Content

1. Basic concepts
2. playbook policy examples

1 Basic concepts

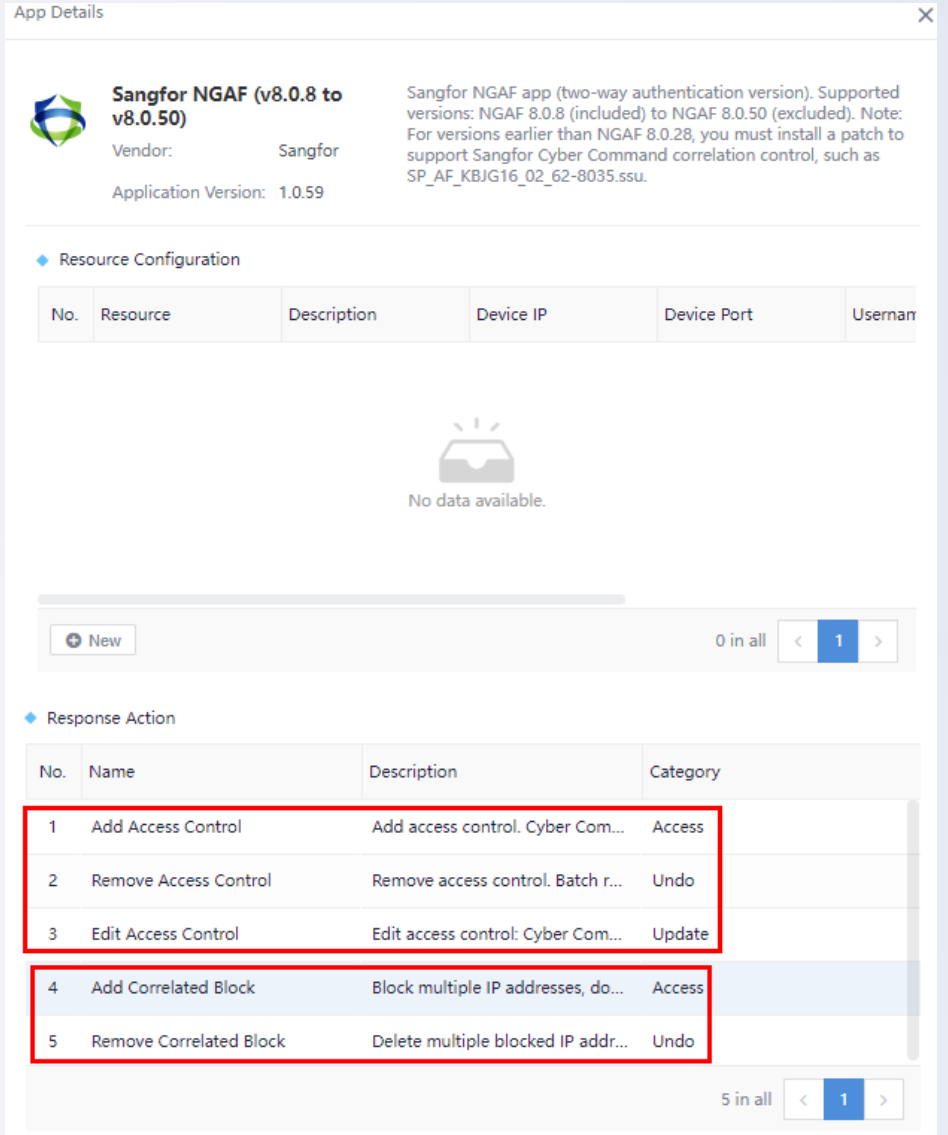
Basic Concepts

1. How to understand the difference between Cyber Command correlation response function and SOAR?

SOAR emphasizes more on sense of technology, policy orchestration and security incident response, emphasizing the realization of security incident (automated) disposal through orchestration;
The response function of Cyber Command (starting from version 3.0.60 of Cyber Command) takes SOAR technology in principle, which support the correlation response of both self-developed products and various third-party devices, and can be programmed in playbook, for security incidents or security alerts. The execution method can be either automatic or manual

2. How to understand the ability of a certain type App?

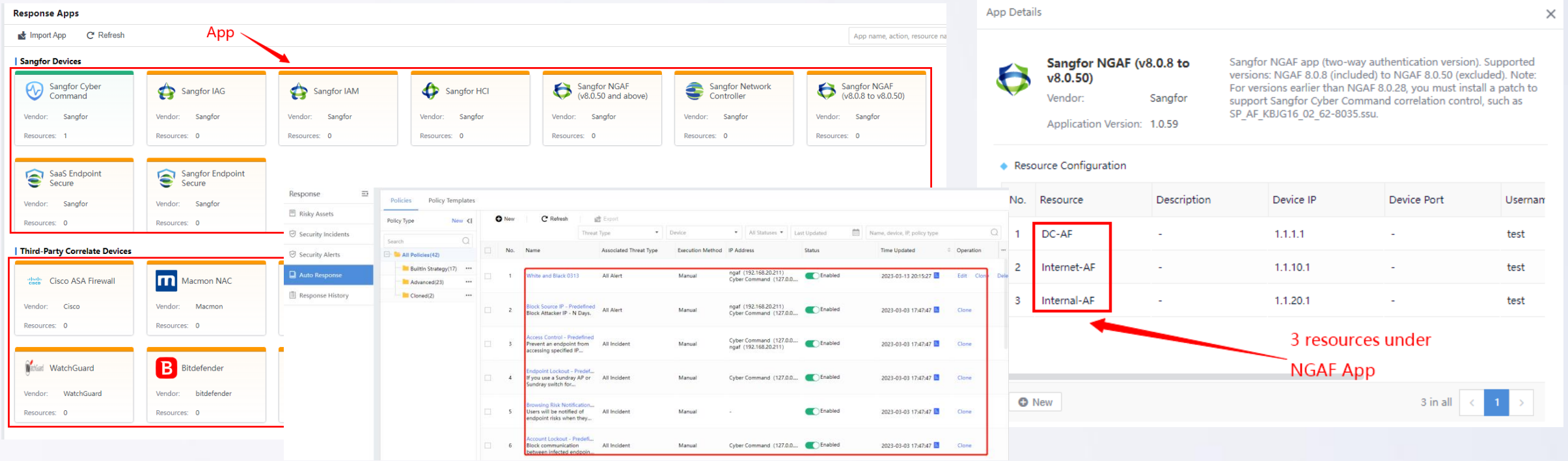
On Cyber Command [System Settings/Device Management/correlation Response] page, select a certain type of App, and we can see the action sorts. Response action can reveal the ability of such App, for example, The Sangfor NGAF(v8.0.50 and above) app contains two sorts capabilities: Access Control and Block. Same methods as other devices.



Basic Concepts

3. Some new high-frequency words related to correlation response

App: represents a certain type of device, such as: IAG, NGAF, ES or other third-party devices.
Resource: represents a specific device added under app, for example: there are 3 NGAFs configured in NGAF app, probably means 3 devices distributed in Internet zone、terminal access zone and public servers zone. **Notice:** some apps due to different versions can be split into two or more apps, such as NGAF and IAG, which have 2 apps and can be directly seen on the [System Settings/Device Management/correlation Response] page.
playbook lolicy: On the [Response/Auto Response] page, the list shows current playbook policies, and these policies include manual type and automatic type. All policies' effect scope is targeted for security incidents and security alerts, rather than logs.



Basic Concepts

4. How we evaluate whether certain third party devices has been adapted by Cyber Command?

Step1: Check product page in latest version;

Step2: If it does not occur in product page, contact with product design manager(Kevin Hu/41214) for further confirmation. In some scenarios, to some third party devices which have not been adapted, project manager has to apply R&D team devotion in advance, otherwise it may become a risky point to PoC test or implementation.

Notice: correlation response API document of third party device is necessary and should be achieved in advance and then PM submit it to R&D team.

Basic Concepts

5、Which pages in Cyber Command can trigger response policies?

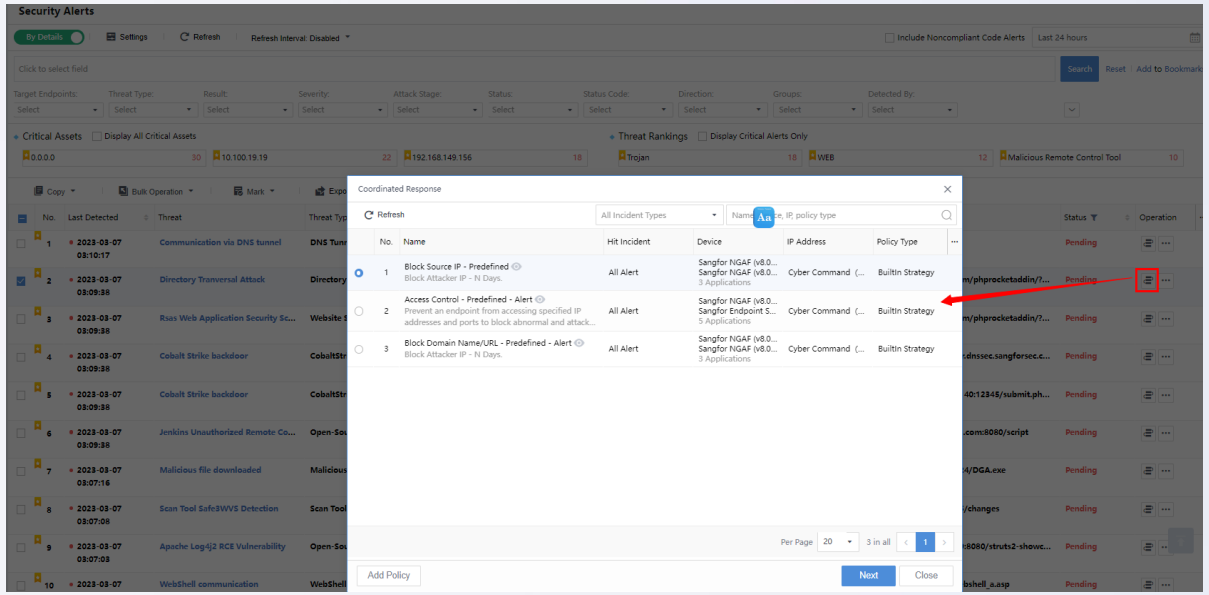
Since security incidents and alerts are the two types of effect scope of response policies, some relevant pages are included as below:

- **risky asset level**:[Response/Risky Assets], select certain item and click "" ;
- **security incidents level**:[Response/Security Incidents], select certain alert item and click " " ;
- **security alerts level**:

① [Response/Security Alerts], By Details mode, select certain item and click ""

② [Detection/Threats], On sub-pages of Ransomware, Cryptomining, and File Threats, select certain items and click "" ;

Of course, above mentioned is about how to execute in manual policies, auto policies can be triggered in these same pages.



Basic Concepts

6. What are the key points of correlation response policy settings?

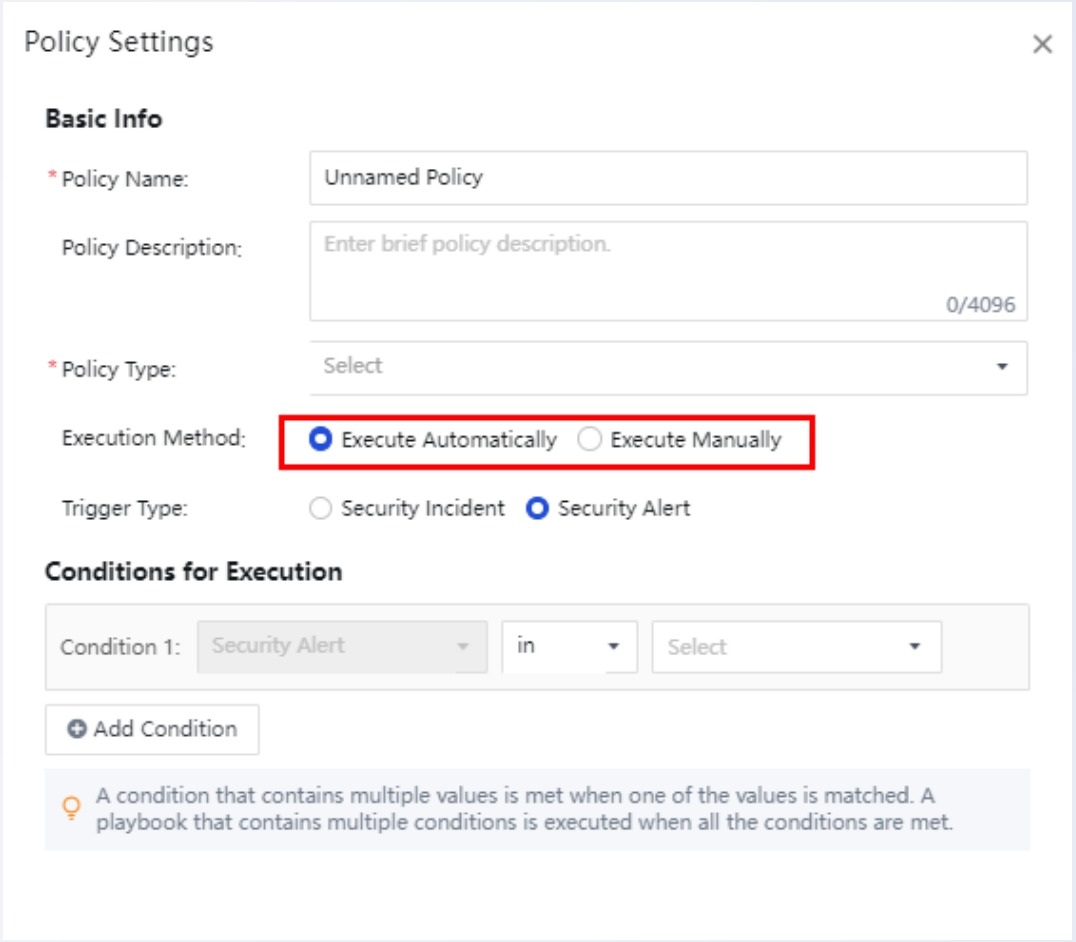
When configuring policies, it is necessary to grasp some overall factors.

① **Execution method**: Execute automatically and execute manually, are very different, especially in automatic sinarios, some inaccurate policies can lead to considerable unexpected blocks;

Extended questions:

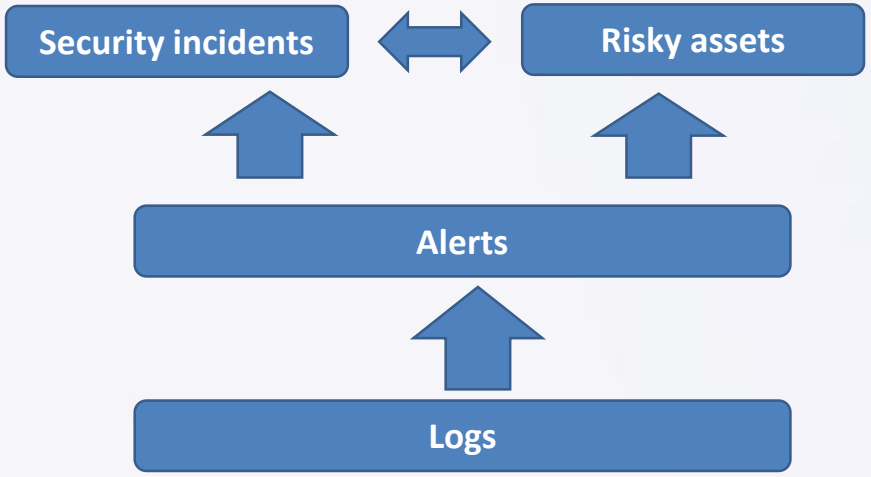
1. What level of importance assets are recommended to execute automatically?

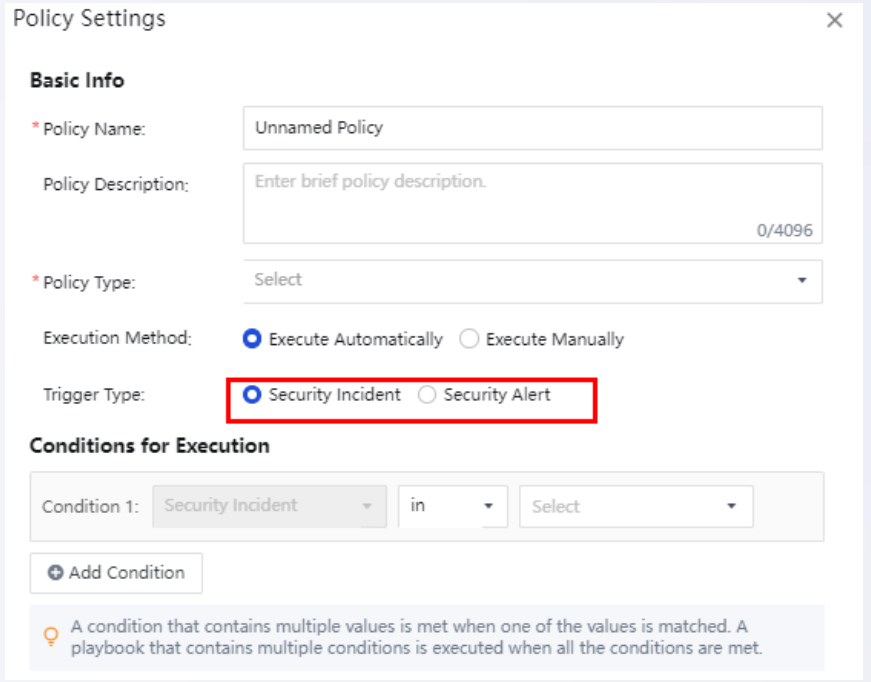
2. Shall we configure auto policies directly and execute them in a large scale without a period of verification?



Basic Concepts

② **Trigger Type**: Cyber Command contains several types of threaten data, that are logs, alerts, and incidents(equal to risky asset), but only alerts or incidents can be selected to be configured playbook policies. They have different effect scope, but one suggestion recommended is that the level we selected should be consistent with daily security operation disposal unit(*for example, small companies may concern more on sercurity incidents and do not have sufficient human resources to handle security alerts*).





Basic Concepts

7. Default product logic related to disposal status of security incidents

[Status Priority order]: "fixed" < "fixing" < "suspended" < "pending"

How do we understand this priority order?

The overall disposal status of a certain incident depends on every single corresponding risky asset, we can include that as below:

① **Pending status**: represents at least one corresponding risky asset is pending status;

② **Suspended status**: represents at least one corresponding risky asset is suspended status,others are ether fixing or fixed;

③ **Fixing status** :represents at least one corresponding risky is fixing, others are fixed;

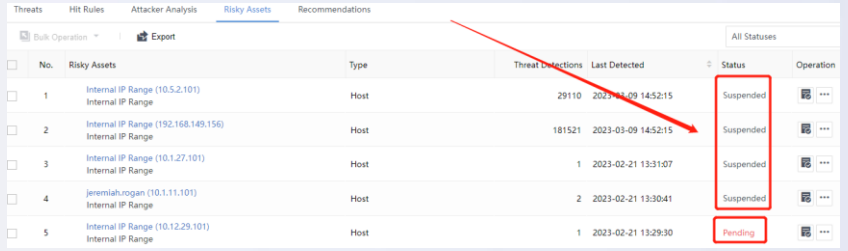
④ **Fixed status**: all corresponding risky assets are fixed, no other status displays for every single risky asset;

Notice: risky assets has the same principal with security incidents presented above.

Basic Concepts

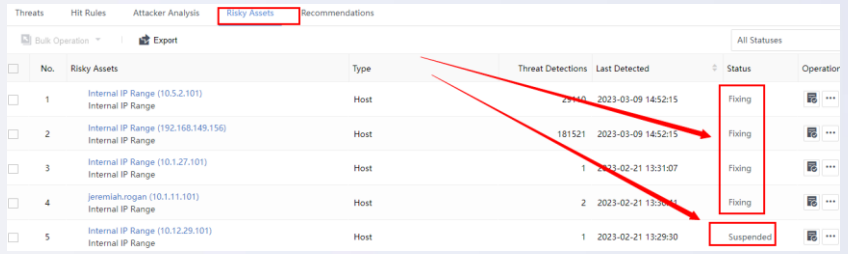
original

No.	Threat	Risky Assets	Severity	Attack Stage	Threat Type	Last Detected	Status	Operation
1	Malicious file downloaded	7	High	Propagation	Malicious File ...	2023-03-09 14:39:58	Fixing	
2	General system command injection att...	3	High	Propagation	System Comm...	2023-03-09 14:45:53	Suspended	
3	Infected with a common virus	5	High	C&C	Bots	2023-03-09 14:42:53	Pending	
4	Cobalt Strike backdoor	3	High	Propagation	CobaltStrike	2023-03-09 14:42:54	Fixing	



Pending-->Suspended

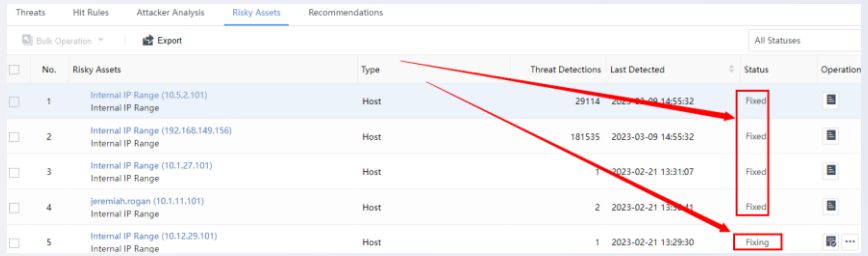
No.	Threat	Risky Assets	Severity	Attack Stage	Threat Type	Last Detected	Status	Operation
1	Malicious file downloaded	7	High	Propagation	Malicious File ...	2023-03-09 14:46:07	Fixing	
2	General system command injection att...	3	High	Propagation	System Comm...	2023-03-09 14:45:53	Suspended	
3	Infected with a common virus	5	High	C&C	Bots	2023-03-09 14:52:15	Suspended	
4	Cobalt Strike backdoor	3	High	Propagation	CobaltStrike	2023-03-09 14:52:42	Fixing	



Export

Suspended-->Fixing

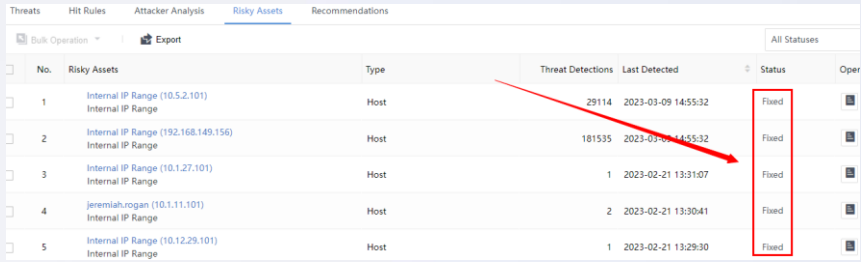
No.	Threat	Risky Assets	Severity	Attack Stage	Threat Type	Last Detected	Status	Operation
1	Malicious file downloaded	7	High	Propagation	Malicious File ...	2023-03-09 14:46:07	Fixing	
2	General system command injection att...	3	High	Propagation	System Comm...	2023-03-09 14:45:53	Suspended	
3	Infected with a common virus	5	High	C&C	Bots	2023-03-09 14:55:32	Fixing	
4	Cobalt Strike backdoor	3	High	Propagation	CobaltStrike	2023-03-09 14:57:05	Fixing	



Export

Fixing-->Fixed

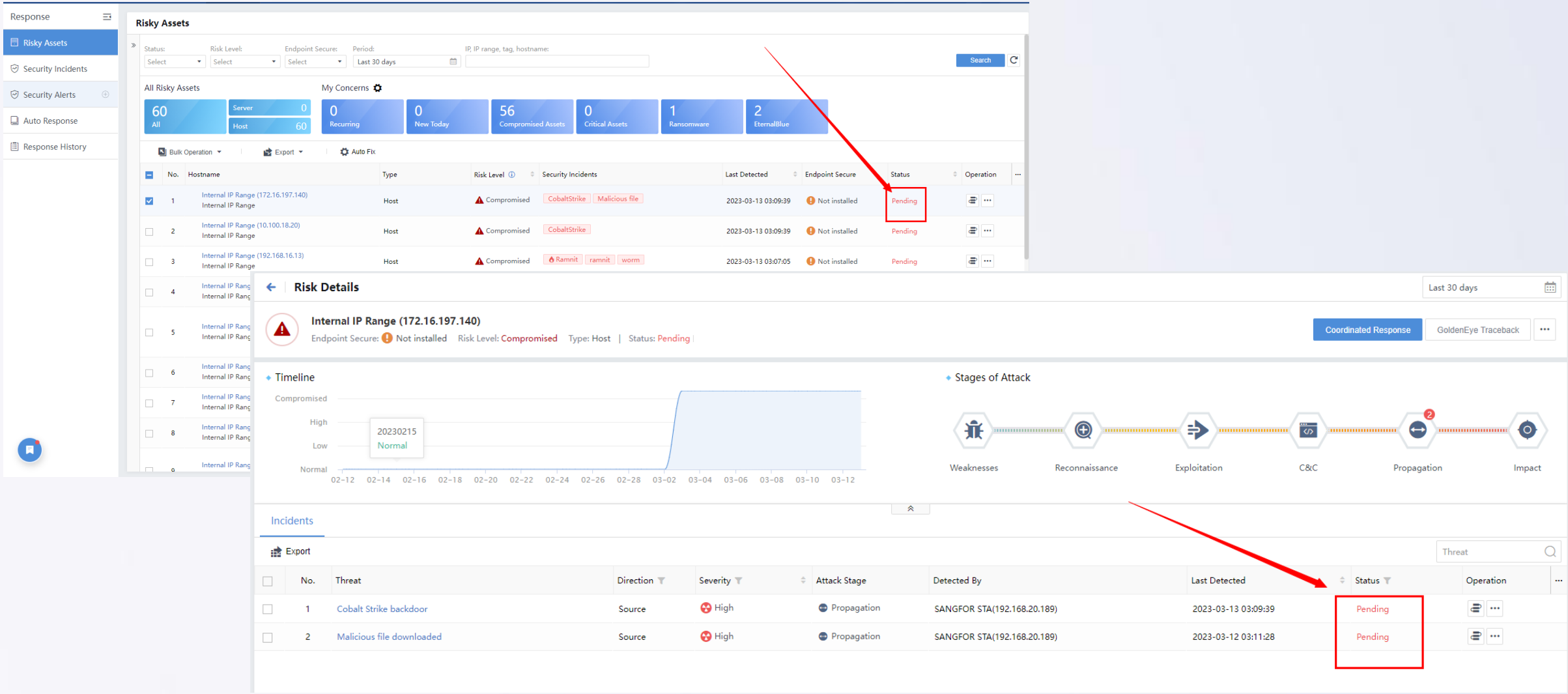
No.	Threat	Risky Assets	Severity	Attack Stage	Threat Type	Last Detected	Status	Operation
1	Malicious file downloaded	7	High	Propagation	Malicious File ...	2023-03-09 14:55:44	Fixing	
2	General system command injection att...	3	High	Propagation	System Comm...	2023-03-09 14:45:53	Suspended	
3	Infected with a common virus	5	High	C&C	Bots	2023-03-09 14:55:32	Fixed	
4	Cobalt Strike backdoor	3	High	Propagation	CobaltStrike	2023-03-09 14:57:05	Fixing	



Basic Concepts

8. Default product logic related to disposal status of risky assets

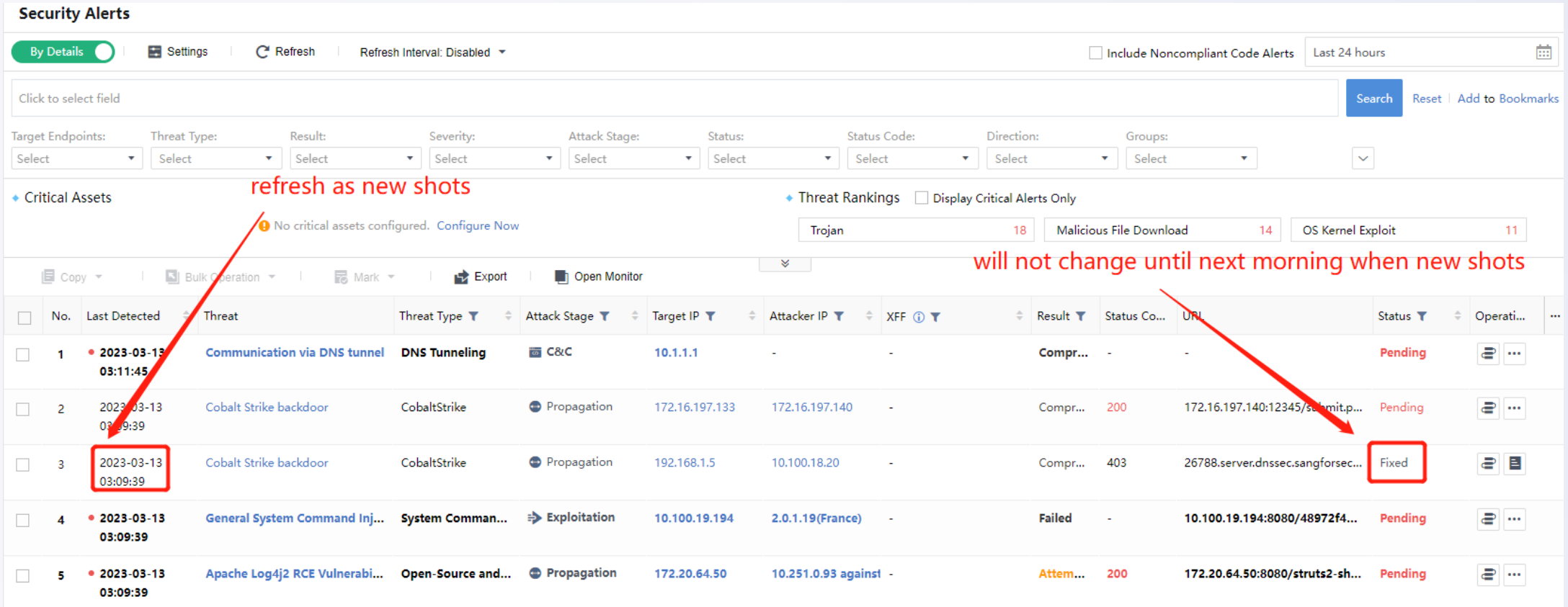
Risky assets follow the similar logic principle with security incidents presented above.



Basic Concepts

9. Differences with security alerts

In by details mode, once a security alert is turned into fixed status, the disposal status will not change until next morning (the default cycle of status aggregation is one day),while the attribute of last detected in the security alert will refresh.



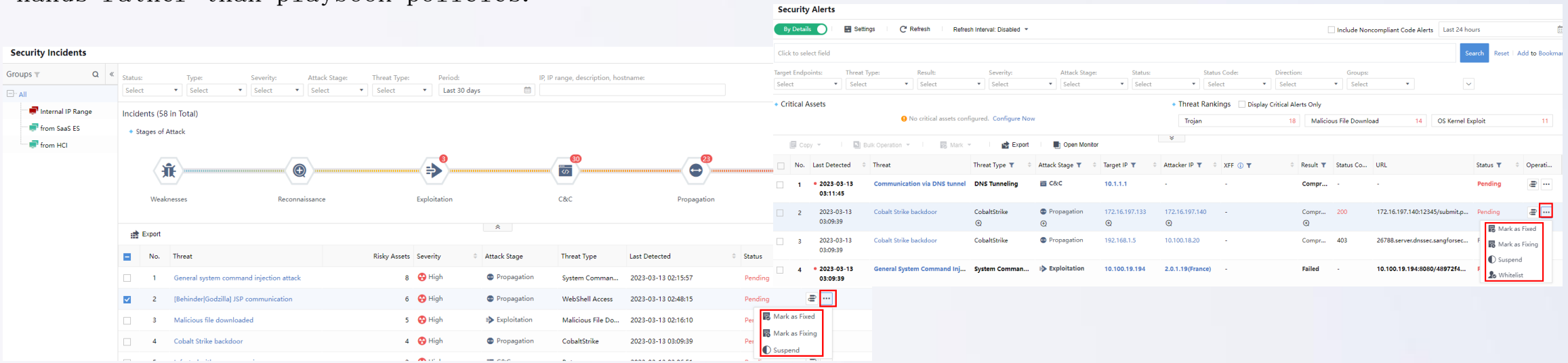
Basic Concepts

10. How do we understand the relationship between correlation response and disposal closed loop in daily cybersecurity operation?

For example, how we design auto response policy to solve unencrypted web traffic alerts?

In fact, correlation response can deal with particular attack types instead of all the attacks. The rest sorts have to consider other measures, such as, whitelists may be alternative.

As a result in daily operation, it is common and necessary to make incidents and alerts fixed by hands rather than playbook policies.

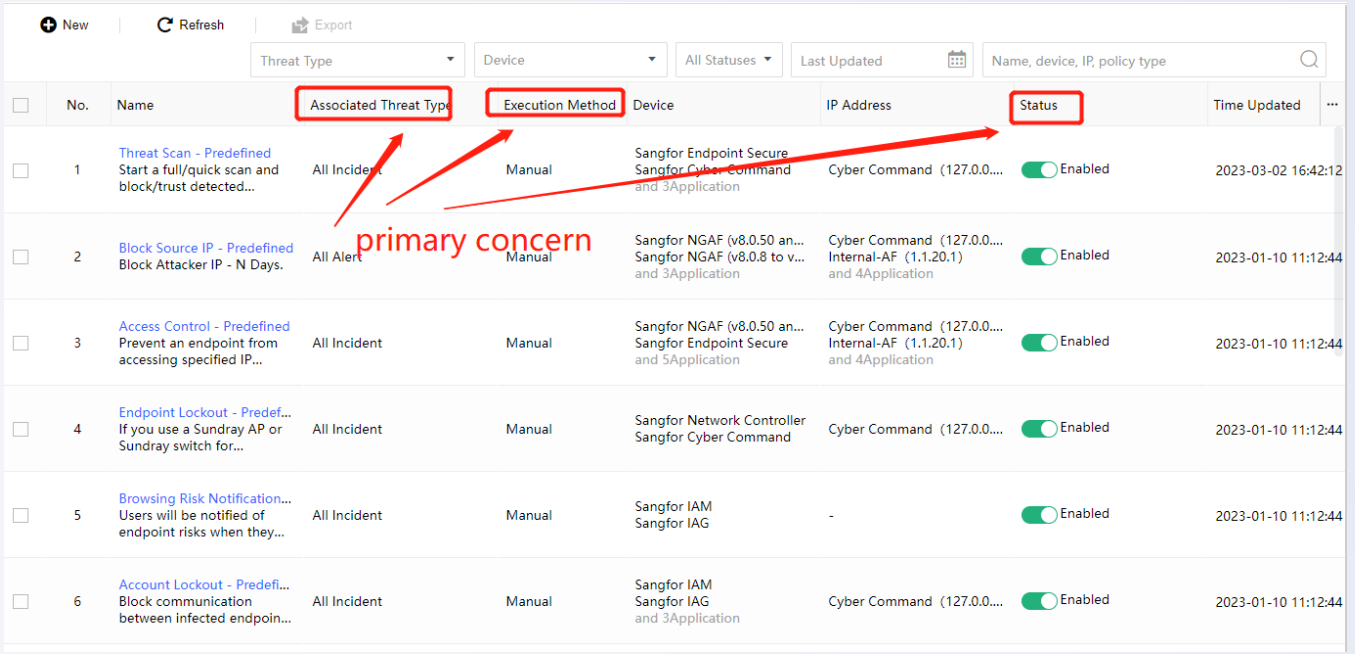


Basic Concepts

11. What attributes should concern more or how to quickly distinguish the key points in response policy lists?

【Primary concern】

- **Execution Method:** it is very important especially when there exists a few auto response policies and make sure these policies have been well verified before they formally come into effect in a large scale;
- **Status:** check the status and make sure switch is on when you want to perform some policies;
- **Associated threat type**: distinguish whether it is targeted for incidents or alerts, it matters a lot since it would have impact on different pages and objectives;



Basic Concepts

12. Cyber Command has dozens of built-in playbook policies by default. These policies have covered most disposal scenarios. For most customers,built-in policies should be given priority in daily operations to avoid a large amount of self-defined workload.

13. What is general procedure of self-defined playbook policies?

- **Step1 Evaluate the possiblity:** decompose it based on the correlation requirement scenario, and determine whether it can be customized. For example, a customer wants to lock a specific type of security log by playbook policy which is obviously impossible....
- **Step2 Policy formulation:** there are several methodologies and precautions in the process:

① Sort out key actions of the entire policy and arrange them in logical order;

② Be good at using the process filtering, logical judgements will be conducted by filtering rules

③ Some actions should be paid attention as they may include delayed execution or cyclic execution cooperated with process filtering;

④ Some specific data(such as ip address、blacklist or writelist) try to summarize in constants for flexible call;

Basic Concepts

14. There is a sheet explaining parameters in details and it can help us to create playbook policies.

We should recognize that what sorts are used with high-frequency, even though there are so many action parameters.

No.	Classification	Parameter	Name	Parameter Example	Parameter Type	Description	Devices	Action	Remarks
1	Security Incidents	${incident.oid}	Incident ID	event62d00102a29c1521938022	str	When the Coordinated Response is clicked, an oid will be generated based on the clicked data	Cyber Command	Obtain Asset Info Send Notification Check File Status Change Security Incident Status Change Security Alert Status	1. It is not the same as the ID of the event details page. In fIAGt, it is useless for the front end, and the "rule ID of the security event" is more used. 2. This ID is only used for data screening and maintenance in the bIAGkground, and has
2	Security Incidents	${incident.asset_id}	Asset ID	46	int	Asset ID	Cyber Command	Change Risky Endpoint Status Obtain Asset Scan Information	The ID of the latest asset where the current security incident occurred, you can query the unique asset by entering the asset table of the database through this ID
3	Security Incidents	${incident.ip}	Asset IP	1.1.1.1	str	Asset IP	Cyber Command	Obtain Asset Virus Status in Endpoint Secure Tips Query Information About Endpoint Secure Installation of Assets	IP address of the latest asset where the current security incident occurred
4	Security Incidents	${incident.branch_id}	Asset Group ID	0	int	Asset Group ID	Cyber Command	Obtain Malicious Processes of Incidents Isolate Malicious Processes Query Isolation Status of Malicious Processes Obtain Isolation	The asset group ID of the latest asset where the current security incident occurred
5	Security Incidents	${incident.linkage_recommend.common.src_ip}	Src IP	[1.1.1.1, 1.1.1.2]	Array	Src IP	Integrated Device	Actions of Integrated Devices	under normal circumstances, the aggregation of the source IP in the relevant security log is taken //Unavailable, when the linkage blockade of security events is called directly, it
6	Security Incidents	${incident.linkage_recommend.common.dst_ip}	Dst IP	[1.1.1.1, 1.1.1.2]	Array	Dst IP	Integrated Device		under normal circumstances, the aggregation of the destination IP in the relevant security log is taken //Unavailable, when the linkage blockade of
7	Security Incidents	${incident.linkage_recommend.common.src_port}	Src Port	[443]	Array	Src Port	Integrated Device		the port is read from the configuration file //In Cyber Command3.0.69 and earlier versions, only individual security events can be matched, which is basically unavailable;

Revision History | Security Incident Field Desc | Security Alert Field Desc

2 playbook policy examples

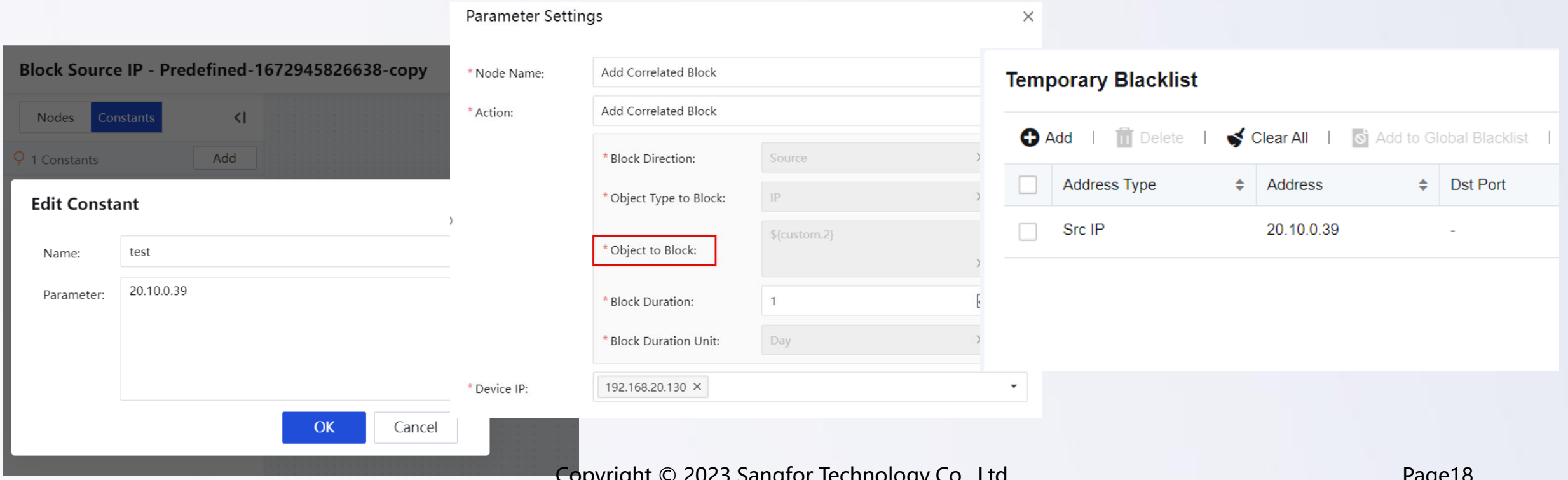
Example 1

【Background】

One of Sangfor customers have purchased more than 10 NGAF and Cyber Command. The customer wants to configure a blacklist to all devices once;

【Method to Achieve】 - Method 1

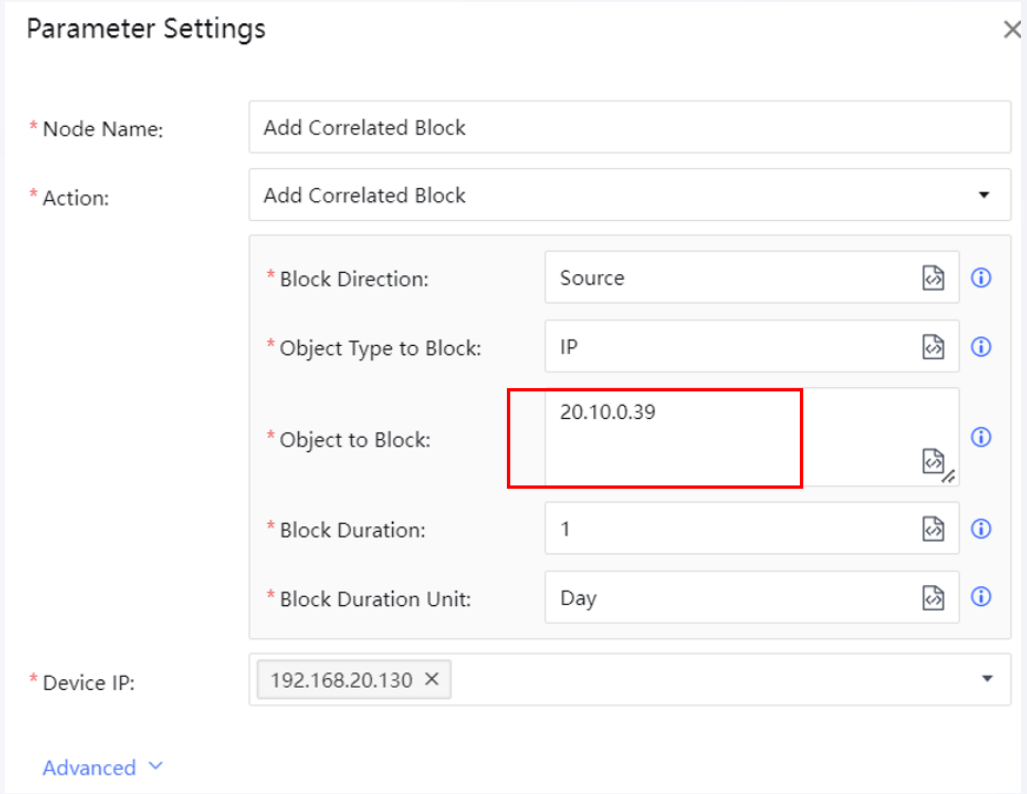
create correlation response policy, fill the blacklist addresses in a constant, and then select all NGAF devices;

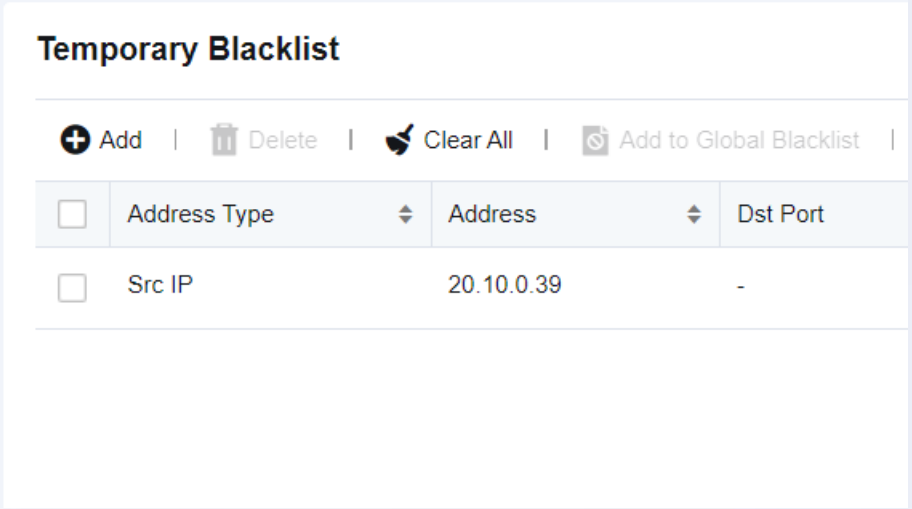


Example 1

【Method to Achieve】- Method 2

create correlation response policy directly fill blacklist addresses in the area of “Object to Block”, and then push down the policy to all NGAF devices;





Example 2

【Background】

A branch of customer, as a defender, is participating external offensive and defensive drills. Due to the shortage of security analysts , it is necessary to adopt the "black-and-white" mode for blocking attacks from Internet, that is to say, any global ip addresses not in whitelists issued by HQ should be blocked in time when those access to intranet;

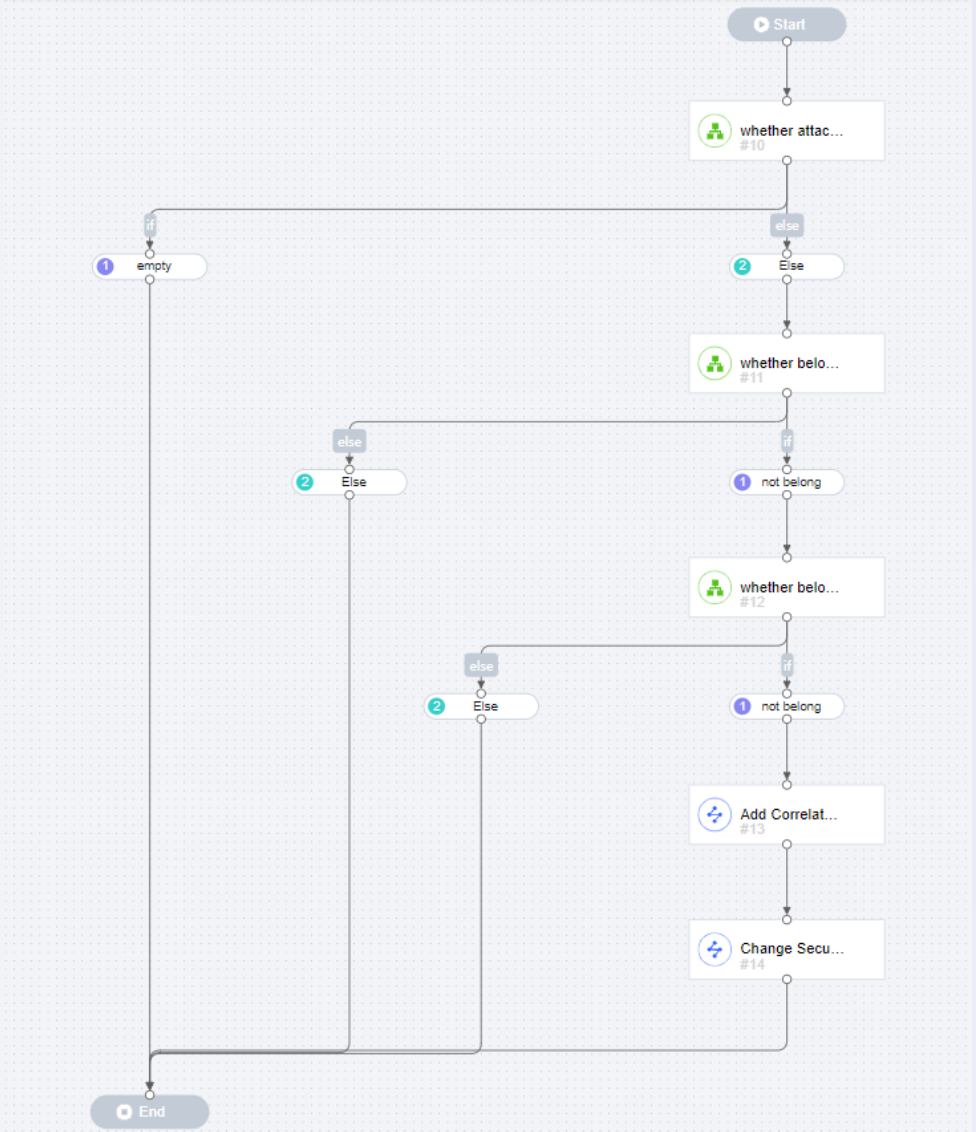
【Method to Achieve】

According to the requirement, firstly, we have the common concept that this policy should be oriented to security alerts and be automatic,and then define a constant including all ip addresses. The key action is blocking by NGAF, but we should consider some necessary check before it performs, for example, whether the attacker ip address exists, whether the attacker ip address belongs to whitelists and whether the attacker ip is an intranet asset. After we exclude such conditions it will be appropriate to perform block action in all NGAF devices and change the status of alerts automatically by following action.

Example 2

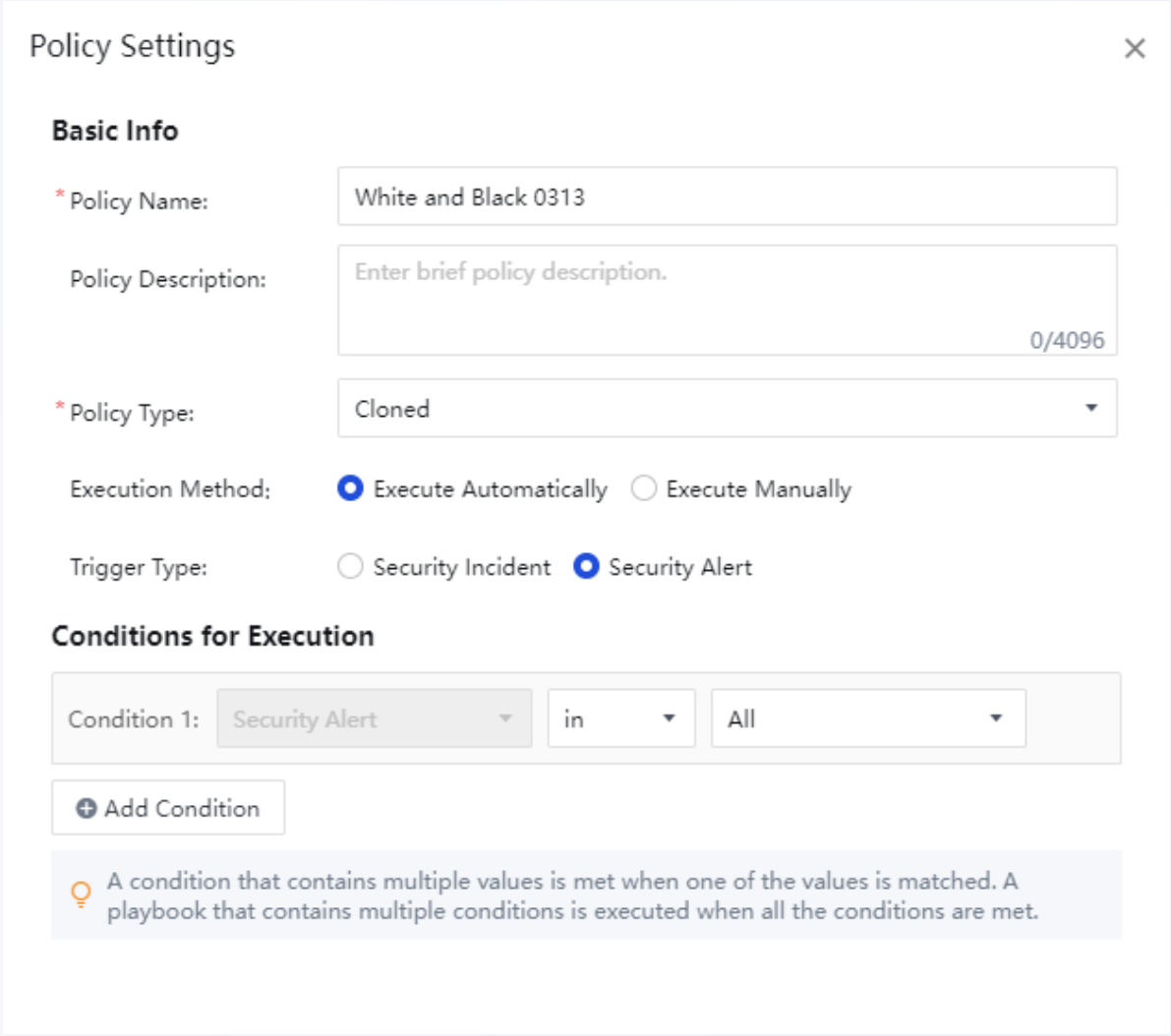
【Method to Achieve】

- **Step1**: Policy setting, execute automatically, security alert, all attack types;(*In reality, we should not set auto execution directly, manual execution is recommended at the begining*)
- **Step2**:Create a constant and fill in whitelist ip addresses, create another constant and fill in intranet assets ip addresses range;
- **Step3**: Decision, excludes the case where the attacker ip is empty in security alerts;
- **Step4**: Decision, excludes the case where the attacker ip is an intranet address in security alerts;
- **Step5**: Decision, excludes the situation that the attacker ip is in the white list address ;
- **Step6**: Action, block the attacker's ip address;
- **Step7**: Action, modify the disposal status of corresponding security alert;



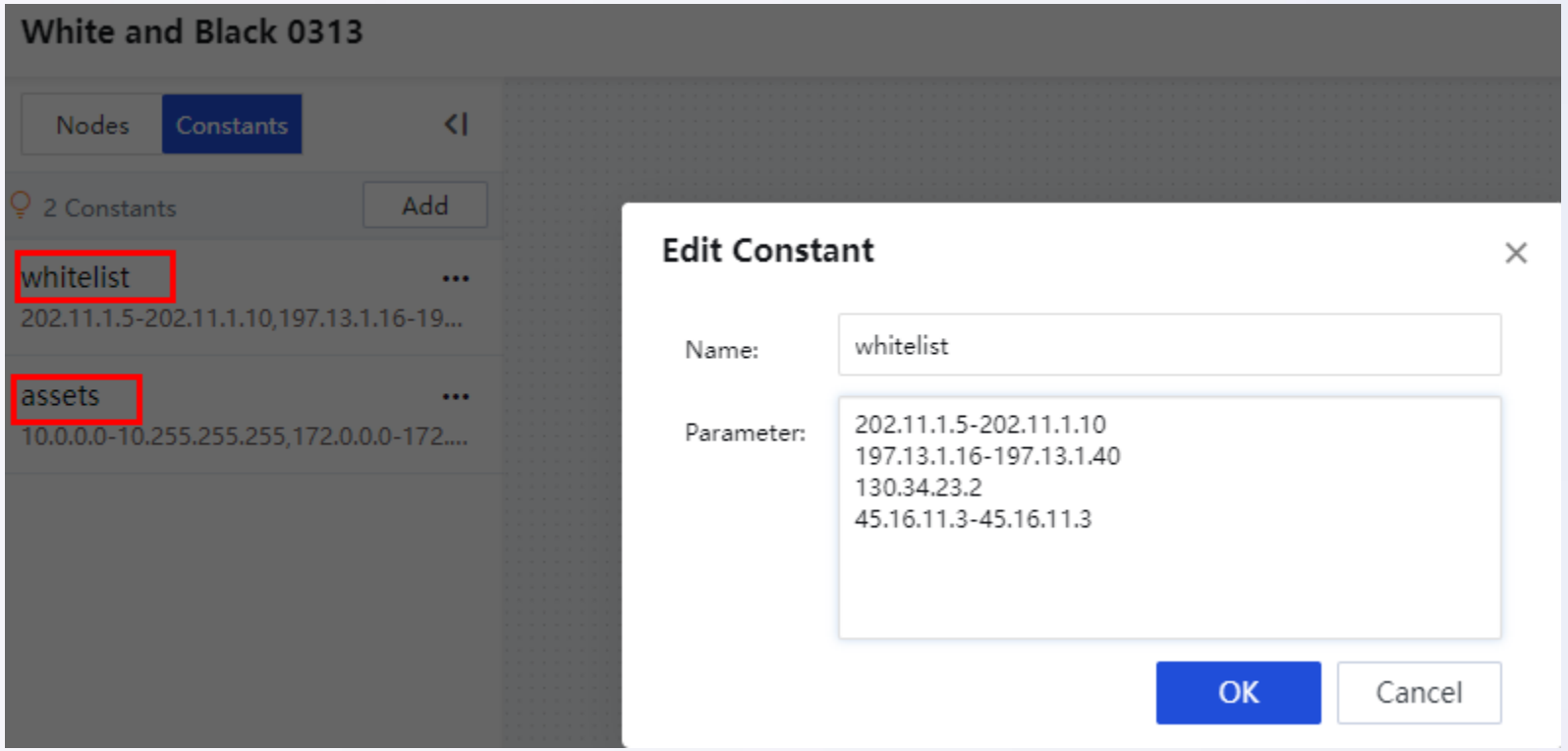
Example 2

Step1: Policy setting, execute automatically, security alert, all attack types;



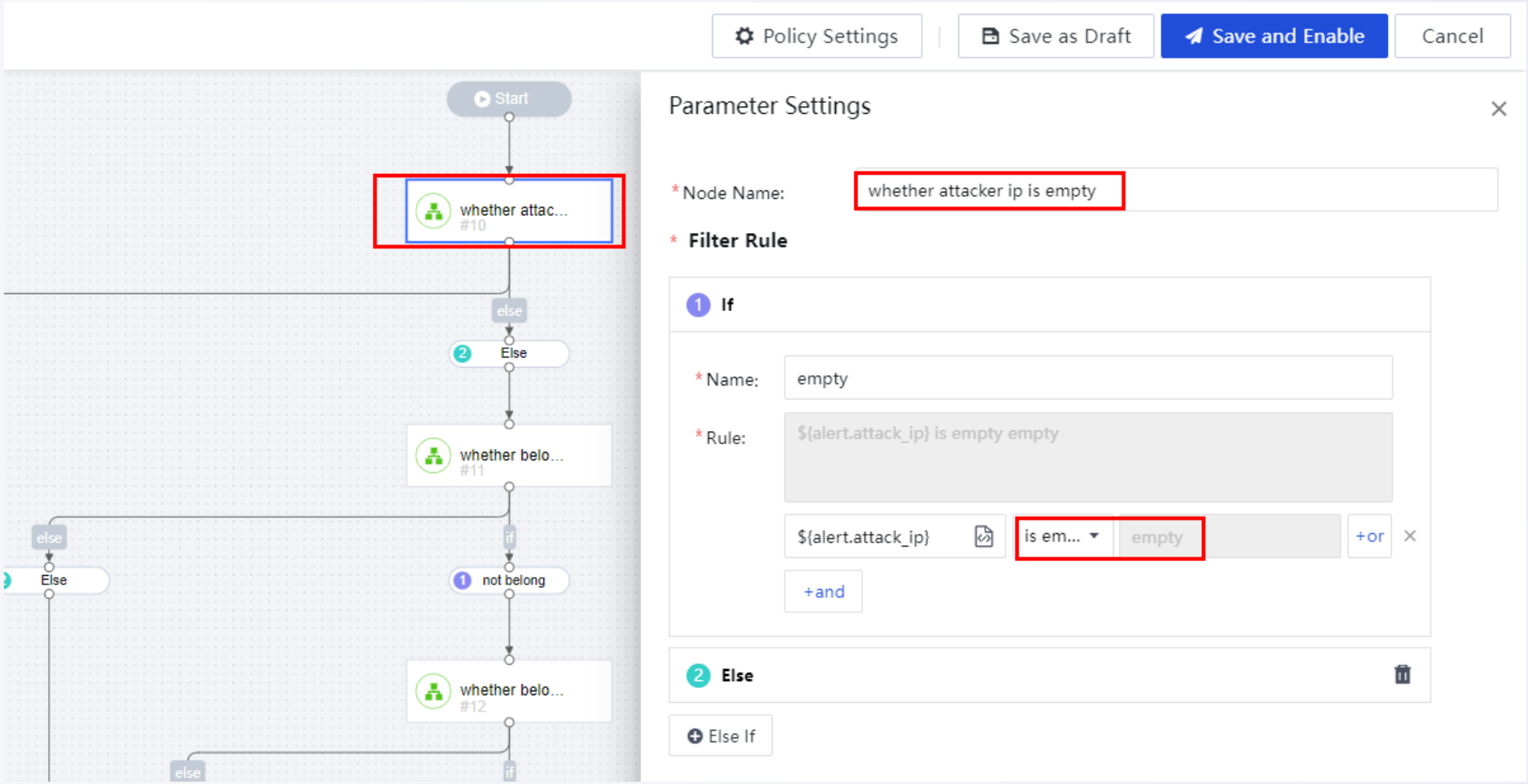
Example 2

Step2:Create a constant and fill in whitelist ip addresses, create another constant and fill in intranet assets ip addresses range;



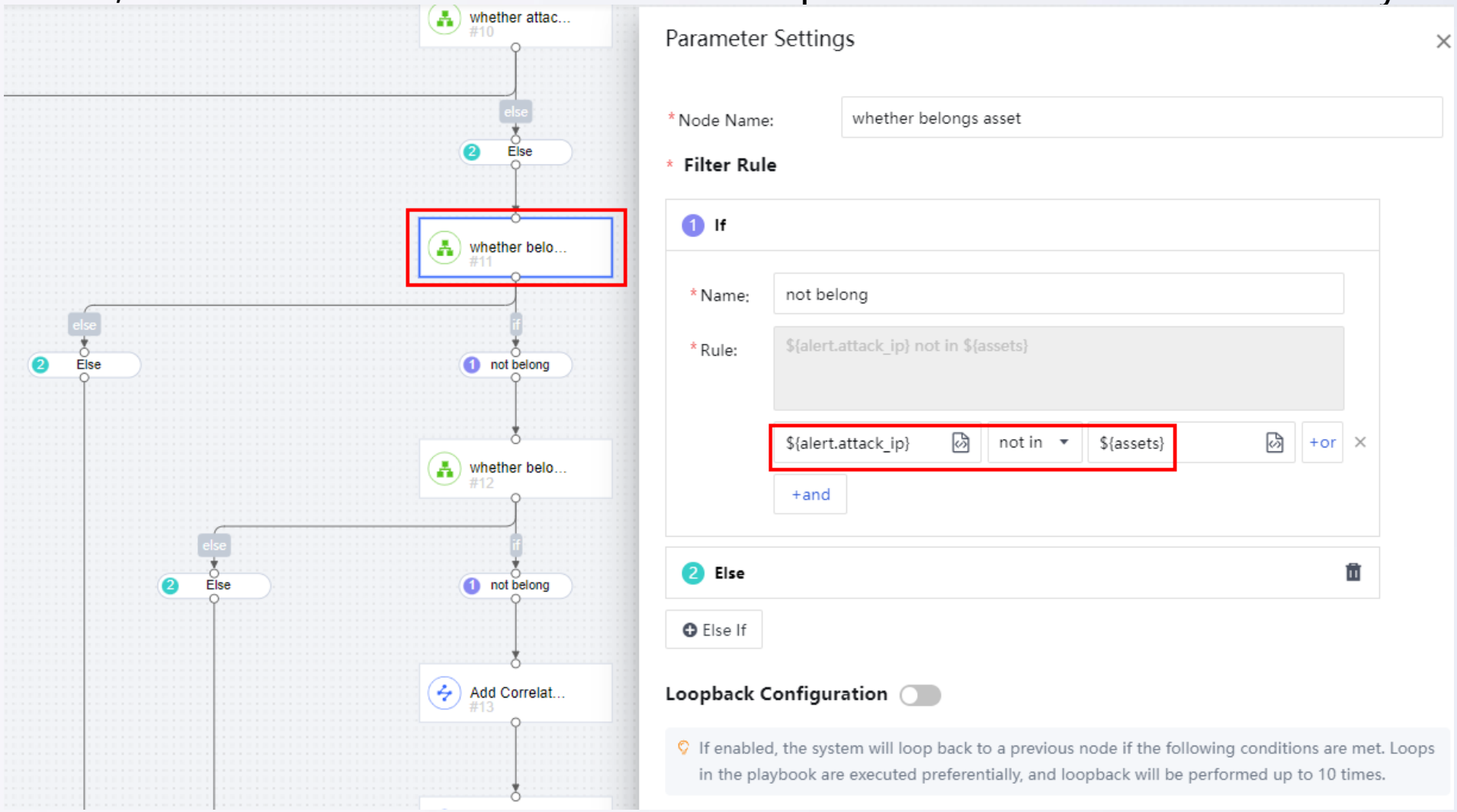
Example 2

Step3: Decision, excludes the case where the attacker ip is an intranet address in security alerts;



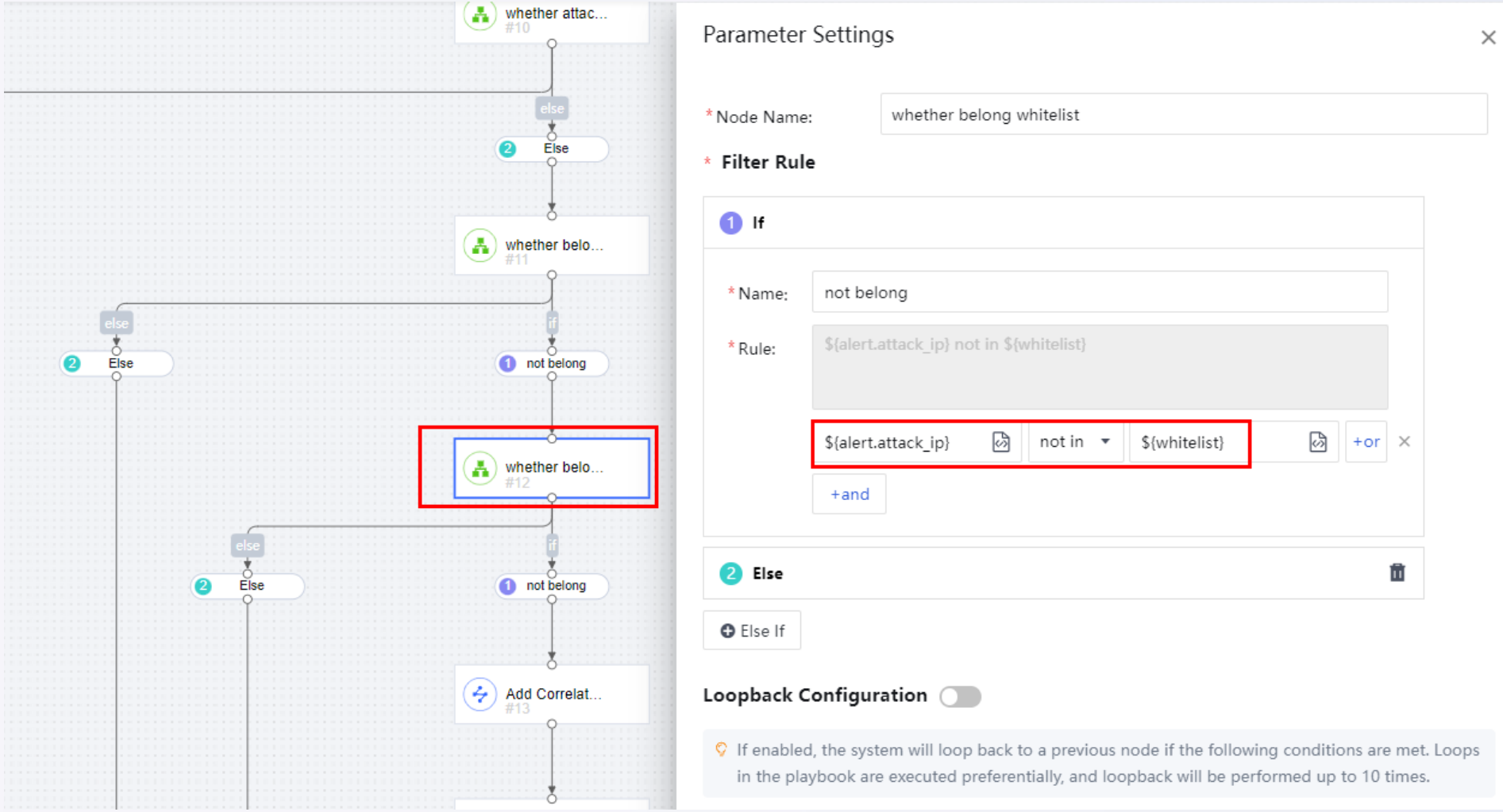
Example 2

Step4: Decision, excludes the case where the attacker ip is an intranet address in security alerts;



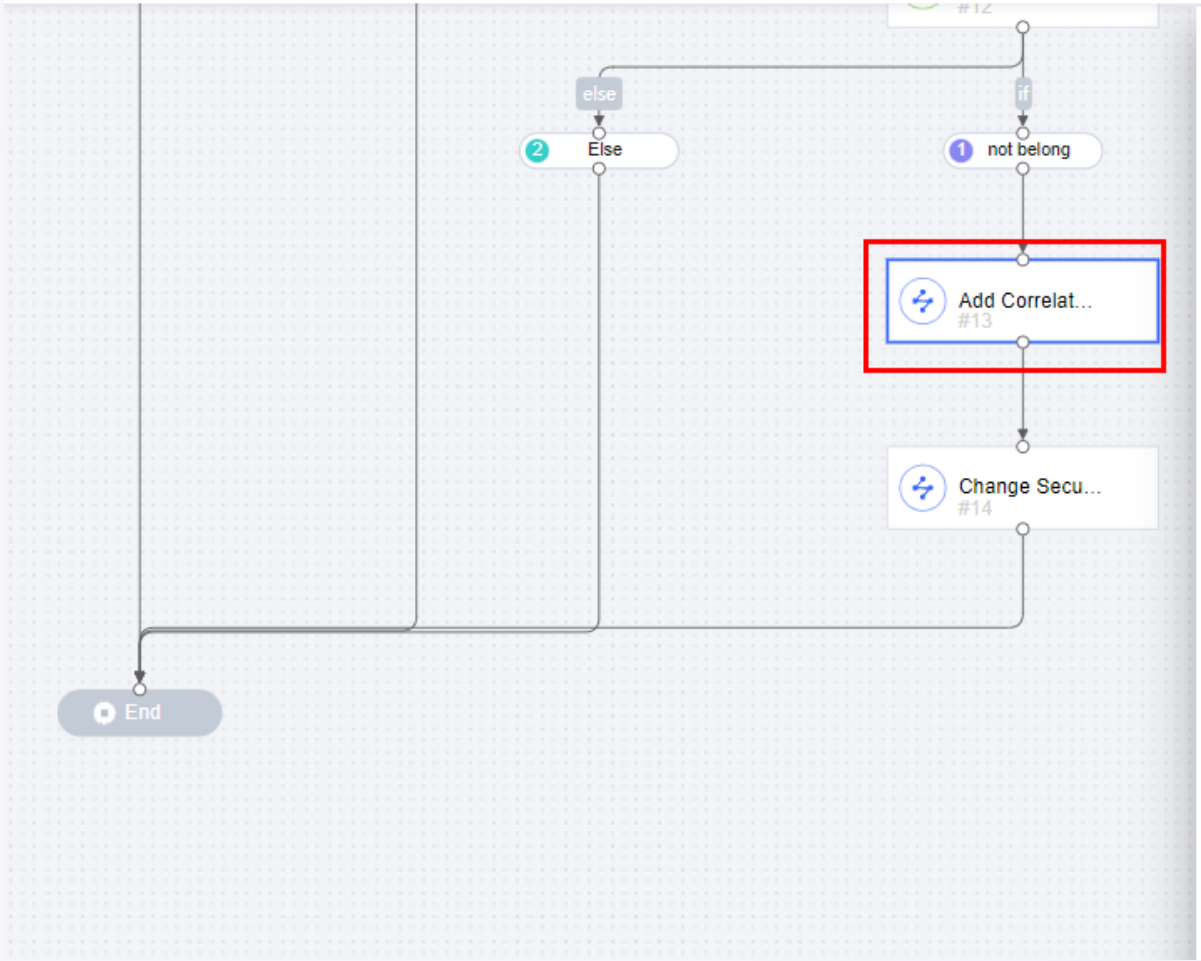
Example 2

Step5: Decision, excludes the situation that the attacker ip is in the white list address in security alerts;



Example 2

Step6: Action, block the attacker's ip address;



Parameter Settings

* Node Name: Add Correlated Block

* Action: Add Correlated Block

* Block Direction: Source and Destination

* Object Type to Block: IP

* Object to Block: ${alert.linkage_recommend.af.block.attack.item}

* Block Duration: -1

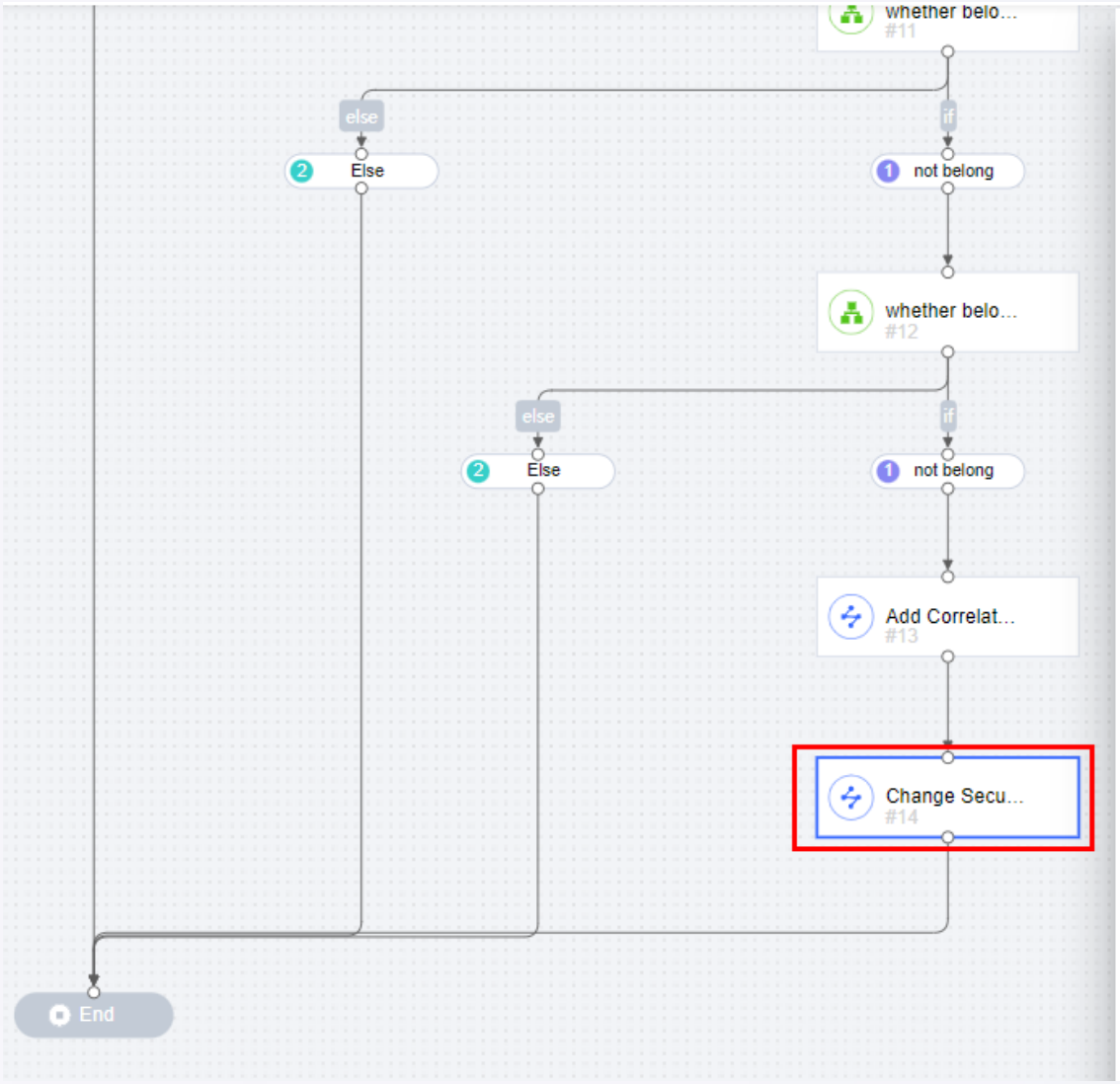
* Block Duration Unit: Day

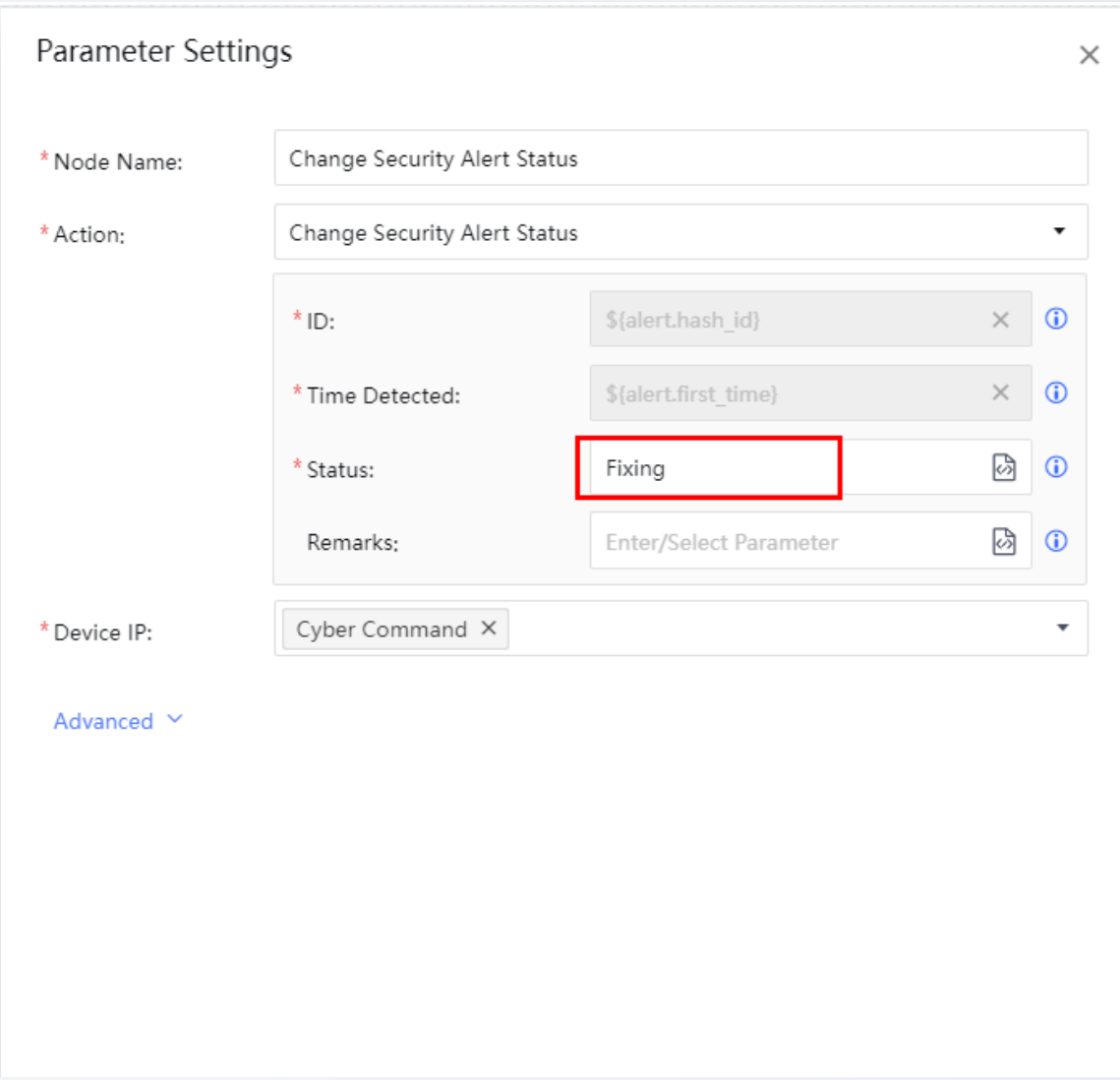
* Device IP: ngaf

Advanced

Example 2

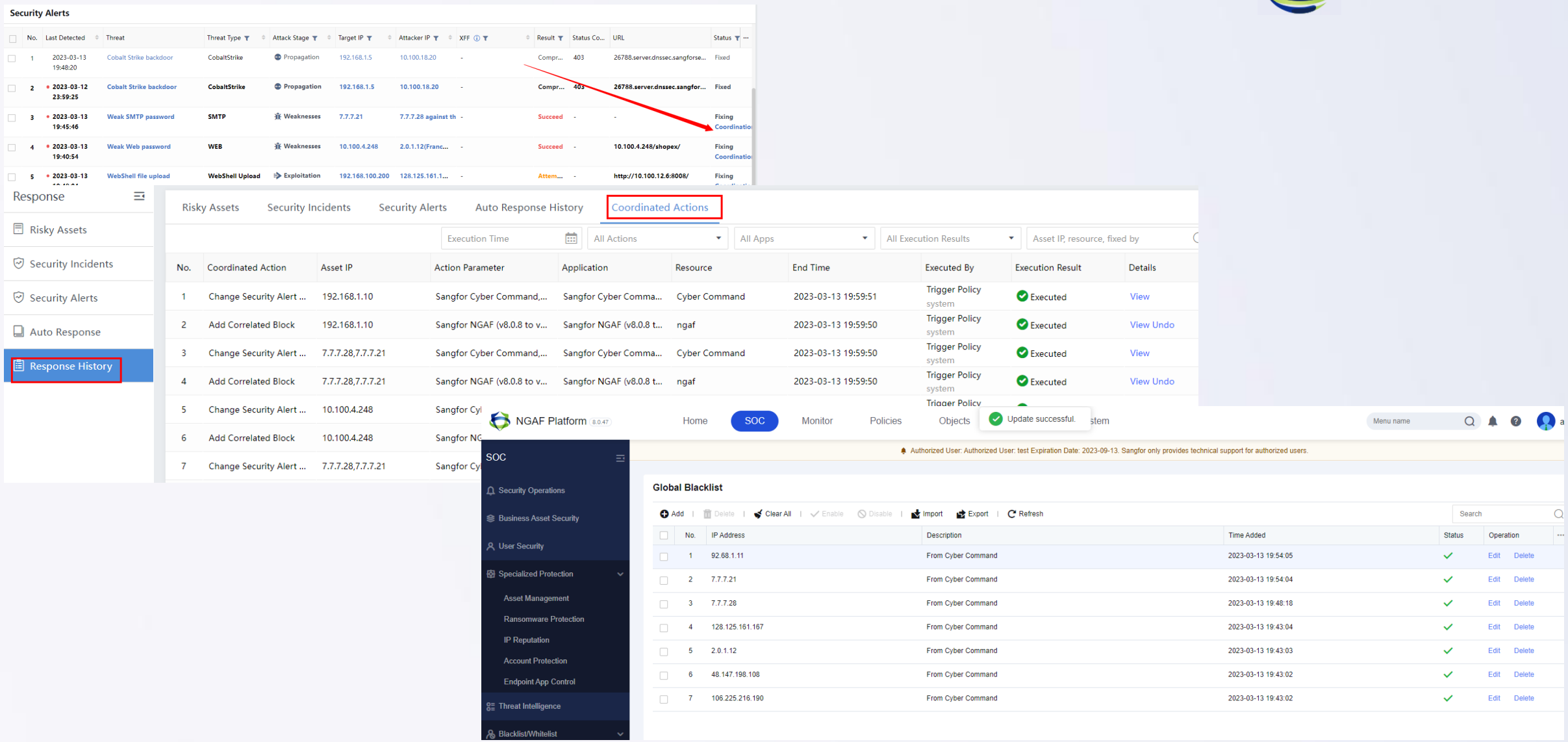
Step7: Action, modify the disposal status of corresponding security alert;





Example 2

Execution results



Example 3

【Background】

A customer found that TOP5 security incidents mainly include bots, trojans and worms through daily intranet operation. The fact is that most intranet assets have been installed ES , customer hopes to implement correlation processing through Cyber Command and ES device. When a security incidentsuch as zombies and worms is detected, it will be disposed by auto response policies . After the disposal is completed, security incidents status will be modified.

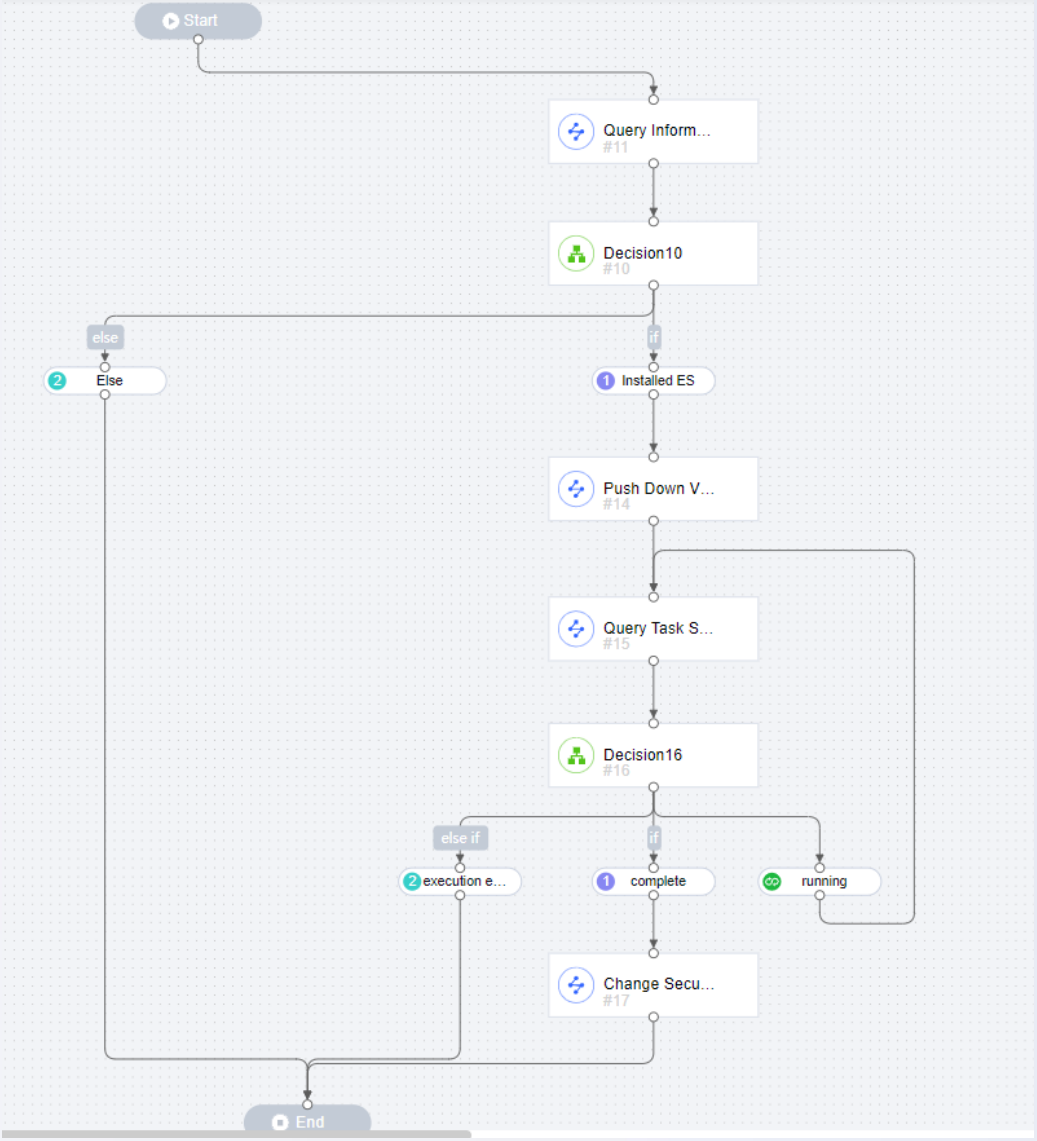
【Method to Achieve】

Firstly, the policy setting delimits the threat classification of bots, trojans and worms. In the process of policy orchestration, it is necessary to judge whether ES is installed. if it is not installed, it will end directly. The assets installed ES will receive virus scan task by Cyber Command. When the task is completed, the disposal status will be turned into fixing or fixed.

Example 3

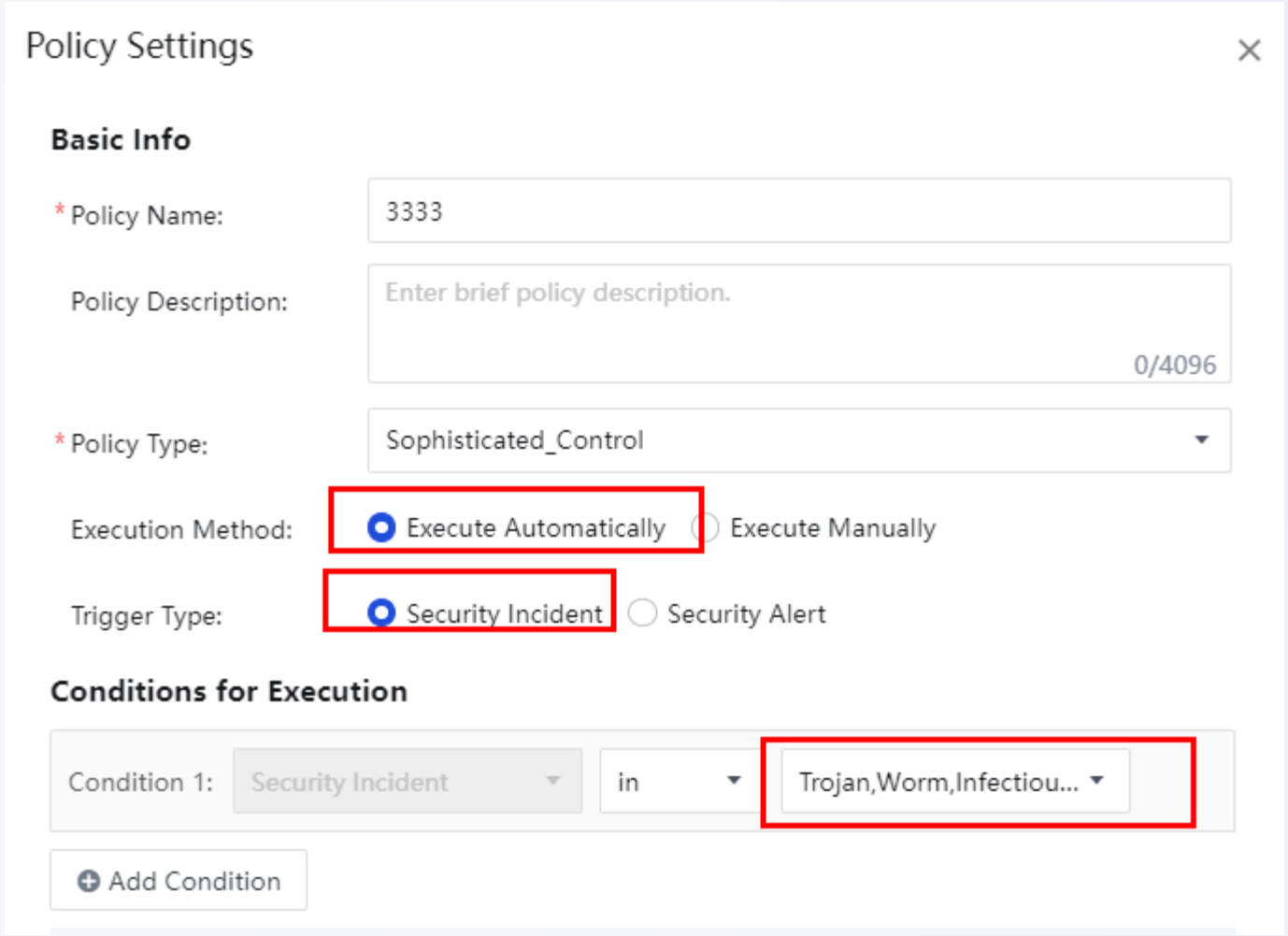
【Method to Achieve】

- **Step1:** Policy setting, automatic execution for security events,select relevant threat classfication;
- **Step2:** Action,query whether the terminal is installed ES client by Cyber Command;
- **Step3:** Decision,the decision ends directly for assets that are not installed ES client, for those installed perform a quick virus scan task;
- **Step4:** Action, push down vircus scan action ;
- **Step5**:Action,since virus scan task last minutes, it is necessary to configure delayed execution time.
- **Step6:** Decision,there are mainly 3 types of outcomes, they are running, execution exception and execution completed. It will go forward next node when it matches execution completed. It will ends directly when it matches execution exception. For running status, it will perform loopback till the task ends;
- **Step7**:Action, modify disposal status of this incident into fixing



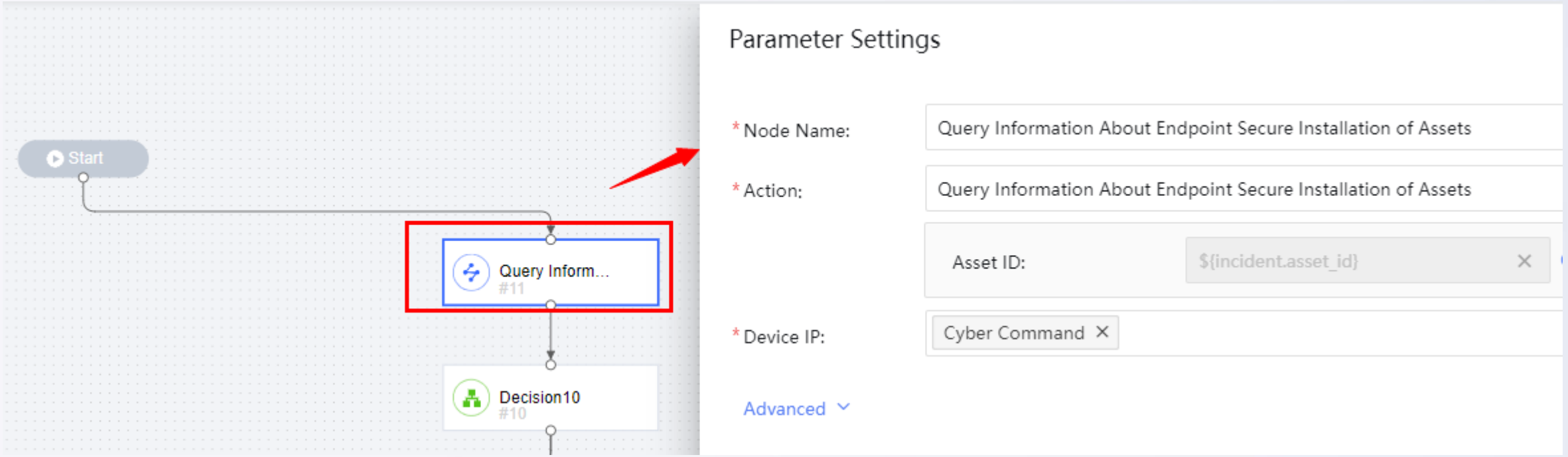
Example 3

- **Step1**： Policy setting, auto policy for security events,select relevant incident threat classfication



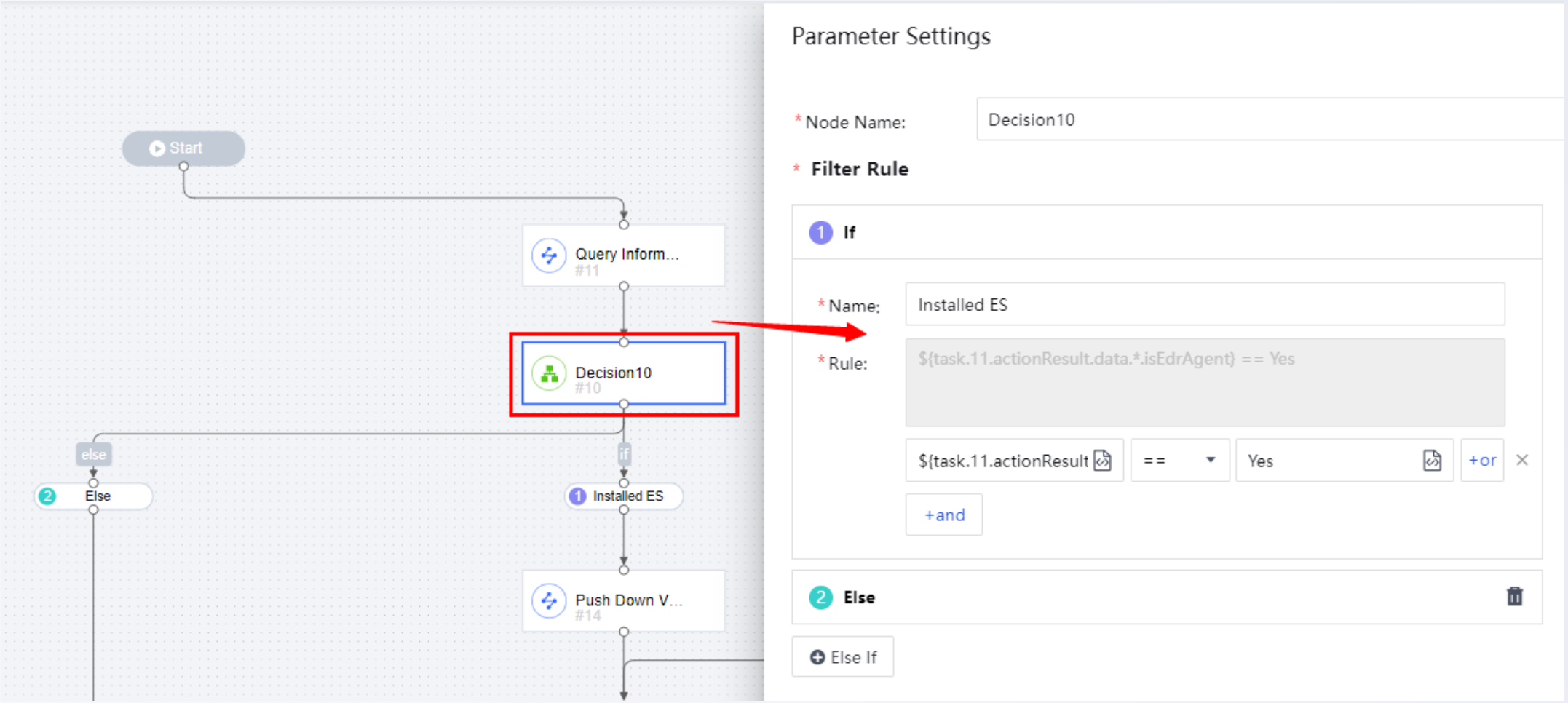
Example 3

- **Step2**： Action,query whether the terminal is installed ES client by Cyber Command



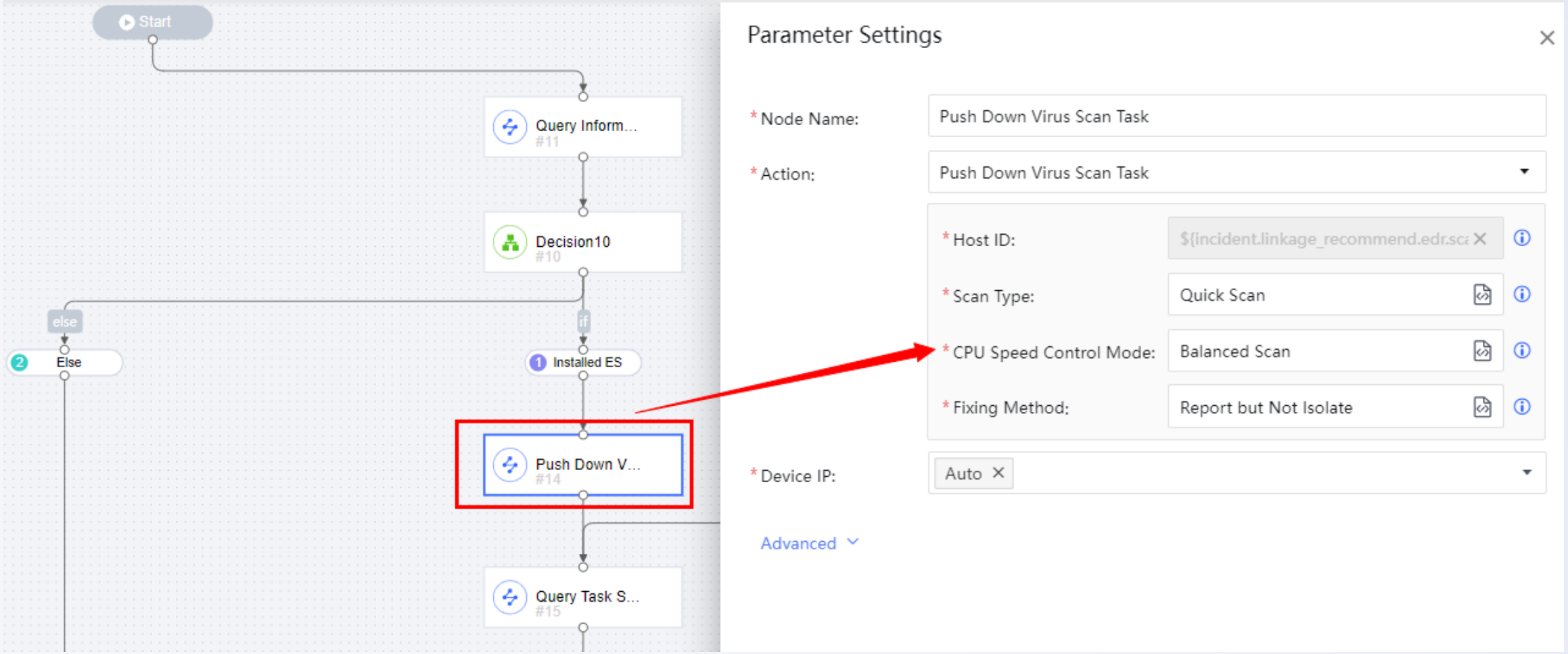
Example 3

- **Step3**：Decision,the filter rule ends directly for assets that are not installed ES client, for those installed perform a quick virus scan task;



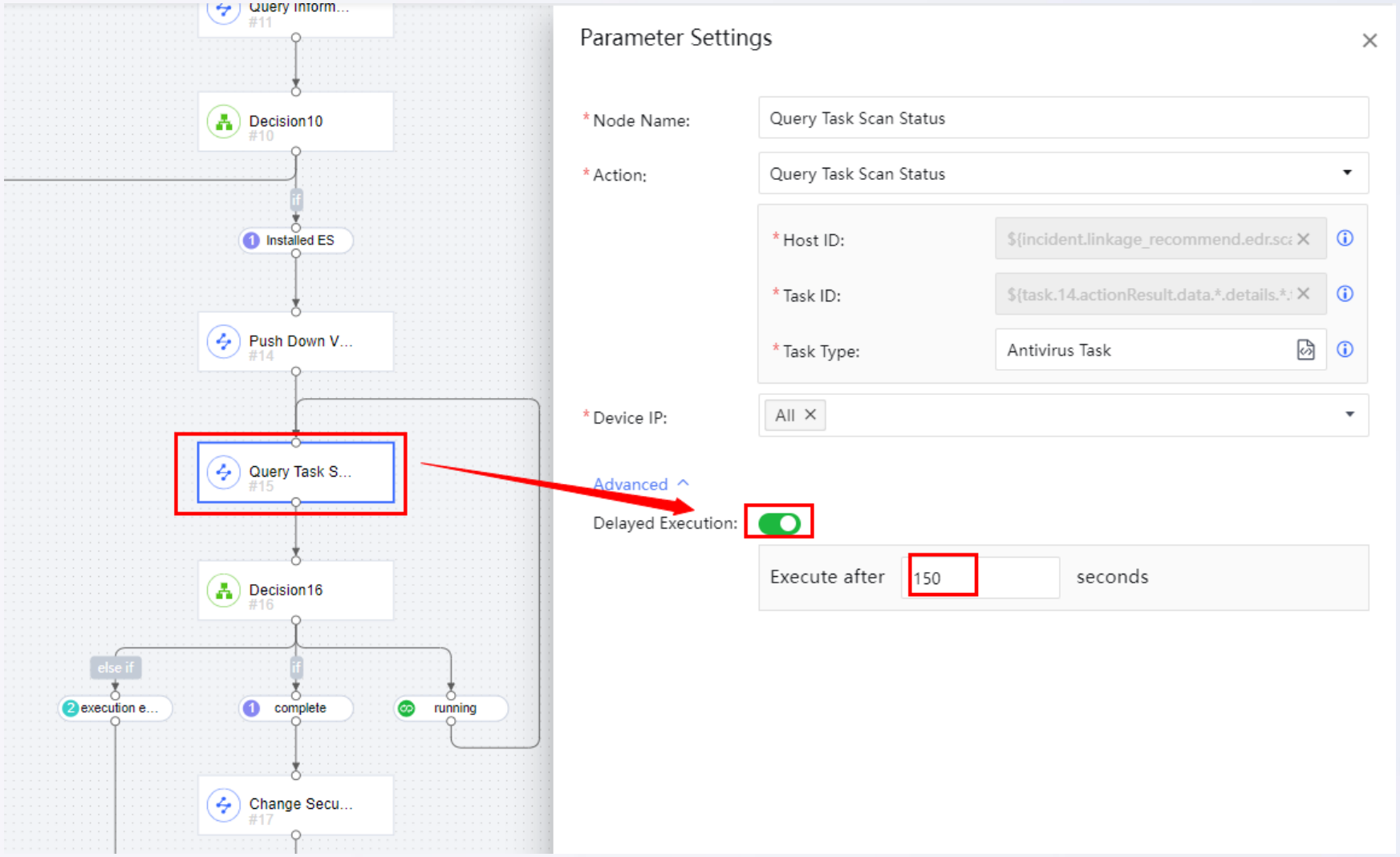
Example 3

- **Step4**: Action, push down vircus scan action ;



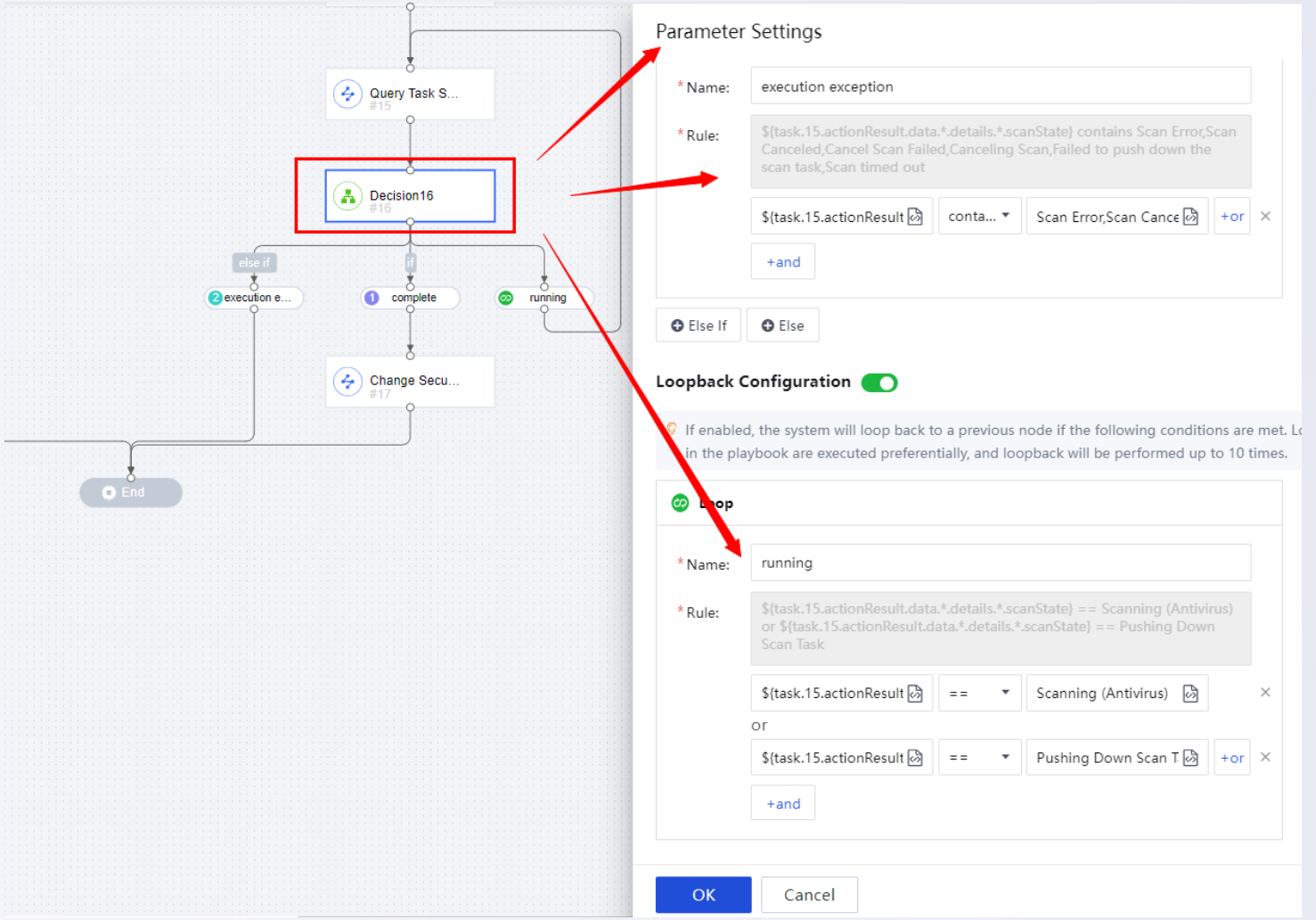
Example 3

- **Step5**:Action,since virus scan task last minutes, it is necessary to configure delayed execution time.



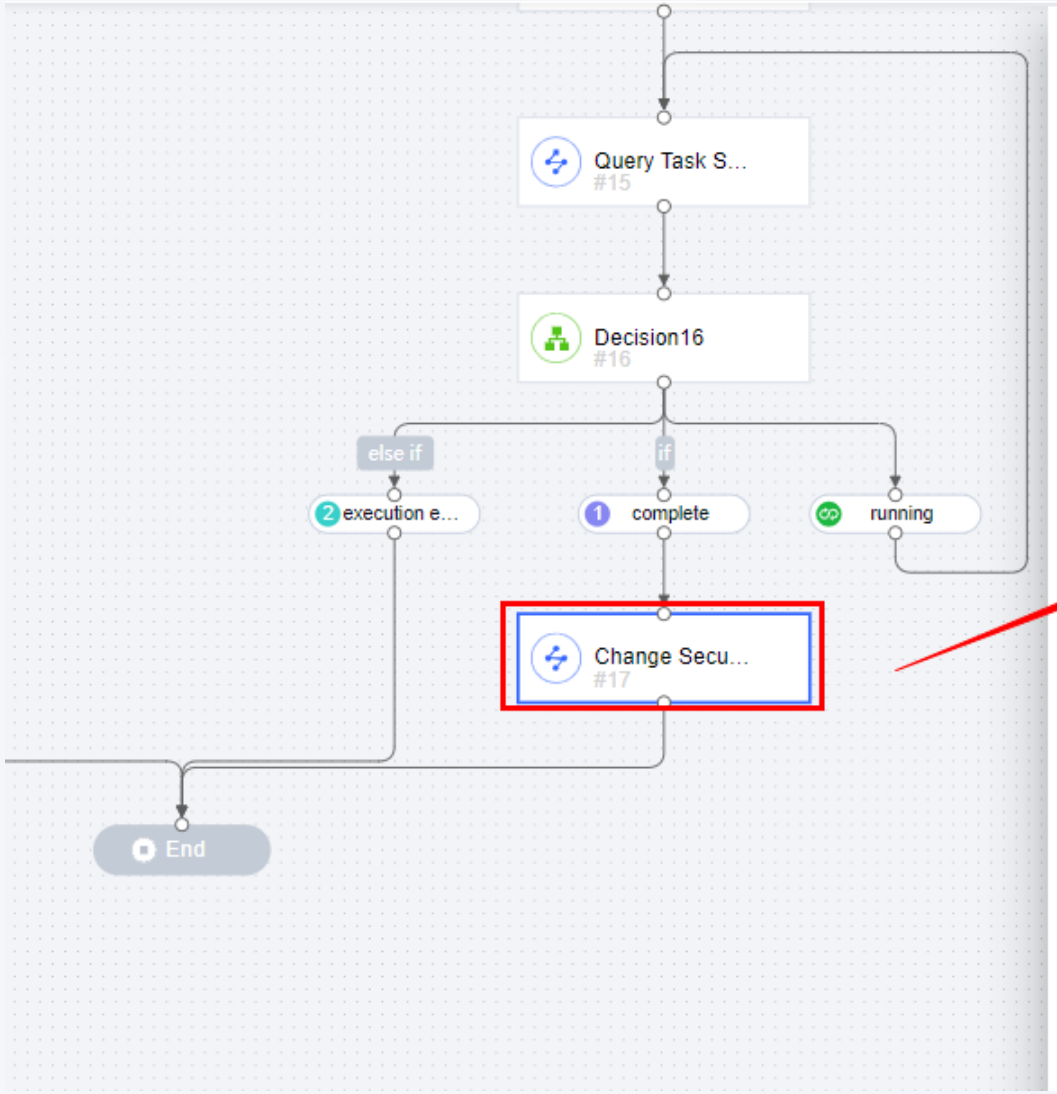
Example 3

- **Step6**:Decision,there are mainly 3 types of outcomes, they are running, execution exception and execution completed. It will go forward next node when it matches execution completed. It will ends directly when it matches execution exception. For running type, it will perform loopback till the end of action.



Example 3

- **Step7**：Action, modify disposal status of this incident into fixing;



Parameter Settings

* Node Name: Change Security Incident Status

* Action: Change Security Incident Status

* ID: ${incident.oid}

* Time Detected: ${incident.first_time}

* Status: Fixing

Remarks: Enter/Select Parameter

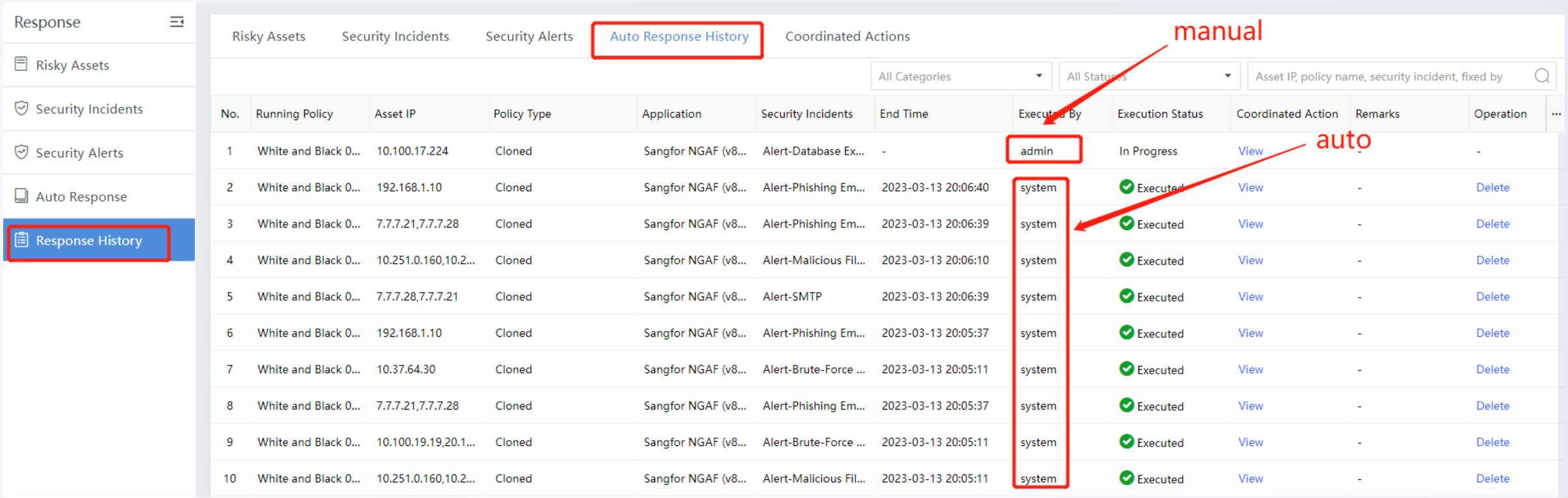
* Device IP: Cyber Command

Advanced

Expended

How we distinguish from auto and manual playbook policies in response history?

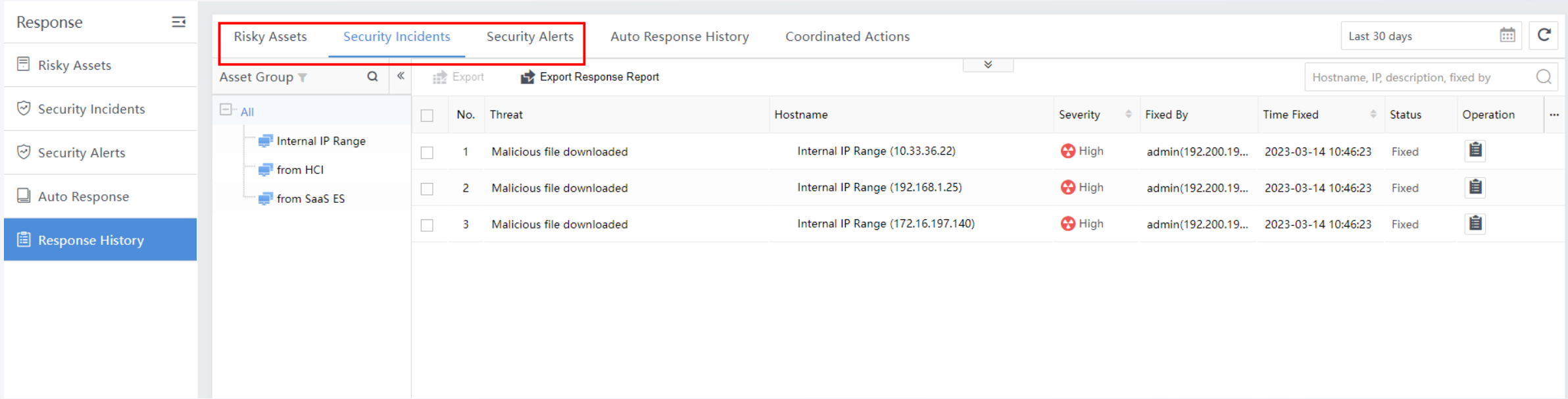
The difference is that executed role in the colum of **executed by**, as it displays below:



Expended

Where we can see the disposal history by hands rather than correlation response?

Here is the page:



Thank you