NGAF

Pedoman terbaik untuk Skenario_Integrated Coorelation & Response dengan Endpoint Secure

Versi 8.0.17

Perubahan Data

Tanggal	Keterangan Perubahan
June 09, 2020	Versi 8.0.17 rilis dokumen.
Mar 18, 2021	Pembaruan Dokumen.
May 17, 2021	Pembaruan Dokumen.

DAFTAR ISI

BAB 1 Keterangan Fungsi

ES dapat terkoneksi dengan NGAF untuk proteksi PC pengguna melawan virus.

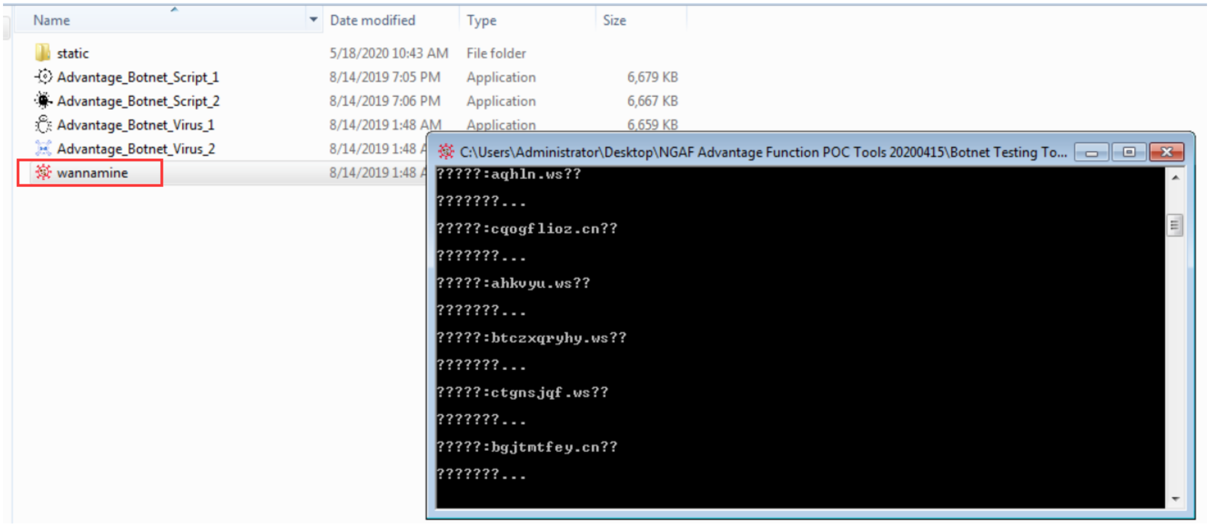
BAB 2 Rekomendasi Pedoman

2.1 Skenario:

Pada perusahaan besar IT mengalami ancaman keamanan internal dan eksternal sejak lama. setelah membeli NGAF dan ES Sangfor secara bersama diharapkan dapat melawan ancaman keamanan tersebut.

2.2 Test Tools

1. Untuk menguji Botnet, anda dapat menggunakan **SANGFOR_NGAF_v8.0.17_Best Practice_Integrated Coorelation & Response with Endpoint Secure.7z**, cari di PMO. Jalankan wannamine.exe di PC, wannamine.exe akan memcoba menggunakan DNS untuk mencari URL dari Botnet, tetapi sebenarnya tidak akan mengakses URL dari Botnet...



Name	Date modified	Type	Size
static	5/18/2020 10:43 AM	File folder	
Advantage_Botnet_Script_1	8/14/2019 7:05 PM	Application	6,679 KB
Advantage_Botnet_Script_2	8/14/2019 7:06 PM	Application	6,667 KB
Advantage_Botnet_Virus_1	8/14/2019 1:48 AM	Application	6,659 KB
Advantage_Botnet_Virus_2	8/14/2019 1:48 A		
wannamine	8/14/2019 1:48 A		

C:\Users\Administrator\Desktop\NGAF Advantage Function POC Tools 20200415\Botnet Testing To...

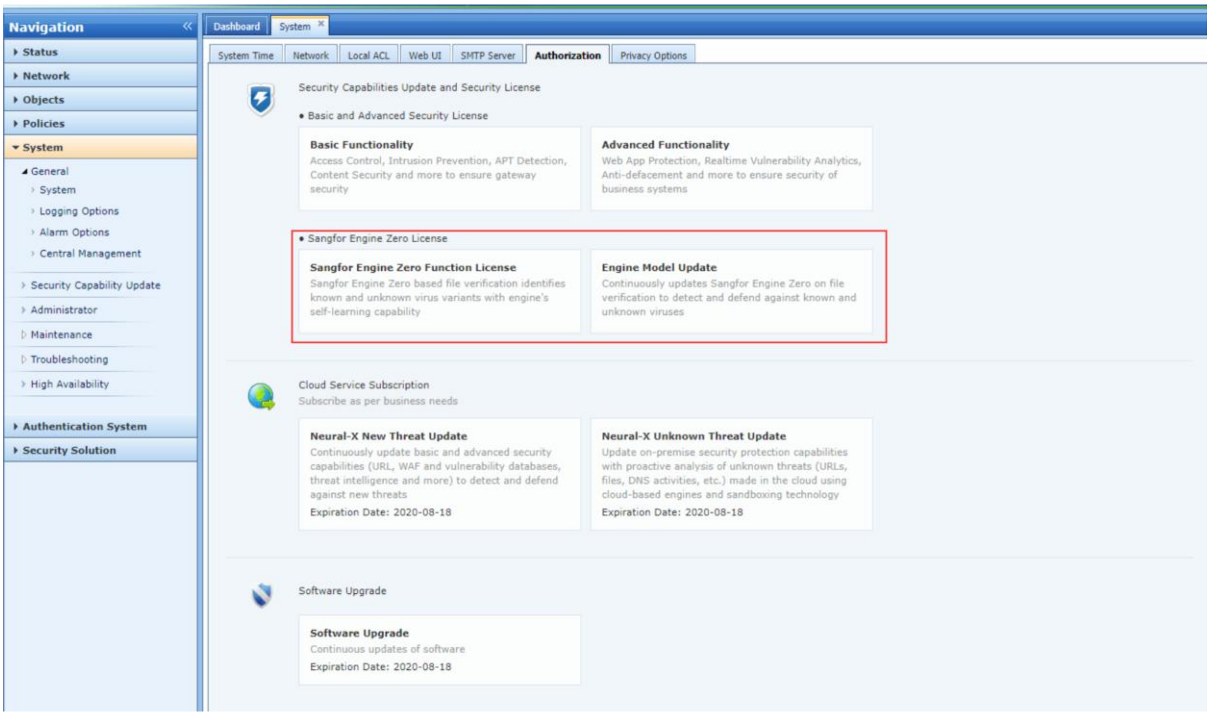
```
?????:aqhln.ws??
???????...
?????:cqogflioz.cn??
???????...
?????:ahkvyu.ws??
???????...
?????:btczxqryhy.ws??
???????...
?????:ctgnsjqf.ws??
???????...
?????:bgjtmtfey.cn??
???????...
```

2. Ketika anda menjalankan program, mungkin akan terjadi kesalahan terkait api-ms-win-crt-runtime-l1-1-0.dll, Jadi disarangkan untuk mengunduh **Visual C++ Redistributable Runtimes All-in-One** dan menginstall semua yang berkaitan dengan Visual C runtime libraries.

Catatan: Sistem Operasi yang berbeda akan muncul kesalahan yang berbeda. Anda dapat mencari solusi tersebut di Internet, akan tetapi biasanya kasus kesalahan tersebut adalah file Visual C Runtimes yang hilang.

BAB 3 Konfigurasi

1. Periksa apakah NGAF diperbolehkan.



Security Capabilities Update and Security License

- Basic and Advanced Security License

Basic Functionality
Access Control, Intrusion Prevention, APT Detection, Content Security and more to ensure gateway security

Advanced Functionality
Web App Protection, Realtime Vulnerability Analytics, Anti-defacement and more to ensure security of business systems

- Sangfor Engine Zero License

Sangfor Engine Zero Function License
Sangfor Engine Zero based file verification identifies known and unknown virus variants with engine's self-learning capability

Engine Model Update
Continuously updates Sangfor Engine Zero on file verification to detect and defend against known and unknown viruses

Cloud Service Subscription
Subscribe as per business needs

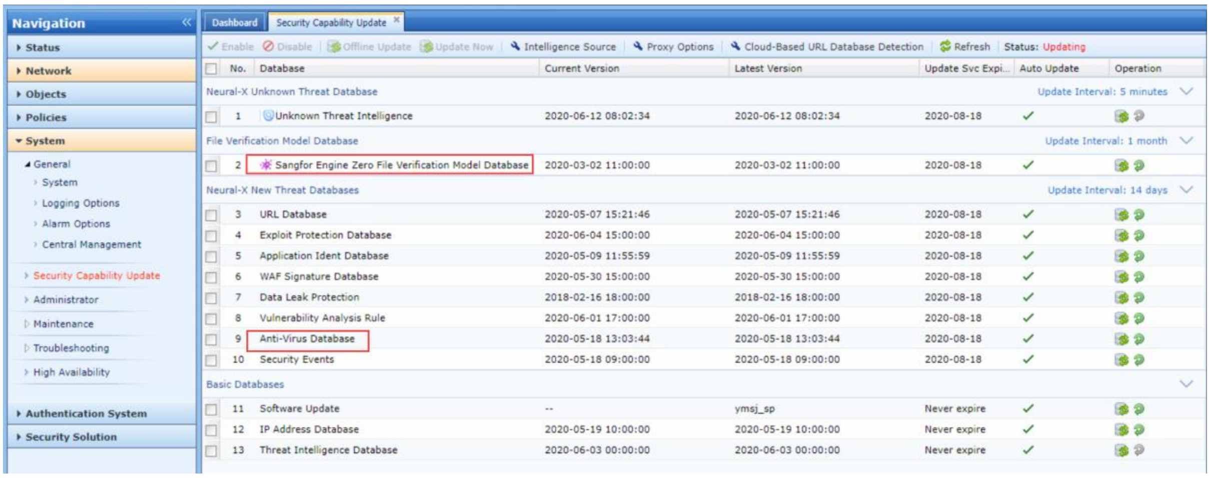
Neural-X New Threat Update
Continuously update basic and advanced security capabilities (URL, WAF and vulnerability databases, threat intelligence and more) to detect and defend against new threats
Expiration Date: 2020-08-18

Neural-X Unknown Threat Update
Update on-premise security protection capabilities with proactive analysis of unknown threats (URLs, files, DNS activities, etc.) made in the cloud using cloud-based engines and sandboxing technology
Expiration Date: 2020-08-18

Software Upgrade

Software Upgrade
Continuous updates of software
Expiration Date: 2020-08-18

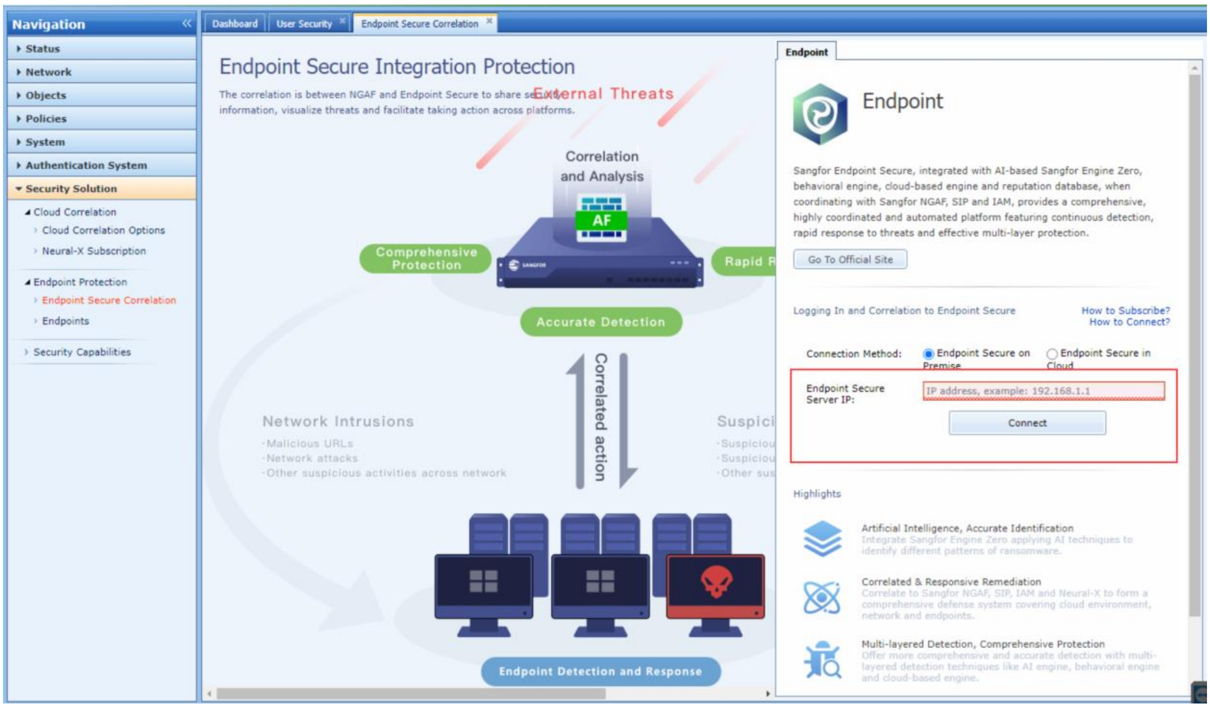
2. Pastikan telah diperbaharui sampai yang terbaru.



Status: Updating

□	No.	Database	Current Version	Latest Version	Update Svc Expi...	Auto Update	Operation
Neural-X Unknown Threat Database							Update Interval: 5 minutes
□	1	Unknown Threat Intelligence	2020-06-12 08:02:34	2020-06-12 08:02:34	2020-08-18	✓	
File Verification Model Database							Update Interval: 1 month
□	2	Sangfor Engine Zero File Verification Model Database	2020-03-02 11:00:00	2020-03-02 11:00:00	2020-08-18	✓	
Neural-X New Threat Databases							Update Interval: 14 days
□	3	URL Database	2020-05-07 15:21:46	2020-05-07 15:21:46	2020-08-18	✓	
□	4	Exploit Protection Database	2020-06-04 15:00:00	2020-06-04 15:00:00	2020-08-18	✓	
□	5	Application Ident Database	2020-05-09 11:55:59	2020-05-09 11:55:59	2020-08-18	✓	
□	6	WAF Signature Database	2020-05-30 15:00:00	2020-05-30 15:00:00	2020-08-18	✓	
□	7	Data Leak Protection	2018-02-16 18:00:00	2018-02-16 18:00:00	2020-08-18	✓	
□	8	Vulnerability Analysis Rule	2020-06-01 17:00:00	2020-06-01 17:00:00	2020-08-18	✓	
□	9	Anti-Virus Database	2020-05-18 13:03:44	2020-05-18 13:03:44	2020-08-18	✓	
□	10	Security Events	2020-05-18 09:00:00	2020-05-18 09:00:00	2020-08-18	✓	
Basic Databases							
□	11	Software Update	--	ymsj_sp	Never expire	✓	
□	12	IP Address Database	2020-05-19 10:00:00	2020-05-19 10:00:00	Never expire	✓	
□	13	Threat Intelligence Database	2020-06-03 00:00:00	2020-06-03 00:00:00	Never expire	✓	

3. Konfigurasi untuk menghubungkan NGAF dan ES, anda hanya perlu mengisi IP dari ES.



Endpoint Secure Integration Protection

The correlation is between NGAF and Endpoint Secure to share security information, visualize threats and facilitate taking action across platforms.

Endpoint

Sangfor Endpoint Secure, integrated with AI-based Sangfor Engine Zero, behavioral engine, cloud-based engine and reputation database, when coordinating with Sangfor NGAF, SIP and IAM, provides a comprehensive, highly coordinated and automated platform featuring continuous detection, rapid response to threats and effective multi-layer protection.

Logging In and Correlation to Endpoint Secure

Connection Method: ● Endpoint Secure on Premise ○ Endpoint Secure in Cloud

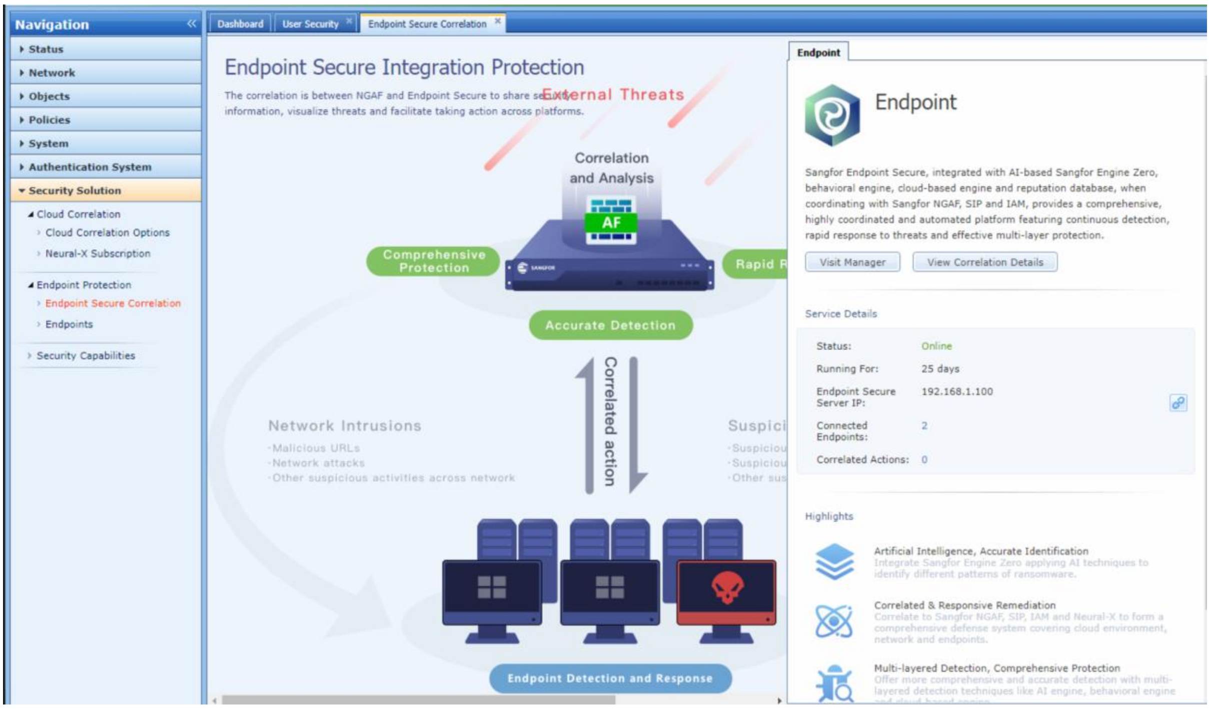
Endpoint Secure Server IP: IP address, example: 192.168.1.1

Highlights

Artificial Intelligence, Accurate Identification
Integrate Sangfor Engine Zero applying AI techniques to identify different patterns of ransomware.

Correlated & Responsive Remediation
Correlate to Sangfor NGAF, SIP, IAM and Neural-X to form a comprehensive defense system covering cloud environment, network and endpoints.

Multi-layered Detection, Comprehensive Protection
Offer more comprehensive and accurate detection with multi-layered detection techniques like AI engine, behavioral engine and cloud-based engine.



Endpoint Secure Integration Protection

The correlation is between NGAF and Endpoint Secure to share security information, visualize threats and facilitate taking action across platforms.

Endpoint

Sangfor Endpoint Secure, integrated with AI-based Sangfor Engine Zero, behavioral engine, cloud-based engine and reputation database, when coordinating with Sangfor NGAF, SIP and IAM, provides a comprehensive, highly coordinated and automated platform featuring continuous detection, rapid response to threats and effective multi-layer protection.

Service Details

Status: Online
Running For: 25 days
Endpoint Secure Server IP: 192.168.1.100
Connected Endpoints: 2
Correlated Actions: 0

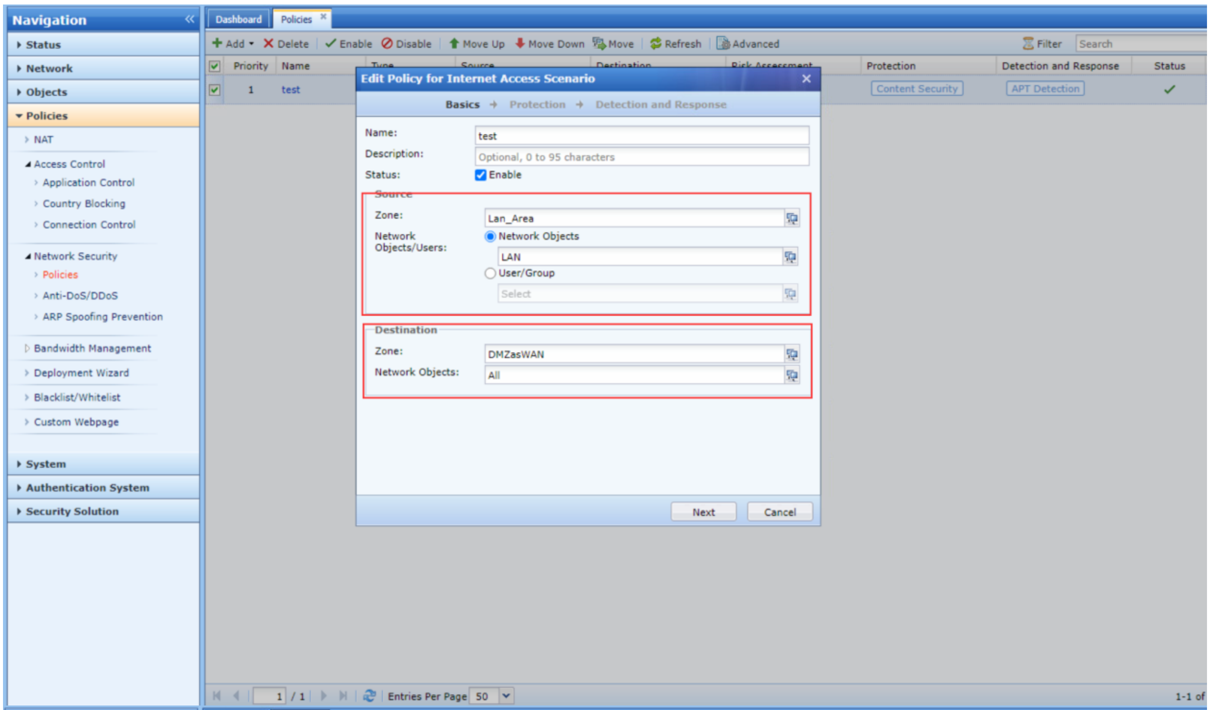
Highlights

Artificial Intelligence, Accurate Identification
Integrate Sangfor Engine Zero applying AI techniques to identify different patterns of ransomware.

Correlated & Responsive Remediation
Correlate to Sangfor NGAF, SIP, IAM and Neural-X to form a comprehensive defense system covering cloud environment, network and endpoints.

Multi-layered Detection, Comprehensive Protection
Offer more comprehensive and accurate detection with multi-layered detection techniques like AI engine, behavioral engine and cloud-based engine.

4. Konfigurasi Security policy dan anda harus memilih sumber dan tujuan yang benar, atau policy tidak akan berfungsi.



Priority	Name	Protection	Detection and Response	Status
1	test	Content Security	APT Detection	✓

Edit Policy for Internet Access Scenario

Name: test

Description: Optional, 0 to 95 characters

Status: ☑ Enable

Source

Zone: Lan_Area

Network Objects/Users: ● Network Objects

LAN

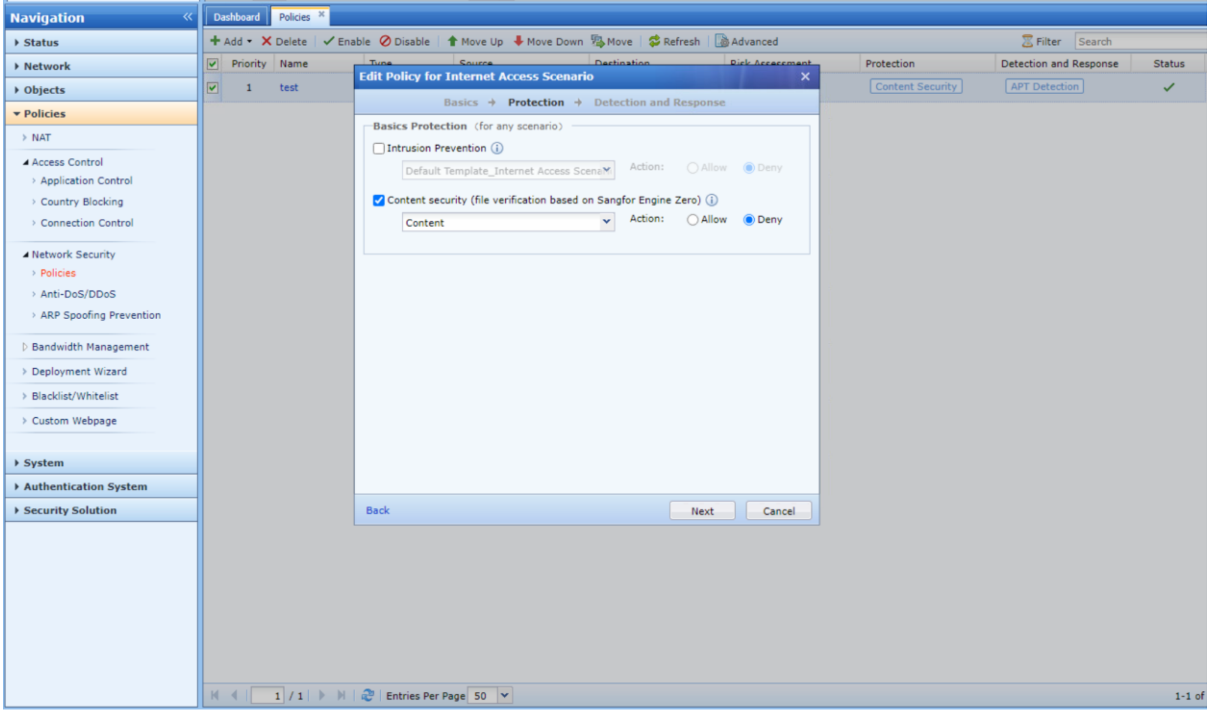
○ User/Group

Select

Destination

Zone: DMZasWAN

Network Objects: All



Priority	Name	Protection	Detection and Response	Status
1	test	Content Security	APT Detection	✓

Edit Policy for Internet Access Scenario

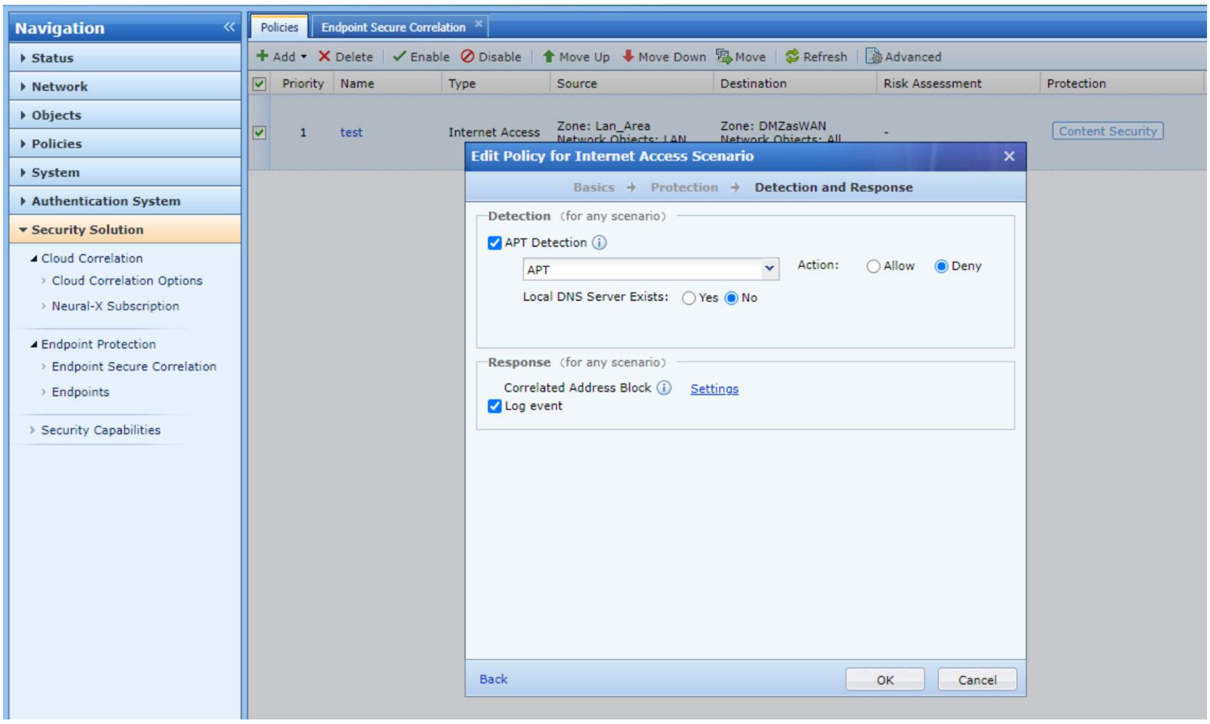
Basics Protection (for any scenario)

□ Intrusion Prevention

Default Template_Internet Access Scena Action: ○ Allow ● Deny

☑ Content security (file verification based on Sangfor Engine Zero)

Content Action: ○ Allow ● Deny



Priority	Name	Type	Source	Destination	Risk Assessment	Protection
1	test	Internet Access	Zone: Lan_Area Network Objects: LAN	Zone: DMZasWAN Network Objects: All	-	Content Security

Edit Policy for Internet Access Scenario

Detection (for any scenario)

☑ APT Detection

APT

Action: ○ Allow ● Deny

Local DNS Server Exists: ○ Yes ● No

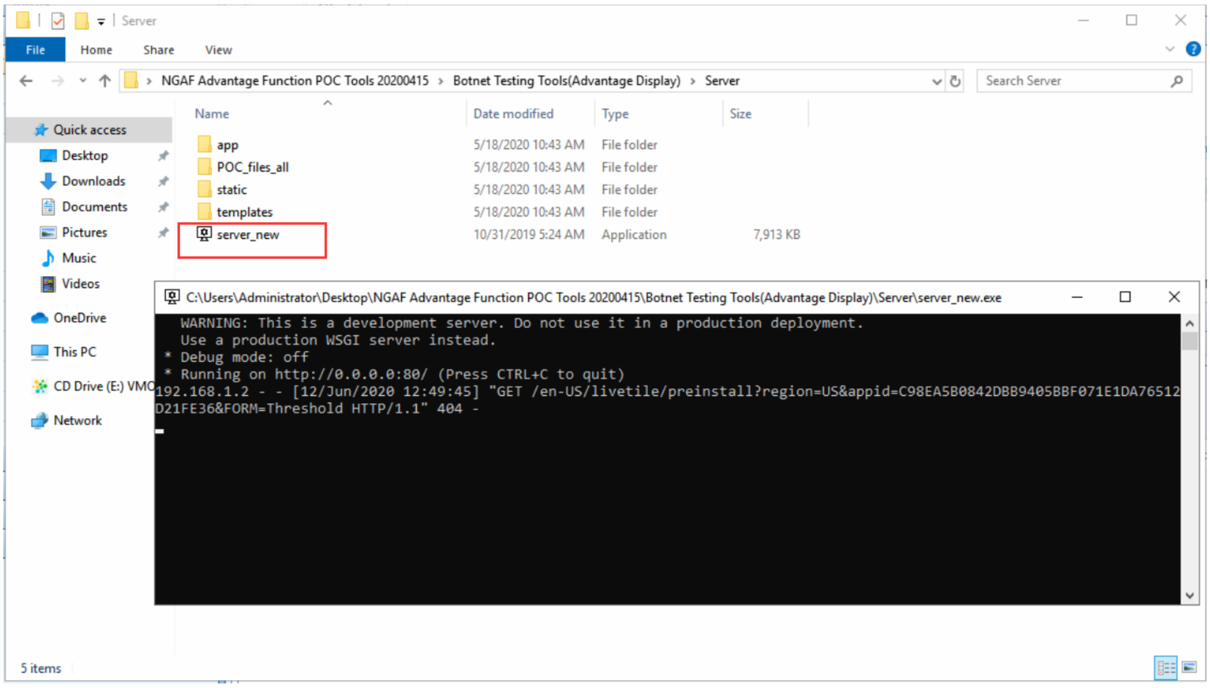
Response (for any scenario)

Correlated Address Block Settings

☑ Log event

1. Penyerang menjebak pengguna LAN untuk memasukan perangkat USB yang tidak dikenal, sehingga memicu virus worm [wannamine.exe] dan AF memblokir kerja yang mengirimkan trafik keluar menuju ke alamat domain yang berbahaya.

Jalankan Server_new.exe pada PC Server:

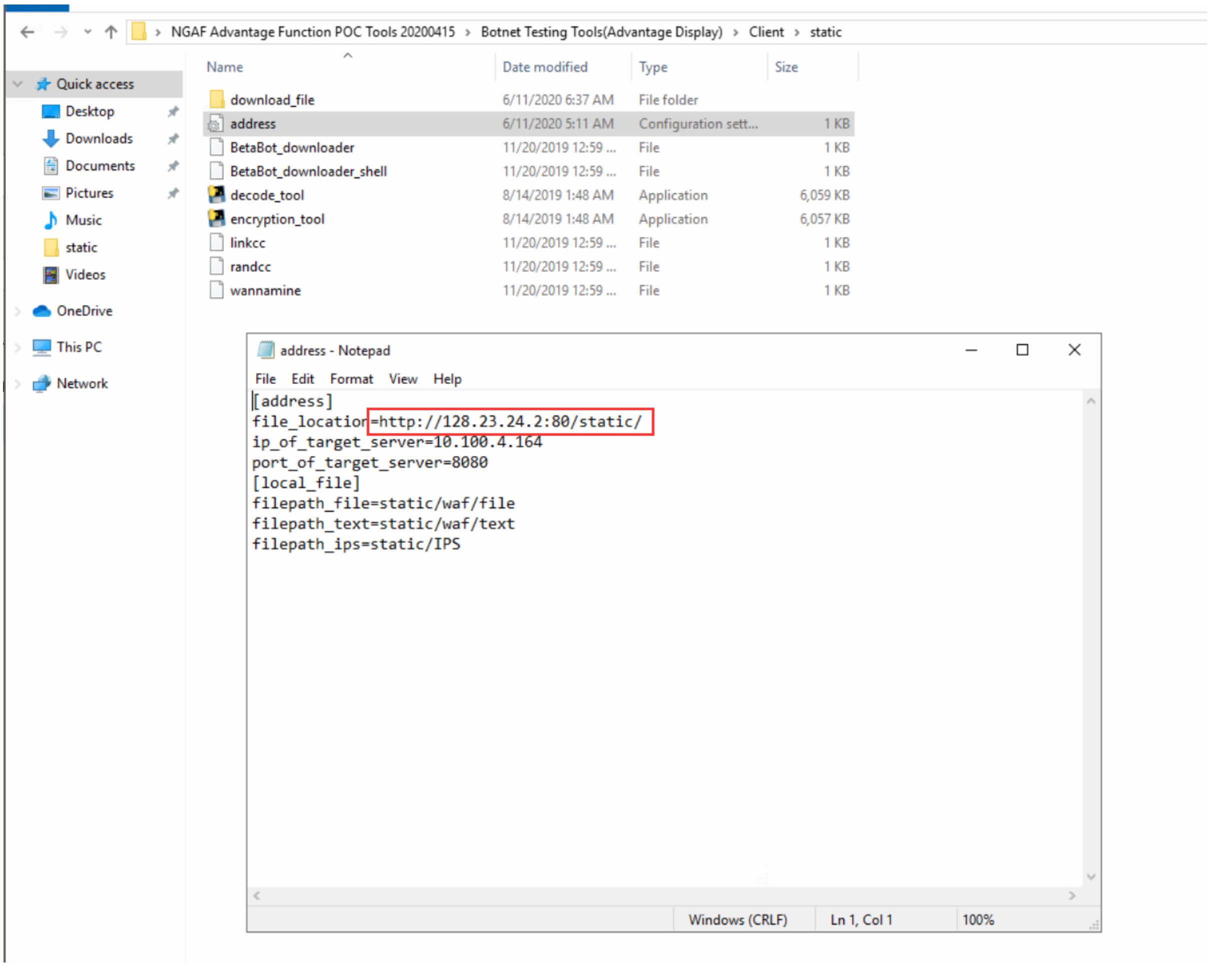


Name	Date modified	Type	Size
app	5/18/2020 10:43 AM	File folder	
POC_files_all	5/18/2020 10:43 AM	File folder	
static	5/18/2020 10:43 AM	File folder	
templates	5/18/2020 10:43 AM	File folder	
server_new	10/31/2019 5:24 AM	Application	7,913 KB

C:\Users\Administrator\Desktop\NGAF Advantage Function POC Tools 20200415\Botnet Testing Tools(Advantage Display)\Server\server_new.exe

```
  WARNING: This is a development server. Do not use it in a production deployment.
  Use a production WSGI server instead.
* Debug mode: off
* Running on http://0.0.0.0:80/ (Press CTRL+C to quit)
192.168.1.2 - - [12/Jun/2020 12:49:45] "GET /en-US/livetile/preinstall?region=US&appid=C98EA5B0842DBB9405BBF071E1DA76512
D21FE36&FORM=Threshold HTTP/1.1" 404 -
```

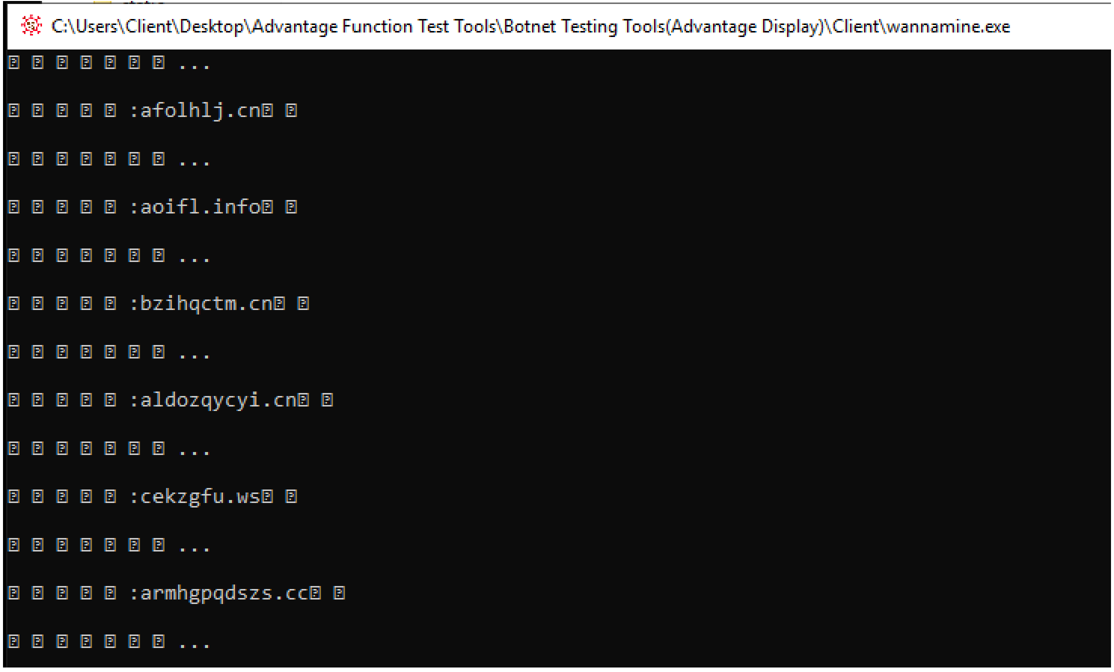
Konfigurasi alamat dari program klien, seting IP dari PC server dalam file:



Name	Date modified	Type	Size
download_file	6/11/2020 6:37 AM	File folder	
address	6/11/2020 5:11 AM	Configuration sett...	1 KB
BetaBot_downloader	11/20/2019 12:59 ...	File	1 KB
BetaBot_downloader_shell	11/20/2019 12:59 ...	File	1 KB
decode_tool	8/14/2019 1:48 AM	Application	6,059 KB
encryption_tool	8/14/2019 1:48 AM	Application	6,057 KB
linkcc	11/20/2019 12:59 ...	File	1 KB
randcc	11/20/2019 12:59 ...	File	1 KB
wannamine	11/20/2019 12:59 ...	File	1 KB

```
[address]
file_location=http://128.23.24.2:80/static/
ip_of_target_server=10.100.4.164
port_of_target_server=8080
[local_file]
filepath_file=static/waf/file
filepath_text=static/waf/text
filepath_ips=static/IPS
```

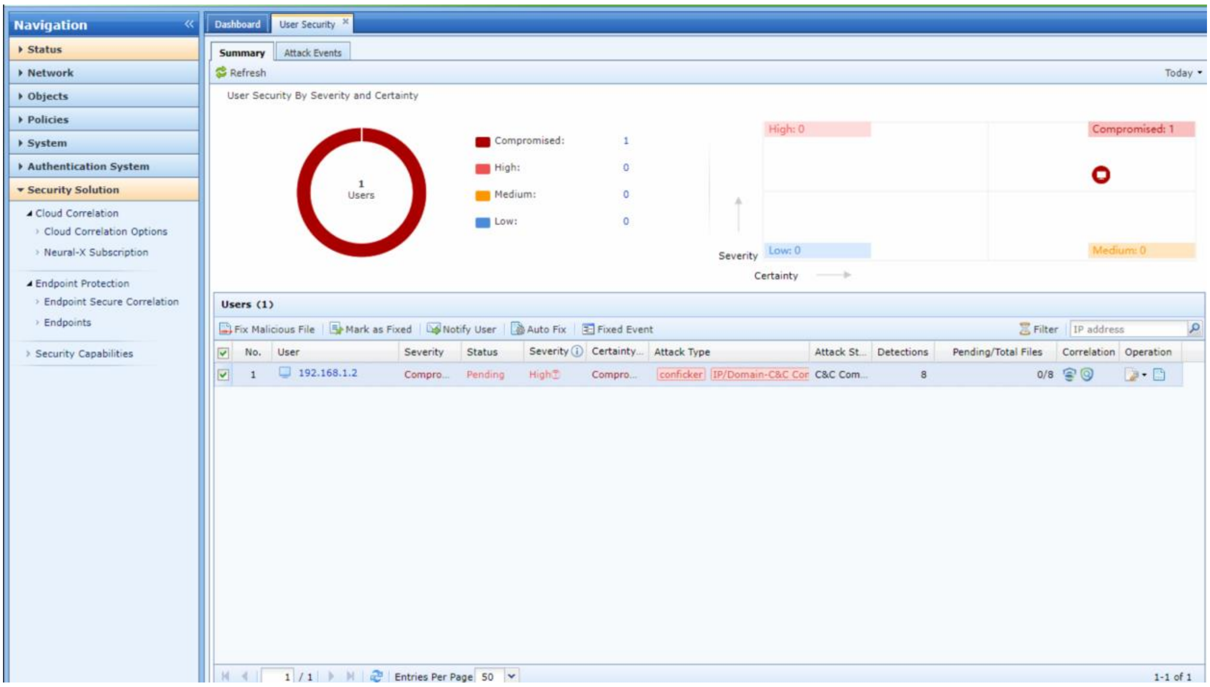
Jalankan wannamine.exe pada PC clien:



C:\Users\Client\Desktop\Advantage Function Test Tools\Botnet Testing Tools(Advantage Display)\Client\wannamine.exe

```
□ □ □ □ □ □ □ □ ...

□ □ □ □ □ :afolhlj.cn□ □

□ □ □ □ □ □ □ □ ...

□ □ □ □ □ :aoifl.info□ □

□ □ □ □ □ □ □ □ ...

□ □ □ □ □ :bzihqctm.cn□ □

□ □ □ □ □ □ □ □ ...

□ □ □ □ □ :aldozqycyi.cn□ □

□ □ □ □ □ □ □ □ ...

□ □ □ □ □ :cekzgfu.ws□ □

□ □ □ □ □ □ □ □ ...

□ □ □ □ □ :armhgpqdszs.cc□ □

□ □ □ □ □ □ □ □ ...
```

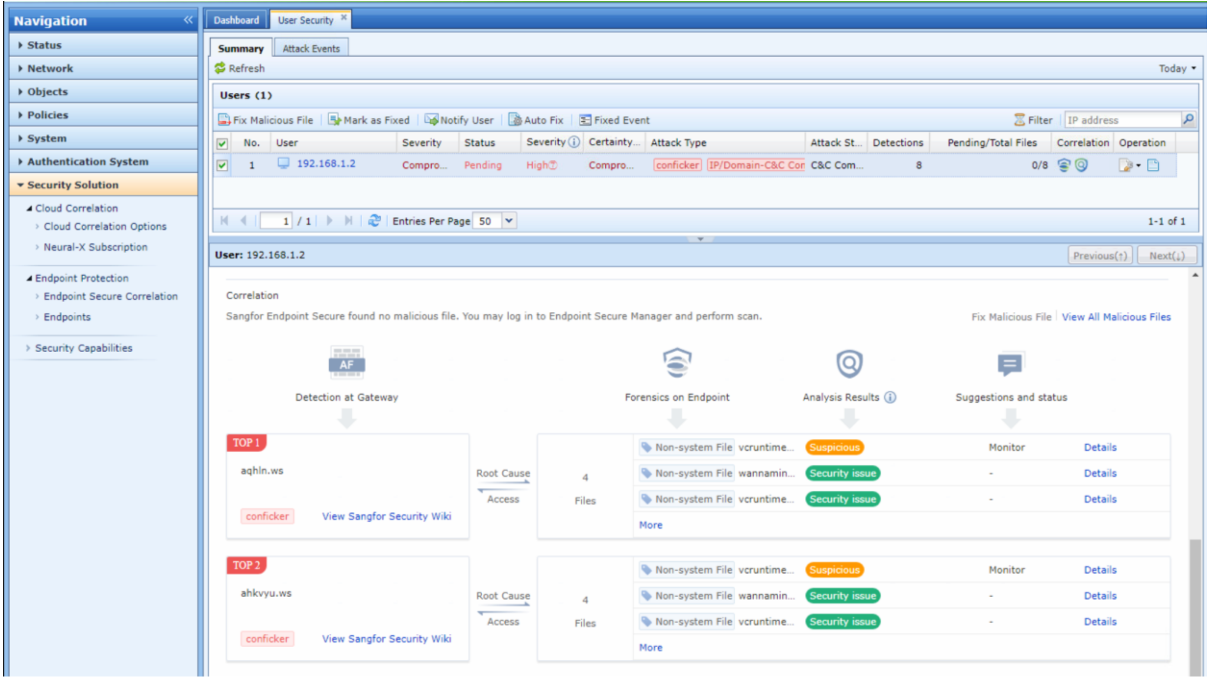
2. Lihat bukti kejadian host yang disusupi pada halaman **User Security.**



🟥 Compromised:	1
🟥 High:	0
🟧 Medium:	0
🟦 Low:	0

☑	No.	User	Severity	Status	Severity	Certainty...	Attack Type	Attack St...	Detections	Pending/Total Files	Correlation	Operation
☑	1	192.168.1.2	Compro...	Pending	High	Compro...	conficker IP/Domain-C&C Cor	C&C Com...	8	0/8		

3. Lewati halaman **Correlated Analysis of Compromised Host Process.**



☑	No.	User	Severity	Status	Severity	Certainty...	Attack Type	Attack St...	Detections	Pending/Total Files	Correlation	Operation
☑	1	192.168.1.2	Compro...	Pending	High	Compro...	conficker IP/Domain-C&C Cor	C&C Com...	8	0/8		

User: 192.168.1.2

Correlation

Sangfor Endpoint Secure found no malicious file. You may log in to Endpoint Secure Manager and perform scan.

Fix Malicious File | View All Malicious Files

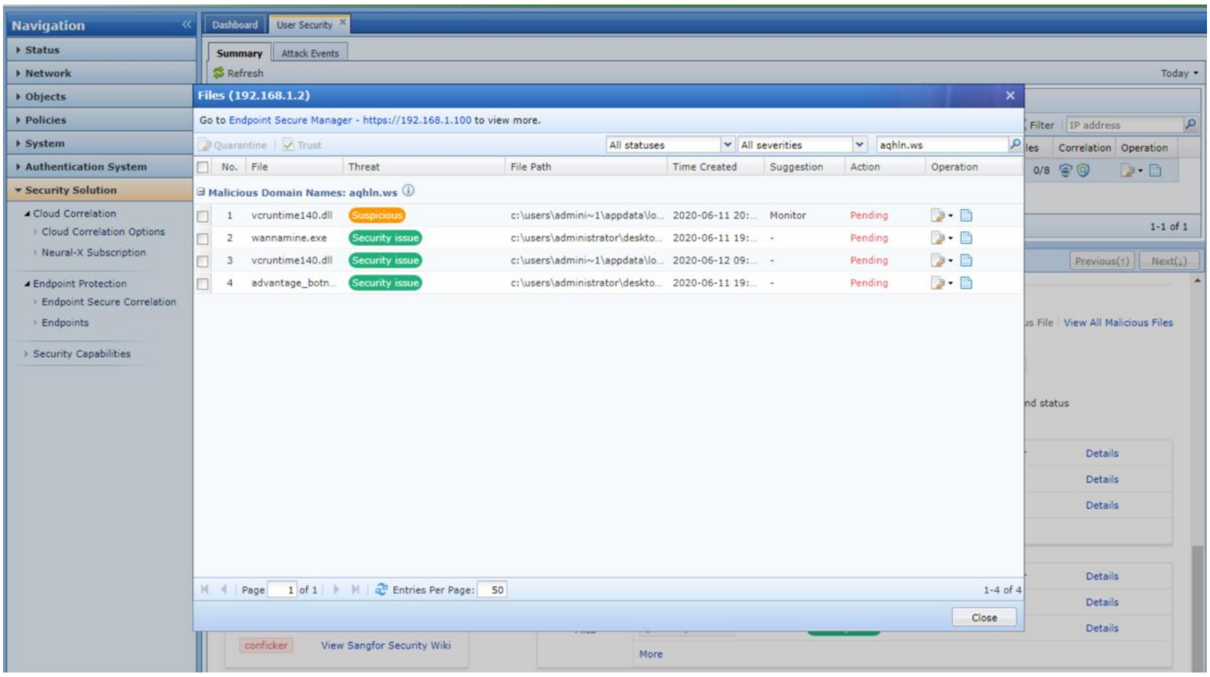
TOP 1
aqhln.ws
conficker
View Sangfor Security Wiki
Root Cause
Access
4 Files

Non-system File	vcruntime...	Suspicious	Monitor	Details
Non-system File	wannamin...	Security issue	-	Details
Non-system File	vcruntime...	Security issue	-	Details
More				

TOP 2
ahkvyu.ws
conficker
View Sangfor Security Wiki
Root Cause
Access
4 Files

Non-system File	vcruntime...	Suspicious	Monitor	Details
Non-system File	wannamin...	Security issue	-	Details
Non-system File	vcruntime...	Security issue	-	Details
More				

4. Cari proses trafik keluar tertentu yang menangani inisiasi file tersebut.



Files (192.168.1.2)

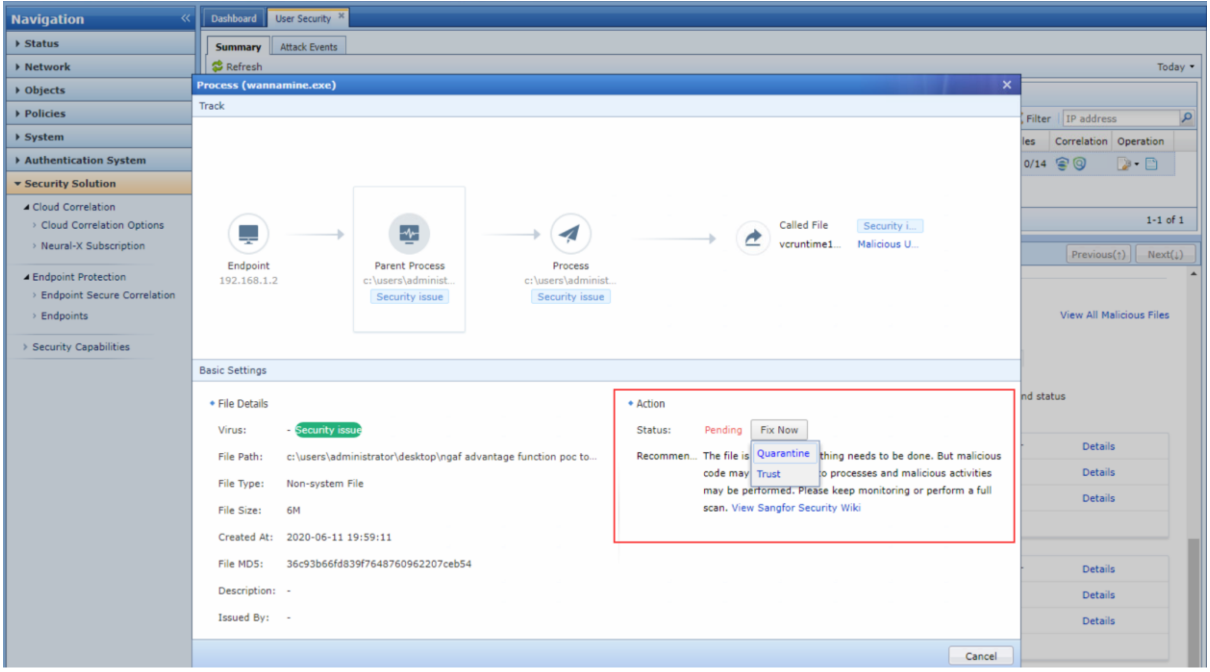
Go to Endpoint Secure Manager - https://192.168.1.100 to view more.

aqhln.ws

Malicious Domain Names: aqhln.ws

No.	File	Threat	File Path	Time Created	Suggestion	Action	Operation
1	vcruntime140.dll	Suspicious	c:\users\admini~1\appdata\lo...	2020-06-11 20:...	Monitor	Pending	
2	wannamine.exe	Security issue	c:\users\administrator\deskto...	2020-06-11 19:...	-	Pending	
3	vcruntime140.dll	Security issue	c:\users\admini~1\appdata\lo...	2020-06-12 09:...	-	Pending	
4	advantage_botn...	Security issue	c:\users\administrator\deskto...	2020-06-11 19:...	-	Pending	

5. Dapat dipilih beberapa cara untuk menangani file virus.



Process (wannamine.exe)

Basic Settings

File Details

Virus: - Security issue

File Path: c:\users\administrator\desktop\ngaf advantage function poc to...

File Type: Non-system File

File Size: 6M

Created At: 2020-06-11 19:59:11

File MD5: 36c93b66fd839f7648760962207ceb54

Description: -

Issued By: -

Action

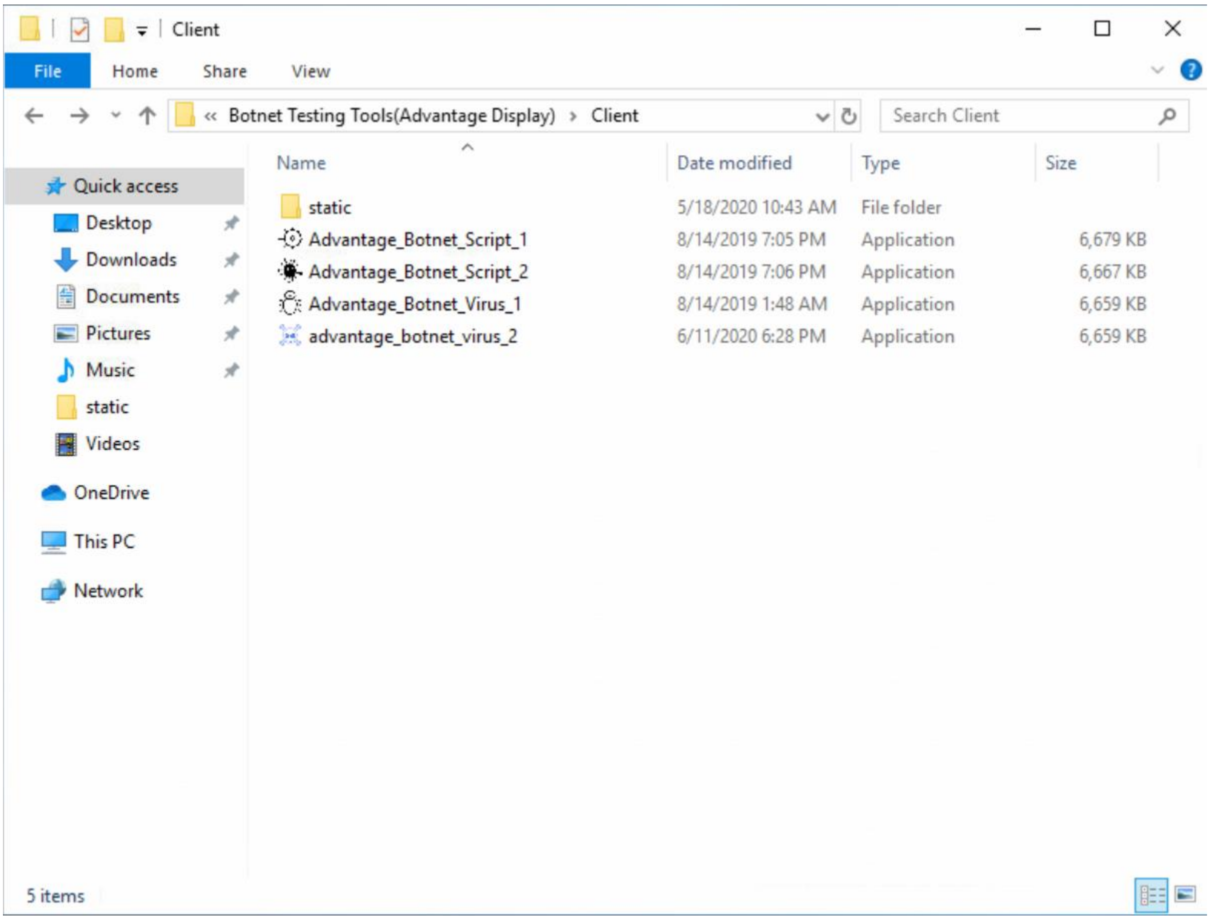
Status: Pending Fix Now

Quarantine

Trust

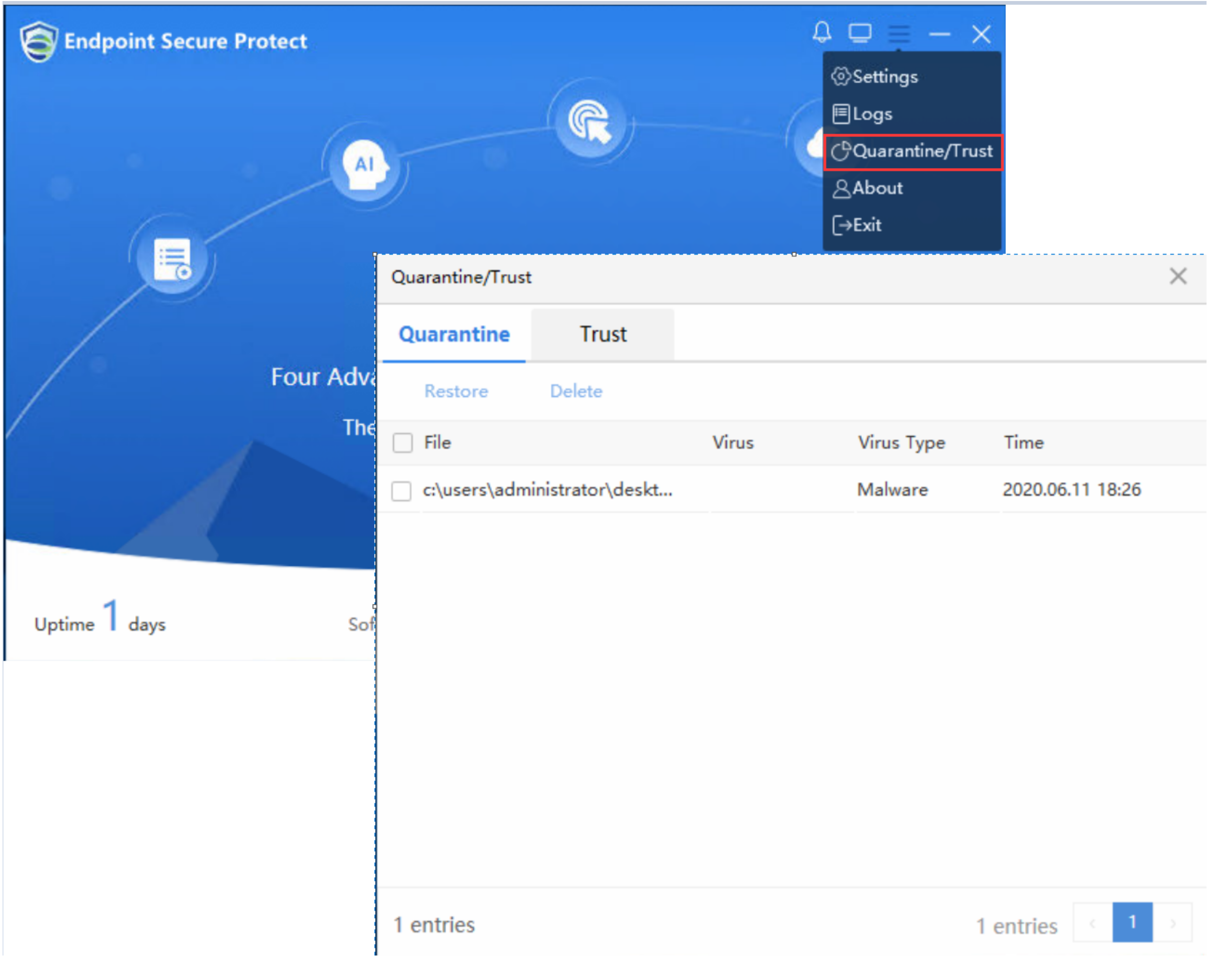
Recommen... The file is thing needs to be done. But malicious code may o processes and malicious activities may be performed. Please keep monitoring or perform a full scan. View Sangfor Security Wiki

6. Ketika virus worm pada klien telah dibersihkan, virus worm [wannamine.ext] akan bersih.



Name	Date modified	Type	Size
static	5/18/2020 10:43 AM	File folder	
Advantage_Botnet_Script_1	8/14/2019 7:05 PM	Application	6,679 KB
Advantage_Botnet_Script_2	8/14/2019 7:06 PM	Application	6,667 KB
Advantage_Botnet_Virus_1	8/14/2019 1:48 AM	Application	6,659 KB
advantage_botnet_virus_2	6/11/2020 6:28 PM	Application	6,659 KB

Anda dapat menemukan bahwa ES telah mengkarantina file virus tersebut.

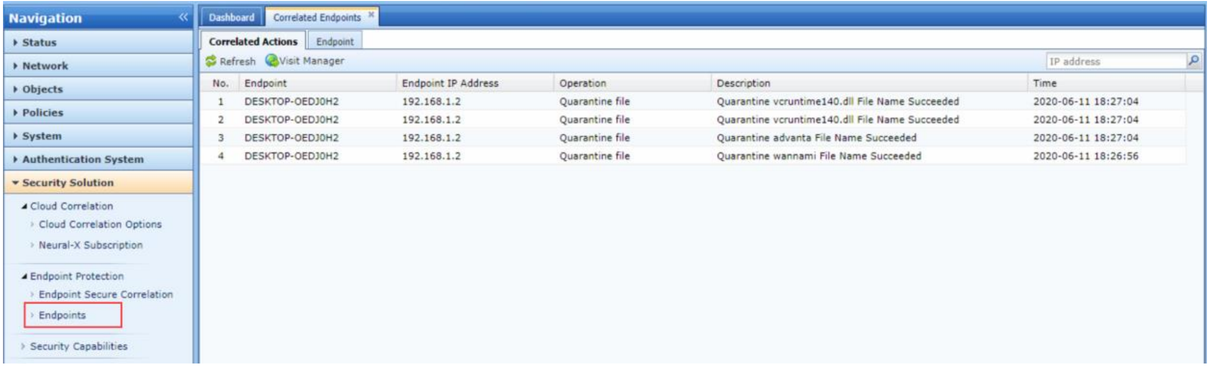


☐ File	Virus	Virus Type	Time
☐ c:\users\administrator\deskt...		Malware	2020.06.11 18:26

1 entries

1 entries ‹ 1 ›

7. Dapat di cari rekam jejak kebiasaan jahat.



No.	Endpoint	Endpoint IP Address	Operation	Description	Time
1	DESKTOP-OEDJ0H2	192.168.1.2	Quarantine file	Quarantine vcruntime140.dll File Name Succeeded	2020-06-11 18:27:04
2	DESKTOP-OEDJ0H2	192.168.1.2	Quarantine file	Quarantine vcruntime140.dll File Name Succeeded	2020-06-11 18:27:04
3	DESKTOP-OEDJ0H2	192.168.1.2	Quarantine file	Quarantine advanta File Name Succeeded	2020-06-11 18:27:04
4	DESKTOP-OEDJ0H2	192.168.1.2	Quarantine file	Quarantine wannami File Name Succeeded	2020-06-11 18:26:56

SANGFOR

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