

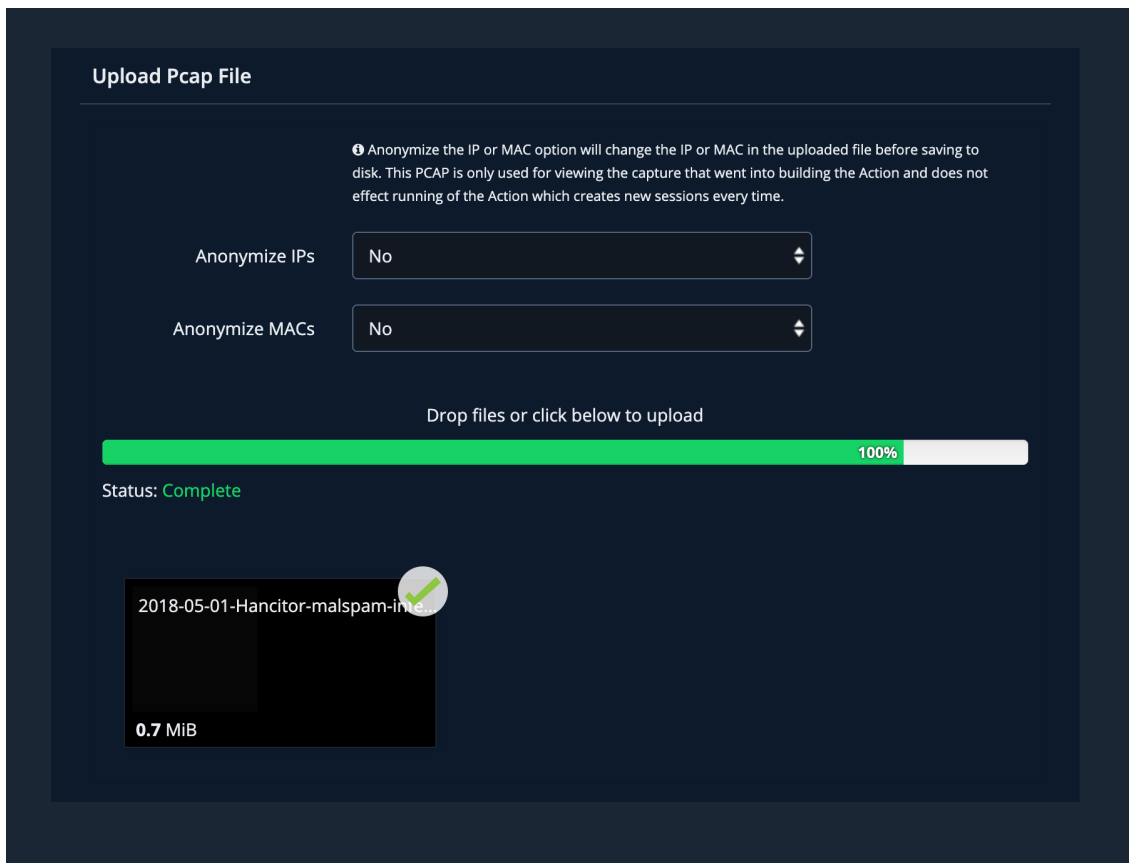


ADDING ACTIONS FROM PACKET CAPTURE

 **NOTE:** All PCAP files should be supported. If you have issues with a PCAP file, submit a support ticket.

1. Go to **Library > Actions**.
2. Select **Add Action > From PCAP**. The Upload PCAP File page comes up.
3. Before uploading your PCAP file, determine if the IP and MAC addresses should be anonymized. You may choose to do this if you don't want to use your network information in an Action.
 - a. If you want to anonymize IP addresses in the PCAP file, select **Yes**.
 - b. If you want to anonymize MACs in the PCAP file, select **Yes**.
4. Add a PCAP (.pcap) file. The platform will automatically advance to the next page after the upload completes.

 **NOTE:** A progress bar that includes an estimated time remaining is displayed to show how the PCAP import is progressing.



Uploading a PCAP file

5. The **Add PCAP Action Step 2** page appears.
The platform analyzes the PCAP and identifies conversations. It automatically displays feedback regarding issues with the PCAP that must be resolved.



- Actions can only contain TCP or UDP traffic, not both. Actions can only have 2 unique IP Addresses.
- If you use **Back to Upload PCAP** or exit this screen without using one of the buttons, your PCAP will stay in the system.

← Back to Upload PCAP
Next Cancel Packet View

Create Action -- 2018-05-01-Hancitor-malspam-infection-traffic.pcap

⚠ Warning! Action is not yet saved.

✔ Removed non-TCP and non-UDP packets from the pcap file.

✔ Stripped VLAN Tags.

⚠ Actions can only include either TCP or UDP traffic. Update the conversations below as appropriate. If you need to execute both TCP & UDP traffic, create separate Actions and add both to a Sequence.

⚠ Actions may only have two unique IP Addresses.

Remove TCP Remove UDP Remove Selected Conversations (25)

<input checked="" type="checkbox"/>	Timestamp ↑	IP1 ↓	IP2 ↓	Proto ↓	App ↓	Port1 ↓	Port2 ↓	Data ↓	Details ↓
<input checked="" type="checkbox"/>	2018-05-01 14:50:18 UTC	192.168.55.231	35.187.117.14	TCP	HTTP	49174	80	271 KB	gamification4you.com - GET Yp5uh16=RBDWGVYUQYQC
<input checked="" type="checkbox"/>	2018-05-01 14:53:23 UTC	192.168.55.231	146.120.110.14	TCP	SSL	49184	443	1.54 KB	
<input checked="" type="checkbox"/>	2018-05-01 14:53:24 UTC	192.168.55.231	146.120.110.14	TCP	SSL	49186	443	8.24 KB	
<input checked="" type="checkbox"/>	2018-05-01 14:53:26 UTC	192.168.55.231	146.120.110.14	TCP	SSL	49188	443	13.7 KB	
<input checked="" type="checkbox"/>	2018-05-01 14:53:26 UTC	192.168.55.231	146.120.110.14	TCP	SSL	49187	443	1.57 KB	
<input checked="" type="checkbox"/>	2018-05-01 14:58:28 UTC	192.168.55.231	146.120.110.14	TCP	SSL	49191	443	1.57 KB	
<input checked="" type="checkbox"/>	2018-05-01 14:58:29 UTC	192.168.55.231	146.120.110.14	TCP	SSL	49193	443	3.27 KB	
<input checked="" type="checkbox"/>	2018-05-01 14:58:31 UTC	192.168.55.231	146.120.110.14	TCP	SSL	49195	443	3.25 KB	
<input checked="" type="checkbox"/>	2018-05-01 14:58:31 UTC	192.168.55.231	146.120.110.14	TCP	SSL	49194	443	1.57 KB	
<input checked="" type="checkbox"/>	2018-05-01 15:03:23 UTC	192.168.55.231	146.120.110.14	TCP	SSL	49199	443	1.57 KB	

⏪ 1 to 10 of 50 rows ⏩ Rows Per Page: 10

PCAP upload feedback

6. Remove Conversations as necessary.

- a. (Optional) Select one or more conversations and click **Remove Conversations**.



NOTE: This button only appears when conversations are selected.



TIP: You can select conversations across pages. This includes selecting a conversation on one page, using the page arrows to advanced to another page, and then Shift +clicking on a conversation to select all conversations in between.

- b. (Optional) Select **Remove TCP** or **Remove UDP** to remove all conversations of that type.

7. (Optional) Click **Packet View** to view remaining packets.



NOTE: When viewing PCAP (Packet View) in MA-SV, you will see rows of gray alternately, not the color scheme available in MSV.

Enter Display Filter Here				<input checked="" type="checkbox"/> TCP	<input checked="" type="checkbox"/> UDP	<input checked="" type="checkbox"/> HTTP	Include all IPs	Test.pcap 20.8 KB - 34 packets
1	0.000000	145.254.160.237	65.208.228.223	TCP	62	tip2 > http [SYN] Seq=0 Win=8760 Len=0 MSS=1460 SACK_PEF		
2	0.911310	65.208.228.223	145.254.160.237	TCP	62	http > tip2 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=13		
3	0.911310	145.254.160.237	65.208.228.223	TCP	54	tip2 > http [ACK] Seq=1 Ack=1 Win=9660 Len=0		
4	0.911310	145.254.160.237	65.208.228.223	HTTP	533	GET /download.html HTTP/1.1		
5	1.472116	65.208.228.223	145.254.160.237	TCP	54	http > tip2 [ACK] Seq=1 Ack=480 Win=6432 Len=0		
6	1.682419	65.208.228.223	145.254.160.237	TCP	1434	[TCP segment of a reassembled PDU]		
7	1.812606	145.254.160.237	65.208.228.223	TCP	54	tip2 > http [ACK] Seq=480 Ack=1381 Win=9660 Len=0		
8	1.812606	65.208.228.223	145.254.160.237	TCP	1434	[TCP segment of a reassembled PDU]		
9	2.012894	145.254.160.237	65.208.228.223	TCP	54	tip2 > http [ACK] Seq=480 Ack=2761 Win=9660 Len=0		
10	2.443513	65.208.228.223	145.254.160.237	TCP	1434	[TCP segment of a reassembled PDU]		
11	2.553672	65.208.228.223	145.254.160.237	TCP	1434	[TCP segment of a reassembled PDU]		
12	2.553672	145.254.160.237	65.208.228.223	TCP	54	tip2 > http [ACK] Seq=480 Ack=5521 Win=9660 Len=0		
13	2.633787	65.208.228.223	145.254.160.237	TCP	1434	[TCP segment of a reassembled PDU]		
14	2.814046	145.254.160.237	65.208.228.223	TCP	54	tip2 > http [ACK] Seq=480 Ack=6901 Win=9660 Len=0		
15	2.894161	65.208.228.223	145.254.160.237	TCP	1434	[TCP segment of a reassembled PDU]		
16	3.014334	145.254.160.237	65.208.228.223	TCP	54	tip2 > http [ACK] Seq=480 Ack=8281 Win=9660 Len=0		
17	3.374852	65.208.228.223	145.254.160.237	TCP	1434	[TCP segment of a reassembled PDU]		
18	3.495025	65.208.228.223	145.254.160.237	TCP	1434	[TCP segment of a reassembled PDU]		
19	3.495025	145.254.160.237	65.208.228.223	TCP	54	tip2 > http [ACK] Seq=480 Ack=11041 Win=9660 Len=0		
20	3.635227	65.208.228.223	145.254.160.237	TCP	1434	[TCP segment of a reassembled PDU]		
21	3.815486	145.254.160.237	65.208.228.223	TCP	54	tip2 > http [ACK] Seq=480 Ack=12421 Win=9660 Len=0		
22	4.105904	65.208.228.223	145.254.160.237	TCP	1434	[TCP segment of a reassembled PDU]		
23	4.216062	145.254.160.237	65.208.228.223	TCP	54	tip2 > http [ACK] Seq=480 Ack=13801 Win=9660 Len=0		
24	4.226076	65.208.228.223	145.254.160.237	TCP	1434	[TCP segment of a reassembled PDU]		

▶ Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
 ▶ Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
 ▶ Internet Protocol Version 4, Src: 145.254.160.237 (145.254.160.237), Dst: 65.208.228.223 (65.208.228.223)
 ▶ Transmission Control Protocol, Src Port: tip2 (3372), Dst Port: http (80), Seq: 0, Len: 0

```

0000 fe ff 20 00 01 00 00 00 01 00 00 00 08 00 45 00  .. .....E.
0010 00 30 0f 41 40 00 80 06 91 eb 91 fe a0 ed 41 d0  .0.A@.....A.
0020 e4 df 0d 2c 00 50 38 af fe 13 00 00 00 00 70 02  ....P8.....p.
0030 22 38 c3 0c 00 00 02 04 05 b4 01 01 04 02     *8.....
  
```

Adding Actions from packet

8. When all errors have been resolved, you will see the Originator IP and the Treat all traffic as valid HTTP whether it is or not fields. Make your desired selections and click **Next**.
 - a. Originator IP: Choose which of the two IP Addresses the traffic should come from
 - b. Treat all traffic as valid HTTP whether it is or not: This is only used when you know the HTTP traffic is intentionally not in a valid format. If you use this option, there is a high chance the traffic will be blocked by a proxy.

← Back to Upload PCAP
Next Cancel Packet View

Create Action -- 2018-05-01-Hancitor-malspam-infection-traffic.pcap

⚠ Warning! Action is not yet saved.

✔ Removed non-TCP and non-UDP packets from the pcap file.

✔ Stripped VLAN Tags.

Originator IP *

Destination IP *

Treat all traffic as valid HTTP whether it is or not

Conversations

■	Timestamp ↑	IP1 ↓	IP2 ↓	Proto ↓	App ↓	Port1 ↓	Port2 ↓	Data ↓	Details ↓
■	2018-05-01 14:51:13 UTC	192.168.55.231	185.220.33.217	TCP	HTTP	49179	80	1.84 KB	supratparfa.com - POST /4/forum.php
■	2018-05-01 14:51:20 UTC	192.168.55.231	185.220.33.217	TCP	HTTP	49181	80	799 Bytes	supratparfa.com - POST /mlu/forum.php
■	2018-05-01 14:51:22 UTC	192.168.55.231	185.220.33.217	TCP	HTTP	49182	80	806 Bytes	supratparfa.com - POST /d2/about.php
■	2018-05-01 14:53:22 UTC	192.168.55.231	185.220.33.217	TCP	HTTP	49183	80	574 Bytes	supratparfa.com - POST /4/forum.php
■	2018-05-01 14:55:23 UTC	192.168.55.231	185.220.33.217	TCP	HTTP	49189	80	574 Bytes	supratparfa.com - POST /4/forum.php
■	2018-05-01 14:57:23 UTC	192.168.55.231	185.220.33.217	TCP	HTTP	49190	80	574 Bytes	supratparfa.com - POST /4/forum.php
■	2018-05-01 14:59:24 UTC	192.168.55.231	185.220.33.217	TCP	HTTP	49196	80	574 Bytes	supratparfa.com - POST /4/forum.php
■	2018-05-01 15:01:24 UTC	192.168.55.231	185.220.33.217	TCP	HTTP	49197	80	574 Bytes	supratparfa.com - POST /4/forum.php
■	2018-05-01 15:03:25 UTC	192.168.55.231	185.220.33.217	TCP	HTTP	49202	80	574 Bytes	supratparfa.com - POST /4/forum.php
■	2018-05-01 15:05:25 UTC	192.168.55.231	185.220.33.217	TCP	HTTP	49207	80	574 Bytes	supratparfa.com - POST /4/forum.php

⏪ 1 to 10 of 15 rows ⏩ Rows Per Page: 10

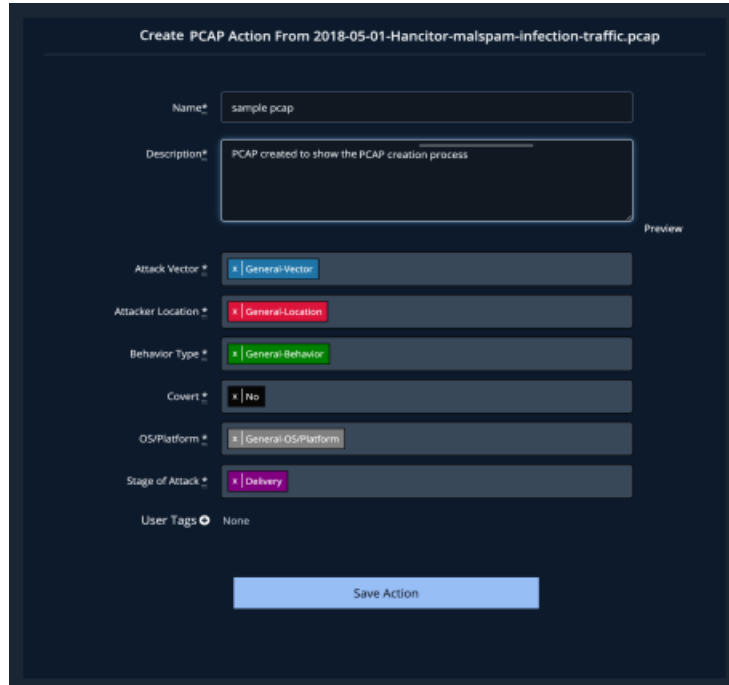
Errors resolved in PCAP upload

9. Complete the applicable Dimensions presented and click **Save Action**.

The Action Library displays. A confirmation message that your Action was created successfully is shown and the Action is selected and displayed in the Action preview.



NOTE: If you click Cancel during the creation process, the Action will not be created.



Create PCAP Action From 2018-05-01-Hancitor-malspam-infection-traffic.pcap

Name* sample pcap

Description* PCAP created to show the PCAP creation process

Attack Vector* General-Vector

Attacker Location* General-Location

Behavior Type* General-Behavior

Covert* No

OS/Platform* General-OS/Platform

Stage of Attack* Delivery

User Tags None

Save Action

Complete Dimension selections

HTTP Headers for Hex Actions

The Validation Platform includes a global setting, **Hex Actions - Update Host in HTTP Header**. This allows you to configure the platform so the host is always or never replaced when running Actions. However, to demonstrate specific behavior, such as demonstrating Header Spoofing techniques or leveraging web services as C2s, you may need the Action to run the opposite of the global setting. To support this, there is a **Update Host in HTTP Header** runtime parameter. This defaults to the global setting but can be modified. We recommend you add a note in the Action's description if the Action requires a specific setting for that parameter.