This tool serves as a security tool that integrates with the Cisco Firepower and VirusTotal API to enhance network protection. The script is designed to accept a destination IP address as input from the FMC Remediation Module. Upon receiving the IP address, it checks against the VirusTotal database to determine if there have been any reported malicious activities associated with that IP. This tool serves as a complementary solution in cases where Talos is unable to identify the malicious hosts.

Workflow:

- **Input Collection:** The script receives the destination IP address from cisco fmc remediation module.
- **VirusTotal API Check:** It then sends this IP address to the VirusTotal API, which performs a security check against its comprehensive database of known security threats.
- **Analysis of Response:** The script analyzes the response from VirusTotal to ascertain whether any malicious activity has been detected related to the provided IP address.
- **FMC Integration:** If malicious activity is detected, the script automatically adds the malicious IP address to a dynamic object on the Cisco Firepower Management Center (FMC). There should be a Block ACP (Access Control Policy) in the Cisco Firepower Management Center (FMC) that includes this Dynamic Object as a destination in the Dynamic Attributes tab.

Follow the instruction below to setup system:

Step 1: Deploy the OVF and Configure the API Machine

The primary purpose of installing the OVA file is to access a specialized portal designed for enhanced management of blocked IP addresses. This portal offers improved functionality, allowing users to manage blocked IP addresses more efficiently. The portal provides the following features:

1. The ability to easily remove blocked IP addresses and add them to a dynamic object within the FMC using the provided API.
2. The option to select a preferred company in the Virus Total API to periodically check blocked IP addresses against them. If an IP become safe it will remove it automatically from dynamic object in FMC.

After deploying the machine, use the following credentials to log in:

- Username: **root**
- Password: **cisco123**

Once logged in, type the command 'serverconfig' to access the server configuration wizard. There are three configuration options within the wizard:

1. **Configure Network:** By choosing this option, you can set the IP address of the machine.

2. **Enter Cisco Firepower Information:** In this section, you should provide the following details: FMC IP address, username, password, and the name of the dynamic object.

3. **Enter Virus Total API Key:** In this menu, you should input your Virus Total API key.

Step 2: Create a Dynamic Object in FMC

1. Log in to the Cisco Firepower Management System.
2. Navigate to the "Objects" menu and select "Object Management".
3. Under "Object Management", choose "External Attributes" and then select "Dynamic Object".
4. Create a dynamic object named "**VirusCheckDetection**".

Step 3: Create an Access Control Policy (ACP)

1. Log in to the Cisco Firepower Management System.
2. Navigate to the "Policies" menu and select "Access Control".
3. Create an Access Control Policy with a block action.
4. Within the policy, add the **VirusCheckDetection** dynamic object as the destination in the "Dynamic Attribute" tab.

Step 4: Install the Remediation Module

1. Log in to the Cisco Firepower Management System.
2. Navigate to the "Policies" menu and then go to the "Module" menu.
3. In the "Install New Module" section, choose the "BlockUnknownTalos.tar.gz" file from the "RemediationModule" folder and install it.
4. After installation, click on the eye icon next to the "Unknown Talos Remediation Module" row.
5. In the "Configured Instances" section, click "Add" to create a new instance.
6. Enter a name for the instance, then input the IP address of the deployed API machine, and click "Create".
7. In the "Configured Remediations" section, select "Block Unknown Talos" and click "Add".
8. Enter a name for the remediation and click "Create".
9. Click "Done" to complete the setup of the remediation module.

Step 5: Create a Policy for the Remediation Module

1. Log in to the Cisco Firepower Management System.
2. Navigate to the "Policies" menu and then go to the "Correlation" menu.
3. In the "Rule Management" tab, create a rule with the following conditions:
    - Enter a rule name.
    - In the "Select the type of event for this rule" section, choose "a connection event occurs" and "at the beginning of the connection".* In the "Conditions" section, select "URL Category" and set it to "Uncategorized".
    - Save the rule.
4. In the "Policy Management" tab, create a new policy with the following information:
    - Enter a policy name.

- Click on "Add Rules" and then select the name of the rule you created in the previous step.
- At the end of the row, click on the "Responses" icon and choose the remediation module name you created in the previous step (step 4).
- Save the policy.