Cyber Command

Praktik Terbaik untuk Skenario_Bagaimana untuk Berkorelasi dengan IAM untuk Operasi Sederhana

Versi 3.0.49

Catatan Perubahan

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

Daftar Isi

Bab 1 Skenario

1.1 Skenario

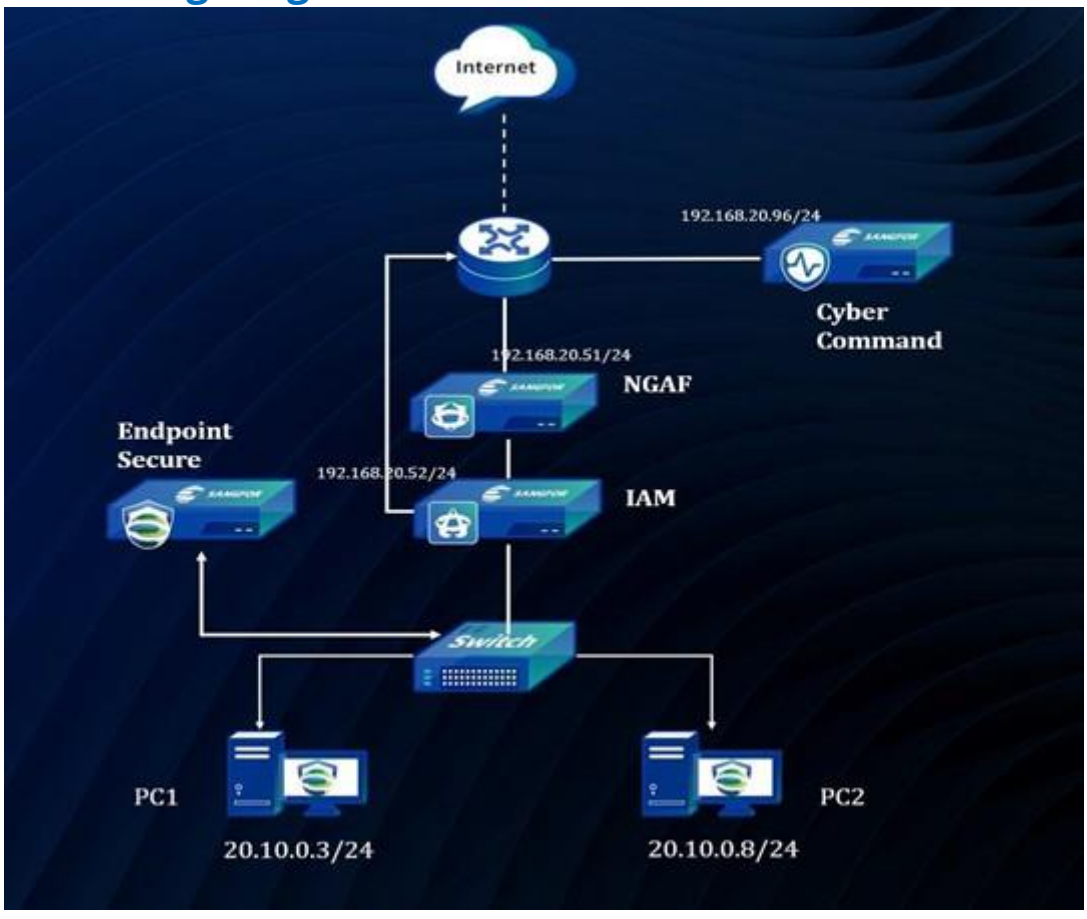
Cyber Command mengumpulkan data dari probe deteksi security dari setiap node intranet, mempersembahkan pengguna dengan bisnis asset intranet dan attack dan potensi ancaman terhadap asset bisnis utama intranet dalam bentuk visual, dan menggunakan platform untuk attack semua sistem security di network yang ada membawa keluar manajemen terpadu dan penerbitan policy.

IAM mendukung visual kontrol dari endpoint, aplikasi, data, dan traffic di seluruh network, dan secara cerdas merasakan risiko internal seperti pelanggaran akses endpoint, Pelanggaran Internet, dan kebocoran data sensitif, dan menyadari integrasi dari endpoint akses kontrol, Internet akses kontrol, dan kontrol kebocoran data. Kontrol keamanan perilaku.

Di Cyber Command dan Korelasi IAM, IAM sinkronisasi informasi pengguna online ke Cyber Command untuk ringkasan terpadu dan analisis, membantu menemukan pengguna dengan risiko security dengan cepat, jadi untuk mewujudkan pengingat yang akurat, dan memperkuat kontrol security online.

1.2 Lingkungan

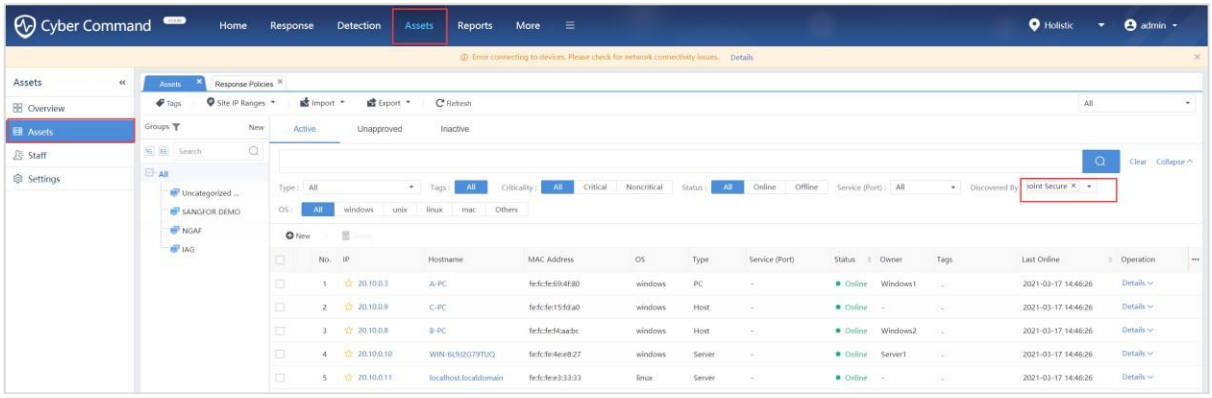
1.2.1 Lingkungan Network



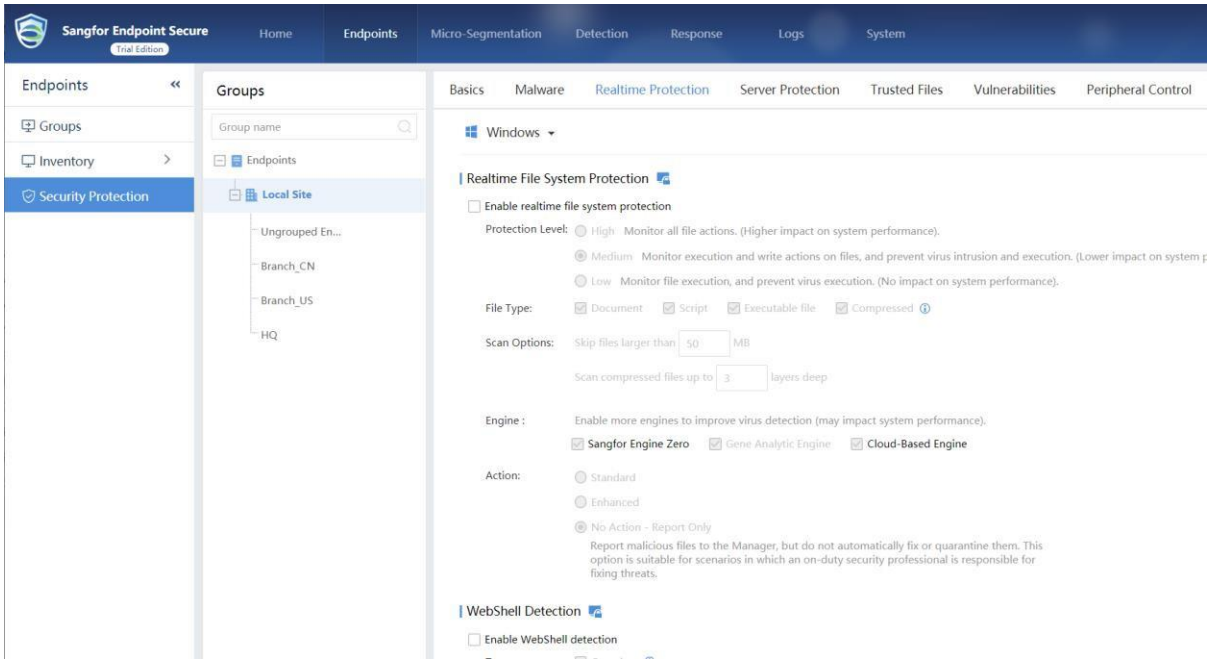
1.3 Tindakan Pencegahan

1. IAM tidak mendukung Sinkronisasi security log ke Cyber Command dan tidak mendukung anti virus di endpoint, Cyber Command hanya mendukung masalah lockout atau pengingat policy ke IAM, jadi Anda perlu instal Endpoint Secure agar IAM berkorelasi untuk scan virus dan sinkronisasi security log ke Cyber Command, then maka Anda dapat konfigurasi response policy di Cyber Command.

2. Harap pastikan bahwa Endpoint Secure sinkronisasi semua asset ke Cyber Command.



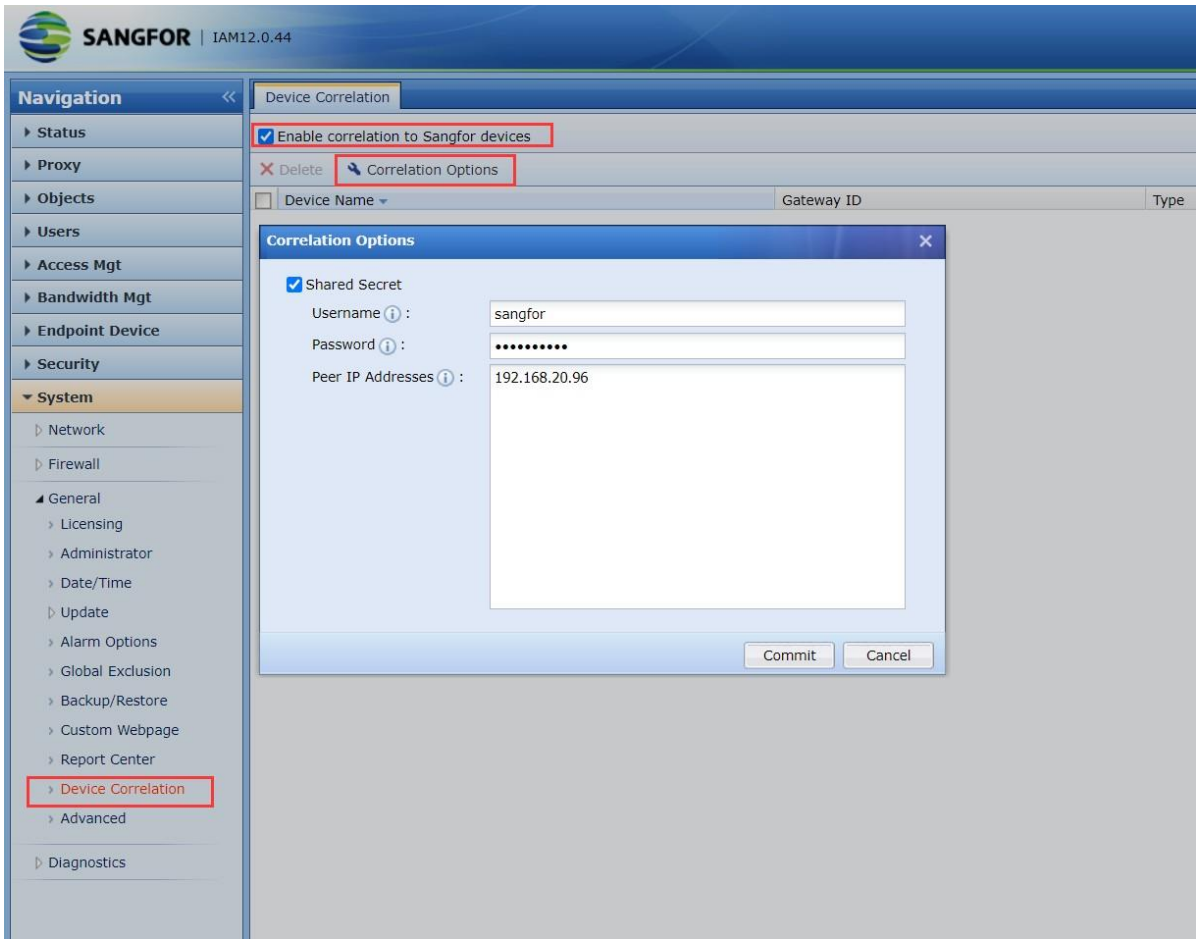
3. Nonaktifkan Realtime File System Protection dan Protection lainnya, untuk itu kita harus menghindari Endpoint Secure memusnahkan virus secara langsung, setelah nonaktifkan Realtime Protection dari Endpoint Secure, lalu IAM dapat deteksi traffic dari Botnet. **Sampel virus yang kami gunakan hanya untuk testing internal dari efek korelasi, dan deteksi real-time perlu diaktifkan saat efek korelasi di tes atau saat implementasi selesai.**



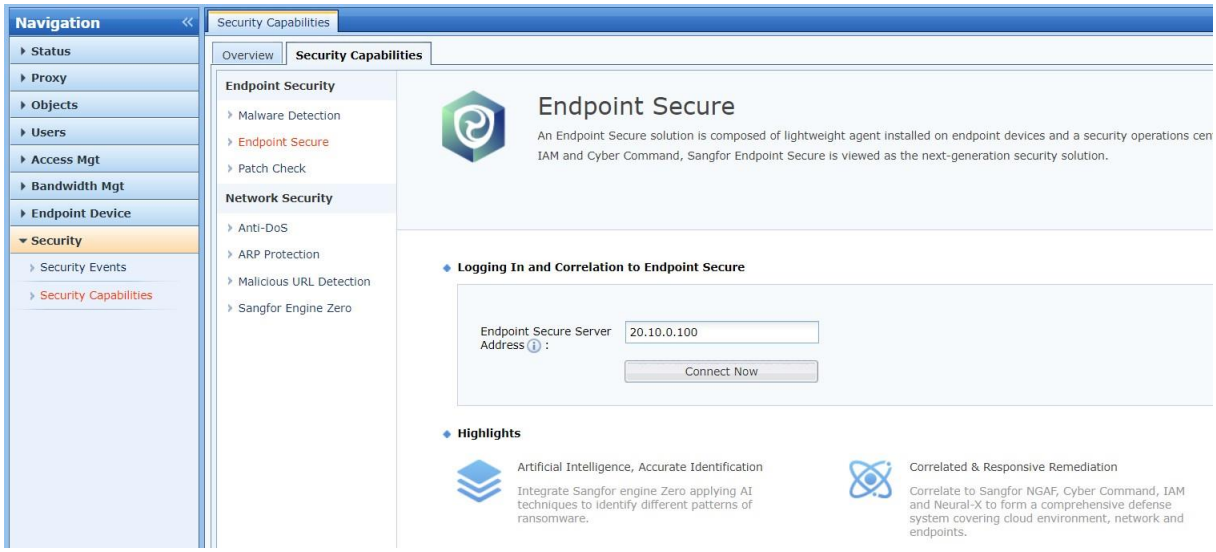
Bab 2 Konfigurasi

2.1 Konfigurasi IAM

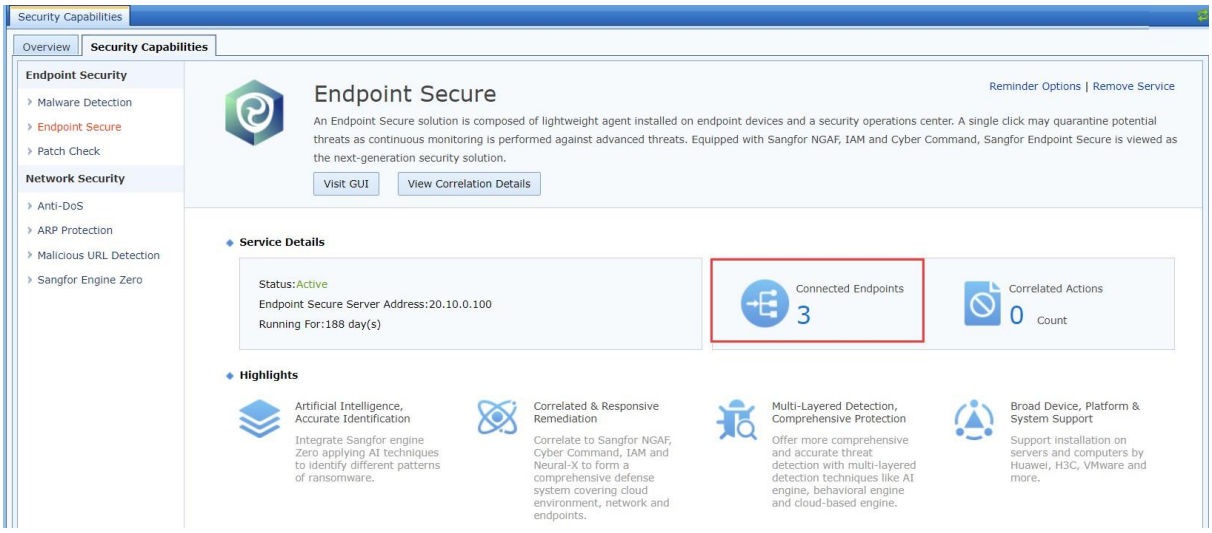
1. Pergi ke System-> General->Device Correlation.



2. Pergi ke Security-> Security Capabilities path. Masukkan IP address dari Endpoint Secure.



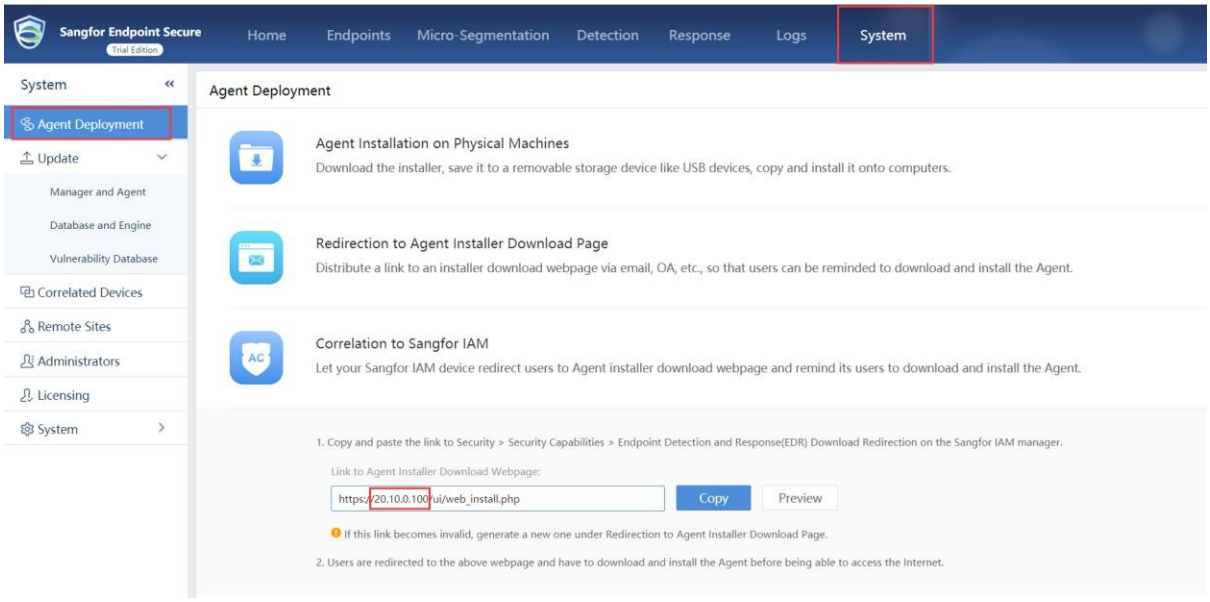
3. Setelah IAM terkoneksi ke Endpoint Secure, Anda dapat melihat endpoint count bahwa berapa banyak endpoint yang sudah terkoneksi ke MGR.



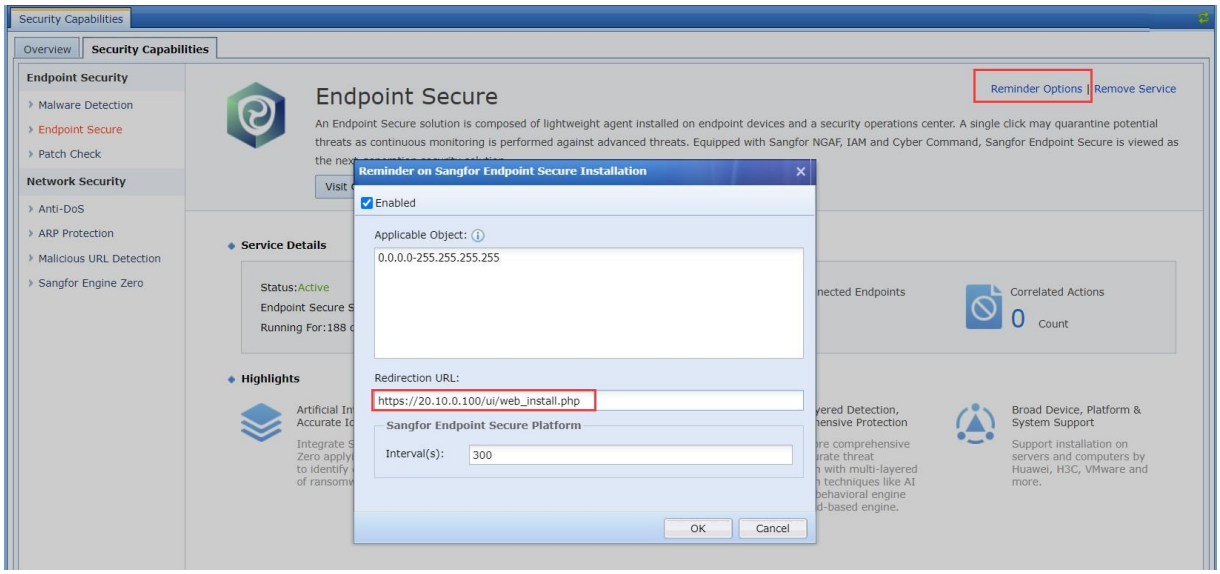
4. Dalam order ke IAM dapat mengarahkan halaman pengingat ke risk endpoint, Anda harus konfigurasi policy pengingat di IAM.

Pertama, konfigurasi risk reminder page address di Endpoint Secure, Anda dapat ke System-> Agent Deployment-> Correlation to Sangfor IAM page dan konfigurasi ES agent download address sehingga IAM dapat mengarahkan PC ke halaman agent download.

Catatan: Anda harus memastikan bahwa internal endpoint dapat mengakses ES agent download address.

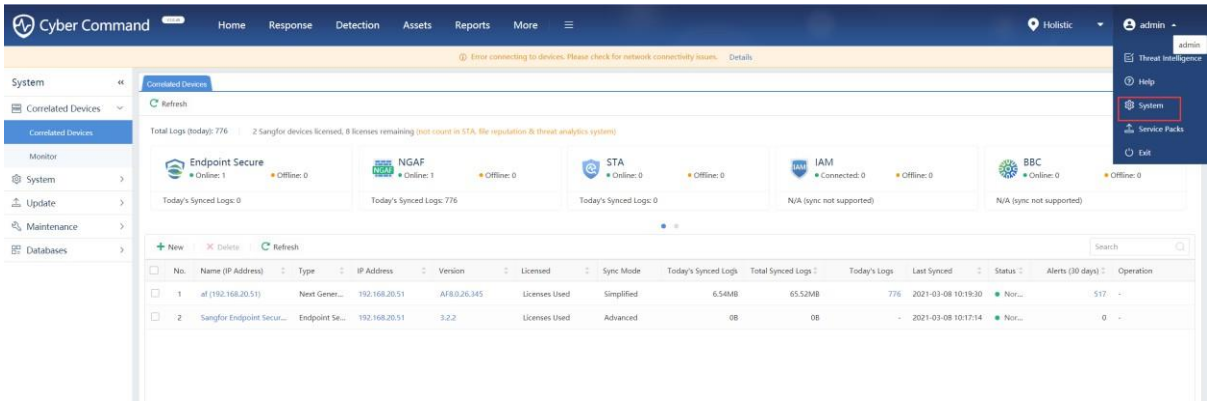


Kedua, konfigurasi pengingat policy di IAM, silakan pastikan URL redireksi sama seperti yang Anda konfigurasi di ES.

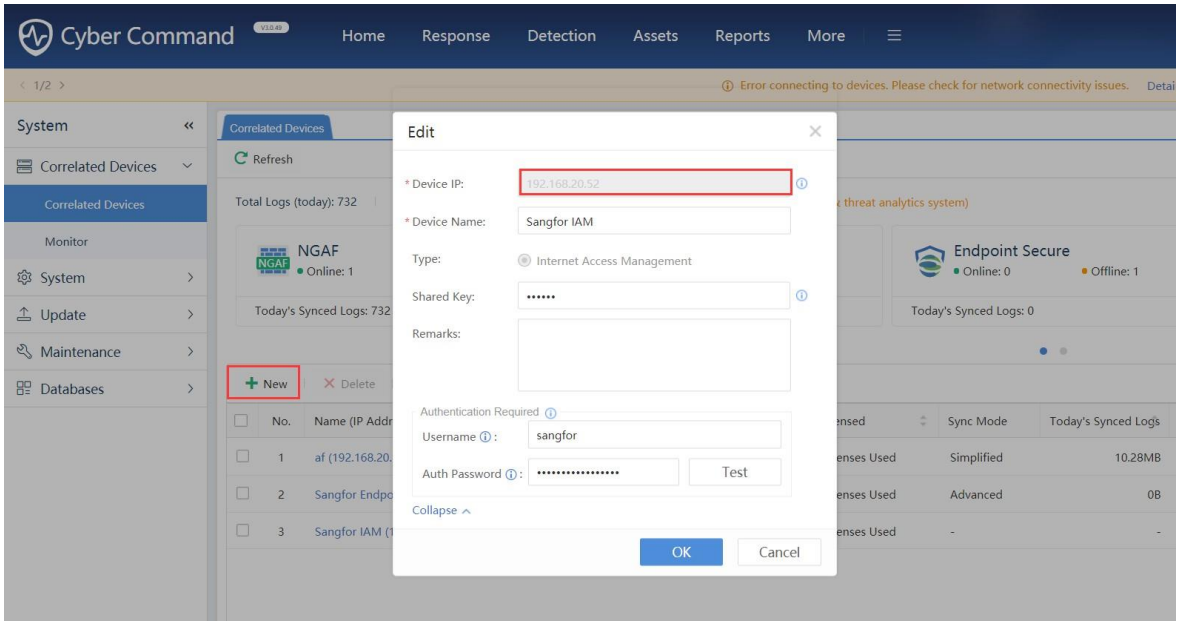


2.2 Konfigurasi Cyber Command

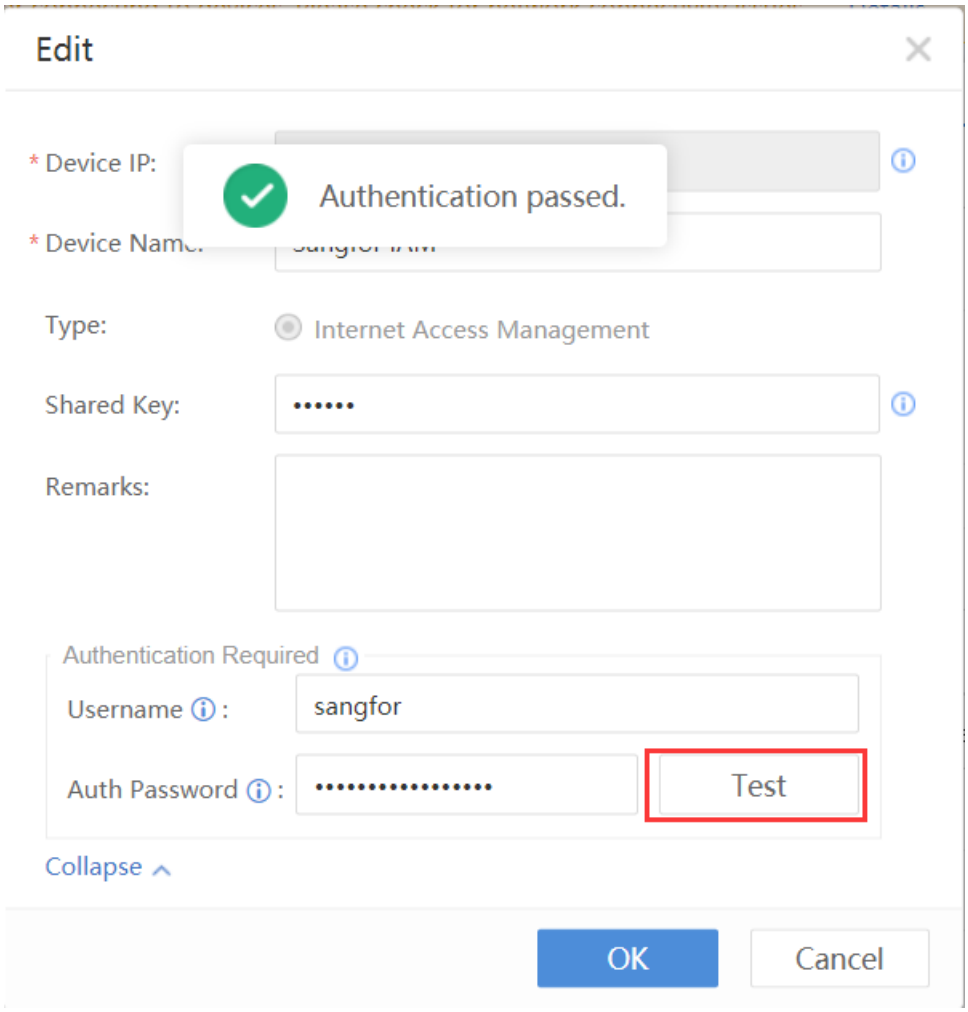
1. Pergi ke System->Correlated Devices-> Correlated Devices.



2. Klik New untuk membuat korelasi, Anda harus memasukkan username dan password yang benar yang Anda konfigurasi di IAM.



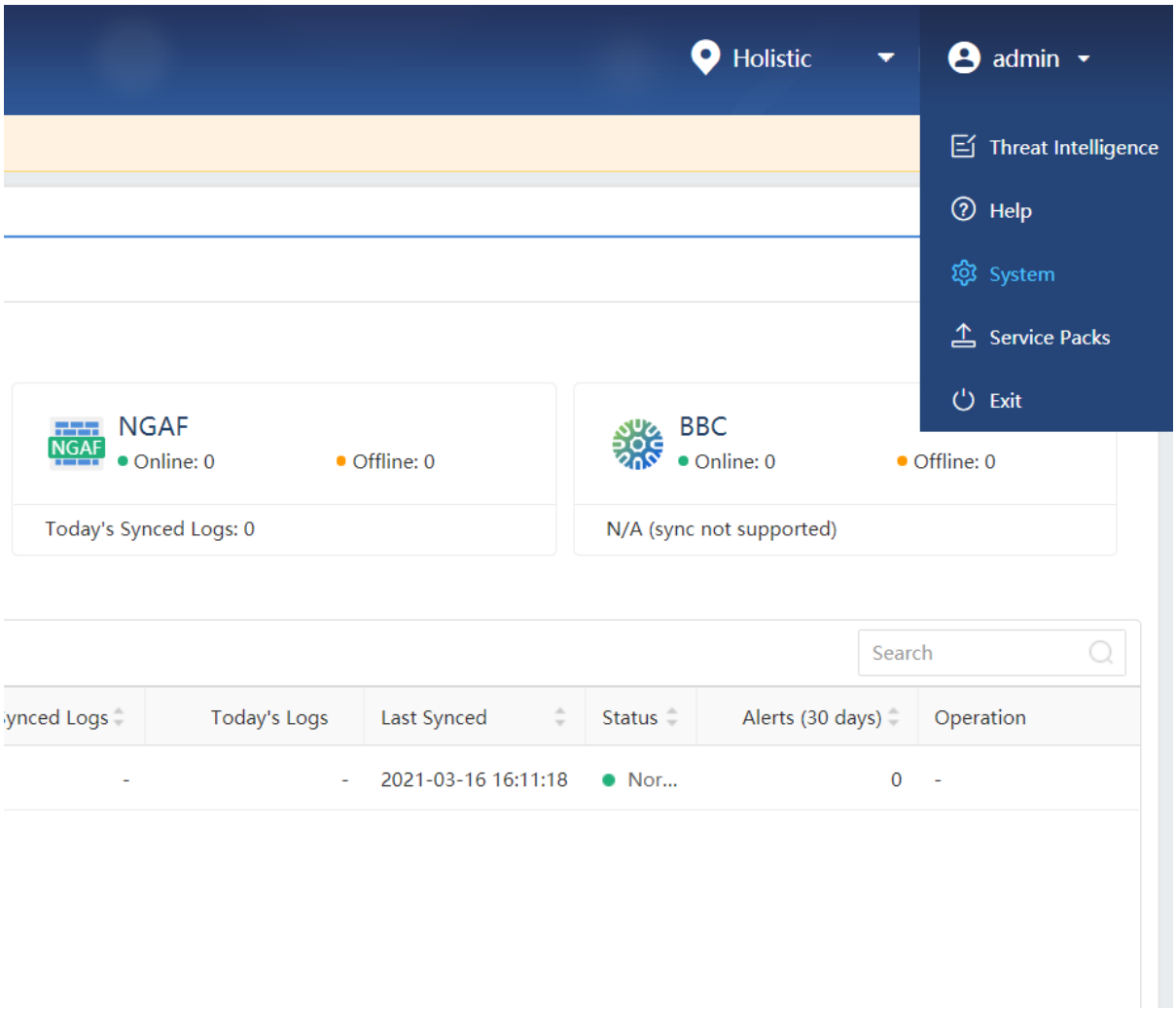
3. Jika Anda tidak yakin apakah username dan password sudah benar, Anda dapat klik tes untuk memeriksa validitas akun.



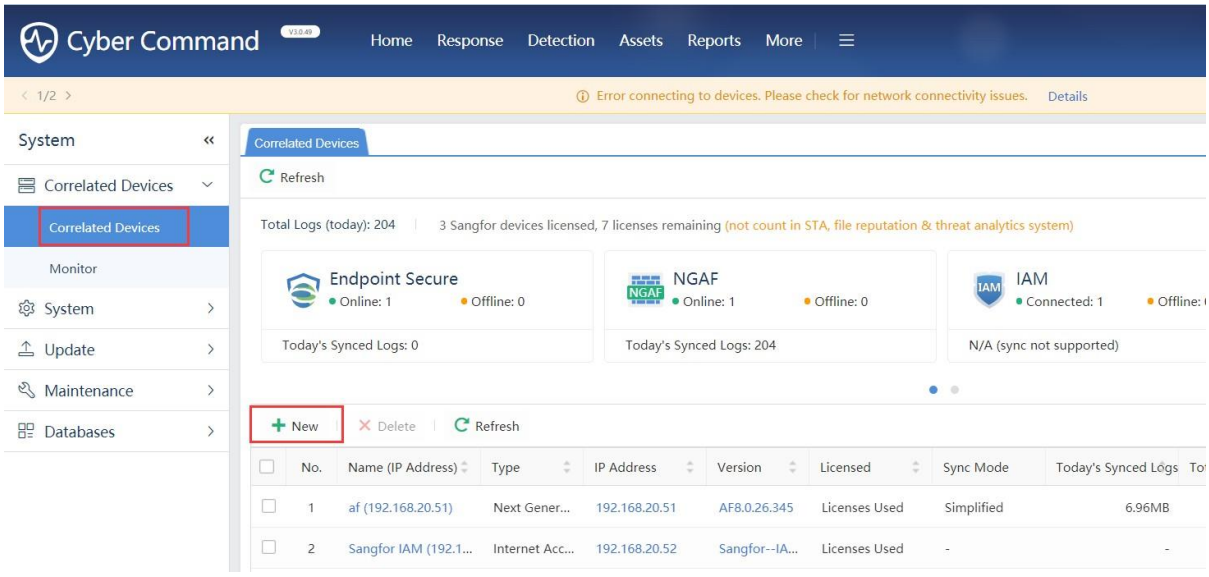
2.3 Konfigurasi Endpoint Secure

1. Pergi ke System Path.

Bagaimana untuk Berkorelasi dengan IAM untuk Operasi Sederhana

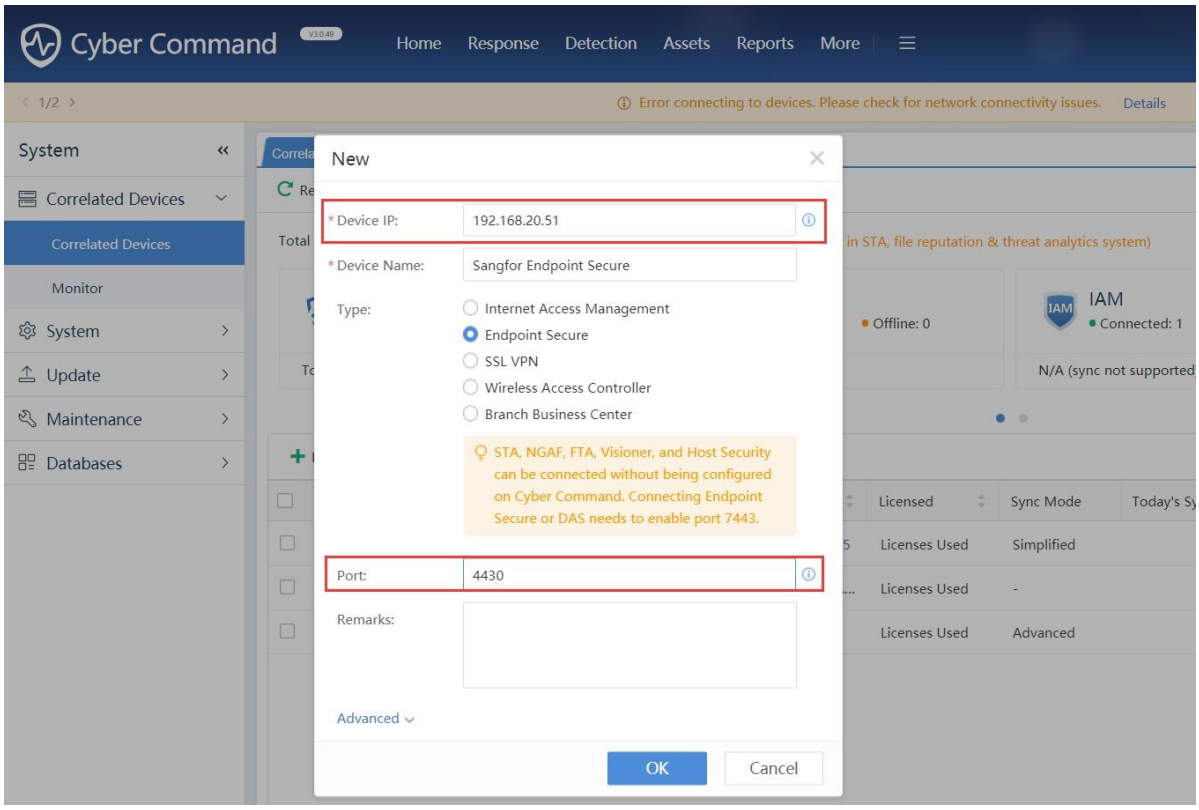


2. Pergi ke Correlated Devices-> Correlated Devices path, dan klik New untuk membuat korelasi.

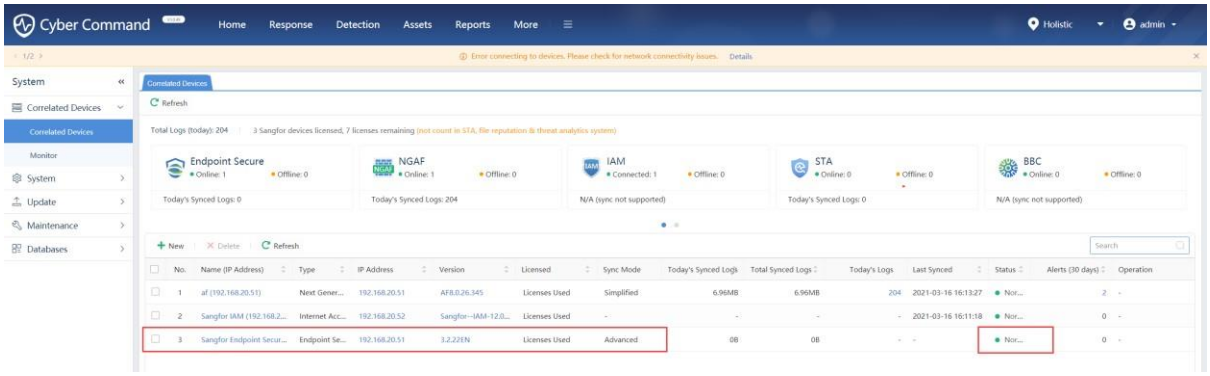


3. Masukkan IP dari Endpoint Secure dan Port, jika Endpoint Secure deploy setelah perangkat NAT, Silakan map port 443 dari Endpoint Secure ke perangkat NAT. Misalnya, ini adalah port 4430 yang di map ke perangkat NAT.

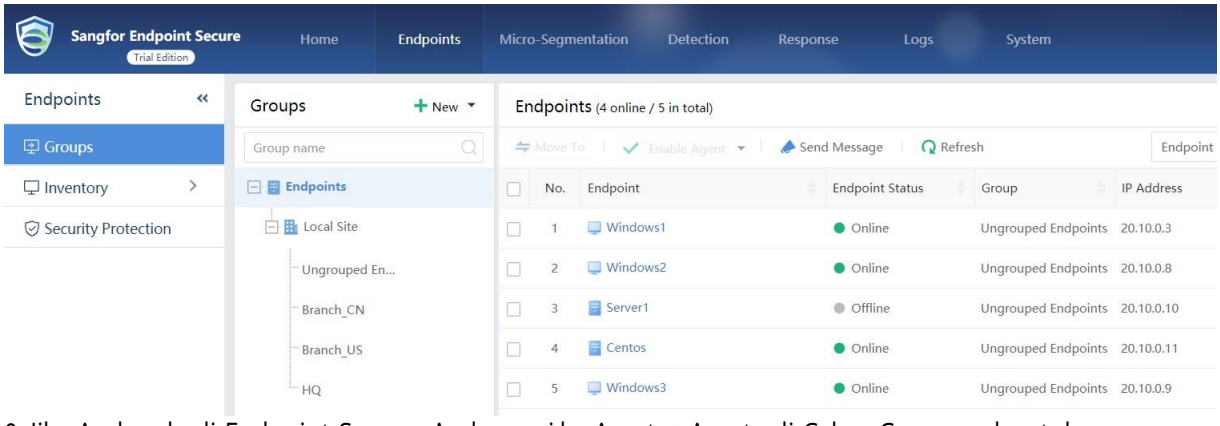
Bagaimana untuk Berkorelasi dengan IAM untuk Operasi Sederhana



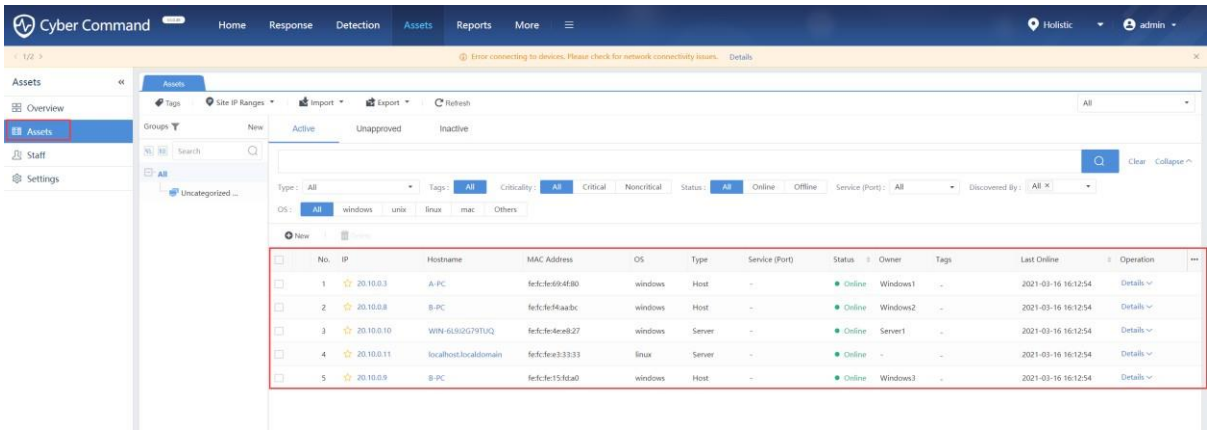
4. Setelah klik OK, Anda dapat melihat status korelasi di console.



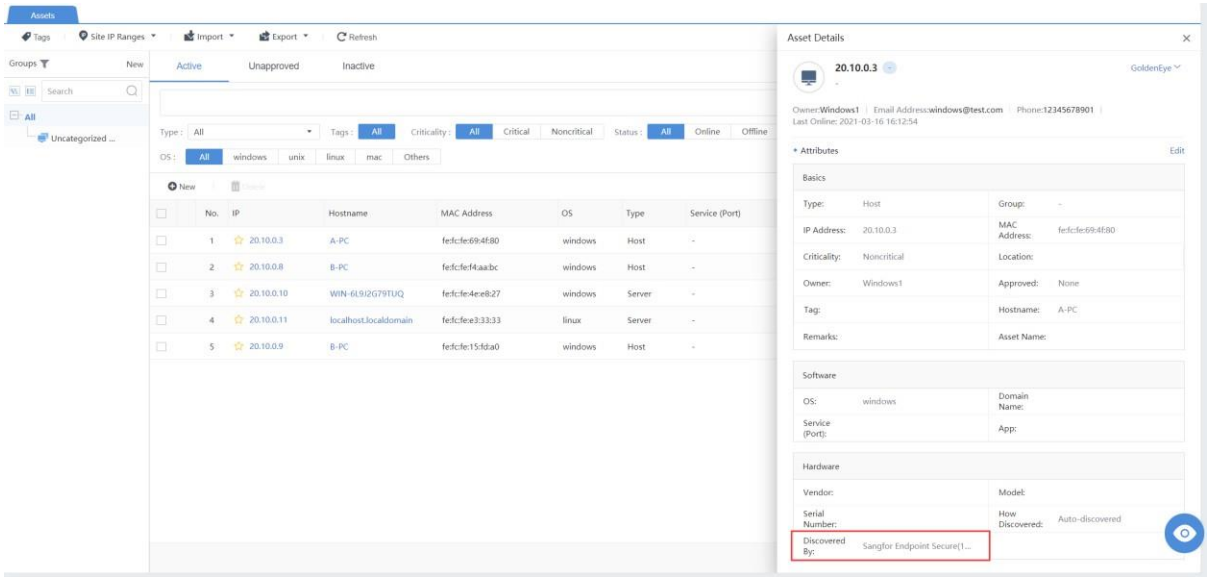
5. Anda dapat memeriksa apakah ada asset di Endpoint Secure.



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



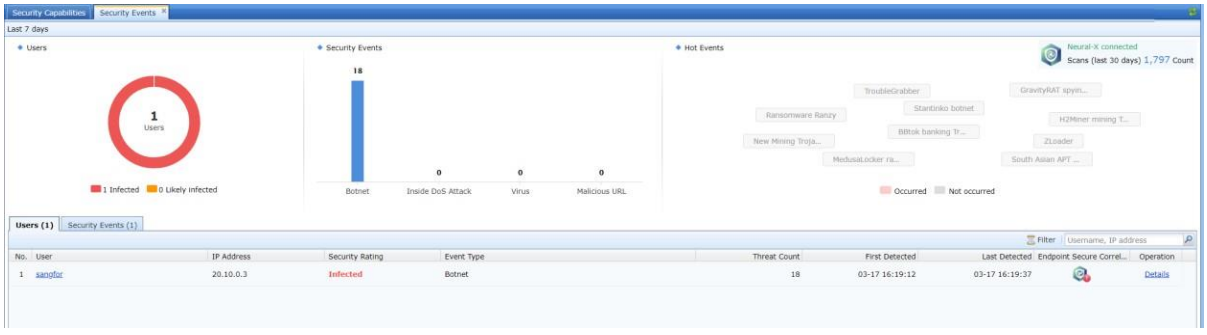
7. Anda dapat melihat detail untuk melihat assets source, seperti berikut detail, Anda dapat melihat asset ini ditemukan oleh Endpoint Secure.



Bab 3 Korelasi

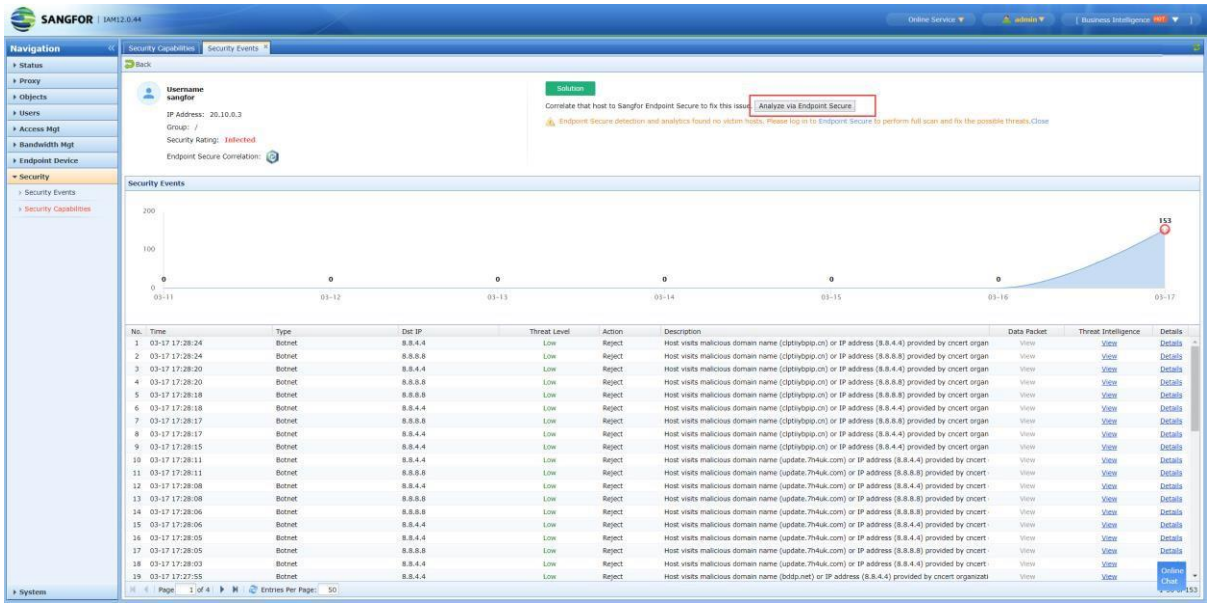
3.1 Sinkronisasi Log ke Cyber Command

1. Ketika IAM deteksi traffic Botnet, Anda dapat melihat log di web console.

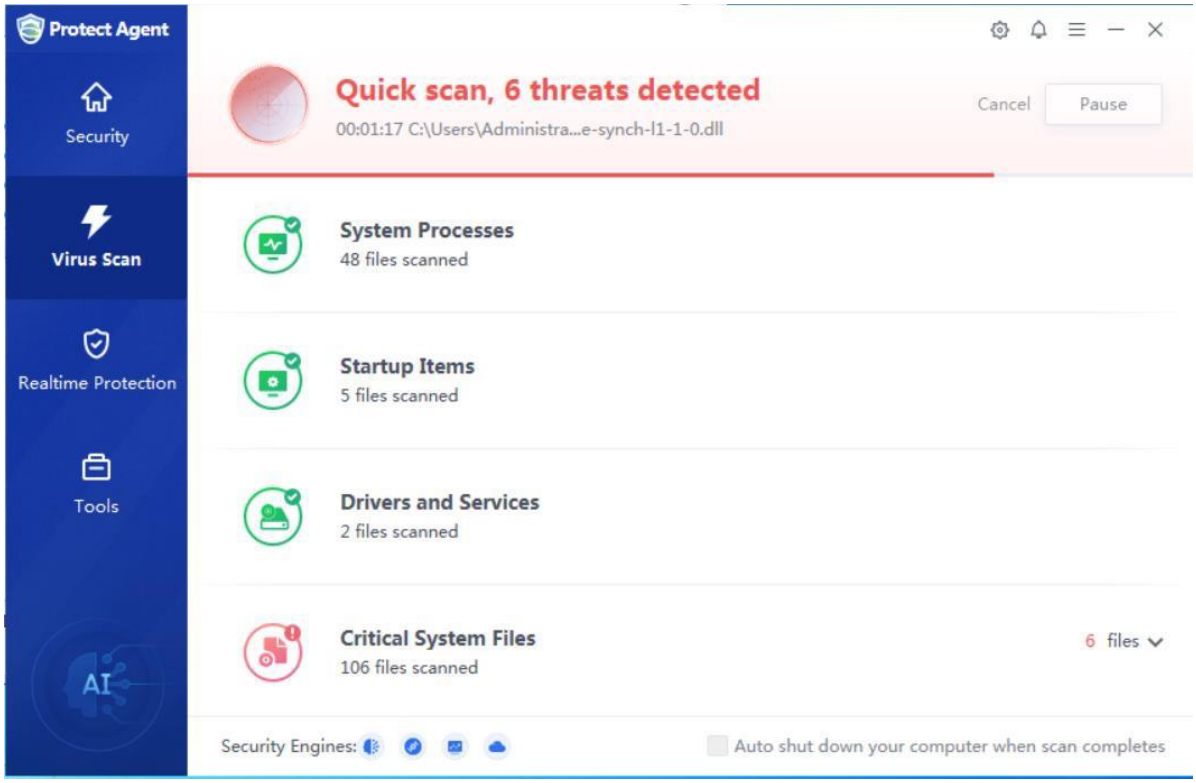


2. Klik Analyze melalui Endpoint Secure untuk mengeluarkan scan task.

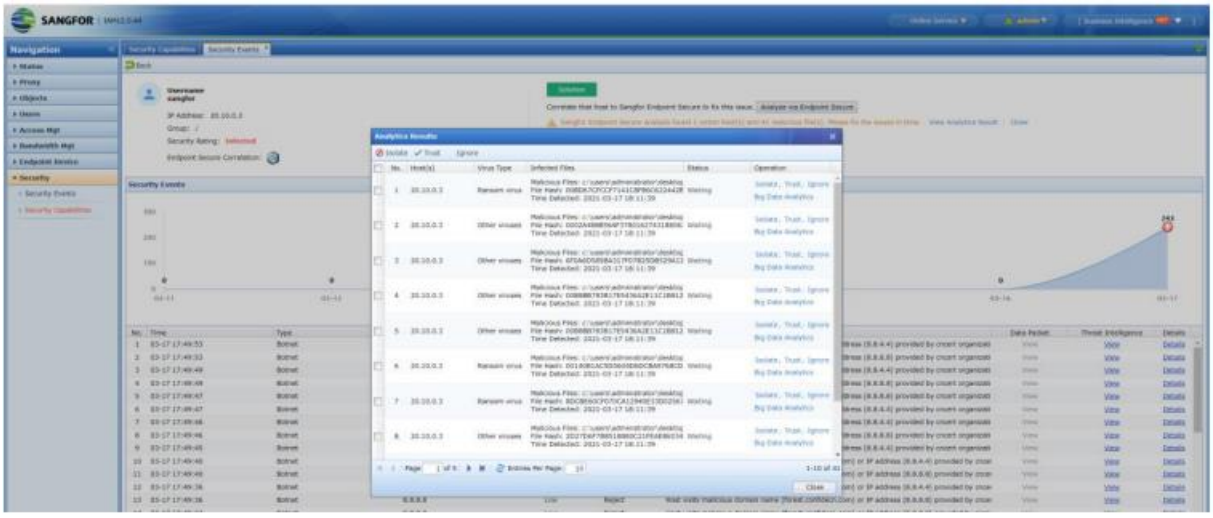
Bagaimana untuk Berkorelasi dengan IAM untuk Operasi Sederhana

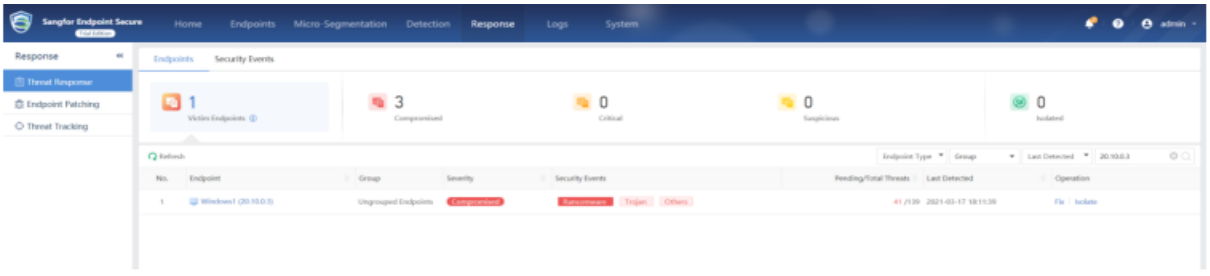


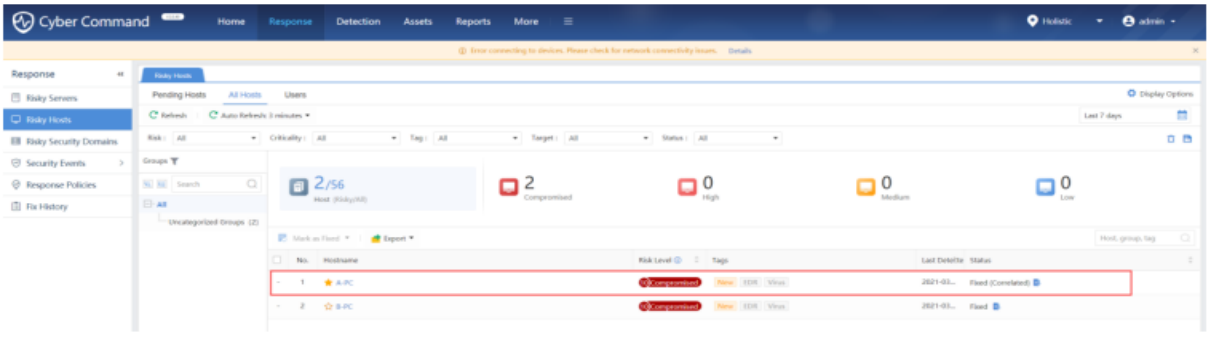
Kemudian, Anda dapat melihat scan task running di endpoint.

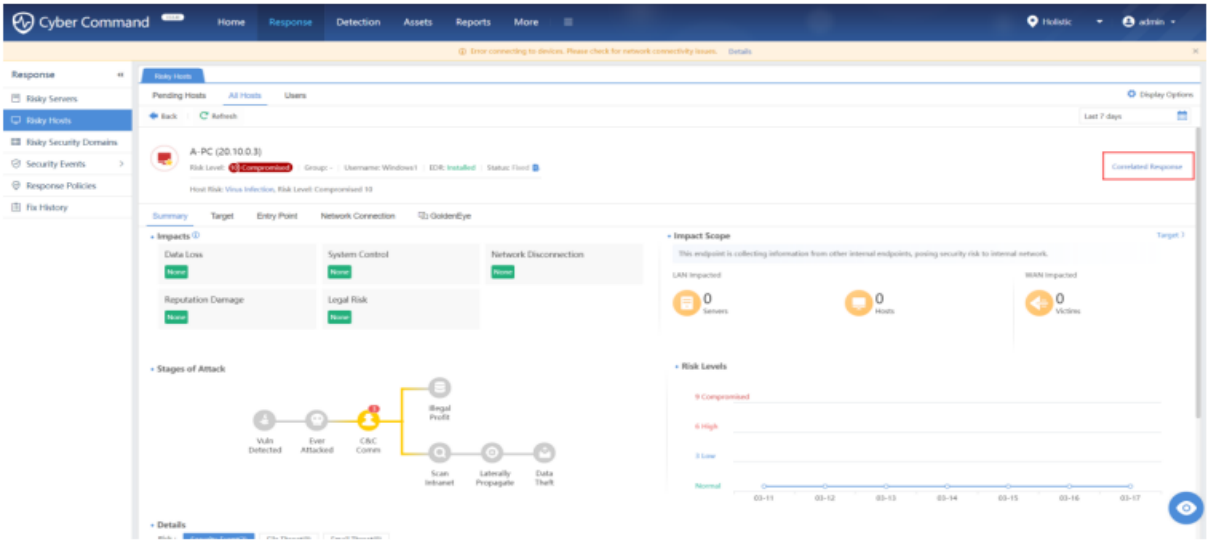


Bagaimana untuk Berkorelasi dengan IAM untuk Operasi Sederhana





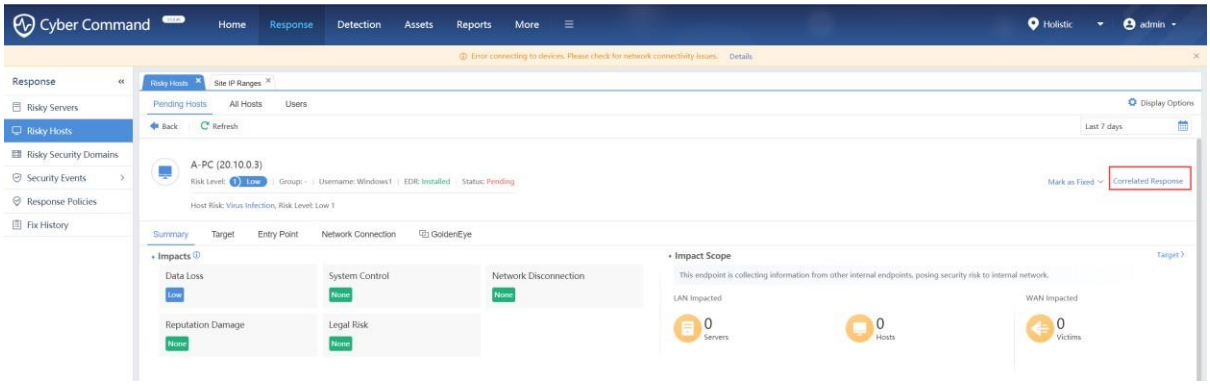




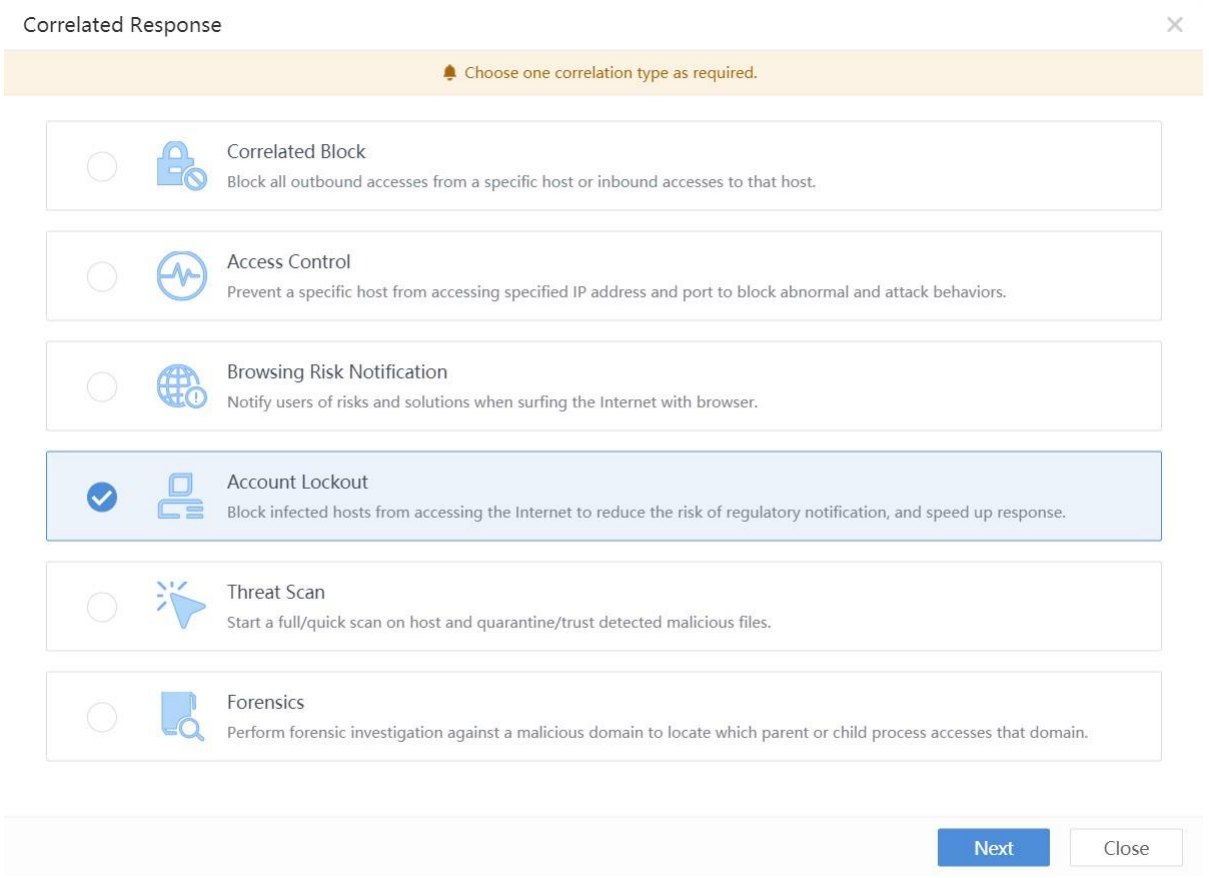
3.2 Response di Cyber Command

3.2.1 Lockout Account

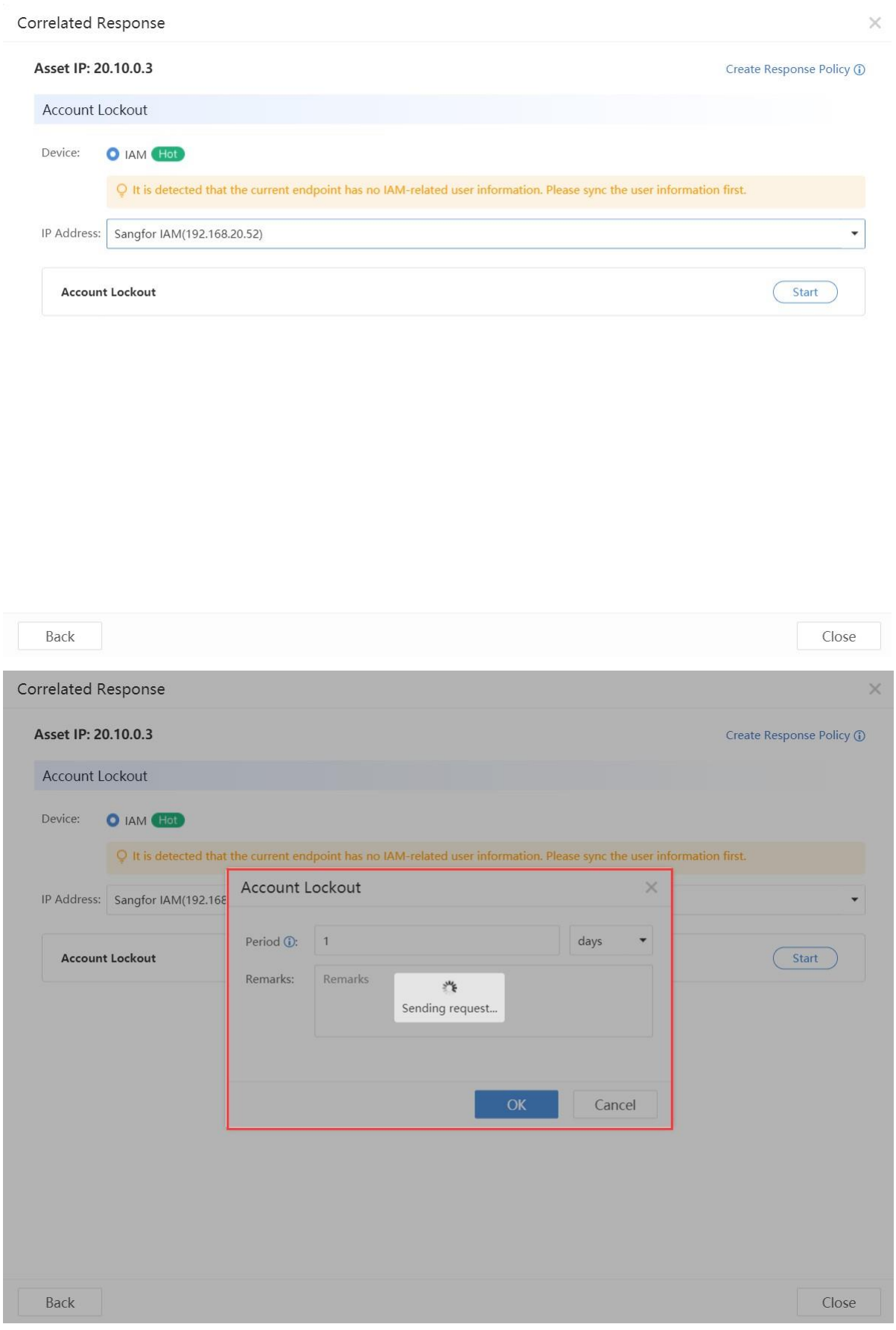
1. Jika Anda ingin memblokir host botnet, Anda dapat klik Correlated Response.



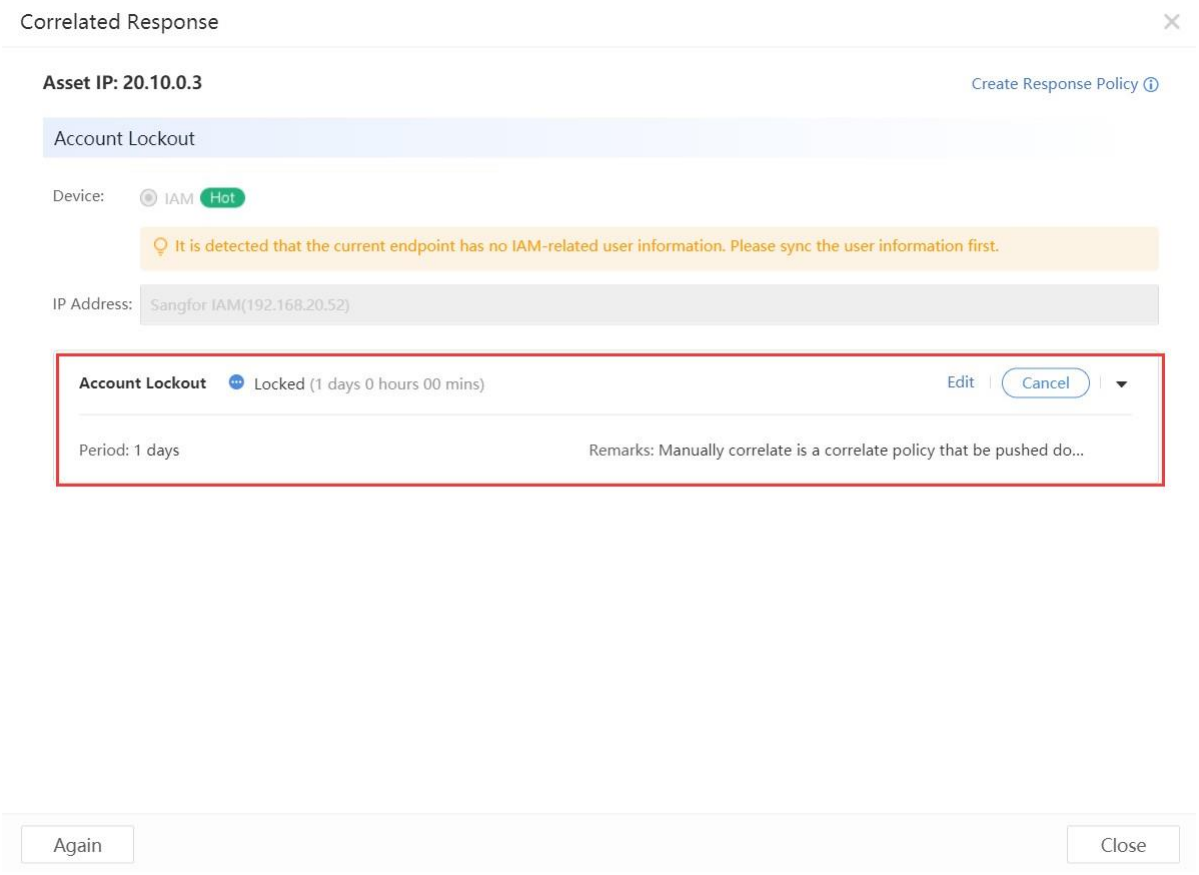
2. Pilih Account Lockout.



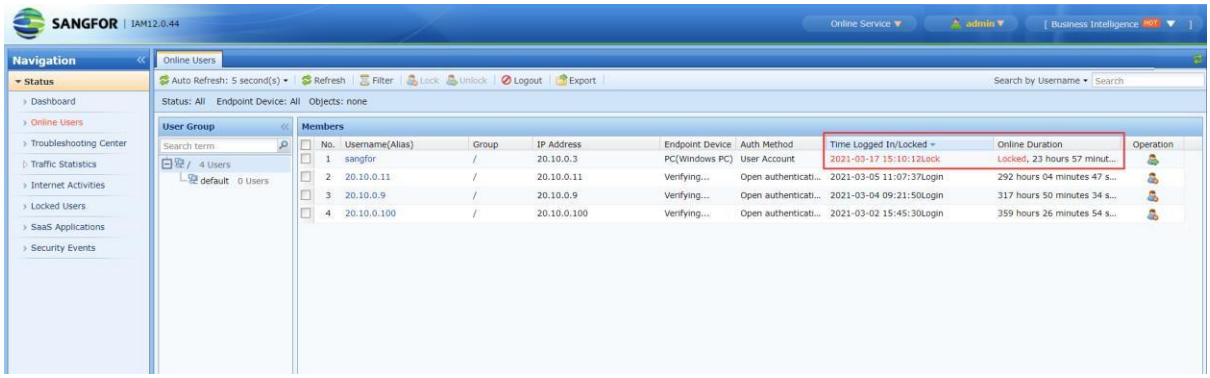
3. Pilih IAM terkait dan klik Start untuk mengatur waktu lockout .



4. Tunggu beberapa saat, Anda dapat melihat Cyber Command menunjukkan bahwa policy diterbitkan berhasil.

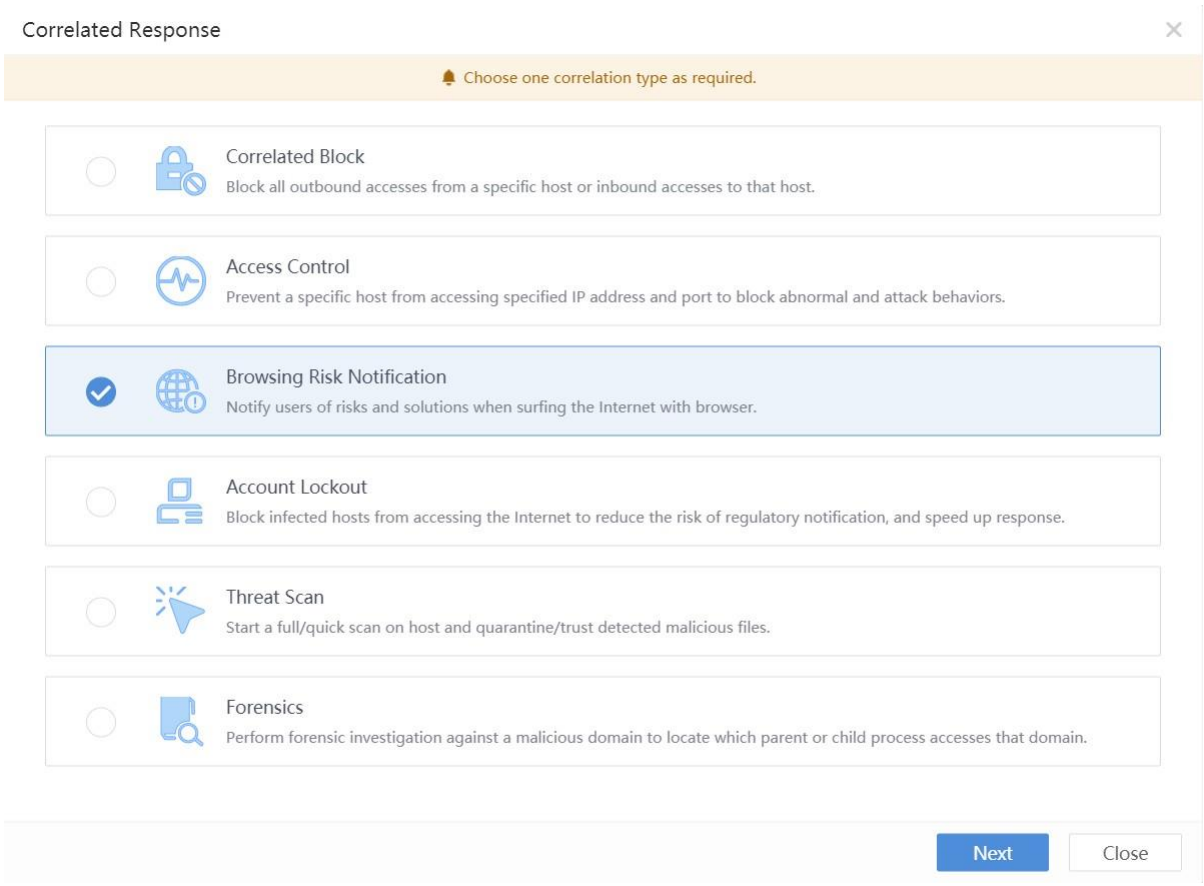


5. Log in IAM web console dan pergi ke Status-> Online Users path, Anda dapat melihat pengguna sudah di locked oleh IAM.

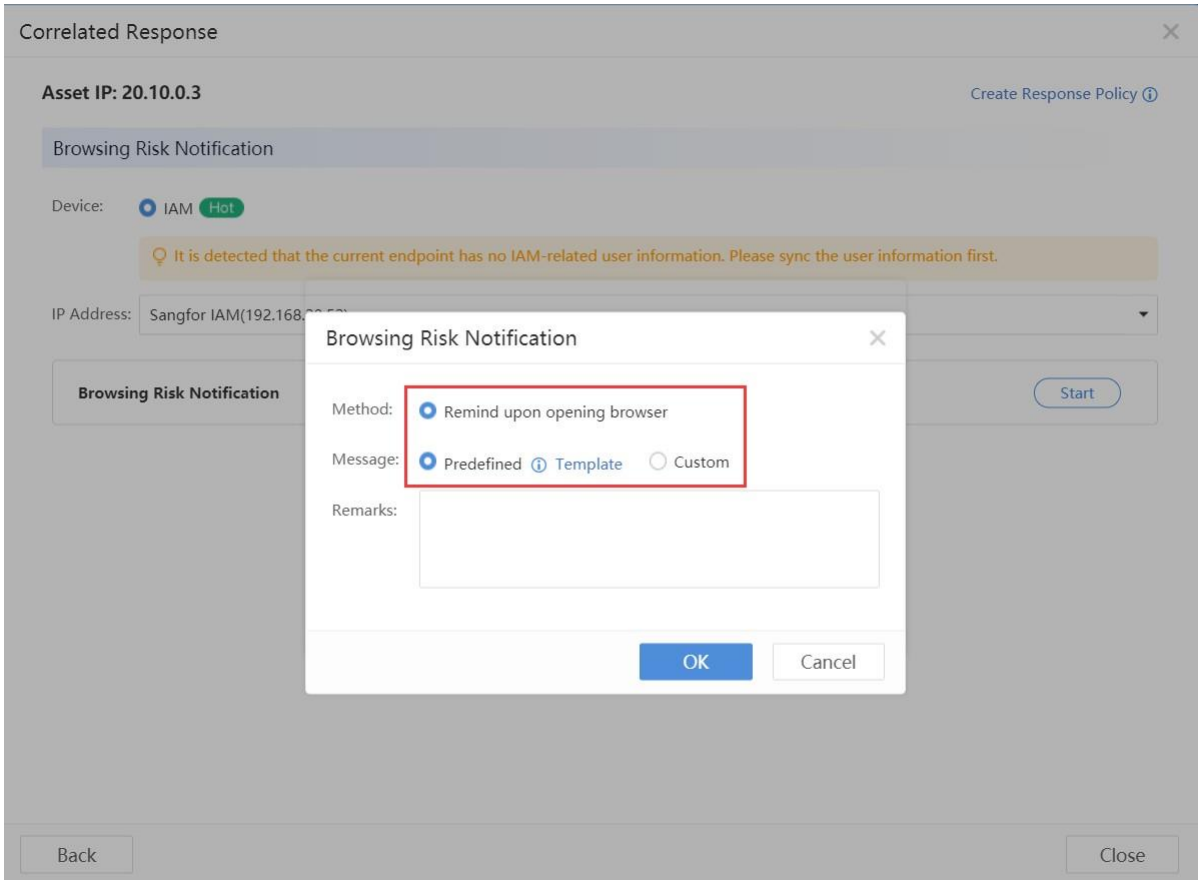


3.2.2 Browsing Risk Notification

1. Jika Anda hanya ingin memberitahu pengguna endpoint untuk mengetahui masalah security, Anda dapat klik Correlated Response.

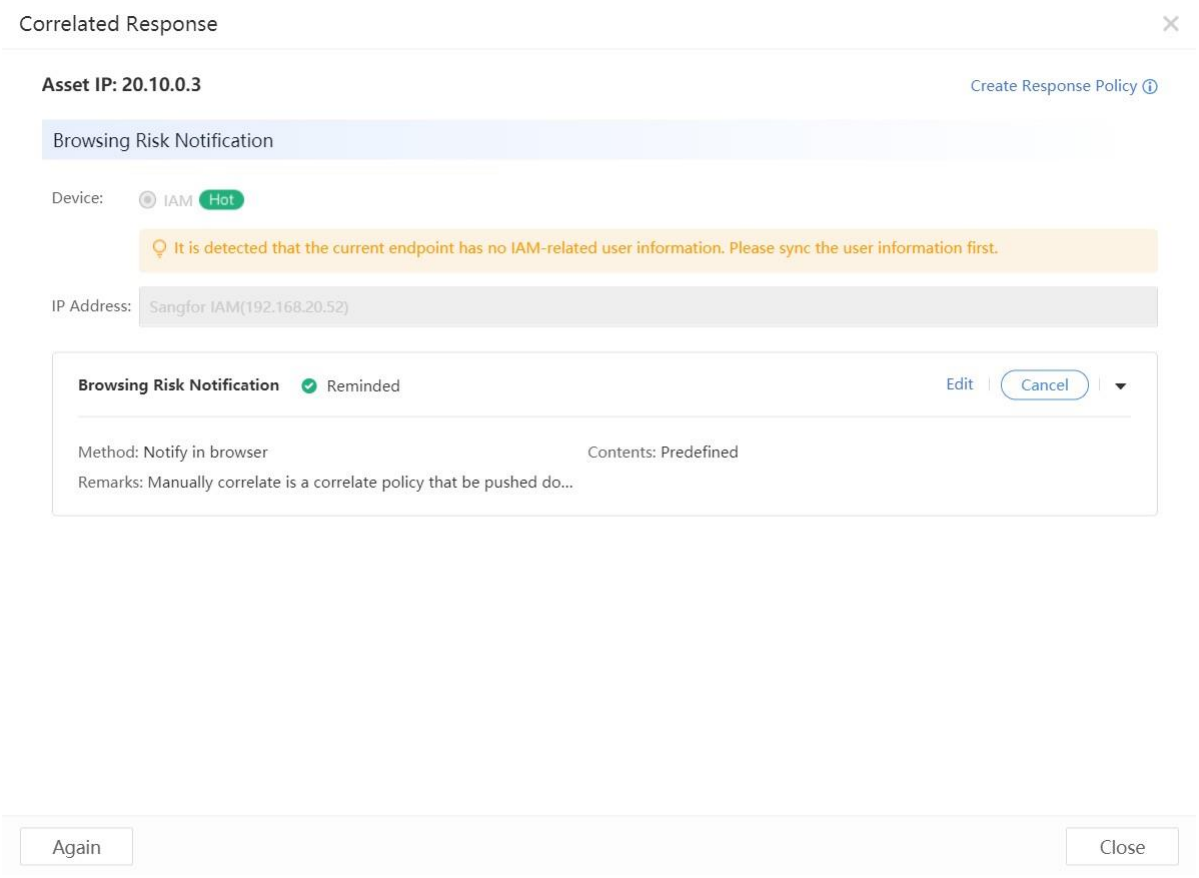


2. Pilih halaman predefined notification yang telah ditentukan atau Anda dapat kustom halaman sendiri .



3. Klik OK dan tunggu sebentar, Anda dapat melihat policy diterbitkan dengan sukses.

Bagaimana untuk Berkorelasi dengan IAM untuk Operasi Sederhana



4. Ketika pengguna endpoint mencoba mengakses internet, IAM akan mengarahkan halaman akses ke halaman notification.