

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.

App Details

 **Sangfor NGAF (v8.0.8 to v8.0.50)**
Vendor: Sangfor
Application Version: 1.0.59

Sangfor NGAF app (two-way authentication version). Supported versions: NGAF 8.0.8 (included) to NGAF 8.0.50 (excluded). Note: For versions earlier than NGAF 8.0.28, you must install a patch to support Sangfor Cyber Command correlation control, such as SP_AF_KBJG16_02_62-8035.ssu.

◆ Resource Configuration

No.	Resource	Description	Device IP	Device Port	Username
 No data available.					

◆ Response Action

No.	Name	Description	Category
1	Add Access Control	Add access control. Cyber Com...	Access
2	Remove Access Control	Remove access control. Batch r...	Undo
3	Edit Access Control	Edit access control: Cyber Com...	Update
4	Add Correlated Block	Block multiple IP addresses, do...	Access
5	Remove Correlated Block	Delete multiple blocked IP addr...	Undo

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 policy: 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.

The screenshot displays the Sangfor security management interface. On the left, the 'Response Apps' section shows various Sangfor devices (Cyber Command, IAG, IAM, HCI, NGAF, Network Controller) and third-party devices (Cisco ASA Firewall, Macmon NAC, WatchGuard, Bitdefender). A red arrow points to the 'App' label. The 'App Details' panel on the right shows 'Sangfor NGAF (v8.0.8 to v8.0.50)' with a resource configuration table. A red box highlights the 'DC-AF', 'Internet-AF', and 'Internal-AF' resources. A red arrow points to these resources with the text '3 resources under NGAF App'. The 'Policies' section shows a list of policies, with a red box highlighting the first three: 'White and Black 0513', 'Block Source IP - Predefined', and 'Access Control - Predefined'.

No.	Resource	Description	Device IP	Device Port	Username
1	DC-AF	-	1.1.1.1	-	test
2	Internet-AF	-	1.1.10.1	-	test
3	Internal-AF	-	1.1.20.1	-	test

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

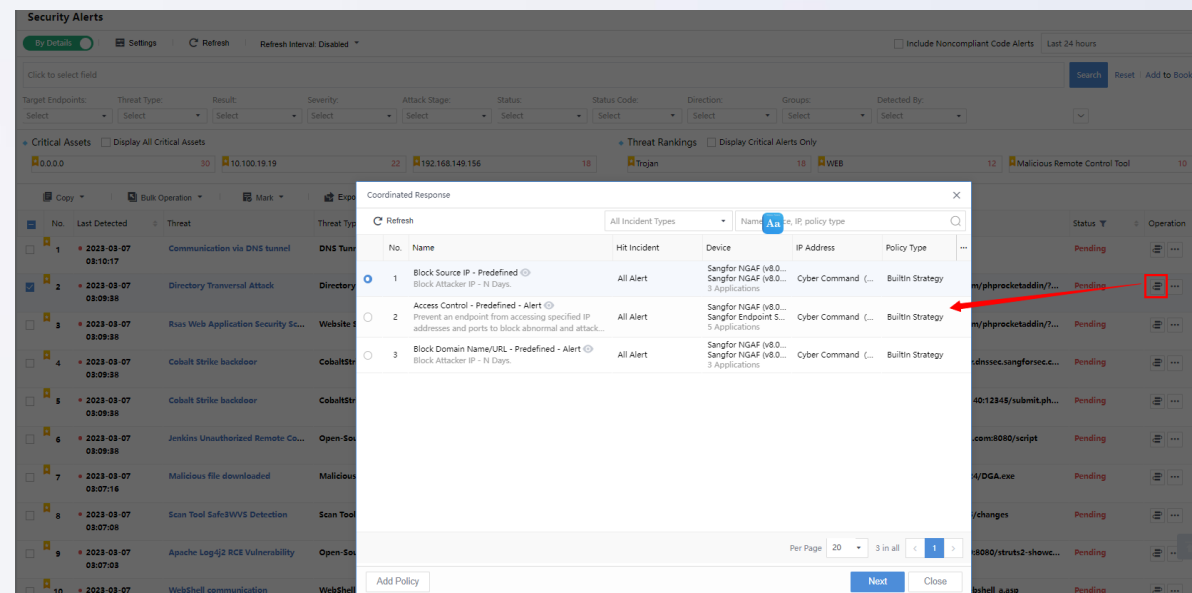


5、Which pages in Cyber Command can trigger response policies?

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 scenarios, some inaccurate policies can lead to considerable unexpected blocks;

Extended questions:

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

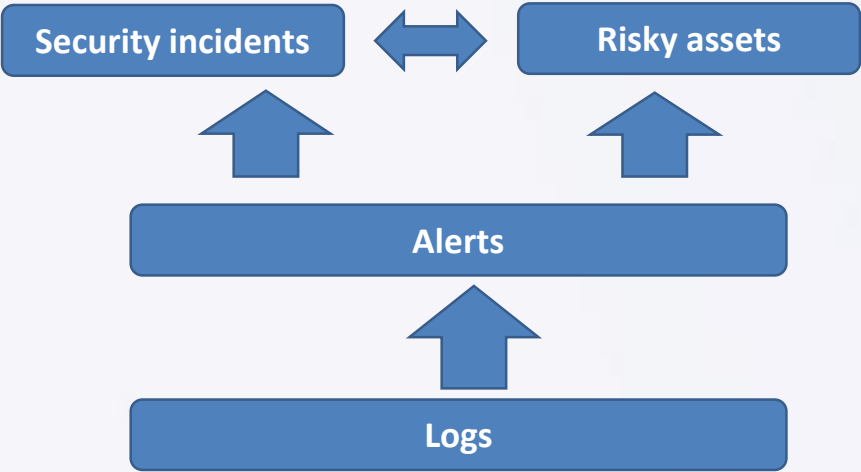
2. Shall we configure auto policies directly and execute them in a large scale without a period of verification?

A screenshot of the "Policy Settings" window in a Sangfor management console. The window has a title bar with a close button (X). It is divided into two main sections: "Basic Info" and "Conditions for Execution". In the "Basic Info" section, there are fields for "Policy Name" (containing "Unnamed Policy"), "Policy Description" (with a placeholder "Enter brief policy description." and a character count "0/4096"), "Policy Type" (a dropdown menu showing "Select"), "Execution Method" (with two radio buttons: "Execute Automatically" which is selected and highlighted with a red box, and "Execute Manually"), and "Trigger Type" (with two radio buttons: "Security Incident" and "Security Alert" which is selected). The "Conditions for Execution" section shows a single condition: "Condition 1: Security Alert in Select", where "Security Alert" and "in" are dropdown menus and "Select" is a text input field. Below this is a button labeled "+ Add Condition". At the bottom, there is a light blue informational box with a question mark icon and text explaining that a condition with multiple values is met when one value is matched, and a playbook with multiple conditions is executed when all conditions are met.

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*).



Policy Settings

Basic Info

* Policy Name:

Unnamed Policy

Policy Description:

Enter brief policy description.

0/4096

* Policy Type:

Select

Execution Method:

☒ Execute Automatically

☐ Execute Manually

Trigger Type:

☒ Security Incident

☐ Security Alert

Conditions for Execution

Condition 1:

Security Incident

in

Select

Add Condition

A condition that contains multiple values is met when one of the values is matched. A playbook that contains multiple conditions is executed when all the conditions are met.

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 either 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



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

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

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

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

Threats	Hit Rules	Attacker Analysis	<u>Risky Assets</u>	Recommendations			
Bulk Operation		Export		All Statuses			
<input type="checkbox"/>	No.	Risky Assets	Type	Threat Detections	Last Detected	Status	Operation
<input type="checkbox"/>	1	Internal IP Range (10.5.2.101) Internal IP Range	Host	29110	2023-03-09 14:52:15	Suspended	
<input type="checkbox"/>	2	Internal IP Range (192.168.149.156) Internal IP Range	Host	181521	2023-03-09 14:52:15	Suspended	
<input type="checkbox"/>	3	Internal IP Range (10.1.27.101) Internal IP Range	Host	1	2023-02-21 13:31:07	Suspended	
<input type="checkbox"/>	4	jeremiah.rogan (10.1.11.101) Internal IP Range	Host	2	2023-02-21 13:30:41	Suspended	
<input type="checkbox"/>	5	Internal IP Range (10.12.29.101) Internal IP Range	Host	1	2023-02-21 13:29:30	Pending	

Threats	Hit Rules	Attacker Analysis	Risky Assets	Recommendations			
Bulk Operation		Export		All Statuses			
<input type="checkbox"/>	No.	Risky Assets	Type	Threat Detections	Last Detected	Status	Operation
<input type="checkbox"/>	1	Internal IP Range (10.5.2.101) Internal IP Range	Host	29114	2023-03-09 14:52:15	Fixing	
<input type="checkbox"/>	2	Internal IP Range (192.168.149.156) Internal IP Range	Host	181521	2023-03-09 14:52:15	Fixing	
<input type="checkbox"/>	3	Internal IP Range (10.1.27.101) Internal IP Range	Host	1	2023-02-21 13:31:07	Fixing	
<input type="checkbox"/>	4	jeremiah.rogan (10.1.11.101) Internal IP Range	Host	2	2023-02-21 13:30:41	Fixing	
<input type="checkbox"/>	5	Internal IP Range (10.12.29.101) Internal IP Range	Host	1	2023-02-21 13:29:30	Suspended	

Threats		Hit Rules	Attacker Analysis	Risky Assets	Recommendations		
Bulk Operation		Export			All Statuses		
	No.	Risky Assets	Type	Threat Detections	Last Detected	Status	Operations
<input type="checkbox"/>	1	Internal IP Range (10.5.2.101) Internal IP Range	Host	29114	2023-03-09 14:55:32	Fixed	
<input type="checkbox"/>	2	Internal IP Range (192.168.149.156) Internal IP Range	Host	181535	2023-03-09 14:55:32	Fixed	
<input type="checkbox"/>	3	Internal IP Range (10.1.27.101) Internal IP Range	Host	1	2023-02-21 13:31:07	Fixed	
<input type="checkbox"/>	4	jeremiah.rogan (10.1.11.101) Internal IP Range	Host	2	2023-02-21 13:30:41	Fixed	
<input type="checkbox"/>	5	Internal IP Range (10.12.29.101) Internal IP Range	Host	1	2023-02-21 13:29:30	Fixing	

Threats		Hit Rules	Attacker Analysis	Risky Assets	Recommendations		
<div><div>Bulk Operation</div><div>Export</div></div>					All Statuses		
	No.	Risky Assets	Type	Threat Detections	Last Detected	Status	Ops
<input type="checkbox"/>	1	Internal IP Range (10.5.2.101) Internal IP Range	Host	29114	2023-03-09 14:55:32	Fixed	
<input type="checkbox"/>	2	Internal IP Range (192.168.149.156) Internal IP Range	Host	181535	2023-03-09 14:55:32	Fixed	
<input type="checkbox"/>	3	Internal IP Range (10.1.27.101) Internal IP Range	Host	1	2023-02-21 13:31:07	Fixed	
<input type="checkbox"/>	4	jeremiah.rogan (10.1.11.101) Internal IP Range	Host	2	2023-02-21 13:30:41	Fixed	
<input type="checkbox"/>	5	Internal IP Range (10.12.29.101) Internal IP Range	Host	1	2023-02-21 13:29:30	Fixed	

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.

Response

Risky Assets

Security Incidents

Security Alerts

Auto Response

Response History

Risky Assets

Status: Select Risk Level: Select Endpoint Secure: Select Period: Last 30 days IP, IP range, tag, hostname: Search

All Risky Assets My Concerns

60 All 0 Server 60 Host 0 Recurring 0 New Today 56 Compromised Assets 0 Critical Assets 1 Ransomware 2 EternalBlue

Bulk Operation Export Auto Fix

No.	Hostname	Type	Risk Level	Security Incidents	Last Detected	Endpoint Secure	Status	Operation
1	Internal IP Range (172.16.197.140)	Host	Compromised	CobaltStrike Malicious file	2023-03-13 03:09:39	Not installed	Pending	
2	Internal IP Range (10.100.18.20)	Host	Compromised	CobaltStrike	2023-03-13 03:09:39	Not installed	Pending	
3	Internal IP Range (192.168.16.13)	Host	Compromised	Ramnit ramnit worm	2023-03-13 03:07:05	Not installed	Pending	
4	Internal IP Range							
5	Internal IP Range							
6	Internal IP Range							
7	Internal IP Range							
8	Internal IP Range							
9	Internal IP Range							

Risk Details

Internal IP Range (172.16.197.140)

Endpoint Secure: Not installed Risk Level: Compromised Type: Host Status: Pending

Timeline

Stages of Attack

Weaknesses Reconnaissance Exploitation C&C Propagation Impact

Incidents

Export

No.	Threat	Direction	Severity	Attack Stage	Detected By	Last Detected	Status	Operation
1	Cobalt Strike backdoor	Source	High	Propagation	SANGFOR STA(192.168.20.189)	2023-03-13 03:09:39	Pending	
2	Malicious file downloaded	Source	High	Propagation	SANGFOR STA(192.168.20.189)	2023-03-12 03:11:28	Pending	

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.

Security Alerts													
<div>By Details <input checked="" type="radio"/> Settings Refresh Refresh Interval: Disabled <input type="checkbox"/> Include Noncompliant Code Alerts Last 24 hours</div>													
<div>Click to select field Search Reset Add to Bookmarks</div>													
<div>Target Endpoints: Select Threat Type: Select Result: Select Severity: Select Attack Stage: Select Status: Select Status Code: Select Direction: Select Groups: Select</div>													
<div>Critical Assets No critical assets configured. Configure Now Threat Rankings Display Critical Alerts Only Trojan 18 Malicious File Download 14 OS Kernel Exploit 11</div>													
<div>Copy Bulk Operation Mark Export Open Monitor</div>													
No.	Last Detected	Threat	Threat Type	Attack Stage	Target IP	Attacker IP	XFF	Result	Status Co...	URI	Status	Operati...	
1	2023-03-13 03:11:45	Communication via DNS tunnel	DNS Tunneling	C&C	10.1.1.1	-	-	Compr...	-	-	Pending		
2	2023-03-13 03:09:39	Cobalt Strike backdoor	CobaltStrike	Propagation	172.16.197.133	172.16.197.140	-	Compr...	200	172.16.197.140:12345/submit.p...	Pending		
3	2023-03-13 03:09:39	Cobalt Strike backdoor	CobaltStrike	Propagation	192.168.1.5	10.100.18.20	-	Compr...	403	26788.server.dnssec.sangforsec...	Fixed		
4	2023-03-13 03:09:39	General System Command Inj...	System Comman...	Exploitation	10.100.19.194	2.0.1.19(France)	-	Failed	-	10.100.19.194:8080/48972f4...	Pending		
5	2023-03-13 03:09:39	Apache Log4j2 RCE Vulnerabi...	Open-Source and...	Propagation	172.20.64.50	10.251.0.93 against	-	Attem...	200	172.20.64.50:8080/struts2-sh...	Pending		

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.

Security Incidents

Groups

All

Internal IP Range

from SaaS ES

from HCI

Incidents (58 in Total)

Stages of Attack

Weaknesses

Reconnaissance

Exploitation

C&C

Propagation

Export

No.	Threat	Risky Assets	Severity	Attack Stage	Threat Type	Last Detected	Status
1	General system command injection attack		8 High	Propagation	System Comman...	2023-03-13 02:15:57	Pending
2	[Behinder]Godzilla JSP communication		6 High	Propagation	WebShell Access	2023-03-13 02:48:15	Pending
3	Malicious file downloaded		5 High	Exploitation	Malicious File Do...	2023-03-13 02:16:10	Pei
4	Cobalt Strike backdoor		4 High	Propagation	CobaltStrike	2023-03-13 03:09:39	Pei

Security Alerts

By Details

Settings

Refresh

Refresh Interval: Disabled

Include Noncompliant Code Alerts

Last 24 hours

Click to select field

Search

Reset

Add to Bookmar...

Target Endpoints

Threat Types

Result

Severity

Attack Stages

Status

Status Code

Direction

Groups

Critical Assets

No critical assets configured. Configure Now

Threat Rankings

Display Critical Alerts Only

Trojan

18

Malicious File Download

14

OS Kernel Exploit

11

Copy

Bulk Operation

Mark

Export

Open Monitor

No.	Last Detected	Threat	Threat Type	Attack Stage	Target IP	Attacker IP	XFF	Result	Status Co...	URL	Status	Operati...
1	2023-03-13 03:11:45	Communication via DNS tunnel	DNS Tunneling	C&C	10.1.1.1	-	-	Compr...	-	-	Pending	...
2	2023-03-13 03:09:39	Cobalt Strike backdoor	CobaltStrike	Propagation	172.16.197.133	172.16.197.140	-	Compr...	200	172.16.197.140:12345/submit.p...	Pending	...
3	2023-03-13 03:09:39	Cobalt Strike backdoor	CobaltStrike	Propagation	192.168.1.5	10.100.18.20	-	Compr...	403	26788.server.dnssec.sangforsec...	Pending	...
4	2023-03-13 03:09:39	General System Command Inj...	System Comman...	Exploitation	10.100.19.194	2.0.1.19(France)	-	Failed	-	10.100.19.194:8080/48972f4...	Pending	...

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;

	No.	Name	Associated Threat Type	Execution Method	Device	IP Address	Status	Time Updated	...
<input type="checkbox"/>	1	Threat Scan - Predefined Start a full/quick scan and block/trust detected...	All Incident	Manual	Sangfor Endpoint Secure Sangfor Cyber Command and 3Application	Cyber Command (127.0.0...	<input checked="" type="checkbox"/> Enabled	2023-03-02 16:42:12	
<input type="checkbox"/>	2	Block Source IP - Predefined Block Attacker IP - N Days.	All Alert	Manual	Sangfor NGAF (v8.0.50 an... Sangfor NGAF (v8.0.8 to v... and 3Application	Cyber Command (127.0.0... Internal-AF (1.1.20.1) and 4Application	<input checked="" type="checkbox"/> Enabled	2023-01-10 11:12:44	
<input type="checkbox"/>	3	Access Control - Predefined Prevent an endpoint from accessing specified IP...	All Incident	Manual	Sangfor NGAF (v8.0.50 an... Sangfor Endpoint Secure and 5Application	Cyber Command (127.0.0... Internal-AF (1.1.20.1) and 4Application	<input checked="" type="checkbox"/> Enabled	2023-01-10 11:12:44	
<input type="checkbox"/>	4	Endpoint Lockout - Predef... If you use a Sundray AP or Sundray switch for...	All Incident	Manual	Sangfor Network Controller Sangfor Cyber Command	Cyber Command (127.0.0...	<input checked="" type="checkbox"/> Enabled	2023-01-10 11:12:44	
<input type="checkbox"/>	5	Browsing Risk Notification... Users will be notified of endpoint risks when they...	All Incident	Manual	Sangfor IAM Sangfor IAG	-	<input checked="" type="checkbox"/> Enabled	2023-01-10 11:12:44	
<input type="checkbox"/>	6	Account Lockout - Predefi... Block communication between infected endpoin...	All Incident	Manual	Sangfor IAM Sangfor IAG and 3Application	Cyber Command (127.0.0...	<input checked="" type="checkbox"/> Enabled	2023-01-10 11:12:44	

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 possibility:** 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 Change Risky Endpoint 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 no effect on the linkage strategy.
2	Security Incidents	\${incident.asset_id}	Asset ID	46	int	Asset ID	Cyber Command	Obtain Asset Scan Information Obtain Asset Virus Status in Endpoint Secure	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	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 Status of Malicious Processes	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 is not taken
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 security events is called directly, it is not taken
7	Security Incidents	\${incident.linkage_recommend.common.src_port}	Src Port	[443]	Array	Src Port	Integrated Device		Under normal circumstances, the aggregation of the port in the relevant security log is taken //Unavailable, when the linkage blockade of security events is called directly, it is not taken //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;

Block Source IP - Predefined-1672945826638-copy

Nodes

Constants

1 Constants

Add

Edit Constant

Name:

test

Parameter:

20.10.0.39

OK

Cancel

Parameter Settings

* Node Name:

Add Correlated Block

* Action:

Add Correlated Block

* Block Direction:

Source

* Object Type to Block:

IP

* Object to Block:

`\${custom.2}`

* Block Duration:

1

* Block Duration Unit:

Day

* Device IP:

192.168.20.130

Temporary Blacklist

+ Add

Delete

Clear All

Add to Global Blacklist

<input type="checkbox"/>	Address Type	Address	Dst Port
<input type="checkbox"/>	Src IP	20.10.0.39	-

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;

Parameter Settings

* Node Name:

Add Correlated Block

* Action:

Add Correlated Block

* Block Direction:

Source

* Object Type to Block:

IP

* Object to Block:

20.10.0.39

* Block Duration:

1

* Block Duration Unit:

Day

* Device IP:

192.168.20.130

Advanced

Temporary Blacklist

+ Add

🗑 Delete

🧹 Clear All

📁 Add to Global Blacklist

<input type="checkbox"/>	Address Type	Address	Dst Port
<input type="checkbox"/>	Src IP	20.10.0.39	-

Copyright © 2023 Sangfor Technology Co., Ltd.

Page19

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】

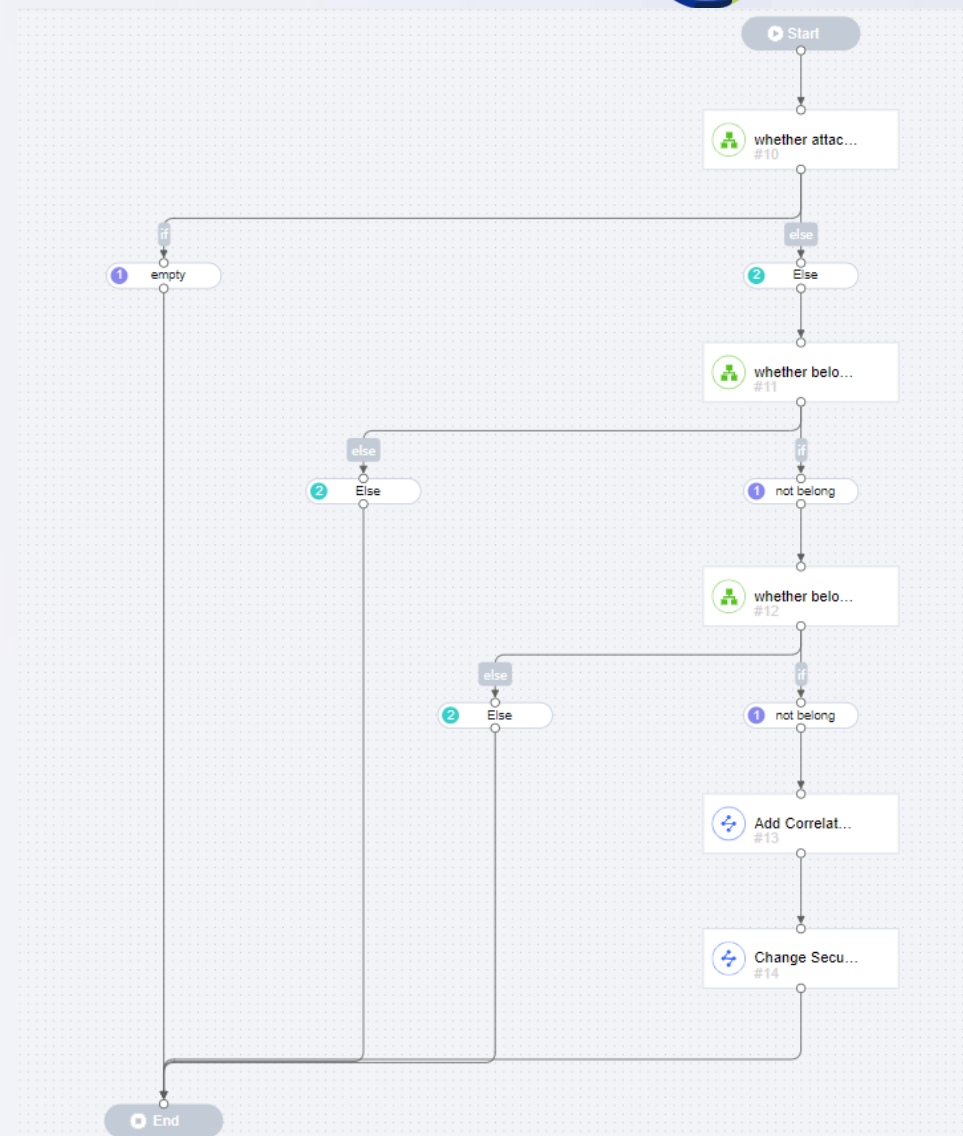
According to the requirement, firstly, we have the common concept that this policy should be oriented to security alerts and be automatic,and then define a constant including all ip addresses. The key action is blocking by NGAF, but we should consider some necessary check before it performs, for example, 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 beginning*)
- **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;

Policy Settings

Basic Info

* Policy Name:

White and Black 0313

Policy Description:

Enter brief policy description.

0/4096

* Policy Type:

Cloned

Execution Method:

☒ Execute Automatically

☐ Execute Manually

Trigger Type:

☐ Security Incident

☒ Security Alert

Conditions for Execution

Condition 1:

Security Alert

in

All

+

Add Condition

ⓘ

A condition that contains multiple values is met when one of the values is matched. A playbook that contains multiple conditions is executed when all the conditions are met.

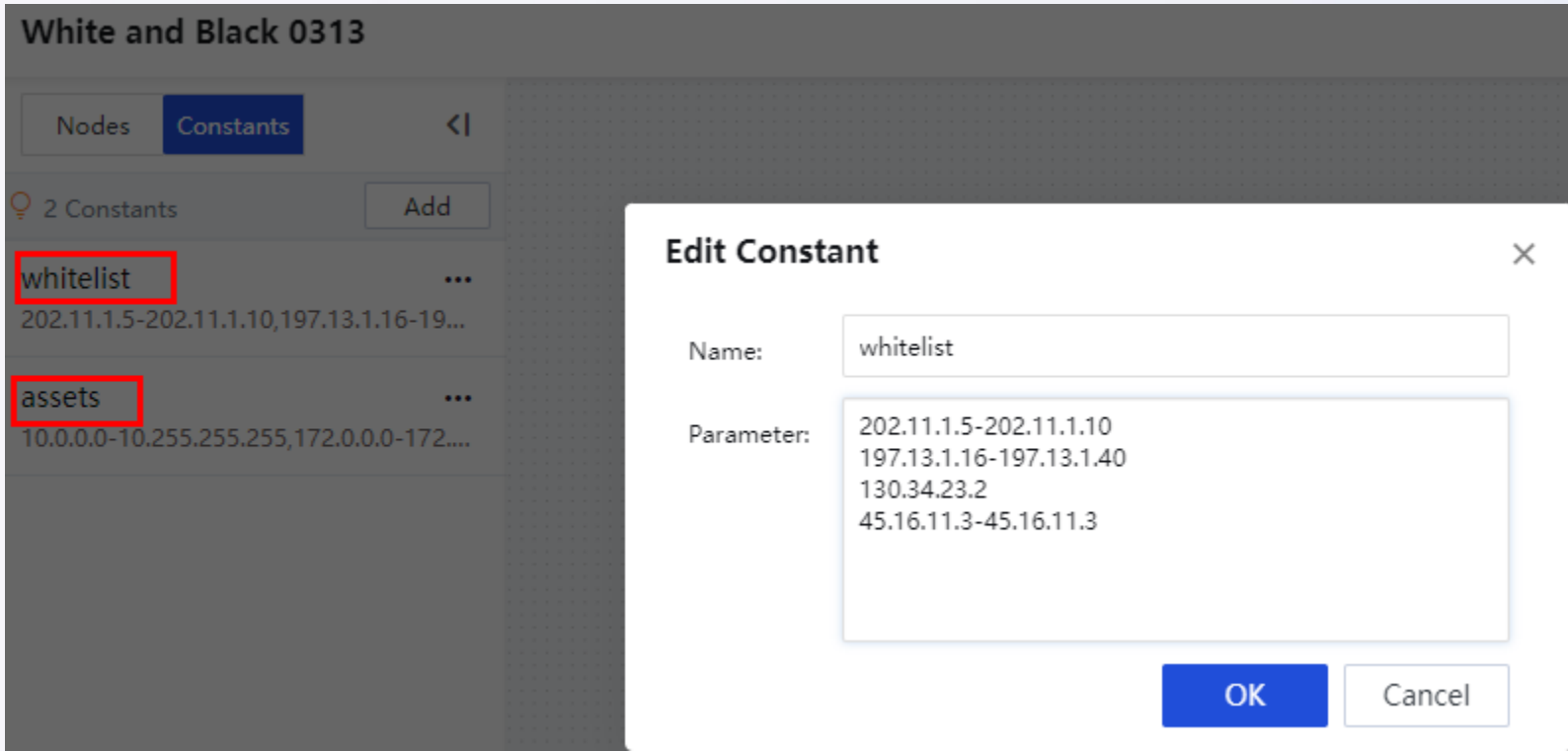
Copyright © 2023 Sangfor Technology Co., Ltd.

Page22

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;

Policy Settings | Save as Draft | Save and Enable | Cancel

Start

whether attac... #10

else

2 Else

whether belo... #11

if

1 not belong

whether belo... #12

if

else

Else

Parameter Settings

* Node Name: whether attacker ip is empty

* Filter Rule

1 If

* Name: empty

* Rule:

`\${alert.attack_ip}` is empty empty

`\${alert.attack_ip}`

is em...

empty

+or

2 Else

+ Else If

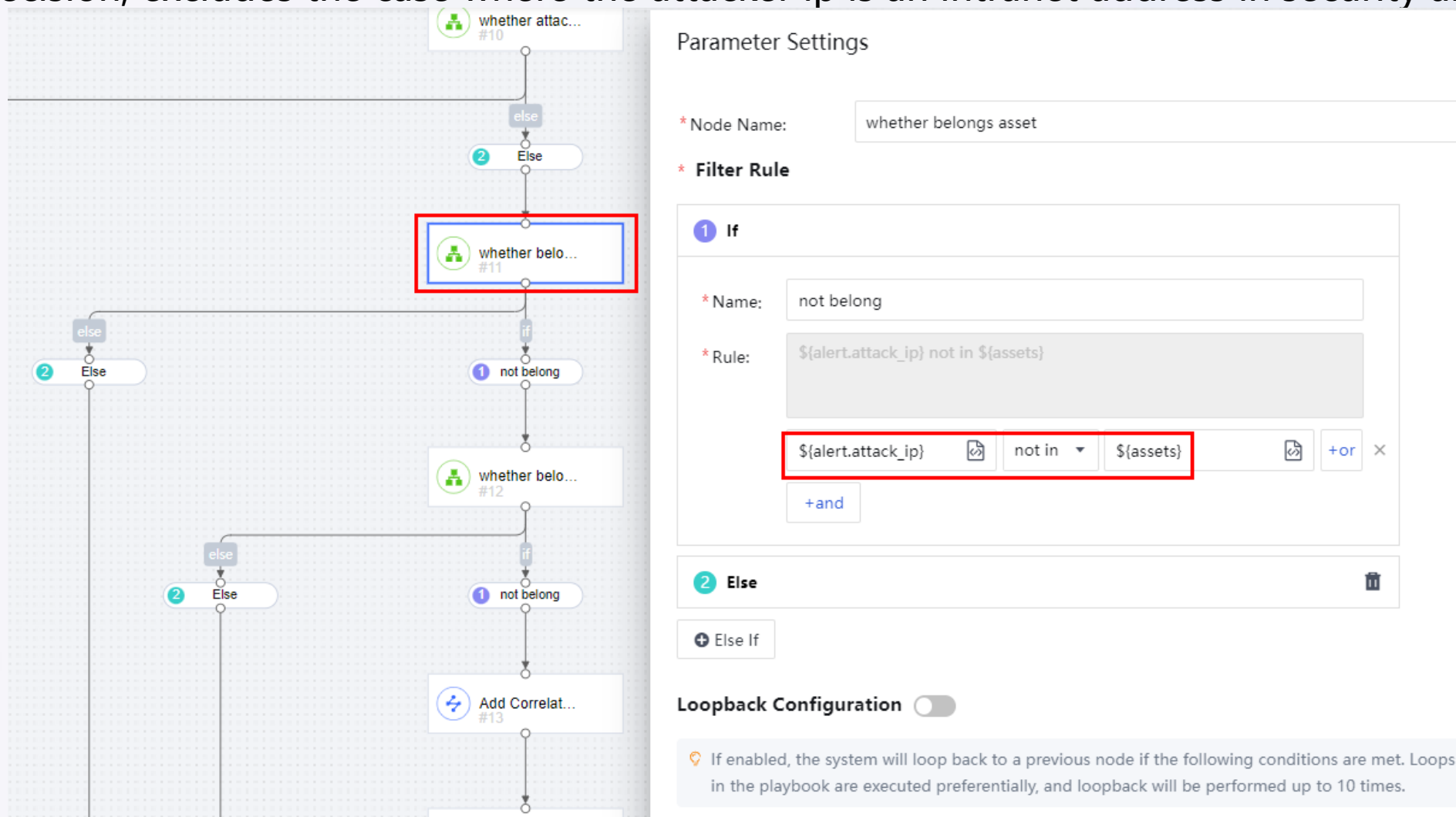
Copyright © 2023 Sangfor Technology Co., Ltd.

Page24

Example 2



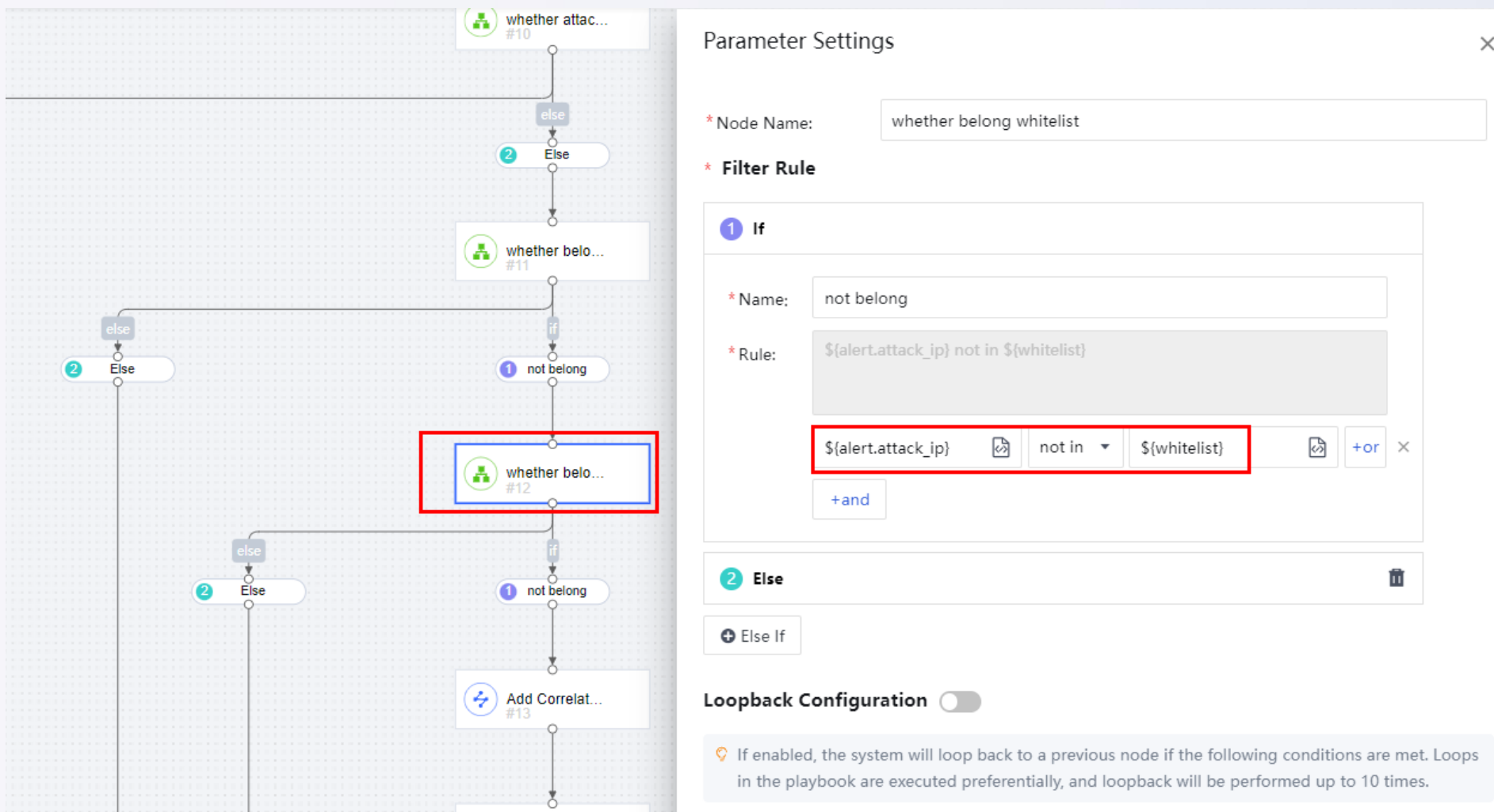
Step4: Decision, excludes the case where the attacker ip is an intranet address in security alerts;



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;

The image displays a workflow diagram on the left and its corresponding 'Parameter Settings' window on the right.

Flowchart: The workflow starts with a node labeled '#12'. It branches into two paths. The top path goes through a decision node '1 not belong' (labeled 'if') to an action node 'Add Correlat... #13' (labeled 'Add Correlat...'). The bottom path goes through a decision node '2 Else' (labeled 'Else') to an action node 'Change Secu... #14' (labeled 'Change Secu...'). Both paths converge at an 'End' node.

Parameter Settings: The settings for the 'Add Correlat... #13' node are shown. The 'Node Name' and 'Action' are both set to 'Add Correlated Block'. The 'Block Direction' is set to 'Source and Destination'. The 'Object Type to Block' is set to 'IP'. The 'Object to Block' is set to the expression `${alert.linkage_recommend.af.block.attack.item}`. The 'Block Duration' is set to '-1' and the 'Block Duration Unit' is set to 'Day'. The 'Device IP' is set to 'ngaf'.

The 'Parameter Settings' window includes the following fields:

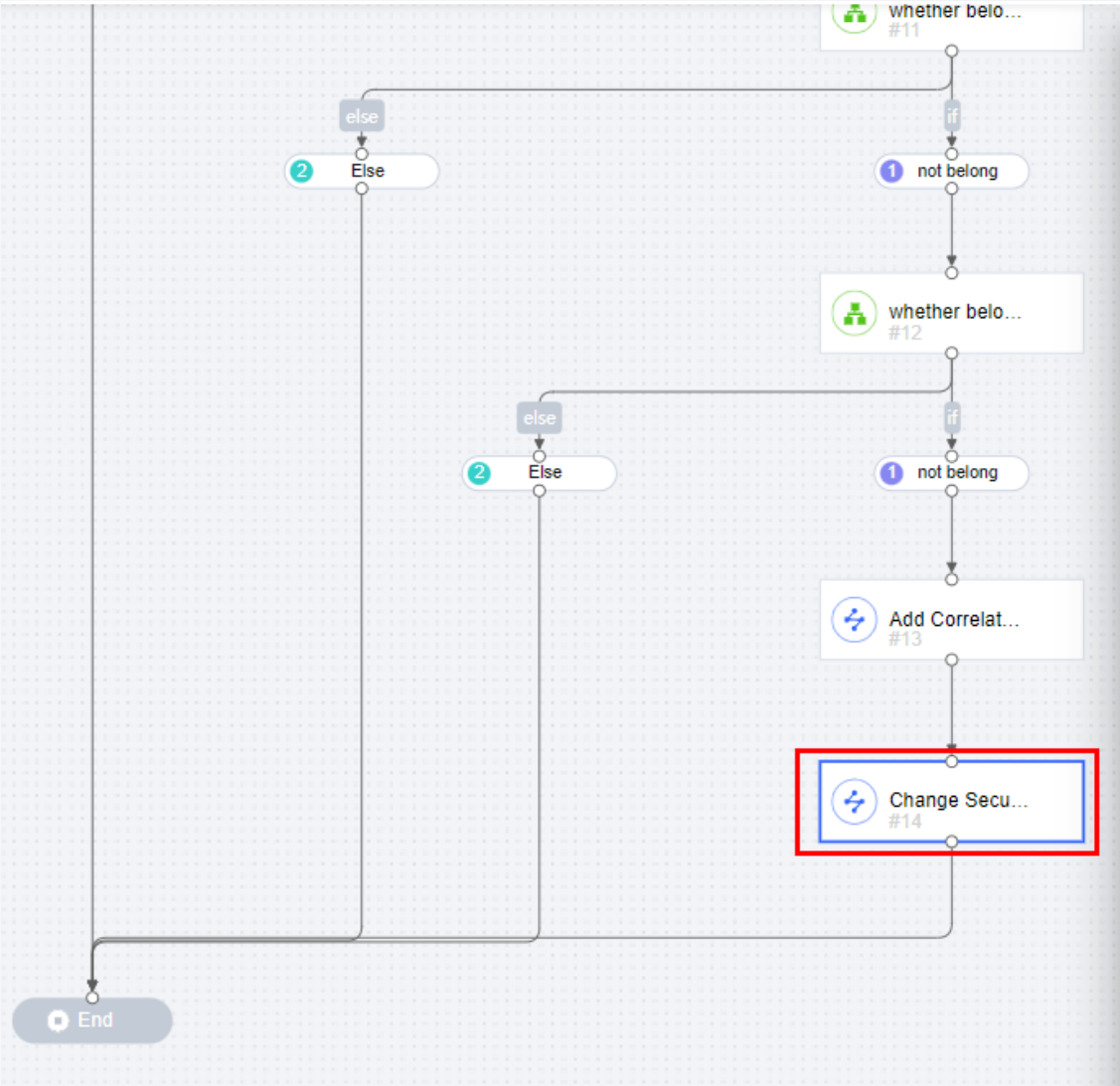
- * Node Name: Add Correlated Block
- * Action: Add Correlated Block
- * Block Direction: Source and Destination
- * Object Type to Block: IP
- * Object to Block: `${alert.linkage_recommend.af.block.attack.item}`
- * Block Duration: -1
- * Block Duration Unit: Day
- * Device IP: ngaf

Advanced ▾

Example 2



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



Parameter Settings

* Node Name:	Change Security Alert Status
* Action:	Change Security Alert Status
* ID:	<input type="text" value="\${alert.hash_id}"/>
* Time Detected:	<input type="text" value="\${alert.first_time}"/>
* Status:	<input type="text" value="Fixing"/>
Remarks:	<input type="text" value="Enter/Select Parameter"/>
* Device IP:	<input type="text" value="Cyber Command"/>

Advanced ▾

Example 2



Execution results

Security Alerts

No.	Last Detected	Threat	Threat Type	Attack Stage	Target IP	Attacker IP	XFF	Result	Status Co...	URL	Status
1	2023-03-13 19:48:20	Cobalt Strike backdoor	CobaltStrike	Propagation	192.168.1.5	10.100.18.20	-	Compr...	403	26788.server.dnsec.sangfor...	Fixed
2	2023-03-12 23:59:25	Cobalt Strike backdoor	CobaltStrike	Propagation	192.168.1.5	10.100.18.20	-	Compr...	403	26788.server.dnsec.sangfor...	Fixed
3	2023-03-13 19:45:46	Weak SMTP password	SMTP	Weaknesses	7.7.7.21	7.7.7.28 against th	-	Succeed	-	-	Fixing Coordination
4	2023-03-13 19:40:54	Weak Web password	WEB	Weaknesses	10.100.4.248	2.0.1.12(Franc...	-	Succeed	-	10.100.4.248/shopex/	Fixing Coordination
5	2023-03-13	WebShell file upload	WebShell Upload	Exploitation	192.168.100.200	128.125.161.1...	-	Attem...	-	http://10.100.12.6:8008/	Fixing

Response

Risky Assets

Security Incidents

Security Alerts

Auto Response History

Coordinated Actions

No.	Coordinated Action	Asset IP	Action Parameter	Application	Resource	End Time	Executed By	Execution Result	Details
1	Change Security Alert ...	192.168.1.10	Sangfor Cyber Command,...	Sangfor Cyber Comma...	Cyber Command	2023-03-13 19:59:51	Trigger Policy system	Executed	View
2	Add Correlated Block	192.168.1.10	Sangfor NGAF (v8.0.8 to v...	Sangfor NGAF (v8.0.8 t...	ngaf	2023-03-13 19:59:50	Trigger Policy system	Executed	View Undo
3	Change Security Alert ...	7.7.7.28,7.7.7.21	Sangfor Cyber Command,...	Sangfor Cyber Comma...	Cyber Command	2023-03-13 19:59:50	Trigger Policy system	Executed	View
4	Add Correlated Block	7.7.7.28,7.7.7.21	Sangfor NGAF (v8.0.8 to v...	Sangfor NGAF (v8.0.8 t...	ngaf	2023-03-13 19:59:50	Trigger Policy system	Executed	View Undo
5	Change Security Alert ...	10.100.4.248	Sangfor Cyl	NGAF Platform 8.0.47	Home	SOC	Monitor	Policies	Objects
6	Add Correlated Block	10.100.4.248	Sangfor NC						
7	Change Security Alert ...	7.7.7.28,7.7.7.21	Sangfor Cy						

SOC

Security Operations

Business Asset Security

User Security

Specialized Protection

Asset Management

Ransomware Protection

IP Reputation

Account Protection

Endpoint App Control

Threat Intelligence

Blacklist/Whitelist

Global Blacklist

+ Add

Delete

Clear All

Enable

Disable

Import

Export

Refresh

No.	IP Address	Description	Time Added	Status	Operation
1	92.68.1.11	From Cyber Command	2023-03-13 19:54:05	✓	Edit Delete
2	7.7.7.21	From Cyber Command	2023-03-13 19:54:04	✓	Edit Delete
3	7.7.7.28	From Cyber Command	2023-03-13 19:48:18	✓	Edit Delete
4	128.125.161.167	From Cyber Command	2023-03-13 19:43:04	✓	Edit Delete
5	2.0.1.12	From Cyber Command	2023-03-13 19:43:03	✓	Edit Delete
6	48.147.198.108	From Cyber Command	2023-03-13 19:43:02	✓	Edit Delete
7	106.225.216.190	From Cyber Command	2023-03-13 19:43:02	✓	Edit Delete

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】

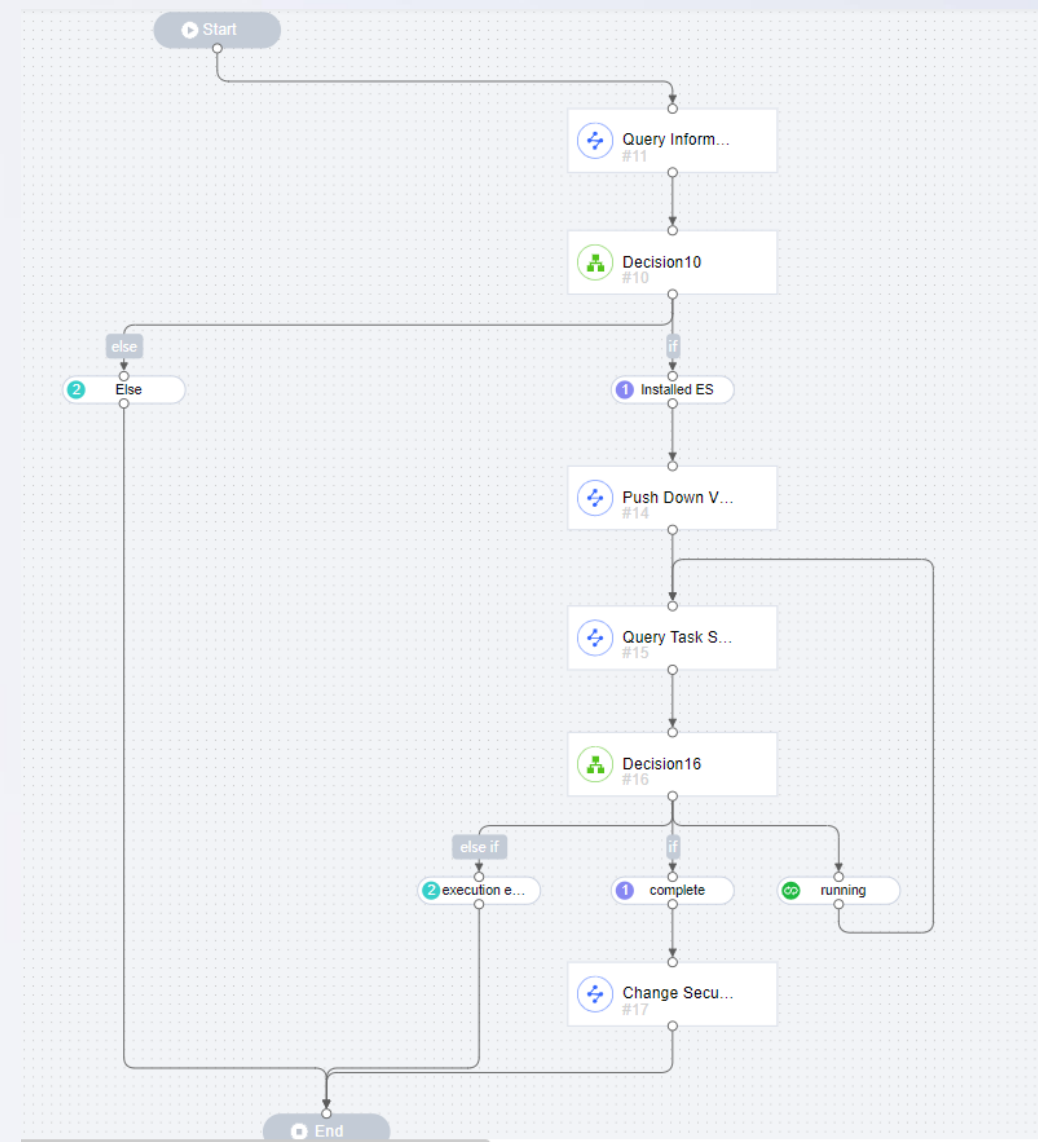
Firstly, the policy setting delimits the threat classification of bots, trojans and worms. In the process of policy orchestration, it is necessary to judge whether ES is installed. if it is not installed, it will end directly. The assets installed ES will receive virus scan task by Cyber Command. When 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 classification;
- **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 virus 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 end 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 classification

Policy Settings

Basic Info

* Policy Name:

3333

Policy Description:

Enter brief policy description.

0/4096

* Policy Type:

Sophisticated_Control

Execution Method:

☒ Execute Automatically

☐ Execute Manually

Trigger Type:

☒ Security Incident

☐ Security Alert

Conditions for Execution

Condition 1:

Security Incident

in

Trojan,Worm,Infectiou...

+ Add Condition

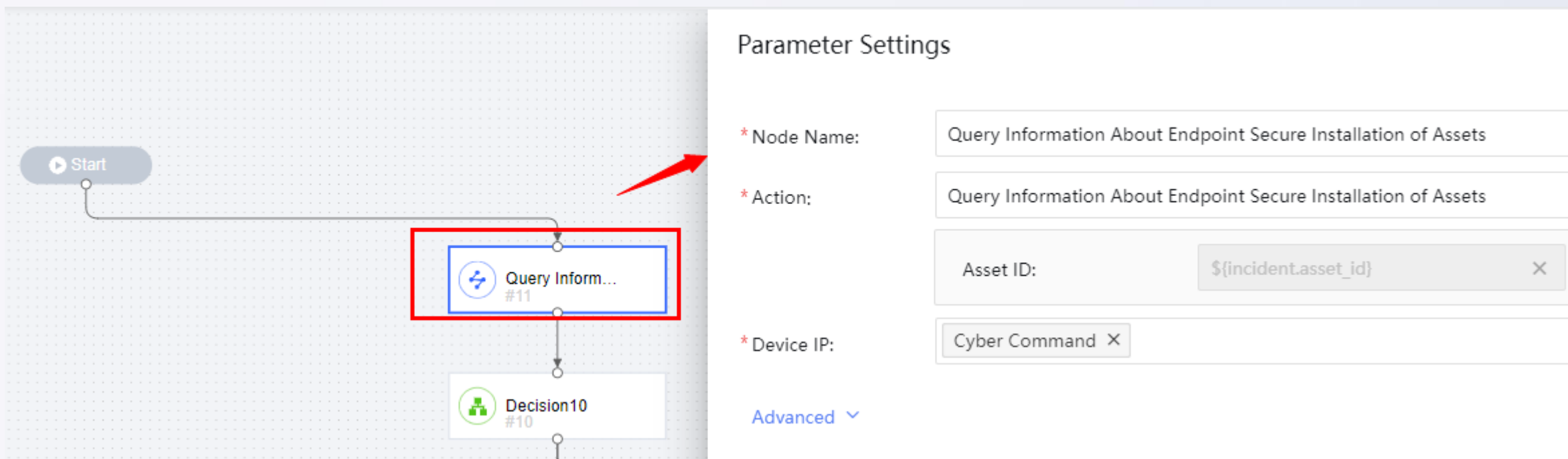
Copyright © 2023 Sangfor Technology Co., Ltd.

Page32

Example 3



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



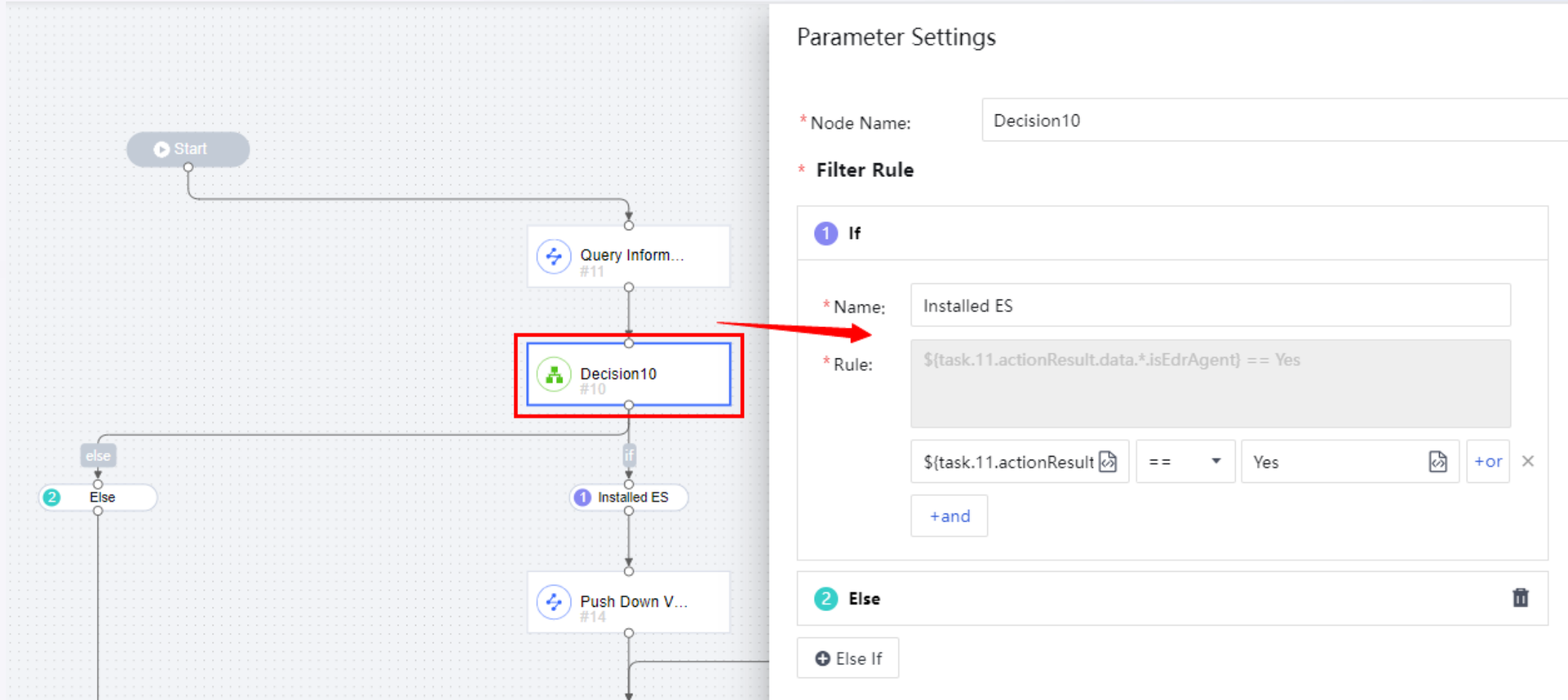
The image displays a workflow diagram on the left and a 'Parameter Settings' panel on the right. The workflow starts with a 'Start' node, followed by a 'Query Inform...' node (labeled #11), which is highlighted with a red box and a red arrow. Below this is a 'Decision10' node (labeled #10). The 'Parameter Settings' panel on the right is titled 'Parameter Settings' and contains the following fields:

- * Node Name: Query Information About Endpoint Secure Installation of Assets
- * Action: Query Information About Endpoint Secure Installation of Assets
- Asset ID: \${incident.asset_id} (with a clear button 'X')
- * Device IP: Cyber Command (with a clear button 'X')
- Advanced (with a dropdown arrow)

Example 3



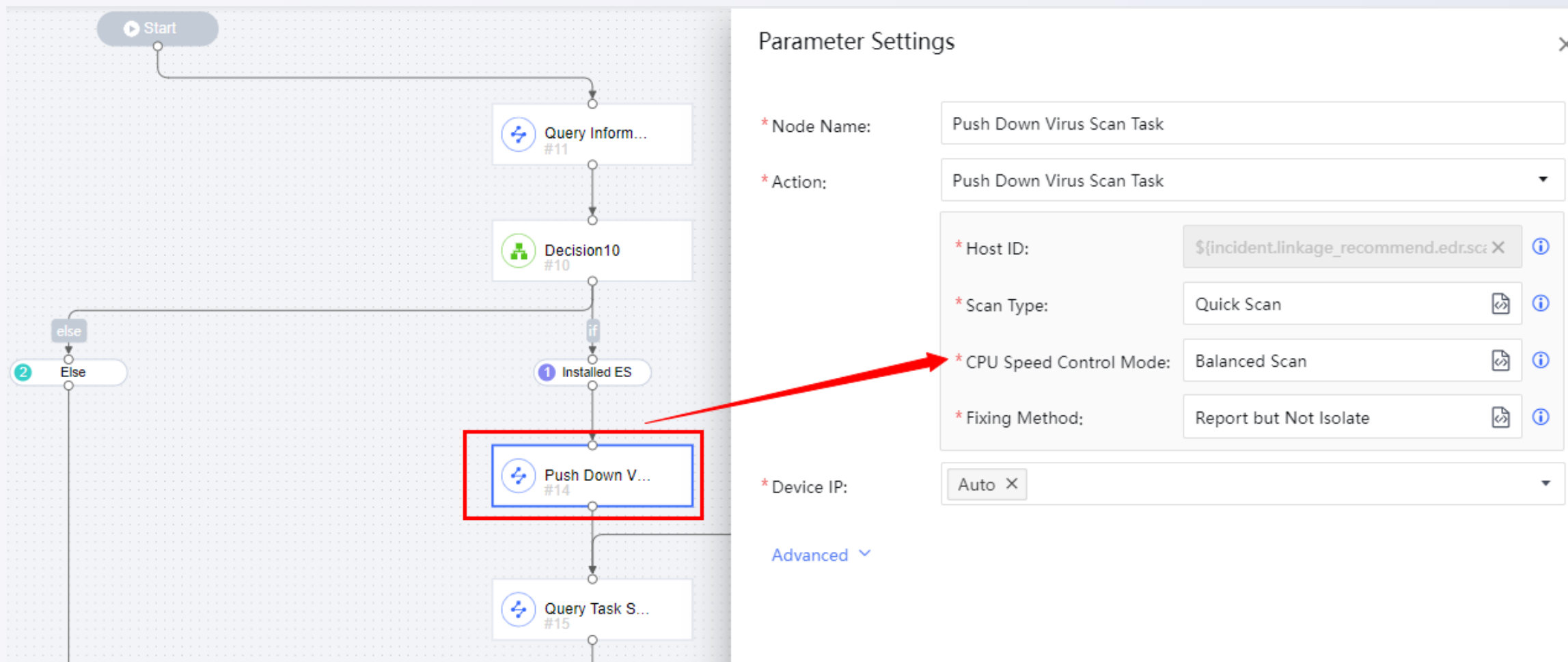
- **Step3:** Decision, the filter rule ends directly for assets that are not installed ES client, for those installed perform a quick virus scan task;



Example 3



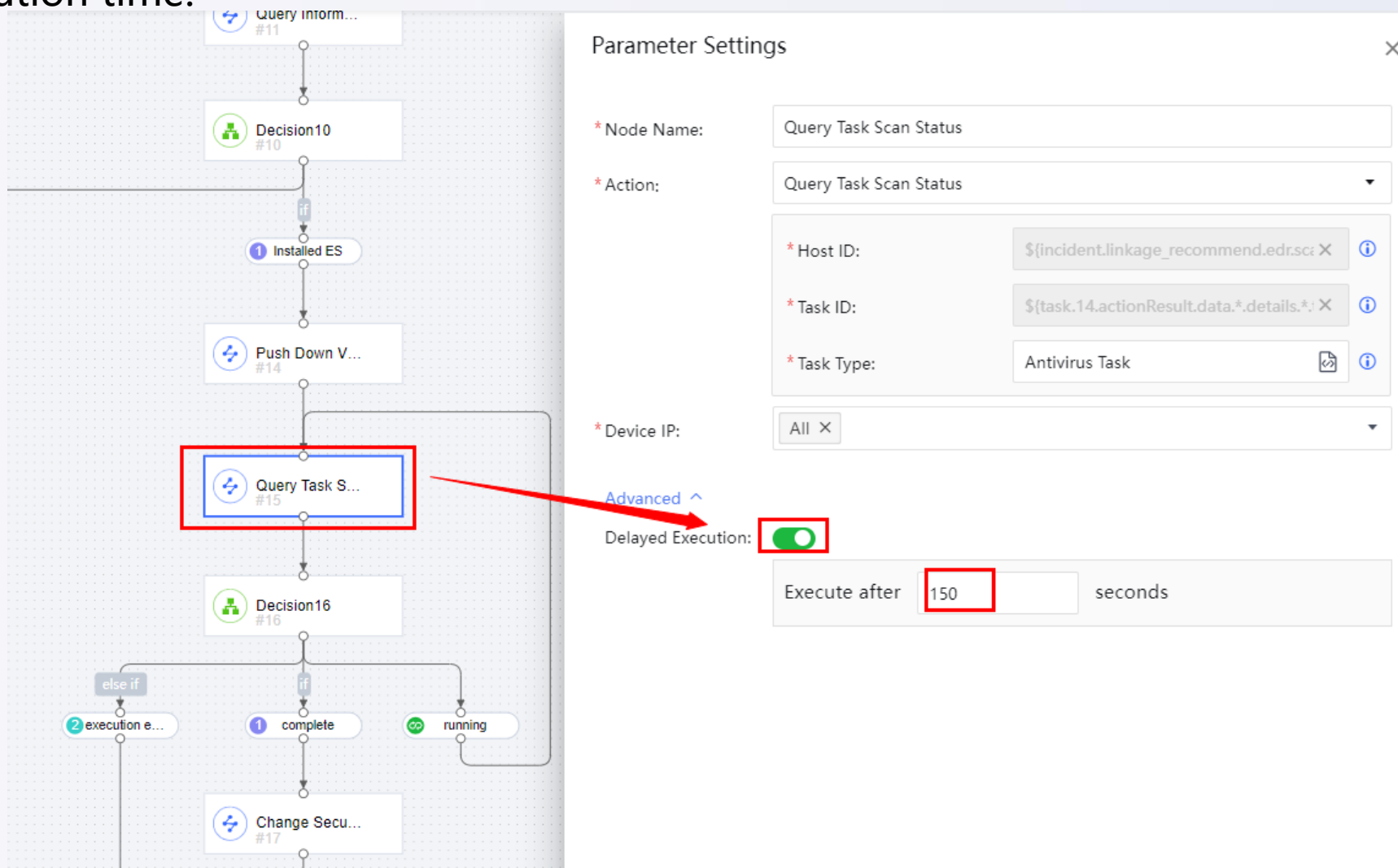
- **Step4:** Action, push down virus scan action ;



Example 3



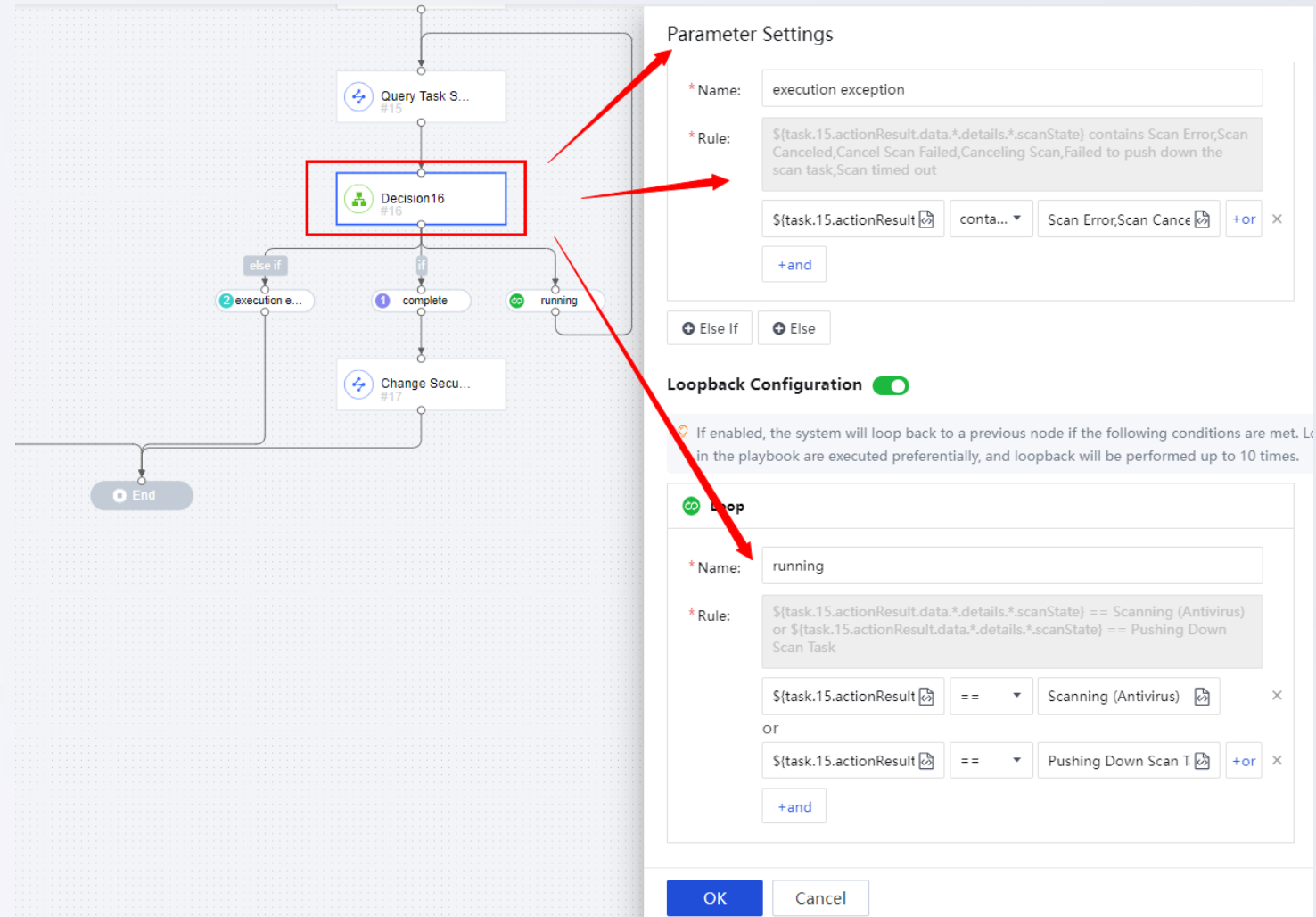
- **Step5:**Action,since virus scan task last minutes, it is necessary to configure delayed execution time.



Example 3



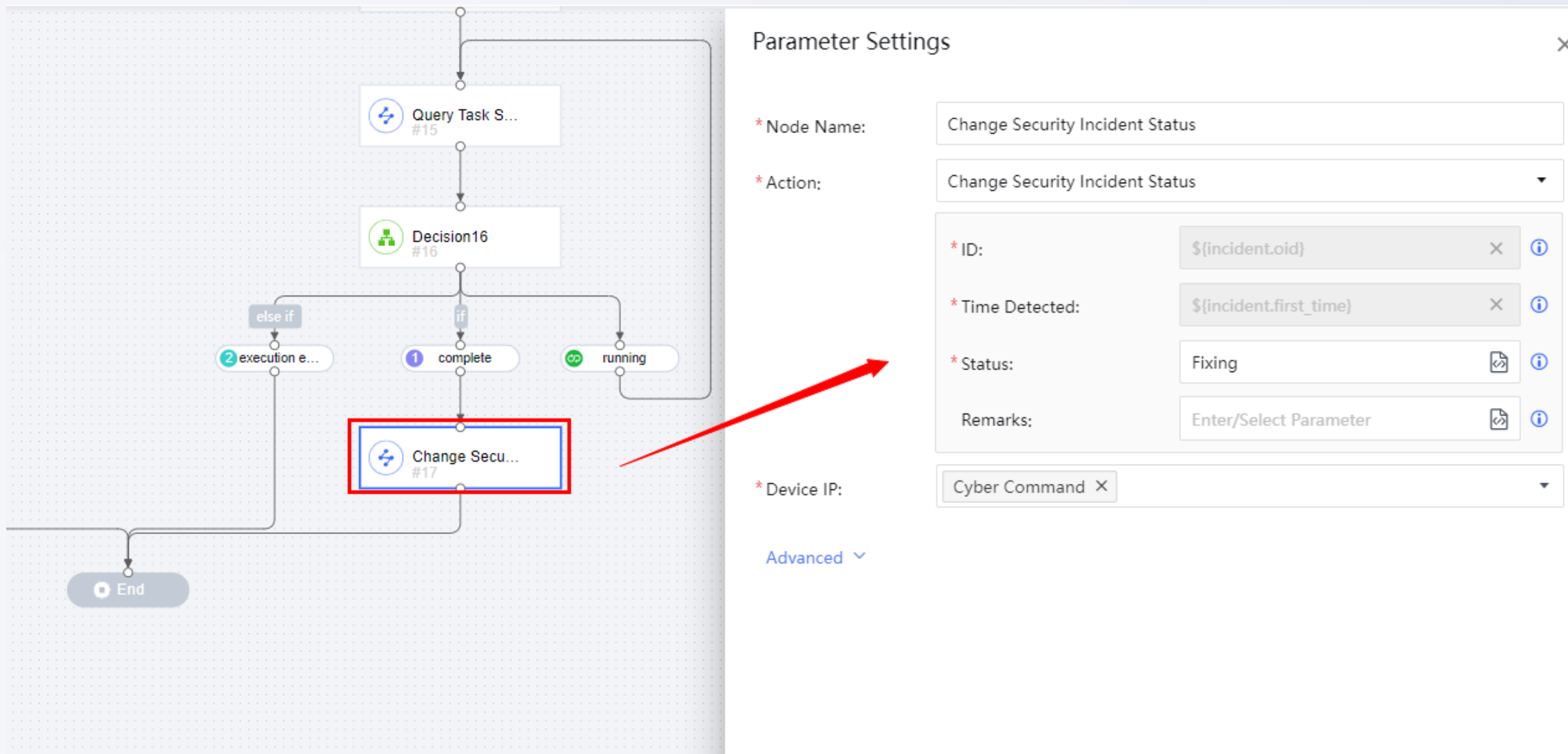
- **Step6:**Decision,there are mainly 3 types of outcomes, they are running, execution exception and execution completed. It will go forward next node when it matches execution completed. It will ends directly when it matches execution exception. For running type, it will perform loopback till the end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



Example 3



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



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:

Response												
<div>Risky Assets</div> <div>Security Incidents</div> <div>Security Alerts</div> <div>Auto Response</div> <div>Response History</div>												
Risky Assets Security Incidents Security Alerts Auto Response History Coordinated Actions												
All Categories All Statuses Asset IP, policy name, security incident, fixed by												
No.	Running Policy	Asset IP	Policy Type	Application	Security Incidents	End Time	Executed By	Execution Status	Coordinated Action	Remarks	Operation	...
1	White and Black 0...	10.100.17.224	Cloned	Sangfor NGAF (v8...	Alert-Database Ex...	-	admin	In Progress	View	-	-	
2	White and Black 0...	192.168.1.10	Cloned	Sangfor NGAF (v8...	Alert-Phishing Em...	2023-03-13 20:06:40	system	✓ Executed	View	-	Delete	
3	White and Black 0...	7.7.7.21,7.7.7.28	Cloned	Sangfor NGAF (v8...	Alert-Phishing Em...	2023-03-13 20:06:39	system	✓ Executed	View	-	Delete	
4	White and Black 0...	10.251.0.160,10.2...	Cloned	Sangfor NGAF (v8...	Alert-Malicious Fil...	2023-03-13 20:06:10	system	✓ Executed	View	-	Delete	
5	White and Black 0...	7.7.7.28,7.7.7.21	Cloned	Sangfor NGAF (v8...	Alert-SMTP	2023-03-13 20:06:39	system	✓ Executed	View	-	Delete	
6	White and Black 0...	192.168.1.10	Cloned	Sangfor NGAF (v8...	Alert-Phishing Em...	2023-03-13 20:05:37	system	✓ Executed	View	-	Delete	
7	White and Black 0...	10.37.64.30	Cloned	Sangfor NGAF (v8...	Alert-Brute-Force ...	2023-03-13 20:05:11	system	✓ Executed	View	-	Delete	
8	White and Black 0...	7.7.7.21,7.7.7.28	Cloned	Sangfor NGAF (v8...	Alert-Phishing Em...	2023-03-13 20:05:37	system	✓ Executed	View	-	Delete	
9	White and Black 0...	10.100.19.19,20.1...	Cloned	Sangfor NGAF (v8...	Alert-Brute-Force ...	2023-03-13 20:05:11	system	✓ Executed	View	-	Delete	
10	White and Black 0...	10.251.0.160,10.2...	Cloned	Sangfor NGAF (v8...	Alert-Malicious Fil...	2023-03-13 20:05:11	system	✓ Executed	View	-	Delete	

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

Here is the page:

Response

Risky Assets

Security Incidents

Security Alerts

Auto Response

Response History

Risky Assets

Security Incidents

Security Alerts

Auto Response History

Coordinated Actions

Last 30 days

Asset Group

Q

«

Export

Export Response Report

Hostname, IP, description, fixed by

Q

All

Internal IP Range

from HCI

from SaaS ES

	No.	Threat	Hostname	Severity	Fixed By	Time Fixed	Status	Operation	...
<input type="checkbox"/>	1	Malicious file downloaded	Internal IP Range (10.33.36.22)	High	admin(192.200.19...	2023-03-14 10:46:23	Fixed		
<input type="checkbox"/>	2	Malicious file downloaded	Internal IP Range (192.168.1.25)	High	admin(192.200.19...	2023-03-14 10:46:23	Fixed		
<input type="checkbox"/>	3	Malicious file downloaded	Internal IP Range (172.16.197.140)	High	admin(192.200.19...	2023-03-14 10:46:23	Fixed		

Thank you