Create exclusions in ESET Inspect and ESET Inspect Cloud

Lesley | ESET Nederland - 2022-10-24 - Reacties (0) - ESET PROTECT

Issue

- Add exclusions to ESET Inspect or ESET Inspect Cloud
- Add Trigger Event
- Injection into trusted process/system process
- Trusted process loaded suspicious DLL
- Add a Parent process

ESET Security Services for ESET Inspect and ESET Inspect Cloud

ESET offers various security service packages and additional support for these products. Support for ESET Inspect on-premises and ESET Inspect Cloud is limited and managing rules or exclusions are not included without an ESET Security Service package. Contact a sales representative for further assistance.

Added trigger event

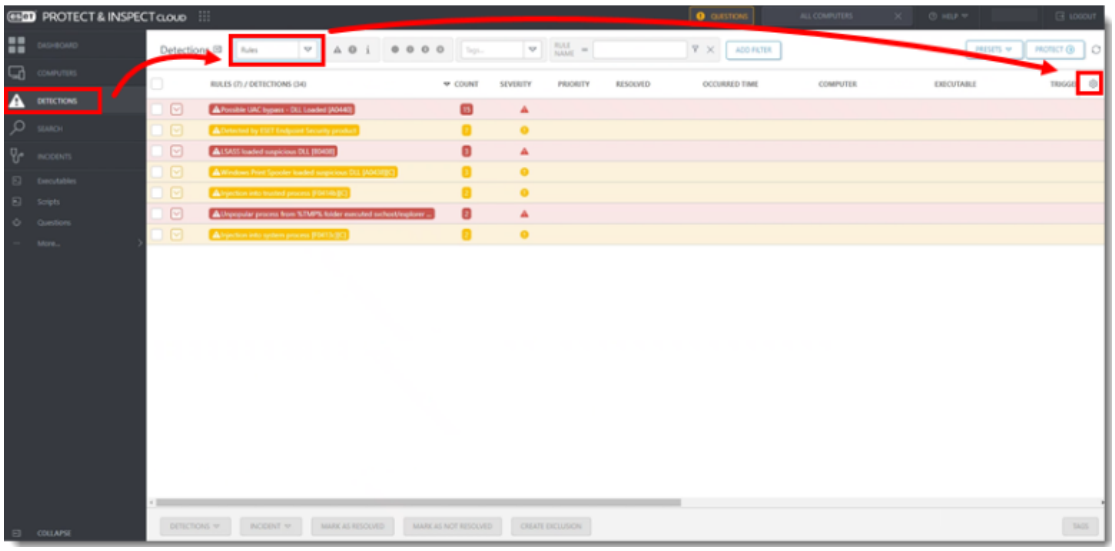
Exclusion rules

The code provided is only for the rules listed below. Other rules will require different coding for their specific exclusion.

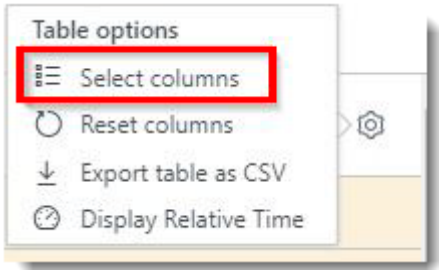
- Injection into trusted process
- Injection into system process
- Trusted process loaded suspicious DLL

Users must create a new exclusion for each rule.

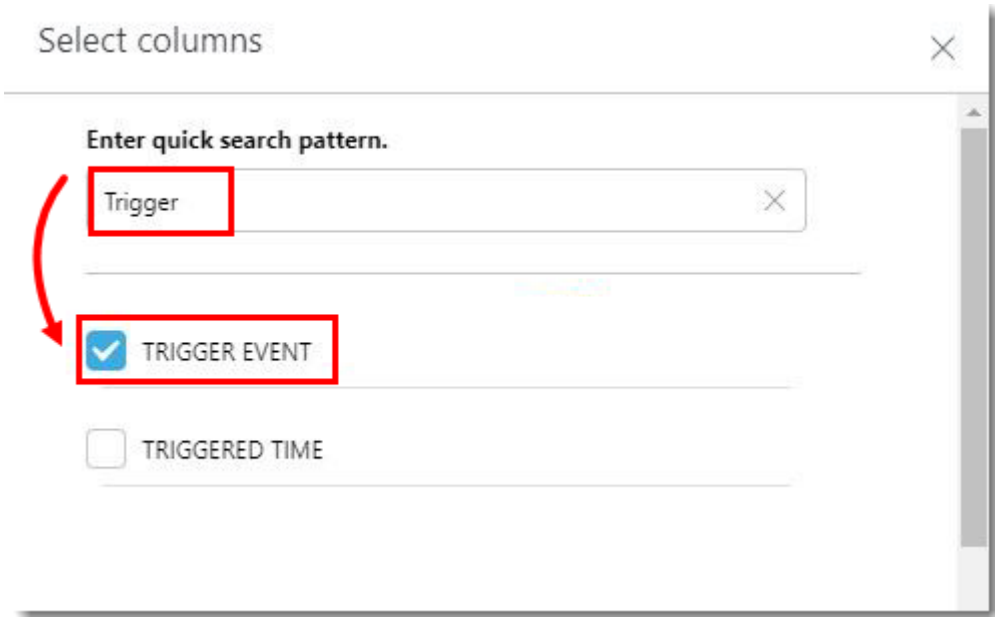
1. Log in to ESET Inspect Cloud.
ESET Inspect users, open the ESET Inspect Web Console in your web browser and log in.
2. Click **Detections**, click the drop-down menu next to **Detections** and select **Rules**. Click the gear icon below the **Protect** button.



3. Select **Select columns**.



4.Type **Trigger** into the **Enter quick search pattern.** field and select the check box next to **Trigger Event**

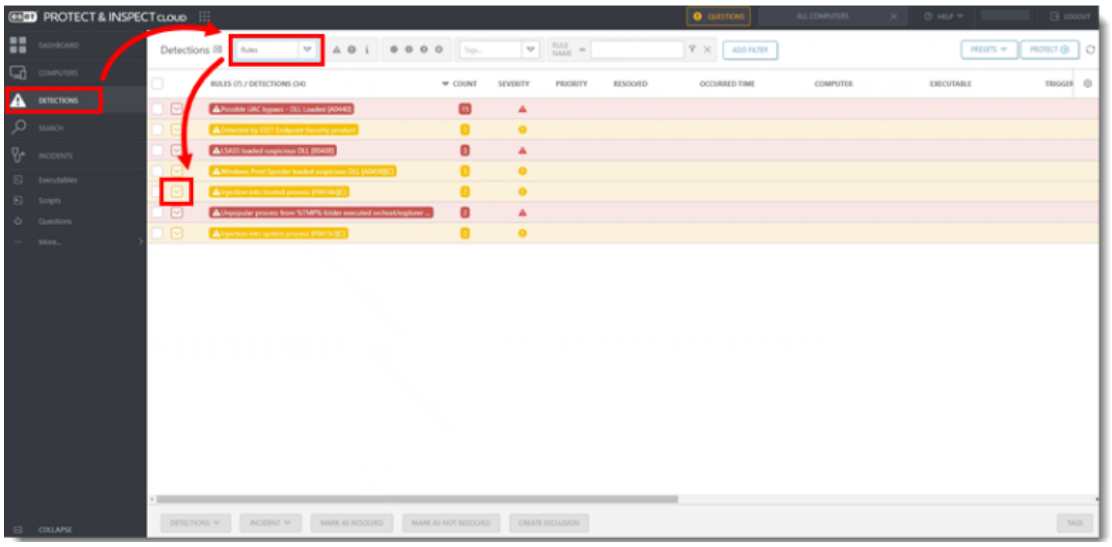


Injection into trusted process/system process

1. Log in to ESET Inspect Cloud.

ESET Inspect users, open the ESET Inspect Web Console in your web browser and log in.

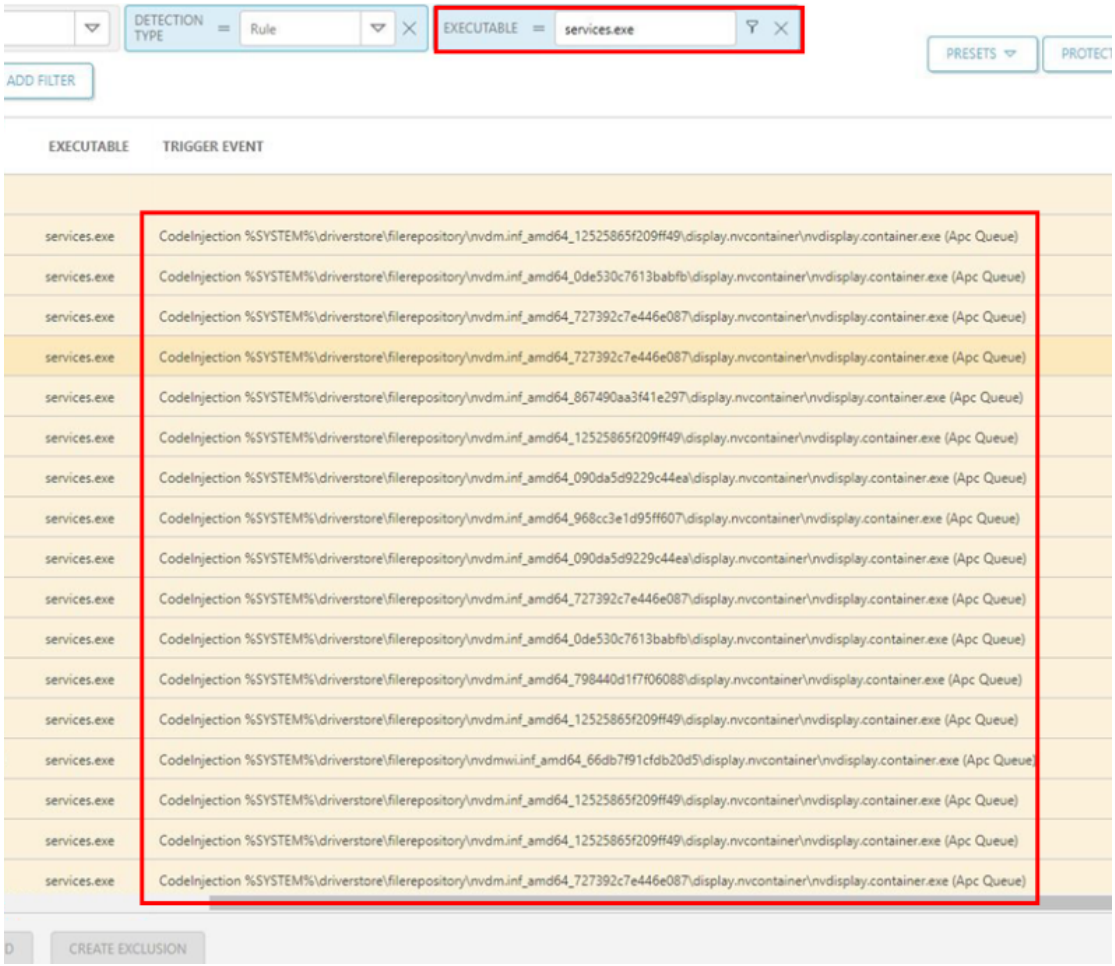
2. Click Detections, click the drop-down menu next to **Detections**, and select **Rules**. Expand the rule to view all detections associated with the rule.



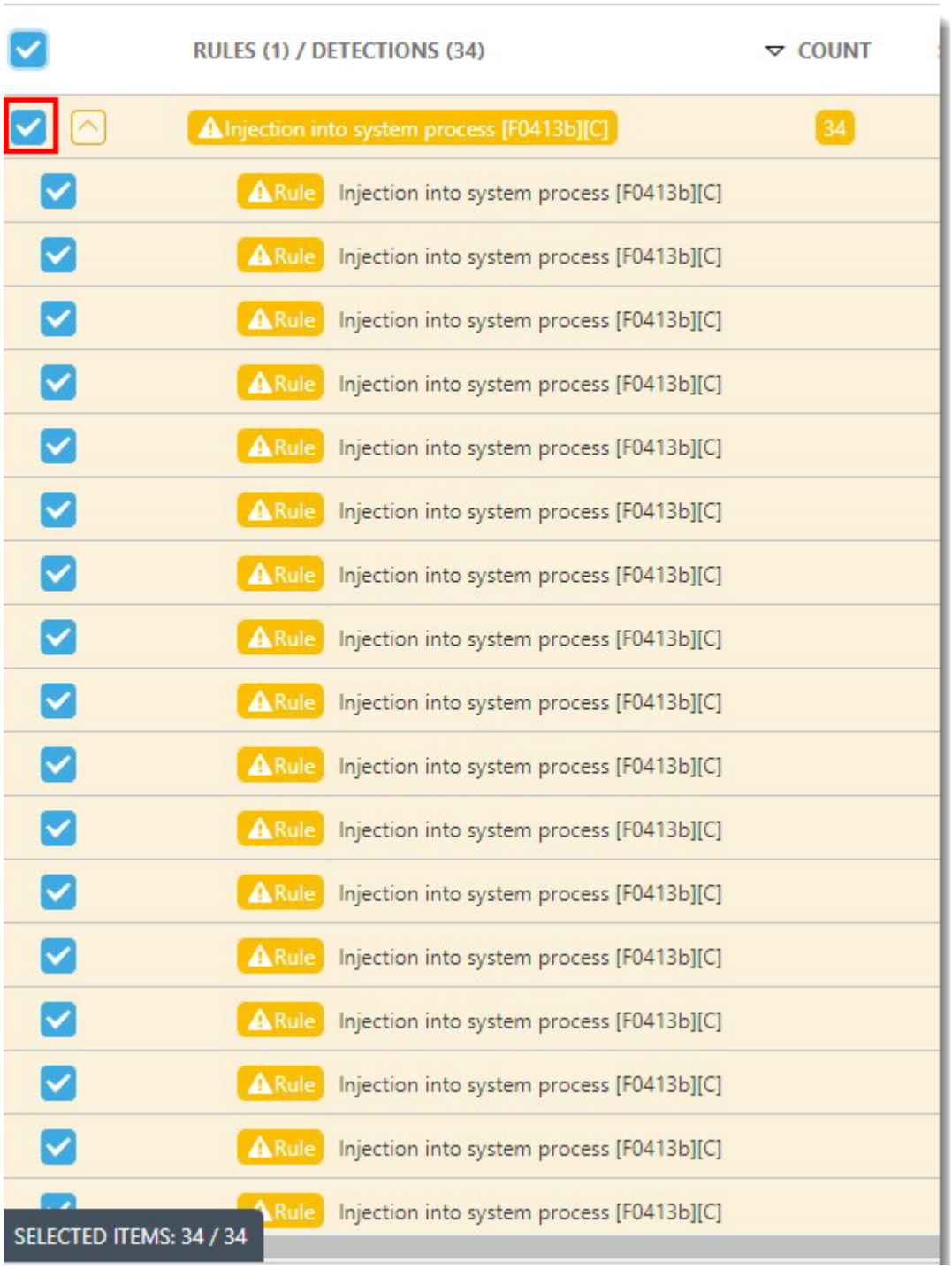
3. In the **Executable** filter type, type the executable name and press Enter. Scroll to the right to view the full Trigger Event name.

Executable and Trigger Event

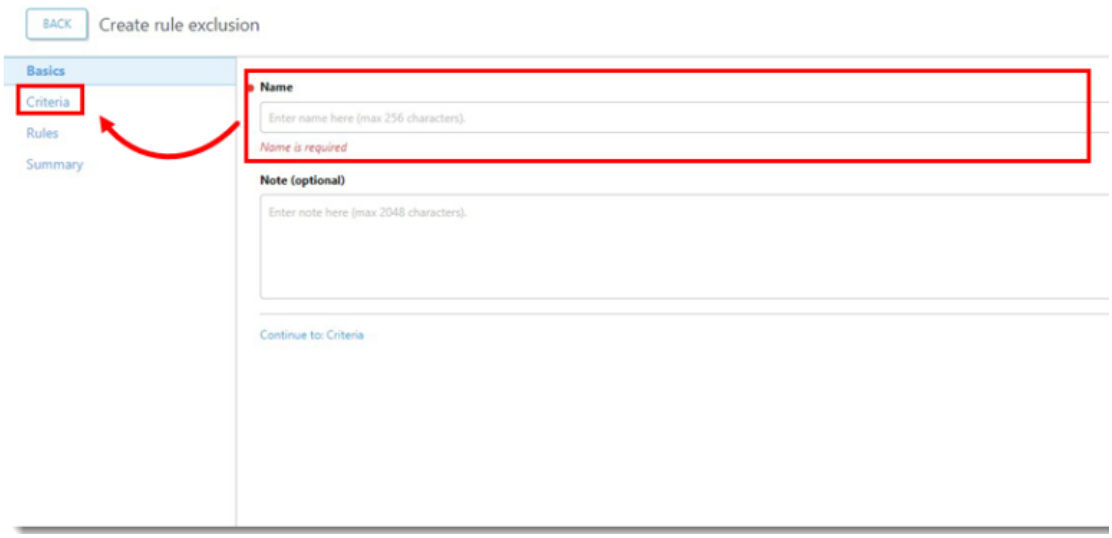
Users will need to compare and contrast the executable type and their Event Trigger information to determine similarities between detections. Detections that have the same Executable, Trigger Event and command will make a proper exclusion. Users may need to create more than one exclusion.



4.Select the check box next to the detection.

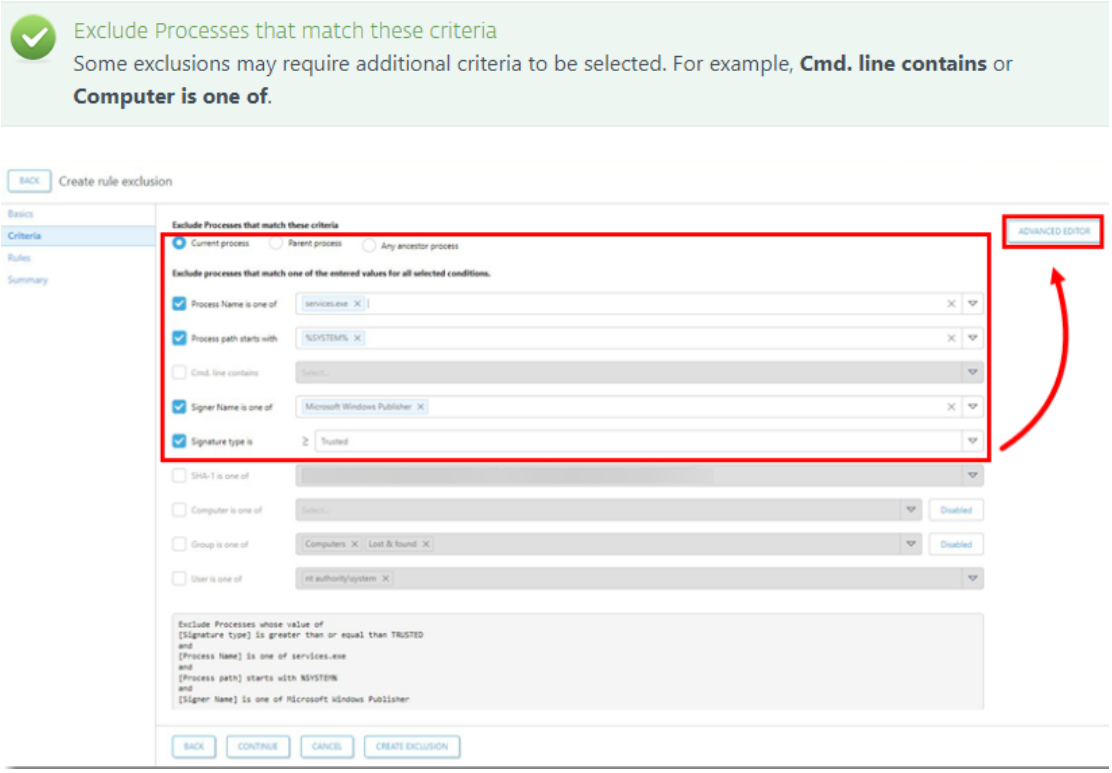


5. Click **Create Exclusion**.
6. Type a **Name** for the exclusion and click **Criteria**.



7. Verify the **Exclude Processes that match these criteria** fields are selected and click **Advanced Editor**.

- **Current process** is selected
- **Process Name is one of** has the correct executable type
- **Signer Name is one of** has the correct signer selected
- **Signer type is** has **Trusted** or **Valid** selected



8. Add the operations code to the **Exclusion expression**. Click **Create Exclusion**.

- The new <operations> tag must be placed between the existing </process> and </definition> closing tags.
- The condition and value in the operation will vary based on the Trigger Event name. For example, if the Trigger Event name is the same for each detection, the condition will equal `is` and the value can equal the Trigger Event name. If the Trigger Event name has unique information, the condition can be set to `starts` and a separate line can be set to `ends`. In Figure 2-6 the example shows the conditions set to `starts` and `ends`.

Add a Parent process

To create a stricter exclusion add a Parent process in addition to the Exclusion expression shown below.

```
<operations>
        <operation type="LoadDLL">
            <operator type="and">
                <condition component="FileItem" property="FullPath" condition="is" value=""/>
            </operator>
        </operation>
    </operations>
```

For more information on XML syntax and rules, see the ESET Inspect Rules Guide. ESET offers security services for ESET Inspect Cloud. Contact your local sales representative for further assistance.

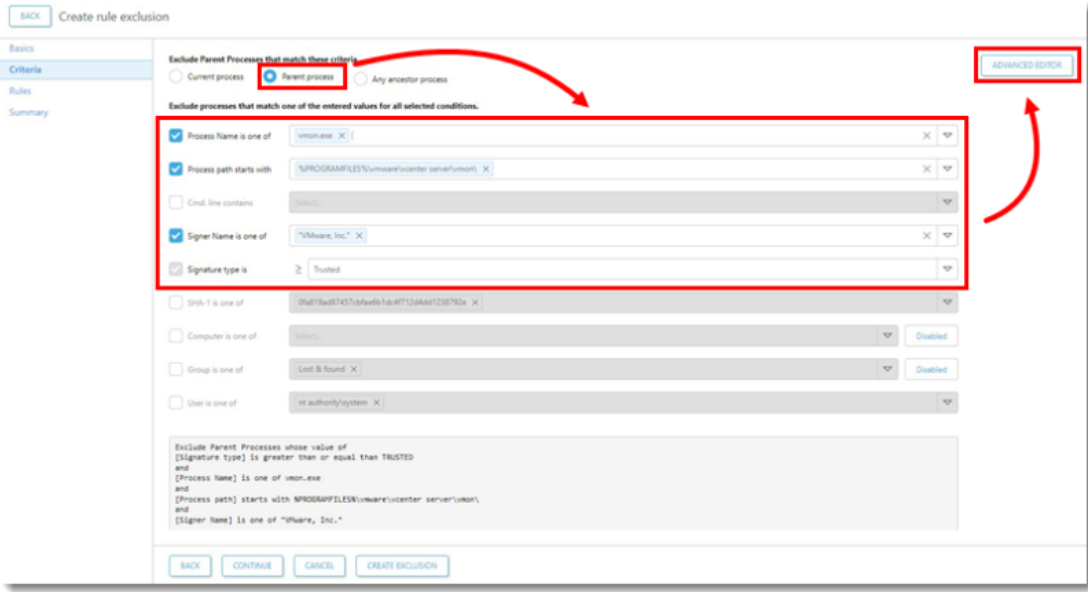
Add a Parent process

Adding a Parent process to the Exclusion expression creates a stricter exclusion.

1. Create the initial exclusion.

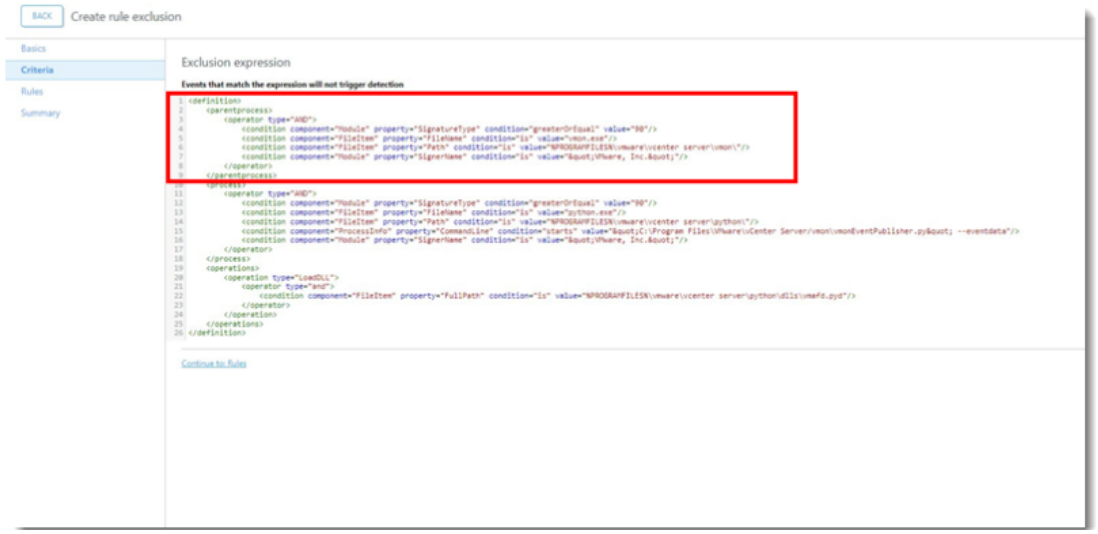
2.Open a new instance of ESET Inspect Cloud or ESET Inspect.
ESET Inspect Cloud users, log in to your ESET Business Account and click **Open Inspect**.
ESET Inspect users, open the ESET Inspect Web Console in your web browser and log in.

3. In the Criteria window select **Parent process**. Select the correct option for **Process Name is one of**, **Process path starts with**, **Signer Name is one of**, and **Signature type is**. Click **Advanced Editor**.



4. Copy the entire expression that starts with `<parentprocess>` and ends with `</parentprocess>`.

5. Go back to the original exclusion and paste the Parent process into the Exclusion expression above the current `<process>`.



6. In the new instance of ESET Inspect Cloud/ESET Inspect, click **Cancel** to cancel the Parent process exclusion.

ESET Security Services for ESET Inspect and ESET Inspect Cloud

ESET offers various security service packages and additional support for these products. Support for ESET Inspect on-premises and ESET Inspect Cloud is limited and managing rules or exclusions are not included without an ESET Security Service package. Contact a sales representative for further assistance.