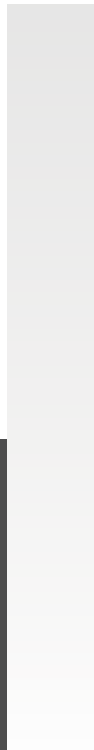
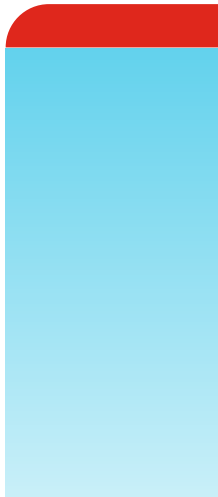


DEPLOYMENT GUIDE

Fortinet and IBM Resilient



Fortinet and IBM Resilient

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



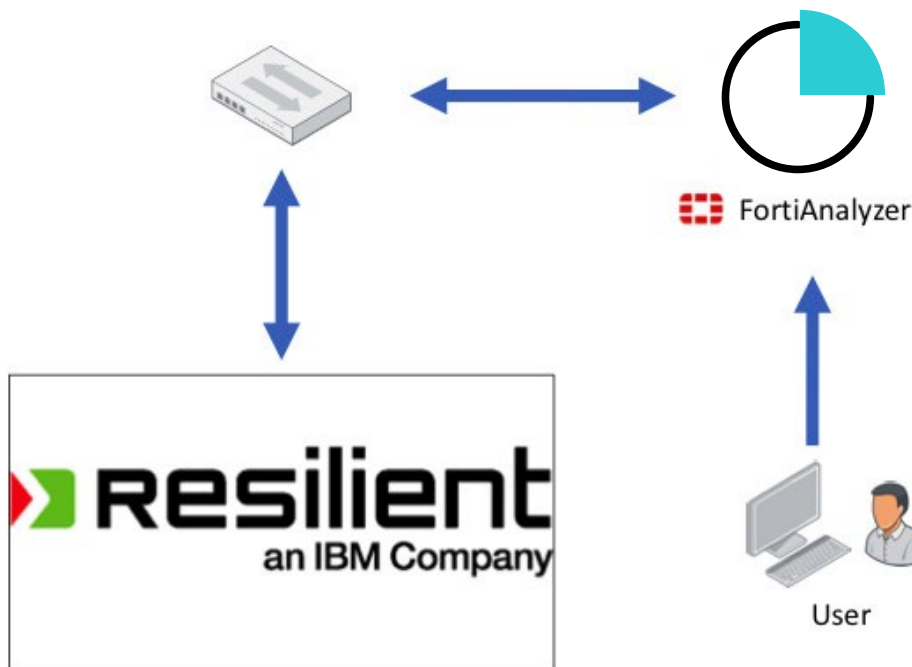
Overview

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



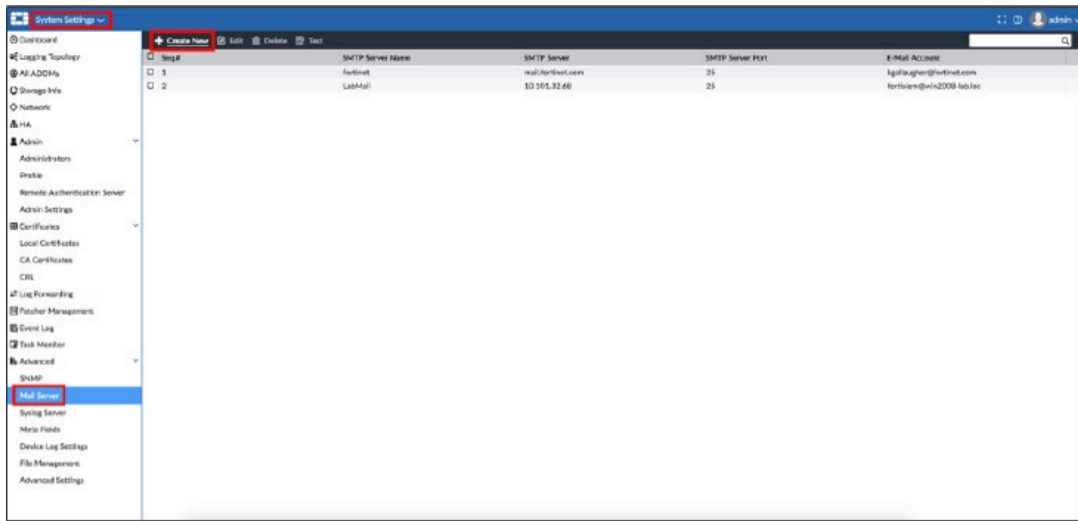
Deployment Prerequisites

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

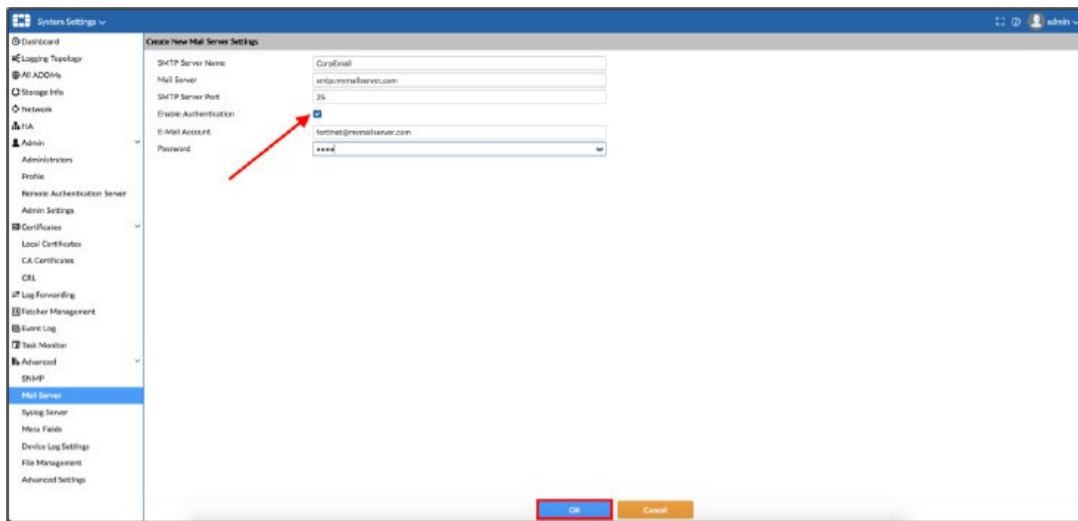


FortiAnalyzer Configuration

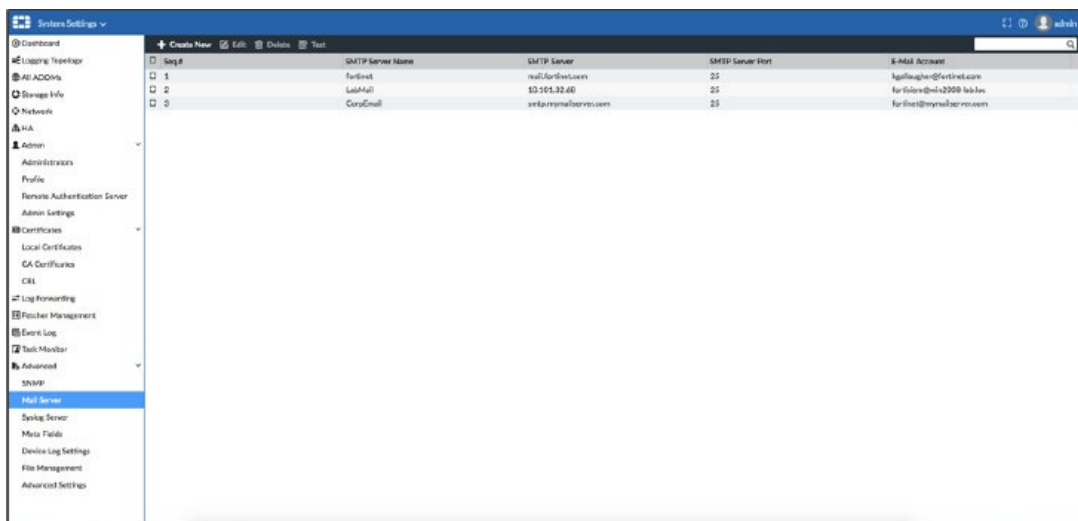
Create and configure an Email Server. From System Settings, go to **Mail Server > Create New**.



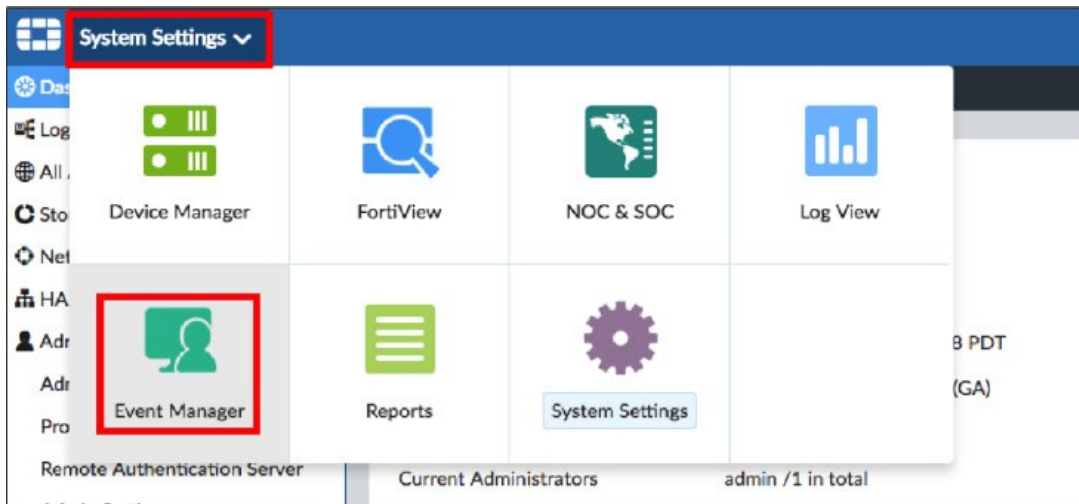
Enter a name to identify the mail server, the hostname, or IP address of your mail server and the SMTP port (typically 25). Be sure to enable Authentication if your mail server requires it. Then, enter a valid Email address and password for the Account. Click **OK** when done.



The screen shot 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.

#	Event	Event Status	Event Type	Count	Severity	Last Update	Additional Info	Handler
1	Proxy.HTTP (335)					16 minutes ago		
	app.Proxy.HTTP		Application Control	2	Critical	2018-06-06 10:10:58		UTM App Ctrl Event
	app.Proxy.HTTP		Application Control	2	Critical	2018-06-06 09:40:48		UTM App Ctrl Event
	app.Proxy.HTTP		Application Control	2	Critical	2018-06-06 09:10:48		UTM App Ctrl Event
	app.Proxy.HTTP		Application Control	3	Critical	2018-06-06 08:57:48		UTM App Ctrl Event
	app.Proxy.HTTP		Application Control	2	Critical	2018-06-06 08:10:38		UTM App Ctrl Event
	app.Proxy.HTTP		Application Control	12	Critical	2018-06-06 07:57:36		UTM App Ctrl Event
	app.Proxy.HTTP		Application Control	2	Critical	2018-06-06 07:10:28		UTM App Ctrl Event
	app.Proxy.HTTP		Application Control	2	Critical	2018-06-06 06:40:18		UTM App Ctrl Event
	app.Proxy.HTTP		Application Control	2	Critical	2018-06-06 06:10:18		UTM App Ctrl Event
	app.Proxy.HTTP		Application Control	2	Critical	2018-06-06 05:40:08		UTM App Ctrl Event

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

The screenshot shows the FortiAnalyzer Event Manager interface. The 'Collapse All' button in the top right corner of the table area is highlighted with a red box. The table below shows the same list of Application Control events as in the previous screenshot.

#	Event	Event Status	Event Type	Count	Severity	Last Update	Additional Info	Handler
1	Proxy.HTTP (335)					21 minutes ago		
	app.Proxy.HTTP		Application Control	2	Critical	2018-06-06 10:10:58		UTM App Ctrl Event
	app.Proxy.HTTP		Application Control	2	Critical	2018-06-06 09:40:48		UTM App Ctrl Event
	app.Proxy.HTTP		Application Control	2	Critical	2018-06-06 09:10:48		UTM App Ctrl Event
	app.Proxy.HTTP		Application Control	3	Critical	2018-06-06 08:57:48		UTM App Ctrl Event
	app.Proxy.HTTP		Application Control	2	Critical	2018-06-06 08:10:38		UTM App Ctrl Event
	app.Proxy.HTTP		Application Control	12	Critical	2018-06-06 07:57:36		UTM App Ctrl Event
	app.Proxy.HTTP		Application Control	2	Critical	2018-06-06 07:10:28		UTM App Ctrl Event
	app.Proxy.HTTP		Application Control	2	Critical	2018-06-06 06:40:18		UTM App Ctrl Event
	app.Proxy.HTTP		Application Control	2	Critical	2018-06-06 06:10:18		UTM App Ctrl Event



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

#	Event	Event Status	Event Type	Count	Severity	Last Update	Additional Info	Handler
1	Proxy-HTTP (335)		Application Control	1371	Critical	23 minutes ago		UTM App Ctrl Event
2	Remove local db (14)		Event	14	Medium	3 hours ago		Local Device Event
3	Trim local db (14)		Event	14	Medium	3 hours ago	Requested to trim database tables older than 60 days to enforce the retention policy of Adom root.	Local Device Event
4	SSL Message Authentication Code corrupted (7)		Event	49	Medium	12 hours ago	Corrupted MAC packet detected	FOS Event Log Higher T
5	User login/logout failed (7)		Event	21	Medium	12 hours ago	user '0 (-: echo Plugin output: \$(1+* login failed from telnet(10.101.32.173)	Local Device Event
6	User login from SSH (7)		Event	7	Medium	12 hours ago	A user login failed from ssh	Local Device Event
7	User login failed (7)		Event	7	Medium	18 hours ago	Device FGVM040000101072 login failed for restapi request due to empty user name.	Local Device Event
8	User login from SSH failed (2)		Event	9	Medium	18 hours ago		Local Device Event
9	Admin login failed (2)		Event	4	Medium	18 hours ago		FOS Event Log Higher T
10	logdesc:Admin login disabled		Event	1	Medium	2018-06-05 16:18:43	Login disabled from IP 10.101.32.254 for 60 seconds because of 3 bad attempts	FOS Event Log Higher T
11	Files dropped by quarantine daemon (12)		Event	20	Medium	A day ago		FOS Event Log Higher T
12	desc:Send mail failed		Event	1	Medium	2018-06-04 16:26:46	Failed to send a test email to kgallagher@fortinet.com through LabMail.	Local Device Event
13	logdesc:FortiGate update failed		Event	1	Medium	2018-06-03 08:43:56	Fortigate scheduled update failed	FOS Event Log Higher T
14	Malicious Websites (16)		Web Filter	45	Medium	6 days ago		UTM Web Filter Event

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.

Edit Event Handler

Status: ON

Name: Local Device Event

Description: Default local device event handler

Devices: All Devices Specify

Filters: +

Filter 1: >

Notifications:

- Send Alert Email
- Send SNMP(v1/v2) Trap
- Send SNMP(v3) Trap
- Send Alert to Syslog Server
- Send Each Alert Separately

To: resilient@mymailserver.com

From: fortianalyzer@mymailserver.com

Subject: User Logon failed via SSH

Email Server: CorpEmail: smtp.mymailserver.com

Buttons: Factory Reset, OK, Cancel

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:

- nEWS endpoint; for example, https://mail.example.com/ews/exchange.asmx
- nTrust the certificate (only prompted if the certificate is untrusted)
- nEWS username; for example, resilient@example.com
- NOTE: It must be in email format. Domain/Username format does not work.
- nEWS 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:

```
Last login: Tue Jun  5 16:21:27 2018 from 10.101.32.254
[-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:

```

kgallaugher — -bash — 80x24
Last login: Wed Jun  6 10:50:07 on ttys000
kgallaugher-mac:~ kgallaugher$ ssh admin@10.101.32.67
Password:
Password:
Password:
Authentication failed.
kgallaugher-mac:~ kgallaugher$
    
```

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

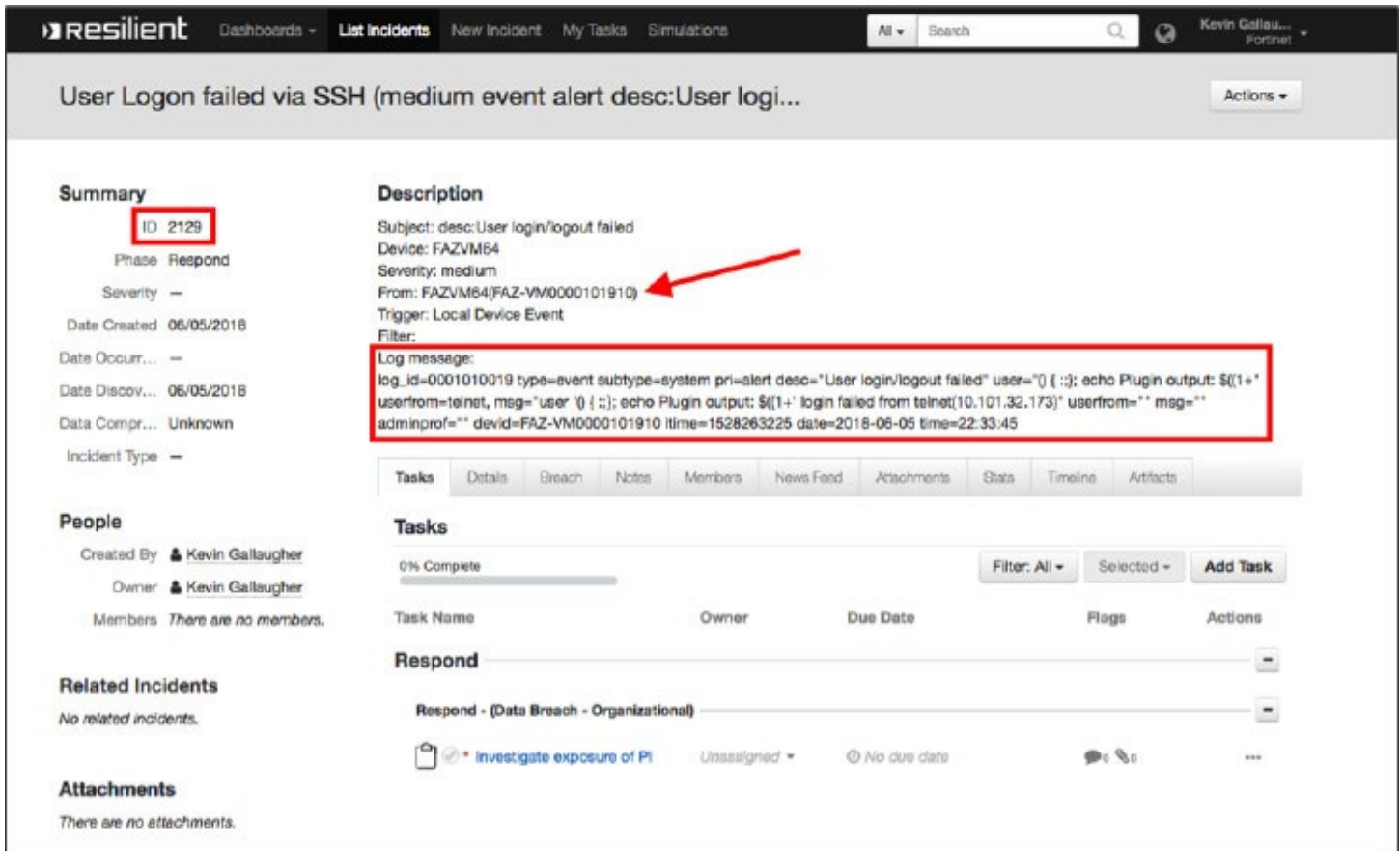
ID	Name	Description	Date Discovered	Next Due Date	Date Created	Owner	Phase	Severity	Status
2131	User Logon failed via SSH (medium event alert desc:Remove local db FAZVM64)	Subject: desc:Remove local db Device: FAZVM64 Severity: medium From: FAZVM64FAZ-VM000101910 Trigger: Local Device Event	06/06/2018	--	06/06/2018	Kevin Gallagher	Respond	--	Active
2130	User Logon failed via SSH (medium event alert desc:Trim local db FAZVM64)	Subject: desc:Trim local db Device: FAZVM64 Severity: medium From: FAZVM64FAZ-VM000101910 Trigger: Local Device Event	06/06/2018	--	06/06/2018	Kevin Gallagher	Respond	--	Active
2129	User Logon failed via SSH (medium event alert desc:User login/logout failed FAZVM64)	Subject: desc:User login/logout failed Device: FAZVM64 Severity: medium From: FAZVM64FAZ-VM000101910 Trigger: Local Device Event	06/05/2018	--	06/05/2018	Kevin Gallagher	Respond	--	Active
2128	User Logon failed via SSH (medium event alert desc:User login from SSH FAZVM64)	Subject: desc:User login from SSH Device: FAZVM64 Severity: medium From: FAZVM64FAZ-VM000101910 Trigger: Local Device Event	06/05/2018	--	06/05/2018	Kevin Gallagher	Respond	--	Active
2127	User Logon failed via SSH (medium event alert desc:Remove local db FAZVM64)	Subject: desc:Remove local db Device: FAZVM64 Severity: medium From: FAZVM64FAZ-VM000101910 Trigger: Local Device Event	06/05/2018	--	06/05/2018	Kevin Gallagher	Respond	--	Active
2126	User Logon failed via SSH (medium event alert desc:Trim local db FAZVM64)	Subject: desc:Trim local db Device: FAZVM64 Severity: medium From: FAZVM64FAZ-VM000101910	06/05/2018	--	06/05/2018	Kevin Gallagher	Respond	--	Active

Notice that the Incident Name is populated by the Email Subject and a description of the Incident is included.

2129 User Logon failed via SSH
 (medium event alert
 desc:User login/logout failed
 FAZVM64)



Click on an Incident Name to view details.



Summary

ID 2129

Phase Respond

Severity —

Date Created 06/05/2018

Date Occur... —

Date Discov... 06/05/2018

Data Compr... Unknown

Incident Type —

People

Created By Kevin Gallagher

Owner Kevin Gallagher

Members There are no members.

Related Incidents

No related incidents.

Attachments

There are no attachments.

Description

Subject: desc:User login/logout failed

Device: FAZVM64

Severity: medium

From: FAZVM64(FAZ-VM0000101910)

Trigger: Local Device Event

Filter:

Log message:

```
log_id=0001010019 type=event subtype=system pri=alert desc="User login/logout failed" user="" ( :); echo Plugin output: $((1+' userfrom=telnet, msg="user ` ` ( :); echo Plugin output: $((1+' login failed from telnet(10.101.32.173)" userfrom="" msg="" adminprof="" devid=FAZ-VM0000101910 ltime=1528263225 date=2018-06-05 time=22:33:45
```

Tasks

0% Complete

Filter: All Selected Add Task

Task Name	Owner	Due Date	Flags	Actions
Respond				
Respond - (Data Breach - Organizational)				
investigate exposure of PI	Unassigned	No due date		

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.

FortiAnalyzer Administration Guide: <https://docs.fortinet.com/uploaded/files/4379/FortiAnalyzer-6.0.0-Administration-Guide.pdf>



www.fortinet.com