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

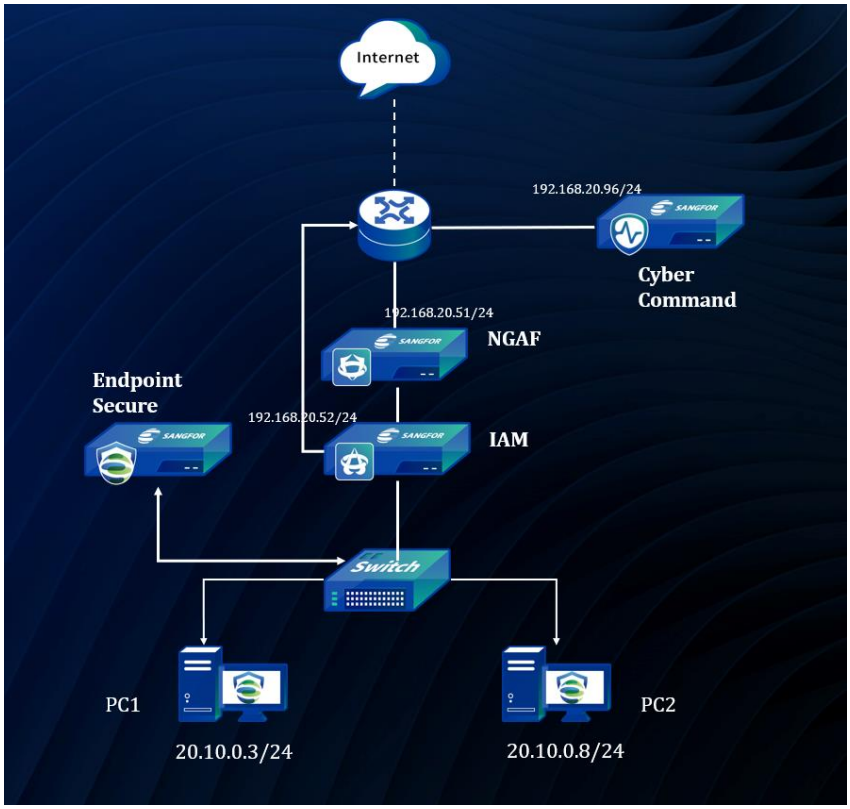
Chapter 1 Scenario

1.1 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.

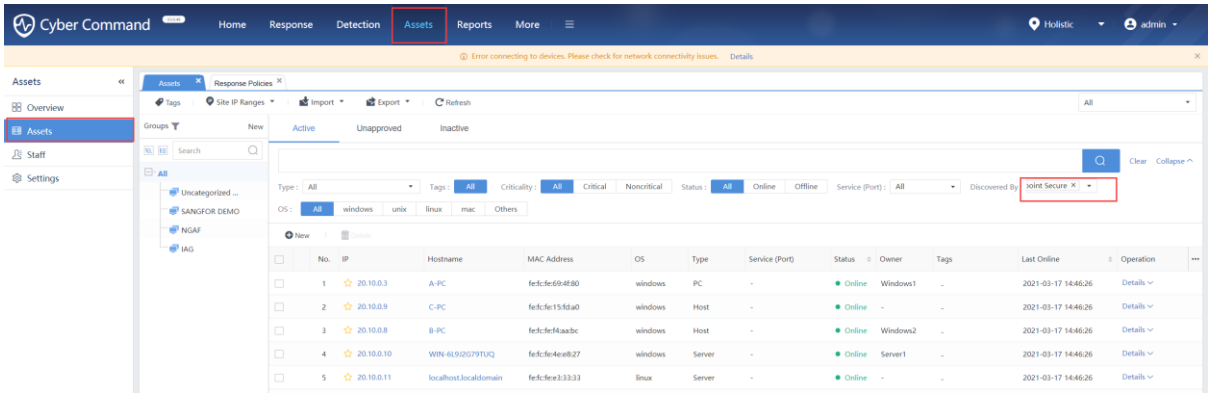
1.2 Environment

1.2.1 Network Environment

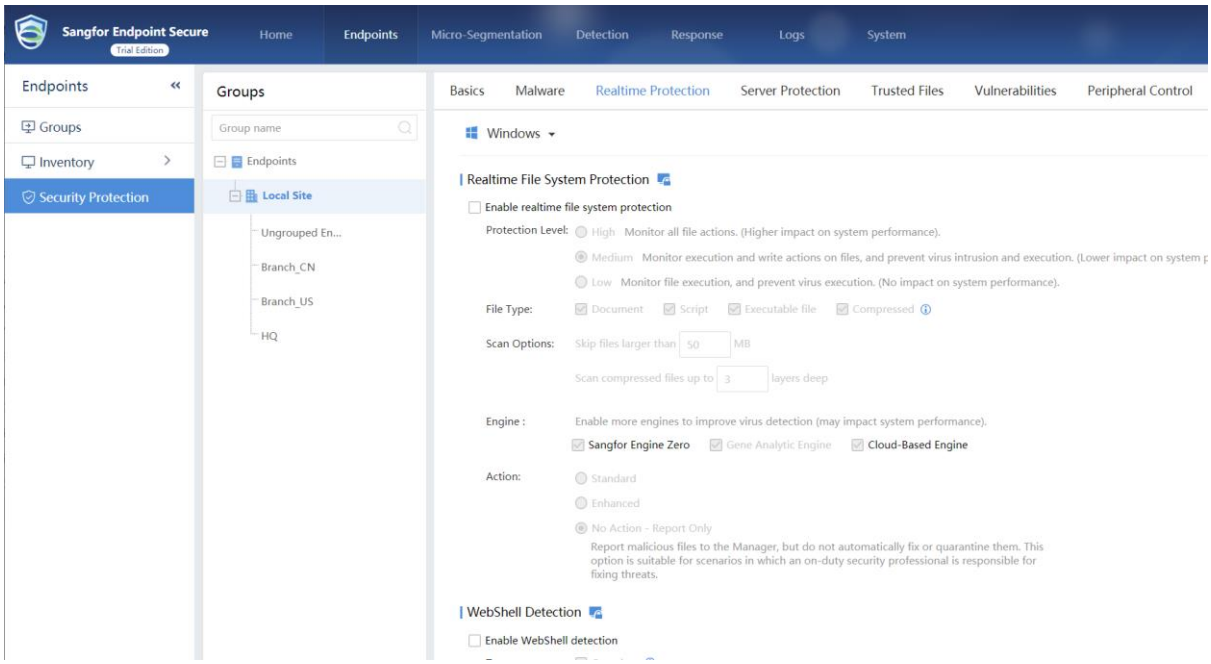


1.3 Precautions

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



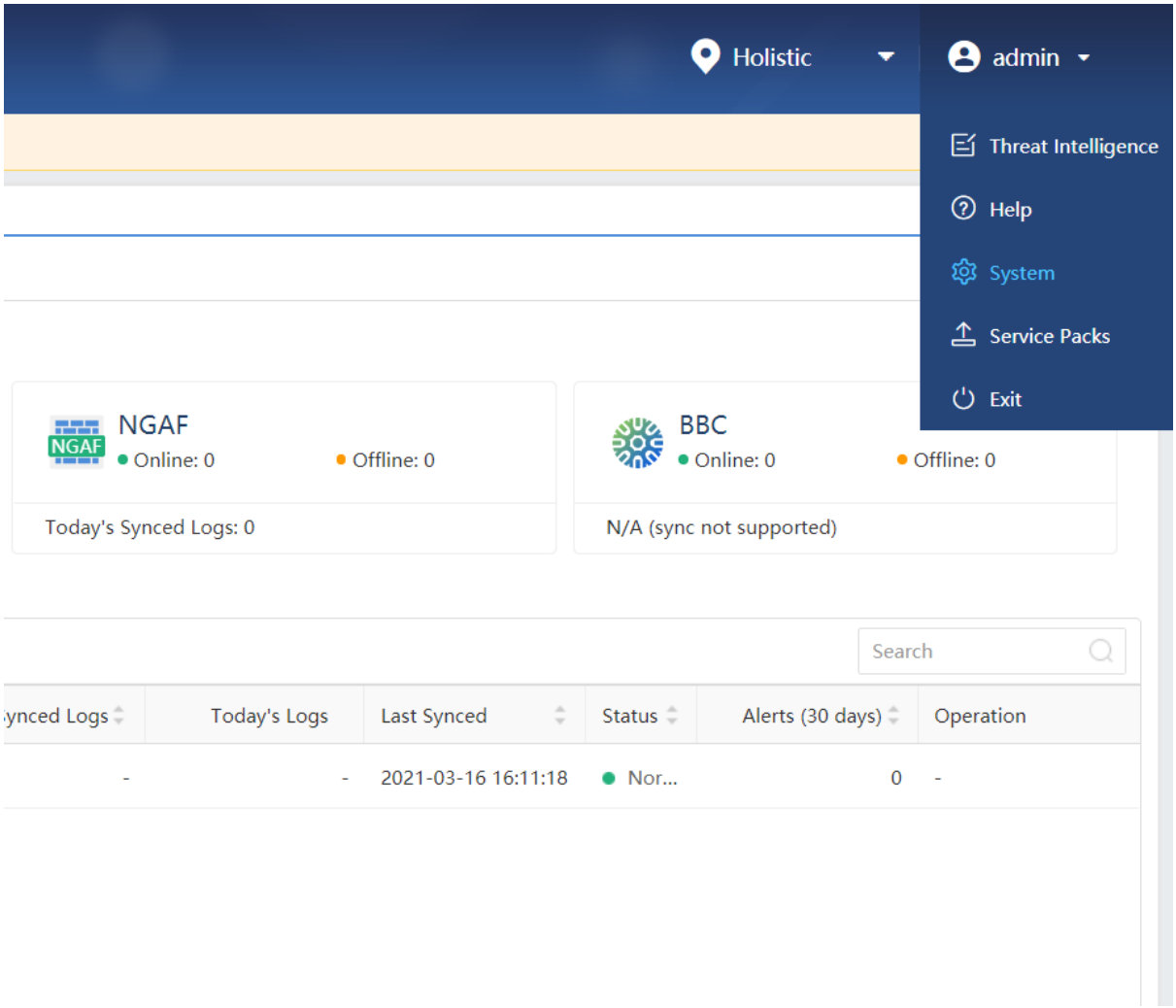
2. Disable the Realtime File System Protection and other Protection, for we should avoid Endpoint Secure kill virus directly, after disabled Realtime Protection of Endpoint Secure, then the virus will not be killed automatically by Endpoint Secure and Endpoint Secure will synchronize the security log 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.**



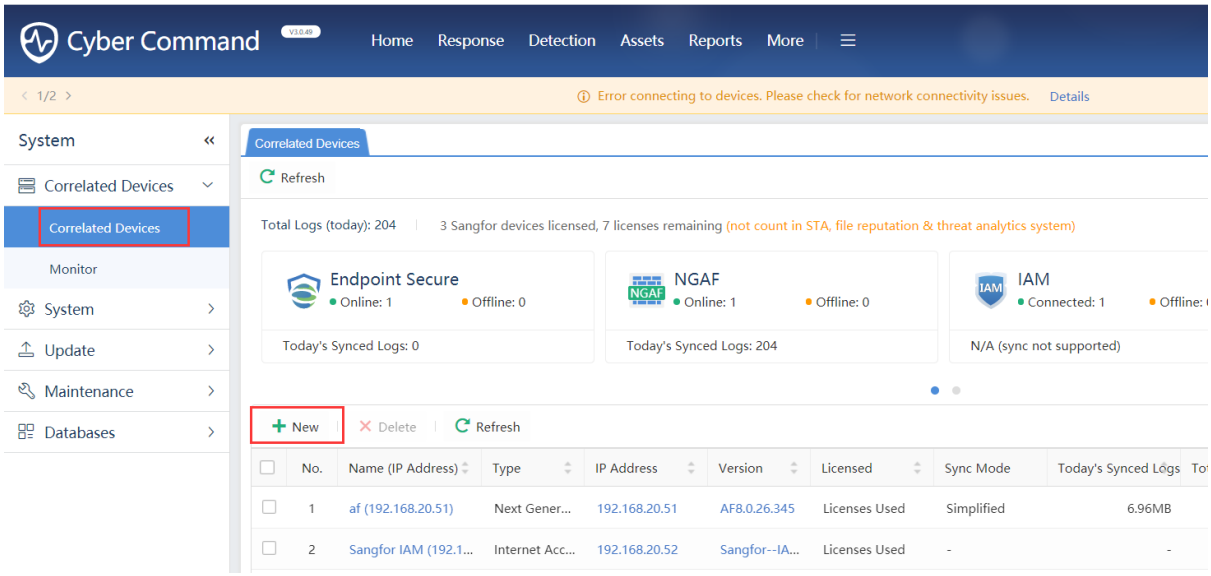
Chapter 2 Configuration

2.1 Configure Cyber Command

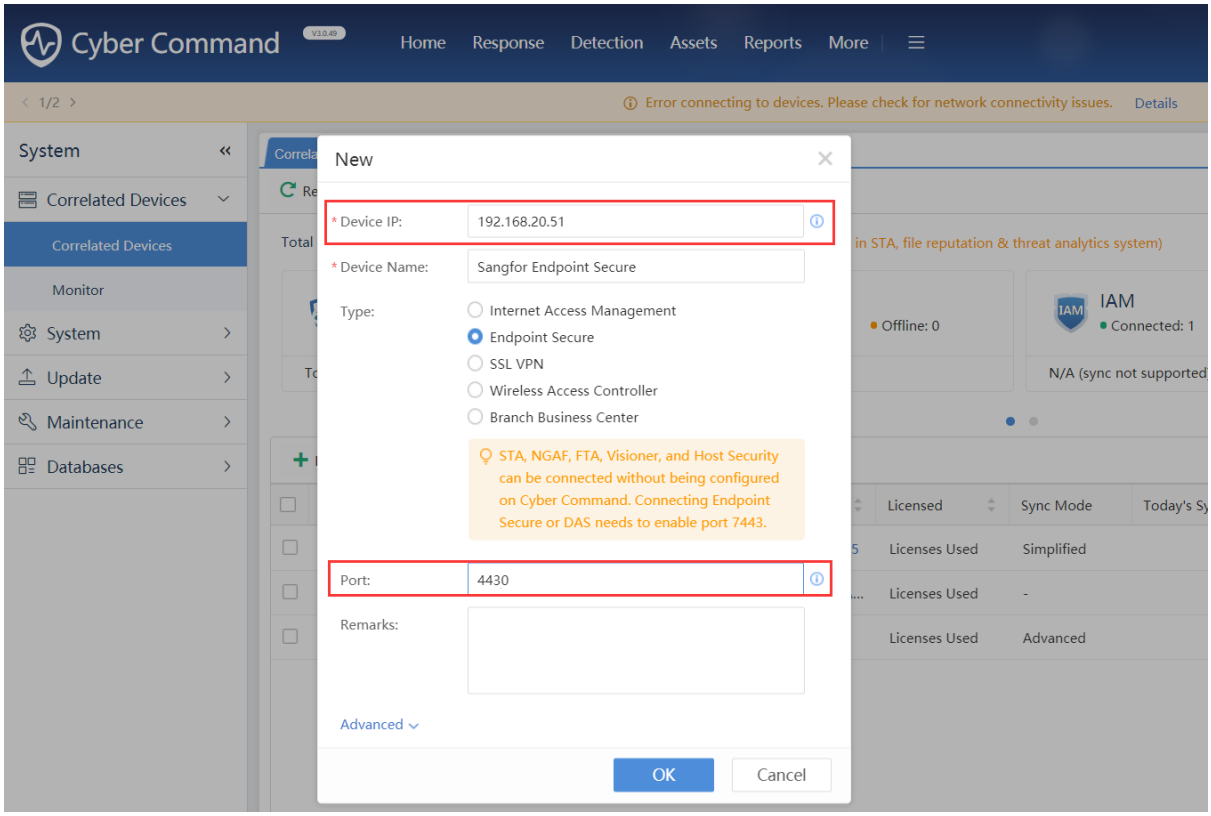
1. Go to System Path.



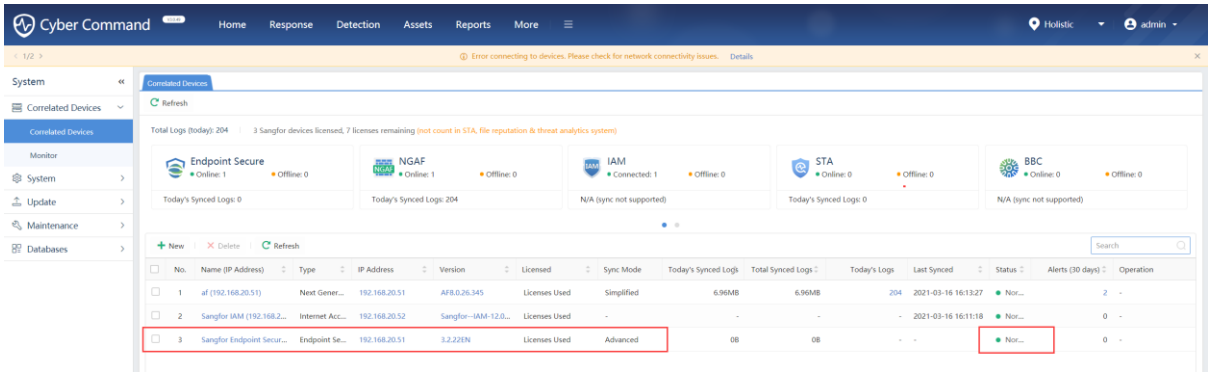
2. Go to Correlated Devices-> Correlated Devices path, and click New to create Correlation.



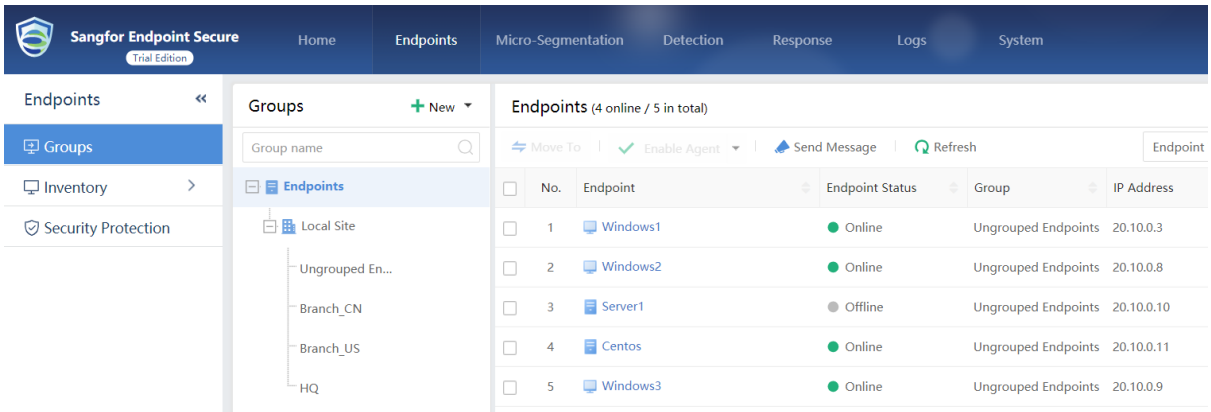
3. Input the IP of Endpoint Secure and the Port, if Endpoint Secure deployed after a NAT device, Please map the 443 port of Endpoint Secure to the NAT device. For example, here is the 4430 port mapped to the NAT device.



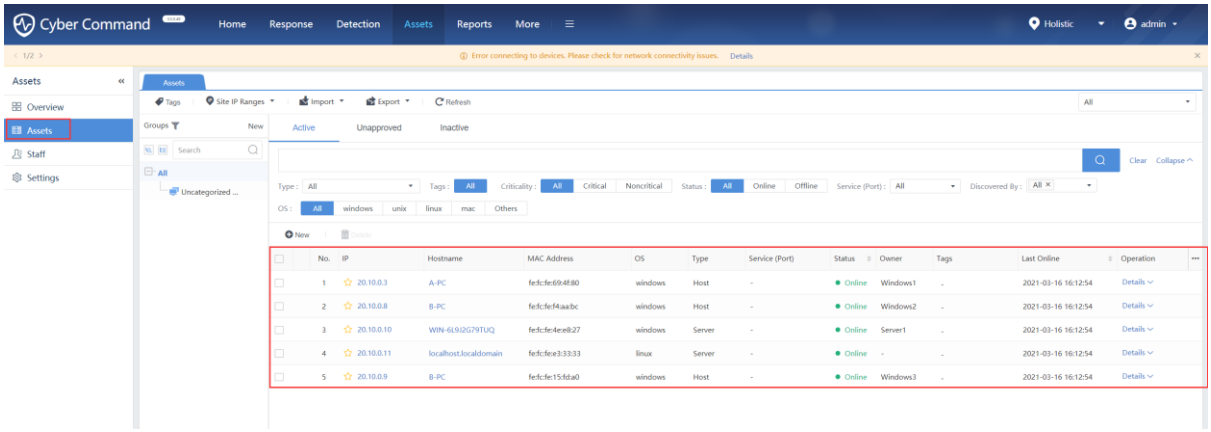
4. After click OK, you can see the correlation status in console.



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



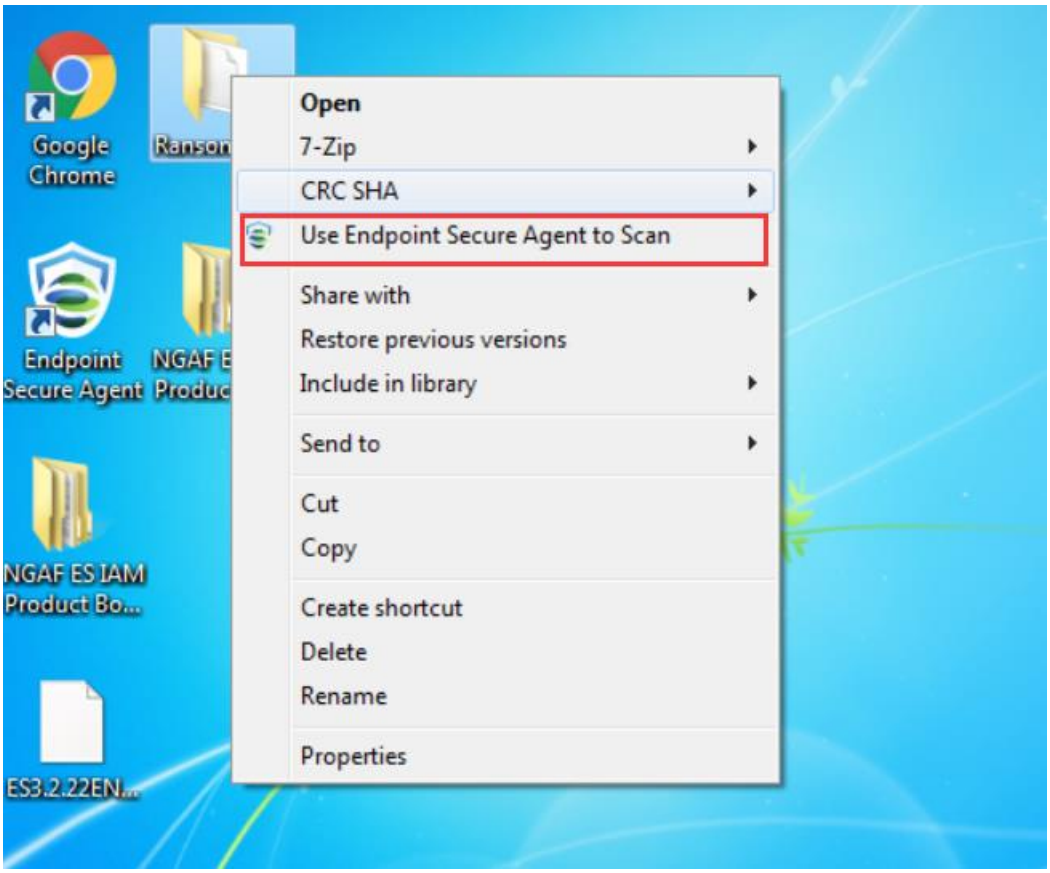
6. If you there exists in Endpoint Secure, go to Assets->Assets in Cyber Command to check whether assts has been synchronized to Cyber Command.



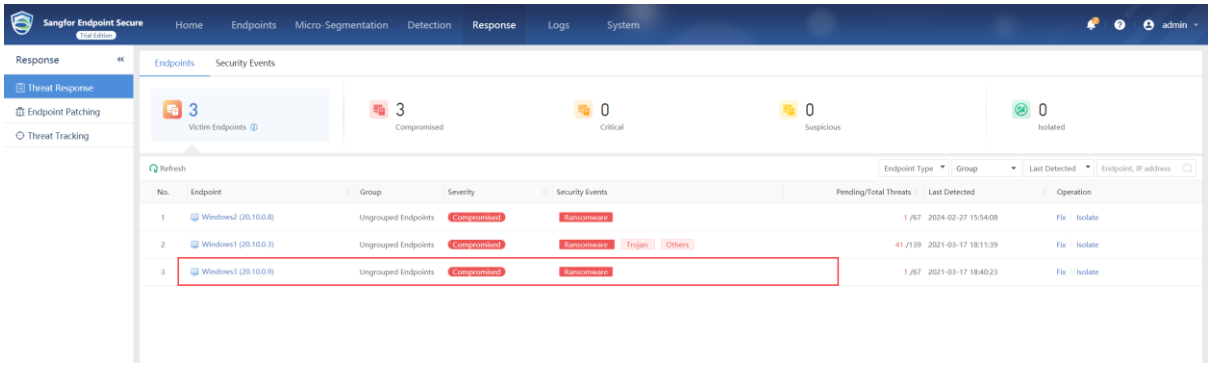
Chapter 3 Correlation

3.1 Generate Security Logs and Synchronize to Cyber Command

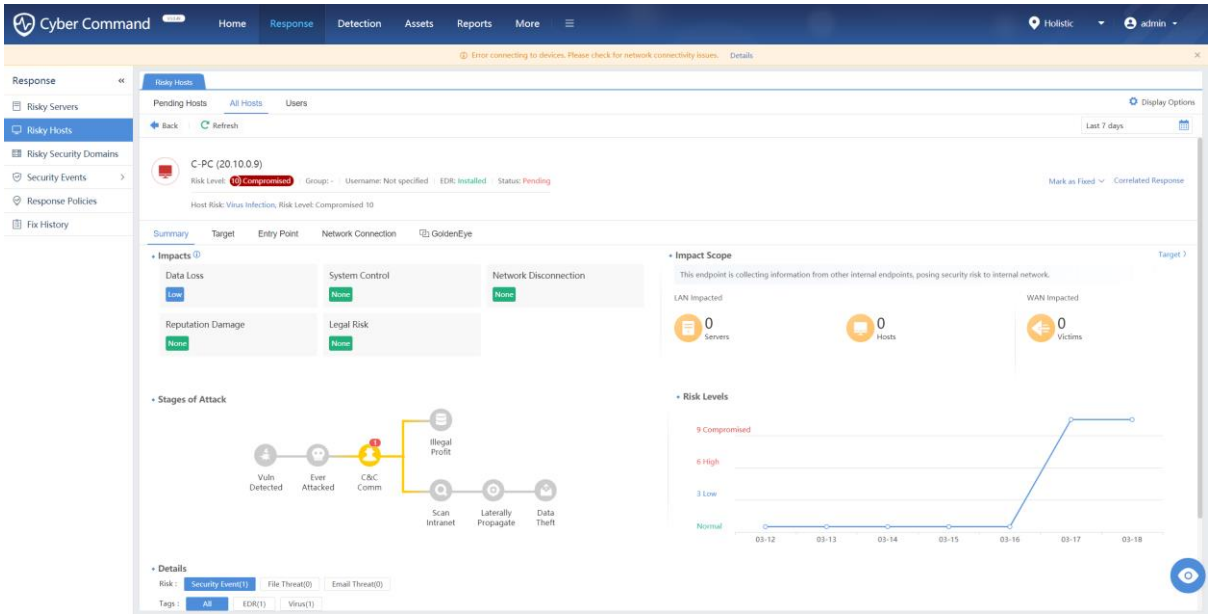
1. After the customer decompresses the file, use Endpoint Secure scan or scheduled scan.



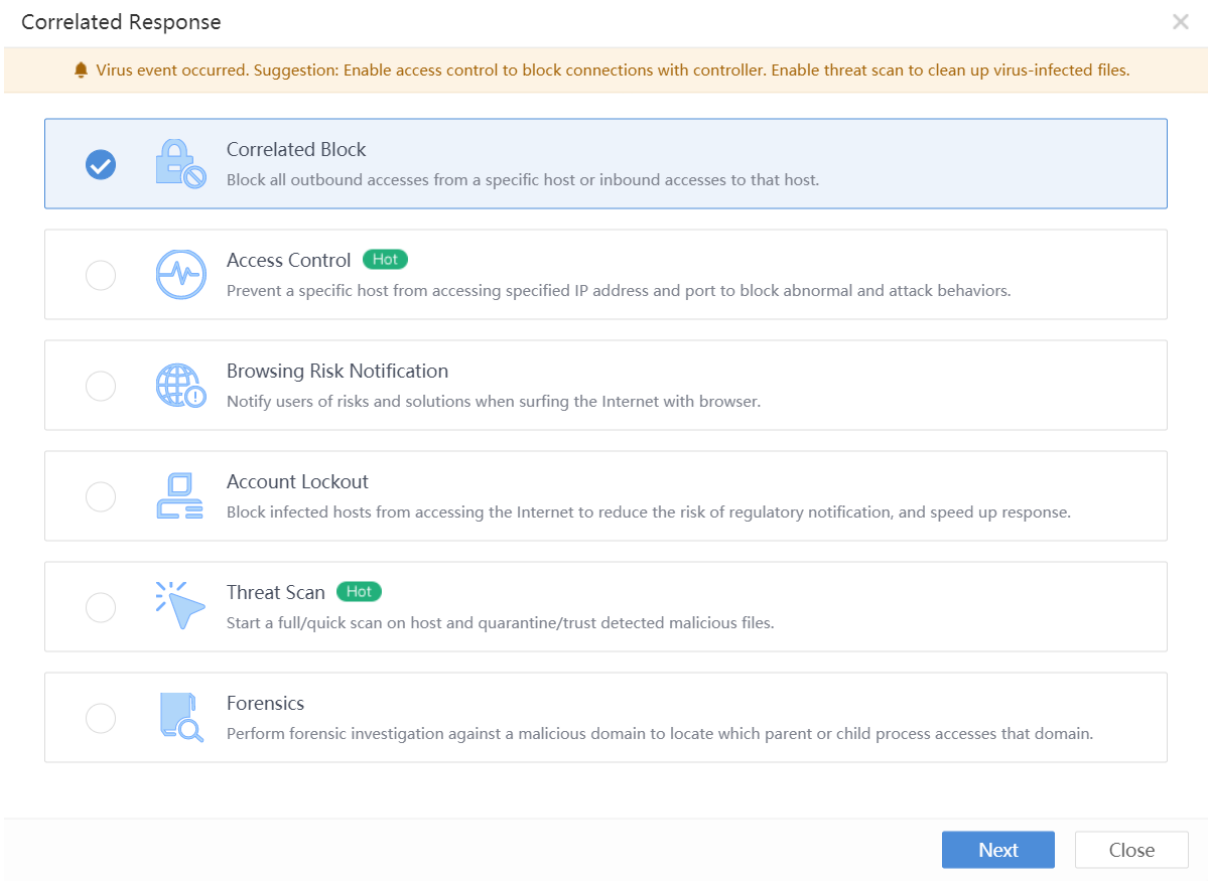
2. If a virus file is detected, you can see the related virus log on Endpoint Secure MGR.



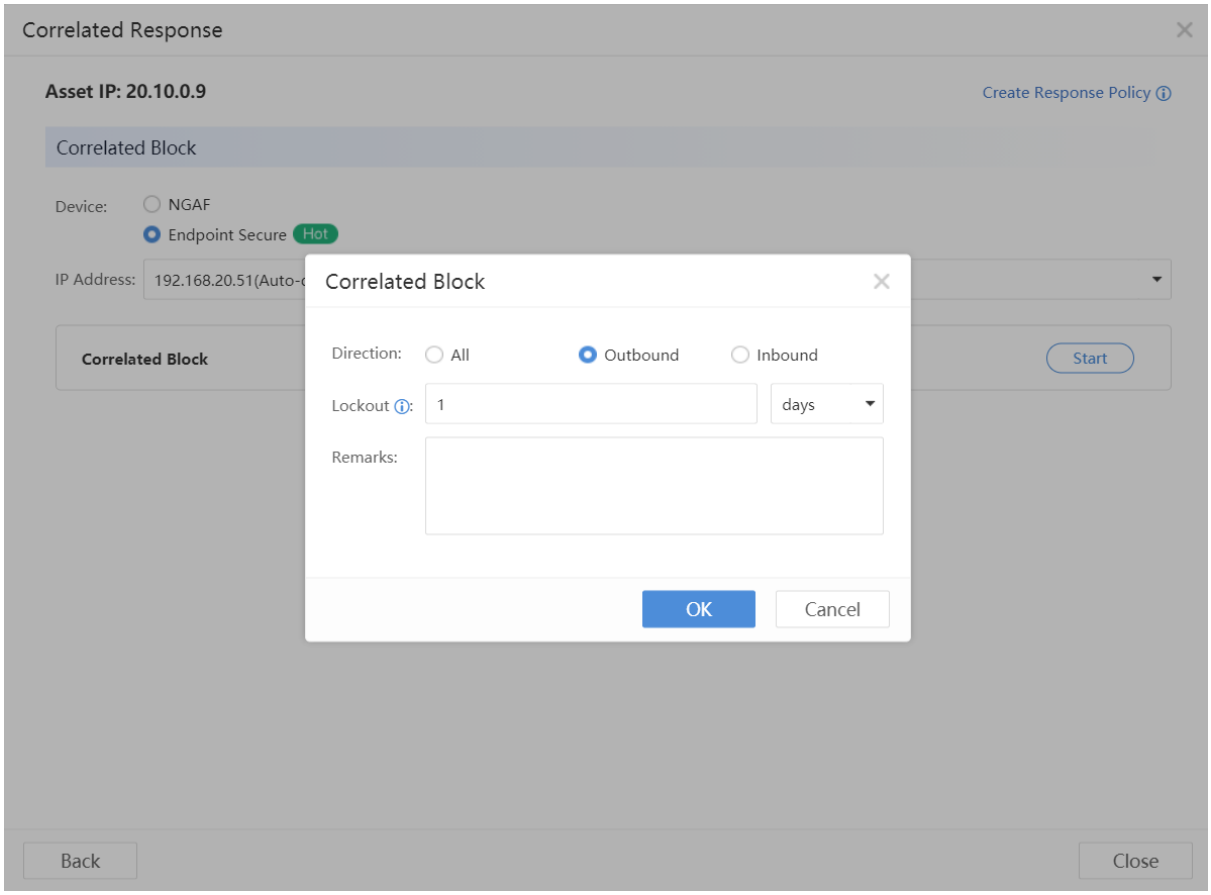
3. Endpoint Secure will synchronize the virus log to Cyber Command, and you can see the detailed virus log on Cyber Command.



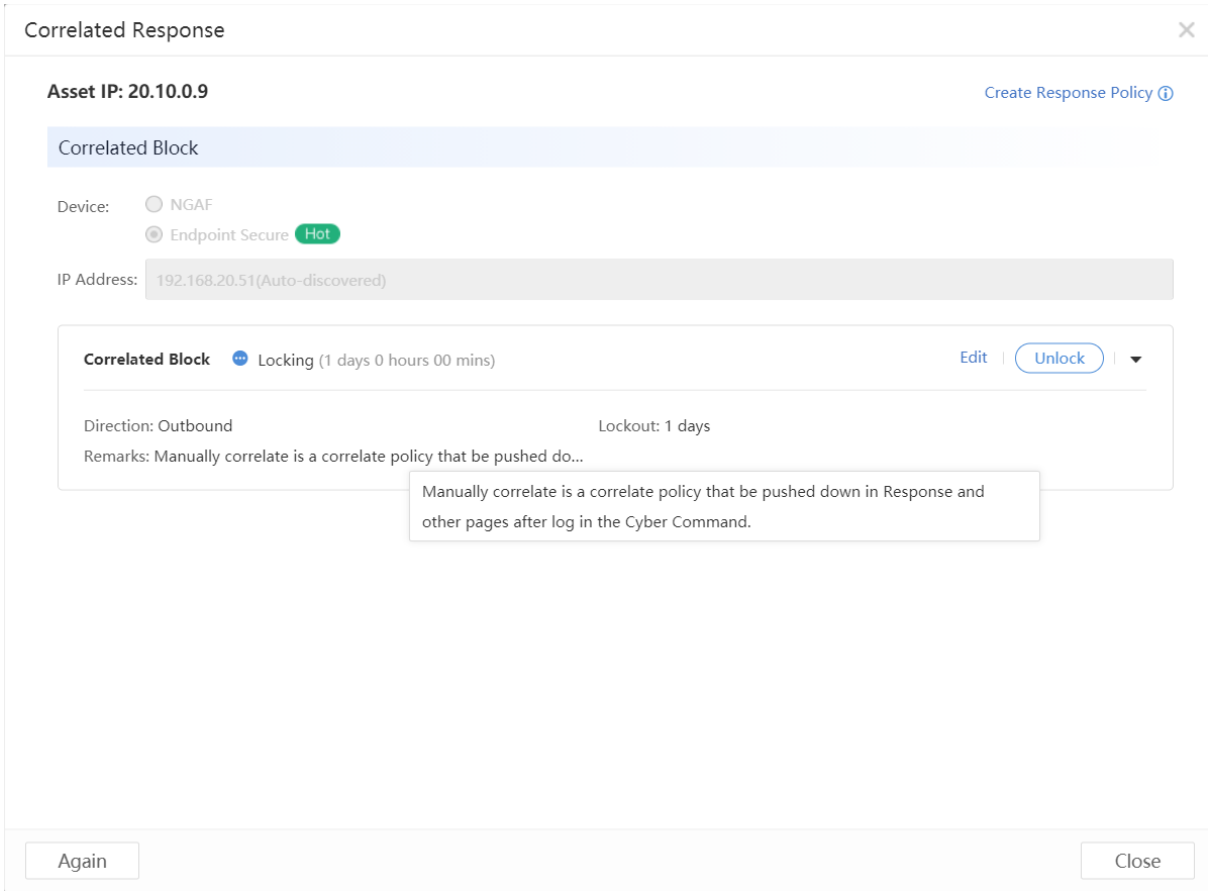
4. Click Correlated Response, and you can choose different action to deal with the victim host, such as you can choose block the victim host.



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



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



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.