Cyber Command

Praktik Terbaik untuk Konfigurasi_Bagaimana untuk Berkorelasi dengan NGAF untuk Operasi Sederhana

Versi 3.0.49

Catatan Perubahan

Tanggal	Deskripsi Perubahan
Mei 7, 2021	Rilis Dokumen.
Mei 17, 2021	Dokumen update.

Daftar Isi

Bab 1 Dasar

Dokumen terkait:

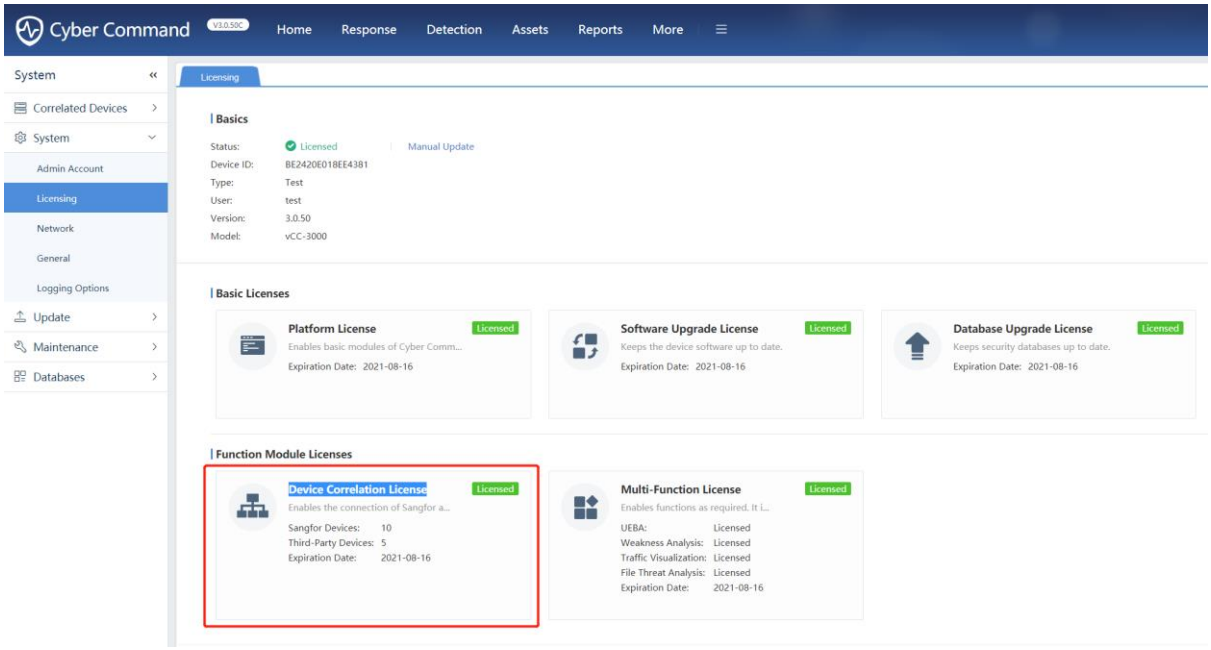
Praktik Terbaik untuk Konfigurasi termasuk pilihan mode deployment, ide konfigurasi, koleksi informasi, keterbatasan fungsi, perbedaan versi. Mengenai ***How to Correlate with NGAF to Simply the Operation***, jika Anda ingin mempelajari tentang skenario POC umumnya dan langkah konfigurasi terperinci, silakan merujuk ke link berikut:

https://sangforltd.sharepoint.com/:w:/s/PMO/EcWMQD_rmRFLul9AnDD7fzUB2Y-jjfvt4yqr94ED_ROq3g?e=Iae2BX

1.1 Konfirmasi Dasar Konfigurasi dan Deployment

1. Mulai dari versi NGAF 8.0.2, Mendukung sinkronisasi monitor informasi event untuk SIP platform untuk monitor perangkat dalam real time dan meminimalkan dampak event pada bisnis .

2. Konfirmasi apakah Device Correlation License pada CCOM telah diaktifkan.



3. Konfirmasi topologi network, seperti apakah CC dan NGAF dapat berkomunikasi, apakah route dapat dijangkau, dan apakah ada perangkat NAT di tengah.

4. Ketika NGAF berkorelasi dengan CC, korelasi dapat dikonfigurasi hanya pada NGAF. Jika tingkat keamanan yang lebih tinggi diperlukan, mutual authentication dapat dikonfigurasi pada NGAF dan CC.

5. NGAF mengakses TCP port 4430 dari CC, CC mengakses TCP port 7443 dari NGAF. Korelasi antara NGAF dan CC tidak mendukung skenario NAT untuk sementara, dan perangkat di kedua side akan periksa IP. Jika IP tidak konsisten, normal linkage tidak dapat dilakukan.

1.2 Fungsi Korelasi

1. NGAF tidak upload semua security log ke CC, NGAF dapat upload botnet dan webshell backdoors, Security log yang dihasilkan oleh black chain ke CC, yang dapat berkorelasi dengan NGAF untuk pemblokiran ancaman dan aplikasi kontrol.

2. CC linkage NGAF dapat mengeluarkan korelasi blok ke blok IP, dan dapat mengeluarkan Akses Kontrol untuk memblokir IP traffic.

3. Untuk mendeteksi ancaman cyber dengan lebih baik, hal ini sangat penting untuk memastikan bahwa aturan security basis NGAF dan CC terus up to date. Ini berarti Anda sebaiknya mengizinkan perangkat NGAF dan CC untuk terkoneksi ke Internet.

4. Jika Anda ingin dapat secara otomatis bekerja sama dengan NGAF untuk menangani ancaman setelah CC terdeteksi, jangan lupa untuk konfigurasi otomatis respon policy di CC.

5. Ketika Anda konfigurasi korelasi policy NGAF dan CC, hal terbaik untuk memastikan bahwa security policy yang relevan di NGAF telah diaktifkan. Jika security policy pada NGAF tidak diaktifkan, banyak ancaman network tidak akan terdeteksi.