SANGFOR

Cyber Command

Implementasi yang Direkomendasikan untuk Skenario_Bagaimana untuk Berkorelasi dengan Endpoint Secure dengan Operasi Sederhana

Versi 3.0.49

Catatan Perubahan

Tanggal	Deskripsi Perubahan
Maret 3, 2021	Rilis Dokumen.
Mei 17, 2021	Dokumen update.

Daftar Isi

Bagaimana untuk Berkorelasi dengan Endpoint Secure dengan Operasi Sederhana

Bab 1 Skenario

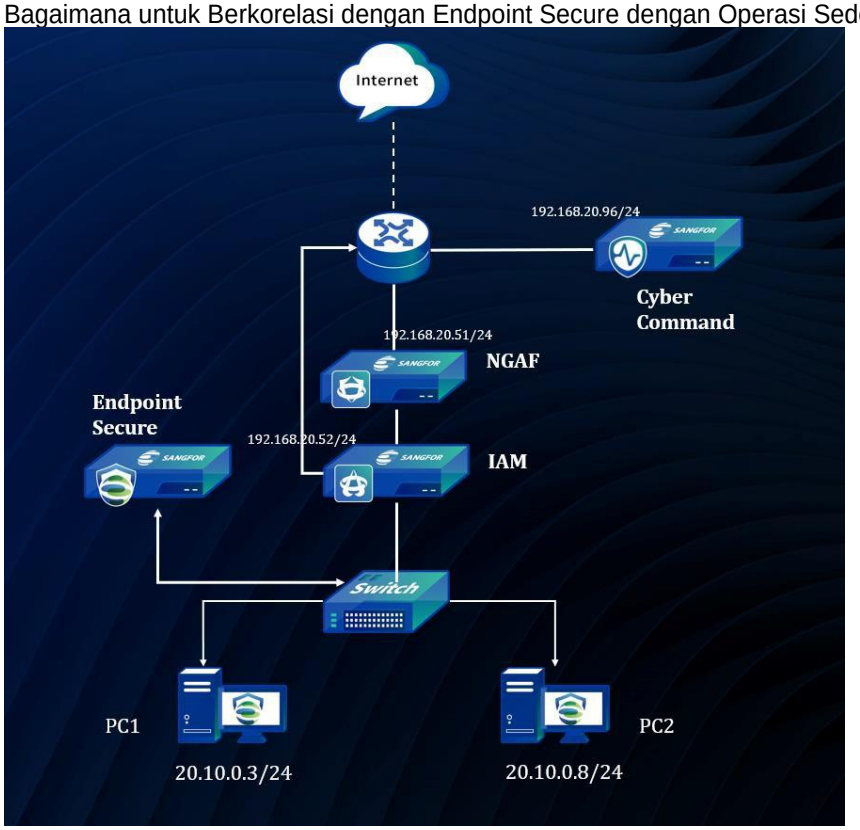
1.1 Skenario

Pelanggan menggunakan Cyber Command untuk mengumpulkan network traffic dan sistem logs, secara efektif mendeteksi network security keseluruhan, cepat urutkan keluar informasi asset, monitor perilaku akses abnormal secara real time, dan melakukan deteksi real-time dan waspada pada external attacks, aktif server outreach, penetrasi horizontal internal dan perilaku lainnya, Setelah insiden security terjadi, dapat dengan cepat diperingatkan dan ditangani untuk melindungi secara keseluruhan aman dan operasi efektif dari private network. Melalui linkage, platform Sangfor Endpoint Secure masalah security policies untuk memblokir attack yang sesuai secara tepat waktu. Untuk host server yang hilang dan terminal, strategi scanning satu-klik dikeluarkan melalui linkage dengan platform manajemen Endpoint Secure untuk mendeteksi dan memusnahkan program jahat dengan cepat, dan fungsi Micro-Segmentation dari Endpoint Secure Agent digunakan untuk memblokir host attack dan mencegah ancaman lebih lanjut dari penyebaran.

1.2 Lingkungan

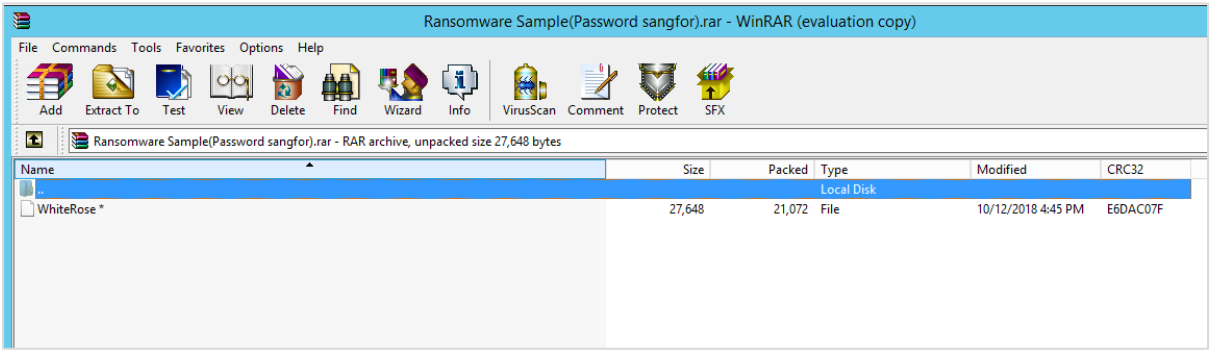
1.2.1 Lingkungan Network

Bagaimana untuk Berkorelasi dengan Endpoint Secure dengan Operasi Sederhana



1.2.2 Contoh Virus

Ransomware Sample(Password sangfor).rar dapat digunakan untuk ransomware testing yang bisa di-download dengan cara searching pada PMO tanpa di-running. Setelah memulai

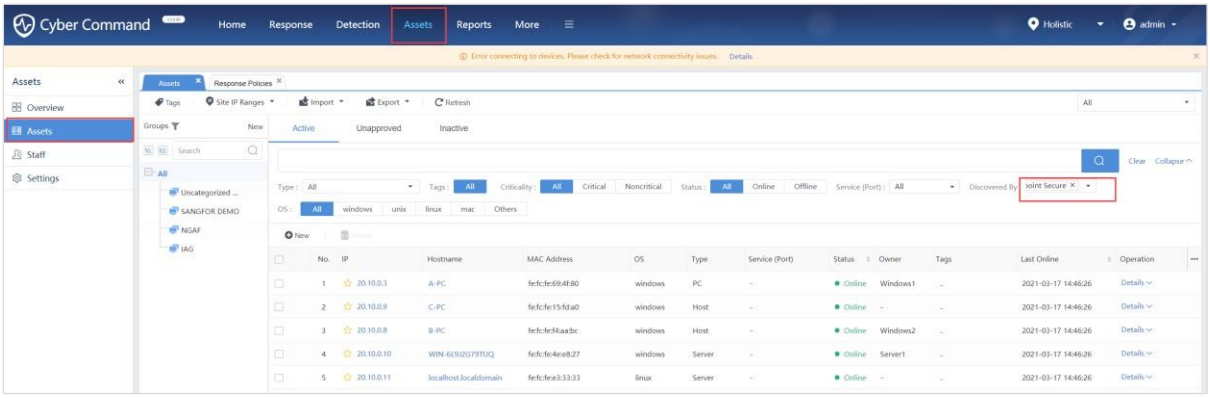


real-time monitoring pada ES, virus dapat terdeteksi setelah file tersebut di-decompressed.

1.3 Tindakan Pencegahan

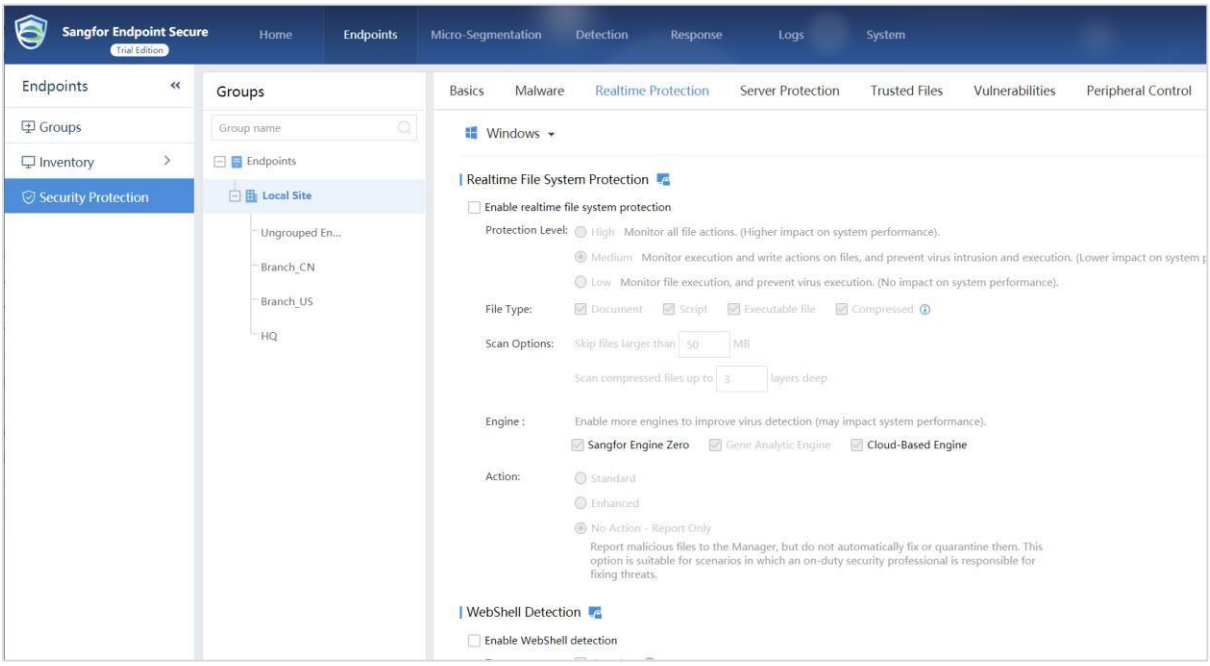
1. Harap pastikan bahwa Endpoint Secure tersinkronisasi semua asset ke Cyber Command.

Bagaimana untuk Berkorelasi dengan Endpoint Secure dengan Operasi Sederhana



2. Nonaktifkan Realtime File System Protection dan Protection lainnya, untuk itu kita harus menghindari Endpoint Secure menghilangkan virus secara langsung, setelah nonaktifkan Realtime Protection dari Endpoint Secure, kemudian virus tidak akan dihilangkan secara otomatis oleh Endpoint Secure dan Endpoint Secure akan tersinkronisasi security log ke Cyber Command.

Sampel virus yang kami gunakan hanya untuk testing internal dari efek korelasi, dan deteksi realtime perlu diaktifkan ketika efek korelasi di tes atau saat implementasi selesai.

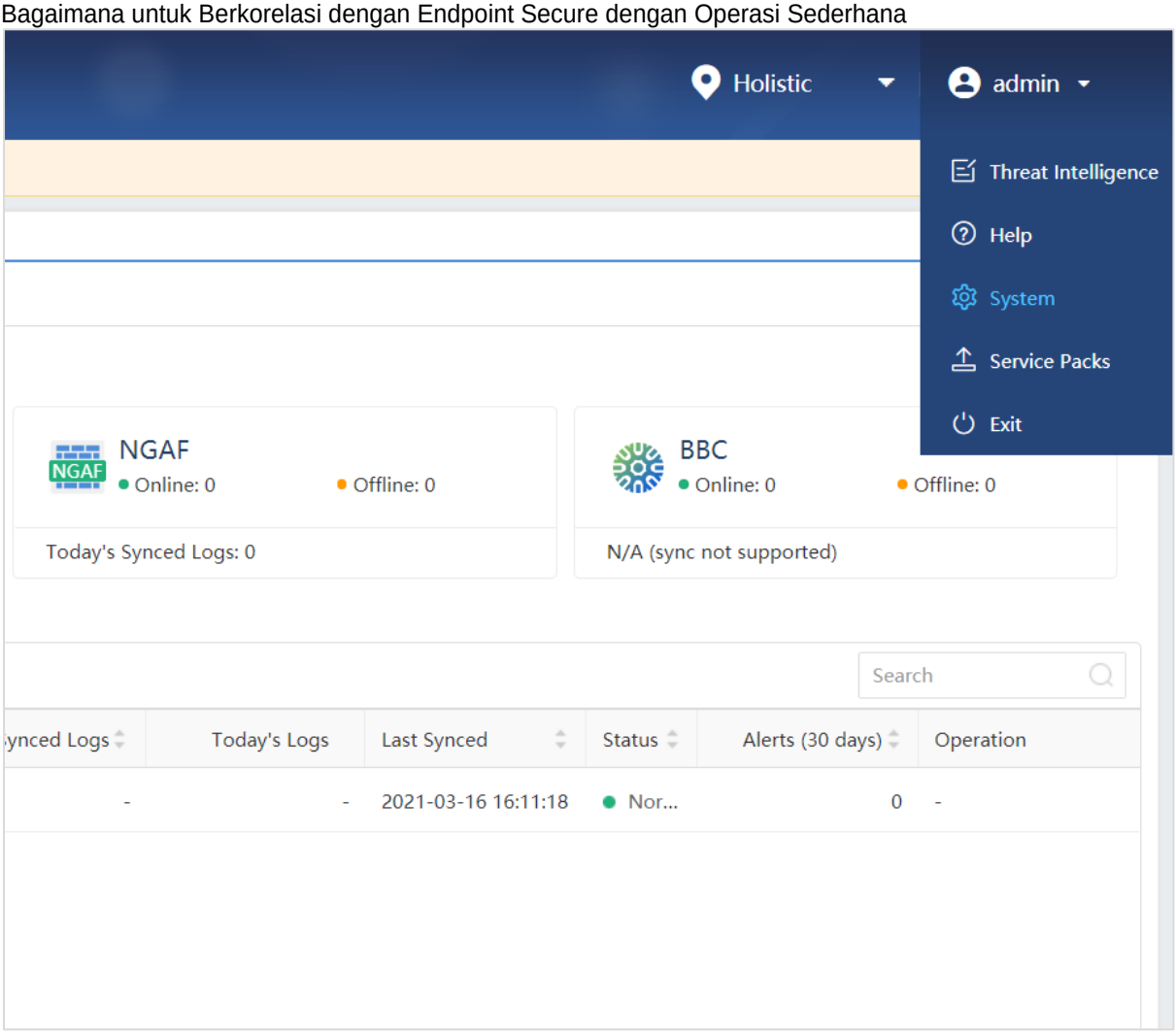


Bab 2 Konfigurasi

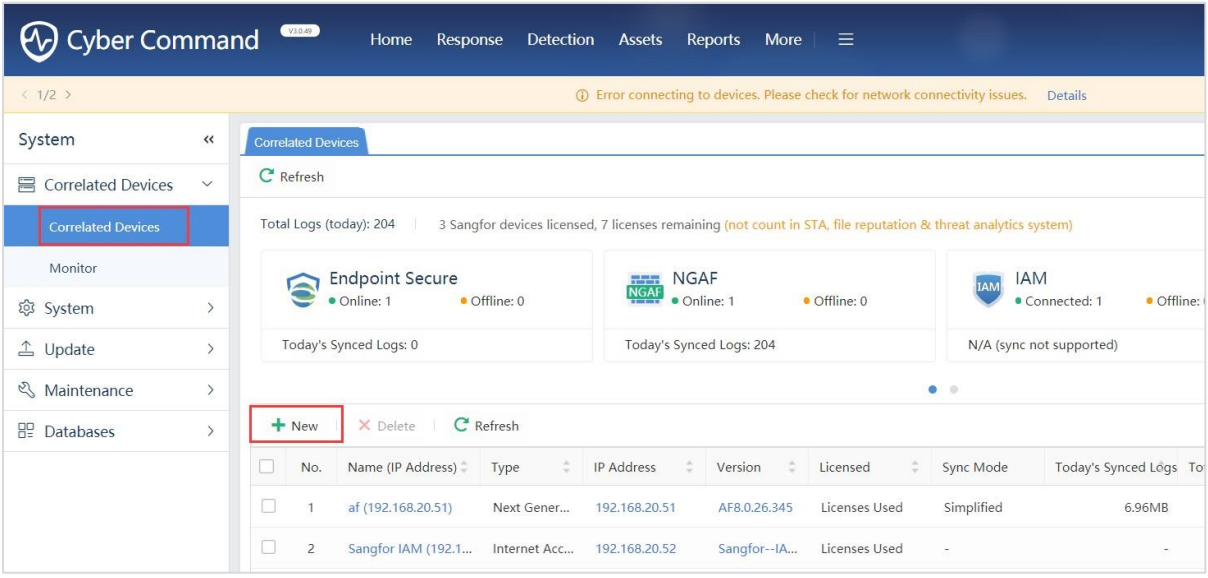
2.1 Konfigurasi Cyber Command

1. Pergi ke System Path.

Bagaimana untuk Berkorelasi dengan Endpoint Secure dengan Operasi Sederhana

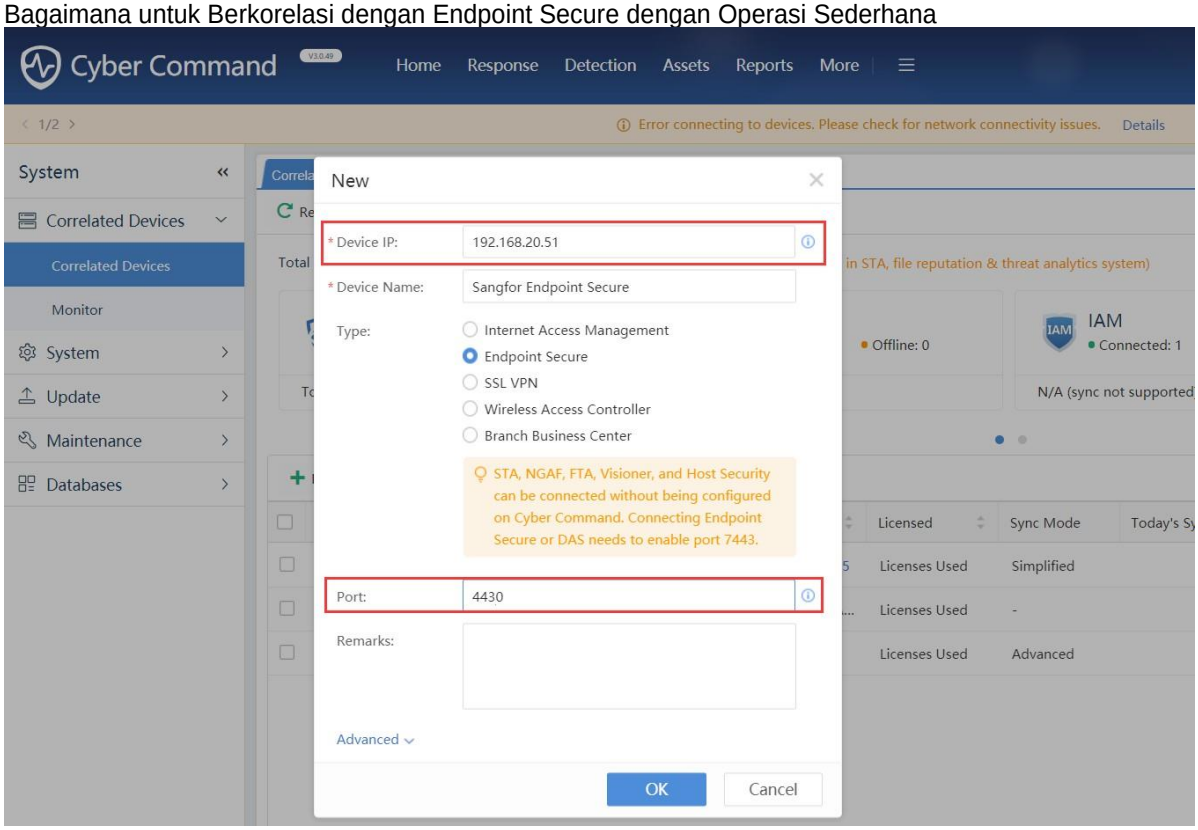


2. Pergi ke Correlated Devices-> Correlated Devices path, dan klik New untuk create Correlation.

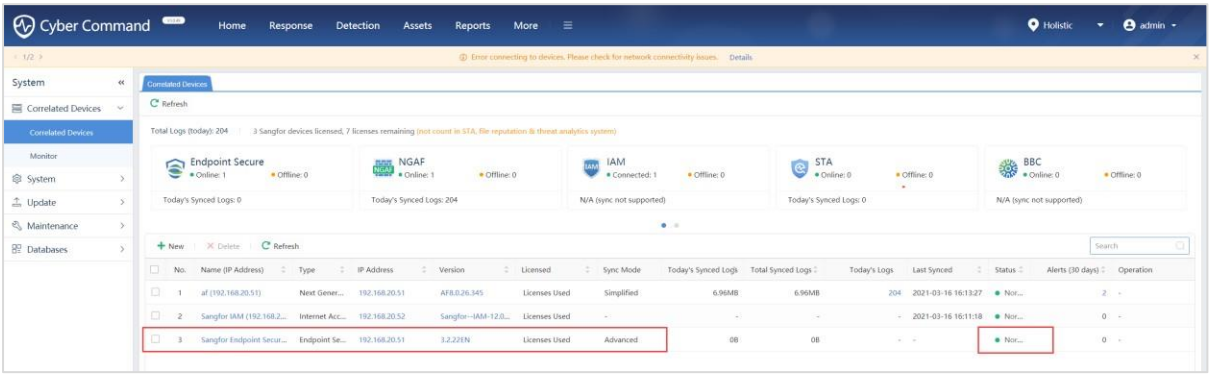


3. Masukkan IP dari Endpoint Secure dan Port, jika Endpoint Secure deploy setelah perangkat NAT, Silakan map port 443 dari Endpoint Secure ke perangkat NAT . Misalnya, ini adalah port 4430 mapped ke perangkat NAT.

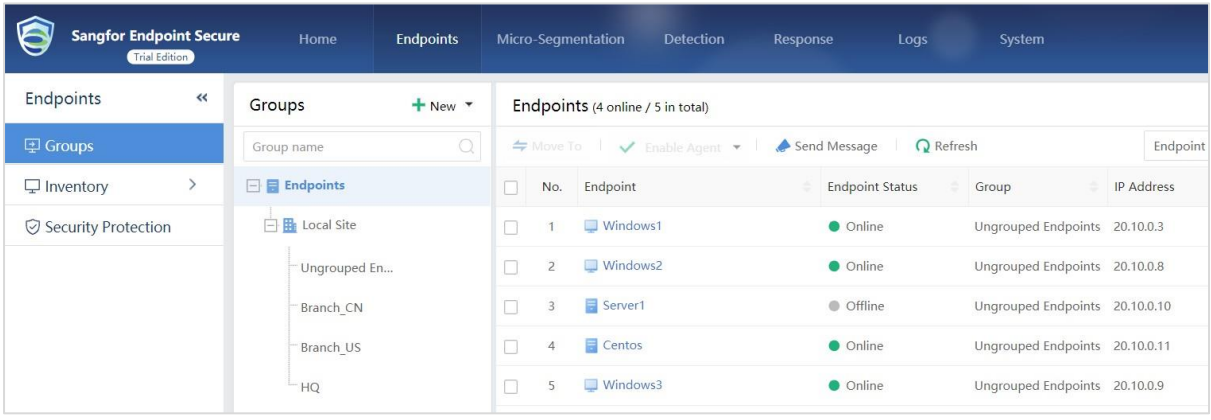
Bagaimana untuk Berkorelasi dengan Endpoint Secure dengan Operasi Sederhana



4. Setelah klik OK, Anda dapat melihat status korelasi di console.

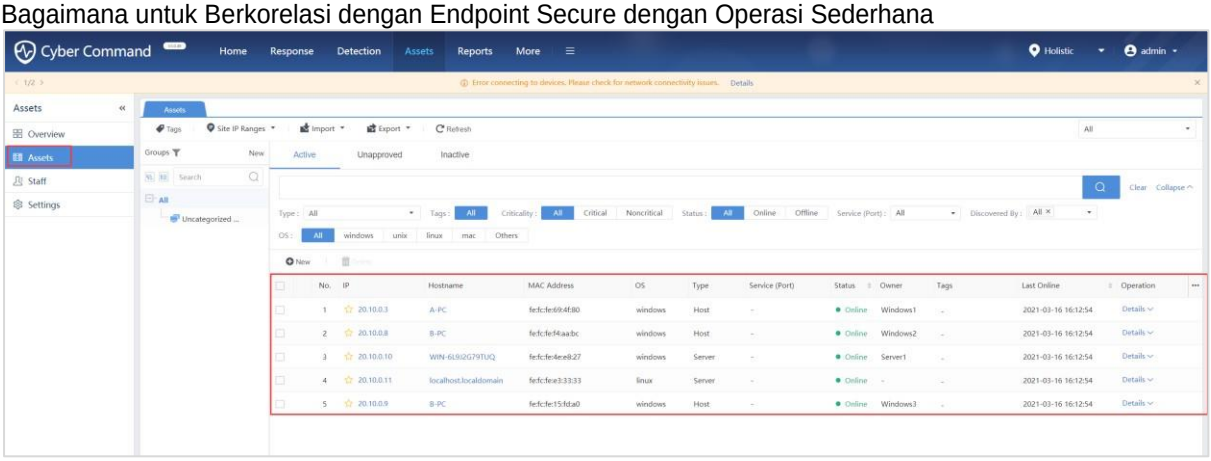


5. Anda dapat memeriksa apakah ada asset di Endpoint Secure.



6. Jika Anda ada di Endpoint Secure, pergi ke Assets->Assets di Cyber Command untuk memeriksa apakah asset telah tersinkronisasi ke Cyber Command.

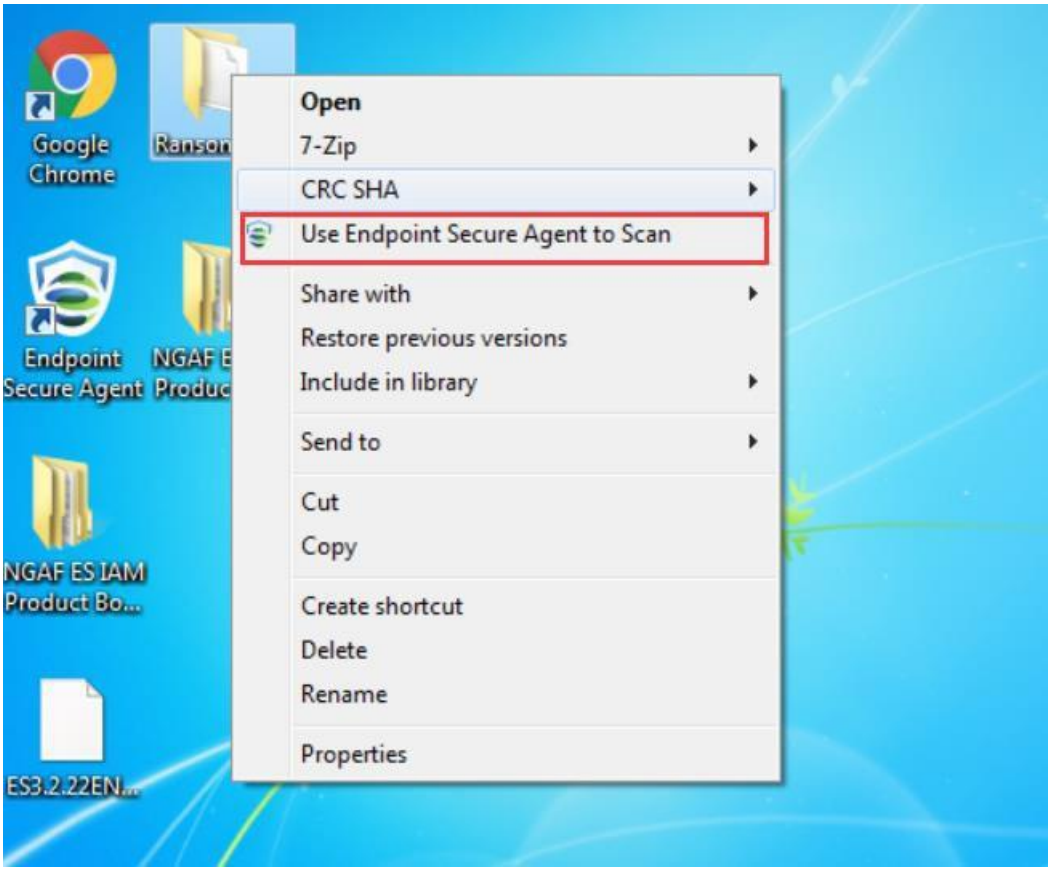
Bagaimana untuk Berkorelasi dengan Endpoint Secure dengan Operasi Sederhana



Bab 3 Korelasi

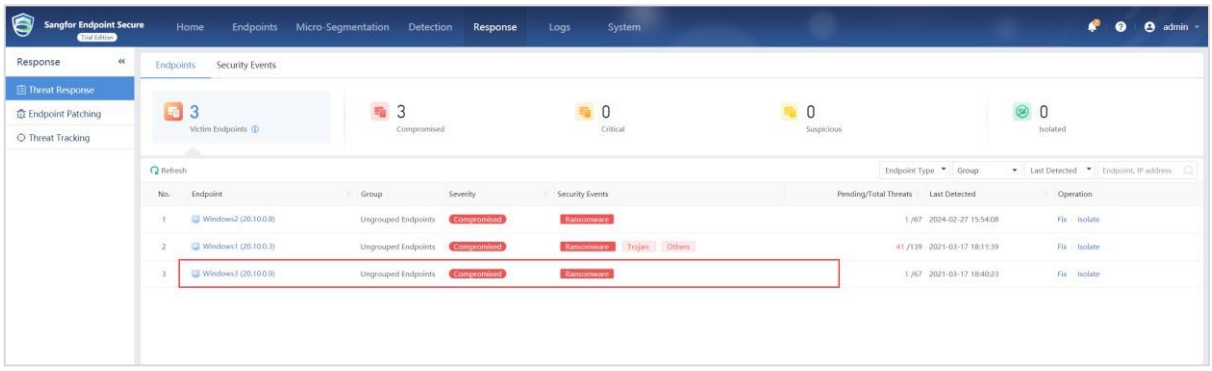
3.1 Generate Security Logs dan Sinkronisasi ke Cyber Command

1. Setelah pelanggan mendekompresi file, gunakan scan Endpoint Secure atau schedule scan.

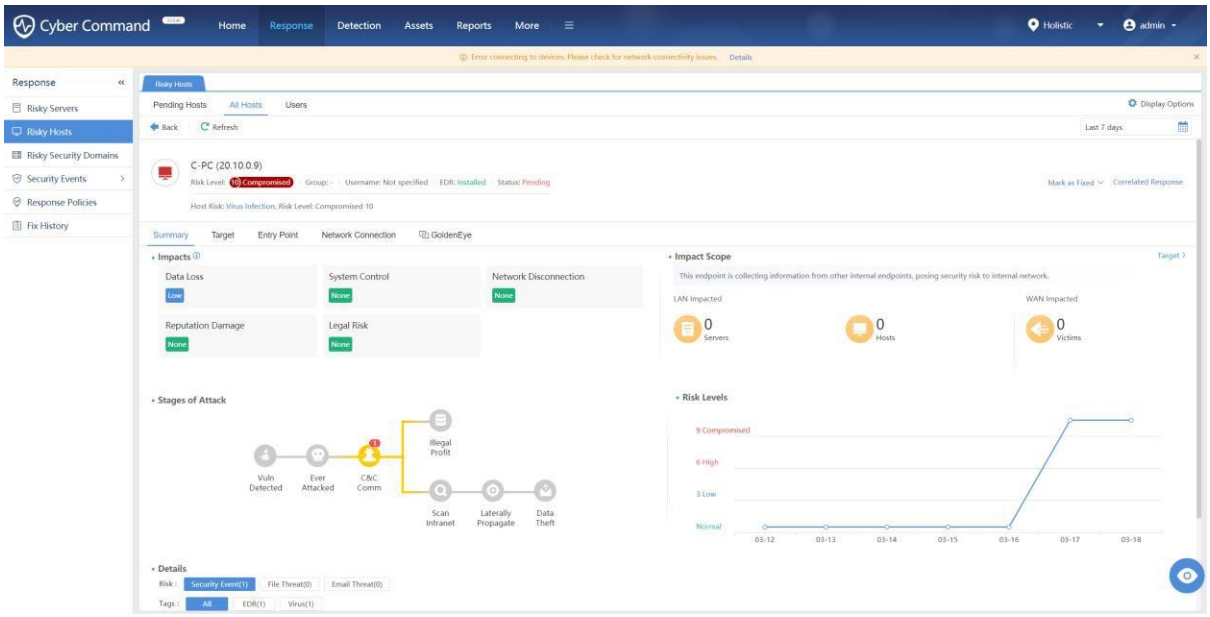


2. Jika file virus terdeteksi, Anda dapat melihat virus log terkait di Endpoint Secure MGR.

Bagaimana untuk Berkorelasi dengan Endpoint Secure dengan Operasi Sederhana

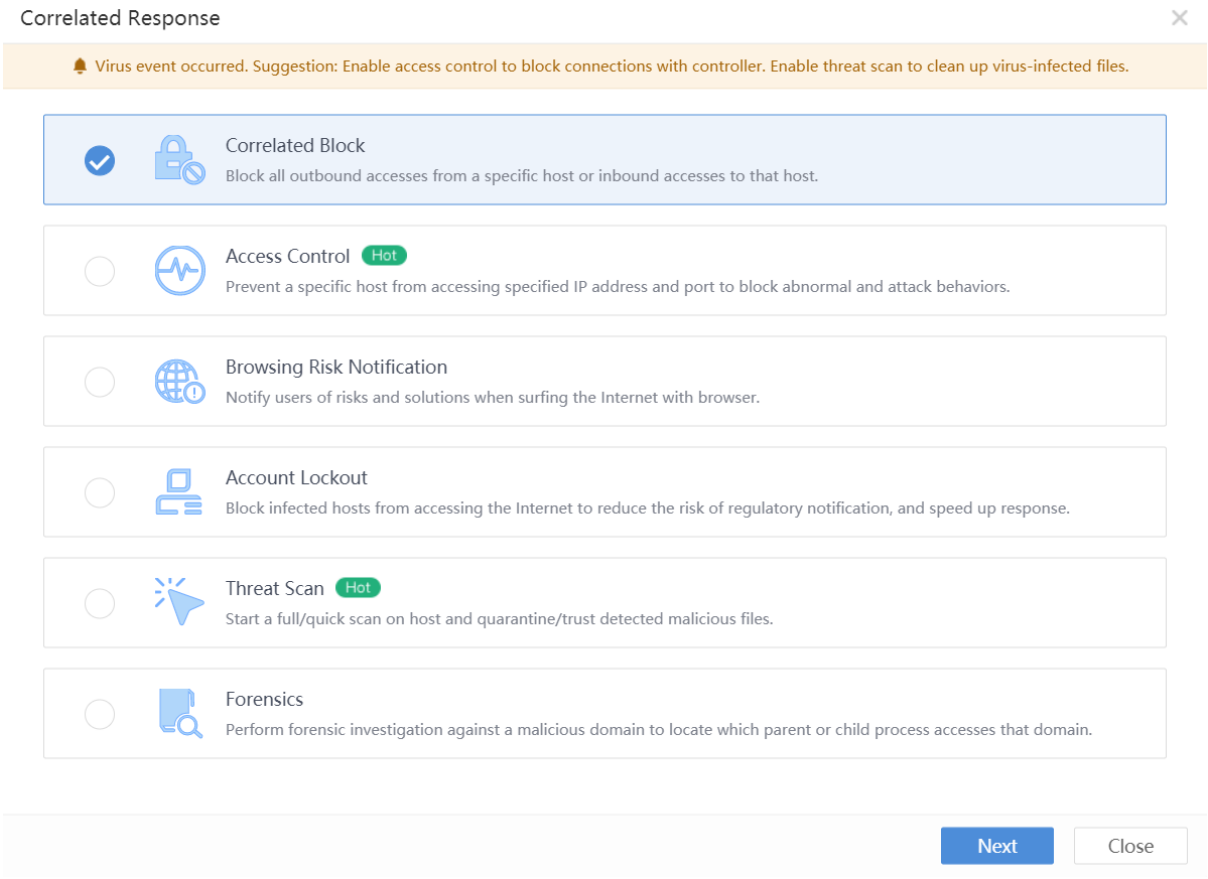


3. Endpoint Secure akan sinkronisasi virus log ke Cyber Command, dan Anda dapat melihat detail

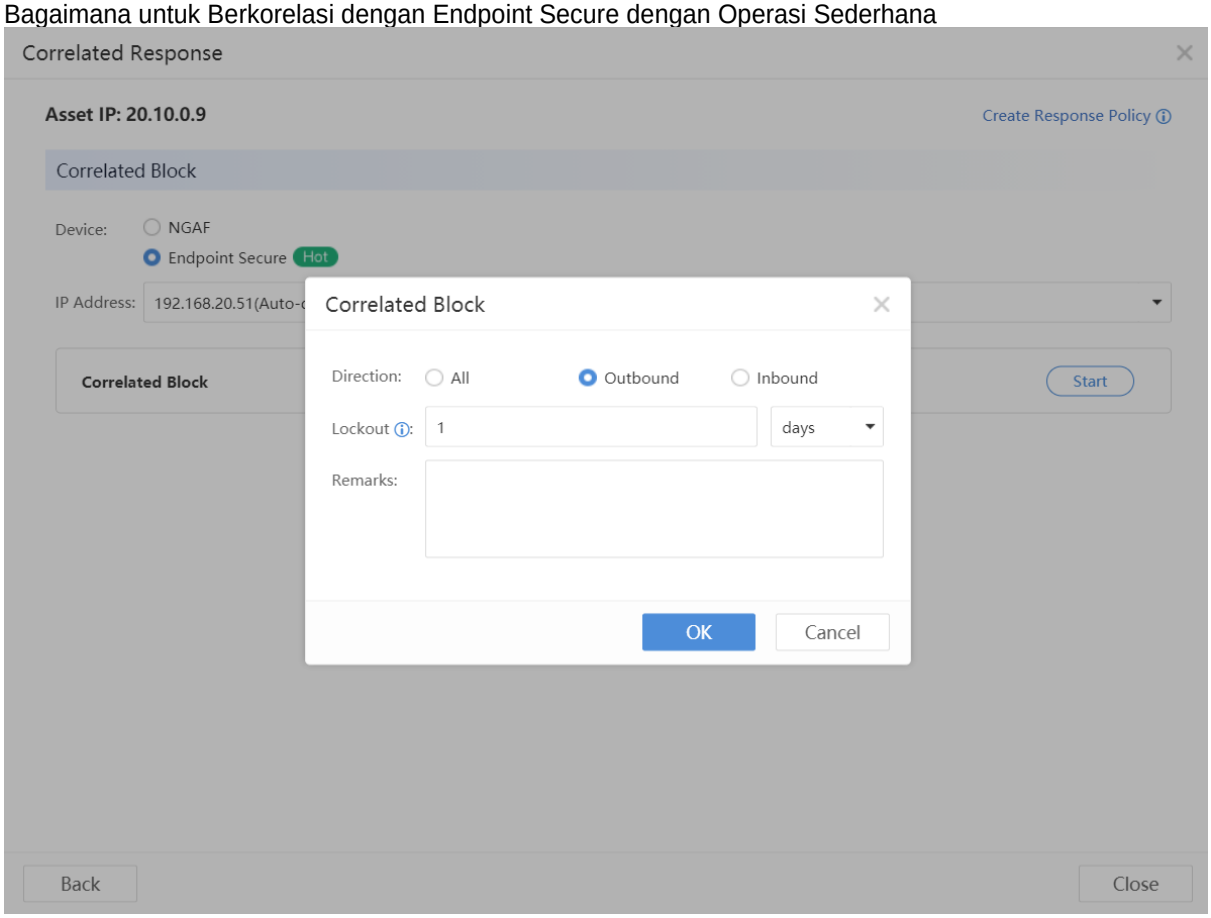


virus log masuk.

4. Klik Correlated Response, dan Anda dapat memilih tindakan yang berbeda untuk menangani dengan victim host, seperti Anda dapat memilih memblokir victim host.

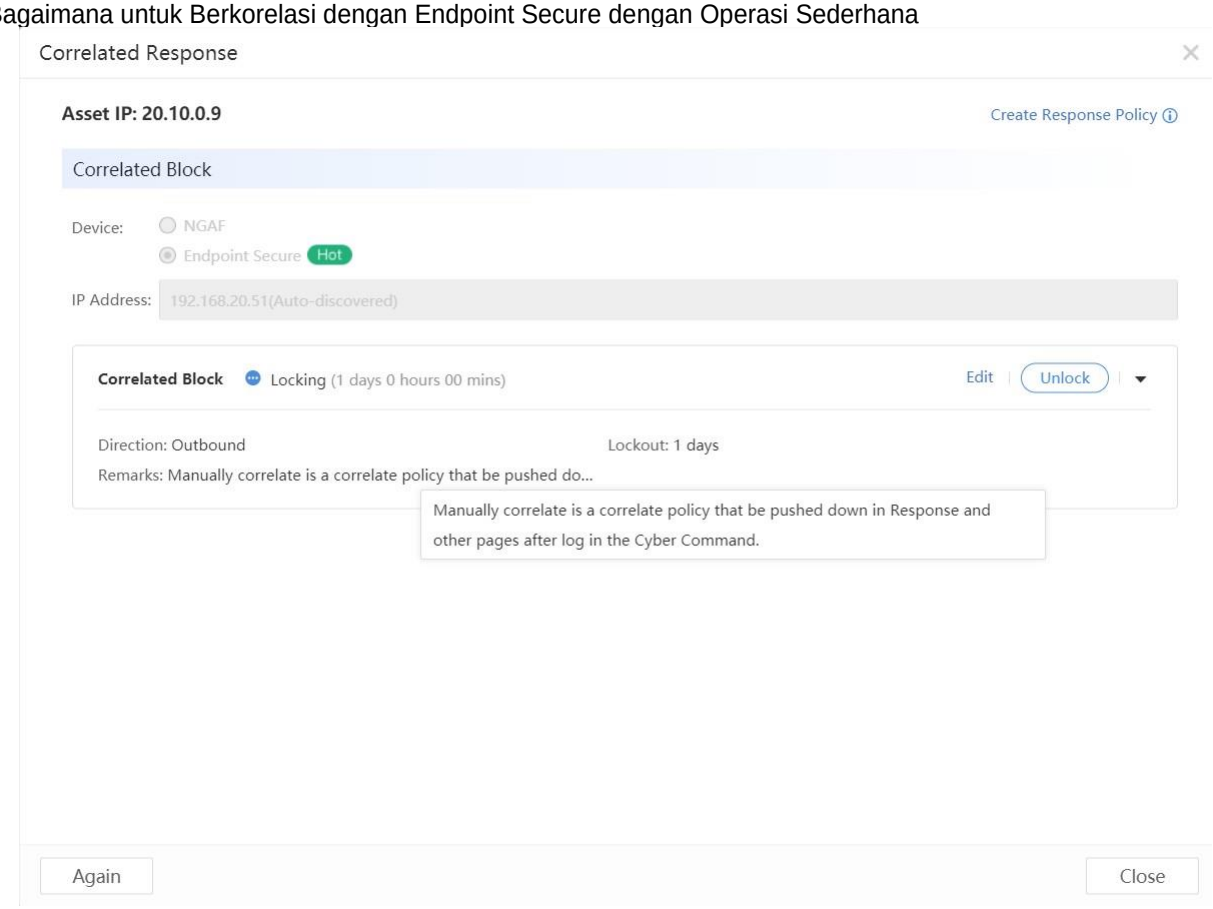


5. Pilih Endpoint Secure sebagai correlated device dan klik Start.



6. Setelah klik OK, tunggu beberapa detik, maka Anda dapat melihat block policy berhasil dikeluarkan.

Bagaimana untuk Berkorelasi dengan Endpoint Secure dengan Operasi Sederhana



7. Anda dapat pergi ke Response->Threat Response->Isolated path, dan kemudian Anda dapat melihat host yang telah diisolasi oleh policy yang dikeluarkan oleh Cyber Command.