Sangfor Correlated Policy Practice Guidance

Document Version	v1.0
Released on	2023-04-24

Disclaimer

Products, services or features described in this document, whether wholly or in part, may be not within your purchase scope or usage scope. The products, services or features you purchase must be subject to the commercial contract and terms as agreed by you and Sangfor. Unless otherwise provided in the contract, Sangfor disclaims warranties of any kind, either express or implied, for the content of this document.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Unless otherwise agreed, this document is used for reference only, and all statements, information, and recommendations therein do not constitute any express or implied warranties.

Technical Support

For technical support, please visit: https://www.sangfor.com/en/about-us/contact-us/technical-support

Send information about errors or any product related problem to tech.support@sangfor.com.

Intended Audience

This document is intended for:

- Pre-sale
- FAE

Note Icons

English Icon	Description
⚠ DANGER	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
⚠ CAUTION	Indicates a hazardous situation, which if not avoided, could result in minor or moderate injury.
⚠ NOTICE	Indicates a hazardous situation, which if not avoided, could result in settings failing to take effect, equipment damage, or data loss. NOTICE addresses practices not related to personal injury.
📖 NOTE	Calls attention to important information, best practices, and tips. NOTE addresses information not related to personal injury or equipment damage.

Change Log

Date	Change Description
2023-04-24	This is the first release of this document.

Contents

1 Case

This document aims to carry out high-frequency correlated processing between different self-developed devices(ES/IAG/NGAF/CC) and integrate gateway, terminal, and platform products to achieve continuous threat detection and efficient security operations, bringing value to customers.

According to solutions based on marketing, we provide scenario-based playbook strategies for different customer environments.

No	Solution Type	Main Products Involved	Remark
1	XDDR	ES、NGAF、CC	playbook,security operations improvement.

1.1 Scene

1.1.1 Customer Pain Points

The customer has invested in a range of cybersecurity solutions, including IAG, CC, ES, and NGAF devices, yet continues to experience numerous daily security alerts related to botnets, Trojan horses, and worms. These alerts occasionally occur during nighttime hours, increasing the risk to information security. Although the information department has been promoting the installation of EDR, some terminals remain unprotected, exacerbating these risks.

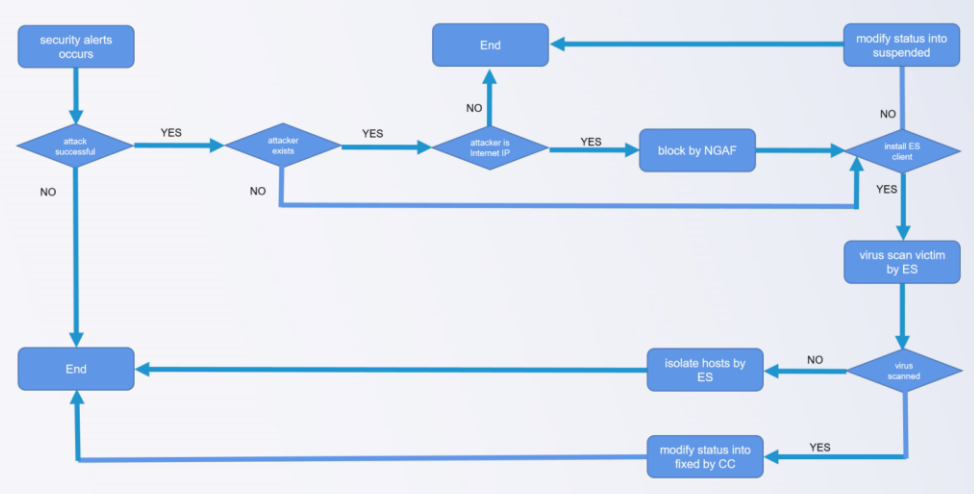
To address these concerns, the customer seeks an effective integration of these security products through the playbook of CC, enabling timely and automated detection and resolution of potential threats. By reducing the burden of manual security operations, the team can more efficiently manage threats and control their spread, even during overnight hours when security personnel may not be readily available.

1.1.2 Implementation Method Analysis

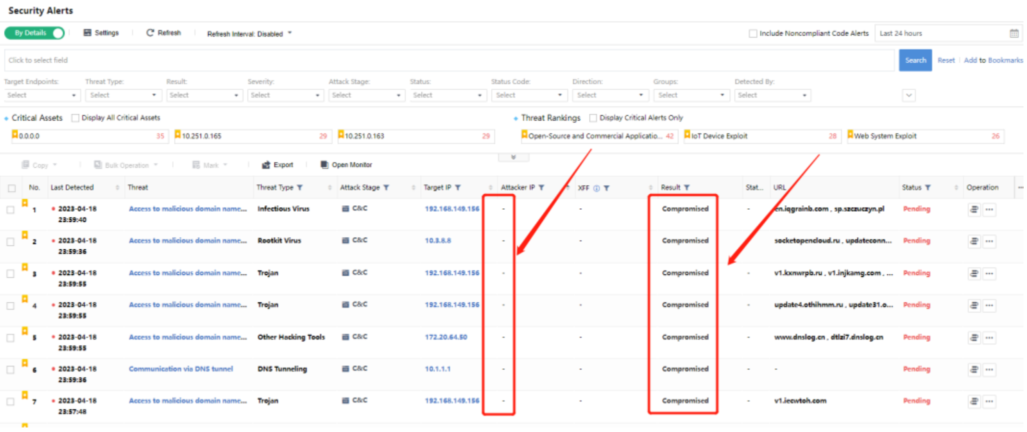
The IAG solution can control user access to the Internet, while the ES solution scans and eliminates malicious processes on terminals, enabling the identification of the root cause of these threats. The NGAF can block communication between malicious processes and known Internet malicious websites, preventing further infection. The CC solution can set playbook policies that integrate and streamline the use of these devices.

For clients, threats often occur when accessing the Internet, as they unknowingly come into contact with malicious servers and other harmful elements. However, by utilizing these automation playbook policies, the risk of such threats can be effectively mitigated and controlled, ensuring that the system remains secure and protected against potential cyber risks.

Based on the above ideas, we can draw the following flow chart:



- **Step 1**： Once alerts are triggered, they hit the predefined policy settings, initiating the first step in the process of assessing and addressing potential threats.
- **Step2**： If the attack results belong to attempted or failed, this suggests that there has been no adverse impact, and the alerts may be safely ignored. However, if the attack results belong to compromised or successful, immediate action must be taken to mitigate the risk.
- **Step 3：** If the attacker's IP does not exist, the system will proceed to make a subsequent judgment regarding whether it is an Internet address. If the IP does exist, the next step is to consider whether the ES client has been installed on the relevant asset.


Security Alerts

By Details | Settings | Refresh | Refresh Interval: Disabled

☐ Include Noncompliant Code Alerts | Last 24 hours

Click to select field | Search | Reset | Add to Bookmarks

Target Endpoints: Select | Threat Type: Select | Result: Select | Severity: Select | Attack Stage: Select | Status: Select | Status Code: Select | Direction: Select | Groups: Select | Detected By: Select

Critical Assets ☐ Display All Critical Assets

0.0.0.0 35 | 10.251.0.165 29 | 10.251.0.163 29

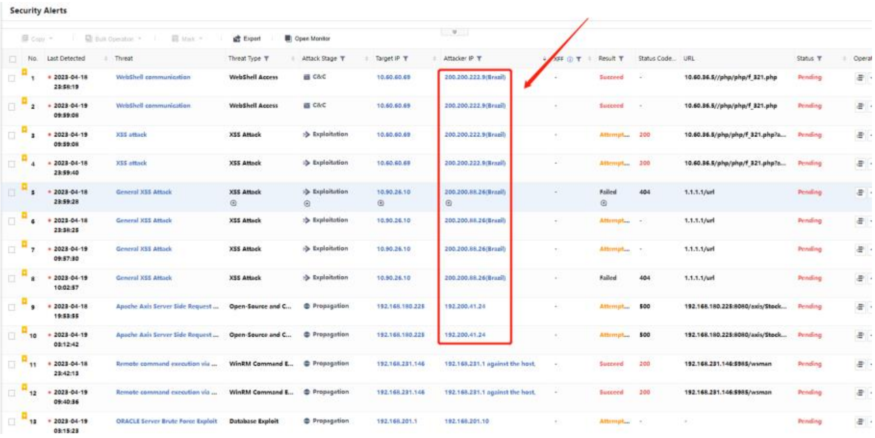
Threat Rankings ☐ Display Critical Alerts Only

Open-Source and Commercial Applicatio... 42 | IoT Device Exploit 28 | Web System Exploit 26

Copy | Bulk Operation | Mark | Export | Open Monitor

☐	No.	Last Detected	Threat	Threat Type	Attack Stage	Target IP	Attacker IP	XFF	Result	Stat...	URL	Status	Operation
☐	1	2023-04-18 23:59:40	Access to malicious domain name...	Infectious Virus	C&C	192.168.149.156	-	-	Compromised	-	en.iqgrainb.com , sp.szczuczyn.pl	Pending	···
☐	2	2023-04-18 23:59:36	Access to malicious domain name...	Rootkit Virus	C&C	10.3.8.8	-	-	Compromised		socketopencloud.ru , updateconn...	Pending	···
☐	3	2023-04-18 23:59:55	Access to malicious domain name...	Trojan	C&C	192.168.149.156	-	-	Compromised	-	v1.kxnwrpb.ru , v1.injkamg.com , ...	Pending	···
☐	4	2023-04-18 23:59:55	Access to malicious domain name...	Trojan	C&C	192.168.149.156	-	-	Compromised	-	update4.othihmm.ru , update31.o...	Pending	···
☐	5	2023-04-18 23:59:55	Access to malicious domain name...	Other Hacking Tools	C&C	172.20.64.50	-	-	Compromised	-	www.dnslog.cn , dtlzi7.dnslog.cn	Pending	···
☐	6	2023-04-18 23:59:36	Communication via DNS tunnel	DNS Tunneling	C&C	10.1.1.1	-	-	Compromised	-	-	Pending	···
☐	7	2023-04-18 23:57:48	Access to malicious domain name...	Trojan	C&C	192.168.149.156	-	-	Compromised	-	v1.iecwtoh.com	Pending	···

- **Step 4**： In general, the NGAF solution will block Internet malicious addresses rather than asset addresses. As a result, it is necessary to determine whether the attacker’s IP belongs to the Internet, enabling the exclusion of lateral and outbound access attacks.



Security Alerts

No.	Last Detected	Threat	Threat Type	Attack Stage	Target IP	Attacker IP	XFF	Result	Status Code...	URL	Status	Operat
1	2023-04-18 23:56:19	WebShell communication	WebShell Access	C&C	10.60.60.69	200.200.222.9(Brazil)	-	Succeed	-	10.60.36.5//php/php/f_321.php	Pending	
2	2023-04-19 09:59:08	WebShell communication	WebShell Access	C&C	10.60.60.69	200.200.222.9(Brazil)	-	Succeed	-	10.60.36.5//php/php/f_321.php	Pending	
3	2023-04-19 09:59:08	XSS attack	XSS Attack	Exploitation	10.60.60.69	200.200.222.9(Brazil)	-	Attempt...	200	10.60.36.5/php/php/f_321.php?a...	Pending	
4	2023-04-18 23:59:40	XSS attack	XSS Attack	Exploitation	10.60.60.69	200.200.222.9(Brazil)	-	Attempt...	200	10.60.36.5/php/php/f_321.php?a...	Pending	
5	2023-04-18 23:59:28	General XSS Attack	XSS Attack	Exploitation	10.90.26.10	200.200.88.26(Brazil)	-	Failed	404	1.1.1.1/url	Pending	
6	2023-04-18 23:38:25	General XSS Attack	XSS Attack	Exploitation	10.90.26.10	200.200.88.26(Brazil)	-	Attempt...	-	1.1.1.1/url	Pending	
7	2023-04-19 09:57:30	General XSS Attack	XSS Attack	Exploitation	10.90.26.10	200.200.88.26(Brazil)	-	Attempt...	-	1.1.1.1/url	Pending	
8	2023-04-19 10:02:57	General XSS Attack	XSS Attack	Exploitation	10.90.26.10	200.200.88.26(Brazil)	-	Failed	404	1.1.1.1/url	Pending	
9	2023-04-18 19:53:55	Apache Axis Server Side Request ...	Open-Source and C...	Propagation	192.168.180.225	192.200.41.24	-	Attempt...	500	192.168.180.225:8080/axis/Stock...	Pending	
10	2023-04-19 03:12:42	Apache Axis Server Side Request ...	Open-Source and C...	Propagation	192.168.180.225	192.200.41.24	-	Attempt...	500	192.168.180.225:8080/axis/Stock...	Pending	
11	2023-04-18 23:42:13	Remote command execution via ...	WinRM Command E...	Propagation	192.168.231.146	192.168.231.1 against the host.	-	Succeed	200	192.168.231.146:5985/wsman	Pending	
12	2023-04-19 09:40:36	Remote command execution via ...	WinRM Command E...	Propagation	192.168.231.146	192.168.231.1 against the host.	-	Succeed	200	192.168.231.146:5985/wsman	Pending	
13	2023-04-19 03:15:23	ORACLE Server Brute Force Exploit	Database Exploit	Propagation	192.168.201.1	192.168.201.10	-	Attempt...	-	-	Pending	

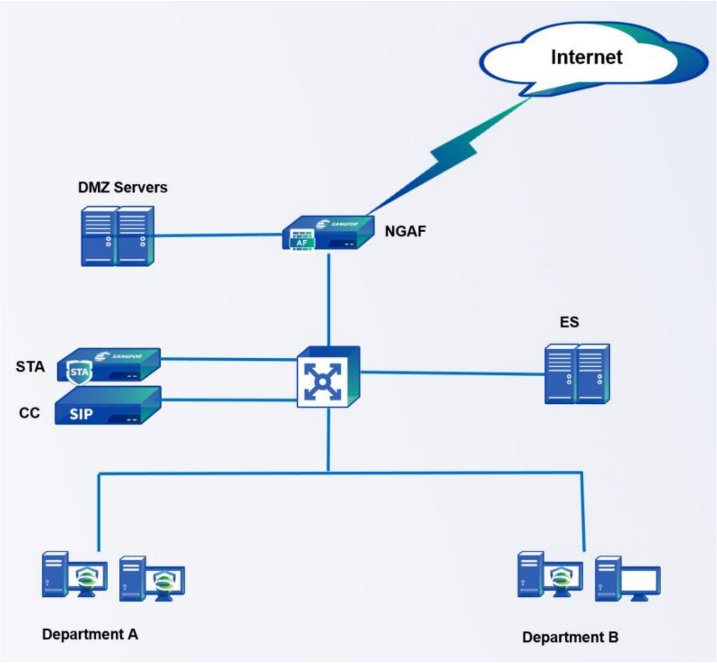
- **Step 5：** Thus, you can ascertain that the attackers's IP address is associated with malicious internet activity and subsequently initiate a blocking action, which is then executed by the NGAF.

- **Step 6**： It is essential to determine if the target assets have the ES client installed. If not, you can change the status to "suspended" as a reminder for the administrator to install the ES client and perform additional checks. If the ES client is already installed, you can directly initiave a virus scan task.

- **Step 7：** It is unrealistic to expect every virus scan task to identify the primary virus program. In some situations, if a virus scan does not detect any malicious software, isolating the host may still be necessary to prevent potential spreading. However, if a virus is detected and addressed promptly, you can update the status to 'fixed,' signifying the successful mitigation of the threat.

1.2 Network Toplogy

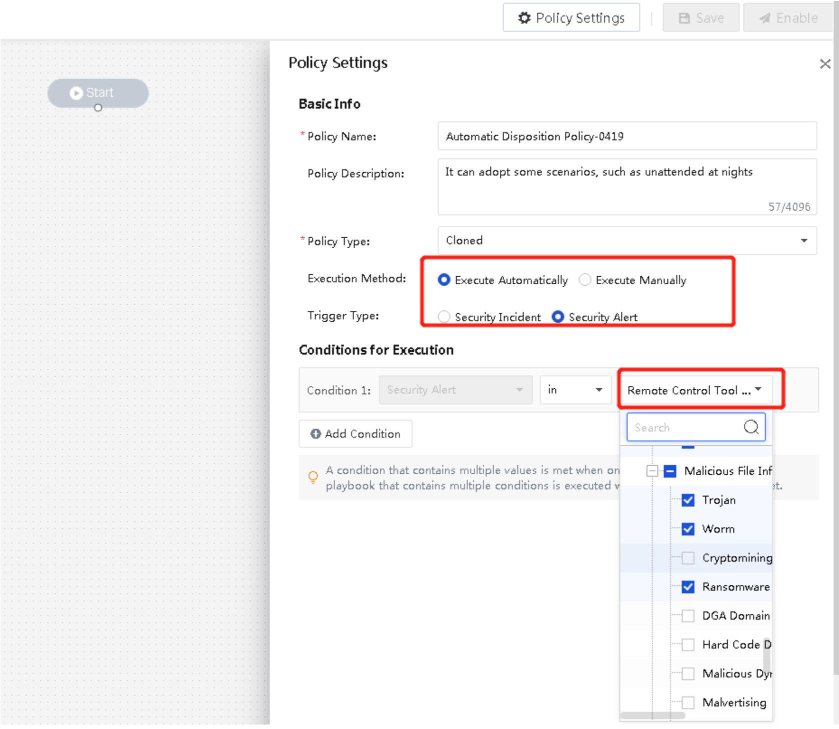
Based on the topology provided, the customer has implemented the Security Threat Analytics (STA), Cyber Command (CC), Endpoint Security (ES), and Next-Generation Application Firewall (NGAF) solutions. However, it is evident that some hosts have not yet installed the ES client, which may leave them vulnerable to potential threats.



1.3 Configuration Process

1.3.1 Policy Settings

Select security alert types, primarily encompassing worms, trojans and virus



Policy Settings

Basic Info

* Policy Name: Automatic Disposition Policy-0419

Policy Description: It can adopt some scenarios, such as unattended at nights 57/4096

* Policy Type: Cloned

Execution Method: ● Execute Automatically ○ Execute Manually

Trigger Type: ○ Security Incident ● Security Alert

Conditions for Execution

Condition 1: Security Alert in Remote Control Tool ...

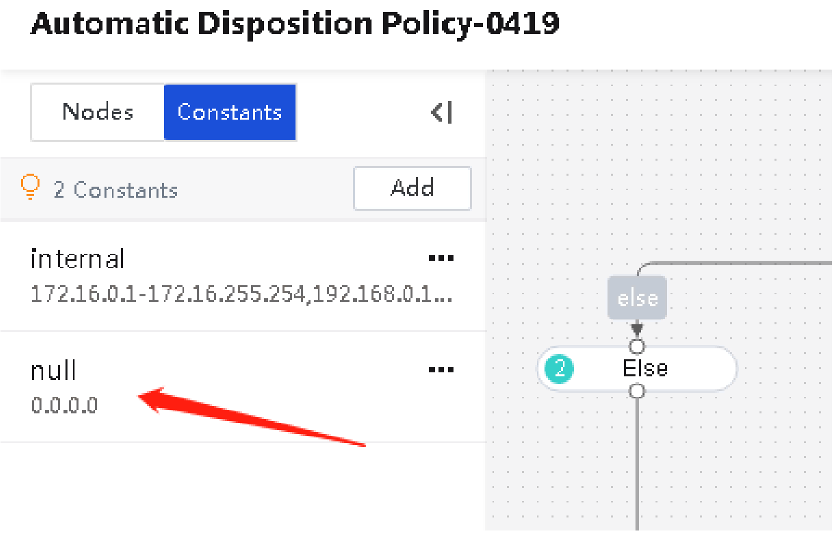
Add Condition

A condition that contains multiple values is met when on
playbook that contains multiple conditions is executed v t.

Malicious File Inf
☑ Trojan
☑ Worm
☐ Cryptomining
☑ Ransomware
☐ DGA Domain
☐ Hard Code D
☐ Malicious Dy
☐ Malvertising

1.3.2 Creating playbook policy

(1)、Firstly, you need to add internal assets' address range , along with as well as 0.0.0.0, into a constant, as you will need it for decision later.

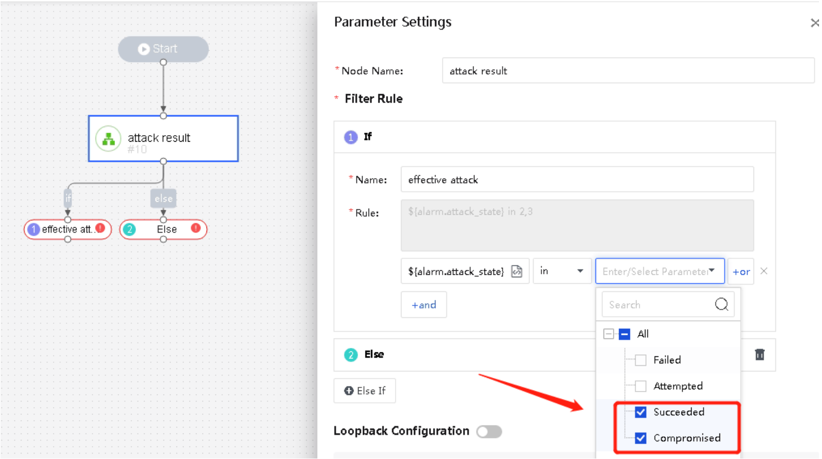


Automatic Disposition Policy-0419

internal
172.16.0.1-172.16.255.254,192.168.0.1...

null
0.0.0.0

(2)、You can define if an effective attack by seeing the attack result marked as "succeeded" and "compromised" .



Parameter Settings

*Node Name: attack result

*Filter Rule

1 If

*Name: effective attack

*Rule: ${alarm.attack_state} in 2,3

${alarm.attack_state} in Enter/Select Parameter +or

+and

2 Else

Else If

Loopback Configuration

Search

☐ All

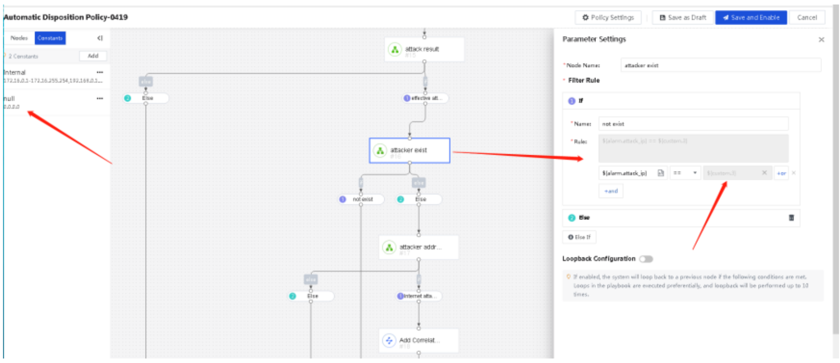
☐ Failed

☐ Attempted

☑ Succeeded

☑ Compromised

(3)、Determine whether an attacker exist by quoting null constant



Parameter Settings

*Node Name: attacker exist

*Filter Rule

1 If

*Name: not exist

*Rule: ${alarm.attack_ip} == ${custom.3}

${alarm.attack_ip} == ${custom.3} +or

+and

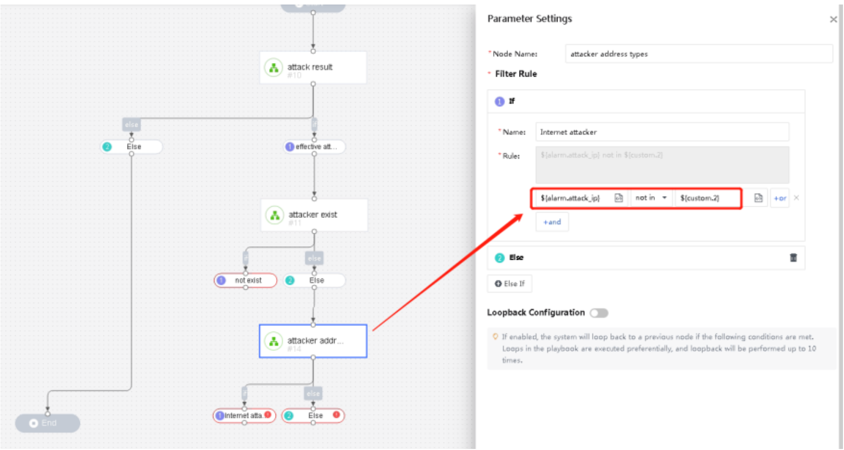
2 Else

Else If

Loopback Configuration

If enabled, the system will loop back to a previous node if the following conditions are met. Loops in the playbook are executed preferentially, and loopback will be performed up to 10 times.

(4)、Judge if the attacker’ address belongs to the internet or internal assets.



Parameter Settings

*Node Name: attacker address types

*Filter Rule

1 If

*Name: Internet attacker

*Rule: ${alarm.attack_ip} not in ${custom.2}

${alarm.attack_ip} | not in | ${custom.2}

+or +and

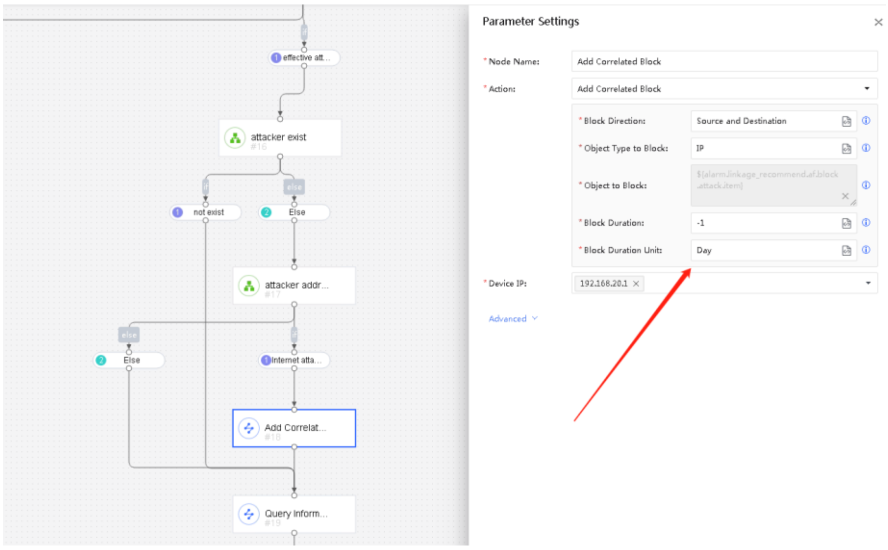
2 Else

Else If

Loopback Configuration

If enabled, the system will loop back to a previous node if the following conditions are met. Loops in the playbook are executed preferentially, and loopback will be performed up to 10 times.

(5)、Initiate correlated block to NGAF



Parameter Settings

*Node Name: Add Correlated Block

*Action: Add Correlated Block

*Block Direction: Source and Destination

*Object Type to Block: IP

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

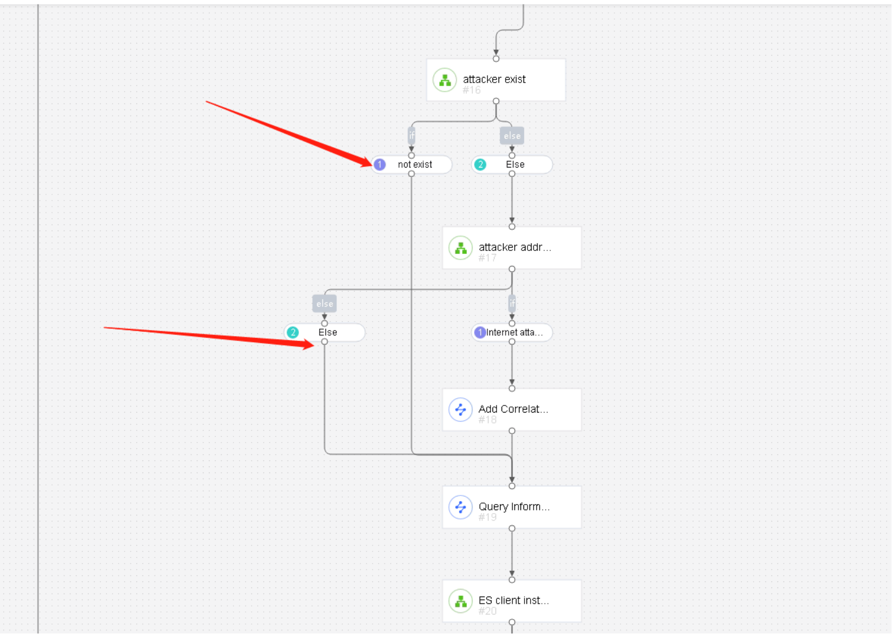
*Block Duration: -1

*Block Duration Unit: Day

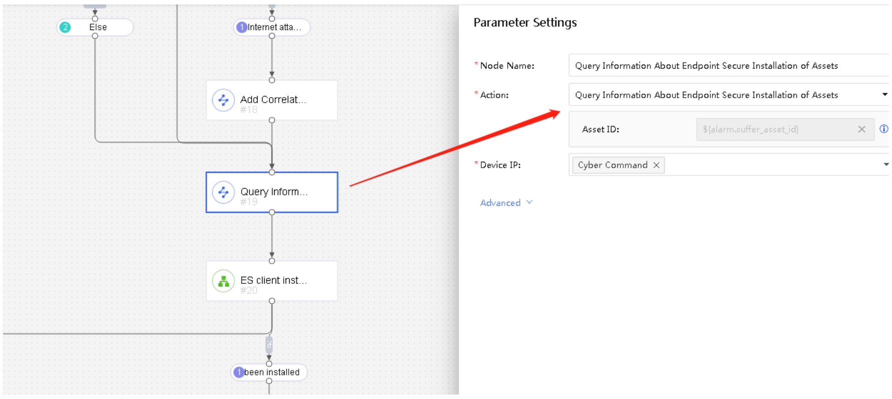
*Device IP: 192.168.20.1

Advanced

(6)、Prior to proceeding with subsequent steps, it is crucial to evaluate scenarios in which the attacker is identified as an internal asset, as well as situations where the attack’s originating address is nonexisten.



(7)、Query whether target assets have been installed ES clients.



Parameter Settings

* Node Name: Query Information About Endpoint Secure Installation of Assets

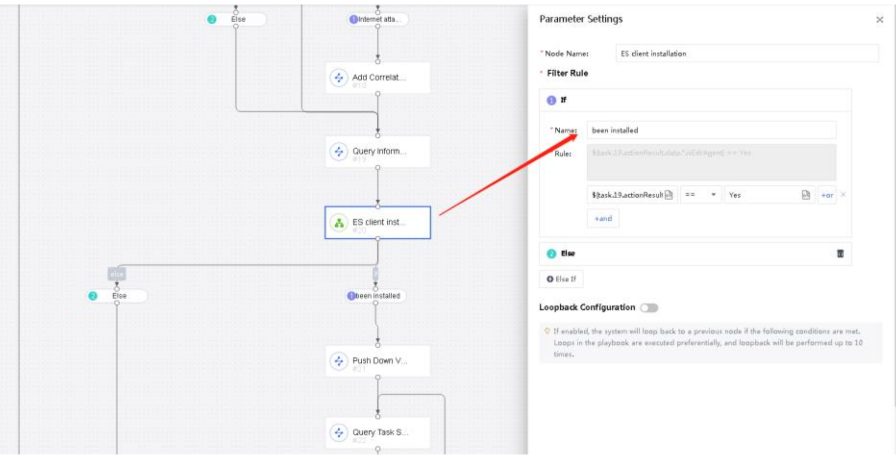
* Action: Query Information About Endpoint Secure Installation of Assets

Asset ID: ${alarm.suffer_asset_id}

* Device IP: Cyber Command ×

Advanced

(7)、 If the necessary components are installed, you can proceed with further operations. However, if they are not, the status of these alerts will be modified to 'suspended,'



Parameter Settings

* Node Name: ES client installation

* Filter Rule

1 If

* Name: been installed

Rule: ${task.19.actionResult.data.*.isEdrAgent} == Yes

${task.19.actionResult == Yes +or

+and

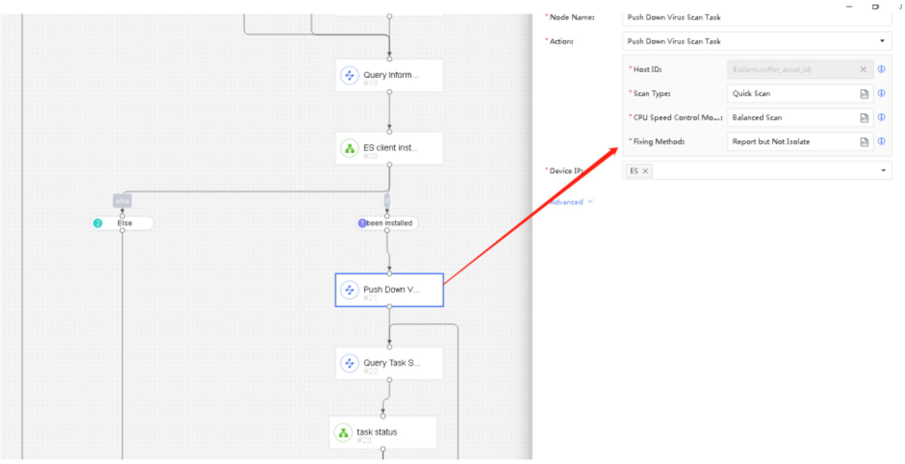
2 Else

Else If

Loopback Configuration

If enabled, the system will loop back to a previous node if the following conditions are met. Loops in the playbook are executed preferentially, and loopback will be performed up to 10 times.

(8)、 Initiate virus scan tasks for those hosts that have ES client installed



* Node Name: Push Down Virus Scan Task

* Action: Push Down Virus Scan Task

* Host ID: ${alarm.suffer_asset_id}

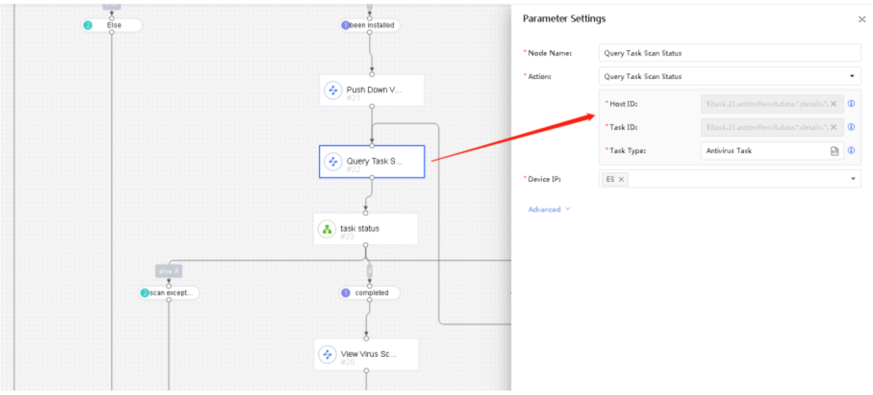
* Scan Type: Quick Scan

* CPU Speed Control Mo...: Balanced Scan

* Fixing Method: Report but Not Isolate

* Device IP: ES

（9）、 Given that virus scan tasks may take several minutes to complete, it is important to verify the completion of these tasks before proceeding.



Parameter Settings

* Node Name: Query Task Scan Status

* Action: Query Task Scan Status

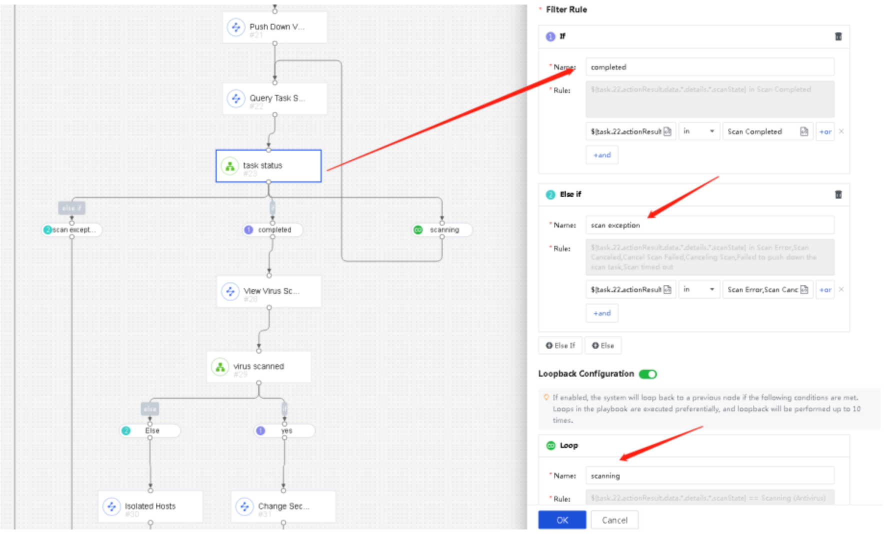
* Host ID: ${task.21.actionResult.data.*.details.*.

* Task ID: ${task.21.actionResult.data.*.details.*.

* Task Type: Antivirus Task

* Device IP: ES

（10）、 When making a decision, there will be three possible outcomes: scan exception, scanning, and completed. Each of these results requires a distinct approach. Notably, if the task is not yet finished and remains in the scanning stage, the process will loop back to the previous action



* Filter Rule

1 If

* Name: completed

* Rule: ${task.22.actionResult.data.*.details.*.scanState} in Scan Completed

${task.22.actionResult | in | Scan Completed | +or

+and

2 Else if

* Name: scan exception

* Rule: ${task.22.actionResult.data.*.details.*.scanState} in Scan Error,Scan Canceled,Cancel Scan Failed,Canceling Scan,Failed to push down the scan task,Scan timed out

${task.22.actionResult | in | Scan Error,Scan Canc | +or

+and

Loopback Configuration

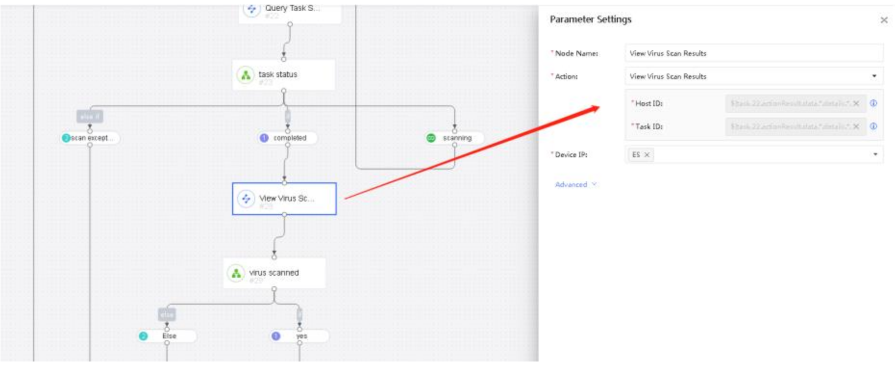
If enabled, the system will loop back to a previous node if the following conditions are met. Loops in the playbook are executed preferentially, and loopback will be performed up to 10 times.

Loop

* Name: scanning

* Rule: ${task.22.actionResult.data.*.details.*.scanState} == Scanning (Antivirus)

（11）、You have different methods regarding to the results of virus scan task.



Parameter Settings

*Node Name: View Virus Scan Results

*Action: View Virus Scan Results

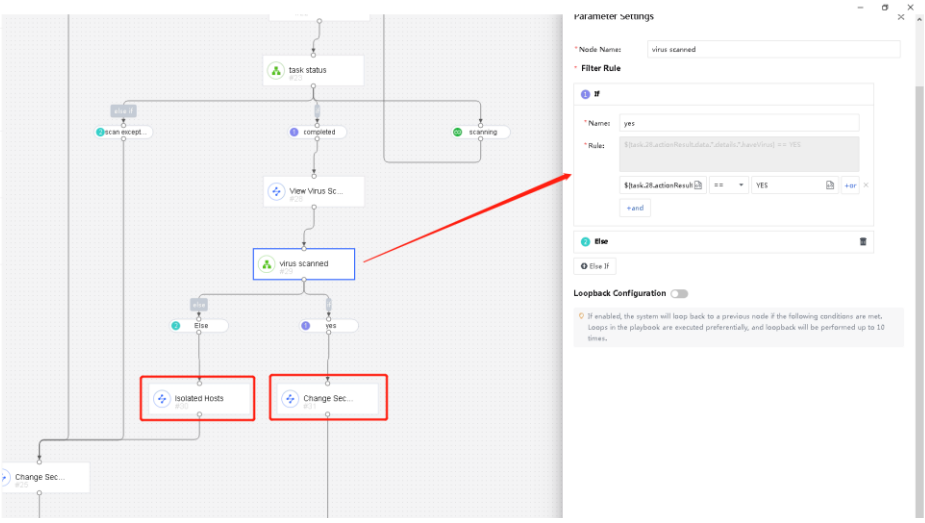
Host ID: ${task.22.actionResult.data..details.*.

Task ID: ${task.22.actionResult.data..details.*.

*Device IP: ES

Advanced

（12）、 Upon making a decision, you will isolate the hosts if the virus scan task did not detect any viruses, and remind the security administrator to conduct further analysis. However, if the scan detects viruses and automatically disposes of them, you can update the security alerts to ‘fixed’.



Parameter Settings

*Node Name: virus scanned

*Filter Rule

1 If

*Name: yes

Rule: ${task.28.actionResult.data..details.*.haveVirus} == YES

${task.28.actionResult == YES +or

+and

2 Else

Else If

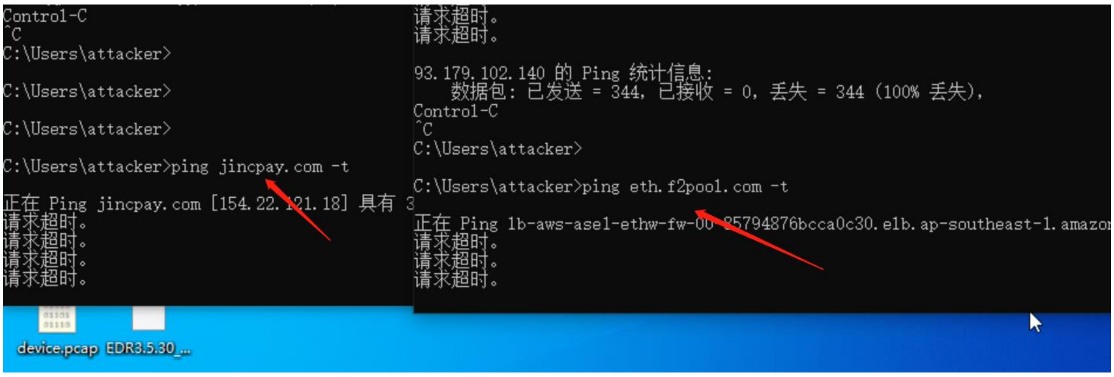
Loopback Configuration

If enabled, the system will loop back to a previous node if the following conditions are met. Loops in the playbook are executed preferentially, and loopback will be performed up to 10 times.

1.4 Strategy Effect Verification

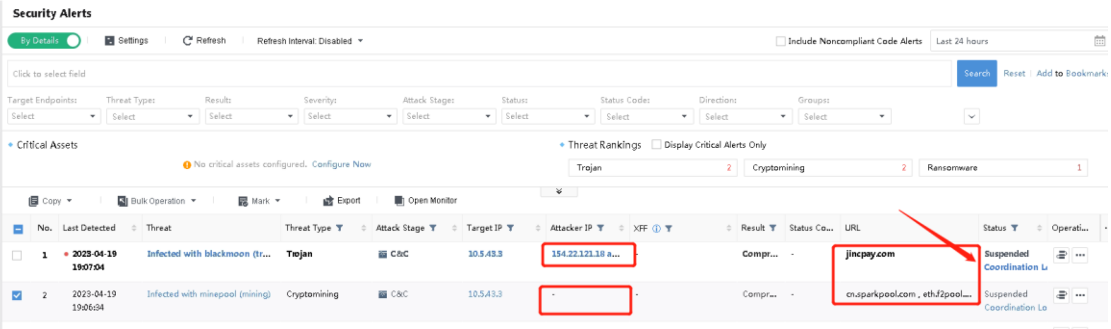
1.4.1 Test Terminal-A (without ES client)

The test terminal simulates an attack by pinging malicious domain names (jincpay.com, eth.f2pool.com). When the STA analyzes this malicious traffic, it will generate security alerts.


```
Control-C
^C
C:\Users\attacker>

C:\Users\attacker>

C:\Users\attacker>

C:\Users\attacker>ping jincpay.com -t

正在 Ping jincpay.com [154.22.121.18] 具有 3
请求超时。
请求超时。
请求超时。
请求超时。
```

```
请求超时。
请求超时。

93.179.102.140 的 Ping 统计信息:
    数据包: 已发送 = 344, 已接收 = 0, 丢失 = 344 (100% 丢失),
Control-C
^C
C:\Users\attacker>

C:\Users\attacker>ping eth.f2pool.com -t

正在 Ping lb-aws-asel-ethw-fw-00 85794876bcca0c30.elb.ap-southeast-1.amazo
请求超时。
请求超时。
请求超时。
```

Within seconds, you will observe the anticipated alerts, and simultaneously, these alerts will trigger the predefined automatic policy.

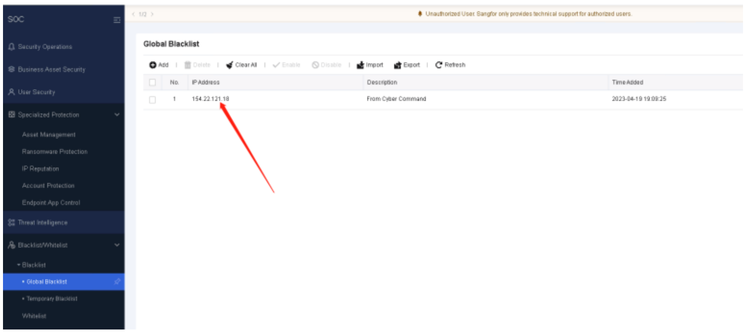


Threat Rankings	
Trojan	2
Cryptomining	2
Ransomware	1

No.	Last Detected	Threat	Threat Type	Attack Stage	Target IP	Attacker IP	XFF	Result	Status Co...	URL	Status	Operati...
1	2023-04-19 19:07:04	Infected with blackmoon (tr...	Trojan	C&C	10.5.43.3	154.22.121.18 a...	-	Compr...	-	jincpay.com	Suspended Coordination L	
2	2023-04-19 19:06:34	Infected with minepool (mining)	Cryptomining	C&C	10.5.43.3	-	-	Compr...	-	cn.sparkpool.com , eth.f2pool....	Suspended Coordination Lo	

Next, you can view the execution process of the automatic policy by clicking on "Coordination Response Details".

Check the NGAF blacklist

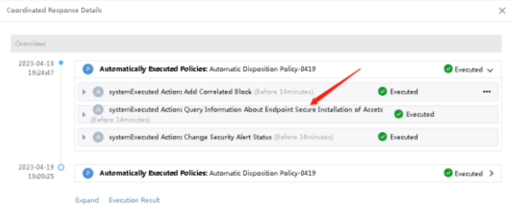


Unauthorized User. Sangfor only provides technical support for authorized users.

Global Blacklist

No.	IP Address	Description	Time Added
1	154.22.121.18	From Cyber Command	2023-04-19 19:09:25

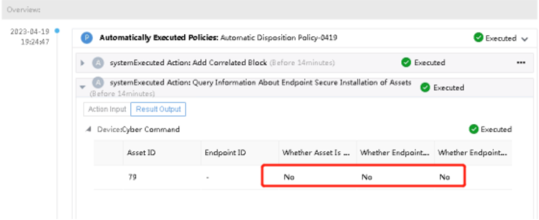
As observed, the test terminal does not have the ES client installed.



Coordinated Response Details

2023-04-19 19:24:47 Automatically Executed Policies: Automatic Disposition Policy-0419 Executed
- systemExecuted Action: Add Correlated Block (Before 14minutes) Executed
- systemExecuted Action: Query Information About Endpoint Secure Installation of Assets (Before 14minutes) Executed
- systemExecuted Action: Change Security Alert Status (Before 14minutes) Executed

2023-04-19 19:09:25 Automatically Executed Policies: Automatic Disposition Policy-0419 Executed

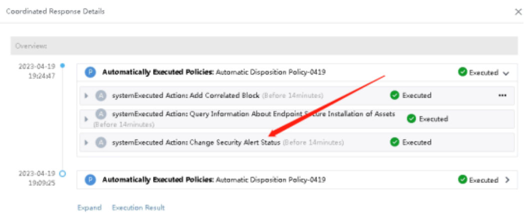


2023-04-19 19:24:47 Automatically Executed Policies: Automatic Disposition Policy-0419 Executed
- systemExecuted Action: Add Correlated Block (Before 14minutes) Executed
- systemExecuted Action: Query Information About Endpoint Secure Installation of Assets (Before 14minutes) Executed

Device:Cyber Command Executed

Asset ID	Endpoint ID	Whether Asset Is ...	Whether Endpoint...	Whether Endpoint...
79	-	No	No	No

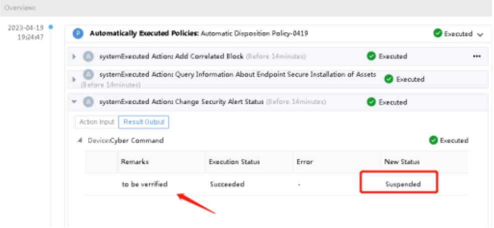
Given this situation, the appropriate course of action is to update the alert status to 'suspended'.



Coordinated Response Details

2023-04-19 19:24:47 Automatically Executed Policies: Automatic Disposition Policy-0419 Executed
- systemExecuted Action: Add Correlated Block (Before 14minutes) Executed
- systemExecuted Action: Query Information About Endpoint Secure Installation of Assets (Before 14minutes) Executed
- systemExecuted Action: Change Security Alert Status (Before 14minutes) Executed

2023-04-19 19:09:25 Automatically Executed Policies: Automatic Disposition Policy-0419 Executed



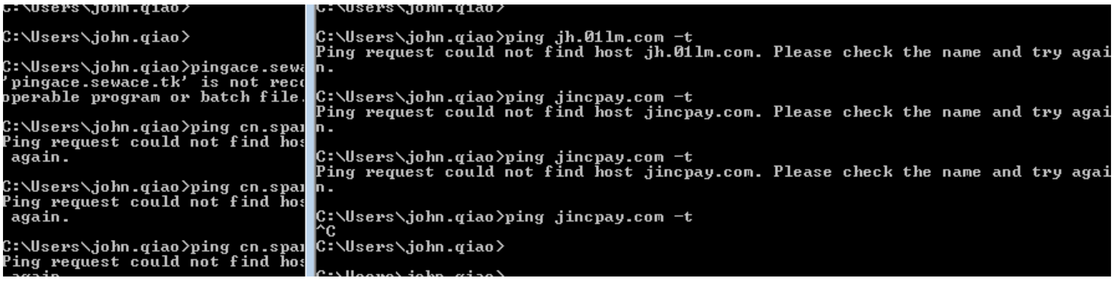
2023-04-19 19:24:47 Automatically Executed Policies: Automatic Disposition Policy-0419 Executed
- systemExecuted Action: Add Correlated Block (Before 14minutes) Executed
- systemExecuted Action: Query Information About Endpoint Secure Installation of Assets (Before 14minutes) Executed
- systemExecuted Action: Change Security Alert Status (Before 14minutes) Executed

Device:Cyber Command Executed

Remarks	Execution Status	Error	New Status
to be verrified	Succeeded	-	Suspended

1.4.2 Test Terminal-B (with ES client)

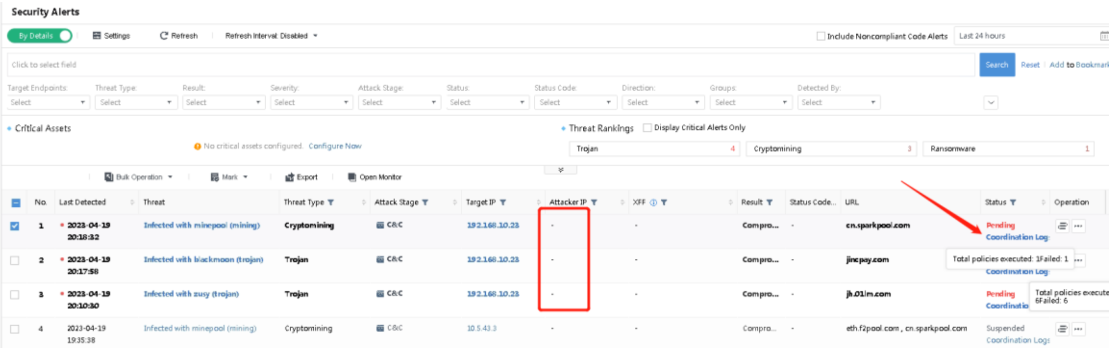
The test terminal simulates an attack by pinging malicious domain names (jincpay.com, eth.f2pool.com). When the STA analyzes this malicious traffic, it will generate security alerts.



```
C:\Users\john.qiao>

C:\Users\john.qiao>

C:\Users\john.qiao>pingace.sewa
'pingace.sewace.tk' is not reco
operable program or batch file.

C:\Users\john.qiao>ping cn.spar
Ping request could not find hos
 again.

C:\Users\john.qiao>ping cn.spar
Ping request could not find hos
 again.

C:\Users\john.qiao>ping cn.spar
Ping request could not find hos
 again.
```

```
C:\Users\john.qiao>

C:\Users\john.qiao>ping jh.01lm.com -t
Ping request could not find host jh.01lm.com. Please check the name and try agai
n.

C:\Users\john.qiao>ping jincpay.com -t
Ping request could not find host jincpay.com. Please check the name and try agai
n.

C:\Users\john.qiao>ping jincpay.com -t
Ping request could not find host jincpay.com. Please check the name and try agai
n.

C:\Users\john.qiao>ping jincpay.com -t
^C
C:\Users\john.qiao>

C:\Users\john.qiao>
```

Within seconds, you will observe the anticipated alerts, and simultaneously, these alerts will trigger the predefined automatic policy.



Security Alerts

By Details | Settings | Refresh | Refresh Interval: Disabled | ☐ Include Noncompliant Code Alerts | Last 24 hours

Click to select field | Search | Reset | Add to Bookmark

Target Endpoints: Select | Threat Type: Select | Result: Select | Severity: Select | Attack Stage: Select | Status: Select | Status Code: Select | Direction: Select | Groups: Select | Detected By: Select

Critical Assets

No critical assets configured. Configure Now

Threat Rankings ☐ Display Critical Alerts Only

Trojan	4
Cryptomining	3
Ransomware	1

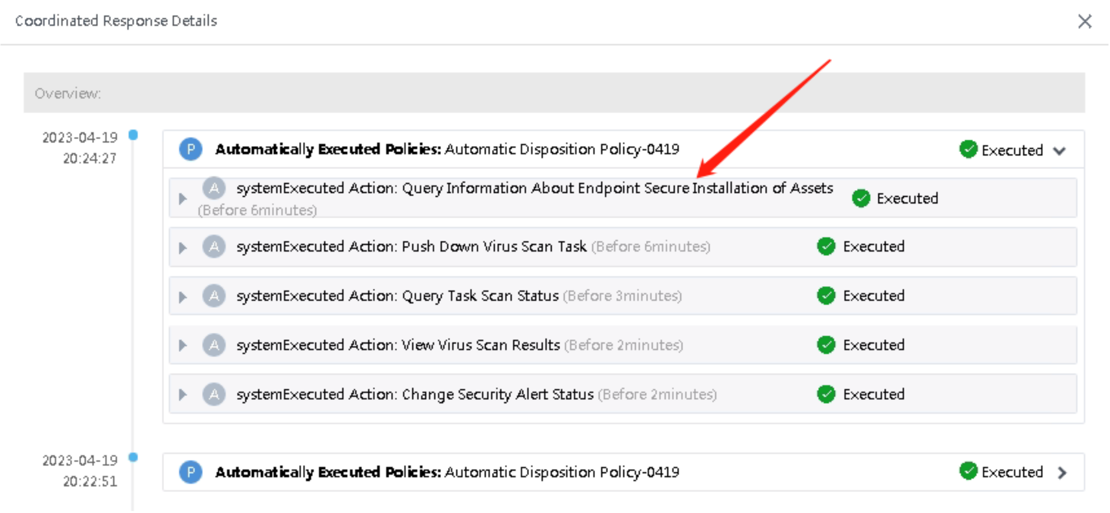
Bulk Operation | Mark | Export | Open Monitor

	No.	Last Detected	Threat	Threat Type	Attack Stage	Target IP	Attacker IP	XFF	Result	Status Code...	URL	Status	Operation
☑	1	2023-04-19 20:18:32	Infected with minepool (mining)	Cryptomining	C&C	192.168.10.23	-	-	Compro...	-	cn.sparkpool.com	Pending Coordination Log	
☐	2	2023-04-19 20:17:58	Infected with blackmoon (trojan)	Trojan	C&C	192.168.10.23	-	-	Compro...	-	jincpay.com	Coordination Log	
☐	3	2023-04-19 20:10:30	Infected with zusy (trojan)	Trojan	C&C	192.168.10.23	-	-	Compro...	-	jh.01lm.com	Pending Coordinatio	
☐	4	2023-04-19 19:35:38	Infected with minepool (mining)	Cryptomining	C&C	10.5.43.3	-	-	Compro...	-	eth.f2pool.com , cn.sparkpool.com	Suspended Coordination Logs	

Total policies executed: 1Failed: 1

Total policies execute 6Failed: 6

Next, you can view the execution process of the automatic policy by clicking on “Coordination Response Details”.



Coordinated Response Details

Overview:

2023-04-19 20:24:27

P **Automatically Executed Policies:** Automatic Disposition Policy-0419 — Executed

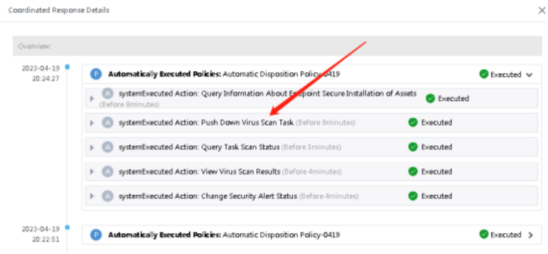
- A systemExecuted Action: Query Information About Endpoint Secure Installation of Assets (Before 6minutes) — Executed
- A systemExecuted Action: Push Down Virus Scan Task (Before 6minutes) — Executed
- A systemExecuted Action: Query Task Scan Status (Before 3minutes) — Executed
- A systemExecuted Action: View Virus Scan Results (Before 2minutes) — Executed
- A systemExecuted Action: Change Security Alert Status (Before 2minutes) — Executed

2023-04-19 20:22:51

P **Automatically Executed Policies:** Automatic Disposition Policy-0419 — Executed

As there is no identifiable attack IP, the system will execute the "Query Information About Endpoint Secure Installation of Assets".

Following that, initiate a virus scan task targeted at the Endpoint Security (ES) client.



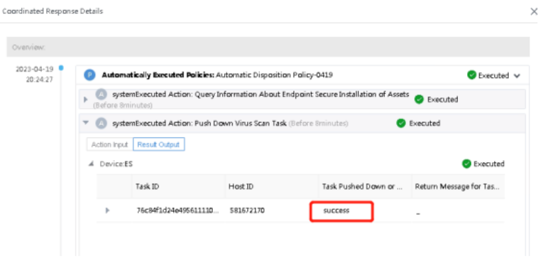
Coordinated Response Details

Overview:

2023-04-19 20:24:27 — **Automatically Executed Policies:** Automatic Disposition Policy-0419 — Executed

- systemExecuted Action: Query Information About Endpoint Secure Installation of Assets (Before 8minutes) — Executed
- systemExecuted Action: Push Down Virus Scan Task (Before 8minutes) — Executed
- systemExecuted Action: Query Task Scan Status (Before 5minutes) — Executed
- systemExecuted Action: View Virus Scan Results (Before 4minutes) — Executed
- systemExecuted Action: Change Security Alert Status (Before 4minutes) — Executed

2023-04-19 20:22:51 — **Automatically Executed Policies:** Automatic Disposition Policy-0419 — Executed



Coordinated Response Details

Overview:

2023-04-19 20:24:27 — **Automatically Executed Policies:** Automatic Disposition Policy-0419 — Executed

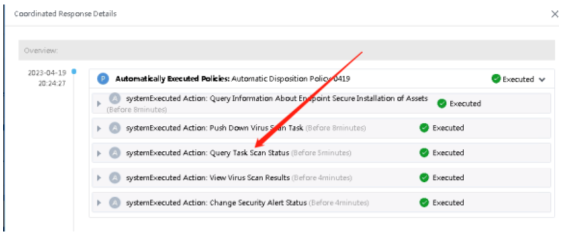
- systemExecuted Action: Query Information About Endpoint Secure Installation of Assets (Before 8minutes) — Executed
- systemExecuted Action: Push Down Virus Scan Task (Before 8minutes) — Executed

Action Input | Result Output

Device:ES — Executed

Task ID	Host ID	Task Pushed Down or ...	Return Message for Tas...
76c84f1d24e495611110...	581672170	success	-

A few minutes later, it becomes evident that the task has been completed.

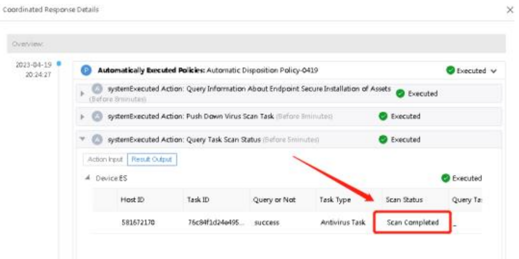


Coordinated Response Details

Overview:

2023-04-19 20:24:27 — **Automatically Executed Policies:** Automatic Disposition Policy-0419 — Executed

- systemExecuted Action: Query Information About Endpoint Secure Installation of Assets (Before 8minutes) — Executed
- systemExecuted Action: Push Down Virus Scan Task (Before 8minutes) — Executed
- systemExecuted Action: Query Task Scan Status (Before 5minutes) — Executed
- systemExecuted Action: View Virus Scan Results (Before 4minutes) — Executed
- systemExecuted Action: Change Security Alert Status (Before 4minutes) — Executed



Coordinated Response Details

Overview:

2023-04-19 20:24:27 — **Automatically Executed Policies:** Automatic Disposition Policy-0419 — Executed

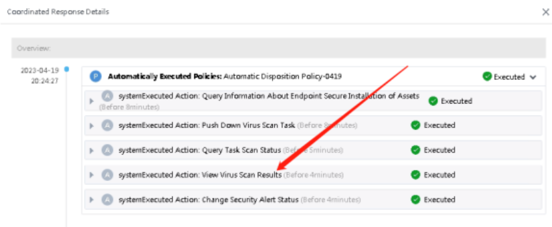
- systemExecuted Action: Query Information About Endpoint Secure Installation of Assets (Before 8minutes) — Executed
- systemExecuted Action: Push Down Virus Scan Task (Before 8minutes) — Executed
- systemExecuted Action: Query Task Scan Status (Before 5minutes) — Executed

Action Input | Result Output

Device:ES — Executed

Host ID	Task ID	Query or Not	Task Type	Scan Status	Query Ta
581672170	76c84f1d24e495...	success	Antivirus Task	Scan Completed	-

Upon examining the results of the virus scan task, we can observe that it has detected some malicious virus files on the desktop, as they were placed there beforehand for testing purposes.

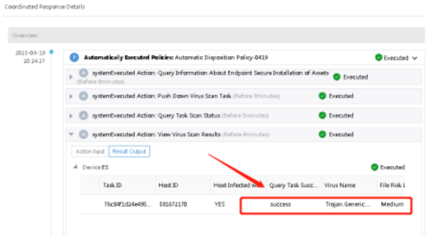


Coordinated Response Details

Overview:

2023-04-19 20:24:27 — **Automatically Executed Policies:** Automatic Disposition Policy-0419 — Executed

- systemExecuted Action: Query Information About Endpoint Secure Installation of Assets (Before 8minutes) — Executed
- systemExecuted Action: Push Down Virus Scan Task (Before 8minutes) — Executed
- systemExecuted Action: Query Task Scan Status (Before 5minutes) — Executed
- systemExecuted Action: View Virus Scan Results (Before 4minutes) — Executed
- systemExecuted Action: Change Security Alert Status (Before 4minutes) — Executed



Coordinated Response Details

Overview:

2023-04-19 20:24:27 — **Automatically Executed Policies:** Automatic Disposition Policy-0419 — Executed

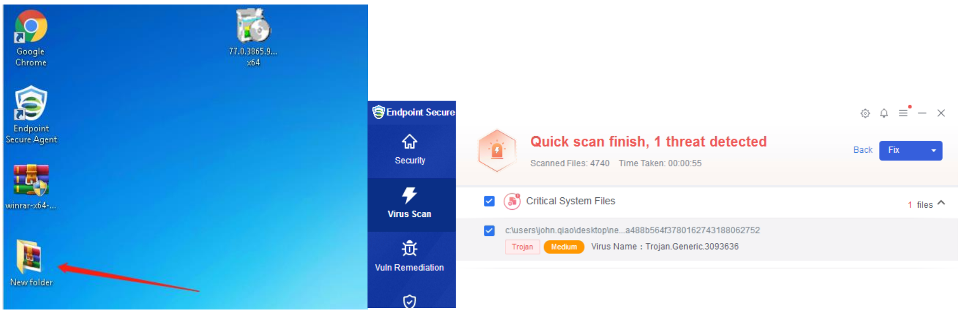
- systemExecuted Action: Query Information About Endpoint Secure Installation of Assets (Before 8minutes) — Executed
- systemExecuted Action: Push Down Virus Scan Task (Before 8minutes) — Executed
- systemExecuted Action: Query Task Scan Status (Before 5minutes) — Executed
- systemExecuted Action: View Virus Scan Results (Before 4minutes) — Executed

Action Input | Result Output

Device:ES — Executed

Task ID	Host ID	Host Infected w...	Query Task Succ...	Virus Name	File Risk L
76c84f1d24e495...	581672170	YES	success	Trojan.Generic...	Medium

You can also view the scan results in the Endpoint Security (ES) client or the Endpoint Security Manager (ES Mgr).



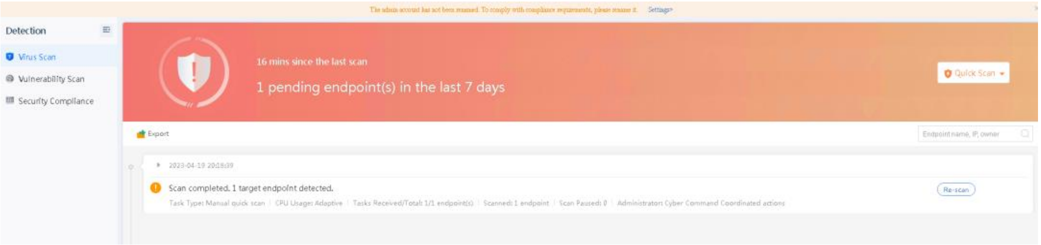
Quick scan finish, 1 threat detected

Scanned Files: 4740 Time Taken: 00:00:55

☑ Critical System Files — 1 files

☑ c:\users\john.qiao\desktop\ne...a488b564f3780162743188062752

Trojan | Medium | Virus Name：Trojan.Generic.3093636



The admin account has not been renamed. To comply with compliance requirements, please rename it. Settings>

16 mins since the last scan

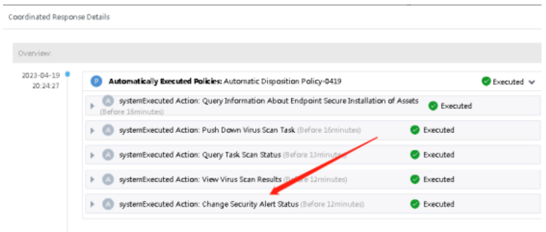
1 pending endpoint(s) in the last 7 days

2023-04-19 20:18:39

Scan completed. 1 target endpoint detected.

Task Type: Manual quick scan | CPU Usage: Adaptive | Tasks Received/Total: 1/1 endpoint(s) | Scanned: 1 endpoint | Scan Paused: 0 | Administrator: Cyber Command Coordinated actions

The final step in the process is to update the disposal status.



Coordinated Response Details

Overview:

2023-04-19 20:24:27

Automatically Executed Policies: Automatic Disposition Policy-0419 ✓ Executed

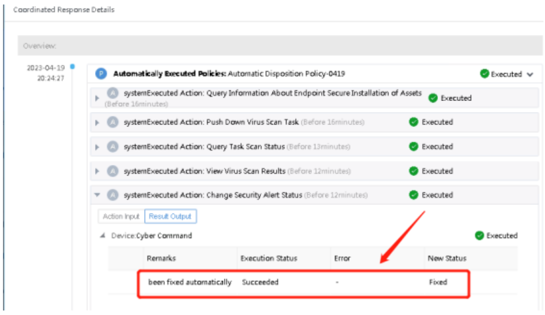
systemExecuted Action: Query Information About Endpoint Secure Installation of Assets (Before 16minutes) ✓ Executed

systemExecuted Action: Push Down Virus Scan Task (Before 16minutes) ✓ Executed

systemExecuted Action: Query Task Scan Status (Before 13minutes) ✓ Executed

systemExecuted Action: View Virus Scan Results (Before 12minutes) ✓ Executed

systemExecuted Action: Change Security Alert Status (Before 12minutes) ✓ Executed



Coordinated Response Details

Overview:

2023-04-19 20:24:27

Automatically Executed Policies: Automatic Disposition Policy-0419 ✓ Executed

systemExecuted Action: Query Information About Endpoint Secure Installation of Assets (Before 16minutes) ✓ Executed

systemExecuted Action: Push Down Virus Scan Task (Before 16minutes) ✓ Executed

systemExecuted Action: Query Task Scan Status (Before 13minutes) ✓ Executed

systemExecuted Action: View Virus Scan Results (Before 12minutes) ✓ Executed

systemExecuted Action: Change Security Alert Status (Before 12minutes) ✓ Executed

Device:Cyber Command ✓ Executed

Remarks	Execution Status	Error	New Status
been fixed automatically	Succeeded	-	Fixed

1.5 Conclusion

From the above example, it is evident that playbook policies can significantly reduce manual intervention for specific types of threats. On the other hand, these policies can also be relied upon in certain scenarios to control the spread of an attack, such as during nighttime hours when security engineers may not typically be on duty. This demonstrates the value of automated policies in maintaining a secure environment and efficiently addressing potential threats, even in the absence of manual oversight.