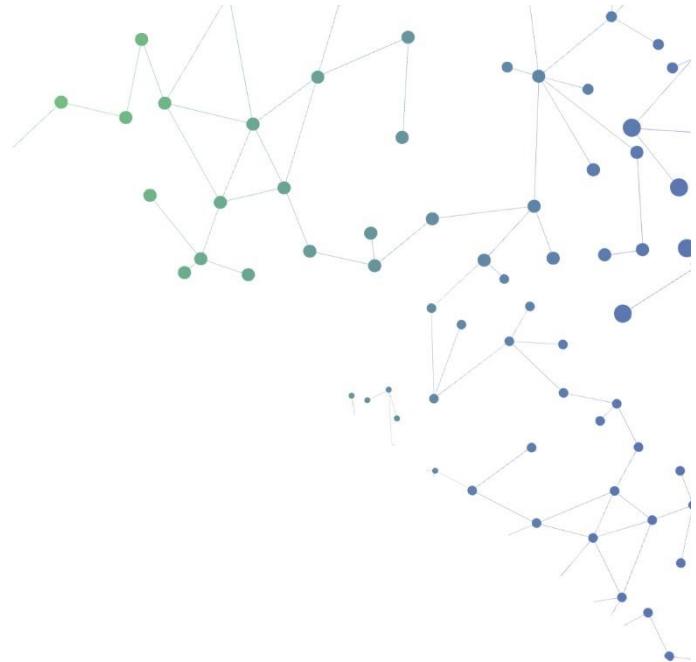




SANGFOR



# NGAF

**Pedoman Terbaik untuk Skenario Menghubungkan  
NGAF ke Platform-X untuk Test Security Log  
Presentation  
Versi 8.0.26**



## Perubahan Data

Tanggal	Keterangan Perubahan
NOV 2, 2019	Rilis dokumen.
May 17, 2021	Pembaruan dokumen.

# DAFTAR ISIS

BAB 1 Konfigurasi Koneksi .....	1
BAB 2 Buat Pencatatan Keamanan .....	2

# BAB 1 Konfigurasi Koneksi

## 1. Tambahkan perangkat cabang pada Platform-X.

The screenshot shows the 'Assets' tab selected in the top navigation bar. On the left, there's a sidebar with 'Branch Device' selected. The main area displays a list of branches: Makati, XCENTRAL\_EDR, Nishat, MK, ABC, and Master. A red box highlights the 'New' button at the top of the list. Below the list, there are sections for 'Virtual Machines' and 'Policy Template' with various status indicators like 'Offline', 'Normal', and 'Inactivated'.

## 2. Konfigur nama dan "Access Token" perangkat untuk perangkat cabang.

The screenshot shows the 'Assets' tab selected. A modal dialog box titled 'Add Branch' is open in the center. It contains fields for 'Branch Name' (Master), 'Branch Device' (NGAF), 'Access Token' (123456), 'Geo Location' (Malaysia), and 'Group' (All). At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

## 3. Rekam CorpID pada kiri atas dari Platform-X

The screenshot shows the 'Assets' tab selected. The main area displays the same list of branches as the previous screen: Makati, XCENTRAL\_EDR, Nishat, MK, ABC, and Master. The 'Master' branch is highlighted with a red box. The 'Status' column for the Master branch shows 'Inactivated' with a yellow warning icon.

## 4. Login ke konsol NGAF, masukan CorpID dan Access Token, dll.

## Best Practice\_NGAF Correlate to Platform-X to Test Security Log Presentation

The screenshot shows the Sangfor NGAF interface. On the left, the navigation menu includes 'Cloud Correlation Options' under 'Next Gen Security System'. In the center, there's a 'Cloud Correlation Options' panel with two sections: 'Neural-X Unknown Threat Update' (Activated) and 'Platform-X' (Not activated). The 'Platform-X' section has fields for CorpID (969939873), Device Name (Master\_NGAF), and Access Token (\*\*\*\*\*). A 'Connect' button is present. To the right, there's a detailed description of 'Platform-X - How to Subscribe?' which highlights its benefits like centralized operations and maintenance of security devices, steps for subscription, and highlights such as integrated and visible security, real-time threat alert, intelligent threat defense, and professional security guide.

5. Setelah menunggu 1-3 menit, anda dapat melihat NGAF telah terkoneksi pada Platform-X dan online.

This screenshot is similar to the previous one but shows the 'Platform-X' status as 'Activated' with a green checkmark icon. The rest of the interface and details remain the same, indicating a successful connection.

## BAB 2 Buat Pencatatan Keamanan

1. Gunakan perintah untuk membuat pencatatan log in secara senyap

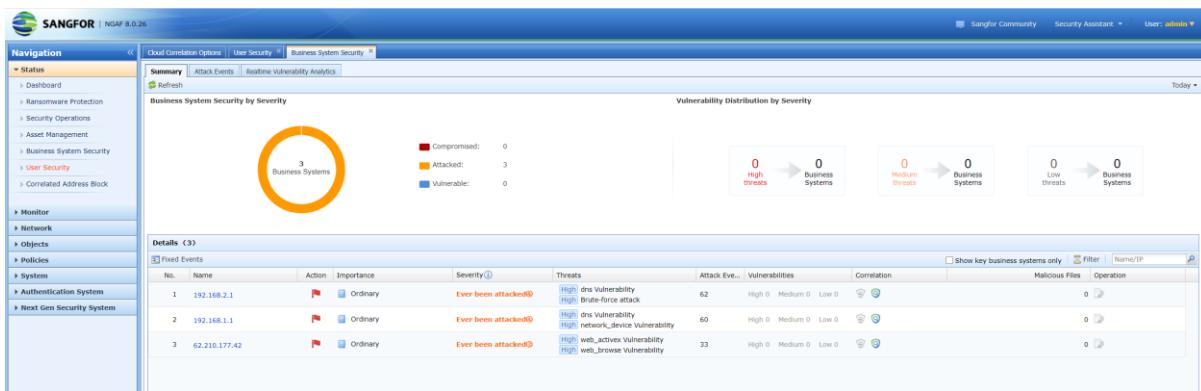
Jalankan perintah: **audit\_log -t waf -T 43 -c 100 -o asset'IP** untuk membuat pencatatan kejadian

Jalankan perintah: **audit\_log -t ips -s 100 -r hacker'IP -o asset'IP -c 100** untuk membuat pencatatan kejadian peretasan lebih terperinci.

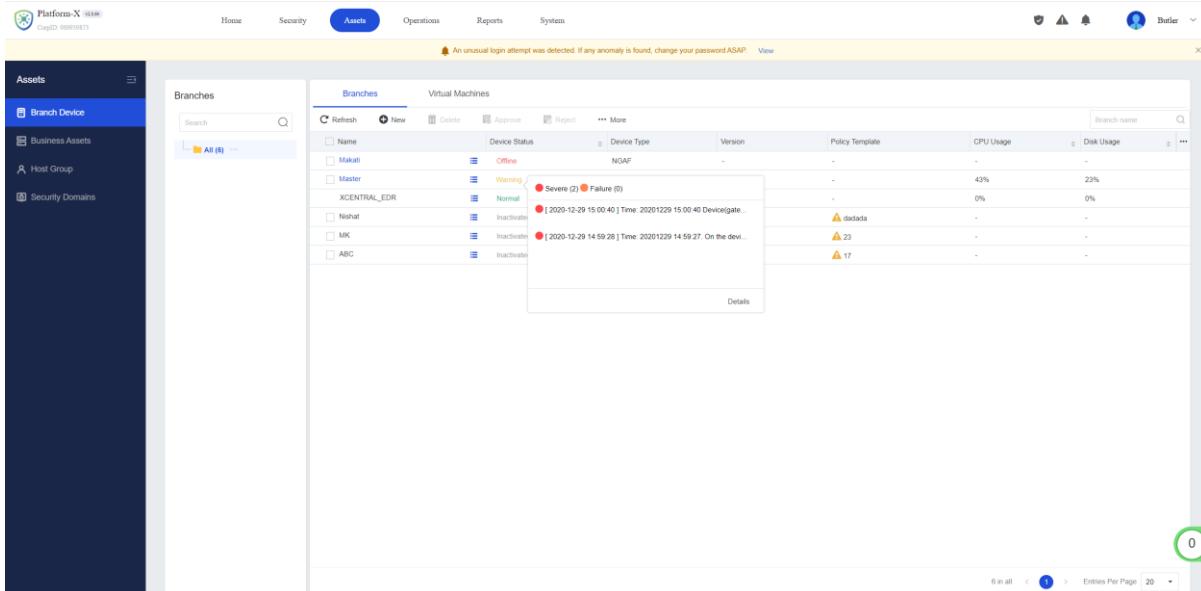
```
AF8.0.26.345 /var/log # audit_log -t ips -s 100 -r 62.210.177.42 -o 192.168.2.1 -c 100
create ini file success: /fwlog/config/audit_log.ini
config file changed, wait fwlog for 8 seconds...
wait end...
start send log to fwlog...
finished: 100
AF8.0.26.345 /var/log # audit_log -t ips -s 100 -r 62.210.177.42 -o 192.168.1.1 -c 100
start send log to fwlog...
finished: 100
AF8.0.26.345 /var/log #
```

## Best Practice\_NGAF Correlate to Platform-X to Test Security Log Presentation

2. setelah 1-2 menit, anda dapat melihat pencatatan log sehubungan dengan keamanan telah dibuat pada NGAF.



3. Anda dapat melihat peringatan dari kejadian yang berhubungan dengan keamanan pada Platform-X.





**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