Cyber Command

Best Practices for Configuration_How to Correlate with NGAF to Simply the Operation

Version 3.0.49

Change Log

Date	Change Description
May 7, 2021	Document release.
May 17, 2021	Document update.

CONTENT

Chapter 1 Basic

Related documents:

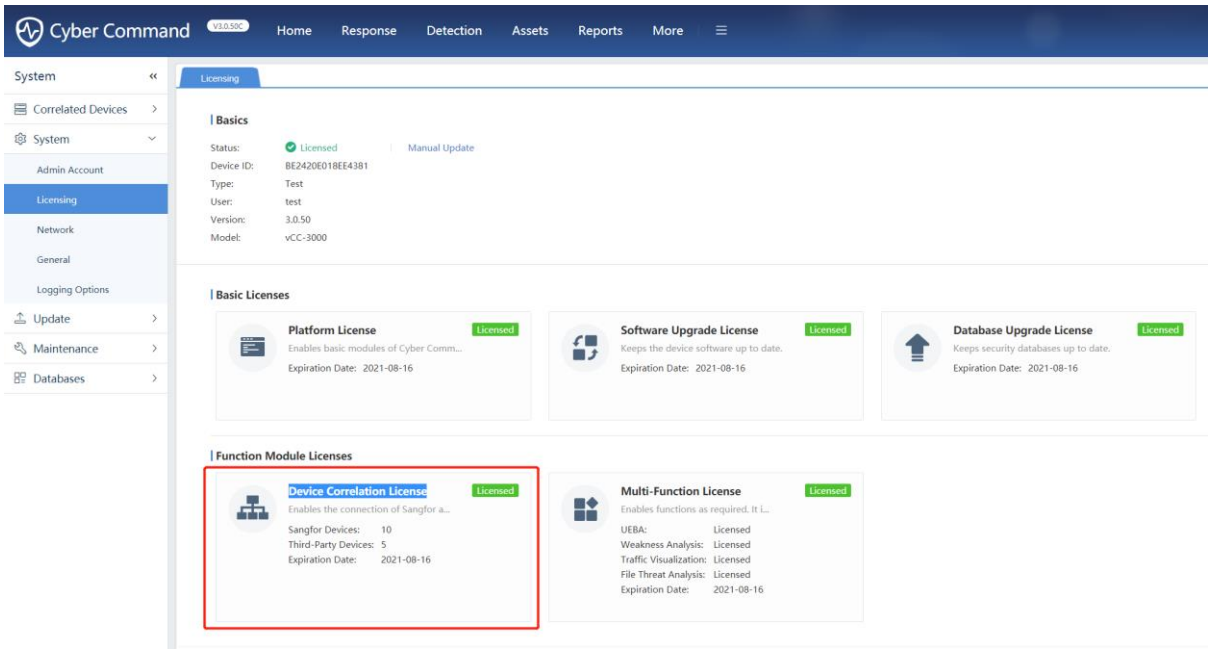
Best Practices for Configuration usually include selection of deployment mode, configuration ideas, information collection, function limitations, version differences. Regarding ***How to Correlate with NGAF to Simply the Operation***, if you want to learn about general POC scenarios and detailed configuration steps, please refer to the following link:

https://community.sangfor.com/plugin.php?id=sangfor_databases:index&mod=viewdatabase&tid=4591

1.1 Confirm Basic Configuration and Deployment

1. Starting from NGAF 8.0.2 version, Support synchronizing monitored event information to SIP platform to monitor devices in real time and minimize event impact on business.

2. Confirm whether CCOM has enabled Device Correlation License.



3. Confirm the network topology, such as whether CC and NGAF can communicate, whether the route is reachable, and whether there is a NAT device in the middle.

4. When NGAF is correlated with CC, correlation can be configured only on NGAF. If higher security is required, mutual authentication can be configured on NGAF and CC.

5. NGAF accesses TCP port 4430 of CC, CC accesses TCP 7443 port of NGAF. The correlation between NGAF and CC does not support NAT scenarios temporarily, and the devices on both sides will check the IP. If the ip is inconsistent, the normal linkage cannot be performed.

1.2 Correlation Function

1. NGAF does not upload all security logs to CC, NGAF can upload botnets and webshell backdoors, Security log generated by the black chain to CC, which can correlate with NGAF for threat blocking and application control.

2. CC linkage NGAF can issue Correlated Block to block IP, and can issue Access Control to block IP traffic.

3. In order to better detect cyber threats, it is very important to ensure that the security rule bases of NGAF and CC are kept up to date. This means you'd better allow NGAF and CC devices to connect to the Internet.

4. If you want to be able to automatically cooperate with NGAF to deal with the threat after CC detected it, please don't forget to configure the automatic response policy on CC.

5. When you configure NGAF and CC correlation policy, it is best to ensure that the relevant security policy on NGAF has been turned on. If the security policy on NGAF is not turned on, many network threats will not be detected.