



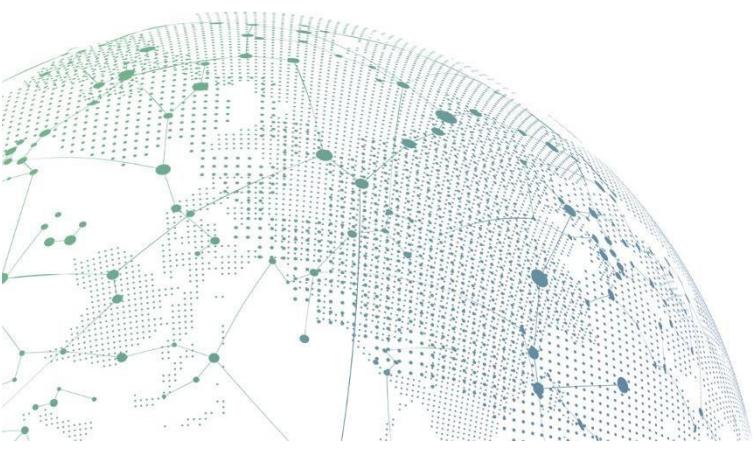
SANGFOR



# 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

Bagaimana untuk Berkorelasi dengan IAM untuk Operasi Sederhana

# Bab 1 Skenario

## 1.1 Skenario

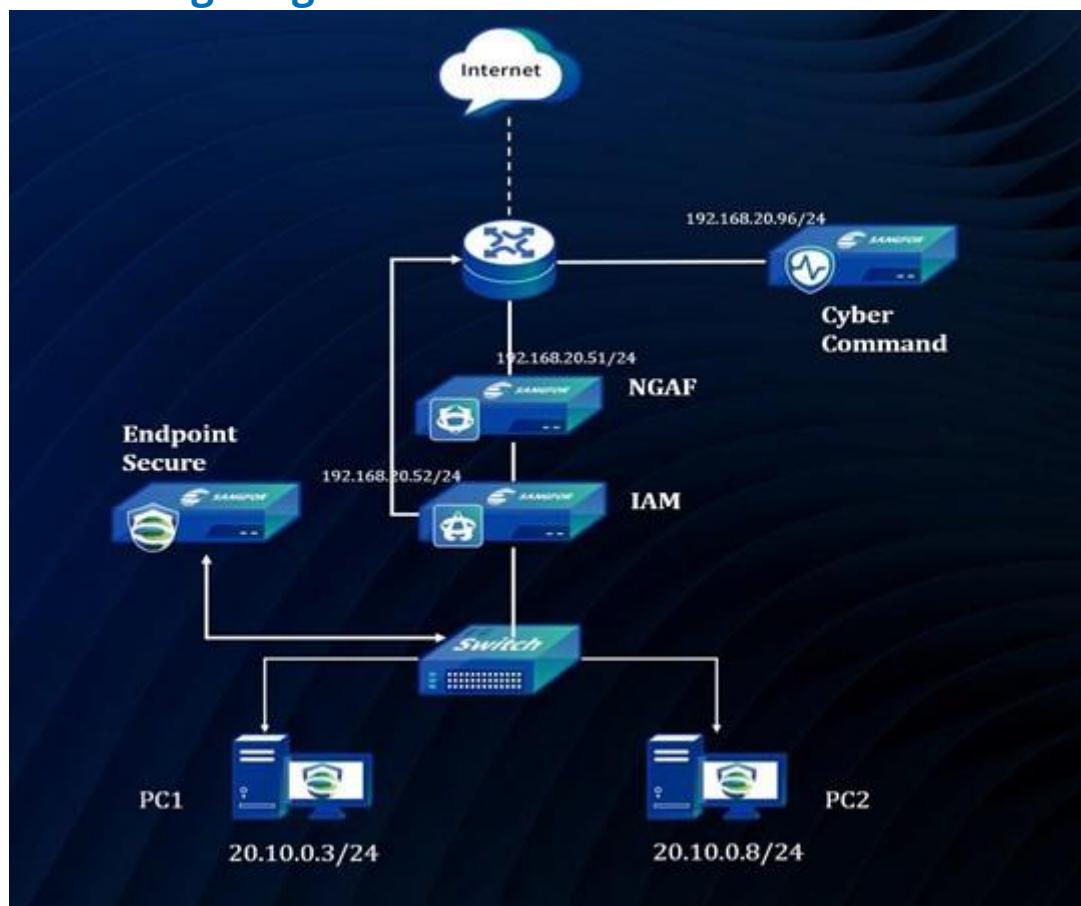
Cyber Command mengumpulkan data dari probe deteksi security dari setiap node intranet, mempersembahkan pengguna dengan bisnis asset intranet dan attack dan potensi ancaman terhadap asset bisnis utama intranet dalam bentuk visual, dan menggunakan platform untuk attack semua sistem security di network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



Bagaimana untuk Berkorelasi dengan IAM untuk Operasi Sederhana

## 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.

No.	IP	Hostname	MAC Address	OS	Type	Service (Port)	Status	Owner	Tags	Last Online	Operation
1	20.10.0.3	A-PC	fe:fc:fe:69:4f:80	windows	PC	-	Online	Windows1	-	2021-03-17 14:46:26	Details
2	20.10.0.8	C-PC	fe:fc:fe:15:fda:0	windows	Host	-	Online	-	-	2021-03-17 14:46:26	Details
3	20.10.0.8	B-PC	fe:fc:fe:64:aabc	windows	Host	-	Online	Windows2	-	2021-03-17 14:46:26	Details
4	20.10.0.10	WIN-6L5QG79TUR	fe:fc:fe:4ee9:27	windows	Server	-	Online	Server1	-	2021-03-17 14:46:26	Details
5	20.10.0.11	localhost.localdomain	fe:fc:fe:33:33	linux	Server	-	Online	-	-	2021-03-17 14:46:26	Details

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.**

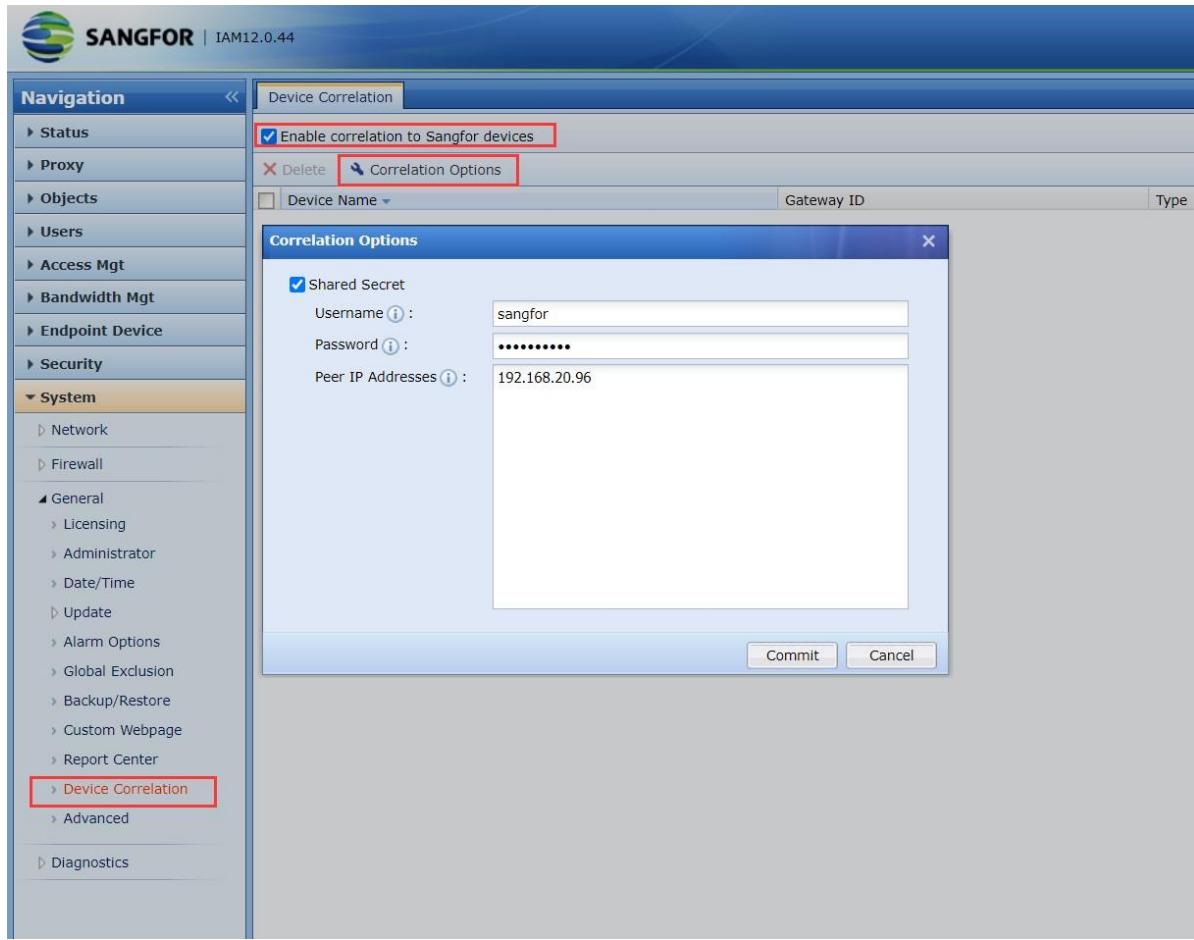
The screenshot shows the Sangfor Endpoint Secure interface. The left sidebar has tabs for Endpoints, Groups, Inventory, and Security Protection, with Security Protection selected. The main area shows a 'Groups' section with a tree view of 'Local Site' containing 'Ungrouped En...', 'Branch\_CN', 'Branch\_US', and 'HQ'. Below this is the 'Realtime File System Protection' section, which is currently active. It includes settings for protection level (High, Medium, Low), file types (Document, Script, Executable file, Compressed), scan options (skip files larger than 50 MB, scan compressed files up to 3 layers deep), engines (Sangfor Engine Zero, Gene Analytic Engine, Cloud-Based Engine), and action (Standard, Enhanced, No Action - Report Only). There is also a 'WebShell Detection' section with an enable checkbox.

## 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.

The screenshot shows the Sangfor IAM 12.0.44 interface. The navigation menu on the left has 'Security' selected, with 'Security Capabilities' highlighted. The main content area shows the 'Endpoint Security' section with 'Endpoint Secure' selected. Below it, there's a 'Logging In and Correlation to Endpoint Secure' section where the 'Endpoint Secure Server Address' is set to '20.10.0.100' and a 'Connect Now' button is present. There are also 'Highlights' sections for 'Artificial Intelligence, Accurate Identification' and 'Correlated & Responsive Remediation'.

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

The screenshot shows the Sangfor Endpoint Secure interface under the Security Capabilities tab. On the left, there's a sidebar with categories like Endpoint Security and Network Security. The main area displays the 'Endpoint Secure' service details, including its status as active, server address (20.10.0.100), and duration (188 days). It also shows metrics for connected endpoints (3) and correlated actions (0). The 'Highlights' section lists four key features: Artificial Intelligence, Accurate Identification; Correlated & Responsive Remediation; Multi-Layered Detection, Comprehensive Protection; and Broad Device, Platform & System Support.

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.

The screenshot shows the Sangfor Endpoint Secure interface with the 'System' tab selected. In the left sidebar, 'Agent Deployment' is highlighted. The main content area is titled 'Agent Deployment' and contains three options: 'Agent Installation on Physical Machines', 'Redirection to Agent Installer Download Page', and 'Correlation to Sangfor IAM'. Under 'Correlation to Sangfor IAM', there are instructions to copy a link from the IAM manager and a preview of the URL (https://20.10.0.100/ui/web\_install.php). A note says if the link becomes invalid, generate a new one.

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

## Bagaimana untuk Berkorelasi dengan IAM untuk Operasi Sederhana

The screenshot shows the Sangfor Security Capabilities interface. On the left, there's a sidebar with categories like Endpoint Security, Network Security, and more. The main area is titled "Endpoint Secure". A modal window titled "Reminder on Sangfor Endpoint Secure Installation" is open, with the "Enabled" checkbox checked. The "Applicable Object" field contains "0.0.0-255.255.255.255". Below it, there's a "Redirection URL" field with the value "https://20.10.0.100/ui/web\_install.php". Other fields include "Sangfor Endpoint Secure Platform" and "Interval(s): 300". Buttons for "OK" and "Cancel" are at the bottom right of the modal.

## 2.2 Konfigurasi Cyber Command

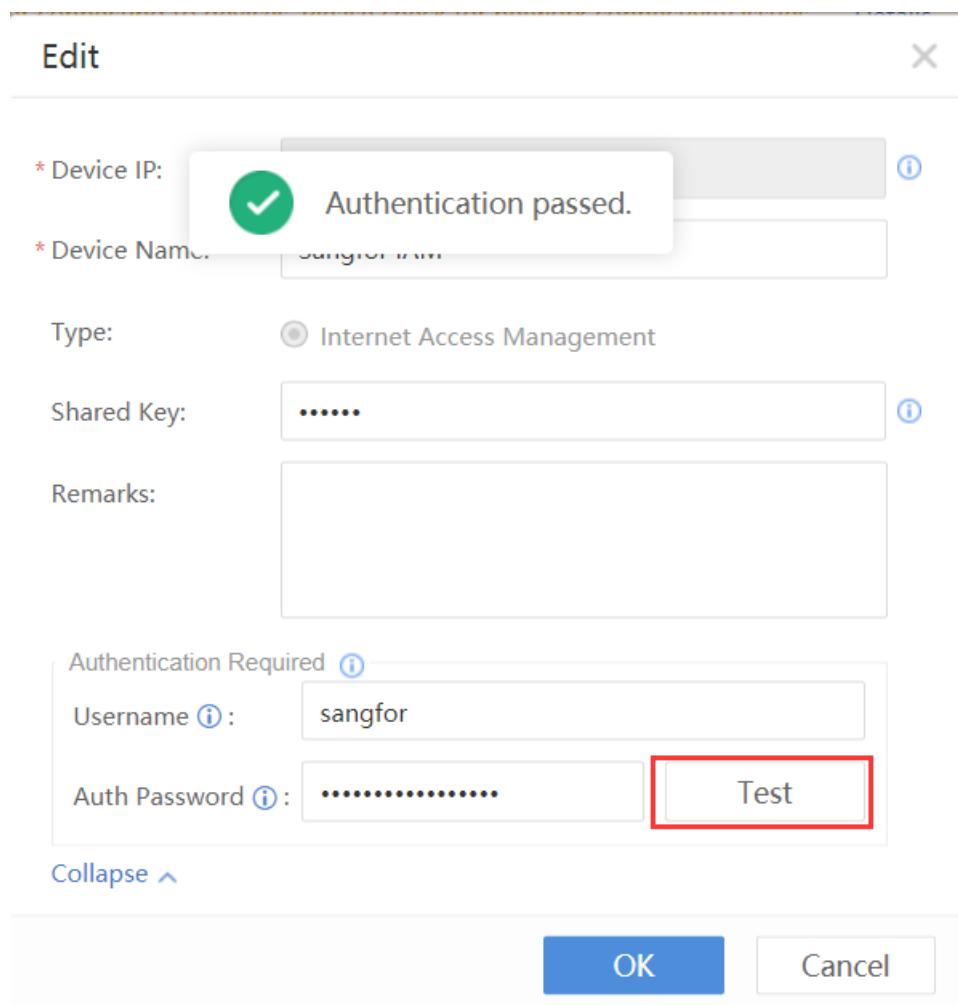
### 1. Pergi ke System->Correlated Devices-> Correlated Devices.

No.	Name (IP Address)	Type	IP Address	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 Generation Firewall	192.168.20.51	Af 8.0.26.345	Licenses Used	Simplified	6.54MB	65.52MB	776	2021-03-08 10:19:30	<span style="color: green;">Normal</span>	517	-
2	Sangfor Endpoint Secure	Endpoint Security	192.168.20.51	3.2.2	Licenses Used	Advanced	0B	0B	-	2021-03-08 10:17:14	<span style="color: green;">Normal</span>	0	-

### 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.



## 2.3 Konfigurasi Endpoint Secure

1. Pergi ke System Path.

Bagaimana untuk Berkorelasi dengan IAM untuk Operasi Sederhana

The screenshot shows the Holistic interface. On the left, there are two cards: one for NGAF (Online: 0, Offline: 0) and one for BBC (Online: 0, Offline: 0). Below each card, it says "Today's Synced Logs: 0" and "N/A (sync not supported)". On the right, a sidebar menu includes options like Threat Intelligence, Help, System, Service Packs, and Exit. At the bottom, there is a search bar and a table with columns: Synced Logs, Today's Logs, Last Synced, Status, Alerts (30 days), and Operation. The table shows a single row with the last sync date as 2021-03-16 16:11:18, status as Normal, and alerts as 0.

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

The screenshot shows the Cyber Command interface. The left sidebar has sections for System, Correlated Devices (which is selected and highlighted with a red box), Monitor, Update, Maintenance, and Databases. The main area is titled "Correlated Devices" and shows three device cards: Endpoint Secure (Online: 1, Offline: 0), NGAF (Online: 1, Offline: 0), and IAM (Connected: 1, Offline: 1). Below the cards, there is a "New" button (highlighted with a red box) and a table with columns: No., Name (IP Address), Type, IP Address, Version, Licensed, Sync Mode, Today's Synced Logs, and Total. The table contains two rows: one for Endpoint Secure (IP 192.168.20.51) and one for 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

The screenshot shows the Cyber Command interface with the 'Assets' tab selected. The main pane displays a table of discovered hosts. The table columns include No., IP, Hostname, MAC Address, OS, Type, Service (Port), Status, Owner, Tags, Last Online, and Operation. The data shows five hosts, all marked as 'Online'. The 'Owner' column lists 'Windows1', 'Windows2', 'Server1', and two entries for 'Windows3'. The 'Last Online' column shows dates from March 16, 2021.

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

This screenshot shows the 'Asset Details' view for host 20.10.0.3. The left side shows the same host list as the previous screenshot. The right panel, titled 'Asset Details' for '20.10.0.3', contains tabs for 'Attributes', 'Software', and 'Hardware'. Under 'Attributes', it shows the host is a Windows machine with IP 20.10.0.3, non-critical status, and owned by Windows1. It was discovered by 'Sangfor Endpoint Secure(1...)'. The 'Software' tab shows it's running windows. The 'Hardware' tab shows it's auto-discovered.

## Bab 3 Korelasi

### 3.1 Sinkronisasi Log ke Cyber Command

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

This screenshot shows the 'Security Events' page. It features a circular chart indicating 1 user, with 1 Infected and 0 Likely infected. Below it is a bar chart showing 18 security events, with Botnet being the most frequent. To the right is a list of hot events including 'Natural-X connected', 'GravitelyAT spy...', 'Ransomware Rancy', etc. At the bottom is a table of users and their threat counts. User 'sangfor' is listed with an IP of 20.10.0.3, a security rating of 'Infected', and a threat count of 18.

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

## Bagaimana untuk Berkorelasi dengan IAM untuk Operasi Sederhana

The screenshot shows the Sangfor IAM 2.0.44 interface. On the left, there's a navigation sidebar with options like Status, Proxy, Objects, Users, Access Mgt, Bandwidth Mgt, Endpoint Device, Security (Security Events and Security Capabilities), and System. The main area has tabs for Security Capabilities and Security Events. Under Security Events, it shows a timeline from 03-11 to 03-17 with a count of 153 events. Below this is a detailed table of security events:

No.	Time	Type	Dst IP	Threat Level	Action	Description	Data Packet	Threat Intelligence	Details
1	03-17 17:28:24	Botnet	8.8.4.4	Low	Reject	Host visits malicious domain name (cdptlyapp.on) or IP address (8.8.4.4) provided by threat actor	<a href="#">View</a>	<a href="#">View</a>	<a href="#">Details</a>
2	03-17 17:28:24	Botnet	8.8.8.8	Low	Reject	Host visits malicious domain name (cdptlyapp.on) or IP address (8.8.8.8) provided by threat actor	<a href="#">View</a>	<a href="#">View</a>	<a href="#">Details</a>
3	03-17 17:28:20	Botnet	8.8.4.4	Low	Reject	Host visits malicious domain name (cdptlyapp.on) or IP address (8.8.4.4) provided by threat actor	<a href="#">View</a>	<a href="#">View</a>	<a href="#">Details</a>
4	03-17 17:28:19	Botnet	8.8.8.8	Low	Reject	Host visits malicious domain name (cdptlyapp.on) or IP address (8.8.8.8) provided by threat actor	<a href="#">View</a>	<a href="#">View</a>	<a href="#">Details</a>
5	03-17 17:28:18	Botnet	8.8.8.8	Low	Reject	Host visits malicious domain name (cdptlyapp.on) or IP address (8.8.8.8) provided by threat actor	<a href="#">View</a>	<a href="#">View</a>	<a href="#">Details</a>
6	03-17 17:28:18	Botnet	8.8.4.4	Low	Reject	Host visits malicious domain name (cdptlyapp.on) or IP address (8.8.4.4) provided by threat actor	<a href="#">View</a>	<a href="#">View</a>	<a href="#">Details</a>
7	03-17 17:28:17	Botnet	8.8.8.8	Low	Reject	Host visits malicious domain name (cdptlyapp.on) or IP address (8.8.8.8) provided by threat actor	<a href="#">View</a>	<a href="#">View</a>	<a href="#">Details</a>
8	03-17 17:28:17	Botnet	8.8.4.4	Low	Reject	Host visits malicious domain name (cdptlyapp.on) or IP address (8.8.4.4) provided by threat actor	<a href="#">View</a>	<a href="#">View</a>	<a href="#">Details</a>
9	03-17 17:28:15	Botnet	8.8.4.4	Low	Reject	Host visits malicious domain name (cdptlyapp.on) or IP address (8.8.4.4) provided by threat actor	<a href="#">View</a>	<a href="#">View</a>	<a href="#">Details</a>
10	03-17 17:28:11	Botnet	8.8.4.4	Low	Reject	Host visits malicious domain name (cdptlyapp.on) or IP address (8.8.4.4) provided by threat actor	<a href="#">View</a>	<a href="#">View</a>	<a href="#">Details</a>
11	03-17 17:28:11	Botnet	8.8.8.8	Low	Reject	Host visits malicious domain name (update.7h4uk.com) or IP address (8.8.8.8) provided by threat actor	<a href="#">View</a>	<a href="#">View</a>	<a href="#">Details</a>
12	03-17 17:28:08	Botnet	8.8.4.4	Low	Reject	Host visits malicious domain name (update.7h4uk.com) or IP address (8.8.4.4) provided by threat actor	<a href="#">View</a>	<a href="#">View</a>	<a href="#">Details</a>
13	03-17 17:28:08	Botnet	8.8.8.8	Low	Reject	Host visits malicious domain name (update.7h4uk.com) or IP address (8.8.8.8) provided by threat actor	<a href="#">View</a>	<a href="#">View</a>	<a href="#">Details</a>
14	03-17 17:28:06	Botnet	8.8.8.8	Low	Reject	Host visits malicious domain name (update.7h4uk.com) or IP address (8.8.8.8) provided by threat actor	<a href="#">View</a>	<a href="#">View</a>	<a href="#">Details</a>
15	03-17 17:28:06	Botnet	8.8.4.4	Low	Reject	Host visits malicious domain name (update.7h4uk.com) or IP address (8.8.4.4) provided by threat actor	<a href="#">View</a>	<a href="#">View</a>	<a href="#">Details</a>
16	03-17 17:28:05	Botnet	8.8.4.4	Low	Reject	Host visits malicious domain name (update.7h4uk.com) or IP address (8.8.4.4) provided by threat actor	<a href="#">View</a>	<a href="#">View</a>	<a href="#">Details</a>
17	03-17 17:28:05	Botnet	8.8.8.8	Low	Reject	Host visits malicious domain name (update.7h4uk.com) or IP address (8.8.8.8) provided by threat actor	<a href="#">View</a>	<a href="#">View</a>	<a href="#">Details</a>
18	03-17 17:28:03	Botnet	8.8.4.4	Low	Reject	Host visits malicious domain name (update.7h4uk.com) or IP address (8.8.4.4) provided by threat actor	<a href="#">View</a>	<a href="#">View</a>	<a href="#">Details</a>
19	03-17 17:27:55	Botnet	8.8.4.4	Low	Reject	Host visits malicious domain name (update.7h4uk.com) or IP address (8.8.4.4) provided by threat actor	<a href="#">View</a>	<a href="#">View</a>	<a href="#">Details</a>

Kemudian, Anda dapat melihat scan task running di endpoint.

The screenshot shows the Protect Agent interface. On the left, there are icons for Security, Virus Scan, Realtime Protection, Tools, and AI. The main area displays a summary: "Quick scan, 6 threats detected" at 00:01:17 C:\Users\Administr...e-synch-l1-1-0.dll. It lists five scanned categories:

- System Processes:** 48 files scanned
- Startup Items:** 5 files scanned
- Drivers and Services:** 2 files scanned
- Critical System Files:** 106 files scanned

At the bottom, it shows "Security Engines: [icons]" and "Auto shut down your computer when scan completes" with a checkbox.

## Bagaimana untuk Berkorelasi dengan IAM untuk Operasi Sederhana

The screenshot shows the Sangfor Endpoint Secure interface. On the left, a navigation sidebar includes sections like Home, Response, Objects, Users, Access Mgt, Bandwidth Mgt, Evaluation Metrics, Security, Security Events, and Security Correlation. The main area has tabs for Security Log and Security Events. A central window displays a timeline of security events from April 11 to April 17, 2021. One event is highlighted: "Malicious File: c:\users\administrator\desktop\file.malicious" with a file hash of MD5(0X9C7F1441D9B6062442F) and a creation time of 2021-04-17 18:11:39. To the right is a "Threat Analysis" window showing a chart of threat levels over time, with a red dot indicating the analyzed event. Below the chart is a table of threat details.

No.	Endpoint	Type	File Hash	Severity	Operator
1	85-07-17-49:53	Ransom virus	MD5(0X9C7F1441D9B6062442F)	High	Suspect, Threat, Ignore Buy Data Analytics
2	85-07-17-49:53	Other viruses	MD5(0X9C7F1441D9B6062442F)	Medium	Suspect, Threat, Ignore Buy Data Analytics
3	85-07-17-49:53	Other viruses	MD5(0X9C7F1441D9B6062442F)	Medium	Suspect, Threat, Ignore Buy Data Analytics
4	85-07-17-49:53	Other viruses	MD5(0X9C7F1441D9B6062442F)	Medium	Suspect, Threat, Ignore Buy Data Analytics
5	85-07-17-49:53	Other viruses	MD5(0X9C7F1441D9B6062442F)	Medium	Suspect, Threat, Ignore Buy Data Analytics
6	85-07-17-49:53	Ransom virus	MD5(0X9C7F1441D9B6062442F)	High	Suspect, Threat, Ignore Buy Data Analytics
7	85-07-17-49:53	Ransom virus	MD5(0X9C7F1441D9B6062442F)	High	Suspect, Threat, Ignore Buy Data Analytics
8	85-07-17-49:53	Ransom virus	MD5(0X9C7F1441D9B6062442F)	High	Suspect, Threat, Ignore Buy Data Analytics
9	85-07-17-49:53	Ransom virus	MD5(0X9C7F1441D9B6062442F)	High	Suspect, Threat, Ignore Buy Data Analytics
10	85-07-17-49:53	Ransom virus	MD5(0X9C7F1441D9B6062442F)	High	Suspect, Threat, Ignore Buy Data Analytics
11	85-07-17-49:49	Ransom virus	MD5(0X9C7F1441D9B6062442F)	High	Suspect, Threat, Ignore Buy Data Analytics
12	85-07-17-49:36	Ransom virus	MD5(0X9C7F1441D9B6062442F)	High	Suspect, Threat, Ignore Buy Data Analytics
13	85-07-17-49:36	Ransom virus	MD5(0X9C7F1441D9B6062442F)	High	Suspect, Threat, Ignore Buy Data Analytics

This screenshot shows the Sangfor Endpoint Secure interface with the Response tab selected. It displays a dashboard with endpoint status counts: 1 Victim Endpoints, 3 Compromised, 0 Critical, 0 Suspicious, and 0 Isolated. Below is a table of endpoints, with one row highlighted for further details.

No.	Endpoint	Group	Severity	Security Events
1	Windows 10 (85.07.0.8)	Ungrouped Endpoints	Compromised	Pending/Total Threats: 41 / 39 Last Detected: 2021-04-17 18:11:39 File: Include

The screenshot shows the Cyber Command interface with the Response tab selected. It displays a dashboard for host risk analysis. Key statistics shown are 2/56 Hosts (Risk: High), 2 Compromised hosts, 0 High risk, 0 Medium risk, and 0 Low risk. Below is a detailed view of host risks, showing two hosts: A-PC and B-PC, both marked as fixed with a status of "Fixed (Correlated)".

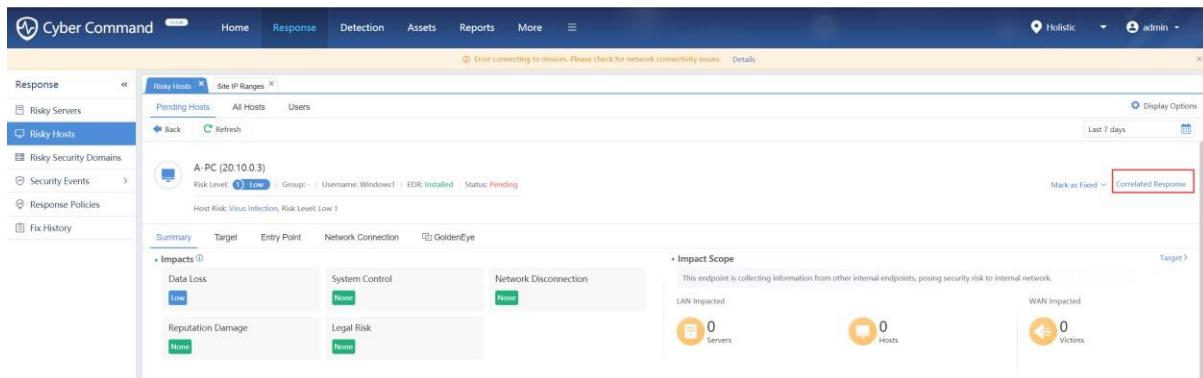
This screenshot provides a detailed view of host risk analysis for host A-PC (IP 20.10.0.3). The host is marked as Compromised. The interface shows various attack stages: Vuln Detected, Ever Attacked, C2C Comes, Scan Initiated, Latently Propagated, and Date Theft. Impact scopes include LAN Impacted (0 servers) and WAN Impacted (0 hosts). Risk levels are categorized as Comprromised, High, and Low. A timeline at the bottom tracks the progression from April 11 to April 17, 2021.

Bagaimana untuk Berkorelasi dengan IAM untuk Operasi Sederhana

## 3.2 Response di Cyber Command

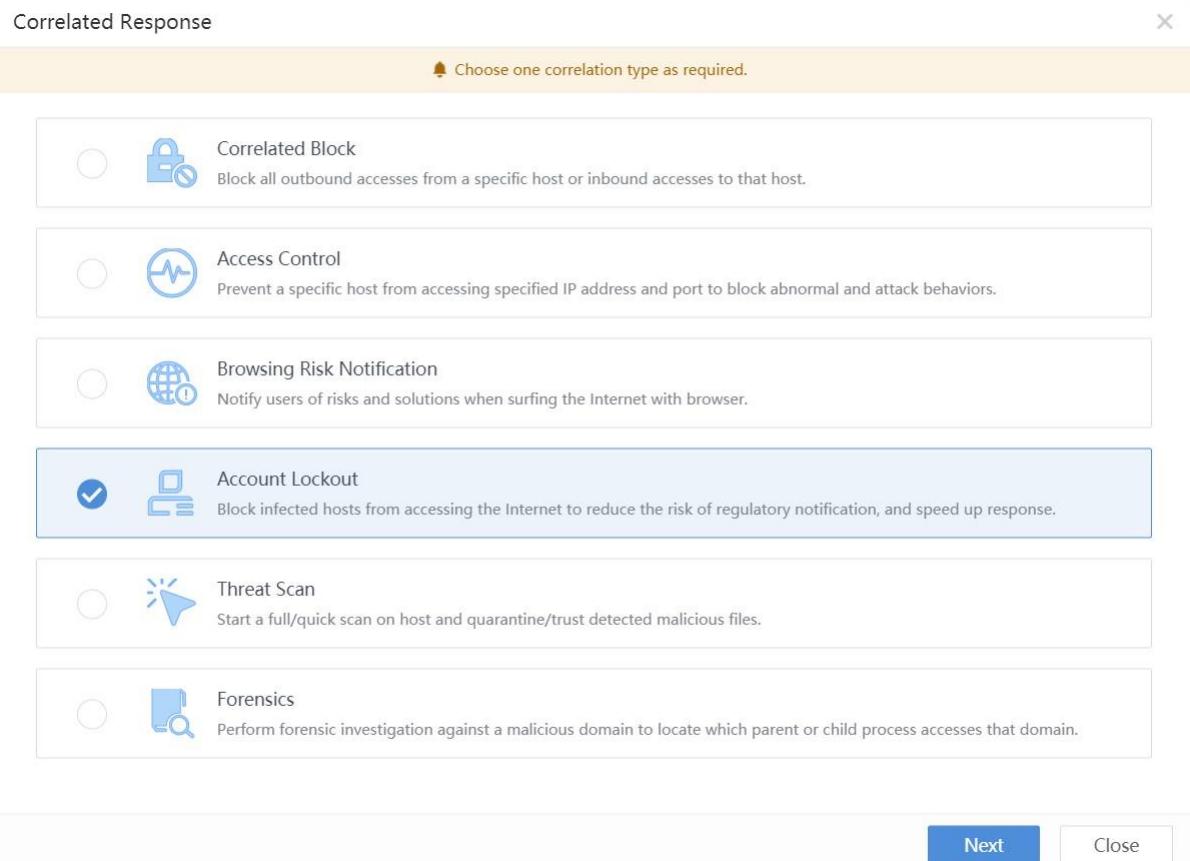
### 3.2.1 Lockout Account

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



The screenshot shows the Cyber Command web interface. On the left, there's a sidebar with 'Response' selected, followed by 'Risky Servers', 'Risky Hosts' (which is currently active), 'Risky Security Domains', 'Security Events', 'Response Policies', and 'Fix History'. The main content area has tabs for 'Pending Hosts', 'All Hosts', and 'Users'. Below these tabs, there's a specific host detail for 'A-PC (20.10.0.3)'. The host details include: Risk Level: Low (Linux), Group: -, Username: Windows1, EDR: Installed, Status: Pending, and Host Risk: Virus Infection, Risk Level: Low 1. To the right of the host details, there's a 'Mark as Fixed' dropdown with 'Correlated Response' highlighted by a red box. Below the host details, there are sections for 'Impacts' (Data Loss: Low, System Control: None, Network Disconnection: None, Reputation Damage: None, Legal Risk: None) and 'Impact Scope' (LAN Impacted: 0 Servers, WAN Impacted: 0 Hosts, Target: 0 Victims).

2. Pilih Account Lockout.



The screenshot shows a modal dialog titled 'Correlated Response'. At the top, it says 'Choose one correlation type as required.' Below are several options, each with an icon and a description:

-  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.

At the bottom right of the dialog are 'Next' and 'Close' buttons.

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

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

IP Address: Sangfor IAM(192.168.20.52)

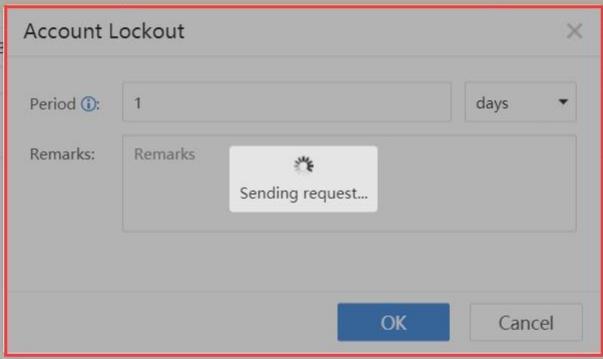
Account Lockout

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 authenticat...	2021-03-05 11:07:37Login	292 hours 04 minutes 47 s...	
3	20.10.0.9	/	20.10.0.9	Verifying...	Open authenticat...	2021-03-04 09:21:50Login	317 hours 50 minutes 34 s...	
4	20.10.0.100	/	20.10.0.100	Verifying...	Open authenticat...	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(192.168.22.5)

#### Browsing Risk Notification

Start

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.

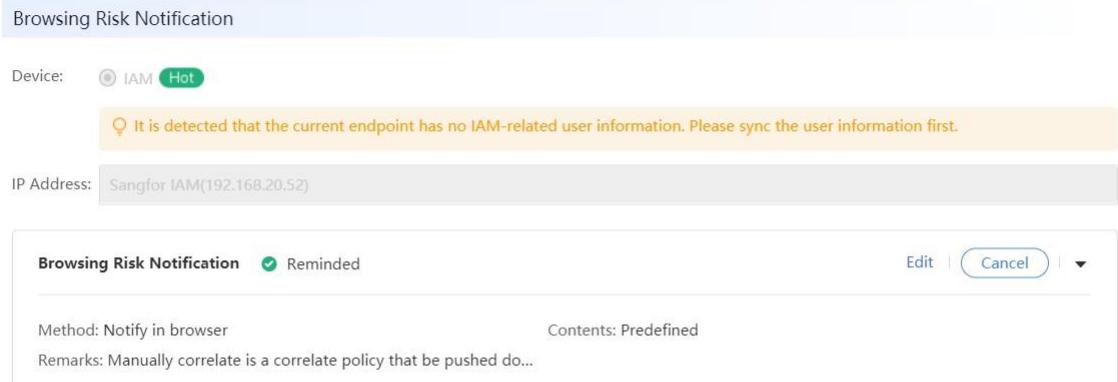
IP Address: Sangfor IAM(192.168.20.52)

Browsing Risk Notification Reminded Edit | Cancel | ▾

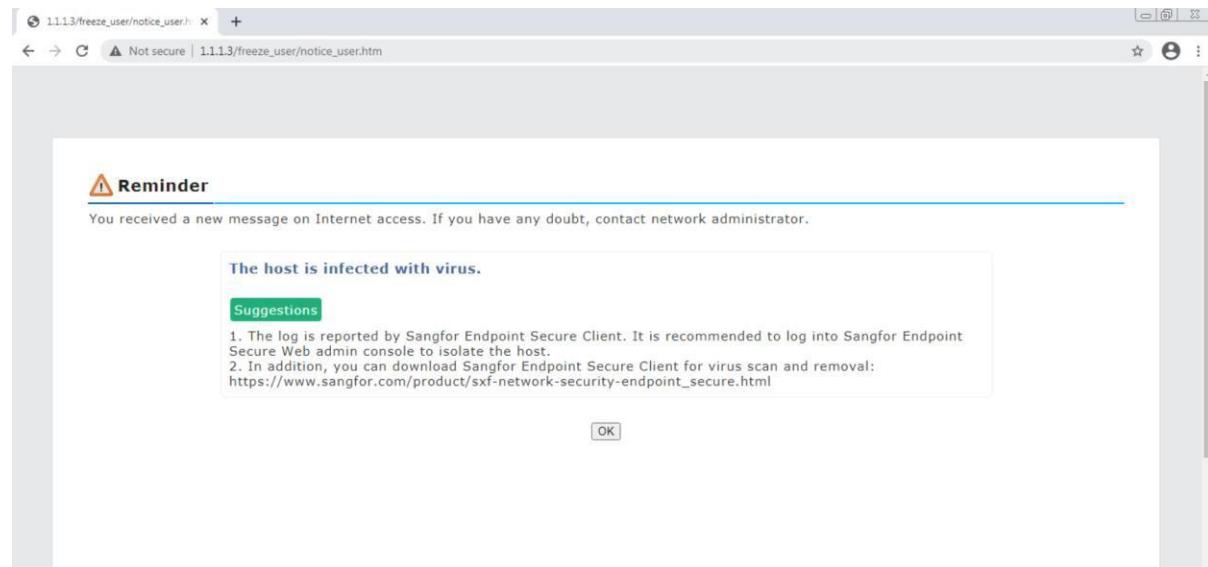
Method: Notify in browser Contents: Predefined

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