Archive or storage for backup data. It is often used in the health care industry for use cases around medical imaging and genomic research. In the finance industry, it used for hosting regulated, long-term compliance data.

IBM Cloud Object Storage System is a preferred Object Storage choice for hosting critical data assets for organizations across industries. It is vital to ensure that data that is on IBM Cloud Object Storage System is safeguarded from threats.

IBM Cloud Object Storage System is available in the following modes:
- Mode 1: On-premises Object Storage called IBM Cloud Object Storage System:
  - IBM hardware appliances with IBM Cloud Object Storage System software
  - IBM certified third-party x86 servers with IBM Cloud Object Storage System software
- Mode 2: Public Cloud Object Storage (multi-tenant)

In this paper, we refer to the solution that is applicable for Mode 1.

For more information about IBM Cloud Object Storage System, see the following publications:
- *IBM Cloud Object Storage System Product Guide, SG24-8439*

**IBM QRadar SIEM introduction**

In cybersecurity, Security Information and Event Management (SIEM) is considered a series of technologies that provides analysis, threat mitigation, and logging of security events across a determined network. SIEM provides a general view of all technical infrastructure, with specific data of security events, and the mitigation of any security threat vectors that are found in the environment.

To better understand SIEM, think of a solution that gathers data from security sources for analysis correlation and action upon possible threats. SIEM management offers various functions in the following areas:

- Event and log collection
- Rule correlation
- Log source management
- Adaptability
- Data normalization and registry
- Reports and Compliance

This solution solves scenarios in advanced threats that cannot be analyzed with normal monitoring tools on a general level, by using a business technical infrastructure, and by unifying all the elements (which are typically agents in a hierarchical model) to gather events from endpoints, servers, and network equipment. It also provides third-party interoperability so that many solutions can be integrated, which makes this product scalable and more robust.
IBM QRadar SIEM is one of the most popular SIEM solutions in the market today that helps you to quickly uncover existing and potential threats by using its advanced analytics capabilities. It also provides many useful features, such as centralized visibility, flexible deployment, automated intelligence, machine learning, and pro-active threat hunting.

Figure 2 provides a high-level overview of IBM QRadar SIEM Security Intelligence Platform coverage.

This solution collects events from different assets that are in the environment, picks up raw packets of data from the network for correlation, and provides session rebuilding capabilities for forensic analysis. IBM Watson® for Security is also integrated to IBM QRadar® SIEM with multiple other third-party security feeds that helps orchestrate responses to unknown threat vectors. Figure 3 shows how IBM QRadar SIEM collects data from extensive data sources and applies correlation and deep inspection to derive an exception and accurate actionable insight.
IBM QRadar on Cloud

IBM QRadar on Cloud is a highly scalable SIEM solution that consolidates log, event, and flow data from thousands of devices that are distributed across on-premises and cloud-based networks. It performs immediate correlation and analysis to distinguish real threats from false positives.

IBM QRadar on Cloud offers integrated capabilities for log management, SIEM, risk and vulnerability management, user behavior analytics, and network packet inspection. Security teams can access IBM QRadar SIEM capabilities from a web browser, just as they do if the infrastructure were deployed on-premises. However, IBM experts manage the infrastructure, on-going maintenance, Disaster Recovery, and technical support.

IBM QRadar on Cloud helps security teams accurately detect and prioritize threats. It also provides intelligent insights that enable teams to respond quickly to reduce the effect of incidents.

In an environment where security requirements are dynamic, IBM QRadar on Cloud provides the security monitoring that you need, and the flexibility to modify your monitoring activities as your requirements change.

With QRadar on Cloud, you can protect your network and meet compliance monitoring and reporting requirements with reduced total cost of ownership. Other than a data gateway appliance, which is used to connect to QRadar, you do not need to install any extra hardware on your premises.

IBM QRadar on Cloud (see Figure 4 on page 6) offers the following key capabilities:

• IBM QRadar SIEM that is configured to customer specifications and deployed within a dedicated private cloud environment. The solution is hosted by IBM within secure IBM Cloud data centers with built-in resiliency and failover-supporting infrastructure.

• A fast, easy, cost-effective way to meet changing needs for security intelligence and analytics. The solution delivers market ready SIEM capabilities as a SaaS solution, which eliminates the need for infrastructure management.
Identifying threats to data and taking action on potential incidents

Data is the new oil for the organizations in this digital world. Protecting data against cyberthreats is one of the key challenges that many organizations are facing.

In a data-centric security paradigm, protecting data is of paramount importance. This necessity leads to having security capabilities of underlying storage systems, such as secure data at rest, secure data in motion, role-based access control for administration, ACL, and anti-virus support, to ensure that the data is constantly secured and protected against malicious use.

IBM Cloud Object Storage System provides industry-leading flexibility that enables your organization to handle unpredictable but always changing needs of business and evolving workloads. IBM Cloud Object Storage System can log all object activity in the access logs on its Accessor nodes, which features all of the object access information.
To identify and detect potential malicious object access and for compliance auditing purposes, such access logs must be integrated with the SIEM solution. This capability is provided by IBM QRadar SIEM to which the IBM Cloud Object Storage access logs from Accessor nodes can be securely directed. IBM QRadar SIEM can detect malicious patterns that are based on the access logs, heuristics, and correlation with logs from other systems (such as network logs or server logs), flow, and packet data. It also can discover unknown threat vectors by using IBM Watson.

Next, we demonstrate the integration of IBM QRadar SIEM and IBM Cloud Object Storage System whereby:

- Unstructured object data is in an IBM Cloud Object Storage System vault.
- IBM Cloud Object Storage System access logs are configured on the Accessor nodes to relay the access logs to IBM QRadar SIEM.
- IBM QRadar SIEM is configured in the same network to receive logs on rsyslog port.
- IBM QRadar SIEM is configured with the required file parsing rules to understand the semantics of IBM Cloud Object Storage access logs.
- IBM QRadar SIEM is configured with sample rules (as manifestation) to identify potential threats based on analyzing IBM Cloud Object Storage access logs and generating insights and alerts an which administrators can act.
- IBM QRadar SIEM is also uploaded with custom scripts to take preventive action on IBM Cloud Object Storage remotely after the threat is detected by IBM QRadar SIEM.

**Note:** The purpose of this demonstration is to show IBM QRadar SIEM integration and the value it can derive to secure the data that is hosted on IBM Cloud Object Storage by using the IBM Cloud Object Storage accessor logs. Deployments can use this demonstration as a sample illustration to configure a solution for cybersecurity of their data that is stored on IBM Cloud Object Storage according to their business needs. Also, the solution can be extended to include IBM Cloud Object Storage administration command logging, which needs extra customization that is not covered in this paper.

**Solution overview**

As shown in Figure 5 on page 8, an IBM Cloud Object Storage System is configured with a management node, Accessor nodes, and IBM Slicestor® nodes. IBM Cloud Object Storage is commonly used to store petabyte and beyond storage data for enterprises worldwide. It uses an innovative and cost-effective approach for storing large volumes of unstructured data while still ensuring scalability, security, availability, reliability, manageability, and flexibility.

Typically, it is used to store and access data by using an object-based access method. It provides S3-compatible interface and is accessed by HTTPS/REST API. Simple **PUT**, **GET**, **DELETE**, and **LIST** commands enable applications to access the data.

REST API access to storage offers the following advantages:

- Tolerates internet latency
- Provides for programmable storage
- Provides efficient global access to large amounts of data
IBM QRadar SIEM is installed on a separate dedicated system that is configured to accept log messages by using \texttt{rsyslog} protocol. IBM Cloud Object Storage System is configured to forward access logs from the Accessor node to IBM QRadar SIEM. This feature enables forwarding HTTP access logs to IBM QRadar SIEM for any object activity on IBM Cloud Object Storage.

IBM QRadar SIEM is configured with parsing logic to understand the log format, parse the logs, and persistently store the logs. After the logs are in IBM QRadar SIEM, the security officer or administrator can set various rules, map log relationships, and so on, to detect a potential malicious access of data.

For our example, we set IBM QRadar SIEM rules on a specific user object access pattern and generate incidents if the file access pattern violates the business policies. On detection of a threat by IBM QRadar SIEM, an alert is raised and it communicates with IBM Cloud Object Storage to protect the data that is threatened.

Various methods can be used to protect the data that is threatened by analyzing the threat and taking preventive action. IBM QRadar SIEM is also uploaded with a custom script that remotely runs to take preventive action based on the threat that is detected.

Various use cases exist in which this solution can be useful, including the following examples:

- Cyber Resiliency
  The solution integration helps to bridge the Detect phase of National Institution of Standards and Technology (NIST) security framework.

- Business Policy on Data access by employees or applications
  The solution detects violation of business policies around data access and proactively protects data by using custom actions.

The IBM Cloud Object Storage with IBM QRadar SIEM solution workflow is shown in Figure 5.

![Figure 5 IBM Cloud Object Storage with IBM QRadar SIEM - Solution Overview](image-url)
Configuring IBM Cloud Object Storage System

IBM Cloud Object Storage System is configured for this solution by using one management node, one Accessor node, and three Slicestor nodes. For more information about the installation and initial configuration of IBM Cloud Object Storage System appliance, see the following resources:

- *IBM Cloud Object Storage System Product Guide, SG24-8439*
- IBM Cloud Object Storage System documentation at IBM Knowledge Center

Environment setup

IBM Cloud Object Storage System version 3.14.0.23 was set up for this demonstration and configured on three slicestor nodes, one Accessor node, and one manager node.

IBM QRadar SIEM Version 7.3.3 appliance is installed in the same network. VM3 node is configured with *rsyslog* to forward the logs to IBM QRadar SIEM. The setup that was used for the demonstration is shown in Figure 6.

![Device Summary](image)

*Figure 6  IBM Cloud Object Storage system: Demonstration configuration*

After IBM Cloud Object Storage System is set up, configure the storage pool and the vaults according to your organization’s requirements.

Consider the following points:

- Create an access pool, which is a logical collection of zero or more IBM Cloud Object Storage System Accessor nodes. Applications use IBM Cloud Object Storage System to connect to storage pools by using the access pools.
- Enable Access Key authentication to use an Access Key and Secret Key to authenticate vault access in IBM Cloud Object Storage System.
- Create user or multiple users to store data or access data in IBM Cloud Object Storage System vaults. Assign appropriate role to the users and provide access to the vaults as per requirements.
- Generate access key for the users to manage objects in the IBM Cloud Object Storage System (default authentication method for S3 is Access Key ID and Secret Key authentication).

For more information about configuring IBM Cloud Object Storage System, see *IBM Cloud Object Storage System Product Guide, SG24-8439*. 
Understanding access logs in IBM Cloud Object Storage System

Access logs are structured logs that are generated by IBM Cloud Object Storage System in JSON format. They provide logs for the storage operations that are performed on the IBM Cloud Object Storage Accessor along with the statistics that are associated with the operations. These access logs can be found at /var/log/dsnet-core on the Accessor nodes of IBM Cloud Object Storage System.

Figure 7 shows a sample logged event in JSON format that is generated for each PUT operation.

```
{
    "server_name": "localhost",
    "remote_address": "127.0.0.1",
    "remote_user": "1fca4a23a02d6b0",
    "timestamp": "2001-01-01T00:00:00.000Z",
    "timezone": "GMT",
    "request_method": "PUT",
    "request_uri": "/s3nouncer-test/bucket/testFolder/sample.pdf",
    "protocol": "HTTP/1.1",
    "status": "200",
    "response_length": "0",
    "http_version": "HTTP/1.1",
    "cookie": "some cookie value",
    "request_id": "5d4b2f9f-9a8d-4b84-9a8d-4b84-9a8d-4b84",
    "request_time": "2001-01-01 00:00:00.000000 UTC",
    "content_type": "application/pdf",
    "content_length": "12345678",
    "extension": "sample.pdf"
}
```

Figure 7  Sample accessor log event for PUT object operation
Figure 8 shows a sample logged event in JSON format that is generated for each GET operation.

```json
{}
```

Figure 8  Sample accessor log event for GET object operation
Figure 9 shows a sample logged event in JSON format that is generated for each DELETE operation.

```

Figure 9   Sample accessor log event for DELETE object operation

Where:

- **request_method** is the name of the HTTP method with which this request was made, for example, GET, POST, or PUT.
- **request_uri** is the request URI.
- **status** is the status code that is returned in the response.
- **remote_address** is the Internet Protocol (IP) address of the client or last proxy that sent the request.
- **remote_user** is the login of the user who is making this request, if the user is authenticated.
- **interface_type** is the API used to make the request.
- **object_name** is the object’s name.
- **vault_name** is the name of the vault that is associated with the request.

For more information about this format and other fields, see IBM Knowledge Center.
Sending IBM Cloud Object Storage System accessor logs to IBM QRadar SIEM

IBM QRadar SIEM supports different mechanisms to direct events and logs toward it and one of them is rsyslog. In this demonstration, we are sending events from an IBM Cloud Object Storage to IBM QRadar SIEM by using alert forwarding configuration in IBM Cloud Object Storage System.

Complete the following steps to configure alert forwarding in IBM Cloud Object Storage System:

1. Log in to IBM Cloud Object Storage manager user interface (UI)

2. In the **Administration** tab, click **Configure Alert Forwarding** (as shown in Figure 10).

![Figure 10  Configuring alert forwarding in IBM Cloud Object Storage System](image)

3. In the Alert Forwarding Configuration section, click **Enable Alert Forwarding** and click the **Accessor Devices** option to forward alerts from Accessor nodes to IBM QRadar SIEM.

4. In the Syslog section, click the **Enable Syslog Forwarding** option and specify the IP address or hostname of IBM QRadar SIEM server instance and port number where syslogs from IBM Cloud Object Storage System are received (as shown in Figure 11 on page 1411). Select **Facility** as syslog from the drop-down list and then, click the **Include HTTP Access Log** option.
5. Click **Update** to save the configuration and start sending IBM Cloud Object Storage System access logs from the Accessor nodes to IBM QRadar SIEM for threat analysis.

**IBM QRadar SIEM configuration**

After IBM Cloud Object Storage starts sending access logs to IBM QRadar SIEM, configuration is required on IBM QRadar SIEM to understand the access logs and then, according write the rules and take preventive action from IBM QRadar SIEM.

**Configuring IBM QRadar SIEM to process IBM Cloud Object Storage accessor logs**

After IBM Cloud Object Storage is configured to send the access logs to IBM QRadar SIEM, log on to the IBM QRadar SIEM system. IBM QRadar SIEM is already installed and configured.

Log in to IBM QRadar SIEM User Interface (UI).

In the Log Activity tab of the IBM QRadar SIEM UI, filter the events based on the IP address of the IBM Cloud Object Storage System Accessor node IP address. You see the events as Unknown/Unparsed, as shown in Figure 12 on page 15.
Because IBM QRadar SIEM does not recognize these events from IBM Cloud Object Storage System Accessor node, they are identified as Unknown log event. For IBM QRadar SIEM to understand and parse the logs, a custom parser must be created by using DSM Editor.

The payload of the events that are sent by IBM Cloud Object Storage to IBM QRadar SIEM resemble one that is shown in Figure 13.
Next, the parsing logic/uDSM for this log source must be created. This logic can be created by using the DSM Editor. For more information about the DSM Editor, see “Related resources” on page 44.

Select several payloads that are received from the Accessor node, which are displayed as Unknown log event. Then, browse to Log Activity and click Actions → DSM Editor (see Figure 14).

**Figure 14** Starting IBM QRadar SIEM DSM Editor for creating parsing logic
After opening the DSM editor, the new Log Source Type must be created first for the IBM Cloud Object Storage System events (see Figure 15). Click **Create New**.

Enter the Log Source Type Name and click **Save** (see Figure 16).

Next, from the list of Log Source Type, select the new Log Source Type.
Configuring Custom Extract Properties in IBM QRadar SIEM

The following attributes from IBM Cloud Object Storage System events are considered for parsing in this document:

- Event
- Log Source Time
- Access key
- Client IP address
- Accessor node server name
- Request URI
- Status
- Request Length

More attributes can also be parsed, and it is up to the security administrator’s needs. For all of these attributes, we must create a custom property for each identified attribute. QRadar immediately provides a list of default properties, which are used to extract data from events or flow payloads; for example, Source IP, Destination IP, and Ports.

Some event sources (such as IBM Cloud Object Storage System accessor logs in this context) send unique information that is not normalized. We must create Custom Extract Properties (CEP) of such information from the event payload post that we can then use in our Rules, Searches, Reports, and so on.

We extract the following CEPs out from the payload of the events:

- event: Event ID
- Log Source Time: ICOS_EventDate
- Access key: ICOS_AccessKey
- Client IP address: ICOS_ClientIP
- Accessor node server name: ICOS_ServerName
- Request URI: ICOS_RequestURI
- Status: ICOS_Status
- Request Length: ICOS_RequestLength

To add custom properties, complete the following steps:

1. Select the plus (+) button from Properties tab under Tuc_ICOS log source type created (see Figure 17).

![Figure 17  Adding New Custom Property in IBM QRadar SIEM](attachment:image.png)
2. In the Choose Custom Property Definition wizard, click **Create New** (see Figure 18).

![Figure 18 Choosing custom property definition](image)

3. Enter the name of new CEP. Select the Field Type as **Text** from the drop-down list and then, enter a description and click the **Enable this Property** option for use in Rules and Search indexing. Click **Save** (see Figure 19).

![Figure 19 Providing details about new custom property definition](image)

Repeat these steps to create the CEPs for any other attributes.
After all CEPs are created, the next task is to add the Regular Expression (Regex) for these attributes so that they can be parsed. Complete the following steps:

1. From the Properties tab, select **ICOS_AccessKey** and add Regex to parse the attribute, as shown in Figure 20.

![Figure 20  Creating custom property for Access Key](image)

2. Add regular expressions for other CEPs. The regular expression for event ID is shown Figure 21.

![Figure 21  Custom property for Event ID](image)

The regular expression for **ICOS_ClientIP** is shown in Figure 22.

![Figure 22  Custom property for Client IP address](image)
The regular expression for ICOS_EventDate is shown in Figure 23.

![Figure 23 Custom property for Event Date](image1.png)

The regular expression for ICOS_RequestURI is shown in Figure 24.

![Figure 24 Custom property for Request URI](image2.png)

The regular expression for ICOS_RequestLength is shown in Figure 25.

![Figure 25 Custom property for Request Length](image3.png)
The regular expression for ICOS_Status is shown in Figure 26.

![Figure 26 Custom property for Status of object activity](image)

The regular expression for ICOS_ServerName is as shown in Figure 27.

![Figure 27 Custom property for IBM Cloud Object Storage server name](image)

3. Click **Save**.

**Configuring QRadar Identifiers in IBM QRadar SIEM**

A QRadar Identifier (QID) is a numeric representation of a specific event. The next step is to map the events and create the QIDs.

QID identifies following event information:

- Name
- Category
- Severity
- Description

Event categories are used to group incoming events for processing by IBM QRadar SIEM. All generated events are aggregated into high-level and low-level categories. Each high-level category contains low-level categories and an associated severity level. QRadar provides in-built utility `qidmap_c1i.sh` to map the events categories. For more information about this script, see “Related resources” on page 44.
On the QRadar AIO (Console if it is a distributed deployment), run the following commands to create and map the QIDs:

- QID mapping for the event PUT (upload an object) mapping to low-level category “Attempt to upload an object”:
  
  ```bash
  # ./qidmap_cli.sh -c --qname PUT_Obj --qdescription "Attempt to upload or copy an object" --severity 3 --lowlevelcategoryid 19086
  ```

- QID mapping for the event GET (download an object) mapping to low-level category “Attempt to download an object”:
  
  ```bash
  # ./qidmap_cli.sh -c --qname GET_Obj --qdescription "Attempt to download or list an object" --severity 3 --lowlevelcategoryid 19083
  ```

- QID mapping for the event DELETE (delete an object) mapping to low-level category “Attempt to delete an object”:
  
  ```bash
  # ./qidmap_cli.sh -c --qname DELETE_Obj --qdescription "Attempt to delete an object" --severity 3 --lowlevelcategoryid 19081
  ```

- QID mapping for the event HEAD (get a header of an object) mapping to low-level category “Attempt to get header on of an object”:
  
  ```bash
  # ./qidmap_cli.sh -c --qname HEADER_Obj --qdescription "Get an object's header" --severity 3 --lowlevelcategoryid 19080
  ```

- QID mapping for the event POST (delete multiple objects) mapping to low-level category “Attempt to delete multiple objects”:
  
  ```bash
  # ./qidmap_cli.sh -c --qname POST_Obj --qdescription "Attempt to delete multiple objects" --severity 3 --lowlevelcategoryid 19082
  ```

Note: For any new event type, we need to add custom property, Regex and then, map the event category. We concentrate on the following event categories in this document:

- PUT
- GET
- DELETE
- POST
- HEADER
Configuring log source in IBM QRadar SIEM

After QIDs are created and configured, the next step is to create the log source for IBM Cloud Object Storage. Complete the following steps to configure the log source:

1. Browse to Admin → Data Sources → Log Sources (see Figure 28).

![Figure 28](image)

2. In the Log Sources wizard, click **Add** to create a log source (see Figure 29).

![Figure 29](image)

3. Configure the log source with the following details (see Figure 30 on page 25):
   - Log Source Name: Add the name for the log source.
   - Log Source Description: Add Description for log source.
   - Log Source Type: Select the Log Source Type from the drop-down list.
   - Protocol Configuration: Syslog (undocumented) from the drop-down list.
   - Log Source Identifier: Enter the hostname or IP for the IBM Cloud Object Storage Accessor node.
   - Enabled: Select this option
- Credibility: Select the default value.
- Target Event Collector: Event collector over which the events are collected.
- Coalescing Events: You can clear or select coalescing on events.
- Incoming Payload Encoding: Keep the default payload encoding.
- Store Event Payload: Select this option.
- Log Source Extension: Select the extension that was created.

4. Click **Save** to add the log source in IBM QRadar SIEM.

---

**Figure 30** Log source details for IBM Cloud Object Storage System
5. After the log source is created, go to Admin tab and then click **Deploy Changes** to deploy the new configuration changes to IBM QRadar SIEM (see Figure 31).

![Figure 31 Deploy changes in IBM QRadar SIEM after creating Log Source](image)

**Mapping IBM Cloud Object Storage events to QRadar Identifiers**

After the log source is created and QIDs are generated, the next step is to map the events to QIDs. Without mapping the events, they are categorized as an Unknown Generic Log Event.

Complete the following steps:

1. From the Log Activity tab on IBM QRadar SIEM, select the events that were generated from IBM Cloud Object Storage and then click **Map Event** (see Figure 32).

![Figure 32 Selecting Map Event in QRadar for QID mappings](image)
2. In the Log Source Event wizard, search the QID by entering QID and then, from the list of the matching QIDs, select the relevant QID and click OK at the bottom on the wizard window (see Figure 33).

For example, for an event ID, PUT select QID PUT_Obj and for GET, select QID as GET_Obj is created. Select the remaining events individually and map the QIDs.

![Log Source Event wizard](image)

**Figure 33  Mapping events to QRadar Identifiers**
After mapping all of the unique events to their respective QIDs, events that are coming from IBM Cloud Object Storage are correctly parsed (see Figure 34).

IBM QRadar SIEM custom script

IBM QRadar SIEM allows administrators to start a custom script and pass data to a script that is based on a rule response.

It allows custom actions to select or define the value that is passed to the custom script and run the resulting action. The use of these custom scripts is structured.

Three options are available for scripting: Bash, Perl, and Python. Custom actions are run in a “jailshell” to protect from potential use on IBM QRadar SIEM.
The custom script must be uploaded into IBM QRadar SIEM by using the Define Actions icon in the Admin tab of the IBM QRadar SIEM UI (see Figure 35).

![Figure 35](image)

Figure 35  Starting Define Actions for uploading custom script

The script is first created by using a standard editor and saved to a location on the local drive that is used to access IBM QRadar SIEM before uploading it onto QRadar. After the script is created, click the **Define Actions** icon, which displays a list of scripts and allows adding a script.

Click **Add** in the menu bar (see Figure 36).

![Figure 36](image)

Figure 36  Adding new custom script in IBM QRadar SIEM
In the Define Custom Action wizard, enter a name and description in the pop-up window, select the script interpreter from the drop-down list, and then, choose the custom script by clicking **Browse** and selecting the file name.

Enter the parameter names to the script per the customer’s requirements. Then, click **Add** to upload the custom script to IBM QRadar SIEM (see Figure 37).

![Figure 37 Define custom action script details](image-url)
Testing custom action scripts

Uploaded custom scripts can be verified by using IBM QRadar SIEM UI. It can be verified by using the Test Execution option in the Define Actions window or by confirming that the custom rule was triggered.

Complete the following steps:
1. Open the Admin tab in IBM QRadar SIEM and then, browse to Custom Actions and then, Define Actions.
2. Highlight the custom script that was uploaded.
3. Click Test Execution and enter the parameters as required. Then, click Execute (see Figure 38).

4. Verify that the script was run successfully.

If any changes must be made to the script or parameters, use the Edit option to customize the script.
Creating rules in IBM QRadar SIEM

After the events are parsed by IBM QRadar SIEM, the next step is to create the co-relation rules that are based on your business use cases. The number of rules that can be created to take advantage of this integration is infinite.

However, you can create several rules in IBM QRadar SIEM to see the benefit of this integration. You can use the sample manifestations that are described next to create your own use cases for this integration. All of these rules can be created by clicking Offenses → Rules → Actions → New Event Rule in IBM QRadar SIEM to which the IBM Cloud Object Storage log source is sending its events.

Sample Rule 1

The objective of this rule is to detect any object activity during business hours where IBM Cloud Object Storage system is used as a backup destination.

Description
Most of the organizations use Object Storage for backup and archival use cases. This sample rule detects any object activity that is done inside of business hours and generates an offense for such an activity.

In this sample rule, we look for any event from the IBM Cloud Object Storage System Log Source with a QID that relates to object activities and events, such as GET, PUT, DELETE, and HEAD and if this event occurs between business hours, such as after 8:00 AM and before 6:30 PM.

If such an event is detected, this rule generates an offense and increases the Severity, Relevance, and Credibility (SRC) values by 2 so that the Magnitude value of the offense that it generates is higher.
Rule Definition window
The Rule Definition is shown in Figure 39.

Figure 39  Sample Rule 1 definition
**Rule Response window**

The Rule Response window is shown in Figure 40.

![Rule Response window](image)

Figure 40 Sample Rule 1 response configuration

In addition to generating events on IBM QRadar SIEM, we start a custom script to temporarily disable an IBM Cloud Object Storage System account that is performing activity during business hours so that backup activity is stopped during business hours (see Figure 41).

![Sample Rule 1 response with custom action configuration](image)

Figure 41 Sample Rule 1 response with custom action configuration
Rule summary window
The Rule Summary window is shown in Figure 42.

Figure 42   Sample Rule 1 summary

After this rule is applied, IBM QRadar SIEM monitors the rule conditions and an offense is generated whenever any object backup activity is detected during office hours on IBM Cloud Object Storage System.

Sample Rule 2
The objective of this rule is to detect any suspicious object activity from a user after continuous failures or access denied messages are received for object access.

Description
IBM Cloud Object Storage System provides Access Key and Secret Access keys to the authorized users. You can configure suitable access on the IBM Cloud Object Storage System vaults and buckets where only authorized users can access the objects that are inside those buckets.

Read-only access also can be configured to the users for a specific bucket or full access to the users for some buckets.

In this sample rule, we look for events (such as GET, PUT, and DELETE) and look for continuous failures or access denied for those events (these issues might relate to a brute force attack to access the data) by reviewing the IBM Cloud Object Storage events. These events can be categorized as an offense where specific user is trying to perform unauthorized object activity and continuously receiving unauthorized requests errors.

If such suspicious activity is detected, this rule generates an offense and increases the SRC values by 2 so that the Magnitude value of the offense that it generates is higher. It also runs a custom action by starting the custom script to disable this unauthorized user on IBM Cloud Object Storage System remotely.
Rule Definition window

The Rule Definition window is shown in Figure 43.
Rule Response window
The Rule Response window is shown in Figure 44.

In addition to generating an event on IBM QRadar SIEM, a custom script is started to disable the IBM Cloud Object Storage System account that is performing suspicious activities by trying to access objects and getting unauthorized access status from IBM Cloud Object Storage events (see Figure 45).
Rule Summary window
The Rule Summary window is shown in Figure 46.

After this rule is applied, IBM QRadar SIEM monitors the rule conditions. An offense is generated whenever any suspicious activity regarding unauthorized access by user is detected on IBM Cloud Object Storage System.

Sample Rule 3

The objective of this rule is to detect object activity on IBM Cloud Object Storage by the same user from different locations within one hour.

Description

This rule detects any user who performs any object activity simultaneously from multiple locations. It is humanly not possible to perform object activity from one location and then travel to another location and perform the object activity from that new location simultaneously. This activity can indicate shared user IDs or compromised user IDs.

This rule also takes care of scenarios in which a user performs object upload or download from one location (or a system with a unique IP address that maps to specific location) and then uploads, downloads, or deletes objects from another location (or another system with another unique IP address that map to another location) simultaneously.

For implementing this use case, we used the same user ID and performed object upload, download, or delete operations from multiple locations to the same IBM Cloud Object Storage System. On detection of such user activity from multiple locations, an offense is generated and it increases SRC values by 2 so that the Magnitude value of the offense that it generates is on higher. A custom action is run by starting the custom script to disable this user on IBM Cloud Object Storage System remotely.
Rule Definition
The Rule Definition window is shown in Figure 47.
Rule Response

The Rule Response window is shown in Figure 48.

Figure 48  Sample Rule 3 response configuration

In addition to generating an event on IBM QRadar SIEM, we start custom scripts to disable the IBM Cloud Object Storage System account that is performing suspicious activities by trying to access objects from multiple locations simultaneously (see Figure 49).

Figure 49  Sample Rule 3 response configuration with custom action
After this rule is applied, IBM QRadar SIEM starts monitoring the rule conditions and an offense is generated whenever any suspicious activity regarding object access from multiple locations by the same user ID is detected on IBM Cloud Object Storage System.

You can tune any of these rules and modify the Rule Responses that are sent to better suit your environment and requirements.
Conclusion

This paper demonstrated integrating IBM Cloud Object Storage appliance with IBM QRadar SIEM by forwarding access logs from the Accessor nodes of IBM Cloud Object Storage. It can be used for threat detection and prevention to safeguard the data that is stored on IBM Cloud Object Storage.

Such integrated deployment aids security administrators to correlate object access logs with other logs or events from other network devices, servers, and applications to assist security officers to find potential threat vectors and take the required mitigation actions.

It also helps to take automated proactive action for data protection on threat detection. This protection improves overall the cybersecurity posture of the deployment. In addition, consolidation of IBM Cloud Object Storage System access logs in a centralized SIEM, such as IBM QRadar SIEM, helps security auditors to ensure and validate business compliance with various applicable regulations.

The examples that are presented in this paper were simplified to provide a better understanding. The threat detection by way of log analysis, events correlation, and network flows for actionable intelligence can be much more advanced to suit the business’ requirements and audit requirements and to identify potential complex, low and slow cyberattacks or malicious use.

Notice

Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation and other compliances. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients’ business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.
Appendix

A sample custom script is shown in Figure 51.

```python
#!/usr/bin/python
import sys
import requests
import urllib
import socket
from requests.packages.urllib3.exceptions import InsecureRequestWarning
from urllib2 import HTTPError
from collections import OrderedDict

def usage():
    msg = "Usage: (0) <url endpoint> <username> <password> <id> <enabled>"
    print(msg.format(sys.argv[0]))
    sys.exit(1)

def main():
    global url, username, password, xid, enabled
    # disable insecure warning during making the call
    requests.packages.urllib3.disable_warnings(InsecureRequestWarning)
    headers = {'Content-type': 'application/x-www-form-urlencoded', 'Accept': 'application/json'
    endpoint = "https://manager/api/json/1.0/editAccountEnabled.adm"
    idstr = urllib.urlencode(OrderedDict([('id',xid),('enabled',enabled)]))
    url = "https://" + urlstrip() + endpoint
    print("Connecting: \nendpoint: [0]\nusername: [1]\npassword: [2]\nvid: [3]\n" . format(url, username, password, idstr))
    try:
        req = requests.post(url, auth=(username, password), data=idstr, headers=headers, verify=False, timeout=10)
        except socket.timeout:
            print("Socket timeout")
            sys.exit(1)
        except HTTPError:
            print("HTTPError !!")
            sys.exit(1)
        except requests.exceptions.ReadTimeout:
            print("Timeout !!")
            sys.exit(1)
    if req:
        print("Response => [0]" . format(req))
    else:
        print("No response received. Check input ")

if __name__ == '__main__':
    argc = len(sys.argv) - 1
    if argc < 3 or sys.argv[1] == '-h':
        usage()
    url = sys.argv[1]
    username = sys.argv[2]
    password = sys.argv[3]
    xid = sys.argv[4]
    enabled = sys.argv[5]
    main()

Figure 51 Sample custom script
```
Related resources

The following resources provide more information about the topics that are discussed in this Blueprint:

- National Institute of Standards and Technology Cyber Security Framework:
  https://www.nist.gov/cyberframework

- IBM Cloud Object Storage Concepts and Architecture System Edition:

- IBM Cloud Object Storage (IBM Knowledge Center):

- IBM Cloud Object Storage System Product Guide:

- IBM QRadar SIEM white paper:
  https://www.ibm.com/downloads/cas/G6E26E3J

- IBM Security™ QRadar Security Intelligence Platform documentation:

- IBM QRadar SIEM Tuning: The Basics of Rules and Building Blocks:
  https://www.youtube.com/watch?v=HXcXocTTHQM

- IBM QRadar SIEM: User Behavior Analytics (UBA):

- IBM QRadar SIEM DSM Editor:

- IBM QRadar SIEM qidmap_cli.sh:

- IBM QRadar on Cloud (IBM Knowledge Center):

- IBM FlashSystem® (IBM Knowledge Center):

- Getting started with IBM Cloud Virtual Private Networking:

- VMware vSphere documentation:
  https://docs.vmware.com/en/VMware-vSphere/index.html
Authors

This solution paper was written by the following authors and subject matter experts:

• Mandar J. Vaidya
• Sandeep Patil
• Boudhayan Chakrabarty
• Ashish Kothekar
• Praphullachandra Mujumdar
• Prateek Jain
• Vincent Hsu
• Adam Frank

Acknowledgments

The authors of this paper would like to acknowledge the following contributors:

• Julio Hernandez, WW Offering Manager for Storage Cyber Resilience, for his guidance and assistance during the creation of this proof of concept and solution paper.
• Nikhil Shah, L3 Product Support Engineer, and Jordan A. Freedman and John K. Butler, Offering Managers for IBM® Cloud Object Storage, for their assistance during the creation of this proof of concept.
• Bubai Maity, Security Consultant working in Advanced Threat Support team, for reviewing this solution paper.
Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user’s responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, MD-NC119, Armonk, NY 10504-1785, US

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM’s future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided “AS IS”, without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.
Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

<table>
<thead>
<tr>
<th>IBM®</th>
<th>IBM Security™</th>
<th>Redbooks (logo) ™</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM Cloud®</td>
<td>IBM Watson®</td>
<td>Redpaper™</td>
</tr>
<tr>
<td>IBM FlashSystem®</td>
<td>QRadar®</td>
<td>Slicestor®</td>
</tr>
</tbody>
</table>

The following terms are trademarks of other companies:

VMware, VMware vSphere, and the VMware logo are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

Other company, product, or service names may be trademarks or service marks of others.
Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Privacy policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.
