SANGFOR

Cyber Command

Praktek Terbaik untuk_Bagaimana Cara Berkolerasi dengan NGAF dalam Operasi Sederhana

Versi 3.0.49

Catatan Perubahan

Tanggal	Catatan Perubahan
7 Mei 2021	Penerbitan Dokumen
17 Mei 2021	Pembaruan Dokumen

Daftar Isi

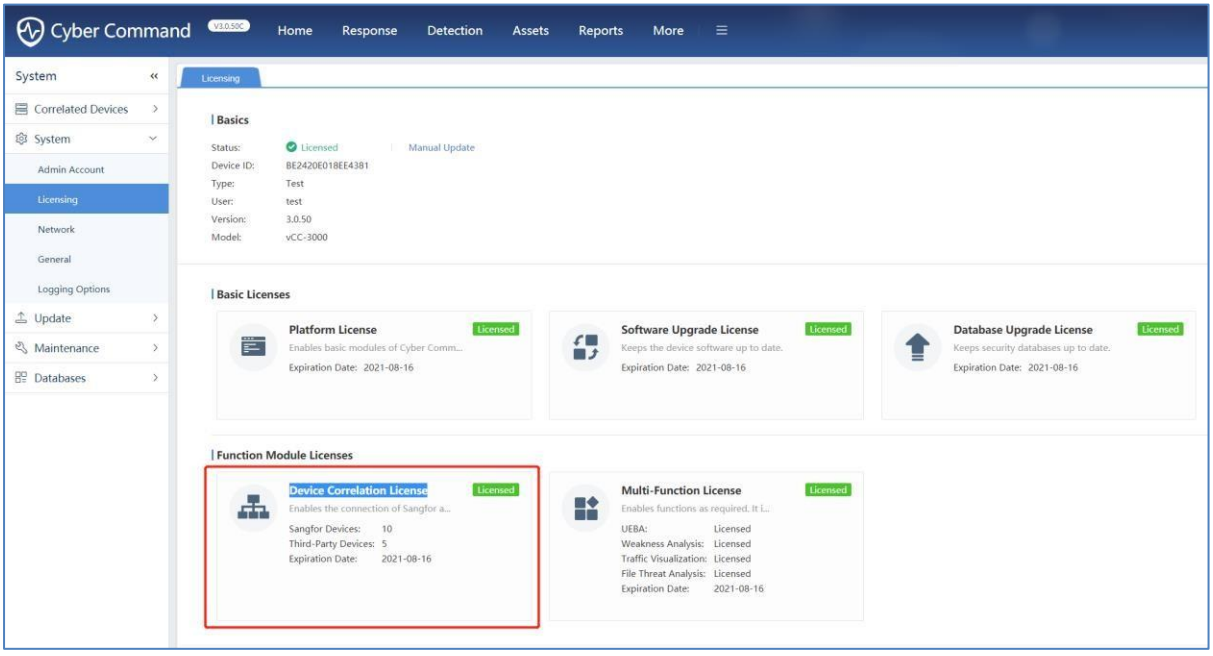
BAB 1 Dasar

Dokumen terkait:

Praktik Terbaik untuk Konfigurasi biasanya mencakup pemilihan mode deployment, ide konfigurasi, pengumpulan informasi, batasan fungsi, perbedaan versi. Mengenai Bagaimana Cara Berkolerasi dengan NGAF dalam Operasi Sederhana, jika Anda ingin belajar tentang skenario POC umum dan langkah-langkah konfigurasi terperinci, silakan lihat tautan berikut: https://community.sangfor.com/plugin.php?id=sangfor_databases:index&mod=viewdatabase&tid=4591

1.1 Konfirmasi Konfigurasi dasar dan Deployment

1. Mulai dari versi NGAF 8.0.2, Dukungan sinkronisasi pemantauan informasi event hingga platform SIP untuk memantau perangkat secara real time dan meminimalkan dampak event pada bisnis.



2. Konfirmasi apakah CCOM telah mengaktifkan Device Correlation License.
3. Konfirmasi topologi jaringan, seperti apakah CC dan NGAF dapat berkomunikasi, apakah rute dapat dijangkau, dan apakah ada perangkat NAT di tengah.
4. Ketika NGAF berkorelasi dengan CC, korelasi hanya dapat dikonfigurasi pada NGAF. Jika diperlukan keamanan yang lebih tinggi, autentikasi timbal balik dapat dikonfigurasi pada NGAF dan CC.

1.2 Fungsi Korelasi

1. NGAF tidak mengunggah semua log keamanan ke CC, NGAF dapat mengunggah botnet dan backdoor webshell, Log keamanan yang dihasilkan oleh blackchain ke CC, yang dapat berkorelasi dengan NGAF untuk pemblokiran ancaman dan kontrol aplikasi.
2. CC linkage NGAF dapat mengeluarkan Correlated Block untuk memblokir IP, dan dapat mengeluarkan Access Control untuk memblokir lalu lintas IP.
3. Untuk mendeteksi ancaman cyber dengan lebih baik, sangat penting untuk memastikan bahwa basis aturan keamanan NGAF dan CC terus diperbarui. Ini berarti Anda sebaiknya mengizinkan perangkat NGAF dan CC untuk terhubung ke Internet.

Jika Anda ingin dapat secara otomatis bekerja sama dengan NGAF untuk menangani ancaman setelah CC mendeteksinya, jangan lupa untuk mengonfigurasi kebijakan respons otomatis pada CC.

Ketika Anda mengkonfigurasi kebijakan korelasi NGAF dan CC, yang terbaik adalah memastikan bahwa kebijakan keamanan yang relevan tentang NGAF telah diaktifkan. Jika kebijakan keamanan pada NGAF tidak diaktifkan, banyak ancaman jaringan tidak akan terdeteksi.

SANGFOR