Cynet

AUTONOMOUS BREACH PROTECTION

CUSTOM REMEDIATION

Block IP via Windows Firewall

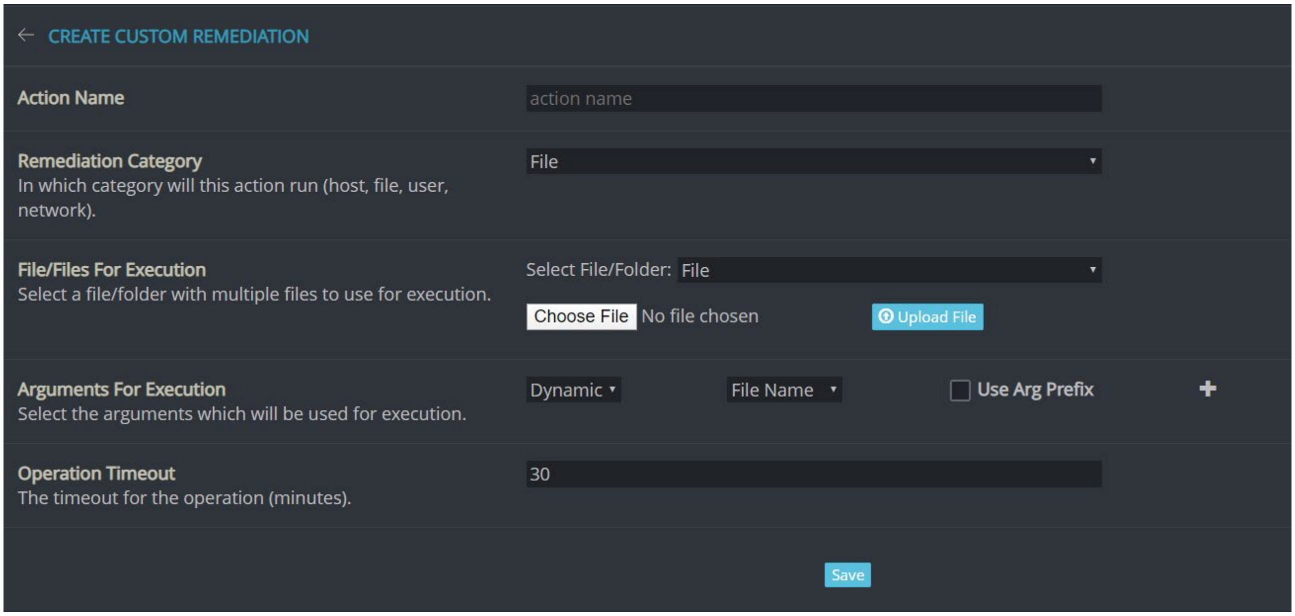
CUSTOM REMEDIATION

Custom Remediation is a great feature which allows us to take variables from an alert (such as process name, process path, process hash, domain, host, etc..) and use them in a custom made script, in order to execute the script itself on the alerted host.

USAGE EXAMPLE

To demonstrate the capabilities of the custom remediation feature, we'll create a custom remediation action that will take an IP Address as a variable from an alert in order to block it in Windows Firewall (Windows firewall can except only IP Addresses, not domain names).

Enter Cynet's console → Settings → REMEDIATION → Create



← CREATE CUSTOM REMEDIATION

Action Name — action name

Remediation Category — File
In which category will this action run (host, file, user, network).

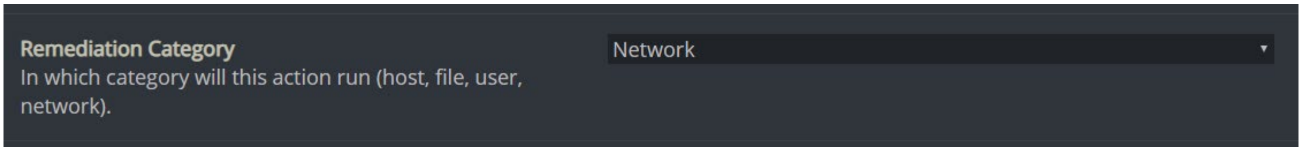
File/Files For Execution — Select File/Folder: File
Select a file/folder with multiple files to use for execution.
Choose File No file chosen — Upload File

Arguments For Execution — Dynamic ▾ — File Name ▾ — □ Use Arg Prefix — ✚
Select the arguments which will be used for execution.

Operation Timeout — 30
The timeout for the operation (minutes).

Save

After filling in an Action Name (for this example "echofirewall"), for Remediation Category select "Network" for network alert:

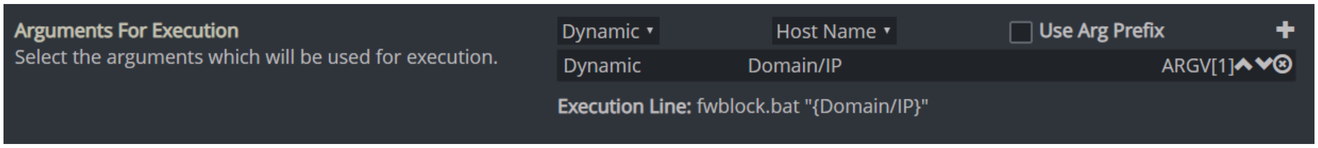


Remediation Category — Network ▾
In which category will this action run (host, file, user, network).

Under “File/Files For Execution” we’ll upload our script (in our case, we’ll create a new “.bat” script and fill in the script bellow), as you can see %1 will be taken as a variable from the alert, representing the malicious domain:

```
echo off
netsh advfirewall firewall add rule name=”%1 Blocking” remoteip=%1 dir=out enable=yes action=block
```

We can use Dynamic or Static arguments for executions, in our case we want to take the “Domain/IP” as dynamic arguments from the alert that will be represented as %1 in our script:



Arguments For Execution
Select the arguments which will be used for execution.

Dynamic ▾ | Host Name ▾ | □ Use Arg Prefix ✚

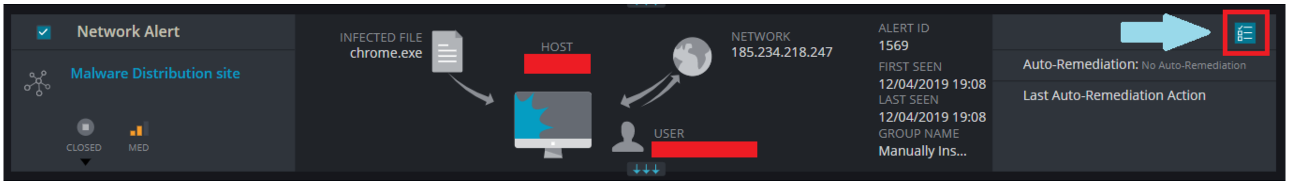
Dynamic | Domain/IP | ARGV[1]

Execution Line: fwblock.bat "{Domain/IP}"

Press “Save”.

APPLY CUSTOM REMEDIATION

In order to use the custom remediation rule we’ve created, we’ll find a network alert such as “Malware Distribution Site”, and press the “Action” button:



☑ Network Alert

Malware Distribution site

CLOSED | MED

INFECTED FILE chrome.exe

HOST [redacted]

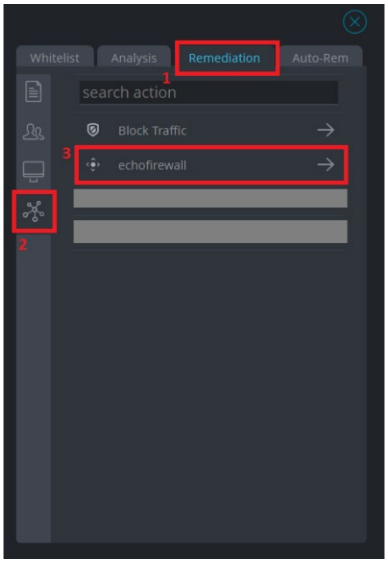
USER [redacted]

NETWORK 185.234.218.247

ALERT ID 1569
FIRST SEEN 12/04/2019 19:08
LAST SEEN 12/04/2019 19:08
GROUP NAME Manually Ins...

Auto-Remediation: No Auto-Remediation

Last Auto-Remediation Action



Whitelist | Analysis | Remediation | Auto-Rem

search action

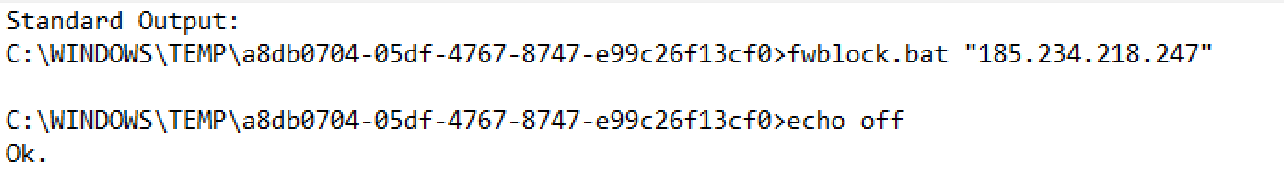
Block Traffic →

echofirewall →

[redacted]

A new menu is opened, in it, select the remediation tab → Network and press on our new custom remediation.

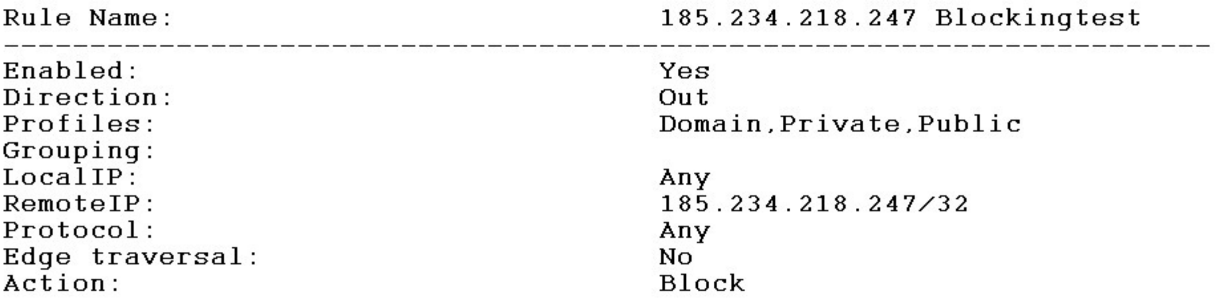
The script’s output will be stored in the page: Actions → NETWORK:



```
Standard Output:
C:\WINDOWS\TEMP\a8db0704-05df-4767-8747-e99c26f13cf0>fwblock.bat "185.234.218.247"

C:\WINDOWS\TEMP\a8db0704-05df-4767-8747-e99c26f13cf0>echo off
Ok.
```

and will create a firewall rule that block traffic to the malicious domain on the alerted host:



```
Rule Name:                            185.234.218.247 Blockingtest
----------------------------------------------------------------------
Enabled:                              Yes
Direction:                            Out
Profiles:                             Domain,Private,Public
Grouping:
LocalIP:                              Any
RemoteIP:                             185.234.218.247/32
Protocol:                             Any
Edge traversal:                       No
Action:                               Block
```