



SANGFOR



Cyber Command

Best Practices for Scenarios_How to Correlate with Endpoint Secure to Simply the Operation

Version 3.0.49



Change Log

Date	Change Description
March 3, 2021	Document release.
May 17, 2021	Document update.

CONTENT

Chapter 1 Scenario	1
1.1 Scenario	1
1.2 Environment	1
1.2.1 Network Environment	1
1.3 Precautions	1
Chapter 2 Configuration.....	2
2.1 Configure Cyber Command	2
Chapter 3 Correlation.....	5
3.1 Generate Security Logs and Synchronize to Cyber Command	5

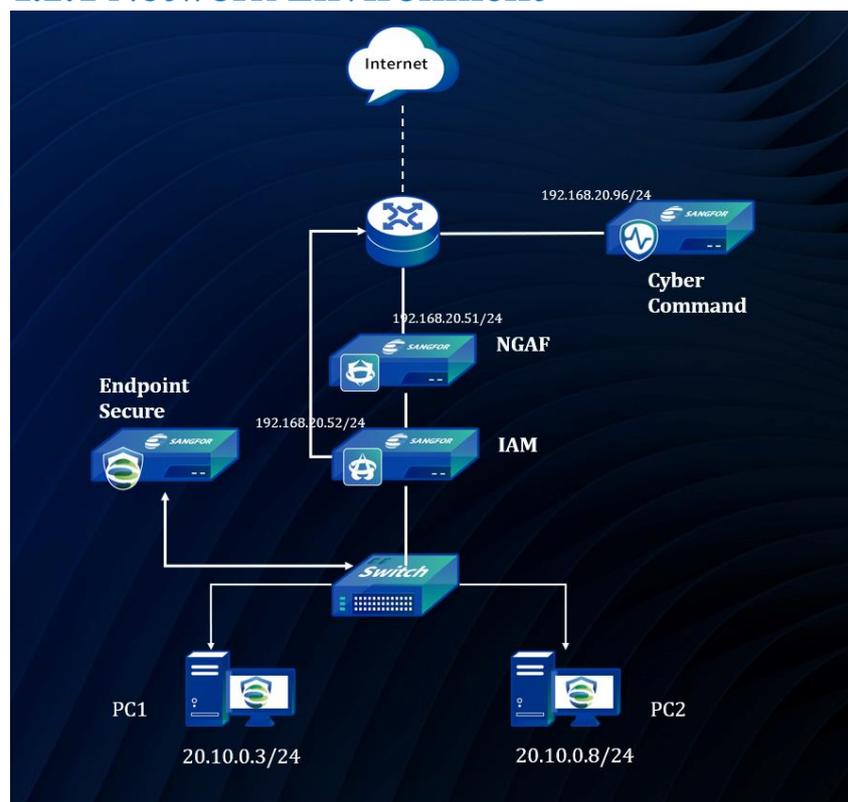
Chapter 1 Scenario

1.1 Scenario

Customers use Cyber Command to collect network traffic and system logs, effectively detect overall network security, quickly sort out asset information, monitor abnormal access behaviors in real time, and perform real-time detection and alerting on external attacks, active server outreach, internal horizontal penetration and other behaviors. Once a security incident occurs, it can be quickly alerted and dealt with to protect the overall safe and effective operation of the private network. Through linkage, Sangfor Endpoint Secure platform issues security policies to block corresponding attacks in a timely manner. For lost hosts of servers and terminals, a one-click scanning strategy is issued through the linkage with the Endpoint Secure management platform to quickly detect and kill malicious programs, and the Micro-Segmentation function of Endpoint Secure Agent is used to block host attacks and prevent further threats from spreading.

1.2 Environment

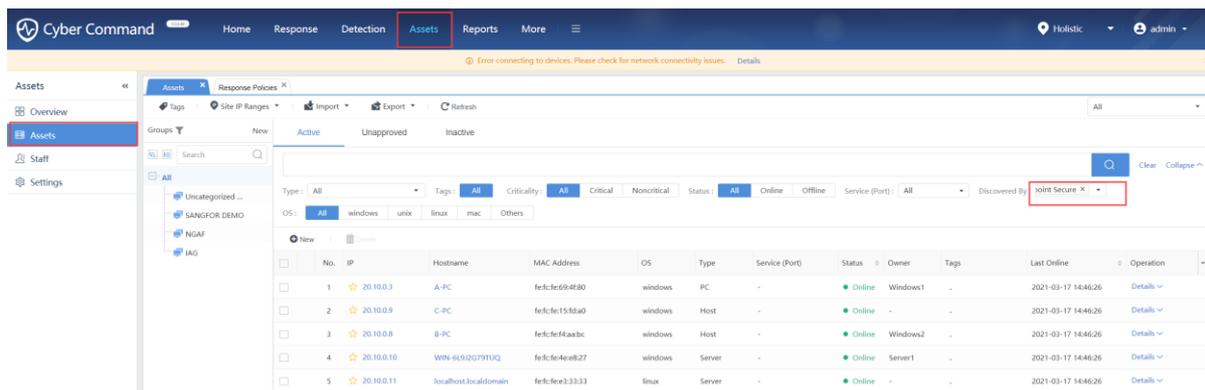
1.2.1 Network Environment



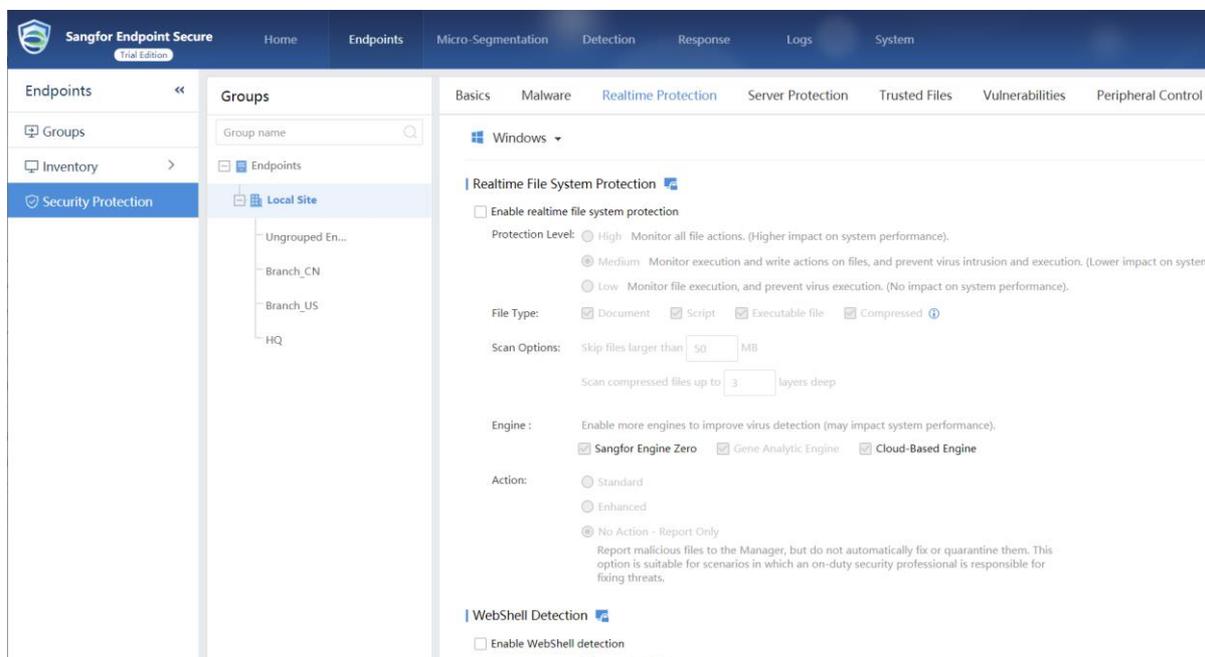
1.3 Precautions

1. Please ensure that Endpoint Secure synchronized all assets to Cyber Command.

How to Correlate with Endpoint Secure to Simply the Operation



2. Disable the Realtime File System Protection and other Protection, for we should avoid Endpoint Secure kill virus directly, after disabled Realtime Protection of Endpoint Secure, then the virus will not be killed automatically by Endpoint Secure and Endpoint Secure will synchronize the security log to Cyber Command. **The virus samples we use are only for internal testing of the correlation effect, and real-time detection needs to be turned on when the correlation effect is tested or when the implement is completed.**

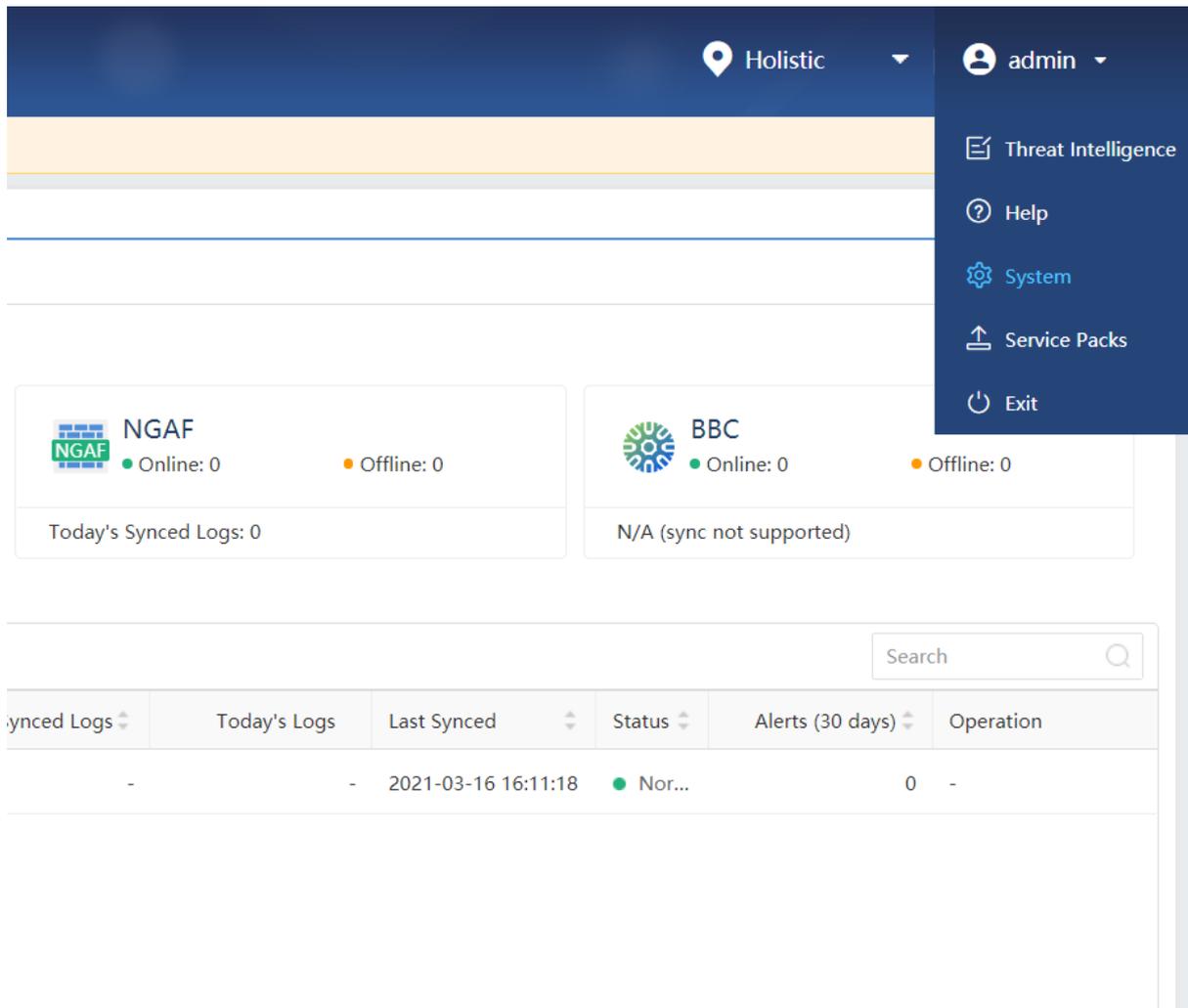


Chapter 2 Configuration

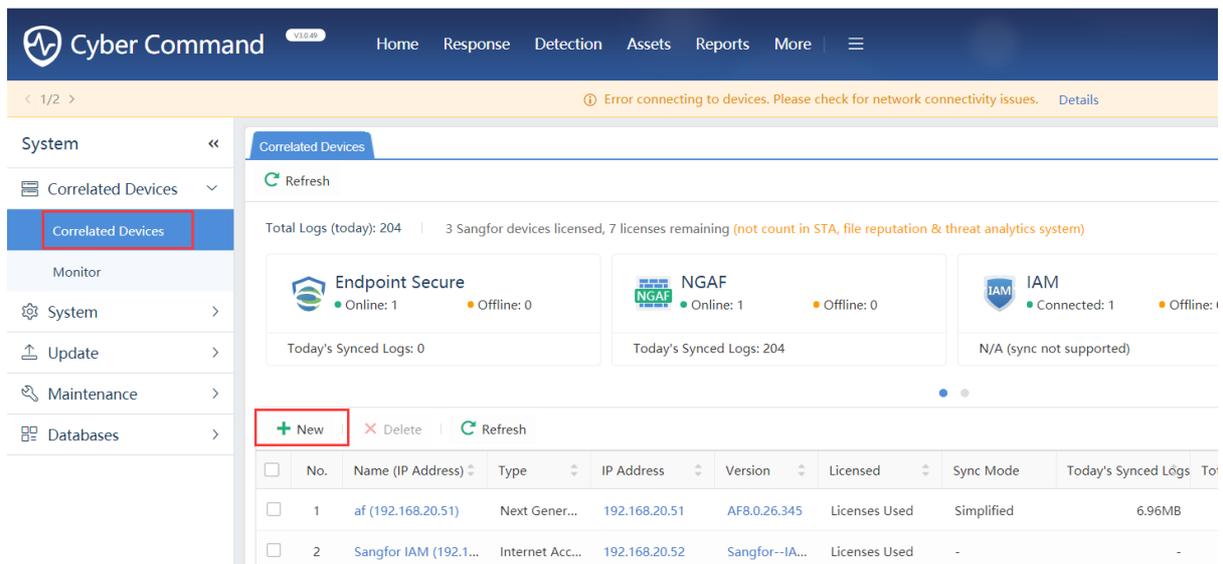
2.1 Configure Cyber Command

1. Go to System Path.

How to Correlate with Endpoint Secure to Simply the Operation

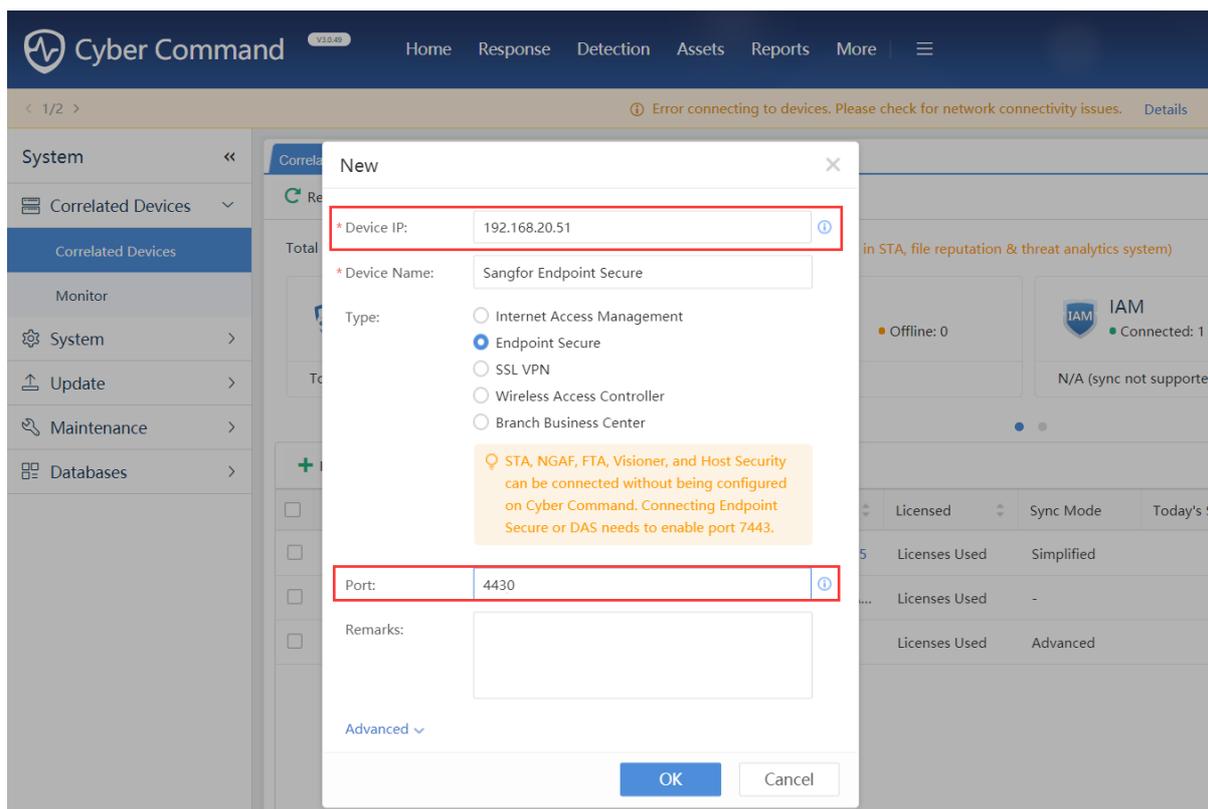


2. Go to Correlated Devices-> Correlated Devices path, and click New to create Correlation.

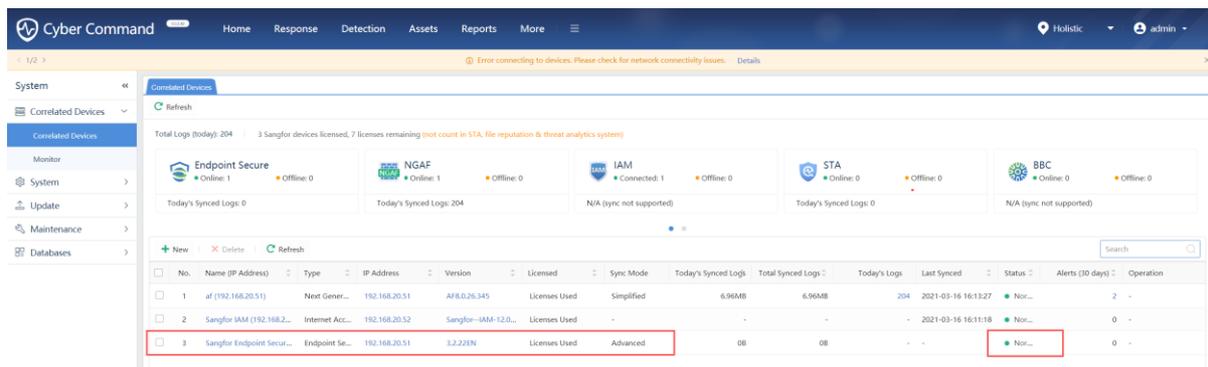


3. Input the IP of Endpoint Secure and the Port, if Endpoint Secure deployed after a NAT device, Please map the 443 port of Endpoint Secure to the NAT device. For example, here is the 4430 port mapped to the NAT device.

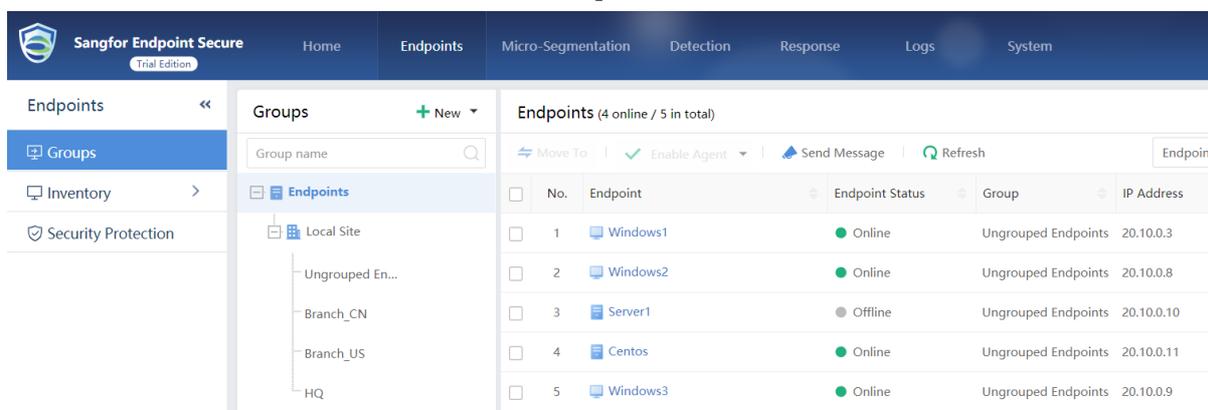
How to Correlate with Endpoint Secure to Simply the Operation



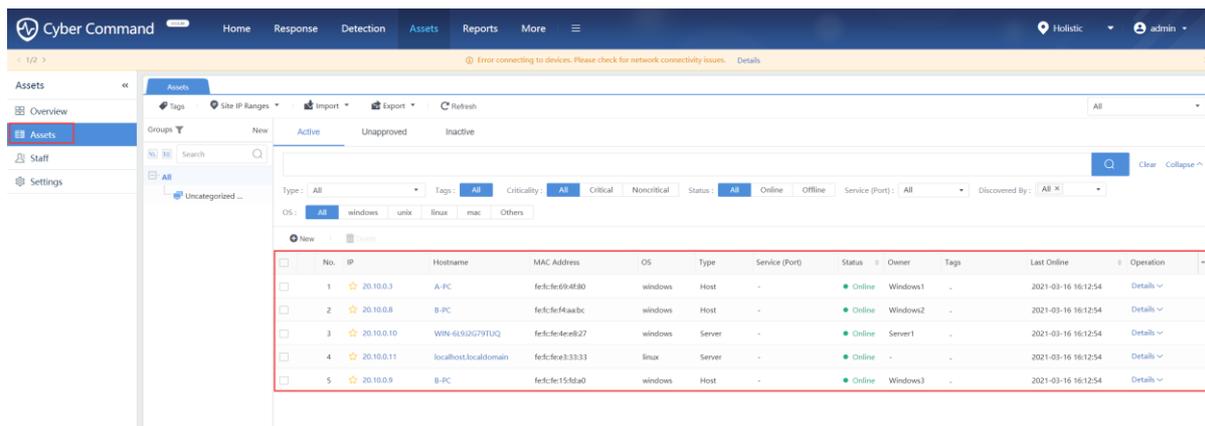
4. After click OK, you can see the correlation status in console.



5. You can check whether there exists assets in Endpoint Secure.



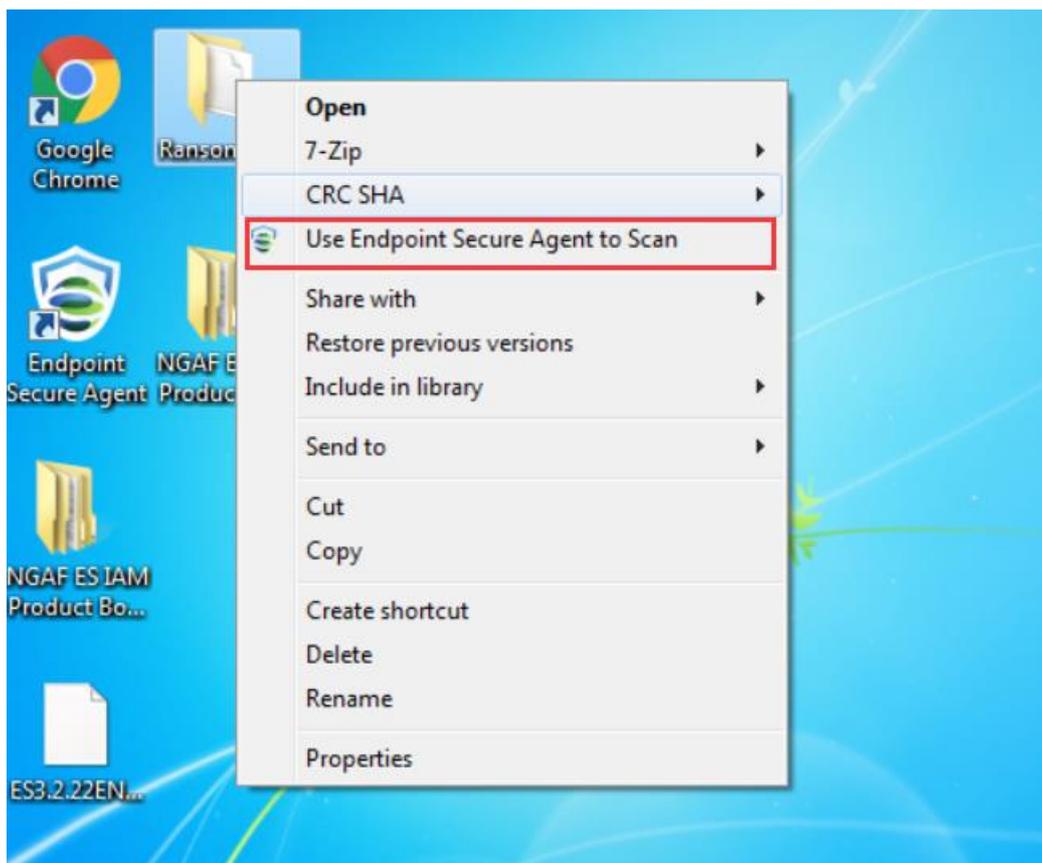
6. If you there exists in Endpoint Secure, go to Assets->Assets in Cyber Command to check whether assts has been synchronized to Cyber Command.



Chapter 3 Correlation

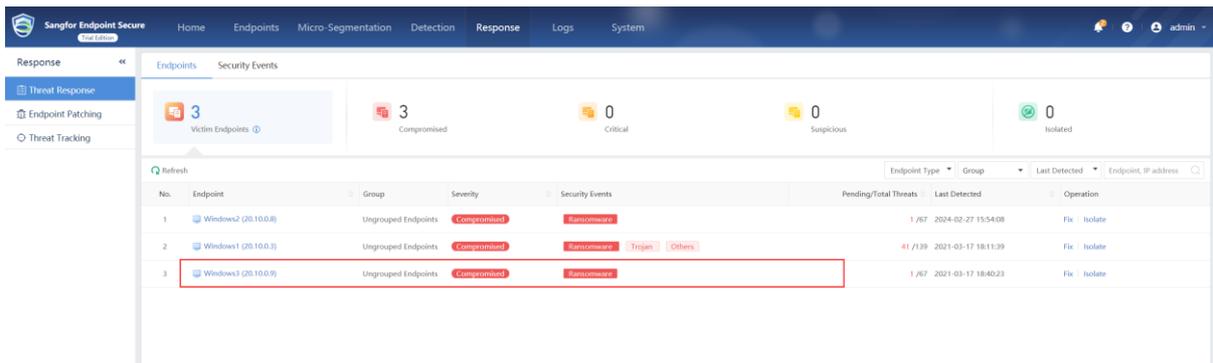
3.1 Generate Security Logs and Synchronize to Cyber Command

1. After the customer decompresses the file, use Endpoint Secure scan or scheduled scan.

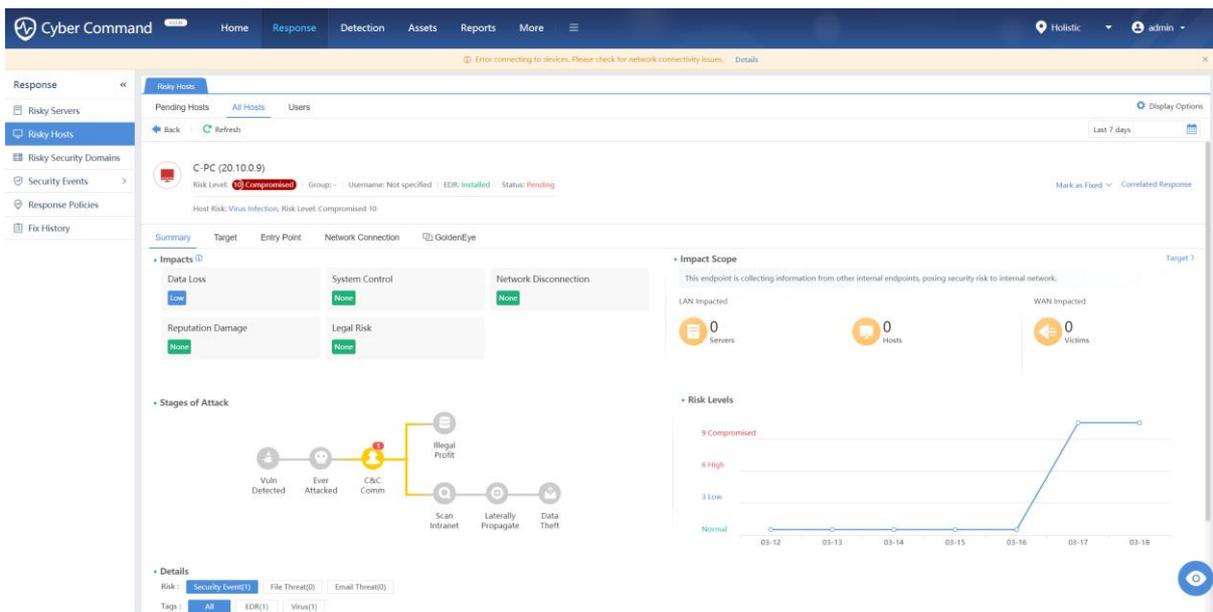


2. If a virus file is detected, you can see the related virus log on Endpoint Secure MGR.

How to Correlate with Endpoint Secure to Simply the Operation



3. Endpoint Secure will synchronize the virus log to Cyber Command, and you can see the detailed virus log on Cyber Command.



4. Click Correlated Response, and you can choose different action to deal with the victim host, such as you can choose block the victim host.

How to Correlate with Endpoint Secure to Simply the Operation

Correlated Response

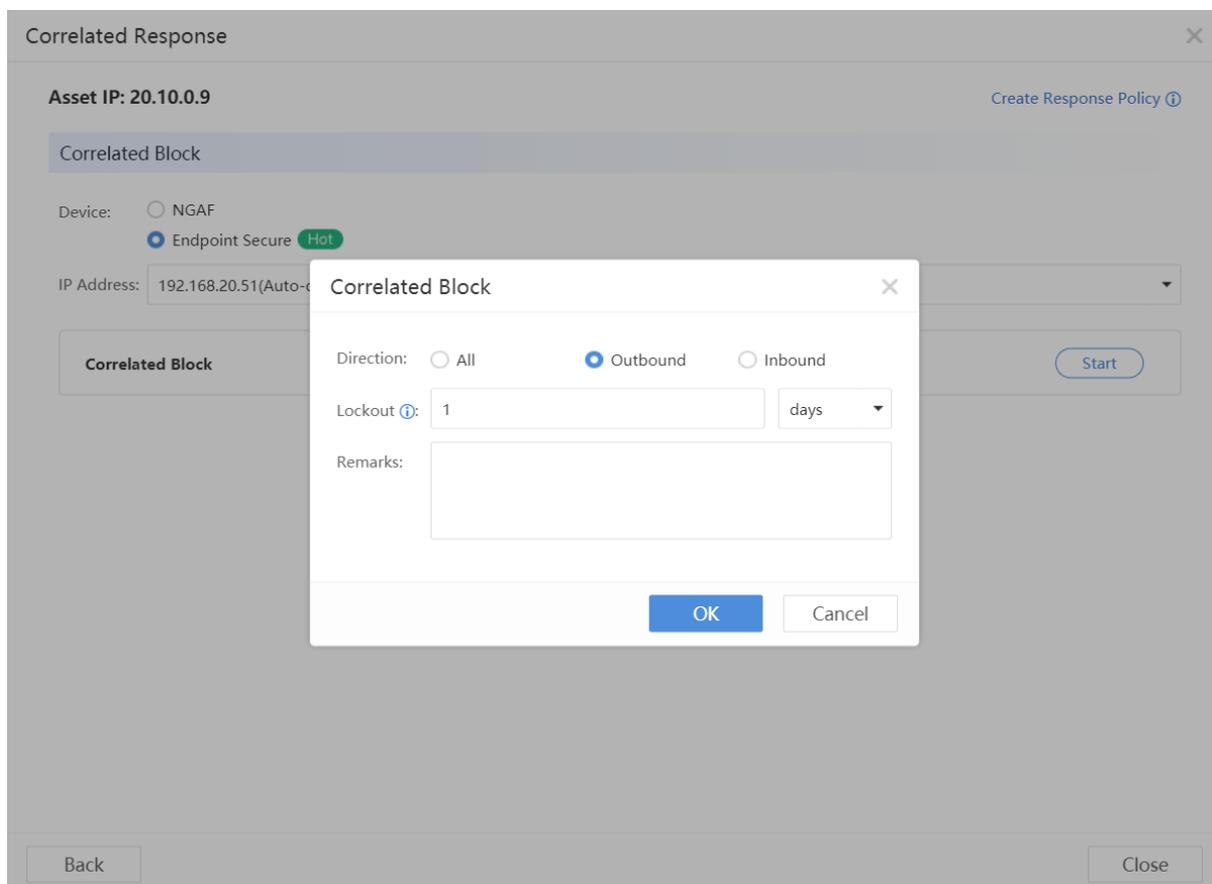
🔔 Virus event occurred. Suggestion: Enable access control to block connections with controller. Enable threat scan to clean up virus-infected files.

-  **Correlated Block**
Block all outbound accesses from a specific host or inbound accesses to that host.
-  **Access Control** Hot
Prevent a specific host from accessing specified IP address and port to block abnormal and attack behaviors.
-  **Browsing Risk Notification**
Notify users of risks and solutions when surfing the Internet with browser.
-  **Account Lockout**
Block infected hosts from accessing the Internet to reduce the risk of regulatory notification, and speed up response.
-  **Threat Scan** Hot
Start a full/quick scan on host and quarantine/trust detected malicious files.
-  **Forensics**
Perform forensic investigation against a malicious domain to locate which parent or child process accesses that domain.

Next

Close

5. Select Endpoint Secure as the correlated device and click Start.



Correlated Response

Asset IP: 20.10.0.9 Create Response Policy ⓘ

Correlated Block

Device: NGAF Endpoint Secure Hot

IP Address: 192.168.20.51(Auto-c)

Correlated Block

Direction: All Outbound Inbound

Lockout ⓘ: 1 days

Remarks:

OK Cancel

Start

Back Close

6. After click OK, just wait for a few seconds, then you can see the block policy issued successfully.

How to Correlate with Endpoint Secure to Simply the Operation

Correlated Response

Asset IP: 20.10.0.9 Create Response Policy ⓘ

Correlated Block

Device: NGAF Endpoint Secure Hot

IP Address: 192.168.20.51(Auto-discovered)

Correlated Block Locking (1 days 0 hours 00 mins) Edit Unlock

Direction: Outbound Lockout: 1 days

Remarks: Manually correlate is a correlate policy that be pushed do...

Manually correlate is a correlate policy that be pushed down in Response and other pages after log in the Cyber Command.

Again Close

7.You can go to Response->Threat Response->Isolated path, and then you can see the host that has been isolated by policy that issued by Cyber Command.

The screenshot shows the Sangfor Endpoint Secure interface. The 'Response' section is active, displaying a summary of endpoint statuses: 3 Victim Endpoints, 3 Compromised, 0 Critical, and 0 Suspicious. The 'Isolated' status is highlighted with a red box, showing a count of 1. Below this, a table lists the isolated endpoint:

No.	Endpoint	Group	Action	Blocked IP	Block Port	Period (Days)	Time Fixed	Administrator	Status	Operation
1	Windows3 (20.10.0.9)	Ungrouped Endpoints	No Outbound	All	All	1day(s)	2021-03-18 09:27:08	Cyber Command Correlatio...	Quarantined	Restore



SANGFOR

Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc