SANGFOR

Endpoint Secure
Praktek Terbaik untuk Skenario_Correlate NGAF dan Endpoint Secure untuk Antivirus

Catatan Perubahan

Tanggal	Deskripsi Perubahan
20 Oktober 2020	Penerbitan Dokumen
17 Mei 2021	Pembaruan Dokumen

DAFTAR ISI

Bab 1 Persiapan Pengujian

Harap persiapkan hal-hal berikut sebelum pengujian:

1. Satu set software ES software (versi terbaru).

2. Satu Perangkat NGAF yang menjalankan versi terbaru NGAF (8.0.12 atau gunakan versi yang lebih tinggi jika versi terbaru tidak tersedia).

3. Perangkat NGAF dapat berkomunikasi dengan port 443 dari platform ES management.

4. Windows 7 (atau versi yang lebih tinggi) dengan ES agent, yang lalu lintas jaringannya akan melewati NGAF.

5. Sampel Virus, yang melekat pada appendix (lebih dari satu sampel yang disediakan; semua sampel perlu diuji). Unzipping password adalah **sangfor**.

Correlate NGAF and Endpoint Secure for Antivirus Samples(sangfor).zip

6. Karena sampel virus perlu diuji. Semua tes perlu dilakukan di area pengujian, untuk menghindari dampak pada jaringan internal pelanggan.

Bab 2 Masalah Pelanggan

1. Dapatkah virus ditemukan dan diisolasi dengan mengeluarkan virus-kill task pada host yang beresiko dibawah NGAF-ES correlation?

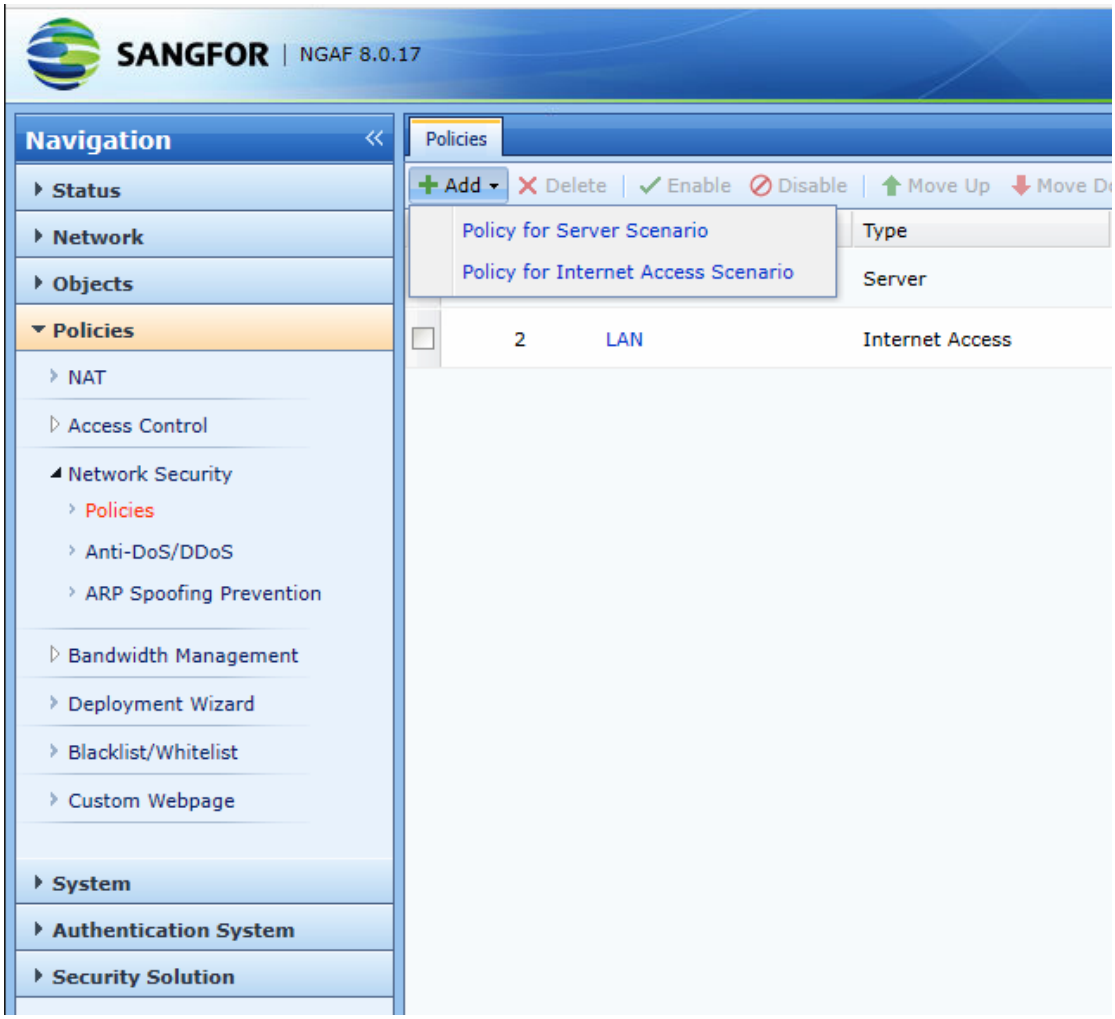
2. Dapatkah proses berbahaya dari risky host yang mengakses nama domain botnet berhasil dilaporkan dibawah NGAF-ES correlation?

Bab 3 Langkah-langkah Pengujian

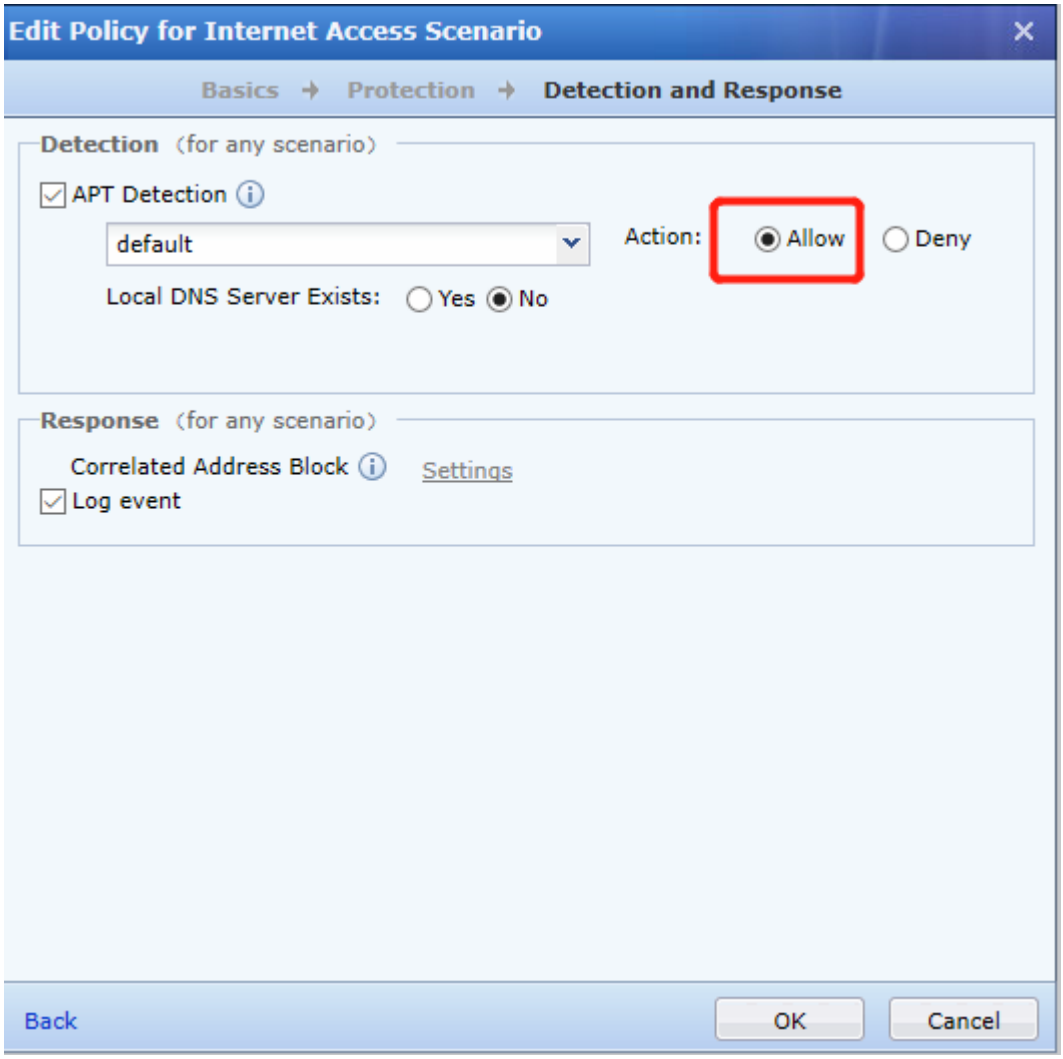
3.1 Konfigurasi NGAF

(1) Mengkonfigurasi NGAF security protection policy

Akses Sangfor NGAF dan pilih **Policies** -> **Network Security** -> **Policies**. Klik **Add** untuk menambahkan **Policy for Server Scenario** dan **Policy for Internet Access Scenario**, seperti tampilan di bawah ini:

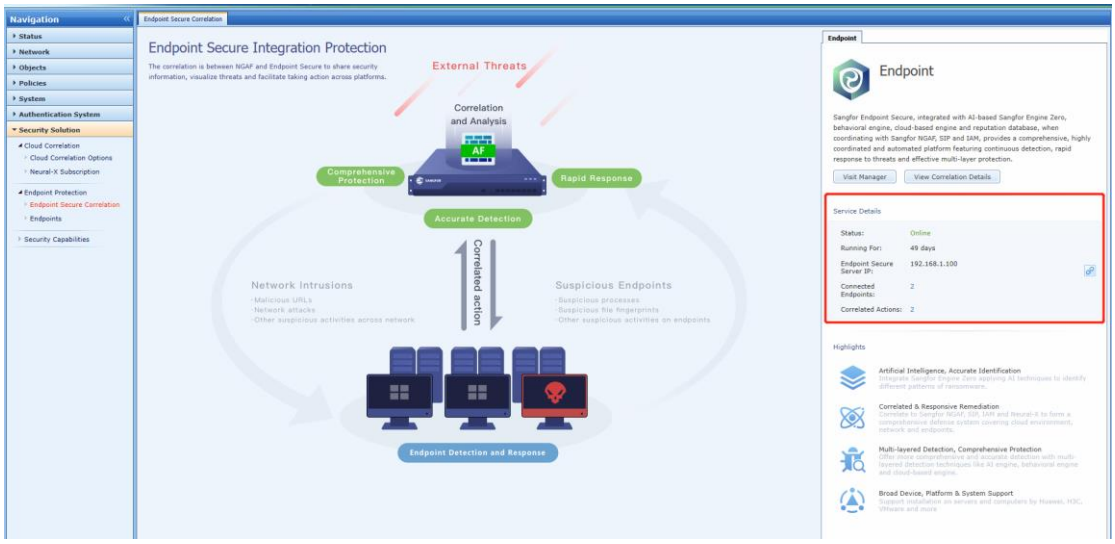


Aktifkan botnet detection untuk **Policy for Server Scenario** dan Policy **for Internet Access Scenario**. Plih **Allow** dan cek **Log event** seperti tampilan di bawah ini:

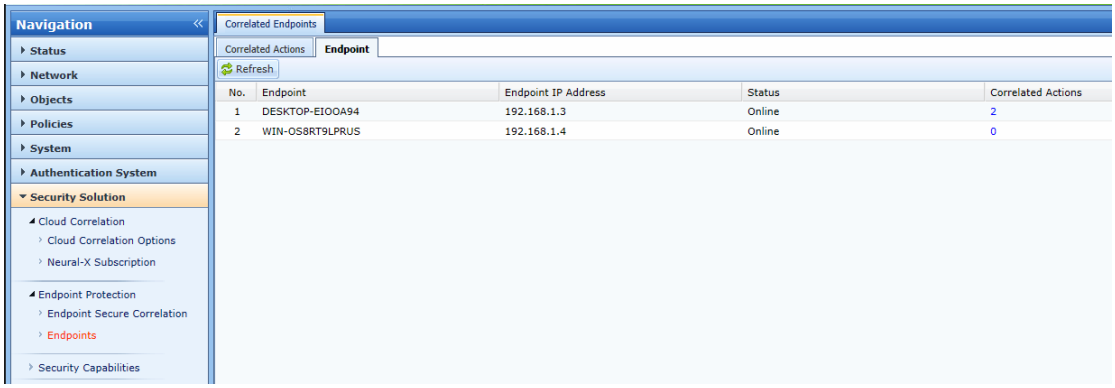


(2) Mengkonfigurasi NGAF-ES correlation

Untuk NGAF-ES correlation, Anda hanya perlu mengkonfigurasi NGAF. Akses NGAF dan pilih **Endpoint Secure Correlation** -> **Service Details**. Pilih ES pada sudut kanan atas, seperti tampilan di bawah ini:



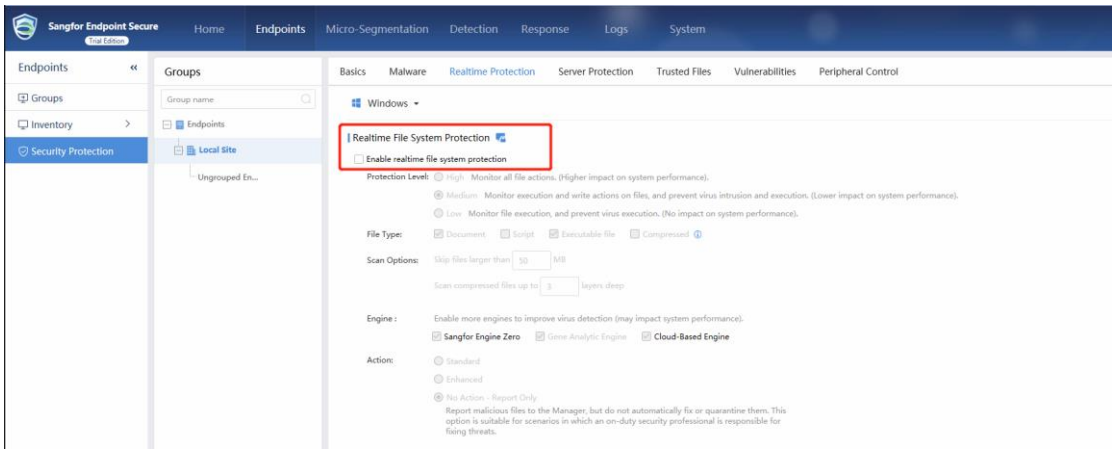
Setelah kolerasi berhasil, kamu dapat melihat online endpoints ES pada NGAF, seperti tampilan di bawah ini:

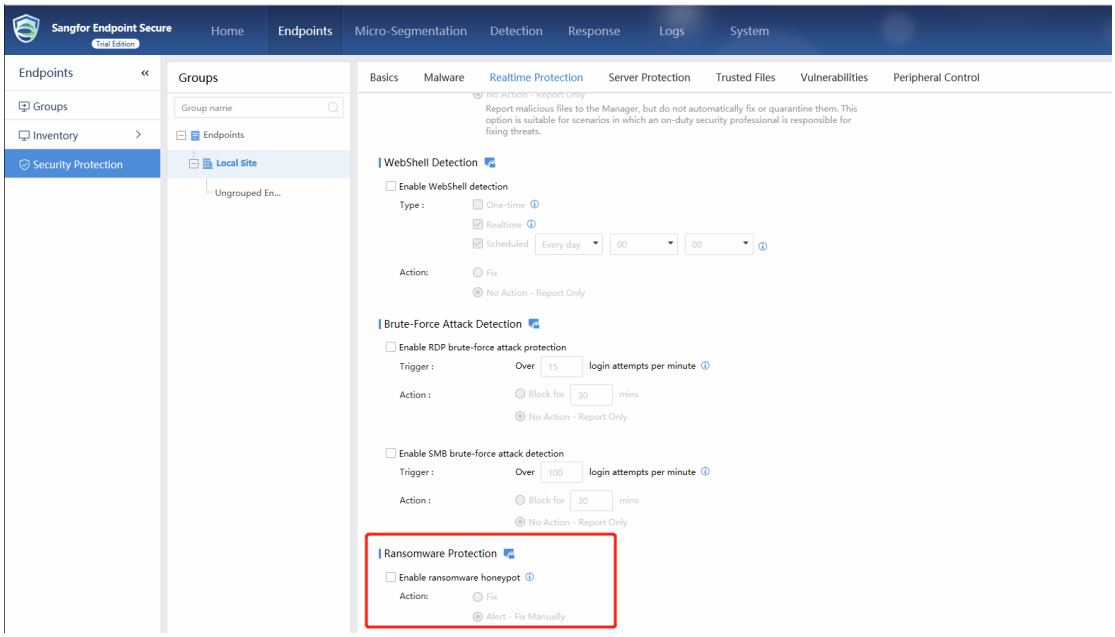


3.2 Konfigurasi ES

(1). Nonaktifkan Real-time File System Protection dan Ransomware Protection functions dari Endpoint Secure.

Real-time file system protection function perlu di nonaktifkan jika membersihkan sampel dan mempengaruhi hasil. klik **Endpoints** -> **Security Protection** dan mengkonfigurasi real-time protection policy dari kelompok dimana konfigurasi endpoint terletak seperti yang ditunjukkan di bawah ini. Nonaktifkan **Real-time File System Protection** dan fungsi **Ransomware Protection**.



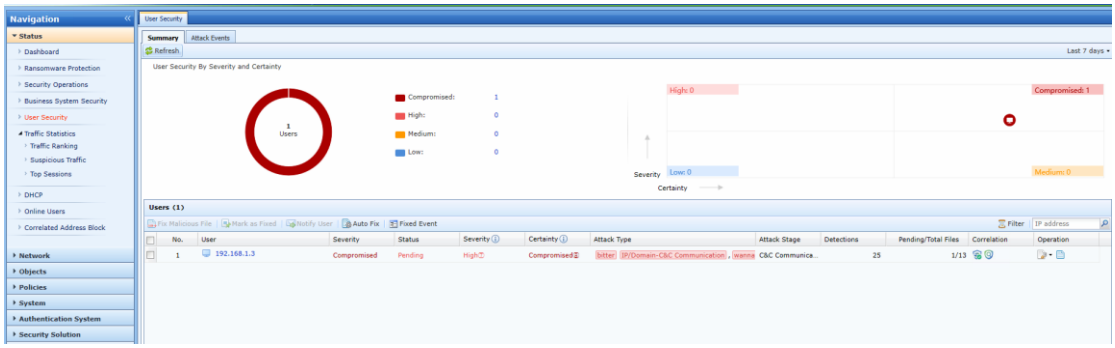


(2) Unzip sampel pengujian (unzipping password: **sangfor**) ke C:\Windows\System32\drivers\ pada perangkat pengujian.

(3) Ubah ekstensi sampel pengujian menjadi **.exe** dan jalankan file sampel (catatan: semua file sampel harus dijalankan).

Bab 4 Perkiraan Hasil

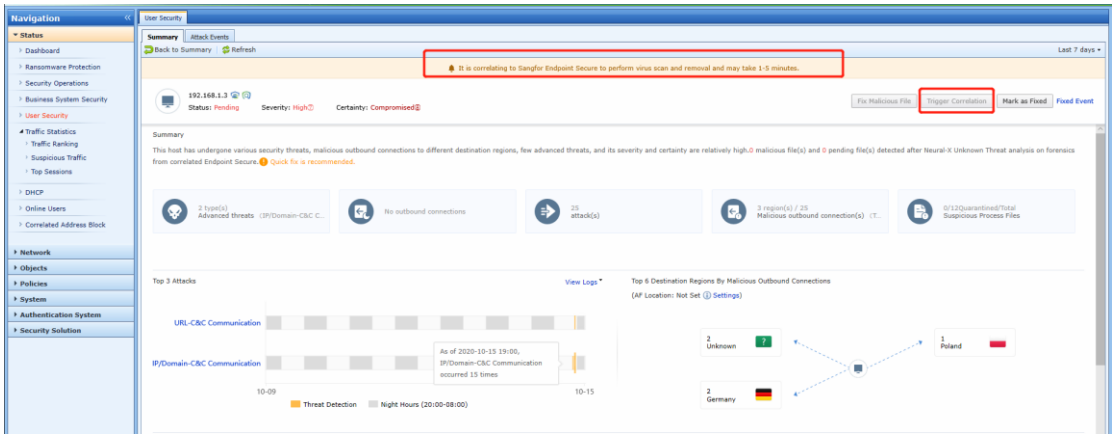
Setelah menjalankan sampel, tunggu setengah jam dan pilih **Status** -> **User Security**. Anda dapat melihat bahwa NGAF telah mengidentifikasi risky host yang menjalankan sampel, seperti tampilan di bawah ini. Klik username pada risky host. Anda dapat pergi ke correlated ES untuk membunuh dan melaporkan virus.



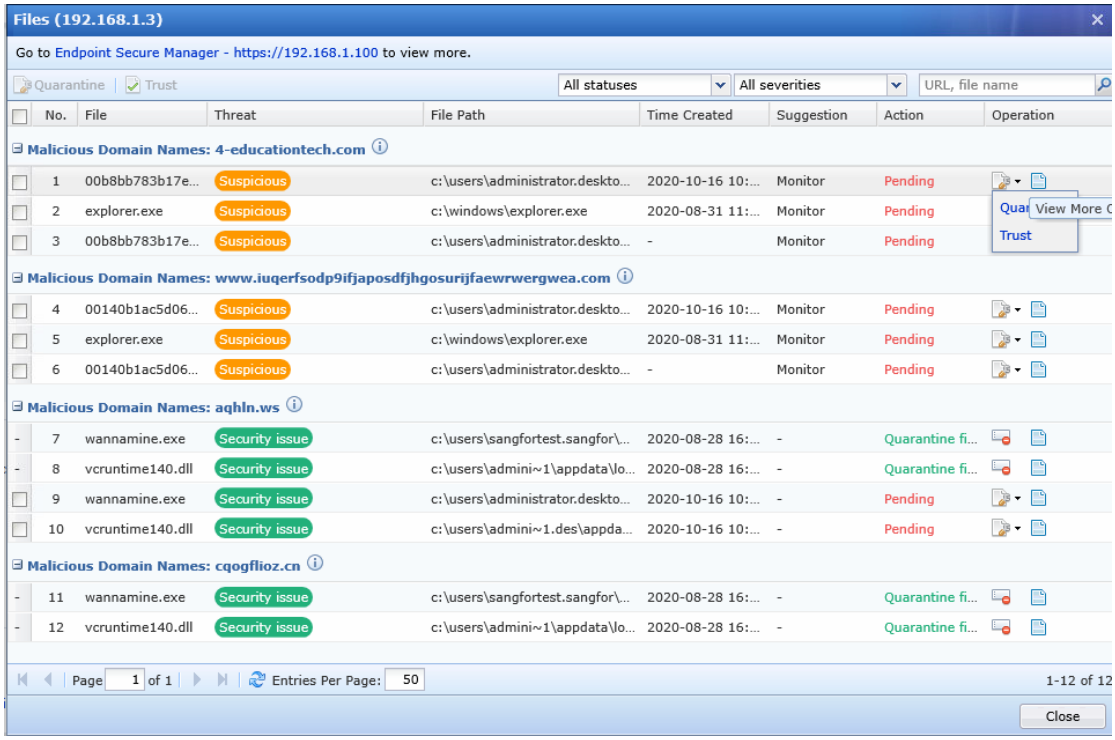
1. Correlated virus killing

Correlated virus killing dapat mengeluarkan virus-kill task terhadap risky users melalui NGAF untuk mengisolasi file ancaman dengan sukses.

Klik username dari risky host. Tampilan halaman ringkasan risiko pengguna, seperti tampilan di bawah ini, Klik **Trigger Correlation** Untuk mengeluarkan virus-kill task dalam korelasi dengan ES.



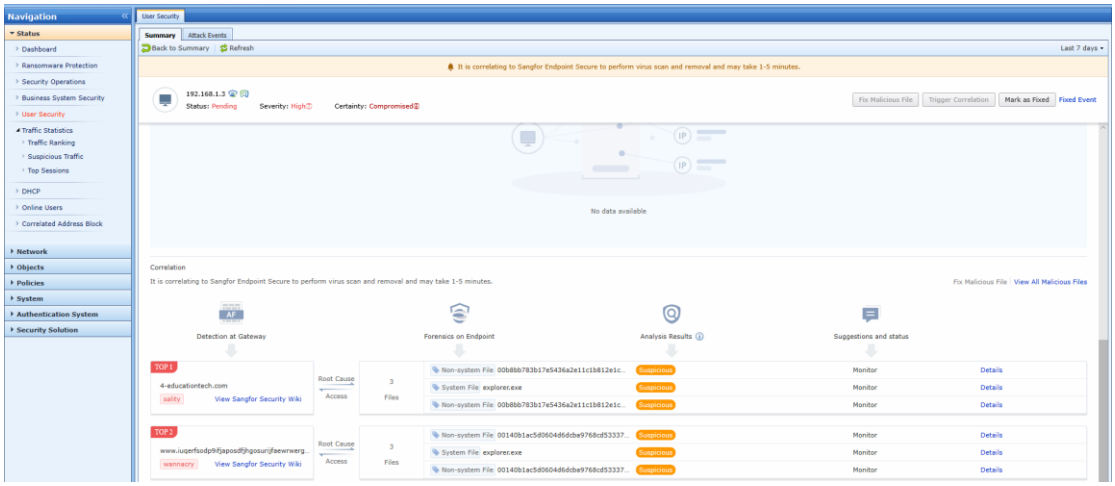
Setelah virus terbunuh, file berbahaya yang ditemukan akan ditampilkan. Klik **Quarantine** untuk mengisolasi atau mempercayai file-file tersebut, seperti tampilan di bawah ini:



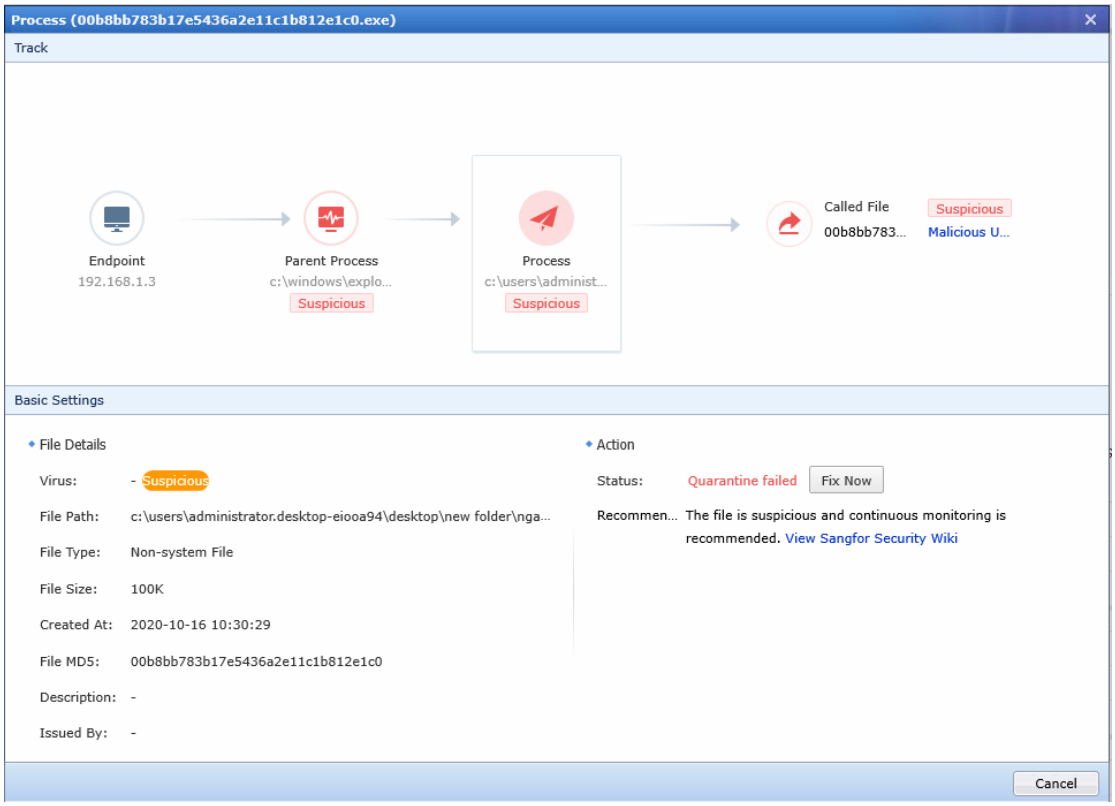
2. Pelaporan Correlated botnet

Untuk botnet yang ditemukan di NGAF, NGAF dapat berkorelasi dengan ES untuk melaporkan proses dan memproses file panggilan yang mengakses nama domain berbahaya, sehingga dapat membantu pelanggan menemukan file ancaman yang mengakses nama domain yang berbahaya.

Klik nama pengguna risky host. Tampilan halaman ringkasan risiko pengguna. Gulir ke bawah ke bawah, seperti tampilan di bawah ini. Halaman ini menunjukkan proses berbahaya yang mengakses nama domain botnet yang dilaporkan oleh NGAF dalam korelasi dengan ES.



Klik **Details and Operations** pada bagian kanan. Anda dapat mengisolasi proses berbahaya, seperti tampilan di bawah ini.



Bab 5 Pencegahan

1. NGAF tidak mendeteksi risky host. Alasan yang mungkin tercantum di bawah ini:

(1) Periksa apakah semua sampel virus dijalankan. Beberapa sampel virus disediakan, dan semua sampel ini harus dijalankan.

(2) Periksa apakah kebijakan keamanan dikonfigurasi pada NGAF, dan apakah deteksi botnet diaktifkan, tindakan diatur ke **Allow**, dan **Log event** diperiksa.

(3) Periksa apakah lalu lintas resolusi DNS dan lalu lintas jaringan dari PC yang diuji lulus NGAF. Lalu lintas jaringan PC yang diuji harus melewati NGAF.

2. Kegagalan untuk mendeteksi virus apa pun di bawah NGAF-ES correlation untuk virus-killing. Alasan yang mungkin tercantum di bawah ini:

(1) Verifikasi bahwa sampel virus berjalan di direktori quick killing. NGAF berkorelasi dengan ES untuk mengeluarkan virus-kill task dalam mode quick killing, bukan mode global killing. Mode quick killing hanya memindai **/windows** dan **/windows/system32**, begitu juga dengan **/windows/system32/drivers** dan sub-direktorinya.

3. Kegagalan untuk melaporkan proses botnet di bawah korelasi NGAF-ES. Alasan yang mungkin tercantum di bawah ini:

(1) Ini membutuhkan waktu untuk melihat hasilnya setelah sampel virus dijalankan. Anda disarankan untuk menunggu setengah jam dan memeriksa lagi. Laporan NGAF mendeteksi perilaku botnet ke ES secara berkala, bukan secara real-time.

(2) Periksa apakah security policy dikonfigurasi pada NGAF, dan apakah deteksi botnet diaktifkan, lakukan pengaturan ke **Allow** (tidak di-**Deny**), dan **Log event** diperiksa.