



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
1.1 Skenario.....	1
1.2 Lingkungan.....	1
1.2.1 Lingkungan Network	1
1.3 Tindakan Pencegahan	1
Bab 2 Konfigurasi	2
2.1 Konfigurasi IAM.....	2
2.2 Konfigurasi Cyber Command	5
2.3 Konfigurasi Endpoint Secure.....	6
Bab 3 Korelasi	9
3.1 Sinkronisasi Logs ke Cyber Command	9
3.2 Response di Cyber Command	12
3.2.1 Lockout Account	12
3.2.2 Browsing Risk Notification	14

Bab 1 Skenario

1.1 Skenario

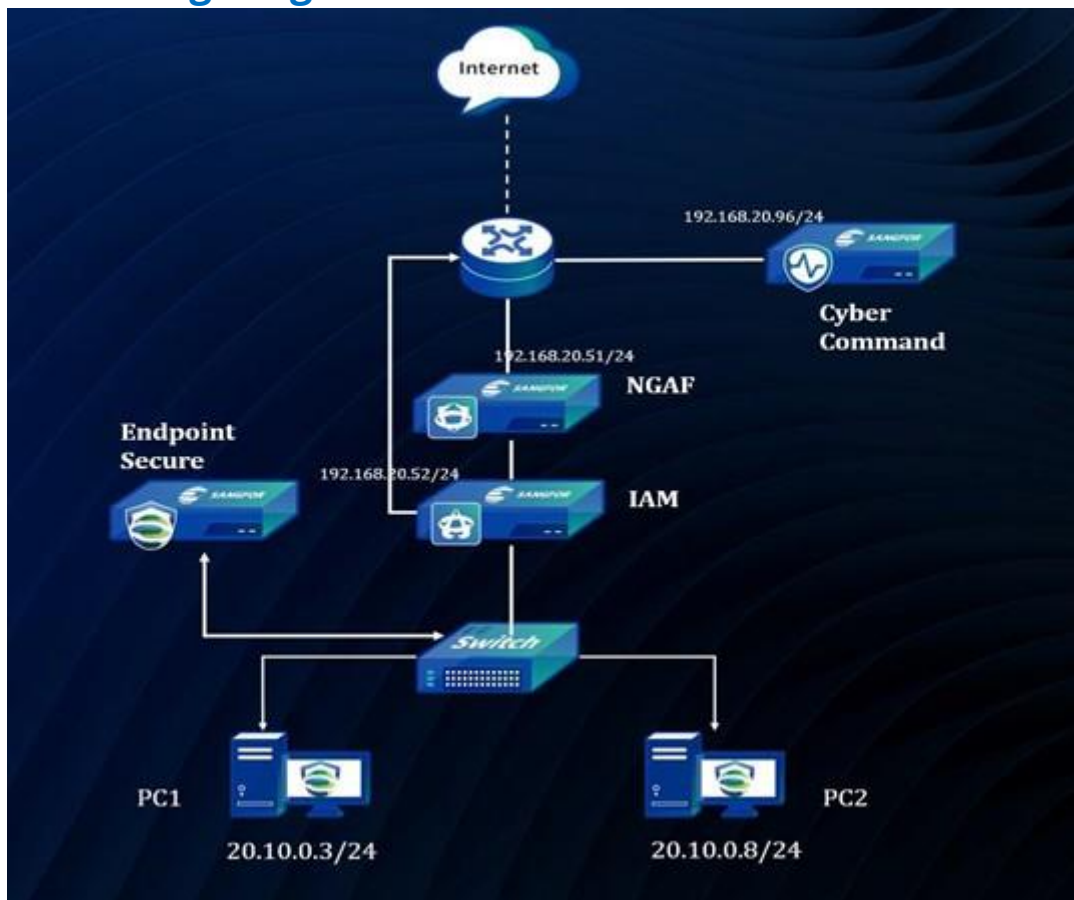
Cyber Command mengumpulkan data dari probe deteksi security dari setiap node intranet, mempersembahkan pengguna dengan bisnis asset intranet dan attack dan potensi ancaman terhadap asset bisnis utama intranet dalam bentuk visual, dan menggunakan platform untuk attack semua sistem security di network 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

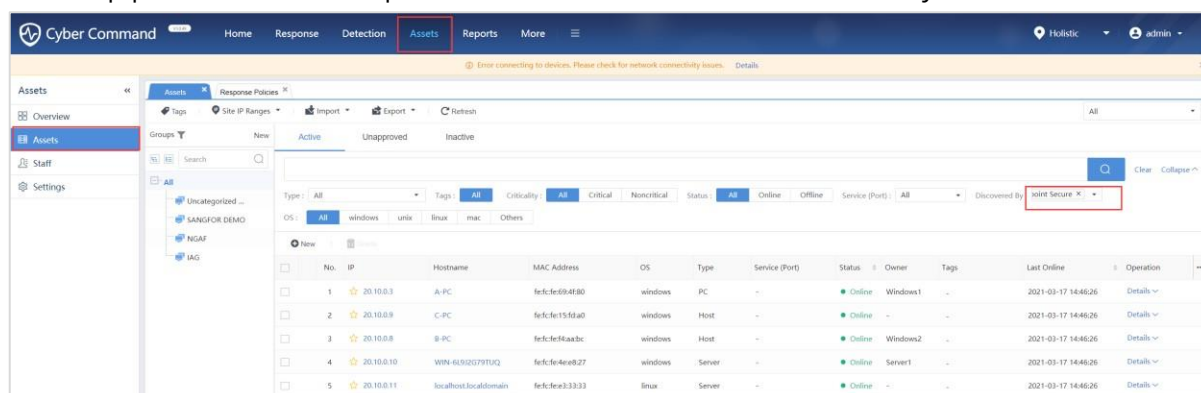
1.2.1 Lingkungan Network



1.3 Tindakan Pencegahan

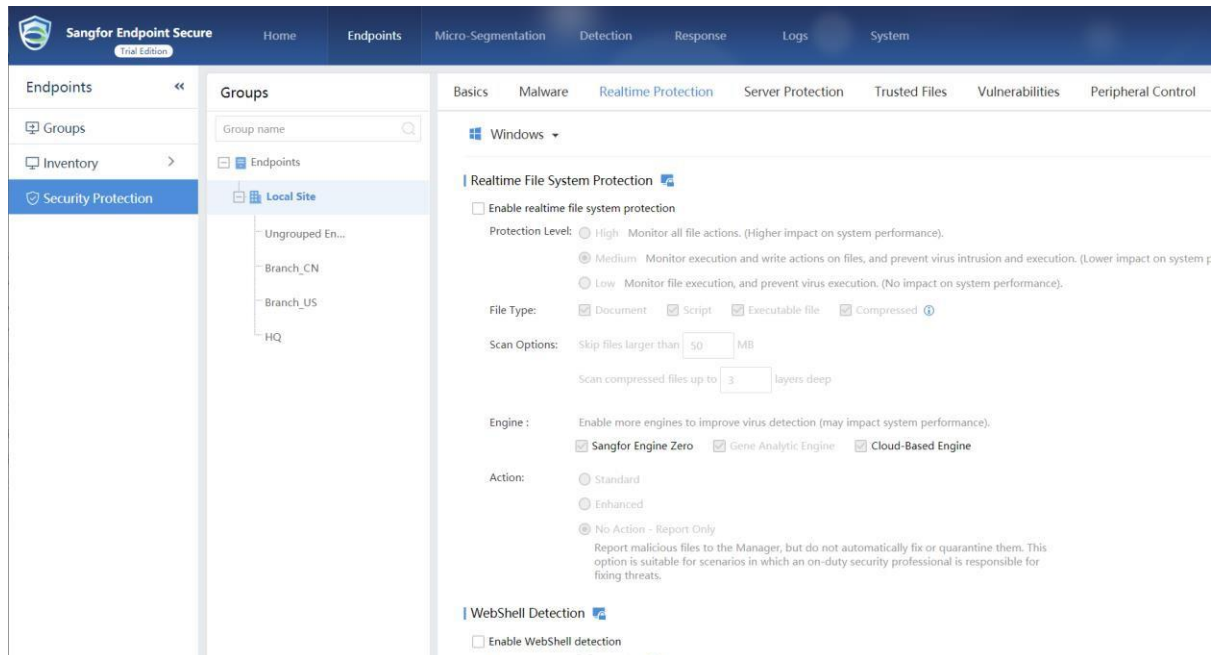
1. IAM tidak mendukung Sinkronisasi security log ke Cyber Command dan tidak mendukung anti virus di endpoint, Cyber Command hanya mendukung masalah lockout atau pengingat policy ke IAM, jadi Anda perlu instal Endpoint Secure agar IAM berkorelasi untuk scan virus dan sinkronisasi security log ke Cyber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

2. Harap pastikan bahwa Endpoint Secure sinkronisasi semua asset ke CyberCommand.



Bagaimana untuk Berkorelasi dengan IAM untuk Operasi Sederhana

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.**

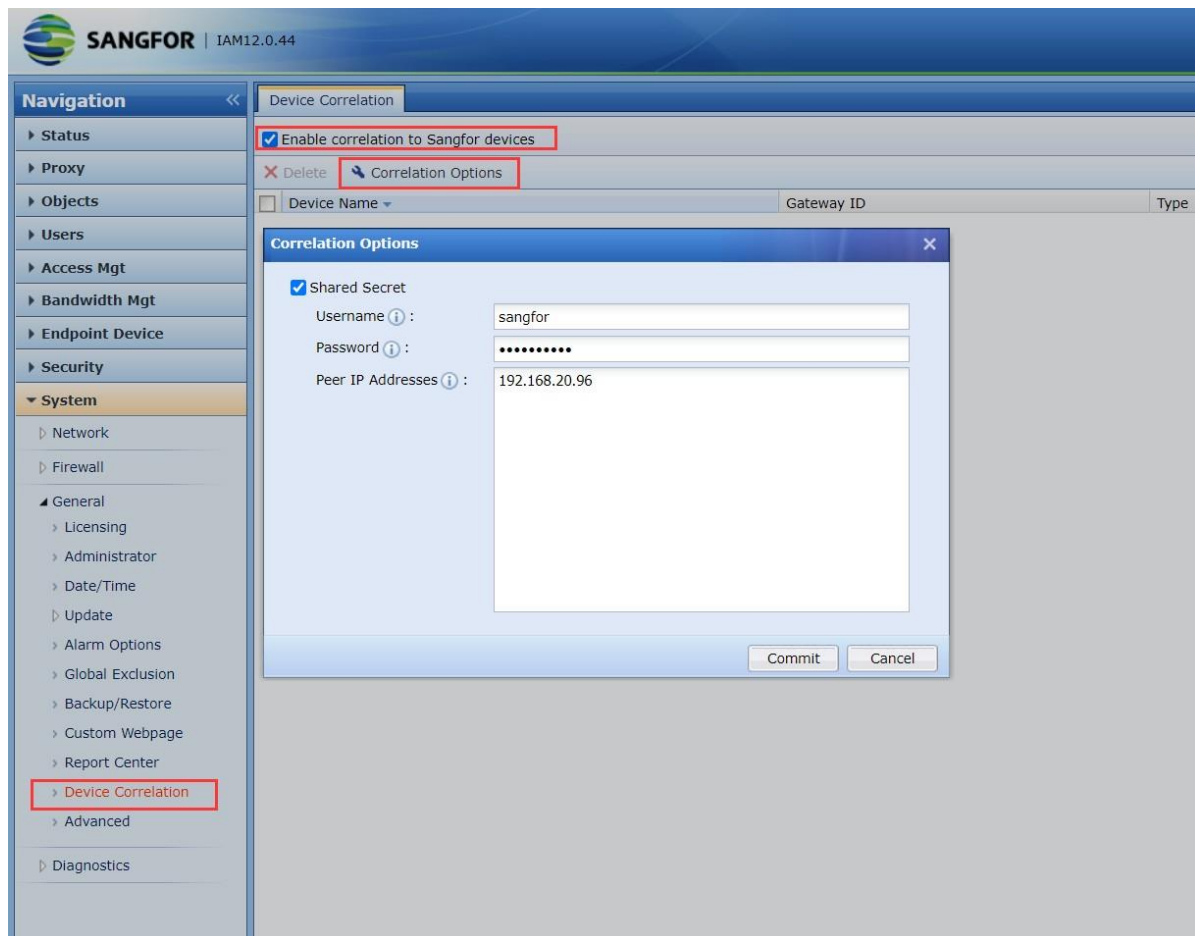


Bab 2 Konfigurasi

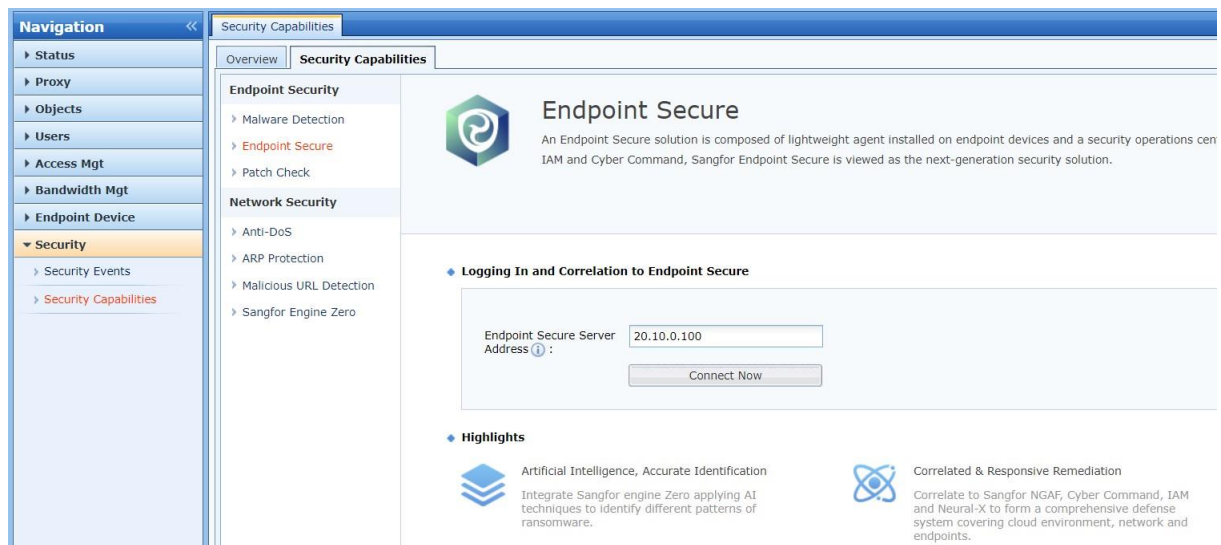
2.1 Konfigurasi IAM

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

Bagaimana untuk Berkorelasi dengan IAM untuk Operasi Sederhana

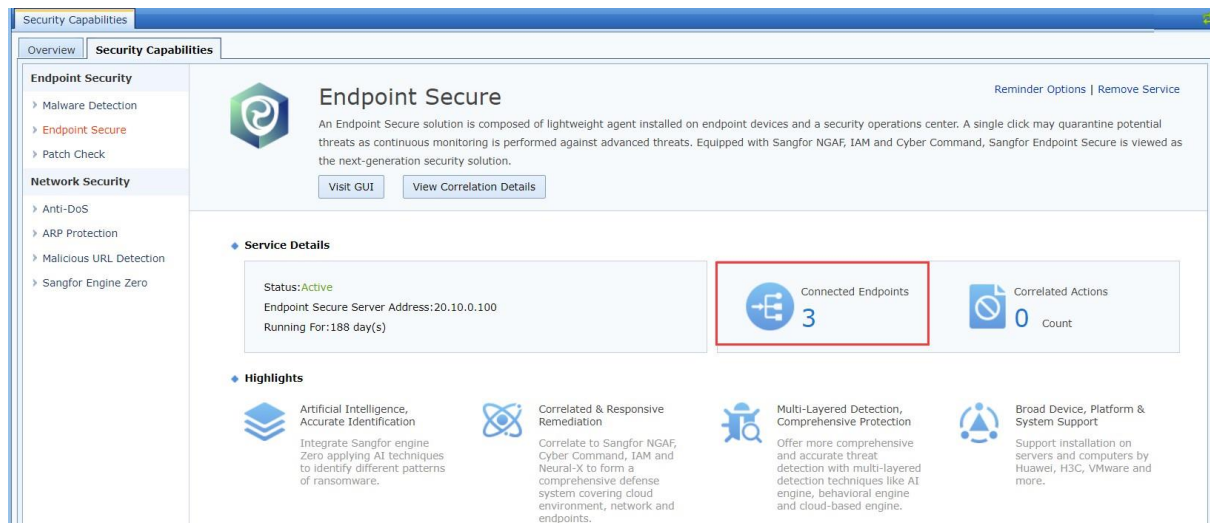


2. Pergi ke Security-> Security Capabilities path. Masukkan IP address dari Endpoint Secure.



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

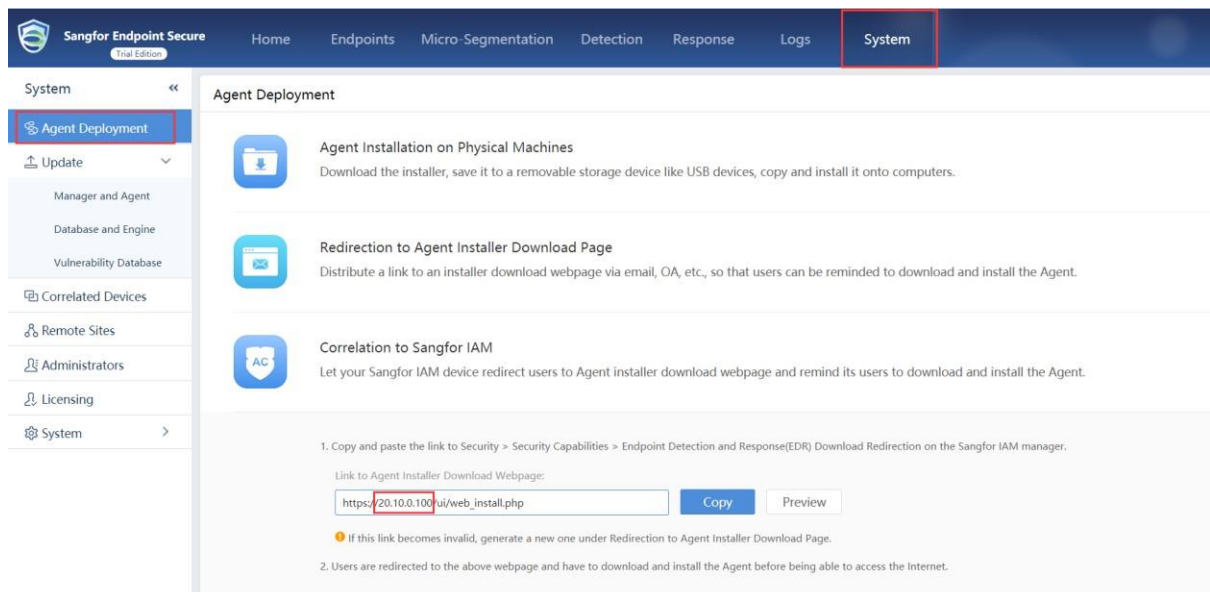
Bagaimana untuk Berkorelasi dengan IAM untuk Operasi Sederhana



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

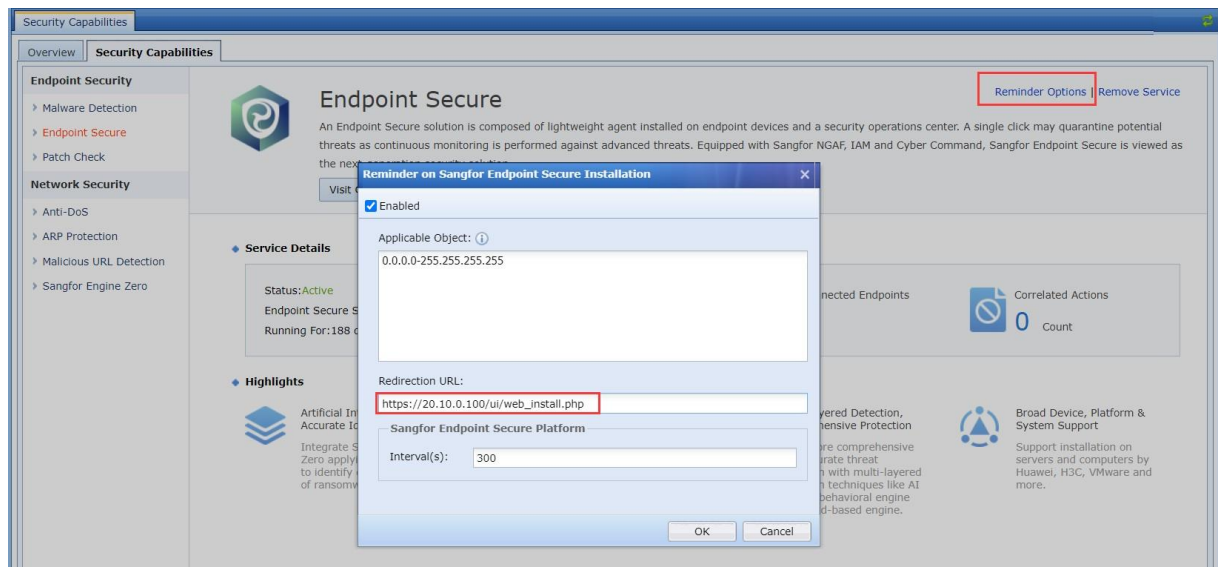
Pertama, konfigurasi risk reminder page address di Endpoint Secure, Anda dapat ke System-> Agent Deployment-> Correlation to Sangfor IAM page dan konfigurasi ES agent download address sehingga IAM dapat mengarahkan PC ke halaman agent download.

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



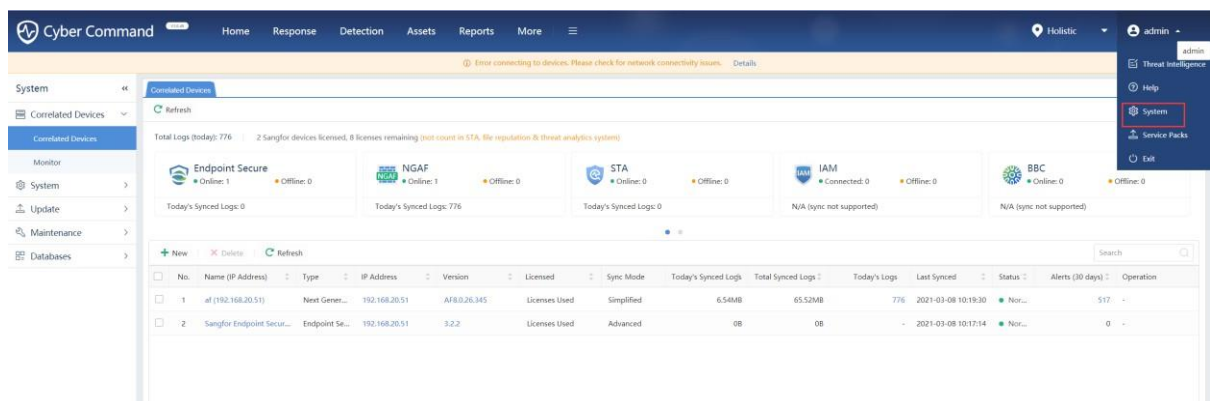
Kedua, konfigurasi peringatan policy di IAM, silakan pastikan URL redireksi sama seperti yang Anda konfigurasi di ES.

Bagaimana untuk Berkorelasi dengan IAM untuk Operasi Sederhana

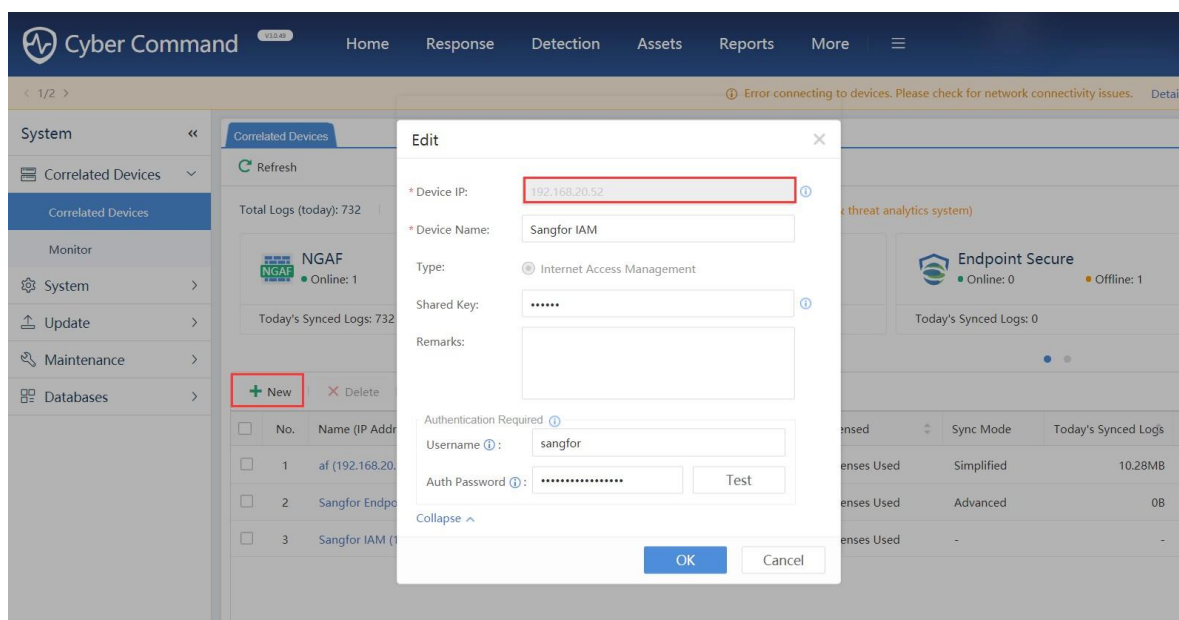


2.2 Konfigurasi Cyber Command

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.



Bagaimana untuk Berkorelasi dengan IAM untuk Operasi Sederhana

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

The image shows a software configuration window titled "Edit". It contains several input fields and a "Test" button. A green checkmark and the text "Authentication passed." are overlaid on the top left. The "Test" button is highlighted with a red rectangle.

Edit [Close]

* Device IP: [Input Field] ⓘ

* Device Name: [Input Field]

Type: ☒ Internet Access Management

Shared Key: [Input Field] ⓘ

Remarks: [Text Area]

Authentication Required ⓘ

Username ⓘ : [Input Field] sangfor

Auth Password ⓘ : [Input Field] **Test**

Collapse ^

[OK] [Cancel]

2.3 Konfigurasi Endpoint Secure

1. Pergi ke System Path.

Bagaimana untuk Berkorelasi dengan IAM untuk Operasi Sederhana

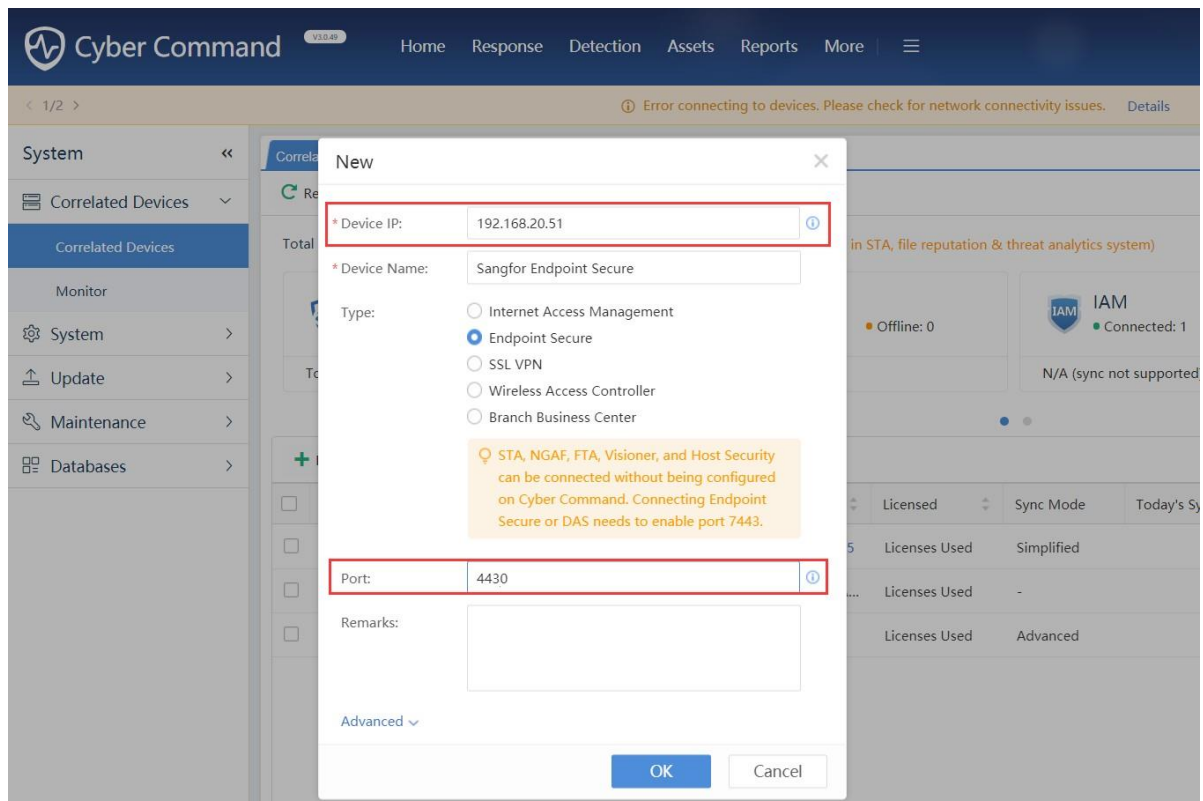
The screenshot shows the Sangfor Cyber Command interface. The top navigation bar includes a location icon, 'Holistic', and a user profile 'admin'. A sidebar on the right contains links for 'Threat Intelligence', 'Help', 'System', 'Service Packs', and 'Exit'. The main content area displays two device status cards: 'NGAF' (Online: 0, Offline: 0) and 'BBC' (Online: 0, Offline: 0). Below these cards is a table with columns: 'Synced Logs', 'Today's Logs', 'Last Synced', 'Status', 'Alerts (30 days)', and 'Operation'. The table shows one entry for 'NGAF' with a status of 'Nor...' and 0 alerts.

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

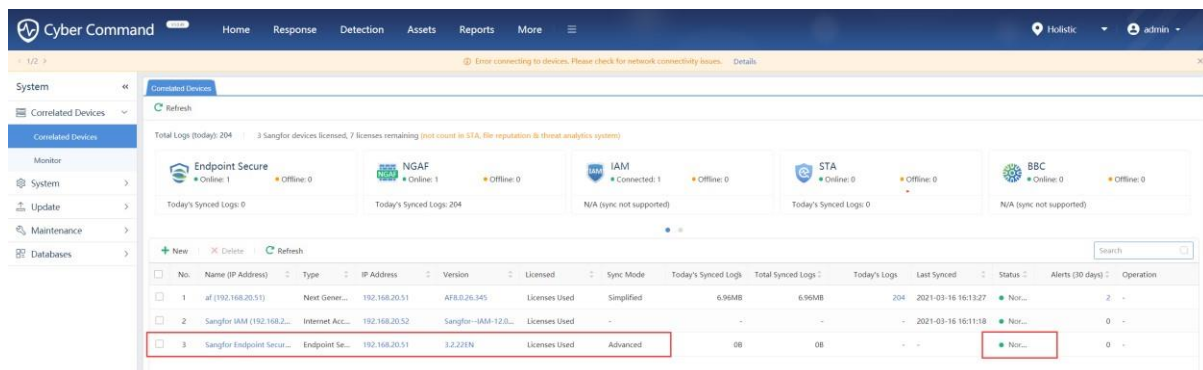
The screenshot shows the Sangfor Cyber Command interface. The top navigation bar includes 'Cyber Command' and a user profile 'admin'. A sidebar on the left contains links for 'System', 'Correlated Devices', 'Monitor', 'System', 'Update', 'Maintenance', and 'Databases'. The main content area displays the 'Correlated Devices' section with a 'Refresh' button and a table of devices. The table has columns: 'No.', 'Name (IP Address)', 'Type', 'IP Address', 'Version', 'Licensed', 'Sync Mode', and 'Today's Synced Logs'. The table shows two entries: 'Endpoint Secure' (IP: 192.168.20.51) and 'Sangfor IAM' (IP: 192.168.20.52).

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.

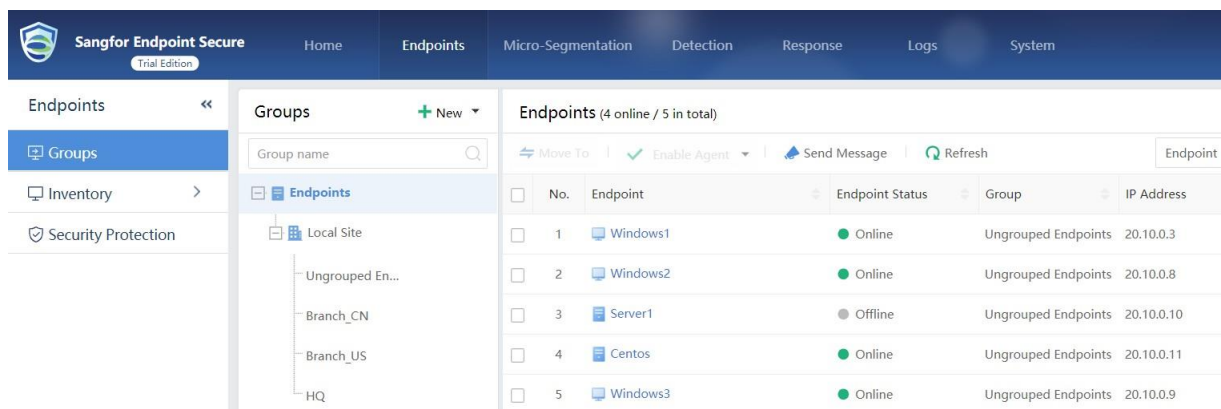
Bagaimana untuk Berkorelasi dengan IAM untuk Operasi Sederhana



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

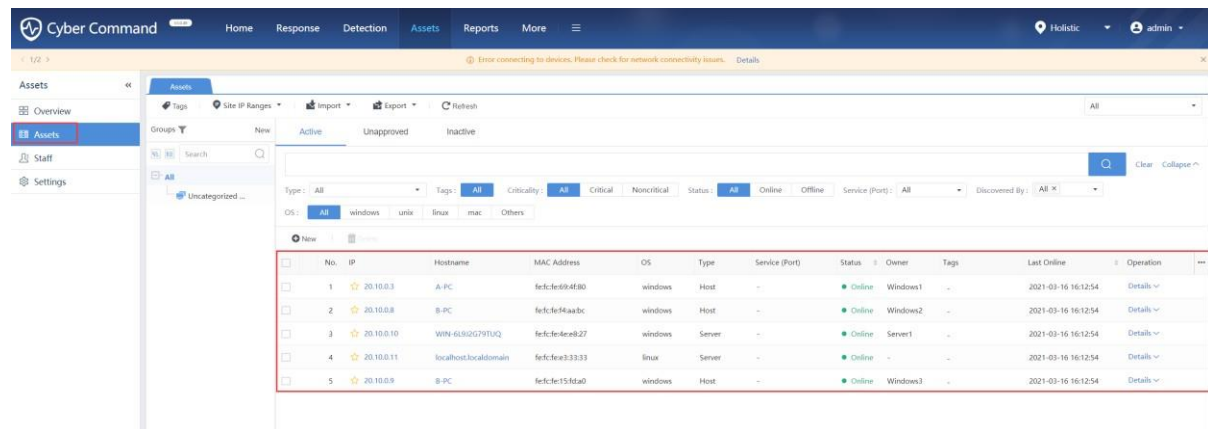


5. Anda dapat memeriksa apakah ada asset di Endpoint Secure.

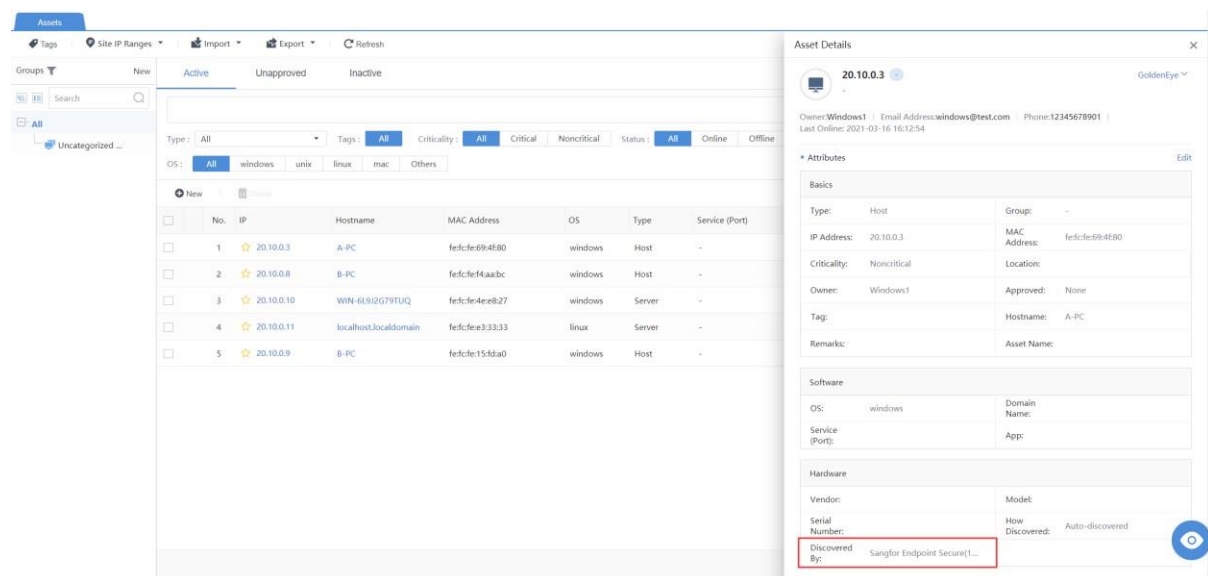


6. Jika Anda ada di Endpoint Secure, Anda pergi ke Assets->Assets di Cyber Command untuk memeriksa apakah asset telah sinkronisasi ke Cyber Command.

Bagaimana untuk Berkorelasi dengan IAM untuk Operasi Sederhana



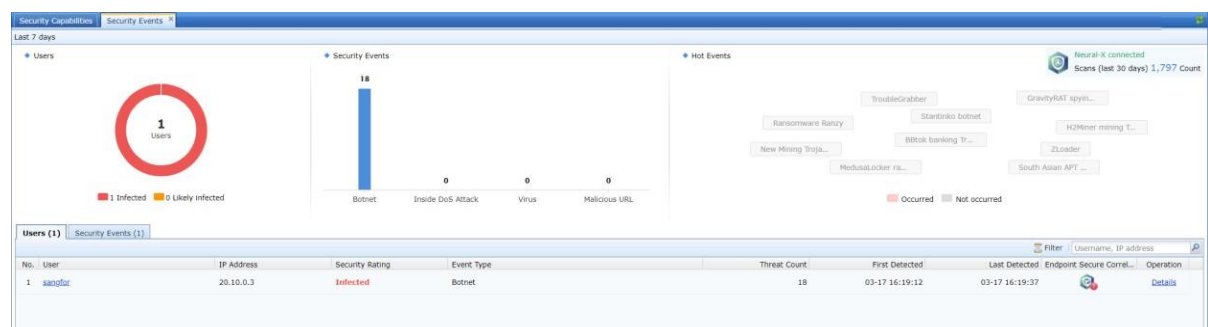
7. Anda dapat melihat detail untuk melihat assets source, seperti berikut detail, Anda dapat melihat asset ini ditemukan oleh Endpoint Secure.



Bab 3 Korelasi

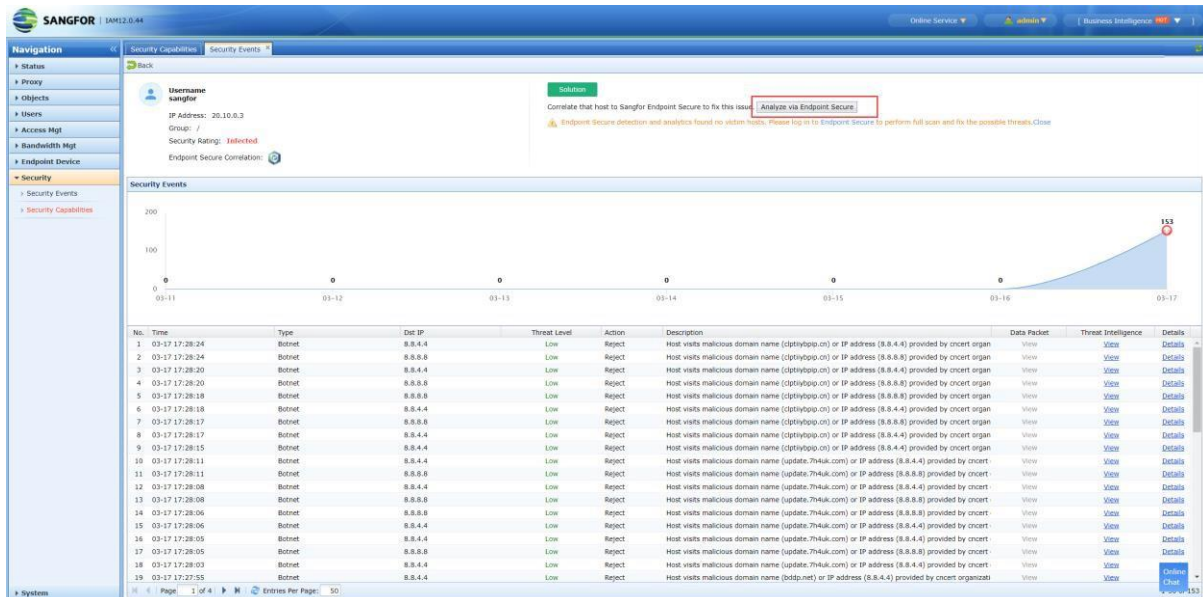
3.1 Sinkronisasi Log ke Cyber Command

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

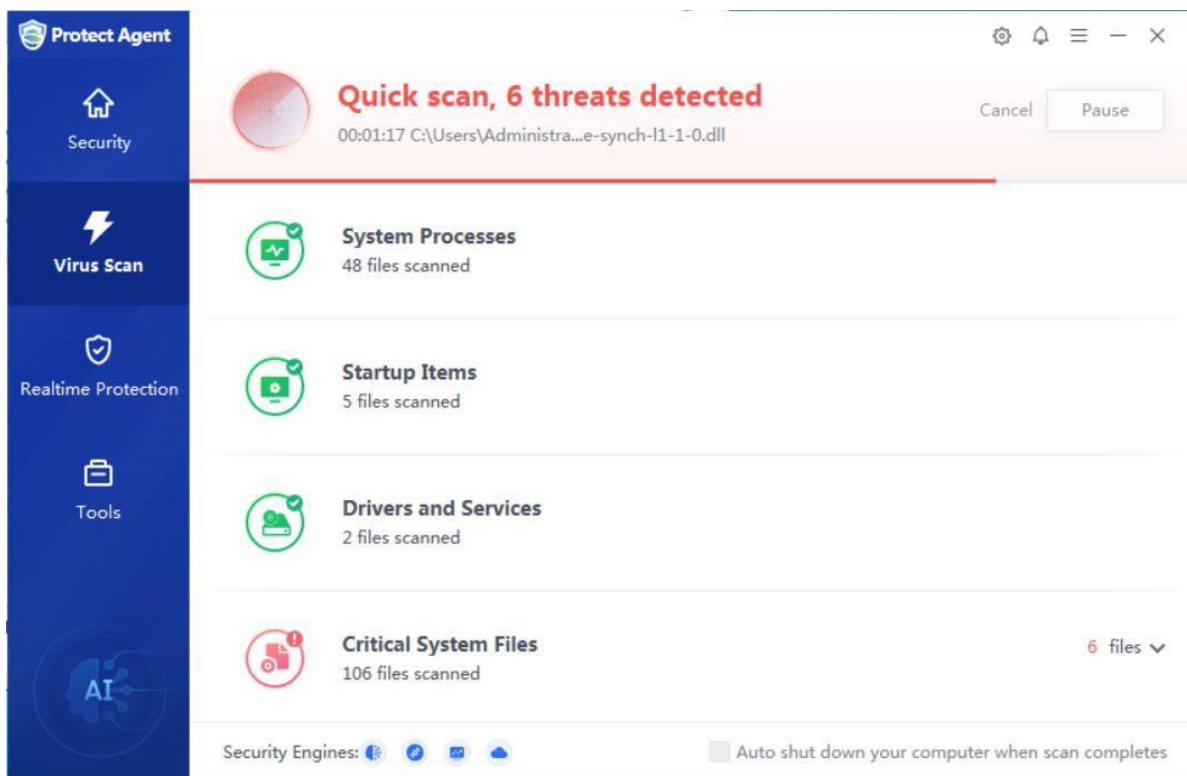


2. Klik Analyze melalui Endpoint Secure untuk mengeluarkan scan task.

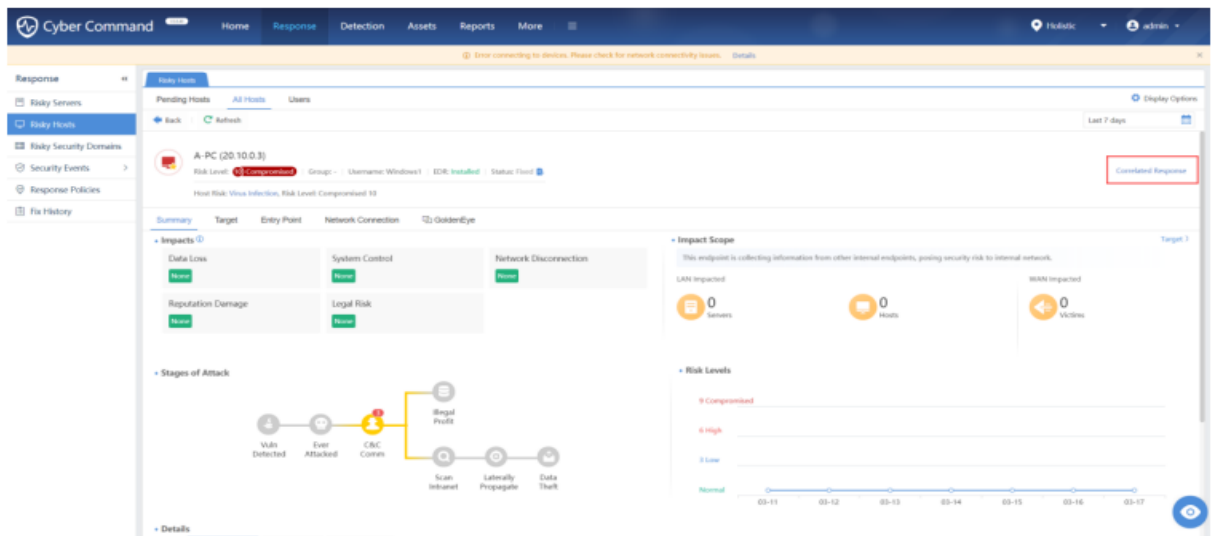
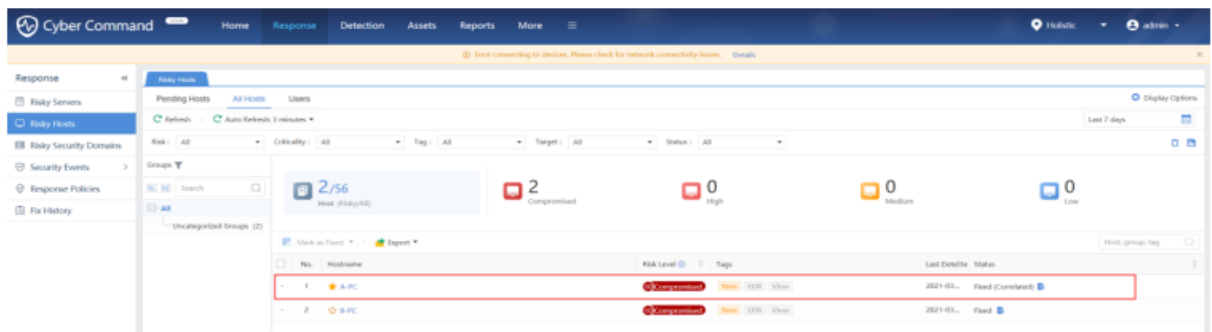
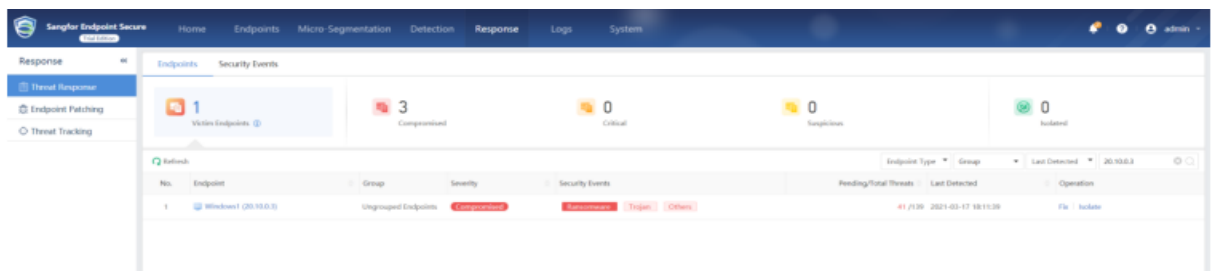
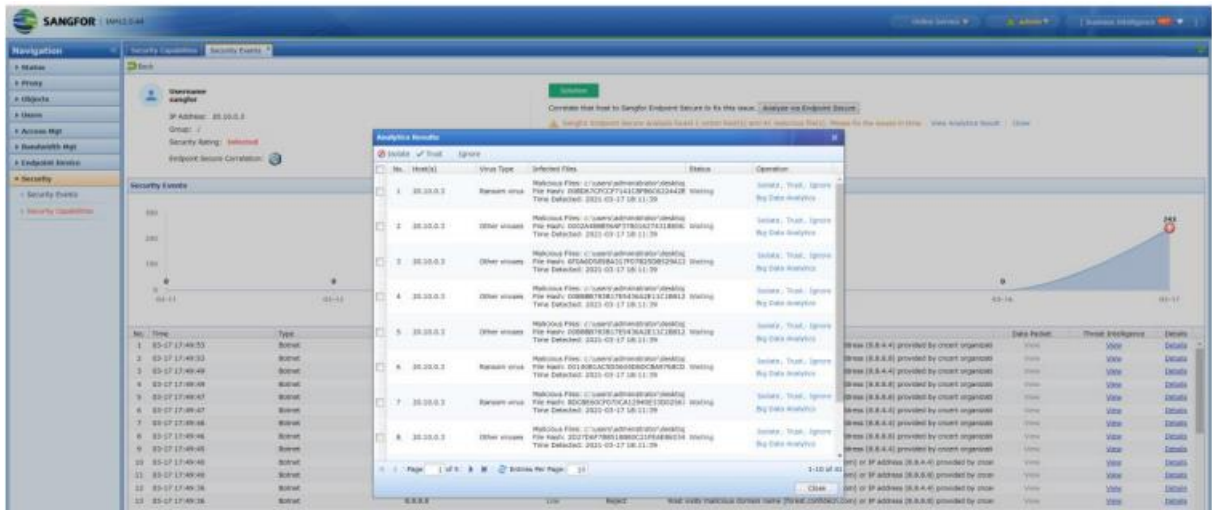
Bagaimana untuk Berkorelasi dengan IAM untuk Operasi Sederhana



Kemudian, Anda dapat melihat scan task running di endpoint.



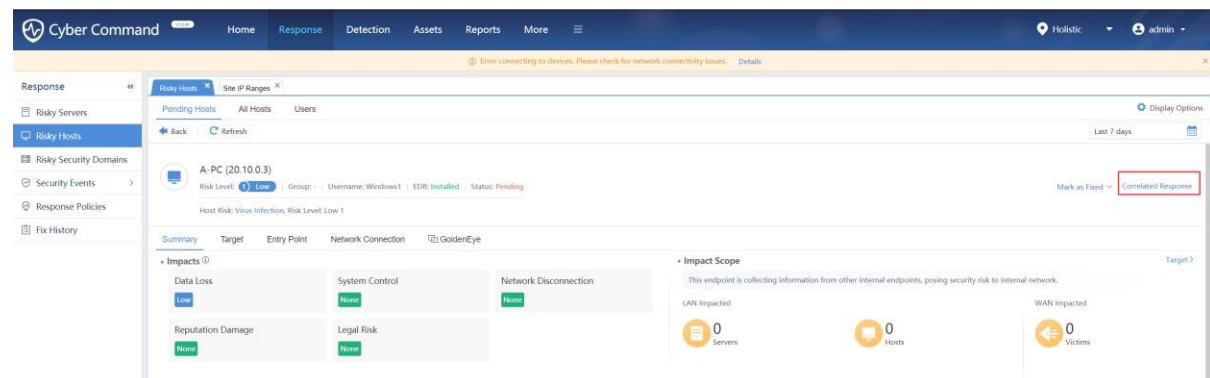
Bagaimana untuk Berkorelasi dengan IAM untuk Operasi Sederhana



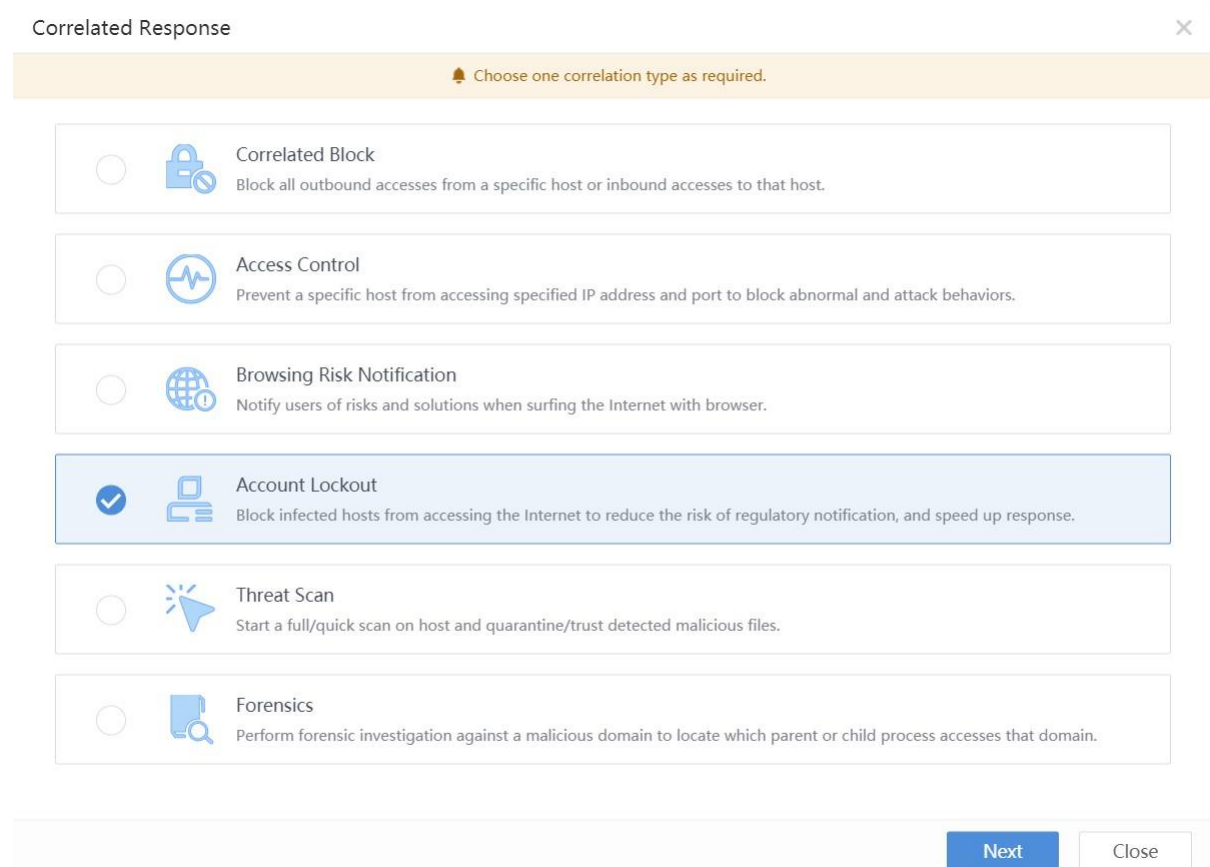
3.2 Response di Cyber Command

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.

Bagaimana untuk Berkorelasi dengan IAM untuk Operasi Sederhana

Correlated Response

Asset IP: 20.10.0.3

Create Response Policy ⓘ

Account Lockout

Device: • IAM Hot

It is detected that the current endpoint has no IAM-related user information. Please sync the user information first.

IP Address: Sangfor IAM(192.168.20.52)

Account Lockout

Start

Back

Close

Correlated Response

Asset IP: 20.10.0.3

Create Response Policy ⓘ

Account Lockout

Device: • IAM Hot

It is detected that the current endpoint has no IAM-related user information. Please sync the user information first.

IP Address: Sangfor IAM(192.168.20.52)

Account Lockout

Period ⓘ: 1 days

Remarks: Remarks

Sending request...

OK

Cancel

Back

Close

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

Bagaimana untuk Berkorelasi dengan IAM untuk Operasi Sederhana

Correlated Response

Asset IP: 20.10.0.3

Create Response Policy ⓘ

Account Lockout

Device: IAM Hot

It is detected that the current endpoint has no IAM-related user information. Please sync the user information first.

IP Address: Sangfor IAM(192.168.20.52)

Account Lockout

Locked (1 days 0 hours 00 mins)

Edit | Cancel | ▼

Period: 1 days

Remarks: Manually correlate is a correlate policy that be pushed do...

Again

Close

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

No.	Username(Alias)	Group	IP Address	Endpoint Device	Auth Method	Time Logged In/Locked	Online Duration	Operation
1	sangfor	/	20.10.0.3	PC(Windows PC)	User Account	2021-03-17 15:10:12Lock	Locked, 23 hours 57 minut...	
2	20.10.0.11	/	20.10.0.11	Verifying...	Open authenticati...	2021-03-05 11:07:37Login	292 hours 04 minutes 47 s...	
3	20.10.0.9	/	20.10.0.9	Verifying...	Open authenticati...	2021-03-04 09:21:50Login	317 hours 50 minutes 34 s...	
4	20.10.0.100	/	20.10.0.100	Verifying...	Open authenticati...	2021-03-02 15:45:30Login	359 hours 26 minutes 54 s...	

3.2.2 Browsing Risk Notification

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

Bagaimana untuk Berkorelasi dengan IAM untuk Operasi Sederhana

Correlated Response ✕

Choose one correlation type as required.

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

Next **Close**

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

Correlated Response ✕

Asset IP: 20.10.0.3 Create Response Policy ⓘ

Browsing Risk Notification

Device: IAM Hot

It is detected that the current endpoint has no IAM-related user information. Please sync the user information first.

IP Address: Sangfor IAM(192.168.0.255)

Browsing Risk Notification Start

Browsing Risk Notification ✕

Method: ☒ Remind upon opening browser

Message: ☒ Predefined ⓘ Template ☐ Custom

Remarks:

OK **Cancel**

Back **Close**

Bagaimana untuk Berkorelasi dengan IAM untuk Operasi Sederhana

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

Bagaimana untuk Berkorelasi dengan IAM untuk Operasi Sederhana

Correlated Response

Asset IP: 20.10.0.3

Create Response Policy ⓘ

Browsing Risk Notification

Device: IAM Hot

It is detected that the current endpoint has no IAM-related user information. Please sync the user information first.

IP Address: Sangfor IAM(192.168.20.52)

Browsing Risk Notification Reminded

Edit Cancel

Method: Notify in browser

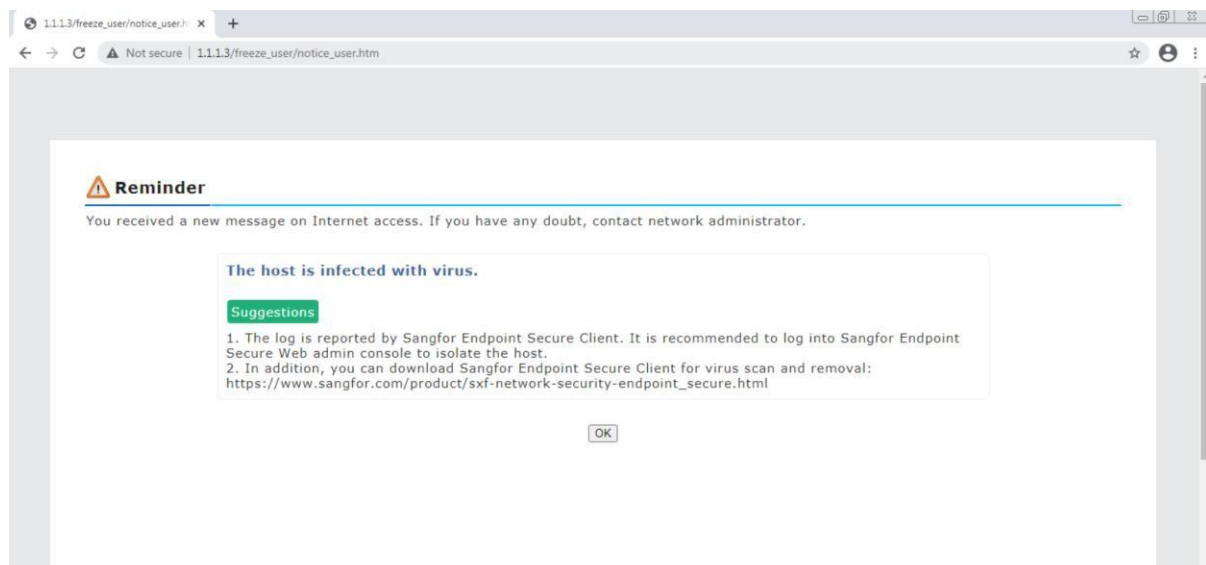
Contents: Predefined

Remarks: Manually correlate is a correlate policy that be pushed do...

Again

Close

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





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