IBM QRadar Incident Forensics
7.5

Administration Guide

Note

Before you use this information and the product that it supports, read the information in "Notices" on page 19.

Contents

Introduction to administrating IBM QRadar Incident Forensics

Information about administrating IBM® QRadar® Incident Forensics.

Intended audience

Administrators create, maintain, and operate an active forensics capability so that users, called investigators, can focus on investigating security incidents, or cases, and exploring data.

Technical documentation

To find IBM QRadar product documentation on the web, including all translated documentation, access the IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

For information about how to access more technical documentation in the QRadar products library, see Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contacting customer support

For information about contacting customer support, see the Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Statement of good security practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Please Note:

Use of this Program may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. IBM QRadar may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of IBM QRadar.

Note

IBM QRadar Incident Forensics is designed to help companies improve their security environment and data. More specifically, IBM QRadar Incident Forensics is designed to help companies investigate and better understand what happened in network security incidents. The tool allows companies to index and search captured network packet data (PCAPs) and includes a feature that can reconstruct such data back into its original form. This reconstruction feature can reconstruct data and files, including email messages, file and picture attachments, VoIP phone calls and websites. Additional information regarding the Program's features and functions and how they may be configured are contained within the manuals and other documentation accompanying the Program. Use of this Program may implicate various laws or regulations. including those related to privacy, data protection, employment, and electronic communications and storage. IBM QRadar Incident Forensics may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of IBM QRadar Incident Forensics.

Chapter 1. Administration workflow and user access to forensics capabilities

After IBM QRadar Incident Forensics is installed and configured, an administrator can troubleshoot, maintain, and monitor the system and its operations and manage user access to cases.

You must have administrative privileges to see the administration tools for QRadar Incident Forensics.

Example: Administration workflow

The following diagram shows a sample workflow for QRadar Incident Forensics administration.

1. Use Server Management to filter web categories and traffic that you, do not want monitor.
2. Use Forensics User Permissions to assign cases to investigators.
3. Use Case Management to create and delete cases and import external content into the system.
4. Use Scheduled Actions to schedule maintenance, such as deleting old documents, tuning the database, and resetting the QRadar Incident Forensics server.

User roles

To add user accounts, you must first create security profiles to meet the specific access requirements of your users. For more information about configuring security profiles, see the *IBM QRadar Administration Guide*.

In the User Roles tool on the **Admin** tab of QRadar, you can assign the following user roles:

Admin
: Users can view and access all cases that are assigned to users and all incidents and are automatically given full access QRadar Incident Forensics.

Forensics
: Users can see and access to the **Forensics** tab, but cannot create cases.

Create cases in Incident Forensics
: Users can automatically create forensics cases.

Chapter 2. Server management

Administrators can troubleshoot, maintain, and monitor the IBM QRadar Incident Forensics system and its operations.

To monitor or change server settings or to view the users that are logged in to the system, open the Server Management tool:

1. Log on to QRadar as an administrator.
2. On the navigation menu (☰), click **Admin**.
3. From the **Forensics** section in the main pane, click **Server Management**.

Server configuration settings

Use server settings in the IBM QRadar Incident Forensics Server Management tool to configure system settings that affect all the managed hosts. After you change a setting, you must deploy your changes by using **Deploy Changes** menu on the **Admin** tab.

Clear Search History on Logout
: Search history is cleared when users log out. The cleared search applies to the query history list in the Query Helper and the last user in the **Search Criteria Input** field on the **Search and Results** page.

Default Number of Nodes to Visualize
: The maximum number of nodes that the Visualize tool shows. You can configure the number of nodes to render after the nodes are rendered for the first time. Adjusting the rendered node count affects only that instance of the Visualize tool.

Protocol and domain inspector filters

You can exclude certain types of traffic from investigations by deactivating protocol or domain inspectors in the Server Management tool. Use the **Inspector Filter** option.

Protocol and domain inspectors process ingested network traffic data and attempt to identify and index the data in a meaningful way. Identifying and indexing that data provides investigators with more control to find the information.

As network traffic data is ingested and protocols are identified, the data is further inspected by the appropriate protocol inspector. Network traffic data that is identified by the HTTP protocol inspector is inspected and indexed further by domain inspectors.

Protocol Inspectors
: Protocol inspectors can identify protocol such as HTTP, POP3, FTP, and telnet. You can exclude protocol inspectors. When the inspectors are excluded, any network traffic data that is associated with the inspector is still ingested, but the traffic is identified and indexed only on a generic level.

Domain Inspectors
: Domain inspectors inspect specific websites. You can exclude domain inspectors. When you exclude domain inspectors, any HTTP network traffic data is associated with the inspector is still ingested, but the traffic is identified and indexed only at the HTTP level. For domain inspectors to be active, the HTTP protocol inspector must also be active.

By default, all filters are turned on.

Remember: When you change the configuration of inspector filters, the new configuration is applied to every new case that is created. The inspectors that are turned on influence the documents that are created for a case and investigators lose the capability of searching for certain inspectors. Users don't know what inspectors are applied to a case.

Any protocol that is not processed by an inspector is categorized as unknown.

Web category filter

You can choose the types of web pages and web servers that are recognized by using web category filters.

For example, you can exclude specific types of HTTP network traffic from investigations. When HTTP network traffic data is ingested, the data is categorized and the resulting documents are grouped.

Administrators can filter HTTP network traffic data to prevent the data from being ingested.

To exclude, or filter traffic, for a category or group, turn off the category or group in the Server Management tool.

Web categorizing, grouping, and filtering affect HTTP network traffic data while it is being ingested and has no effect on data that is already in the system.

When a group filter is set to exclude data, HTTP network traffic data that is associated with categories in that group is filtered out during consumption, regardless of the associated category filters settings.

Example: What happens when you use a web category filter to exclude traffic?

You decide to exclude traffic that contains data from news or magazine sites.

1. On the navigation menu (☰), click **Admin**.
2. You click **Server Management**.
3. You click **Web Category Filter** and click **Off** beside the **News / Magazines** filter.
4. You click the **Webmail / Unified Messaging** filter and click **On**.

Now, when a user investigates ingested traffic on the **Forensics** tab, they see that traffic that contains both **News / Magazines** data and **Webmail / Unified Messaging** is not ingested even though the **Webmail / Unified Messaging** filter is on.

Supported protocols and document types

IBM QRadar Incident Forensics captures the content in network flow packets, and indexes and processes the payload and the metadata.

The following list describes the supported protocols that QRadar Incident Forensics can process:

- AIM
- Berkeley remote commands (**`rexec`**, **`rlogin`**, **`rsh`**)
- BitTorrent
- DHCP
- DNS (Protocol is identified, but documents are not generated by default.)
- Exchange
- FTP
- HTTP
- iCAP
- IMAP
- IRC
- Jabber
- Kerberos
- MySQL
- MSN
- NFS
- NetBIOS Datagram (UDP)

- NetBIOS Session Service (TCP)
- NetBIOS Name Service (TCP) (Protocol is identified, but documents are not generated by default.)
- Oracle
- POP3
- Remote Desktop (RDP)
- SIP Removed in 7.5.0 Update Package 3
- SMB (V1, V2, V3)
- SMTP
- SSH
- Telnet
- Trivial File Transfer Protocol (TFTP)
- TLS (SSL)
- Yahoo Messenger

The following list describes the support domains (websites) and the supported languages for the domain that QRadar Incident Forensics can process:

- AOL (Accessible, Basic, Standard) (EN)
- Charter (EN)
- Comcast (Zimbra) (EN)
- Facebook (Mobile, Desktop) (AR,CN,DE,EN,ES,FR,RU)
- Gmail (Classic, Standard) (AR,CN,DE,EN,ES,FR,RU)
- Hotmail (AR,CN,DE,EN,ES,FR,RU)
- LinkedIn (DE,EN,ES,FR,RU)
- MailCom (CN,EN,ES,FR,RU)
- MailRu (RU)
- Maktoob (AR,EN)
- Myspace (EN)
- QQMail (EN,CN)
- Twitter (EN)
- YAHOO Mail (Standard, Classic) (EN)
- YAHOO Note (EN)
- YouTube (AR,CN,DE,EN,ES,FR,RU)

The following list describes the supported document formats that QRadar Incident Forensics can process:

- HyperText Markup Language
- XML and derived formats
- Microsoft Office document formats
- OpenDocument Format
- Portable Document Format
- Electronic Publication Format
- Rich Text Format
- Compression and packaging formats
- Text formats
- Audio formats
- Image formats

- Video formats
- Java™ class files and archives
- mbox format

Enabling or disabling document generation for specific protocols

In IBM QRadar Incident Forensics, the DNS and NetBIOS Name Service protocols do not generate documents by default. You can change this behavior by changing the document configuration settings for the protocol.

Procedure

1. Using SSH, log in to the QRadar Console.
2. Edit the `/opt/qradar/conf/forensics.xml` file.
3. In the **excludeInspectors** section, add or remove the **nodoc** elements for any inspector that you want to disable document generation for.
   For example, to enable document generation for the DNS protocol, remove the **<nodoc>dns</nodoc>** line.

   To disable document generation for a specific protocol, add a line that matches the `<nodoc>protocol_name</nodoc>` format.
4. Save the changes to the `forensics.xml` file.
5. To push the configuration changes to all managed hosts, type this command:

   ```
   /opt/qradar/support/all_servers.sh -p /opt/qradar/conf/forensics.xml -r /opt/qradar/conf
   ```
6. Using a web browser, log in to the QRadar Console.
7. On the **Admin** tab, click **Advanced** > **Deploy Full Configuration**.
   When the deployment is complete, the configuration changes apply to all future QRadar Incident Forensics recoveries and packet capture file uploads to cases.

Auditing user and system usage in QRadar Incident Forensics

Audit logs are chronological records that identify user accounts that are associated with data access. These logs can detect unusual or unauthorized access can and can identify problems such as failed jobs.

The following activities generate audit log events:

- Create case
- Assign Case
- Delete case
- Delete collection
- All user queries
- Document view
- Export document

Restriction: Logging create collection events is not supported.

Procedure

1. Use SSH to log on to the QRadar Console or QRadar Incident Forensics Standalone as an administrator.
2. Go to the `/var/log/audit` directory.
3. Open the `audit.log` file in an editor, such as vi, to review the contents or use the **grep** command to look for a specific entry.

Chapter 3. Case management

As an administrator, you can manage cases and collections by using Case Management. You can create cases for collections of documents or packet capture (pcap) files and can also import external files in to the IBM QRadar Incident Forensics system.

Distribution graphs

If you plan to delete a case, you can visually use the graphs to quickly review the content of the case. You can review the type of files, the protocols, and the domains that are in the case.

Uploading pcap files to managed hosts

You can manually upload pcap data from external sources. You can specify which QRadar Incident Forensics managed host to upload the data to for processing. For example, if you have three managed hosts and three pcap files, you can upload each one to a different managed host. For larger pcap files, use FTP.

Creating cases

Cases are logical containers for your collection of imported document and pcap files. You can use a single case for all pcap files or create multiple cases. Cases can be restricted to specific users. QRadar Incident Forensics. To avoid out of memory errors, limit the number of cases that are allowed on each instance of QRadar Incident Forensics to 150. Review existing cases and remove the cases that don't have any associated PCAP files.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. Select **Case Management**.
3. Click **Add New Case**.
4. In the **Case Name** field, type a unique name.

   Restriction:

   Case names cannot contain spaces.
5. Click **Save**.

Results

A new directory that is based on the case name is created: `/case_input/<case_name>`. This directory is used to import your pcap files.

Uploading files to cases

As an administrator, you can upload external packet capture (pcap) files and documents, such as spreadsheets, text files, and image files, to IBM QRadar Incident Forensics Case Management.

The following file types are supported:

- HyperText Markup Language
- XML and derived formats
- Microsoft Office document formats
- OpenDocument Format

- Portable Document Format
- Electronic Publication Format
- Rich Text Format
- Compression and packaging formats
- Text formats
- Audio formats
- Image formats
- Video formats
- Java class files and archives
- The mbox format

Case Management restricts both the number of files that you can add to a case and the maximum file size.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **Forensics** section, click **Case Management**.
3. Select a case.
   - To add external files to an existing case, select the case from the **Cases** list.
   - To add files to a new case, click **Add New Case**.

     Restriction: Case names cannot contain spaces.
4. From the **Upload to Host** list, select the managed host that you want to process the files.
5. To add pcap files or other document types, choose one of the following methods:
   - Click **Add files**, select the files, and click **Start upload**.
   - Drag the files to the upload box.

   After the upload is complete, the files are listed in the **Collections** list.

Assigning cases to users

As an administrator, you grant access to forensics data to users, assign cases to users, and configure user permissions such as FTP access. Users cannot see data until they are assigned a case and they can see only the data from the cases to which they are assigned.

Be careful when you assign cases to non-admin users who have restricted access to networks. They can see documents that are from the IP addresses that they don't normally have access to. For example, if you assign a non-admin user a case that contains financial or human resources information, they can see the data when they investigate the case.

About this task

Administrators can do the following tasks:

- Assign multiple users to a case.
- Remove a case from a user.
- View and access all cases that are assigned to a user.

Users can see only the cases that are explicitly assigned to them.

Procedure

1. On the navigation menu (☰), click **Admin**.

2. Click **Forensics User Permissions**.
3. From the **Users** list, select a user.
4. From the list of cases in the **Available** list, select one or more cases and click the arrow (>) to move the cases to the **Assigned** list.

   Tip: By default, a user with administrative privileges is assigned to all cases. The left arrow (<) and right (>) arrow are not displayed.

Manually importing files to a forensics case

Unlike the Case Management tool, there are no restrictions on the file size or the number of files when you manually import files. You can manually create a case and copy files to it or manually copy files to an existing case.

For example, you can use the **scp** command to securely copy files from another host to the /opt/ibm/forensics/case_input/<case_name>/ directory on the IBM QRadar Incident Forensics host.

Before you begin

Make a back-up copy of the imported files. After the file is imported and processed, the original file is deleted.

Procedure

1. Use SSH to log in to QRadar Incident Forensics as a root user.
2. To create a new case, go to the /opt/ibm/forensics/case_input and type the following command:

   mkdir /opt/ibm/forensics/case_input/*<case_name>*
3. To copy files to a case, use a file the **scp** command or another file transfer program to copy the files to the directory that corresponds to the file type.

   The following table lists the directory structure for the imported files.

   Table 1. Directory structure of case files

Directory	Description
/opt/ibm/forensics/case_input/*<case_name>*	The directory that is used to import a series or connected stream of pcap files.
/opt/ibm/forensics/case_input/*<case_name>*/singles	The directory that is used to import individual pcap files.
/opt/ibm/forensics/case_input/*<case_name>*/import	The directory that is used to import a single file of a type other than pcap, for example, Microsoft Word documents, Adobe Acrobat PDFs, text files, and images.

   Important: If a hyphen is used in a file name, it is changed to an underscore when the file is imported.

Results

After a successful import, your file name automatically appears in the **Collections** window of the case that you created.

Enabling users to FTP pcap files and documents from external systems to forensics cases

To upload external data to include in specific cases, administrators can grant secure FTP permissions to users and manage the case to which the data is associated. Users can choose which IBM QRadar Incident Forensics host processes the FTP request.

To change a password after FTP access is enabled, you must disable FTP access and save the user, and then re-enable FTP access, and enter the new password.

Before you begin

Ensure that you create or assign roles for forensics investigators in the User Roles tool on the **Admin** tab.

By default, the `/etc/vsftpd/vsftpd.conf` file is configured so that five ports are open: 55100-55104. You can change the port range by editing the `/etc/vsftpd/vsftpd.conf` file and changing the values of the `pasv_min_port` and `pasv_max_port` settings to the range of ports that you want. You must deploy your configuration changes by clicking **Deploy Changes** on the **Admin** tab.

Note: FTP clients must support TLS v1.2 (`vsftpd.conf` file). The following list describes the minimum FTP client versions that are supported:

- WinSCP 5.7
- FileZilla 3.9.0.6

About this task

IBM QRadar Incident Forensics can import data from any accessible directory that is on the network. The data can be in a number of formats, including but not limited to the following formats:

- Standard PCAP format files from external sources
- Documents such as text files, PDF files, spreadsheets, and presentations
- Image files
- Streaming data from applications
- Streaming data from external PCAP sources

Users can upload multiple files to a case and an administrator can grant multiple users access to the case.

Restriction: The case name must be unique. A single user is associated with a case. Therefore, two users cannot create a case that has the same name.

Procedure

1. On the **Admin**, click **Forensics User Permissions**.
2. From the **Users** list, select a user.
3. In the **Edit User** pane, select the **Enable FTP access** check box.
4. Enter and confirm the FTP password for the user.
5. To save changes to the permissions, click **Save User**.
6. To restart the FTP server, type the following command:

   ```
   systemctl restart ftpmonitor
   ```
7. To restart the server that moves the files from the upload area to the QRadar Incident Forensics directory, type the following command:

   ```
   systemctl restart vsftpd
   ```
8. In the FTP client, do the following steps:

   a) Ensure that Transport Layer Security (TLS) is selected as the protocol.

b) Add the IP address of the QRadar Incident Forensics host.

c) Create a logon that uses the QRadar Incident Forensics user name and password that was created.

9. Connect to the QRadar Incident Forensics server and create a new directory. The new directory that you create is used as the case name.
10. To FTP and store pcap files, create a directory that is named <case_name_from_step_9>/singles and drag the pcap files to that directory.
11. To FTP and store file types that are not pcap files, create a directory that is named <case_name_from_step_9>/import and drag the files to that directory.

Results

An administrator sees the data that is uploaded in Case Management. A user can see their case in one of the tools on the **Forensics** tab.

Chapter 4. Decrypting SSL and TLS traffic in QRadar Incident Forensics

To find hidden threats, it might be necessary to decrypt SSL and TLS traffic that is processed by IBM QRadar.

For IBM QRadar Incident Forensics deployments that include IBM QRadar Network Packet Capture, it is recommended that you use a dedicated man-in-the-middle solution where the clear text output is fed into QRadar.

For deployments that do not include QRadar Network Packet Capture, or if you do not want to deploy a man-in-the-middle solution, limited decryption capabilities are available within QRadar if the required keys are available. You will experience performance degradation if you enable the decryption capability.

Decryption is supported for the following protocols:

- SSL v3
- TLS v1.0
- TLS v1.1
- TLS v1.2

Restriction:

The following restrictions apply:

- Traffic cannot be decrypted if SSL or TLS compression is in use.
- The `Diffie Hellman` key exchange mechanism is not supported when encrypted traffic is decrypted through a private key. When you use a private key, other key exchange methods, such as RSA, are supported. This restriction does not apply when traffic is decrypted with information that is found in a key log.
- In FIPS mode, OpenSSL supports a limited list of ciphers that can be decrypted. Run the **`openssl ciphers`** command to view a full list of ciphers available in FIPS mode. Not all the listed ciphers are supported for decryption.

Decrypting SSL and TLS traffic by using a server's private key

By providing a server's IP address and its private key, you can decrypt traffic that is going to that host.

Procedure

1. Use SSH to log in to the QRadar Incident Forensics host as the root user.
2. Review the location of the keys in the `/opt/qradar/conf/forensics_config.xml` file.

   ```
   <keybag
   keydir="/opt/ibm/forensics/decapper/keys"
   keylogs="/opt/ibm/forensics/decapper/keylogs"/>
   ```

   You will use the `keydir` and `keylogs` locations in the next steps.
3. Copy one or more private keys into the `keydir` directory.
4. In the `keydir` directory, modify the `key_config.xml` file to specify your key file and the IP addresses that it applies to.

   The key file can apply to a single IP address, a range of IP addresses, or both. For example, the `key_config.xml` file might look like this:

   Example:

```
<keys>
<key file=" /opt/ibm/forensics/decapper/keys/key_name">
<address>10.2.3.4</address>
<range>10.2.3.0-10.2.3.255</range>
</key>
</keys>
```

5. Restart the decapper service by typing the following command:

   `systemctl restart decapper`

Results

From this point on, all analysis of new recoveries or flows use the new keys to decrypt traffic.

Decrypting SSL and TLS traffic by using client key log files

If you have the key log files from a client's browser, you can import them into IBM QRadar Incident Forensics to decrypt traffic from that client.

Key log files are generated by Google Chrome, Firefox, and Opera browsers that have the `SSLKEYLOGFILE` environment variable set. Only the RSA and DH key formats are supported for the `SSLKEYLOGFILE` session key.

Procedure

1. Use SSH to log in to the QRadar Console, and then into the QRadar Incident Forensics host as the root user.
2. Review the location of the key logs in the `/opt/qradar/conf/forensics_config.xml` file.

   ```
   <keybag
   keydir="/opt/ibm/forensics/decapper/keys"
   keylogs="/opt/ibm/forensics/decapper/keylogs"/>
   ```

   You will use the `keylogs` location in the next steps.
3. Copy the key log files into the `keylogs` default directory.

   For example, `/opt/ibm/forensics/decapper/keylogs/default`.
4. Restart the decapper service by typing the following command:

   `systemctl restart decapper`

Results

From this point on, all analysis of new recoveries or flows use the new keys to decrypt traffic.

Chapter 5. Scheduled actions in QRadar Incident Forensics

You can schedule maintenance, such as deleting old documents, tuning the database, and resetting the IBM QRadar Incident Forensics server.

If there are many documents, scheduled actions, such as deleting old documents, might take a long time to complete. If you want to delete an entire case, use the Case Management tool.

Deleting documents

Administrators can delete outdated documents that are based on the document network time stamps.

You can delete documents, which include pcap and other file types, from a case or the server. Deleting outdated documents helps maintain speed when you search documents.

Optimizing the database

Administrators can optimize the database to reorganize the search engine index into segments and remove deleted documents.

The **Optimize Database** scheduled action is similar to a **`defrag`** command.

When you optimize the database, a new index builds. After the index is built, the new index replaces the old index. Because two indexes exist until the old index is replaced, the optimize index command requires double the amount of hard disk space.

Before you optimize your database, you must ensure that the size of your index does not exceed 50 percent of the available space on your hard disk.

Scheduling actions for QRadar Incident Forensics hosts

You can schedule maintenance tasks on the IBM QRadar Incident Forensics hosts.

You can schedule a task to build a new index for the currently available cases, or to remove (*age out*) documents that you don't want to retain after a specified time period.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **Forensics** section, click **Schedule Actions**.
3. Click **Add New Action**.
4. From the **Select Action** list, select an action and specify the settings.
   - To build a new index for current cases, select **Optimize Index**.

     The new index requires about twice as much space as the existing index. Ensure that you have adequate space.
   - To delete documents that have a network time stamp older than a specified age, select **Age Out Documents**.

     Indexes are also removed when you delete the documents.
5. Click **Save**.
6. To run, edit, or delete the action, select the action for the **Actions** list and click **run**, **edit**, or **delete**.

Chapter 6. Managing suspicious content

As an administrator, you can flag suspicious content by using the **Suspect Content Management** feature.

Yara rules

To flag suspicious content in the files that are found in QRadar Incident Forensics network traffic, you can import and use existing Yara rules to specify the custom rules that are run on the files.

Each Yara rule starts with the keyword rule followed by a rule identifier. Yara rules are composed of two sections:

String definition
In the strings definition section, specify the strings to form part of the rule. Each string uses an identifier that consists of a dollar sign ($) followed by a sequence of alphanumeric characters that are separated by underscores.

Condition
In the condition section, define the logic of the rule. The condition section must contain a Boolean expression that defines the conditions in which a file satisfies the rule.

The following example shows a simple Yara rule that looks for str1 at an offset of 25 bytes into the file:

```
rule simple_forensics : qradar
{
    meta:
        description = "Simple Yara rule."

    strings:
        $str1 = "pattern of interest"

    condition:
        $str1 at 25
}
```

The following example shows a more complex Yara rule that flags content that contains the hex sequence, and str1 at least three times:

```
rule ibm_forensics : qradar
{
    meta:
        description = "Complex Yara rule."


    strings:
        $hex1 = {4D 2B 68 00 ?? 14 99 F9 B? 00 30 C1 8D}
        $str1 = "IBM Security!"


    condition:
        $hex1 and (#str1 > 3)
}
```

When the Yara rule is uploaded, the decapper uses rules that are specified when it finds a file in a recovery or a PCAP upload. If there is matching content that is found, a **SuspectContent** field is added under the **Attributes** tab for a document. The **Suspect Content Description** property is populated with the Yara rule name and any tags that are identified by the rule.

Restriction: Implementation of Yara modules is not currently available.

Importing Yara rules

You can import your existing Yara rules into IBM QRadar Incident Forensics and IBM QRadar Network Insights, and use those rules for matching and flagging malicious content. More than one Yara rule can exist in an imported file. Uploading a new Yara rules file replaces all existing Yara rules within the system. Upload existing rules in the new file to retain them.

Procedure

1. Click **Main Menu** > **Admin** and select **Suspect Content Management**.
2. Click **Select File**.
3. In the **File Upload** window, browse to the file you want to import and click **Open**.

   Important: Yara rule names must be unique.

Results

You see a message when the Yara rule is imported successfully.

What to do next

Newly imported Yara rules are not applied retroactively. After you import the Yara rules, you must perform a full deployment for the changes to take effect.

Deleting Yara rules

You can delete all existing Yara rules from IBM QRadar Incident Forensics. You upload a file that contains a single empty rule to turn off Yara rules.

Before you begin

Procedure

1. To create a new file that contains a single empty rule, use the following steps:
   a) Copy the following rule into a text editor of your choice:

   ```
   rule empty
   {
       condition:
               false
   }
   ```

   b) Save as a text file.
2. On the navigation menu ( ), click **Admin**.
3. Select **Suspect Content Management**.
4. Click **Select File**.
5. In the **File Upload** window, browse to the file you created in Step 1 and click **Open**.
6. Click **Save**.

Results

The single rule always returns a **`false`** result, which allows it to pass the validator. The single rule deletes all existing rules, and is inserted into the database. The single rule never flags content as suspicious.

Notices

This information was developed for products and services offered in the U.S.A.

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
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

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.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

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.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

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.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., 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 www.ibm.com/legal/copytrade.shtml.

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.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

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.

IBM Online Privacy Statement

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.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user’s session id for purposes of session management and authentication. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

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.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details/ the section entitled “Cookies, Web Beacons and Other Technologies”.

General Data Protection Regulation

Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. 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.

Learn more about the IBM GDPR readiness journey and our GDPR capabilities and Offerings here: https://ibm.com/gdpr