Fortinet and IBM Resilient

Overview ......................................................... 3
Deployment Prerequisites ................................. 3
Architecture Overview ....................................... 3
FortiAnalyzer Configuration ............................... 4
IBM Resilient Configuration ............................... 6
Summary ......................................................... 9
Overview

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network - today and into the future. Only the Fortinet Security Fabric architecture can deliver security features without compromise to address the most critical security challenges, whether in networked, application, cloud or mobile environments. Fortinet ranks #1 in the most security appliances shipped worldwide and more than 400,000 customers trust Fortinet to protect their businesses. Learn more at https://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

About IBM Resilient

IBM Resilient Incident Response Platform (IRP) is the leading platform for orchestrating and automating incident response processes. IBM Resilient IRP quickly and easily integrates with your organization’s existing security and IT investments. It makes security alerts instantly actionable, provides valuable intelligence and incident context, and enables adaptive response to complex cyber threats.

Architecture Overview

Deployment Prerequisites

1. Fortinet FortiAnalyzer version 6.x (tested with version 6.0.0)
2. IBM Resilient version 30.x (tested with version 30.0.3476)
   - With Email Connector version 2.2 installed
FortiAnalyzer Configuration

Create and configure an Email Server.

From System Settings, go to Mail Server > Create New.

Enter a name to identify the mail server, the hostname or IP address of your mail server and the SMTP port (typically 25). Be sure to enable Authentication if your mail server requires it. Then, enter a valid Email address and password for the Account. Click OK when done.

The screen should look like the image below.
Configure FortiAnalyzer to send Email Alerts when certain Events occur.

Click System Settings from the top left then choose Event Manager.

From this view you can see there was an HTTP Event specifically about Application Control. On the right, the Handler is where Email Alerting is configured.

In this example we will configure an Email Alert to be sent when there is an Admin logon failure via SSH.

Click Collapse All.
Then locate the Event User login from SSH. Click Local Device Event under the Handler.

Enable Send Email Alert under Notifications. Enter the Email address you want to send Alerts to. Enter the Email address you want to use as the sender address. Enter a Subject for the Email. Lastly, under Email Server, choose the Email Server created previously.

The FortiAnalyzer Configuration is complete.

**IBM Resilient Configuration**

This guide assumes that the IBM Resilient IRHub is already installed and configured. Refer to Resilient Email Connector Config Guide v2.x for more details. Install the Email Connector package using the following command, where `<version>` is the run file version.

```
Last login: Tue Jun 5 16:21:27 2018 from 10.101.32.254
-bash-4.2$ sudo rpm -i irhub-mail<-version>.rpm
```
If using the IMAP protocol, run the IMAP script to configure the email account to monitor by entering the following command and following the prompts.

```
Last login: Tue Jun  5 16:21:27 2018 from 10.101.32.254
-bash-4.2$ sudo irhub-imap-cfg
```

As prompted, enter the following information:

- IMAP mail server host name; for example, mail.example.com
- Trust the certificate (only prompted if the certificate is untrusted)
- IMAP username; for example, resilient@example.com
- IMAP user password

The script concludes by stating the location of the configuration file. For example:

```
Selecting mailbox INBOX OK
IMAP configuration settings were written to /usr/share/irhub/etc/irhub.mail.cfg
```

If using the EWS protocol, run the EWS script to configure the email account to monitor by entering the following command and following the prompts.

```
Last login: Tue Jun  5 16:21:27 2018 from 10.101.32.254
-bash-4.2$ sudo irhub-ews-cfg
```

As prompted, enter the following information:

- EWS endpoint; for example, https://mail.example.com/ews/exchange.asmx
- Trust the certificate (only prompted if the certificate is untrusted)
- EWS username; for example, resilient@example.com

**NOTE:** it must be in email format. Domain\Username format does not work.

- EWS user password

The EWS script automatically sets the mail_protocol property to EWS. If using the EWS script to make changes after the initial installation, make sure to restart the IRHub for the updates to take effect. The script concludes by stating the location of the configuration file. For example:

Using the following settings:

```
Endpoint = https://mail.example.com/ews/exchange.asmx, Mailbox = Inbox
```

EWS configuration settings were written to /usr/share/irhub/etc/irhub.mail.cfg

Restart IRHub as follows:

```
-bash-4.2$ sudo systemctl restart irhub
[sudo] password for resadmin:
-bash-4.2$ 
```
At this point FortiAnalyzer will send an Email Alert to Resilient when there is a failed Admin logon via SSH. You can test this by making several failed authentication attempts to the FortiAnalyzer CLI:

![Image of failed SSH login attempt]

Now login to the Resilient GUI and check List Incidents. It should look like the image below:

![Image of Resilient GUI showing list of incidents]

The incidents will include details such as the date and time of the login attempt, the username, and the status of the incident.
Notice that the Incident Name is populated by the Email Subject and a description of the Incident is included.

![Incident Name](image)

Click on an Incident Name to view details.

Notice that an ID Number is automatically assigned to the Incident.

The Incident indicates which device the Incident came from, in this case FAZ-VM0000101910.

The full Log message is also included in the Incident.

**Summary**

Fortinet and IBM Resilient.