New Search

```
1  sourcetype=_json datasource=email direction=internal attachment!="None"
```

Last 24 hours

✓ **3 events** (12/13/25 5:00:00.000 AM to 12/14/25 5:23:13.000 AM)   No Event Sampling

Events (3)

Format Timeline

1 hour per column

SELECTED FIELDS

a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS

a attachment 1
a content 3
a datasource 1
a direction 1
a index 1
linecount 1
a punct 2
a recipient 2
a sender 2
a splunk_server 1
a subject 2
a timestamp 3

+ Extract New Fields (/en-US/app/search/field_extractor?sid=1765689793.252)

Time	Event
12/14/25 5:03:43.369 AM	{ [-] attachment: forceupdate.ps1 content: Michelle, here's the updated script. This version should work better - just run it when you get a chance. datasource: email direction: internal recipient: michelle.smith@tryhatme.com sender: yani.zubair@tryhatme.com subject: Force update fix timestamp: 12/14/2025 05:03:43.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:44:29.369 AM	{ [-] attachment: forceupdate.ps1 content: Thanks Yani! I'll run this script right away. The update issues have been really frustrating lately. datasource: email direction: internal recipient: yani.zubair@tryhatme.com sender: michelle.smith@tryhatme.com subject: RE: Force update fix timestamp: 12/14/2025 04:44:29.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time

12/14/25
4:23:34.369 AM

Event

```
{ [-]
   attachment: forceupdate.ps1
   content: Hey Michelle, can you run this PowerShell script to fix the update issue we discussed? It should resolve the problem with the automatic updates not working properly.
   datasource: email
   direction: internal
   recipient: michelle.smith@tryhatme.com
   sender: yani.zubair@tryhatme.com
   subject: Force update fix
   timestamp: 12/14/2025 04:23:34.369
}
```

Show as raw text

host = 10.10.106.238:8989 source = eventcollector sourcetype = _json