LogRhythm Proofpoint TAP API Integration Deployment and Configuration

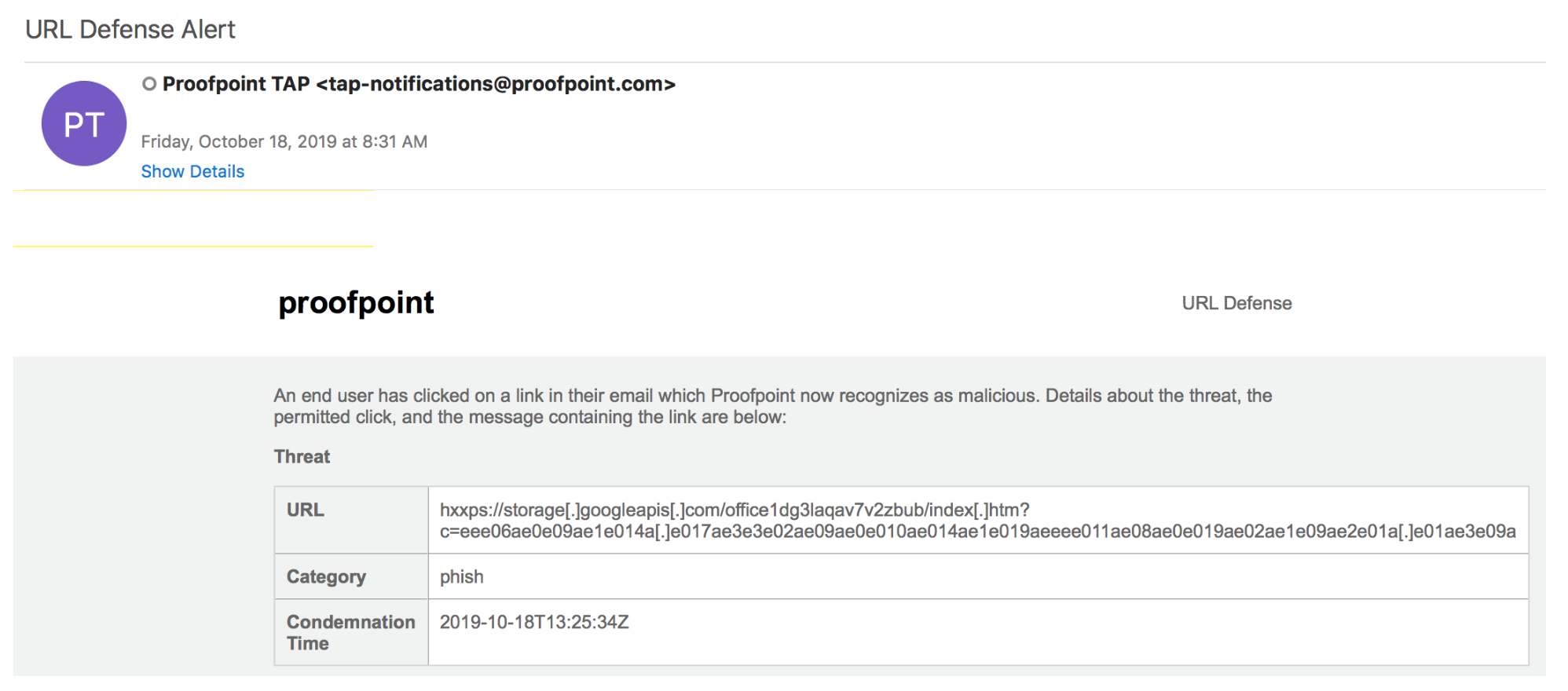
lr proofpoint tap

Issued:10/18/2019

## Configuring and Deploying LogRhythm Proofpoint TAP

#### Introduction

This integration is designed to integrate Proofpoint TAP with LogRhythm’s SIEM to help automate and reduce MTTR behind user impacted phishing incidents. Proofpoint TAP’s URL Defense Alerts indicate an user has clicked through a classified “phish” URL link, and this integration is meant to integrate alerting into a singular platform and shape automated SmartResponses or analyst procedures to help ensure that affected users are protected quicker.

****

#### Pre-Requisites

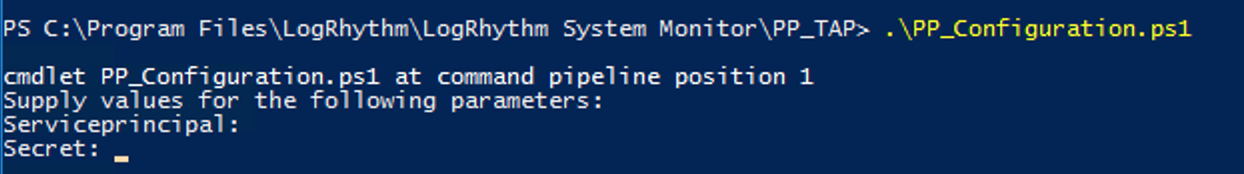
* OS: Windows Server 2016, Windows 2012 R2, Windows 2008
  + Powershell 3.0
  + 1 CPU; 4GB RAM
* Proofpoint TAP Read-Only Service Account
* PP\_TAP.ps1 and PP\_CONF.ps1
* Local administrator privileges on the Windows Server to make write/modifications to the LogRhythm Program Files directories and create Windows local scheduled tasks
  + Depending on the setup, LogRhythm Service Account is needed to have read/write/modify to the LogRhythm Program File directories
* LogRhythm Service Account credentials to set up the Windows local scheduled task
* Network connectivity to call against <https://tap-api-v2.proofpoint.com>

#### Configure the Proofpoint TAP Read-Only Account

Proofpoint TAP Service Credentials can be generated from the TAP Dashboard (Settings > Connected Applications). This requires a user with administrator privilege to generate these credentials. Upon generation, the service principal and secret must be exchanged to be used by the script.

#### Deploying and Configuring the LogRhythm ProofPoint TAP Integration

1. Create a directory within the LogRhythm System Monitor directory named PP\_TAP (C:\Program Files\LogRhythm\LogRhythm System Monitor\PP\_TAP\)
2. Create
3. Drop PP\_TAP.ps1 and PP\_Conf.ps1 into the new PP\_TAP directory
4. Open a Powershell window as the LogRhythm Service Account and run PP\_CONF.ps1
   1. Enter prompted Service Principal
   2. Enter prompted Secret



1. After generating PP\_TAP\_CONFIG.xml, execute PP\_TAP.ps1 (as the same user used o execute PP\_CONF.ps1), this will generate three directories in the \PP\_TAP\ directory: Log, Events, State)
   1. If necessary, create empty text files in child directories (these are meant to be auto-generated when PP\_TAP.ps1 runs and writes to disk)
      1. \PP\_TAP\Log\PP\_TAP.log
      2. \PP\_TAP\Events\PP\_TAP.txt
2. Open Task Scheduler on the Windows Server
3. Create task
   1. General
      1. Name: PP\_TAP
      2. When running the task, use the following account: <SERVICEACCOUNT>
      3. Run whether user is logged in or not
         1. Do not store password. The task will only have access to local computer resources.
      4. Run with highest privileges
      5. Configure for: Windows 7, Windows Server 2008
   2. Triggers
      1. Begin the task On a schedule
      2. Daily
      3. Recur every 1 days
      4. Repeat task every: 10 minutes for the duration of: 1 day
      5. Enabled
   3. Actions
      1. Start a program
      2. Program/script:

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

1. Add Arguments (optional):

-ExecutionPolicy Bypass -File "C:\Program Files\LogRhythm\LogRhythm System Monitor\PP\_TAP\PP\_TAP.ps1"

* 1. Settings
     1. Allow task to be run on demand
     2. Stop the task if it runs for more than: 3 days
     3. If the running task does not end when requested, force it to stop

1. Confirm that the Scheduled Task/PP\_TAP.ps1 is working as intended as it will write and debug to "C:\Program Files\LogRhythm\LogRhythm System Monitor\PP\_TAP\Log\PP\_TAP.log". Content from the log file should be similar to below. In the provided example, the script was able to successfully query the API using the credentials stored and no content was returned (HTTP 204) at the time the script was executed.

"22-Oct-2019 14:20:01.825","Information","State file C:\Program Files\LogRhythm\LogRhythm System Monitor\PP\_TAP\State\PP\_TAP.pos exists."

"22-Oct-2019 14:20:01.841","Information","Requesting PP\_TAP logs from 600 seconds ago"

"22-Oct-2019 14:20:01.857","Information","Calling AMP4EP API: https://tap-api-v2.proofpoint.com/v2/siem/clicks/permitted?format=syslog&sinceSeconds=600"

"22-Oct-2019 14:20:04.062","Information","Returned 204"

"22-Oct-2019 14:20:04.062","Information","No available content within 600seconds"

1. Navigate to the LogRhythm Console on the Platform Manager
2. Create a LogRhythm Source Type in the LogRhythm Deployment Manager (Deployment Manager > Knowledge > Log Source Type Manager)
   1. New Log Source Type
      1. Name: API - Proofpoint TAP
      2. Full Name: API - Proofpoint TAP
      3. Abbreviation: API - Proofpoint TAP
      4. Log Format: Text File
      5. Brief Description: TAP SIEM API
3. Create a Log Processing Policy (Deployment Manager > Log Processing Policy)
   1. Right click to create a new log processing policy
      1. Name: API - Proofpoint TAP
4. Add a new MPE Processing Rule (Deployment Manager > Knowledge > MPE Rule Builder)
   1. Rule Name: CLKPER Event
   2. Common Event: Phishing Activity
   3. Rule Status: Production
   4. Base-rule regular expression:

CLKPER.\*?recipient=\"(?<login>(?<login>[^@]+)@(?<domainorigin>[^"]+)|[^\"]+)?\"\s+sender=\"(?<object>(?<object>(?<account>[^@]+)@(?<domain>[^\"]+))|[^\"]+)?\"\s+senderIP=\"(?<sip>(?<sip>\d+\.\d+\.\d+\.\d+)|[^\"]+)?\".\*?url=\"(?<url>[^\"]+)\".\*clickIP=\"(?<dip>(?<dip>\d+\.\d+\.\d+\.\d+)|[^\"]+)?\".\*userAgent=\"(?<useragent>.\*?)\]

* 1. Select Custom Log Source Type: Proofpoint Tap
  2. Save the MPE Rule

1. Add a new MPE Processing Rule (Deployment Manager > Knowledge > MPE Rule Builder)
   1. Rule Name: MSGDLV Event
   2. Common Event: Phishing Activity
   3. Rule Status: Production
   4. Base-rule regular expression:

MSGDLV.\*?recipient=\"(?<login>(?<login>[^@]+)@(?<domainorigin>[^"]+)|[^\"]+)?\"\s+sender=\"(?<object>(?<object>(?<account>[^@]+)@(?<domain>[^\"]+))|[^\"]+)?\"\s+senderIP=\"(?<sip>(?<sip>\d+\.\d+\.\d+\.\d+)|[^\"]+)?\".\*?threatsInfoMap="\[{(?:\\"[^"]+\":\\"[^"]+\",){5}\\\"threat\\\":\\\"(?<url>[^\\]+)\\.\*?subject="(?<subject>[^"]+)".\*?completelyRewritten="(?<command>[^"]+)\".\*?messageParts=\"(?<vendorinfo>.\*?md5\\":\\"(?<hash>[^\\]+)\\"[^\"]+\"filename\\\":\\\"(?<object>[^\\]+).\*})\\]

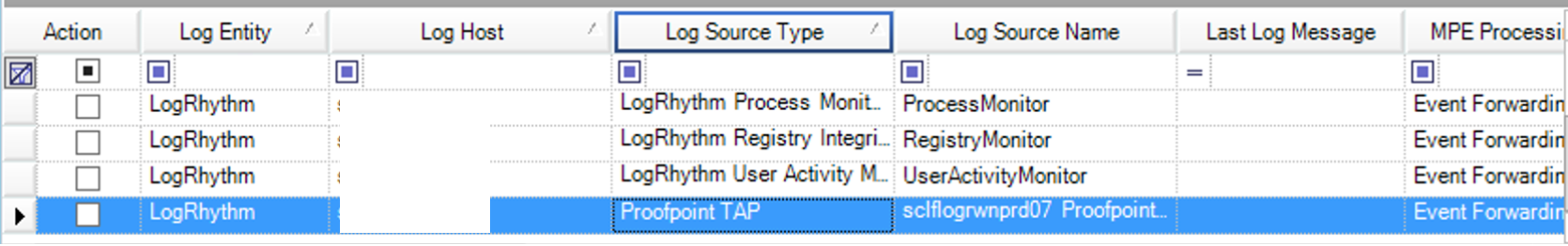
* 1. Select Custom Log Source Type: Proofpoint Tap
  2. Save the MPE Rule

1. Add a base catch-all MPE Processing Rule (Deployment Manager > Knowledge > MPE Rule Builder)
   1. Rule Name: Proofpoint CatchAll lvl 1
   2. Common Event: Phishing Activity
   3. Rule Status: Production
   4. Base-rule regular expression:

^.\*

* 1. Select Custom Log Source Type: Proofpoint Tap
  2. Save the MPE Rule

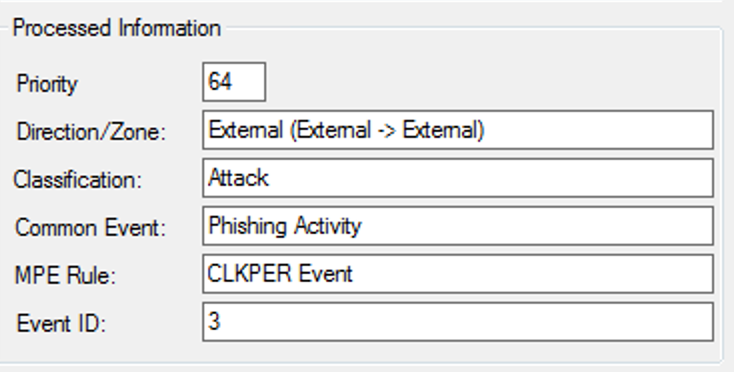
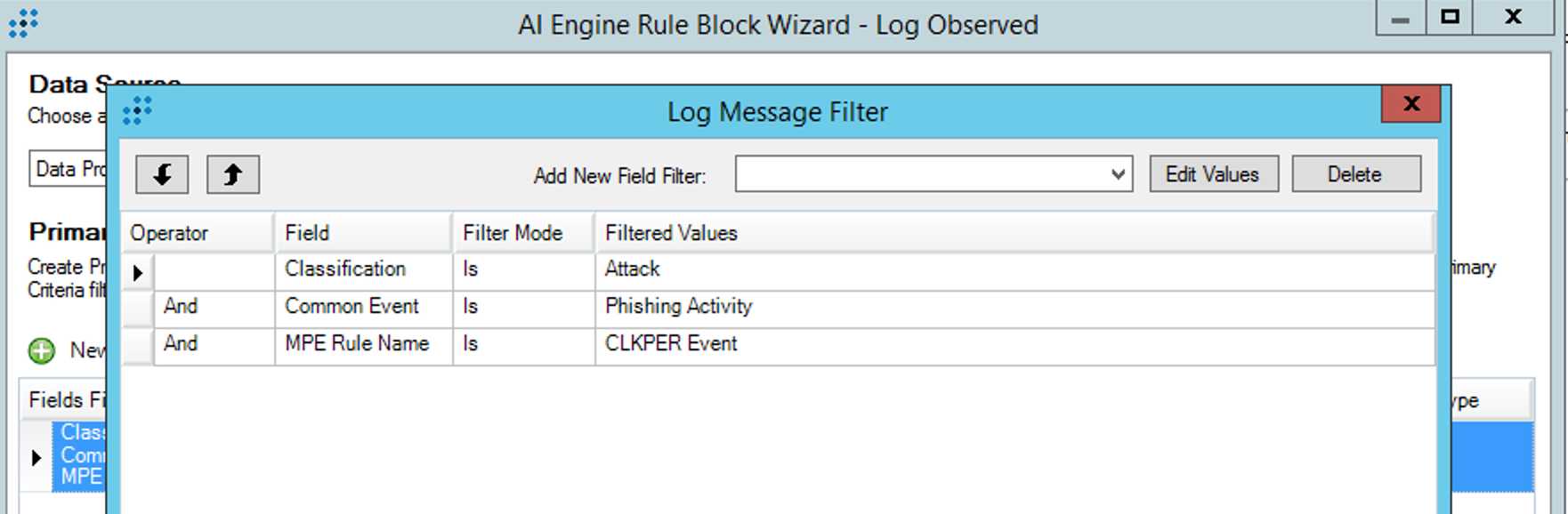
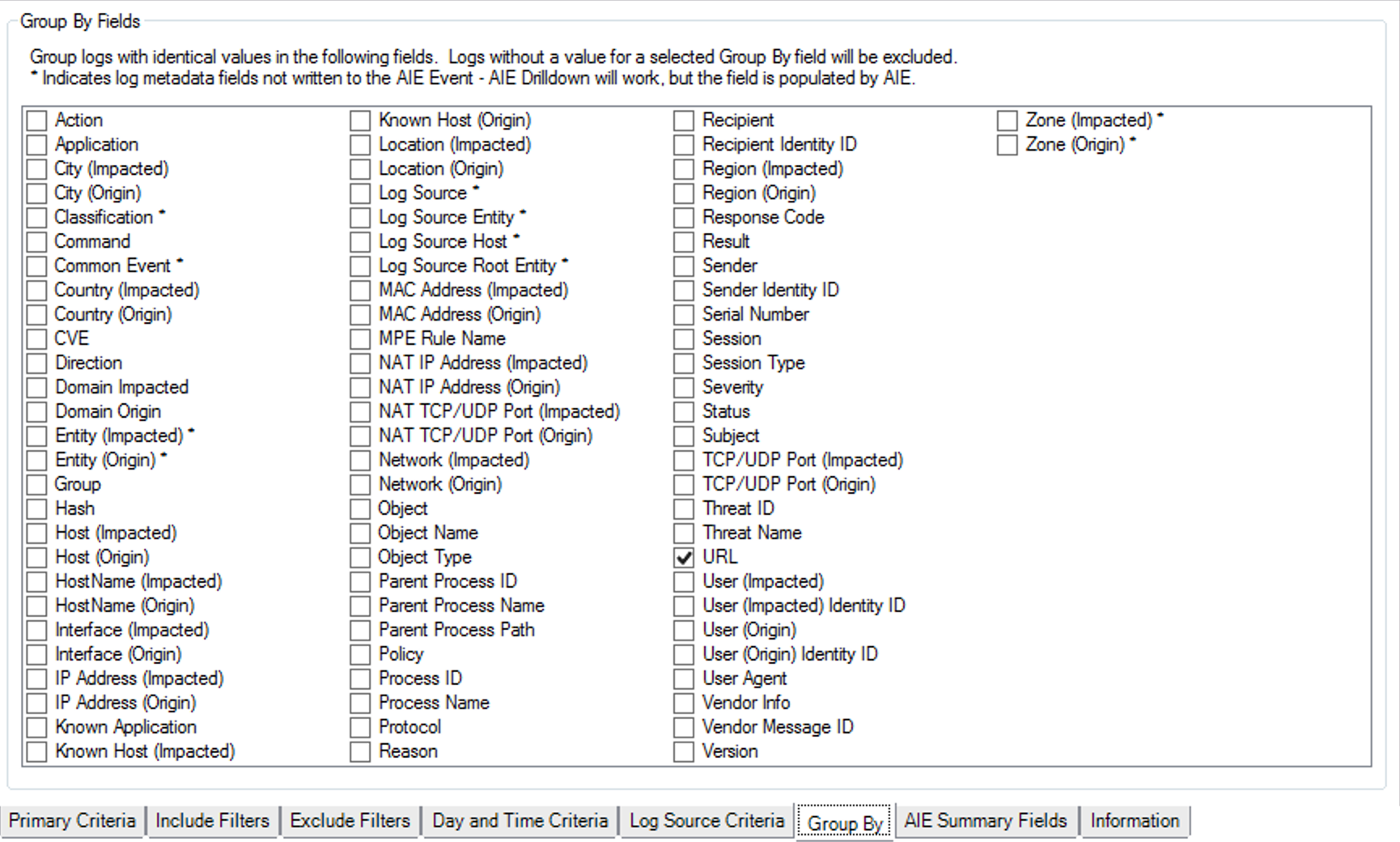
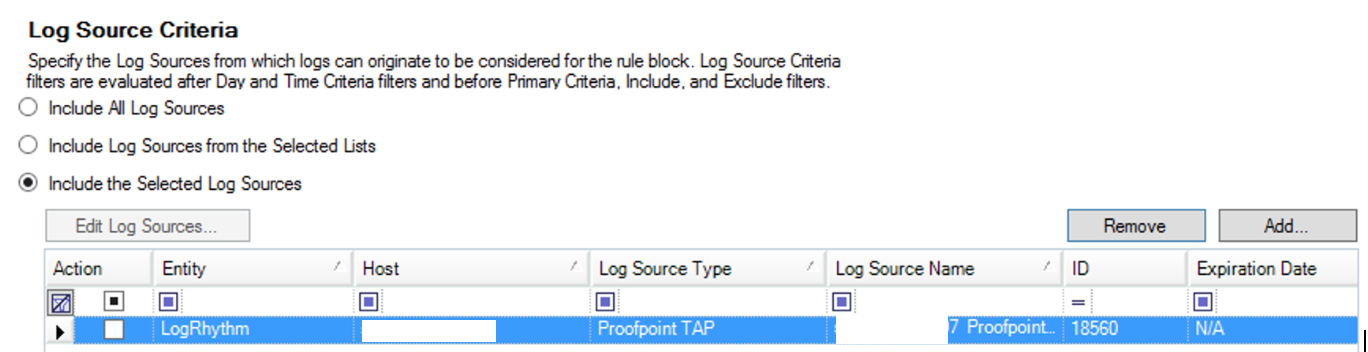
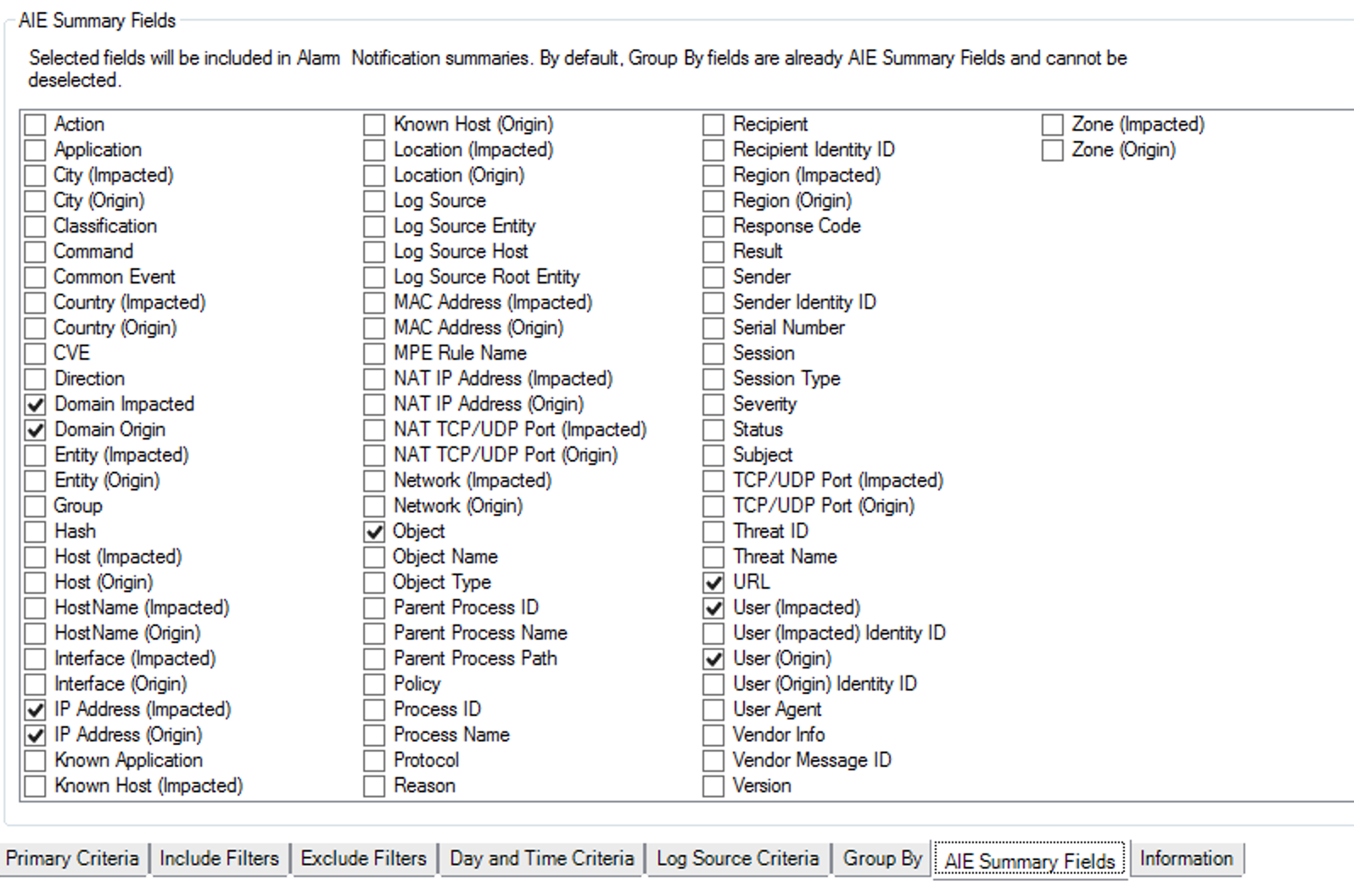
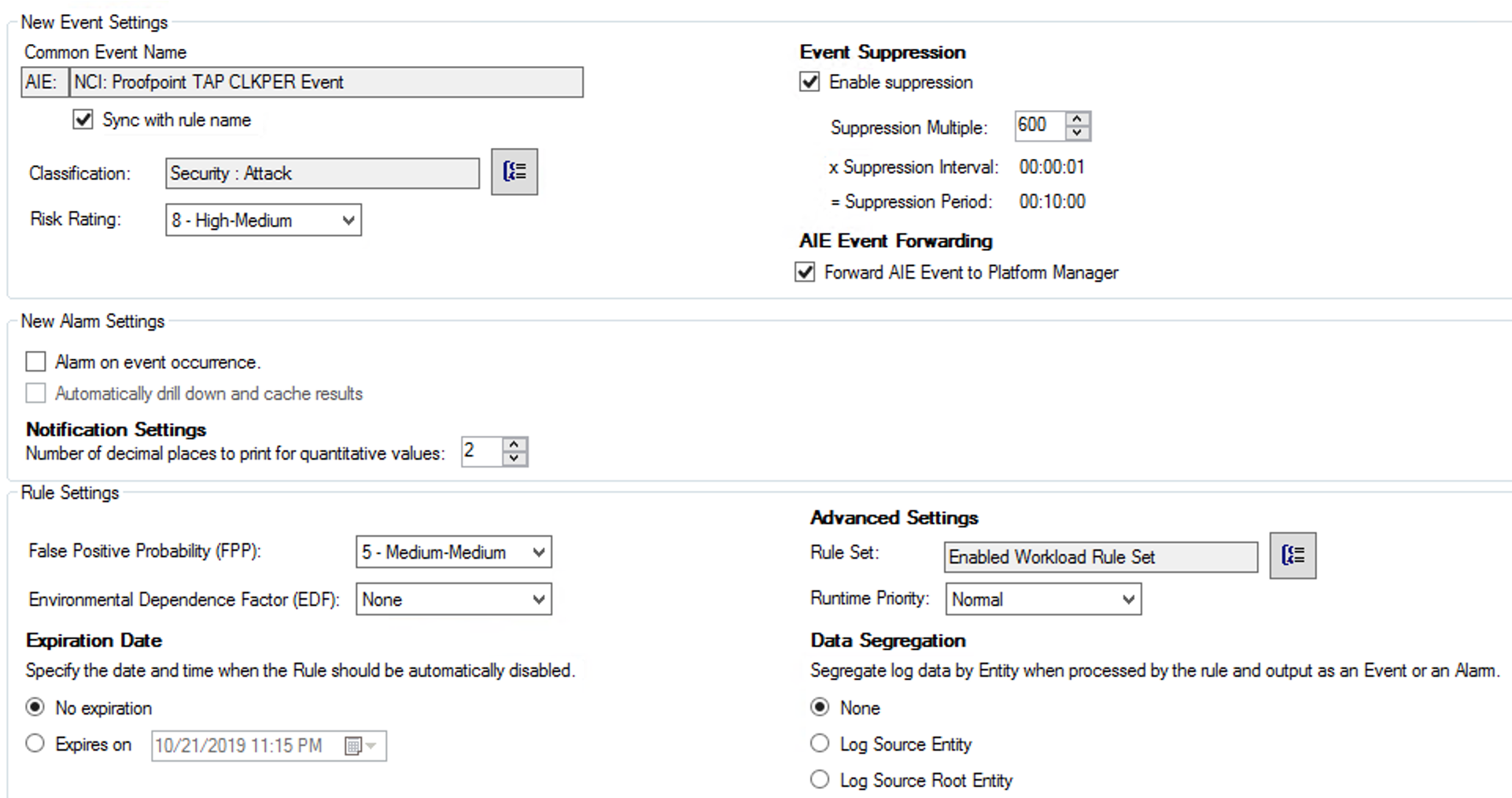
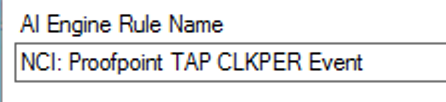
1. Enable the two new MPE Rule within the Proofpoint TAP Log Processing Policy (Deployment Manager > Log Processing Policy)
   1. Open the Proofpoint TAP processing policy
   2. Select the CLKPER and Proofpoint CatchAll rules
   3. Enable the rules
2. Create a new log source from the system monitor agent where the PP\_TAP directory was installed (Deployment Manager > System Monitor Agents > Properties of Agent)
3. Edit the Log Message Source Properties
   1. Basic Configuration
      1. Log Message Source Type: Proofpoint TAP
      2. Log Message Source Name: foobarhostname Proofpoint TAP
      3. Log Message Processing Mode: MPE Processing Enabled, Event Forwarding Enabled
      4. Log Message Processing Engine (MPE) Policy: Proofpoint TAP
      5. Do not Forward Logs to LogRhythm LogMart
   2. Flat File Settings
      1. File Path: C:\Program Files\LogRhythm\LogRhythm System Monitor\PP\_TAP\Events\PP\_TAP.txt
      2. Date Parsing Format: Proofpoint TAP
         1. Click the […] to open the Date Format Manager
         2. Right click the window to create a New Date Format
            1. Name: Proofpoint TAP
            2. Regex: <UTC><yy>-<M>-<d>T<h>:<m>:<s>Z



#### Creating AIE Alarms with Proofpoint TAP CLKPER Events

1. Once a URL Defense Alert is generated within Proofpoint TAP, an event log will be collected by LogRhythm. Sample log:

<33>1 2019-10-01T14:07:00Z - ProofpointTAP - CLKPER [tapclk@21139 clickTime="2019-10-01T14:07:00Z" threatTime="2019-10-01T14:14:06Z" class="phish" recipient="foo.bar@domain.com" sender="rita.geehan@optimityadvisors.com" senderIP="40.107.81.108" GUID="Lr3-D1MXBjADWDE7iDIOb1awdaqeT4" url="https://parksidetiles-my.sharepoint.com/:o:/g/personal/e\_tuttlebury\_parkside\_co\_uk/EgX9faiUAE9MsrG6TYUMFLcBGXhZ4HxaIy\_Oyl28He-JrQ?e=9j9PtV" threatURL="https://threatinsight.proofpoint.com/URLID" threatID="THREATID" threatStatus="active" clickIP="20.15.105.8" campaignID="null" messageID="<C13E8B9F-F89B-4EE0-AC66-B05C20014CCD@optimityadvisors.com>" userAgent="Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36"]

1. After parsing LogRhythm will generate a log classified as an “Attack” with a “Phishing Attack”. 
2. Set up a new LogRhythm AIE Alarm with a Log Observed Block:
   1. 
   2.  
   3. 
   4. 
   5. 
3. Basic Analyst Workflow:
   1. Alert is generated
   2. Analyst checks Proofpoint URL to determine vector against OSINT tools
   3. Analyst checks if other users have been affected
   4. Analyst queries against SIEM for enrichment regarding if URL/IP is blocked or not
   5. If not false positive, Analyst generates ServiceNow ticket/emails team regarding password expiry of affected user

A close up of a logo

Description automatically generated

#### Sample AIE Alarm(s) with Proofpoint TAP EventsA screenshot of a social media post Description automatically generated

**Sample Log Types (CLKPER, MSGDLV):**

<33>1 2019-10-01T14:07:00Z - ProofpointTAP - CLKPER [tapclk@21139 clickTime="2019-10-01T14:07:00Z" threatTime="2019-10-01T14:14:06Z" class="phish" recipient="foo.bar@domain.com" sender="rita.geehan@optimityadvisors.com" senderIP="40.107.81.108" GUID="Lr3-D1MXBjADWDE7iDIOb1awdaqeT4" url="https://parksidetiles-my.sharepoint.com/:o:/g/personal/e\_tuttlebury\_parkside\_co\_uk/EgX9faiUAE9MsrG6TYUMFLcBGXhZ4HxaIy\_Oyl28He-JrQ?e=9j9PtV" threatURL="https://threatinsight.proofpoint.com/URLID" threatID="THREATID" threatStatus="active" clickIP="20.15.105.8" campaignID="null" messageID="<C13E8B9F-F89B-4EE0-AC66-B05C20014CCD@optimityadvisors.com>" userAgent="Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36"]

<36>1 2020-02-21T00:24:18Z - ProofpointTAP - MSGDLV [tapmsg@21139 messageTime="2020-02-21T00:24:18Z" messageID="<20200220162327.B43691E0BCB92B56@dentalartsdsm.com>" recipient="kmei@foobar.org" sender="irs@dentalartsdsm.com" senderIP="23.235.214.214" phishScore="0" spamScore="0" QID="01L0L7H4021636" GUID="LkEaab8nYQ-MubHzEe5Nn\_Yi4s7jUXJD" threatsInfoMap="[{\"threatID\":\"f9ff6ca893f4d9bbbccefe4350d4fca2e445a4a7132b8ae40508f3c45c14d6f4\",\"threatStatus\":\"active\",\"classification\":\"malware\",\"threatUrl\":\"https://threatinsight.proofpoint.com/b822df0a-fae5-70d8-7bcd-30d1fbdf83c7/threat/email/f9ff6ca893f4d9bbbccefe4350d4fca2e445a4a7132b8ae40508f3c45c14d6f4\",\"threatTime\":\"2020-02-21T04:34:24.000Z\",\"threat\":\"f9ff6ca893f4d9bbbccefe4350d4fca2e445a4a7132b8ae40508f3c45c14d6f4\",\"campaignID\":null,\"threatType\":\"attachment\"}\]" malwareScore="0" impostorScore="0.0" cluster="customer\_hosted" subject="Tax Exemption Status" quarantineFolder="null" quarantineRule="null" policyRoutes="default\_inbound,TAP" modulesRun="access,smtpsrv,av,zerohour,spf,dkimv,sandbox,spam,dmarc,pdr,batv,urldefense" messageSize="268245" headerFrom="Internal Revenue Service <irs@dentalartsdsm.com>" headerReplyTo="info@sawchukbrown.co" fromAddress="irs@dentalartsdsm.com" toAddresses="kmei@foobar.org" ccAddresses="null" replyToAddress="info@sawchukbrown.co" xmailer="null" completelyRewritten="false" messageParts="[{\"disposition\":\"attached\",\"sha256\":\"f93075c1a337e2d717335e7e0e80b4401d771d4e9bcbfe8a2d26071f1e469fb4\",\"md5\":\"095b144ae553604a251f3bcab57b4917\",\"filename\":\"download.png\",\"sandboxStatus\":\"NOT\_SUPPORTED\",\"oContentType\":\"image/png\",\"contentType\":\"image/png\"},{\"disposition\":\"attached\",\"sha256\":\"f9ff6ca893f4d9bbbccefe4350d4fca2e445a4a7132b8ae40508f3c45c14d6f4\",\"md5\":\"be66ed937dcdd2e2e6352734ce043007\",\"filename\":\"w-8ben.pdf\",\"sandboxStatus\":\"CLEAN\",\"oContentType\":\"application/pdf\",\"contentType\":\"application/pdf\"},{\"disposition\":\"inline\",\"sha256\":\"2f6eb066ab0edcaa28589d2b7f44034195230380467f100274bf1e6fab870001\",\"md5\":\"89824f7c4ed6b8aad321b939dce51efe\",\"filename\":\"text.html\",\"sandboxStatus\":\"NOT\_SUPPORTED\",\"oContentType\":\"text/html\",\"contentType\":\"text/html\"}\]"]