



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.....	1
Bab 2 Masalah Pelanggan	1
Bab 3 Langkah-langkah Pengujian	1
3.1 Konfigurasi NGAF	1
3.2 Konfigurasi ES	4
Bab 4 Perkiraan Hasil	5
Bab 5 Pencegahan	7

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

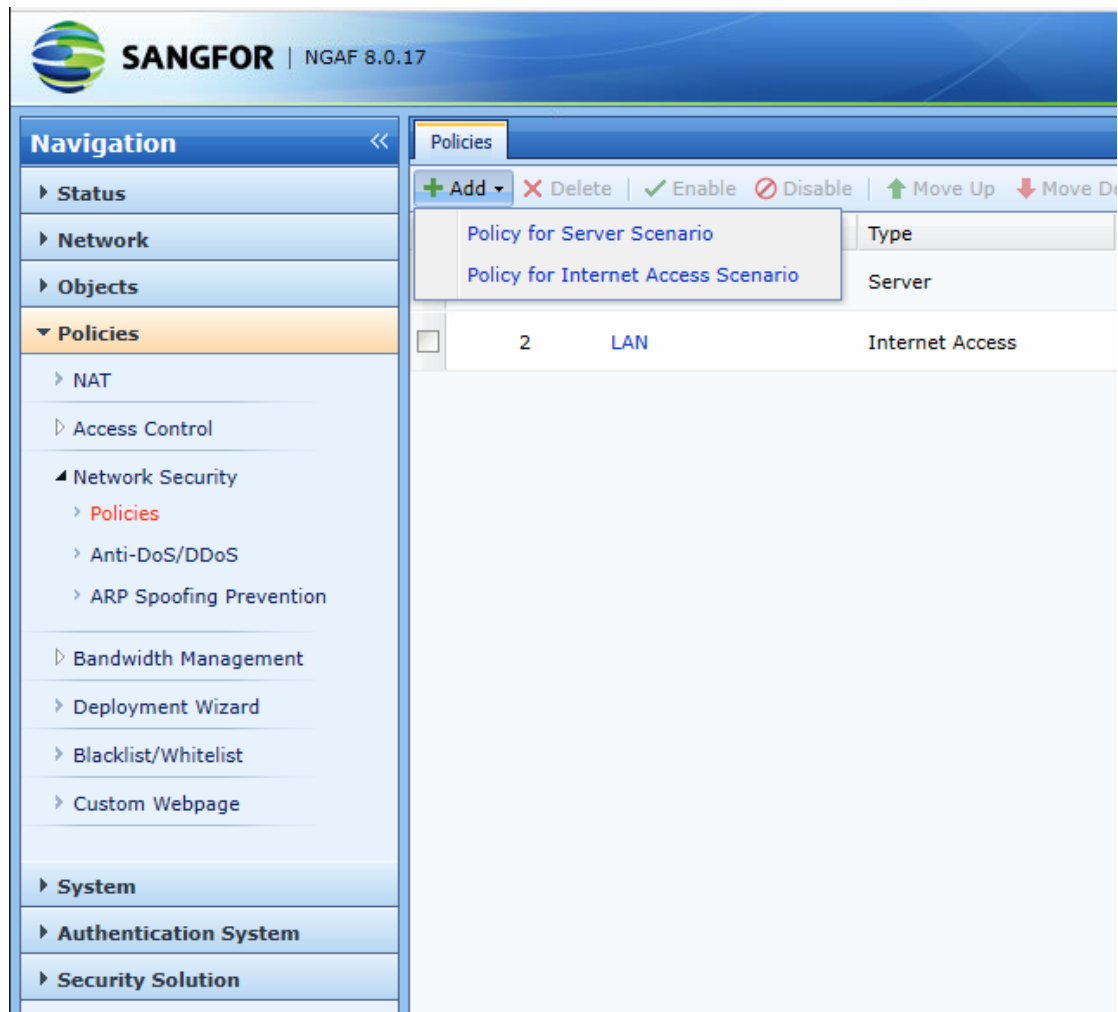
1. Dapatkah virus ditemukan dan diisolasi dengan mengeluarkan virus-kill task pada host yang beresiko dibawah NGAF-ES correlation?
2. Dapatkah proses berbahaya dari risky host yang mengakses nama domain botnet berhasil dilaporkan dibawah NGAF-ES correlation?

Bab 3 Langkah-langkah Pengujian

3.1 Konfigurasi NGAF

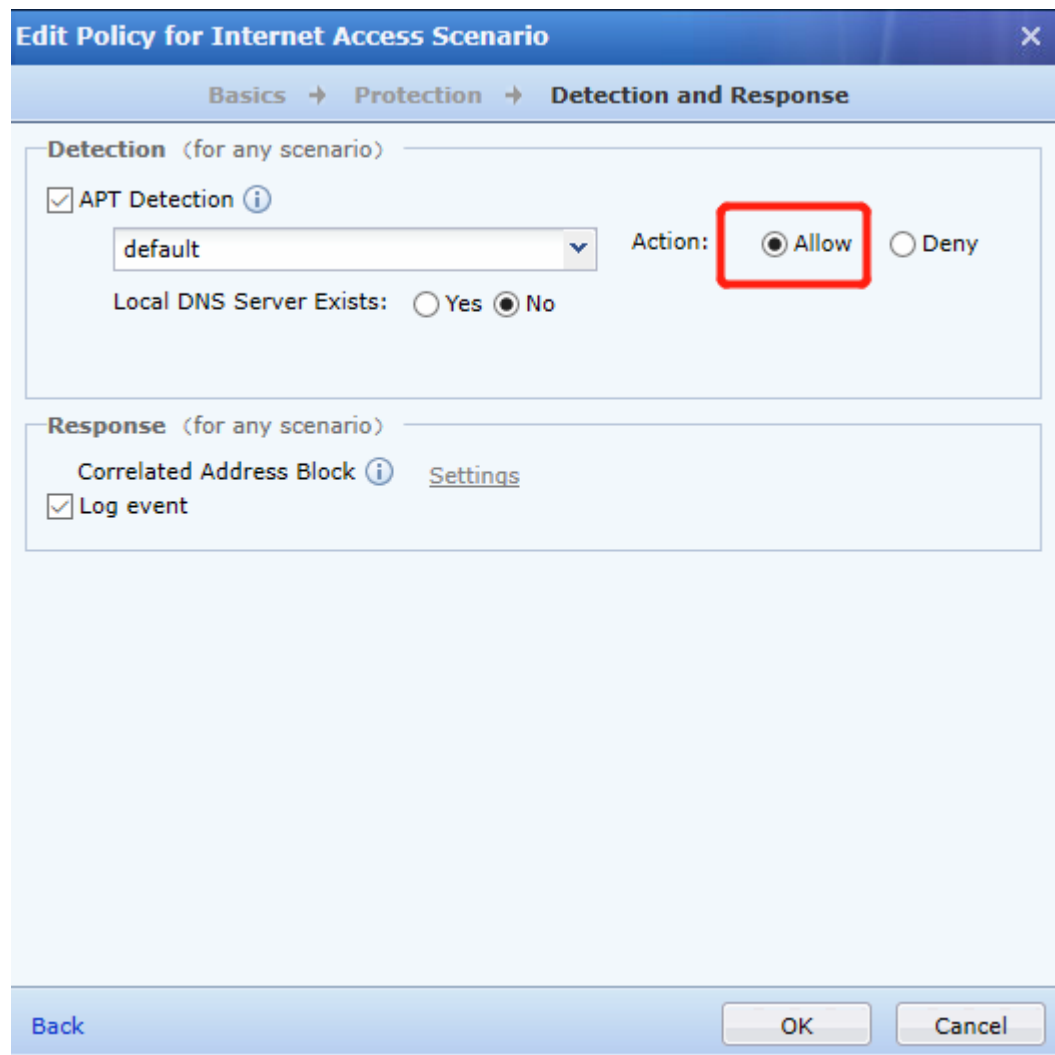
(1) Mengkonfigurasi NGAF security protection policy

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:



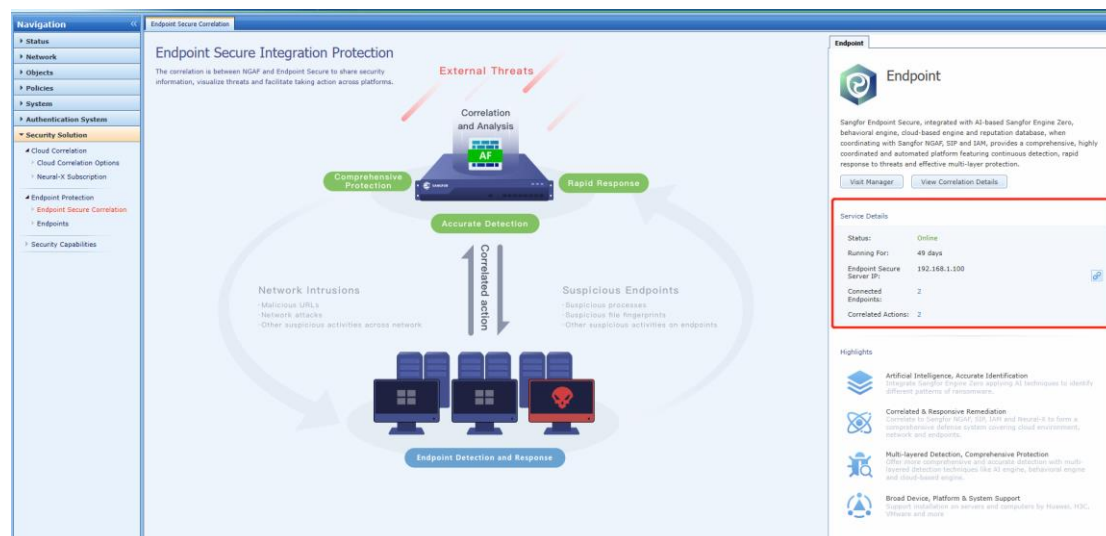
Aktifkan botnet detection untuk **Policy for Server Scenario** dan **Policy for Internet Access Scenario**. Pilih **Allow** dan cek **Log event** seperti tampilan di bawah ini:

Correlate NGAF dan Endpoint Secure untuk Antivirus



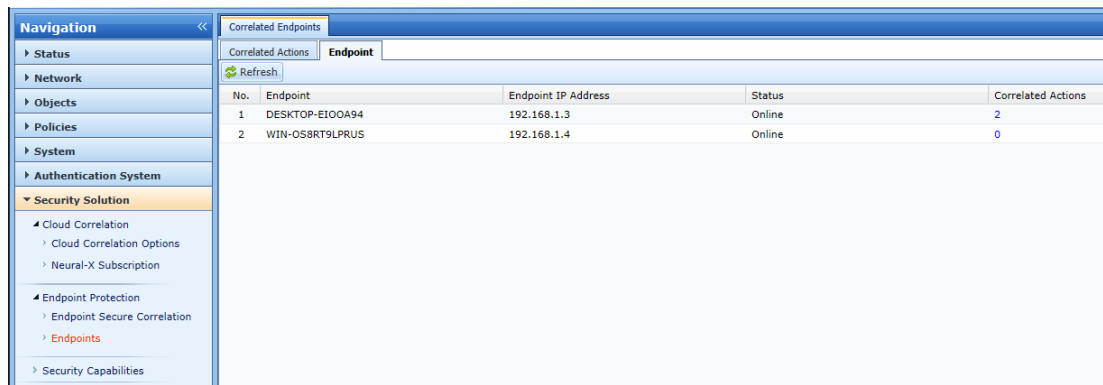
(2) Mengkonfigurasi NGAF-ES correlation

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:

Correlate NGAF dan Endpoint Secure untuk Antivirus



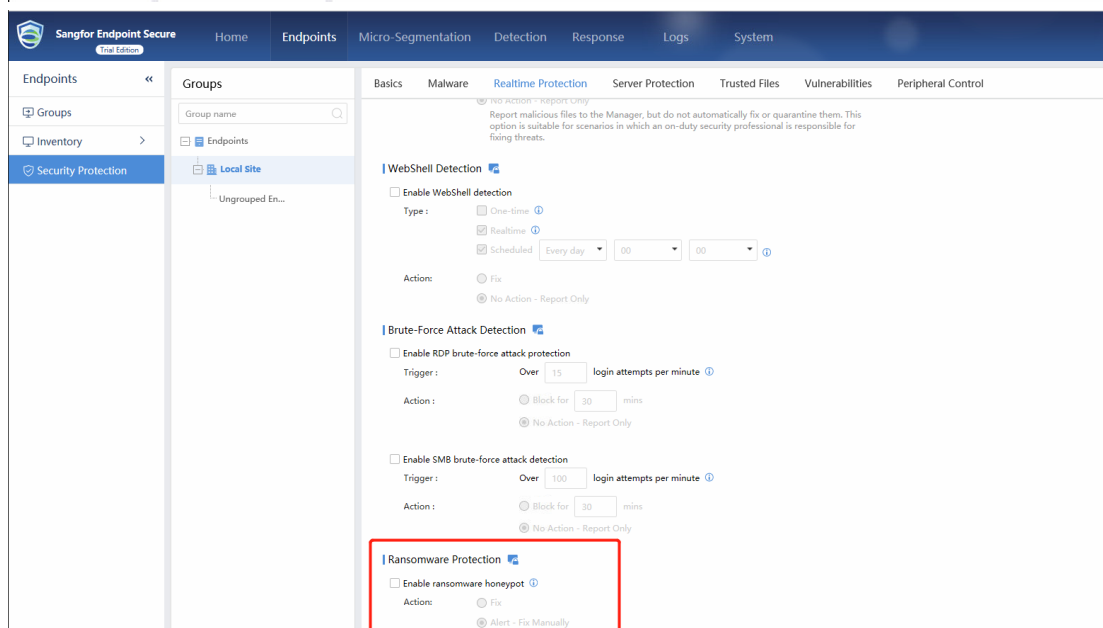
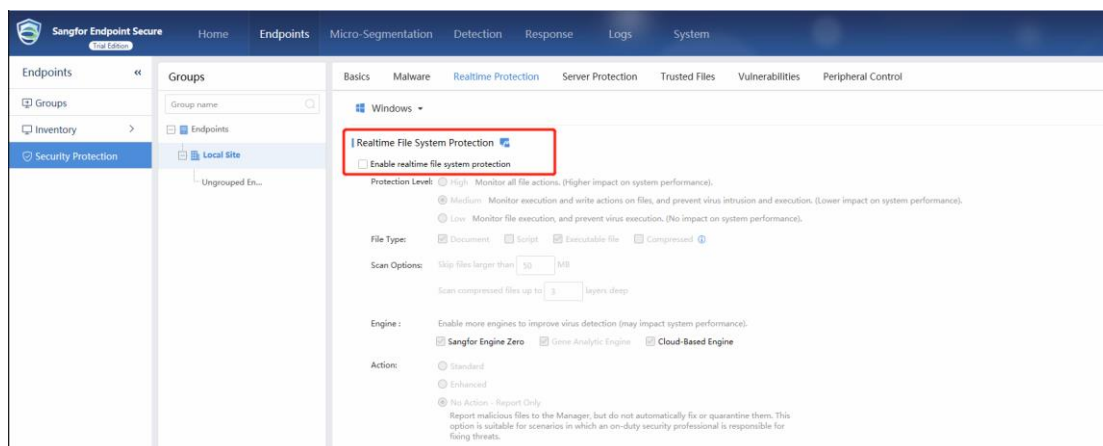
The screenshot shows the 'Correlated Endpoints' section of the Sangfor Endpoint Secure interface. On the left is a navigation menu with categories like Status, Network, Objects, Policies, System, Authentication System, and Security Solution. The 'Security Solution' category is expanded, showing sub-items like Cloud Correlation, Endpoint Protection, and Endpoints. The main area displays a table with the following data:

No.	Endpoint	Endpoint IP Address	Status	Correlated Actions
1	DESKTOP-EIOOA94	192.168.1.3	Online	2
2	WIN-OS8RT9LPRUS	192.168.1.4	Online	0

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**.



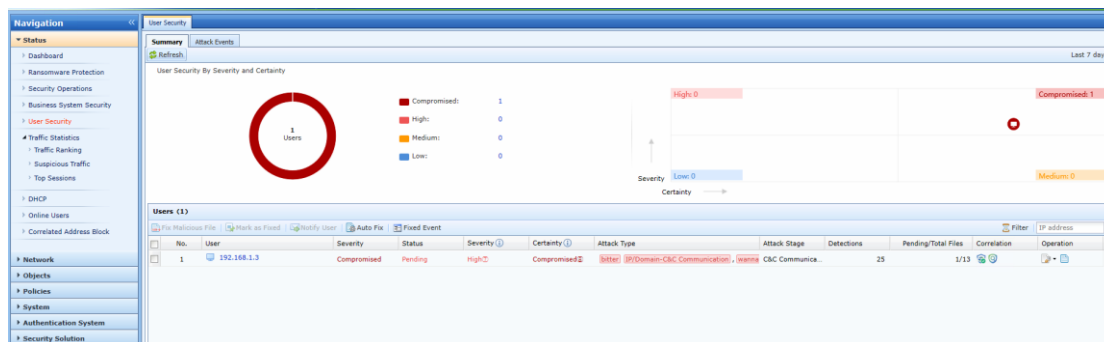
Correlate NGAF dan Endpoint Secure untuk Antivirus

(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

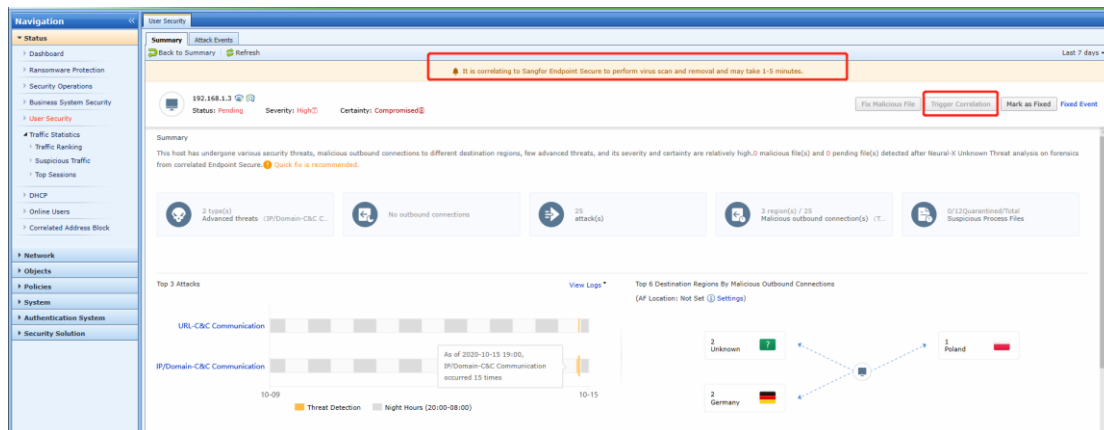
Setelah menjalankan sampel, tunggu setengah jam dan pilih **Status -> User Security**. Anda dapat melihat bahwa NGAF telah mengidentifikasi risky host yang menjalankan sampel, seperti tampilan di bawah ini. Klik username pada risky host. Anda dapat pergi ke correlated ES untuk membunuh dan melaporkan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



1. Correlated virus killing

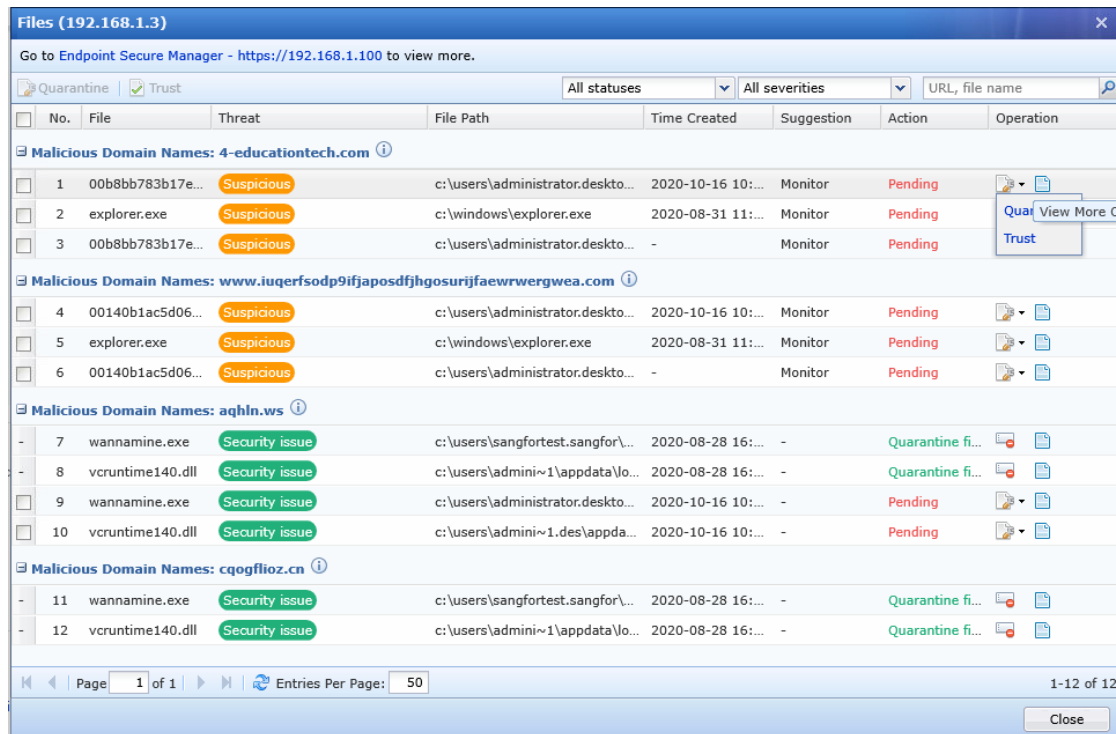
Correlated virus killing dapat mengeluarkan virus-kill task terhadap risky users melalui NGAF untuk mengisolasi file ancaman dengan sukses.

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:

Correlate NGAF dan Endpoint Secure untuk Antivirus



Files (192.168.1.3)

Go to Endpoint Secure Manager - <https://192.168.1.100> to view more.

Quarantine | Trust

All statuses | All severities | URL, file name

No.	File	Threat	File Path	Time Created	Suggestion	Action	Operation
Malicious Domain Names: 4-educationtech.com							
1	00b8bb783b17e...	Suspicious	c:\users\administrator.deskto...	2020-10-16 10:...	Monitor	Pending	Quarantine Trust
2	explorer.exe	Suspicious	c:\windows\explorer.exe	2020-08-31 11:...	Monitor	Pending	Quarantine Trust
3	00b8bb783b17e...	Suspicious	c:\users\administrator.deskto...	-	Monitor	Pending	Quarantine Trust
Malicious Domain Names: www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com							
4	00140b1ac5d06...	Suspicious	c:\users\administrator.deskto...	2020-10-16 10:...	Monitor	Pending	Quarantine Trust
5	explorer.exe	Suspicious	c:\windows\explorer.exe	2020-08-31 11:...	Monitor	Pending	Quarantine Trust
6	00140b1ac5d06...	Suspicious	c:\users\administrator.deskto...	-	Monitor	Pending	Quarantine Trust
Malicious Domain Names: aqhln.ws							
7	wannamine.exe	Security issue	c:\users\sangfortest.sangfor\...	2020-08-28 16:...	-	Quarantine fi...	Quarantine Trust
8	vcruntime140.dll	Security issue	c:\users\admini~1\appdata\lo...	2020-08-28 16:...	-	Quarantine fi...	Quarantine Trust
9	wannamine.exe	Security issue	c:\users\administrator.deskto...	2020-10-16 10:...	-	Pending	Quarantine Trust
10	vcruntime140.dll	Security issue	c:\users\admini~1.des\appda...	2020-10-16 10:...	-	Pending	Quarantine Trust
Malicious Domain Names: cqogfioz.cn							
11	wannamine.exe	Security issue	c:\users\sangfortest.sangfor\...	2020-08-28 16:...	-	Quarantine fi...	Quarantine Trust
12	vcruntime140.dll	Security issue	c:\users\admini~1\appdata\lo...	2020-08-28 16:...	-	Quarantine fi...	Quarantine Trust

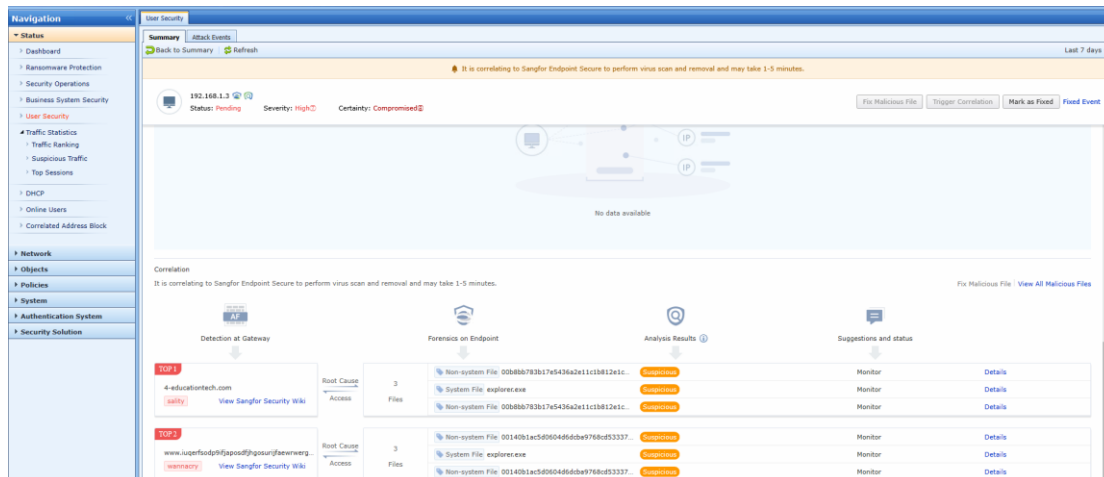
Page 1 of 1 | Entries Per Page: 50 | 1-12 of 12

Close

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.



Navigation

- Dashboard
- Ransomware Protection
- Security Operations
- Business System Security
- User Security
 - Traffic Statistics
 - Traffic Ranking
 - Suspicious Traffic
 - Top Sessions
- DHCP
- Online Users
- Correlated Address Block
- Network
- Objects
- Policies
- System
- Authentication System
- Security Solution

Summary | Attack Events

Back to Summary | Refresh

It is correlating to Sangfor Endpoint Secure to perform virus scan and removal and may take 1-5 minutes.

192.168.1.3 | Status: Pending | Severity: High | Certainty: Compromised

Fix Malicious File | Trigger Correlation | Mark as Fixed | Fixed Event

No data available

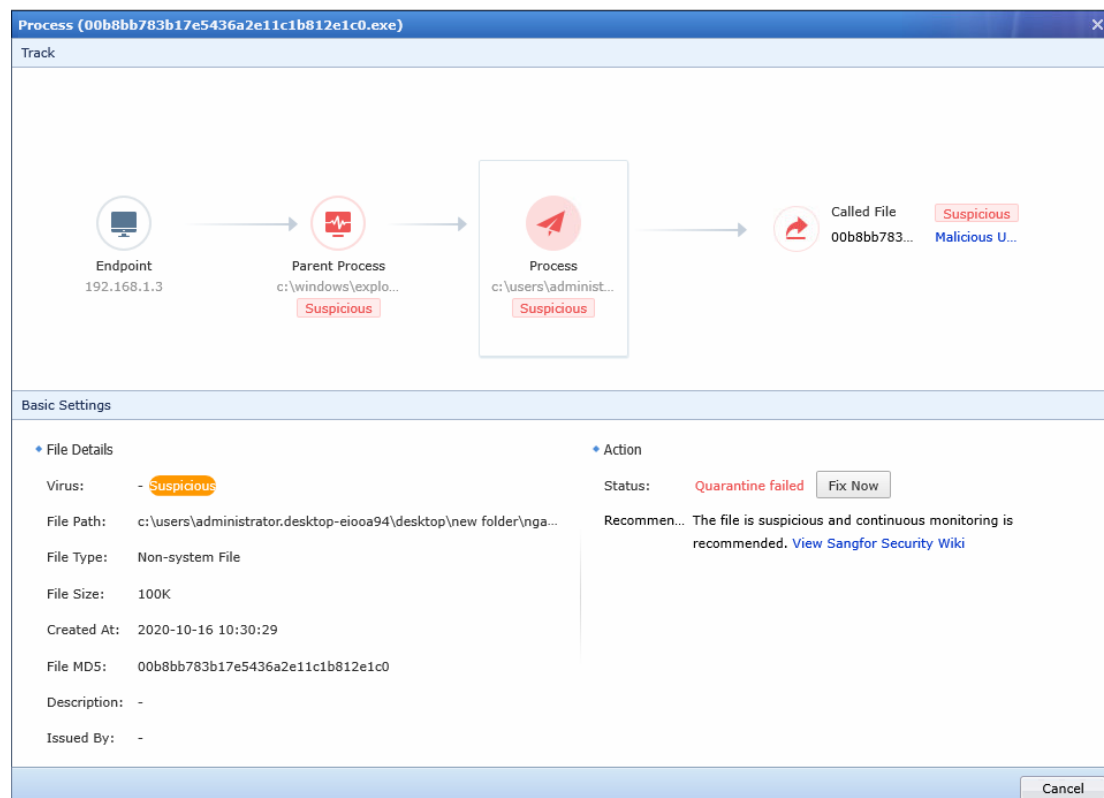
Correlation

It is correlating to Sangfor Endpoint Secure to perform virus scan and removal and may take 1-5 minutes.

Fix Malicious File | View All Malicious Files

Detection at Gateway	Forensics on Endpoint	Analysis Results	Suggestions and status
TOP 1 4-educationtech.com Root Cause Access View Sangfor Security Wiki	3 Files Non-system File: 00b8bb783b17e5436a2e11c0812e1c System File: explorer.exe Non-system File: 00b8bb783b17e5436a2e11c0812e1c	3 Compromised Compromised Compromised	Monitor Monitor Monitor Details
TOP 2 www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com Root Cause Access View Sangfor Security Wiki	3 Files Non-system File: 00140b1ac5d06486dbef76bd53337 System File: explorer.exe Non-system File: 00140b1ac5d06486dbef76bd53337	3 Compromised Compromised Compromised	Monitor Monitor Monitor Details

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-direktornya.

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.



SANGFOR

Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc