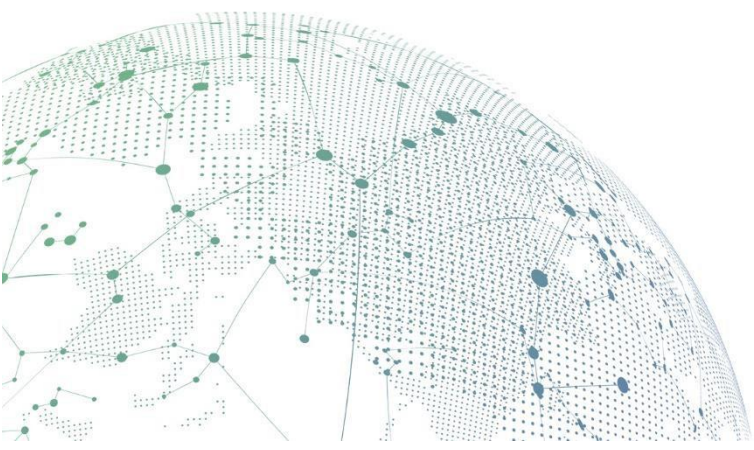




# Cyber Command

**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

Bab 1 Skenario .....	1
1.1 Skenario.....	1
1.2 Lingkungan .....	1
1.2.1 Lingkungan Network.....	1
1.2.2 Contoh Virus .....	2
1.3 Tindakan Pencegahan.....	2
Bab 2 Konfigurasi .....	7
2.1 Konfigurasi Cyber Command .....	7
Bab 3 Korelasi .....	9
3.1 Generate Security Logs dan Sinkronisasi ke Cyber Command .....	9

Bagaimana untuk Berkorelasi dengan Endpoint Secure dengan Operasi Sederhana

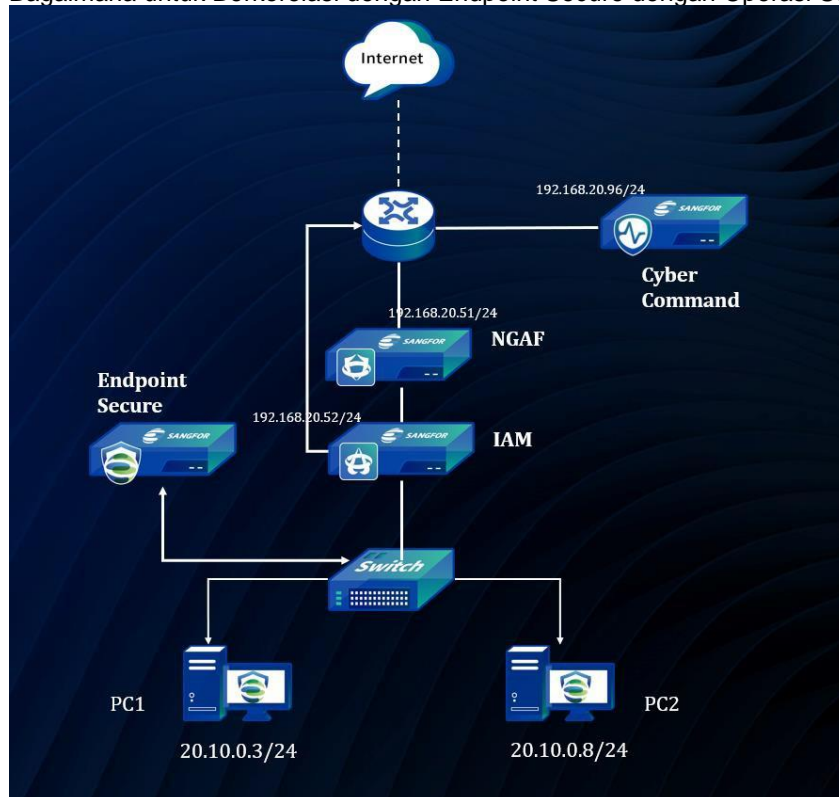
# Bab 1 Skenario

## 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.

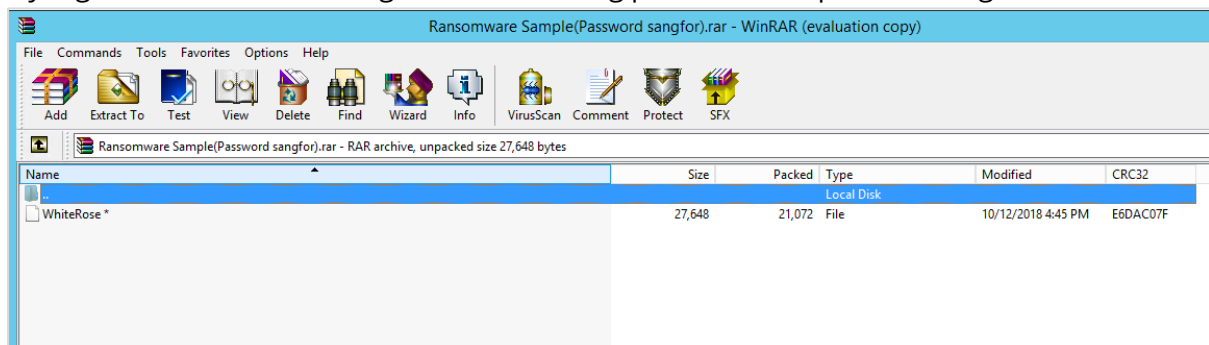
## 1.2 Lingkungan

### 1.2.1 Lingkungan Network



## 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

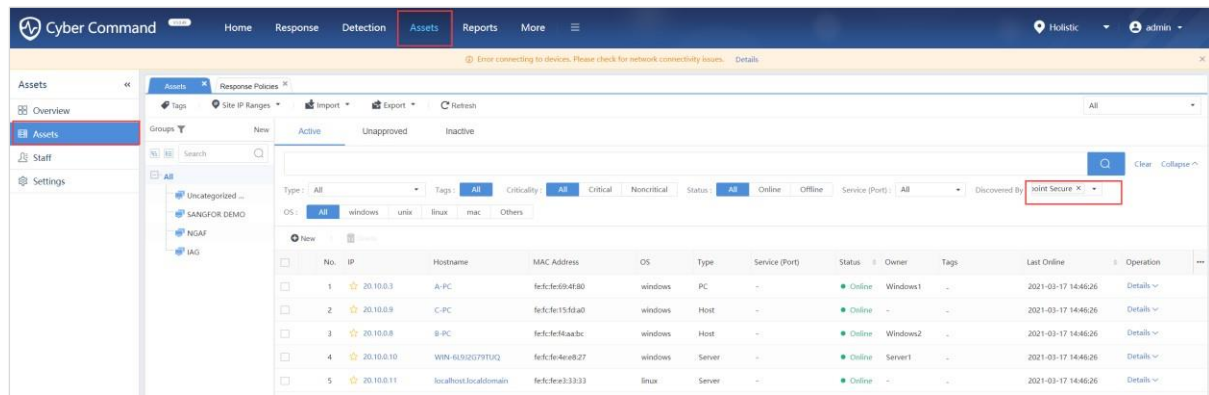


real-time monitoring pada ES, virus dapat terdeteksi setelah file tersebut di-decompressed.

## 1.3 Tindakan Pencegahan

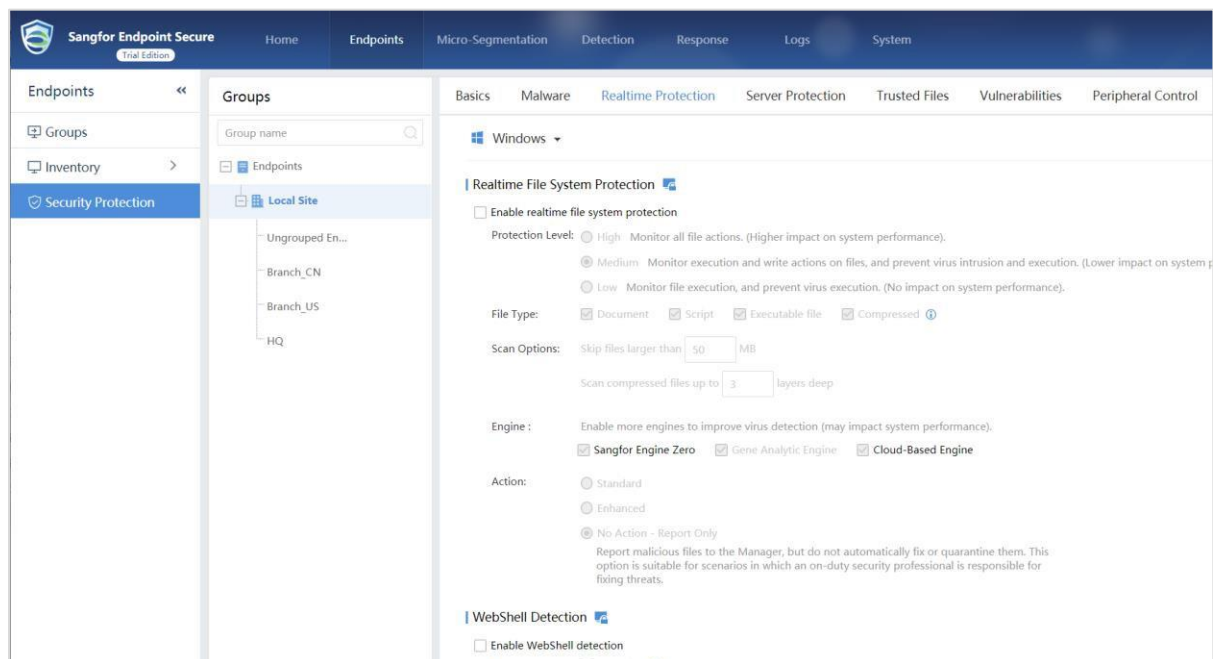
1. Harap pastikan bahwa Endpoint Secure tersinkronisasi semua asset ke CyberCommand.

## 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

The screenshot shows the 'Holistic' dashboard interface. At the top right, there is a user profile 'admin' and a dropdown menu with options: Threat Intelligence, Help, System, Service Packs, and Exit. The main content area displays two status cards: 'NGAF' with 'Online: 0' and 'Offline: 0', and 'BBC' with 'Online: 0' and 'Offline: 0'. Below these, a table shows 'Today's Synced Logs' for NGAF as 0 and for BBC as 'N/A (sync not supported)'. A search bar is located above a table with columns: Synced Logs, Today's Logs, Last Synced, Status, Alerts (30 days), and Operation. The table contains one row with values: -, -, 2021-03-16 16:11:18, ● Nor..., 0, and -.

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

The screenshot shows the 'Cyber Command' interface. The left sidebar has a 'System' menu with 'Correlated Devices' highlighted. The main content area is titled 'Correlated Devices' and shows a 'Refresh' button. Below this, it displays 'Total Logs (today): 204' and '3 Sangfor devices licensed, 7 licenses remaining (not count in STA, file reputation & threat analytics system)'. Three status cards are shown: 'Endpoint Secure' (Online: 1, Offline: 0), 'NGAF' (Online: 1, Offline: 0), and 'IAM' (Connected: 1, Offline: 0). A table at the bottom lists correlated devices with columns: No., Name (IP Address), Type, IP Address, Version, Licensed, Sync Mode, and Today's Synced Logs. The table contains two rows: 1. 'af (192.168.20.51)' with type 'Next Gener...', IP '192.168.20.51', version 'AF8.0.26.345', and 6.96MB of logs. 2. 'Sangfor IAM (192.1...)' with type 'Internet Acc...', IP '192.168.20.52', version 'Sangfor--IA...', and no logs. A '+ New' button is highlighted in the top left of the table area.

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.



The screenshot displays the Cyber Command interface with a 'New' dialog box open for adding a device. The dialog box contains the following fields and options:

- \* Device IP:** 192.168.20.51
- \* Device Name:** Sangfor Endpoint Secure
- Type:**
  - ☐ Internet Access Management
  - ☒ Endpoint Secure
  - ☐ SSL VPN
  - ☐ Wireless Access Controller
  - ☐ Branch Business Center
- Port:** 4430
- Remarks:** (Empty text area)


A yellow tooltip message is displayed within the dialog box:

STA, NGAF, FTA, Visioner, and Host Security can be connected without being configured on Cyber Command. Connecting Endpoint Secure or DAS needs to enable port 7443.

The background shows the Cyber Command dashboard with a sidebar menu (System, Correlated Devices, Monitor, Update, Maintenance, Databases) and a top navigation bar (Home, Response, Detection, Assets, Reports, More). A status bar at the top indicates 'Error connecting to devices. Please check for network connectivity issues.' and 'Details'.

The screenshot shows the Cyber Command interface. The top navigation bar includes 'Cyber Command', 'Home', 'Response', 'Detection', 'Assets', 'Reports', and 'More'. A sidebar on the left contains 'System', 'Correlated Devices', 'Monitors', 'System', 'Update', 'Maintenance', and 'Databases'. The main content area displays a summary of correlated devices, including 'Endpoint Secure', 'NGAF', 'IAM', 'STA', and 'BBC'. Below this is a table with columns for ID, Name, IP Address, Type, Version, Licensed, Sync Mode, Today's Synced Logs, Total Synced Logs, Today's Logs, Last Synced, Status, Alerts, and Operation. The table lists three devices, with the third device, 'Sangfor Endpoint Security', highlighted by a red box.

ID	Name (IP Address)	Type	Version	Licensed	Sync Mode	Today's Synced Logs	Total Synced Logs	Today's Logs	Last Synced	Status	Alerts (30 days)	Operation
1	af (192.168.20.51)	Next Gen...	192.168.20.51	AFR-216.345	Licenses Used	Simplified	6.96MB	6.96MB	204	2021-03-16 16:13:27	Not...	2
2	Sangfor IAM (192.168.20.52)	Internet Acc...	192.168.20.52	Sangfor-IAM-12.0...	Licenses Used	-	-	-	2021-03-16 16:11:18	Not...	0	-
3	Sangfor Endpoint Secur...	Endpoint Se...	192.168.20.51	3.2.22EN	Licenses Used	Advanced	0B	0B	-	Not...	0	-


**Sangfor Endpoint Secure**  
Trial Edition

[Home](#)
[Endpoints](#)
[Micro-Segmentation](#)
[Detection](#)
[Response](#)
[Logs](#)
[System](#)

**Endpoints**

[Groups](#)
[Inventory](#)
[Security Protection](#)

**Groups**

Group name

Endpoints

Local Site

Ungrouped En...

Branch\_CN

Branch\_US

HQ

Move To

Enable Agent

Send Message

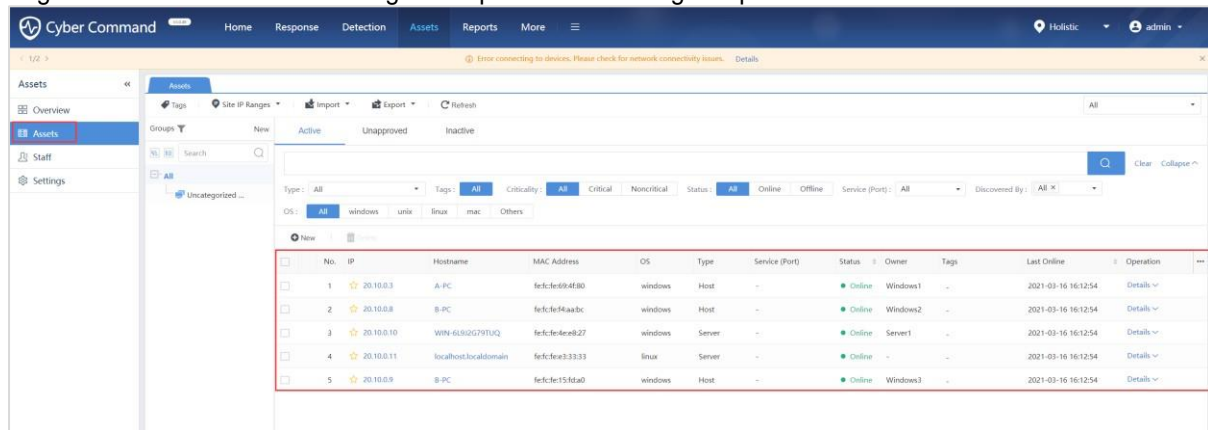
Refresh

Endpoints (4 online / 5 in total)

	No.	Endpoint	Endpoint Status	Group	IP Address
<input type="checkbox"/>	1	Windows1	Online	Ungrouped Endpoints	20.10.0.3
<input type="checkbox"/>	2	Windows2	Online	Ungrouped Endpoints	20.10.0.8
<input type="checkbox"/>	3	Server1	Offline	Ungrouped Endpoints	20.10.0.10
<input type="checkbox"/>	4	Centos	Online	Ungrouped Endpoints	20.10.0.11
<input type="checkbox"/>	5	Windows3	Online	Ungrouped Endpoints	20.10.0.9

5

## Bagaimana untuk Berkorelasi dengan Endpoint Secure dengan Operasi Sederhana

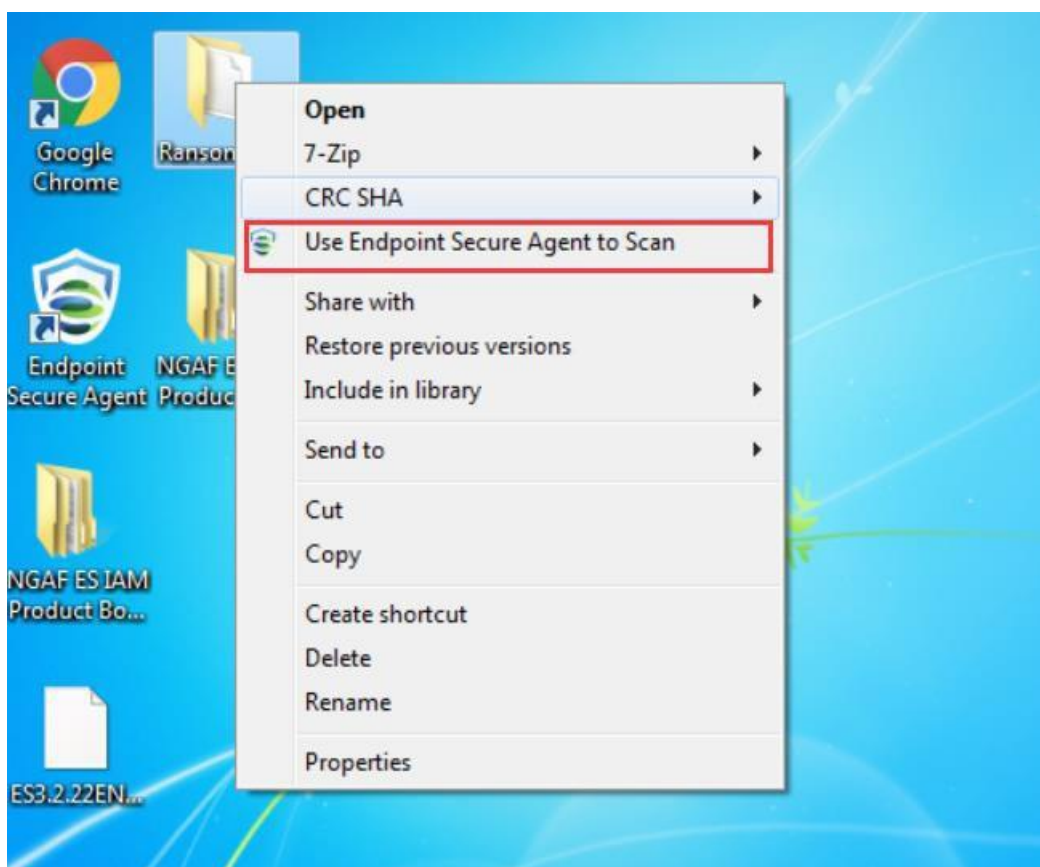


No.	IP	Hostname	MAC Address	OS	Type	Service (Port)	Status	Owner	Tags	Last Online	Operation
1	20.10.0.3	A-PC	fecf-de894f80	windows	Host	-	Online	Windows1	-	2021-03-16 16:12:54	Details
2	20.10.0.8	B-PC	fecf-de894f80	windows	Host	-	Online	Windows2	-	2021-03-16 16:12:54	Details
3	20.10.0.10	WIN-6502G79TUQ	fecf-de894f80	windows	Server	-	Online	Server1	-	2021-03-16 16:12:54	Details
4	20.10.0.11	localhost.localdomain	fecf-de894f80	linux	Server	-	Online	-	-	2021-03-16 16:12:54	Details
5	20.10.0.9	B-PC	fecf-de15fda0	windows	Host	-	Online	Windows3	-	2021-03-16 16:12:54	Details

## Bab 3 Korelasi

### 3.1 Generate Security Logs dan Sinkronisasi ke Cyber Command

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



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

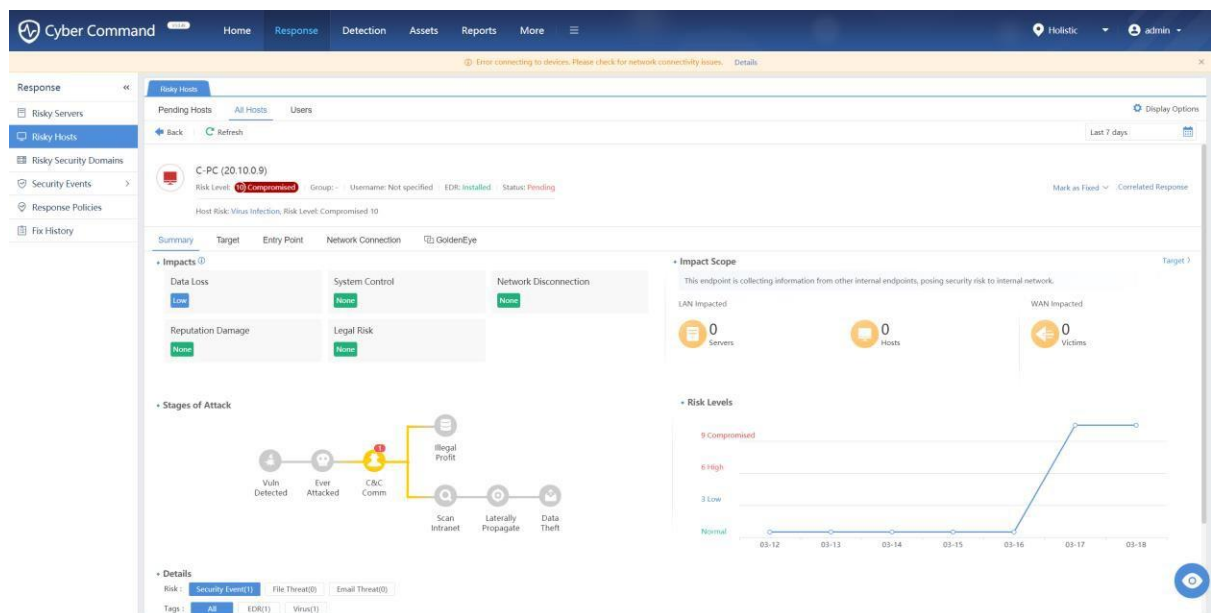
## Bagaimana untuk Berkorelasi dengan Endpoint Secure dengan Operasi Sederhana

The screenshot displays the Sangfor Endpoint Secure console interface. The top navigation bar includes Home, Endpoints, Micro-Segmentation, Detection, Response, Logs, and System. The left sidebar shows the Response menu with options for Threat Response, Endpoint Patching, and Threat Tracking. The main content area is divided into two tabs: Endpoints and Security Events. The Endpoints tab is active, showing a summary of endpoint statuses: 3 Victim Endpoints, 3 Compromised, 0 Critical, 0 Suspicious, and 0 Isolated. Below this, a table lists the endpoints. The third row, representing a Windows3 (20.10.0.8) endpoint, is highlighted with a red border. This endpoint is categorized as 'Ungrouped Endpoints' and has a 'Compromised' severity. The table also shows 'Pending/Total Threats' as 1/67, the 'Last Detected' time as 2021-03-17 18:40:23, and available operations as 'Fix' and 'Isolate'.

No.	Endpoint	Group	Severity	Security Events	Pending/Total Threats	Last Detected	Operation
1	Windows2 (20.10.0.8)	Ungrouped Endpoints	Compromised	Ransomware	1/67	2024-02-27 15:54:08	Fix Isolate
2	Windows1 (20.10.0.8)	Ungrouped Endpoints	Compromised	Ransomware Trojan Others	41/139	2021-03-17 18:11:39	Fix Isolate
3	Windows3 (20.10.0.8)	Ungrouped Endpoints	Compromised	Ransomware	1/67	2021-03-17 18:40:23	Fix Isolate

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.

## Bagaimana untuk Berkorelasi dengan Endpoint Secure dengan Operasi Sederhana

### Correlated Response



Virus event occurred. Suggestion: Enable access control to block connections with controller. Enable threat scan to clean up virus-infected files.

<input checked="" type="checkbox"/>		<b>Correlated Block</b> Block all outbound accesses from a specific host or inbound accesses to that host.
<input type="checkbox"/>		<b>Access Control</b> <span>Hot</span> Prevent a specific host from accessing specified IP address and port to block abnormal and attack behaviors.
<input type="checkbox"/>		<b>Browsing Risk Notification</b> Notify users of risks and solutions when surfing the Internet with browser.
<input type="checkbox"/>		<b>Account Lockout</b> Block infected hosts from accessing the Internet to reduce the risk of regulatory notification, and speed up response.
<input type="checkbox"/>		<b>Threat Scan</b> <span>Hot</span> Start a full/quick scan on host and quarantine/trust detected malicious files.
<input type="checkbox"/>		<b>Forensics</b> Perform forensic investigation against a malicious domain to locate which parent or child process accesses that domain.

Next

Close

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

## Bagaimana untuk Berkorelasi dengan Endpoint Secure dengan Operasi Sederhana

**Correlated Response**

Asset IP: 20.10.0.9 [Create Response Policy ?](#)

**Correlated Block**

Device: ☐ NGAF ☒ Endpoint Secure **Hot**

IP Address: 192.168.20.51(Auto-c)

**Correlated Block**

Direction: ☐ All ☒ Outbound ☐ Inbound

Lockout [?](#): 1 days

Remarks:

**Correlated Block**

OK Cancel

Back Close

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

## Bagaimana untuk Berkorelasi dengan Endpoint Secure dengan Operasi Sederhana

Correlated Response

Asset IP: 20.10.0.9
Create Response Policy ⓘ

Correlated Block

Device:
☐ NGAF
☒ Endpoint Secure Hot

IP Address: 192.168.20.51(Auto-discovered)

Correlated Block
Locking (1 days 0 hours 00 mins)
Edit | Unlock | ▼

Direction: Outbound
Lockout: 1 days
Remarks: Manually correlate is a correlate policy that be pushed do...

Manually correlate is a correlate policy that be pushed down in Response and other pages after log in the Cyber Command.

Again
Close

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.

Sangfor Endpoint Secure										
Response										
Endpoints Security Events										
3 Victim Endpoints ⓘ		3 Compromised		0 Critical		0 Suspicious		1 Isolated		
No.	Endpoint	Group	Action	Blocked IP	Block Port	Period (Days)	Time Fixed	Administrator	Status	Operation
1	Windows (20.10.0.9)	Ungrouped Endpoints	No Outbound	All	All	1day(s)	2021-03-18 09:27:08	Cyber Command Correlati...	Quarantined	Restore



**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