



Sangfor Correlated Policy Practice Guidance

Document Version

v1.0

Released on

2023-04-24



Copyright © Sangfor Technologies Inc. 2023. All rights reserved.

Unless otherwise stated or authorized, Sangfor Technologies Inc. (hereinafter referred to as "Sangfor") and its affiliates reserve all intellectual property rights, including but not limited to copyrights, trademarks, patents, trade secrets, and related rights to text, images, pictures, photographs, audio, videos, charts, colors, and layouts as presented in or concerning this document and content therein. Without prior written consent of Sangfor, this document and content therein must not be reproduced, forwarded, adapted, modified or displayed or distributed by any other means for any purpose.

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
	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
	Indicates a hazardous situation, which if not avoided, could result in minor or moderate injury.
	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.
	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

Technical Support	1
Change Log.....	2
1 Case.....	4
1.1 Scene.....	4
1.1.1 Customer Requirements	4
1.1.2 Implementation Method Analysis.....	4
1.2 Network Toplogy	6
1.3 Configuration Process	6
1.3.1 Policy Settings.....	6
1.3.2 Creating playbook policy	7
1.4 Test Validity.....	9
1.5 Conclusion	10

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	Continuous Threat Detection	NGAF、CC	detection and response in time,improve operation effeciency

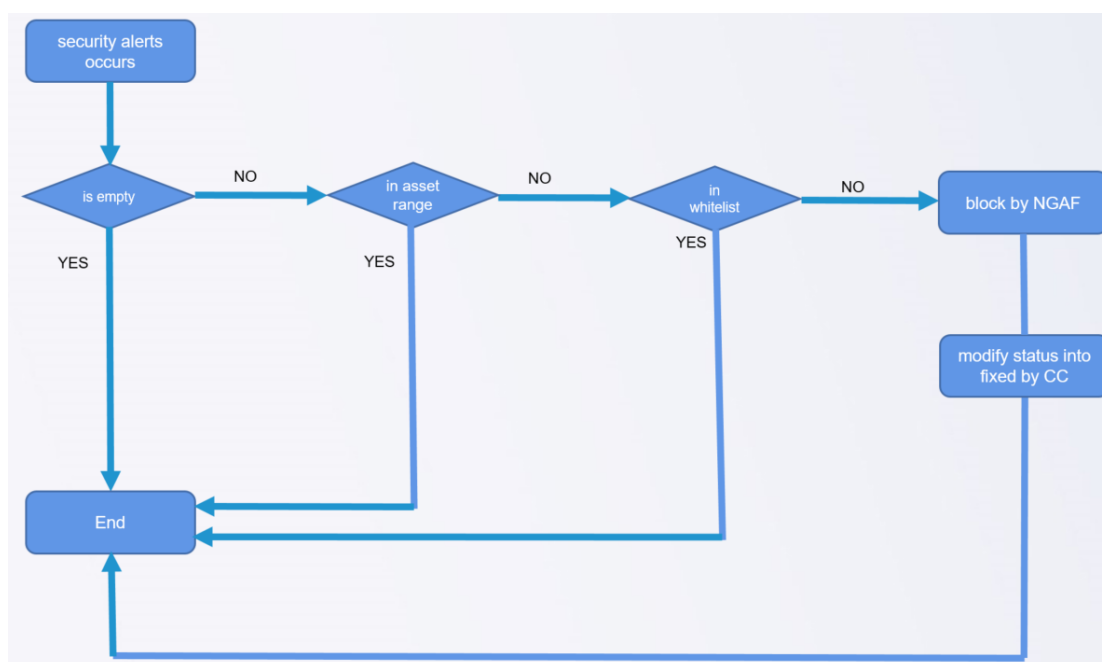
1.1 Scene

1.1.1 Customer Requirements

A branch of customer, as a defender, is participating external offensive and defensive drills. There are totally 4 NGAFs which need to be operated and managed in the customer network. 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.

1.1.2 Implementation Method Analysis

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.



- **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 attacker's IP does not exist, the policy will end directly. If it exists, the system will proceed to make a subsequent judgment regarding whether it is an intranet asset address.

Security Alerts

Click to select field

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

Include Noncompliant Code Alerts Last 24 hours

Threat Rankings Display Critical Alerts Only

No.	Last Detected	Threat	Threat Type	Attack Stage	Target IP	Attacker IP	Result	Status Code	URL	Status	Operation
1	2023-04-24 23:50:34	Access to malicious domain name...	Rootkit Virus	C&C	10.3.8.8	-	Compre...	-	updateconnection.com_sacktop...	Pending	...
2	2023-04-24 23:50:21	Access to malicious domain name...	Bots	C&C	192.168.148.198	-	Compre...	-	v1.kitaplu.ru_v1.mpgangnet...	Pending	...
3	2023-04-24 23:50:21	Access to malicious domain name...	Trojan	C&C	192.168.148.198	-	Compre...	-	update-letblumen.ru_update88...	Pending	...
4	2023-04-24 23:50:21	Access to malicious domain name...	Trojan	C&C	192.168.148.198	-	Compre...	-	v1.kitaplu.ru_v1.mpgangnet...	Pending	...
5	2023-04-24 23:48:16	Access to malicious domain name...	Infectious Virus	C&C	192.168.148.198	-	Compre...	-	enlagrains.com_sp.sasatayn.pl	Pending	...
6	2023-04-24 23:54:29	Communication via DNS tunnel	DNS Tunneling	C&C	10.1.1.1	-	Compre...	-	-	Pending	...
7	2023-04-24 23:49:21	Access to malicious domain name...	Trojan	C&C	192.168.148.198	-	Compre...	-	npkghemore.biz	Pending	...
8	2023-04-24 23:49:16	Access to malicious domain name...	Other Hacking Tools	C&C	172.20.64.80	-	Compre...	-	@B07.dnlog.cn_vnuu.dnlog.cn	Pending	...

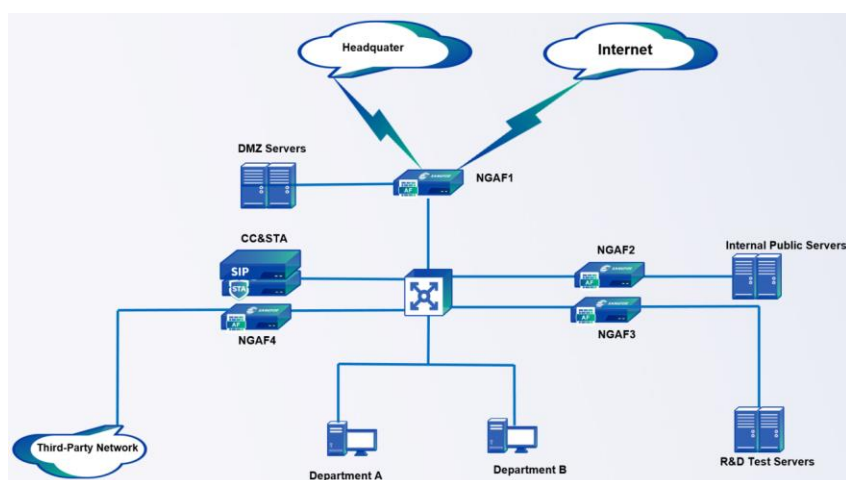
- **Step3:** If the attack's IP is belonged to intranet asset address, the policy will end directly. If not, the system will proceed to make a sub subsequent judgment regarding whether it is belonged whitelist address.
- **Step 4:** If the attacker's IP is belonged to whitelist, the policy will end directly. If not, the system will proceed to push down the block to NGAF.

Security Alerts													
No.	Last Detected	Threat	Threat Type	Attack Stage	Target IP	Attacker IP	Result	Status Code	URL	Status	Oper		
1	2023-04-18 22:05:19	Webshell communication	Webshell Access	CC/C	10.80.80.89	200.200.222.93(nat)	Success	-	10.80.80.89/php/phpf_321.php	Pending			
2	2023-04-18 09:09:01	Webshell communication	Webshell Access	CC/C	10.80.80.89	200.200.222.93(nat)	Success	-	10.80.80.89/php/phpf_321.php	Pending			
3	2023-04-18 09:09:01	XSS attack	XSS Attack	Exploitation	10.80.80.89	200.200.222.93(nat)	Attempt	200	10.80.80.89/php/phpf_321.php	Pending			
4	2023-04-18 23:09:40	XSS attack	XSS Attack	Exploitation	10.80.80.89	200.200.222.93(nat)	Attempt	200	10.80.80.89/php/phpf_321.php	Pending			
5	2023-04-18 23:09:21	General XSS Attack	XSS Attack	Exploitation	10.80.26.10	200.200.88.26(nat)	Failed	404	5.5.5.5/et	Pending			
6	2023-04-18 23:09:21	General XSS Attack	XSS Attack	Exploitation	10.80.26.10	200.200.88.26(nat)	Attempt	-	5.5.5.5/et	Pending			
7	2023-04-18 09:07:00	General XSS Attack	XSS Attack	Exploitation	10.80.26.10	200.200.88.26(nat)	Attempt	-	5.5.5.5/et	Pending			
8	2023-04-18 10:02:37	General XSS Attack	XSS Attack	Exploitation	10.80.26.10	200.200.88.26(nat)	Failed	404	5.5.5.5/et	Pending			
9	2023-04-18 19:03:53	Apache Data Server Side Request	Open Source and C...	Propagation	192.168.180.228	192.200.41.24	Attempt	800	192.168.180.228/0002/solu/Stack...	Pending			
10	2023-04-18 09:12:42	Apache Data Server Side Request	Open Source and C...	Propagation	192.168.180.228	192.200.41.24	Attempt	800	192.168.180.228/0002/solu/Stack...	Pending			
11	2023-04-18 23:02:10	Remote command execution via ...	WinRM Command E...	Propagation	192.168.201.148	192.168.201.1 against the host	Success	200	192.168.201.148/0002/woman	Pending			
12	2023-04-18 09:02:04	Remote command execution via ...	WinRM Command E...	Propagation	192.168.201.148	192.168.201.1 against the host	Success	200	192.168.201.148/0002/woman	Pending			
13	2023-04-18 03:10:23	ORACLE Server Broker Remote Exploit	Database Exploit	Propagation	192.168.201.1	192.168.201.10	Attempt	-	-	Pending			

- **Step 5:** The NGAFs device will block the Internet attacker IP pushed down by CC, and then CC will modify the alerts status into fixed.

1.2 Network Toplogy

Based on the topology provided, the customer has implemented the Security Threat Analytics (STA), Cyber Command (CC), and 4 Next-Generation Application Firewalls (NGAF) for protecting different security zones.



1.3 Configuration Process

1.3.1 Policy Settings

Select security alert types, execute automatically, security alert, all attack types;

Policy Settings ×

Basic Info

* Policy Name:

Policy Description: 0/4096

* Policy Type:

Execution Method: ☒ Execute Automatically ☐ Execute Manually

Trigger Type: ☐ Security Incident ☒ Security Alert

Conditions for Execution

Condition 1: in

+ 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.

1.3.2 Creating playbook policy

(1)、Create a constant and fill in whitelist ip addresses, create another constant and fill in intranet assets address range.

Automatic Disposition Policy-0419

Nodes

Constants

<|

2 Constants

Add

internal

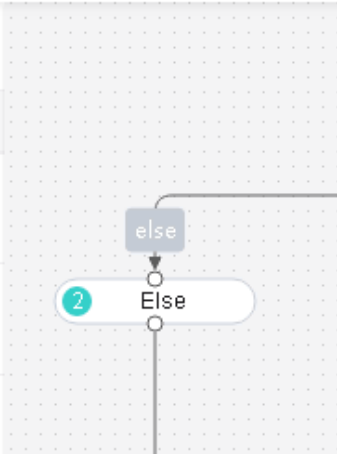

172.16.0.1-172.16.255.254,192.168.0.1...

...

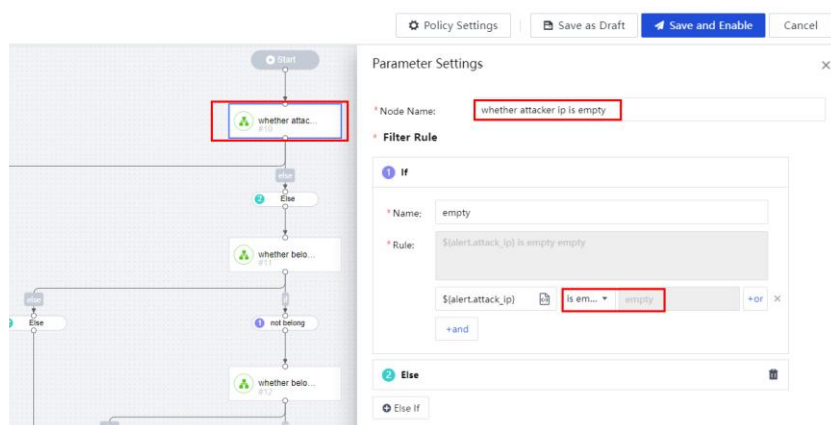
null

0.0.0.0

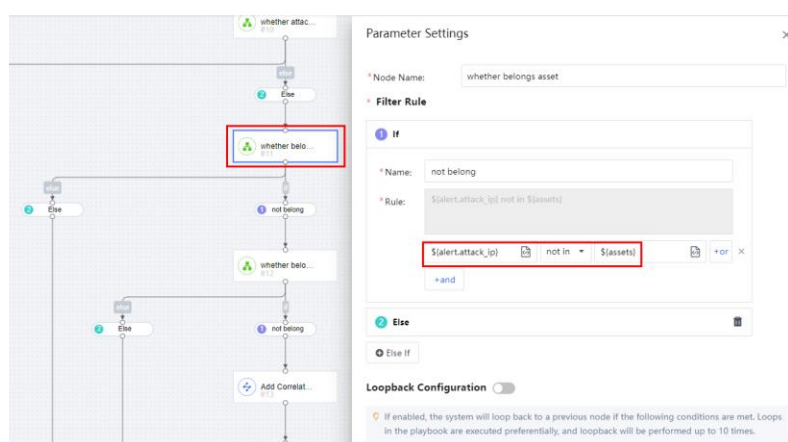
...



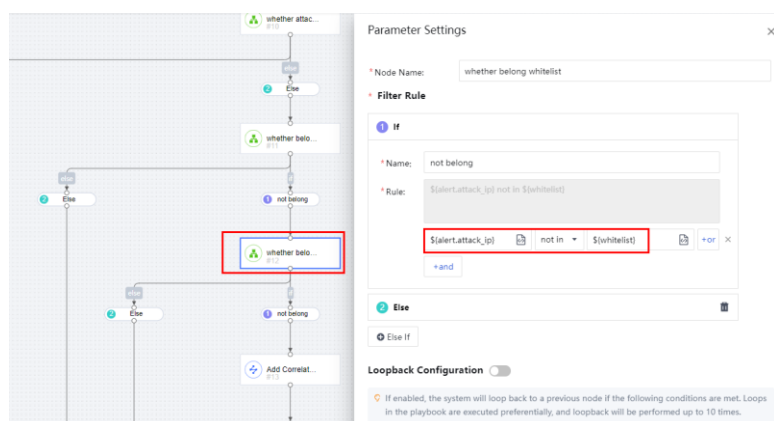
(2)、Decision, excludes the case where the attacker ip is empty.



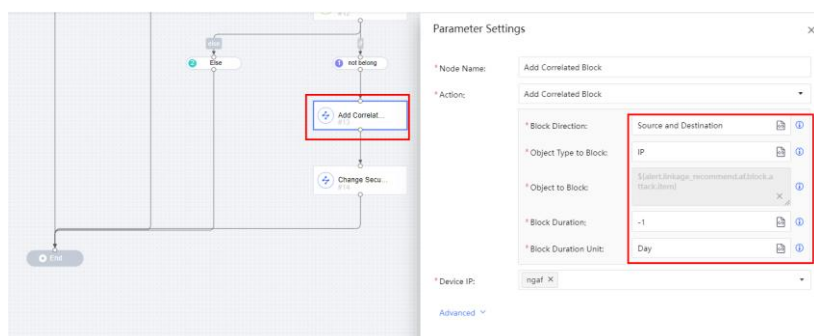
(3)、Define a decision, if the attacker is an intranet address in security alerts;



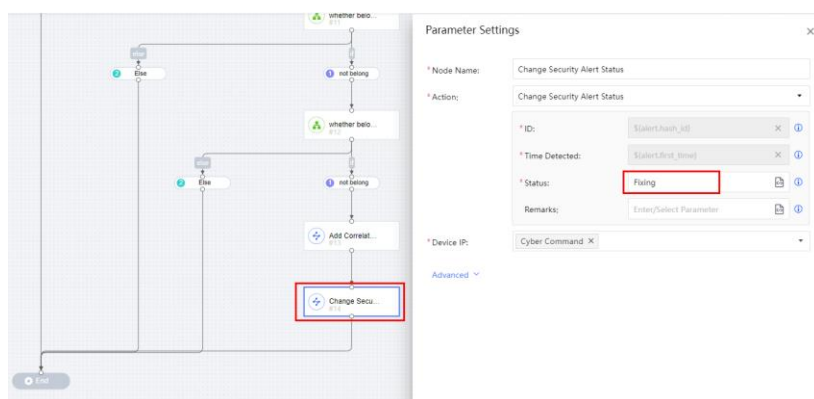
(4)、Decision, excludes the situation that the attacker ip is in the white list address in security alerts.



(5)、Initiate correlated block to NGAF



(6)、Action, modify the disposal status of corresponding security alert into fixing.



1.4 Test Validity

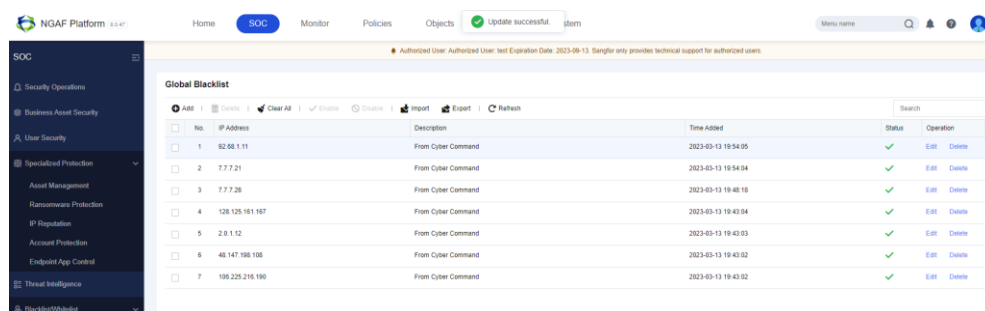
The security alerts flush persistently as usual, when the policy is enabled, new items will hit and executed automatically.

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	-	Compl...	403	26788.server.dnssec.sangfor...	Fixed
2	2023-03-12 23:59:25	Cobalt Strike backdoor	CobaltStrike	Propagation	192.168.1.5	10.100.18.20	-	Compl...	403	26788.server.dnssec.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
4	2023-03-13 19:40:54	Weak Web password	WEB	Weaknesses	10.100.4.248	2.0.1.12/Pran...	-	Succeed	-	10.100.4.248/shopee/	Fixing
5	2023-03-13 19:48:04	WebShell file upload	WebShell Upload	Exploitation	192.168.100.200	128.128.161.1...	-	Attem...	-	http://10.100.12.6.8008/	Fixing
6	2023-03-13 19:43:05	Fast brute-force attack on S...	Brute Force Atta...	Reconnaissance...	10.0.16.8 against t	106.225.216.1...	-	Attem...	-	-	Fixing
7	2023-03-13 19:44:44	Phishing email	Phishing Email	Exploitation	7.7.7.28	7.7.7.21	-	Attem...	-	-	Fixing
8	2023-03-13 19:40:54	Plaintext transmission of th...	Unencrypted W...	Weaknesses	10.100.4.248	2.0.1.12/Pran...	-	Attem...	200	10.100.4.248/shopee/pass...	Fixing
9	2023-03-13 19:54:03	Exploit SQL Server attacks	Database Exploit	Exploitation	10.100.17.237	48.147.198.10...	-	Attem...	-	-	Fixing
10	2023-03-13 19:53:48	SSH Server Brute Force Exp...	Web System Exp...	Exploitation	10.0.16.8	106.225.216.1...	-	Attem...	-	-	Fixing
11	2023-03-13 19:48:04	WebShell Web Trojan Detect...	WebShell Upload	Exploitation	192.168.100.200	128.128.161.1...	-	Attem...	400	10.100.12.6.8008/	Fixing

It is available to view the overall coordinated actions in response history page.

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 Comm...	Cyber Command	2023-03-13 19:59:51	Trigger Policy system	Executed	View
2	Add Correlated Block	192.168.1.10	Sangfor NGAF v6.0.8 to v...	Sangfor NGAF v6.0.8 L...	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 Comm...	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 v6.0.8 to v...	Sangfor NGAF v6.0.8 L...	ngaf	2023-03-13 19:59:50	Trigger Policy system	Executed	View Undo
5	Change Security Alert...	10.100.4.248	Sangfor Cyber Command...	Sangfor Cyber Comm...	Cyber Command	2023-03-13 19:59:49	Trigger Policy system	Executed	View
6	Add Correlated Block	10.100.4.248	Sangfor NGAF v6.0.8 to v...	Sangfor NGAF v6.0.8 L...	ngaf	2023-03-13 19:59:49	Trigger Policy system	Executed	View Undo
7	Change Security Alert...	7.7.7.28/7.7.7.21	Sangfor Cyber Command...	Sangfor Cyber Comm...	Cyber Command	2023-03-13 19:59:48	Trigger Policy system	Executed	View

Login NGAF devices and blocking internet attacker IP addresses can be viewed.



The screenshot displays the NGAF Platform SOC interface. The top navigation bar includes 'Home', 'SOC', 'Monitor', 'Policies', and 'Objects'. A status message 'Update successful' is visible. The left sidebar lists various security modules, with 'SOC' selected. The main content area shows the 'Global Blacklist' table, which lists blocked IP addresses and their associated descriptions. The table includes columns for 'No.', 'IP Address', 'Description', 'Time Added', 'Status', and 'Operation'.

No.	IP Address	Description	Time Added	Status	Operation
1	92.88.1.11	From Cyber Command	2023-05-13 19:54:05	✓	Edit Delete
2	7.7.7.21	From Cyber Command	2023-05-13 19:54:04	✓	Edit Delete
3	7.7.7.26	From Cyber Command	2023-05-13 19:48:19	✓	Edit Delete
4	128.126.161.167	From Cyber Command	2023-05-13 19:43:04	✓	Edit Delete
5	2.0.1.12	From Cyber Command	2023-05-13 19:43:03	✓	Edit Delete
6	48.147.198.106	From Cyber Command	2023-05-13 19:43:02	✓	Edit Delete
7	106.225.216.186	From Cyber Command	2023-05-13 19:43:02	✓	Edit Delete

1.5 Conclusion

From the above example, it is evident that playbook policies of CC can significantly block attacks from internet to intranet with NGAF. The capability can meet the requirement well in some scenarios, such as offensive and defensive, strict inbound access...etc.