Sangfor Cyber Command Restful API to 3rd Party

Sangfor Technologies Inc.

Contents

1. Overview

1.1 Purpose

Sangfor Cyber Command provides the following application programming interfaces (APIs) for 3rd-party users to ingest data:

1. IP Group
2. Server
3. Host
4. Risky Assets (servers and hosts)
5. Security Events
6. Weak Passwords
7. Vulnerabilities Details
8. Unencrypted Traffic
9. Branch

*Note: the Branch is some specific IP Groups tagged with 'Branch' information in *Assets* module.

1.2 Communication APIs and Protocol Formats

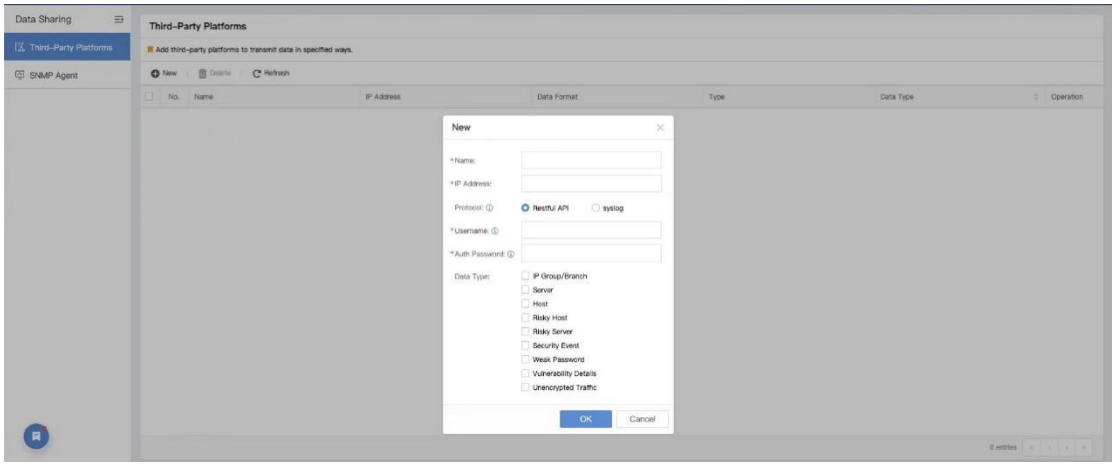
1. The Hypertext Transfer Protocol Secure (HTTPS) protocol is used to carry communication data.
2. Only the GET method is provided for the APIs.
3. JSON is used to describe communication data, and JSON uses UTF-8 encoding.
4. Field formats and information are listed in the tables in the corresponding API sections.

1.3 Authentication Method

1. Use the POST method to send related information to the login API to obtain the authentication token.
2. Use the GET method with the authentication token to pull data from the corresponding APIs.

1.4 Use Guide

1. Log in to Cyber Command, choose **More** > **Compliance and Sharing** > **Data Sharing** > **Third-Party Platforms**, and click **New** in the red box. In the **New** dialog box, configure the device to ingest data.



1) **Name**, **Username**, and **Auth Password**:

These parameters are required during authentication and correspond to the **platformName**, **userName**, and **password** parameters in the authentication request. Values of the parameters carried in the authentication request must be the same as those configured on Cyber Command. Otherwise, the authentication fails.

2) **IP Address**: This parameter indicates the IP address of the device that ingests data. This parameter is required. However, the IP address availability is not supported to verify currently.

3) **Data Type**:

Cyber Command checks whether a data type is selected during data sharing. If a data type is not selected, the corresponding data cannot be ingested. For example, if **Security Event** is not selected, no data will be obtained when the security event API is called.

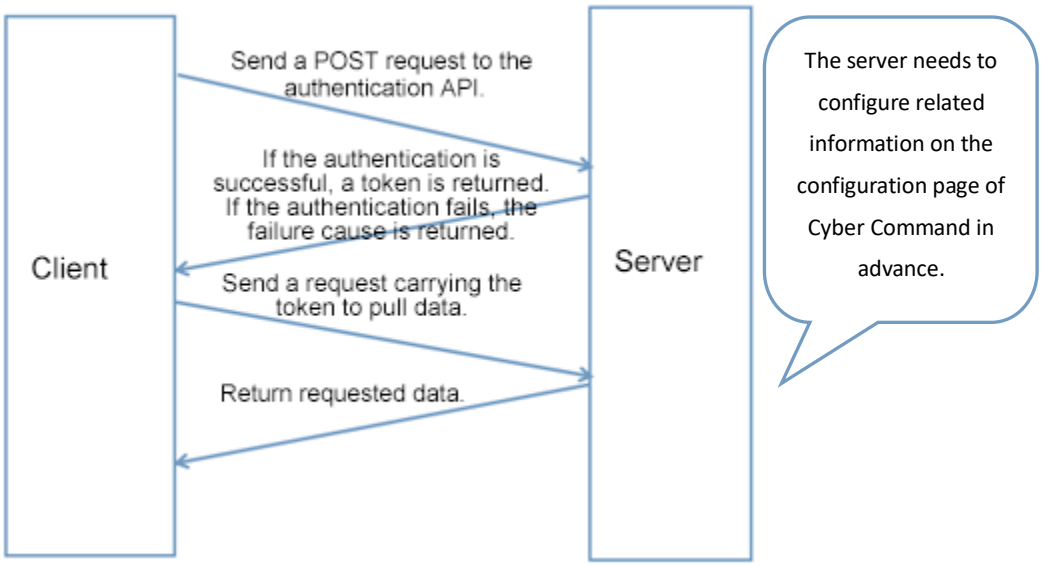
For more information about the APIs, see Chapters 2 and 3.

Data sharing process:

1) Call the authentication API to send an authentication request.

2) After the authentication is successful, send a request carrying the authentication token to pull the corresponding data.

The following figure shows the detailed process.



NOTE

The authentication token expires after the validity period. Then, a new token needs to be obtained.

1.5 Notes

1. If the authentication fails and a message is displayed, indicating that the certificate expires and needs to be updated, disable Secure Sockets Layer (SSL) authentication. The disabling method varies depending on the language. Common disabling methods are as follows:

Python: Configure data to add verify =False in an authentication request by default.
Example: https://ip:7443/sangforinter/v1/auth/party/login?verify =False

PHP:
Example: curl_setopt($this->ch, CURLOPT_SSL_VERIFYPEER, false)

Curl:
Example: curl -XPOST -k url -d @json

2. The server port is 7443 instead of HTTPS port 443.

2. Authentication Method

2.1 Authentication API

API method: POST
API address:
https://ip:7443/sangforinter/v1/auth/party/login

#Request
{
"rand": int32, // 32-bit integer random number generated by the random number library in any language.
"userName": string, // Up to 32 characters (authentication account).
"clientProduct": string, // Up to 32 characters (The value can be empty).
"clientVersion": string, // Up to 16 characters (The value can be empty).
"clientId": int64, // Unique device ID (The value can be empty).
"desc": string, // Description (The value can be empty).
"auth": auth3(userName, password, clientProduct+clientVersion+clientId, rand)
"platformName": // Unique platform name configured in the frontend.
}

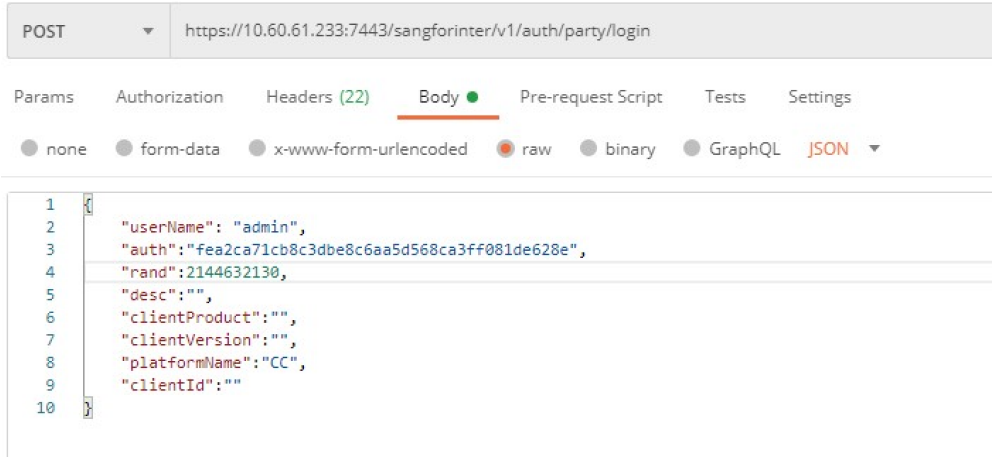
string auth3(const char* userName, const char* password, const char*desc, int32 rand)
{
return sha1(rand + password+"sangfor3party" + userName + desc).toHexString()
}

Field	Type	Meaning	Rule
rand	int32	Random seed	A random 32-bit integer number you prefer to input.
userName	string	Authentication account	The value must be the same as that configured on Cyber Command.
clientProduct	string	Third-party device name	This field is empty by default.
clientId	Int64	Device ID of the third-party device	The value is **0** by default.
clientVersion	string	Version number of the third-party device	This field is empty by default.
desc	string	Description	This field is empty by default.
auth	string	Encrypted user information	The value is obtained by calling the auth3 function, which is generated by the SHA1 algorithm according to the specific inputs
password	string	Authentication	The value must be the same as that

		password	configured on Cyber Command.
platformName	string	Unique platform ID	The value must be the same as that configured on Cyber Command.

For example, if you randomly input the value of ***rand*** as 2144632130 and the password of Cyber Command is **sec@1234**, you can get the auth value as below.

And then you can post the following information to do authorization.



The **Response** will be like following:

success

```
{
    "message":"success",
    "code":0,
    "data":{
        "token":
    }
}
```

fail

```
{
    "message":"invalid argument",        // The request format or encrypted text is incorrect.
    "code":301
}
```

fail

```
{
    "message":"permission denied",    // The authentication account is not found in the configuration file.
    "code":13
}
```

3. API Definition

3.1 Overview

Common fields in the APIs

Field	Type	Meaning	Rule
fromActionTime	long	Start timestamp	Example: 1528747735
toActionTime	long	End timestamp	Example: 1528767735
maxCount	int	Maximum number of data records pulled at a time	Example: 2000 1. The recommended value is 2000/time scope. 2. Data records are displayed in ascending order by timestamp. If the actual quantity of pulled data exceeds the preset value, the start and end timestamps in the time scope need to be adjusted. 3. Up to 10,000 data records can be pulled at a time (5,000 for weakness modules). If the value exceeds 10,000, only 10,000 data records will be shared.

Rules:

(1) For data of the string type, "-" indicates that the data is empty.
For data of the int type, "-1" indicates that the data is meaningless and discarded.

(2) Fields highlighted in green in the tables in chapter 3 indicate the unique data identifier, that is, the key.

3.2 IP Group

API method: GET

API address:

https://IP:7443/sangforinter/v1/data/ipgroup?token=xxx&fromActionTime=xxx&toActionTime=xxx&maxCount=xxx

fromActionTime: Start timestamp, for example, 1528747735.

toActionTime: End timestamp.

maxCount: Maximum number of data records pulled at a time. The maximum value is 10,000.

#Response:

True

HTTP / 1.1 200 OK

```
{
    "code":0,
    "message":"success",
    "data":
    {
        "sendTime":,
        "items":
        [{
            "type":,                                    // IP type
            "author":,                                  // Owner
            "email":,                                   // Email address
            "comment":,                                 // Remarks
            "name":,                                    // IP group name
            "ipRange":,                                 // IP range abbreviation
            "recordTime":,                              // Recording time

         }],
        "count":                                        Actual quantity of obtained data records
        "message":                                      Prompt indicating whether data is completely obtained
        "device_info":                                  Device information
        {
            "source": "SIP",
            "apikey": "ED199EDB4A48CABC241D2FF6FAA18BF5",
            "deviceId": "F99EAAF0",
            "deviceVersion": "SIS3.0.12.20180919110523    Build20180919"
        },
    }
}
```

Field	Type	Meaning	Rule
author	string	Owner	
email	string	Email address	
comment	string	Remarks	
name	string	IP group name	
ipRange	list	IP range abbreviation	Example: ["10.0.0.0-10.255.255.255", "172.16.0.0-172.31.255.255", "192.168.0.0-192.168.255.255"]
recordTime	int	Recording time	
count	int	Number of data records actually	

		pulled	
message		Prompt	
device_info	object	Device information	
source	string	Data source	The default value is Cyber Command.
apikey	string	-	This field is empty by default and does not need to be concerned.
deviceId	string	Device ID	Example: F99EAAF0
deviceVersion	string	Device version	Example: SIS3.0.12.20180919110523 Build20180919

Error (No access permission)

HTTP / 1.1 403 Forbidden

{

"code":13, // Error code ACCES

"message" : "Permission denied!"

}

Error (Data obtaining failed)

{

"code": 301, // The error code indicates a failure no matter whether data obtaining fails partially or fully.

"message" : "Invalid argument"

}

3.3 Server

API method: GET

API address:

https://IP:7443/sangforinter/v1/data/business?token=xxx&fromActionTime=xxx&toActionTime=xxx&maxCount=xxx

fromActionTime: Start timestamp, for example, 1528747735.

toActionTime: End timestamp.

maxCount: Maximum number of data records pulled at a time. The maximum value is 10,000.

#Response:

True

HTTP / 1.1 200 OK

{

"code":0,

"message":"success",

"data":

```
{
    "sendTime":,
    "items":
    [ {
        "assetIp:,
        "system":,
        "findType":,
        "openServer":,
        "status":,
        "recordTime":,
        "id":,
        "name":,
        "author":,
        "email":,
        "comment":,
        "businessStatus":,
        "priority":,
        "devId":,
        "branchName":,
        "type",
        "branchId"
    } ],
    "count":                                    Actual quantity of obtained data records
    "message":                          Prompt indicating whether data is completely obtained
    "device_info":                                  Device information
    {
        "source": "SIP",
        "apikey": "ED199EDB4A48CABC241D2FF6FAA18BF5",
        "deviceId": "F99EAAF0",
        "deviceVersion": "SIS3.0.12.20180919110523 Build20180919"
    },
}
}
```

Field	Type	Meaning	Rule
assetIp	string	Asset IP address	Example: 200.200.155.157
system	string	OS type	"Windows" | "Linux"
findType	string	Discovery method	"manual" | "auto"
openServer	list	Opened ports and services	[// Opened services and ports

		[{},{},{}....]	{"port":"22","protocol":"ssh","find_type":0}, // Specific port and service {"port":"23","protocol":"ftp","find_type":1},],
status	int	Policy status	**0**: Being used **1**: Deleted
recordTime	int	Policy creation time	Second-level timestamp.
(business)id	string	Server ID	Used to find out the server's name and related information in the JSON file.
(business)name	string	Server name	
(Business)author	string	Server owner	
(Business)email	string	Email address of the Server owner	
(Business)comment	string	Server remarks	
businessStatus	int	Server status	**0**: Being used **1**: Deleted
(Business)priority	int	Server criticality	**1**: Critical **2**: Noncritical
devId	string	Device ID	
branchName	**string**	**Branch name**	Group/Branch name
type	**int**	**IP type (All tables share the same logic.)**	The options are as follows: **1**: Categorized **2**: Uncategorized
branchId	**str**	**Branch ID (IP view)**	Example: "1"
count	int	Number of data records actually pulled	
message		Prompt	
device_info	object	Device information	
source	string	Data source	The default value is

			Cyber Command.
apikey	string	-	This field is empty by default and does not need to be concerned.
deviceId	string	Device ID	Example: F99EAAF0
deviceVersion	string	Device version	Example: SIS3.0.12.201809191 10523 Build20180919

Error (No access permission)

HTTP / 1.1 403 Forbidden

{

"code":13, // Error code ACCES

"message" : "Permission denied!"

}

Error (Data obtaining failed)

{

"code": 301,// The error code indicates a failure no matter whether data obtaining fails partially or fully.

"message" : "Invalid argument"

}

3.4 Host

API method: GET

API address:

https://IP:7443/sangforinter/v1/data/terminal?token=xxx&fromActionTime=xxx&toActionTime=xxx&maxCount=xxx

fromActionTime: Start timestamp, for example, 1528747735.

toActionTime: End timestamp.

maxCount: Maximum number of data records pulled at a time. The maximum value is 10,000.

#Response:

True

HTTP / 1.1 200 OK

{

"code":0,

"message":"success",

"data":

{

"sendTime":,

"items":

[{
"ip":,
"comment":,
"groupId":,
"groupName":,
"status":,
"recordTime":,
"author":,
"findType":,
"hostName":,
"devId":,
"type":,
"email":,
"branchName":,
"branchId":
}],
"count": Actual quantity of obtained data records
"message": Prompt indicating whether data is completely obtained
"device_info": Device information
{
"source": "SIP",
"apikey": "ED199EDB4A48CABC241D2FF6FAA18BF5",
"deviceId": "F99EAAF0",
"deviceVersion": "SIS3.0.12.20180919110523 Build20180919"
},

}
}

Field	Type	Meaning	Rule
ip (Abbreviation)	**string**	**Asset IP address**	**Example: "1.1.1.9"**
comment	string	Remarks	
asset_id	int	Asset ID	
groupId	string	Host group ID	
groupName	string	Host group name	If no host group is configured, this field is set to the IP address.
recordTime	int	Policy creation time	Second-level timestamp.
status	int	Policy status	**0**: Being used **1**: Deleted

author	string	Owner	
findType	string	Discovery method	"manual" | "auto"
hostName	string	Username	
devId	string	Device ID	
type	int	IP type	The options are as follows: **3**: Configured to a host group **4**: Not configured to a host group
email	string	Email address	
branchName	string	**Branch name**	
branchId	string	**Branch ID (IP view)**	**Example: "1"**
device_info	object	Device information	
source	string	Data source	The default value is Cyber Command.
apikey	string	-	This field is empty by default and does not need to be concerned.
deviceId	string	Device ID	Example: F99EAAF0
deviceVersion	string	Device version	Example: SIS3.0.12.20180919110523 Build20180919

Error (No access permission)

HTTP / 1.1 403 Forbidden

```
{
    "code":13, // Error code ACCES
    "message" : "Permission denied!"
}
```

Error (Data obtaining failed)

```
{
    "code": 301,// The error code indicates a failure no matter whether data obtaining fails partially or fully.
    "message" : "Invalid argument"
}
```

3.5 Risky Assets (Server and Host)

This section contains two APIs. However, the returned data formats of the APIs are the same.

Risky server API method: GET

API address:
https://IP:7443/sangforinter/v1/data/riskbusiness?token=xxx&fromActionTime=xxx&toActionTime=xxx&maxCount=xxx

Risky host API method: GET
API address:
https://IP:{$port}/sangforinter/v1/data/riskterminal?token=xxx&fromActionTime=xxx&toActionTime=xxx&maxCount=xxx

fromActionTime: Start timestamp, for example, 1528747735.
toActionTime: End timestamp.
maxCount: Maximum number of data records pulled at a time. The maximum value is 10,000.

#Response:
True
HTTP / 1.1 200 OK
{
"code":0,
"message":"success",
"data":
{
"sendTime":,
"items":
[{
"affectType":,
"authUser":,
"branchName":,
"dealStatus":,
"fallLevel":,
"groupName":,
"groupId":,
"tag":,
"ip":,
"lastTime":,
"recordDate":,
"riskLevel":,
"severityLevel":,
"type":,
"isWhite":,
"hostName":,
"dealTime":
}],
"count": Actual quantity of obtained data records
"message": Prompt indicating whether data is completely obtained

```
        "device_info":                                    Device information
         {
                "source":    "SIP",
                "apikey":    "ED199EDB4A48CABC241D2FF6FAA18BF5",
                "deviceId": "F99EAAF0",
                "deviceVersion": "SIS3.0.12.20180919110523 Build20180919"
         },

    }
}
```

Field	Type	Meaning	Rule
affectType	list	Impact scope	Example: [1,2,3] **1**: Self impacted **2**: LAN impacted **3**: WAN impacted
authUser	string	Owner	
branchName	string	Branch name	
dealStatus	int	Fixing status	**0**: Pending **1**: Fixed
fallLevel	int	Compromise level	**0**: Normal **1**: Low **2**: High **3**: Compromised
groupName	string	Asset group name or user group name	
groupId	string	Asset group or user group ID	
tag	list	Tag	Example: ["Tag 1", "Tag 2"]
ip	string	Host/Server IP address	Example: "3.1.1.7"
lastTime	int	Latest visit time	Second-level timestamp
severityLevel	int	Security level	[0-10]
isWhite	int	Whether added to a whitelist	**0**: Not whitelisted **1**: Whitelisted
hostName (Available only for hosts)	string	Hostname	
dealTime	int	Fixing time (If the value of **dealStatus** is **0**, this field is left empty.)	Second-level timestamp
branchId	string	Branch ID	Example: "1"
device_info	object	Device information	

source	string	Data source	The default value is Cyber Command.
apikey	string	-	This field is empty by default and does not need to be concerned.
deviceId	string	Device ID	Example: F99EAAF0
deviceVersion	string	Device version	Example: SIS3.0.12.20180919110523 Build20180919

Error (No access permission)

HTTP / 1.1 403 Forbidden

{

"code":13, // Error code ACCES

"message" : "Permission denied!"

}

Error (Data obtaining failed)

{

"code": 301, // The error code indicates a failure no matter whether data obtaining fails partially or fully.

"message" : "Invalid argument"

}

3.6 Security Event

API method: GET

API address:

https://IP:7443/sangforinter/v1/data/riskevent?token=xxx&fromActionTime=xxx&toActionTime=xxx&maxCount=xxx

fromActionTime: Start timestamp, for example, 1528747735.

toActionTime: End timestamp.

maxCount: Maximum number of data records pulled at a time. The maximum value is 10,000.

#Response:

True

HTTP / 1.1 200 OK

{

"code":0,

"message":"success",

"data":

{

"sendTime":,

"items":

[{

"type":,

"groupName":,

```
            "groupId":,
            "ip":,
            "recordDate":,
            "detectEngine":,
            "ruleId":,
            "firstTime":,
            "lastTime":,
            "eventDes":,
            "infosecurity":,
            "infosecuritysub":,
            "isWhite":,
            "priority":,
            "reliability":,
            "stage":,
            "hostRisk":,
            "branchName":,
            "branchId":,
            "dealStatus":,
            "proof":,
            "solution":,
            "hostName":,
            "eventType":,
            "eventKey":,
            "principle":,
            "tag":,
        } ],
        "count":                                    Actual quantity of obtained data records
        "message":                          Prompt indicating whether data is completely obtained
        "device_info":                                  Device information
        {
            "source": "SIP",
            "apikey":    "ED199EDB4A48CABC241D2FF6FAA18BF5",
            "deviceId":    "F99EAAF0",
            "deviceVersion":    "SIS3.0.12.20180919110523 Build20180919"
        },
    }
}
```

Field	Type	Meaning	Rule
eventKey	string	Event key for querying logs	Example: "coengine|104008"
branchId	string	Branch ID	
groupId	string	Asset group ID	
principle	string	Background	

tag	list	Tag	
groupName	string	Asset or user group name	
ip	string	IP address of the compromised endpoint	
recordDate	int	Event occurrence date (non-timestamp). This field is used for query. For example, this field can be used as a filter criterion for querying data in recent days.	Example: 20170701 Accurate to day
detectEngine	string	Detection engine name	
ruleId	string	Rule ID (used to find the corresponding proof information format)	
firstTime	int	Security event occurrence timestamp. This field indicates the first occurrence time of a security event.	Example: 1494582328 Accurate to seconds
lastTime	int	Security event update timestamp. This field indicates the latest update time of a security event, which can be displayed on the product UI.	Example: 1494582328 Accurate to seconds
eventDes	string	Event description	
infosecurity	string	Event category	
infosecuritysub	string	Event sub-category	
priority	int	Confidence	**1**: Low 2: High 3: Compromised
reliability	int	Threat severity	**1**: Low 2: Medium 3: High
stage	int	Attack stage	**-1**: Full stages **1**: Weakness **2**: Reconnaissance **3**: Exploitation **4**: C&C **5**: Propagation **6**: Impact
hostRisk	string	Risky host (IP address + group name)	Example: "1.1.1.1 (asset 1)"

branchName	string	Branch name	
dealStatus	int	Fixing status	**0**: Not fixed **1**: Fixed

proof	json	**Attack proof**	Actual data stored in the database. When only parameters are transferred, the format is as follows:
			"proof": {
			"detail_list": [
			{
			"count":1, "dst_type":"3",
			"hole_id": "10010236",
			"module_type": "30", "dst_ip":
			"192.201.8.17", "dst_group":
			"94"
			}
			]
			}
			}

solution	string	Troubleshooting suggestion	
hostName	string	Username/Hostname	Obtain the name of the host to which the event belongs.
eventType	int	Whether the event is a hot event	**0**: No **1**: Yes

logParams	json	Used to query corresponding log information	{
			"log_type":
			"param_code":
			"param_origin":
			}
			The options of Log_type are as follows: (Currently, you can only query security logs.)
			Security logs: **1**
			Operation logs: **2**
			DNS logs: **3**
			Third-party logs: **4**
			HTTP flow logs: **5**
			User auditing logs: **6**
			'SAS_LOG': **7**
			'DASDB_LOG': **8**

top10	list	Top 10 security event logs	During data pulling, the top 10 security event logs are not provided.
device_info	object	Device information	
source	string	Data source	The default value is Cyber Command.
apikey	string	-	This field is empty by default and does

			not need to be concerned.
deviceId	string	Device ID	Example: F99EAAF0
deviceVersion	string	Device version	Example: SIS3.0.12.20180919110523 Build20180919

Error (No access permission)

HTTP / 1.1 403 Forbidden

{

"code":13, // Error code ACCES

"message" : "Permission denied!"

}

Error (Data obtaining failed)

{

"code": 301, // The error code indicates a failure no matter whether data obtaining fails partially or fully.

"message" : "Invalid argument"

}

3.7 Weak Password

API method: GET

API address:

https://IP:7443/sangforinter/v1/data/weakpasswd?token=xxx&fromActionTime=xxx&toActionTime=xxx&maxCount=xxx

fromActionTime: Start timestamp, for example, 1528747735.

toActionTime: End timestamp.

maxCount: Maximum number of data records pulled at a time. The maximum value is 5,000.

#Response:

True

HTTP / 1.1 200 OK

{

"code":0,

"message":"success",

"data":

{

"sendTime":,

"items":

[{

"ip":,

"appCrc":,

"branchName":,

"branchId",
"type":,
"groupId":,
"groupName":,
"dstPort":,
"firstTime":,
"dealDetail":,
"dealStatus":,
"branchType":,
"dealTime":,
"level":,
"recordDate":,
"ruleId":,
"weakType":,
"passwd":,
"user":,
"srcIp":,
"lastTime":
}],
"count": Actual quantity of obtained data records
"message": Prompt indicating whether data is completely obtained
"device_info": Device information
{
"source": "SIP",
"apikey": "ED199EDB4A48CABC241D2FF6FAA18BF5",
"deviceId": "F99EAAF0",
"deviceVersion": "SIS3.0.12.20180919110523 Build20180919"
},

}
}

Field	Type	Meaning	Rule
ip	string	Server IP address (destination IP address)	"1.1.1.3"
appCrc	int	Related to the weakness details	
branchId	string	Branch ID	Example: "1"
branchName	string	Branch	
groupId	string	ID of the corresponding type	If no group is configured, **groupName** is set to the ID.
groupName	string	Group name	
dstPort	int	Destination port	

firstTime	int	First discovery timestamp	
dealDetail	string	Fixing details	
dealStatus	int	Fixing status	**0**: Not fixed **1**: Fixed
branchType	Int	Branch type	
dealTime	int	Fixing timestamp	
level	Int	Weakness level	**1**: Low **2**: Medium **3**: High
recordDate	List	Recording date	Example: [20180801, 20180813]
ruleId	string	Weakness rule ID	**501001**: FTP weak password **501002**: LDAP weak password **501003**: MySQL weak password **501004**: POP3 weak password **501005**: SMTP weak password **501006**: Telnet weak password **501007**: Web weak password
weakType	string	Weak password type	Example: FTP weak password
passwd	string	Password	**No password is provided, and the password is replaced by "******".**
user	string	Username	
srcIp	string	Source IP address	
lastTime	int	Latest occurrence time	Latest occurrence timestamp.
eventKey	string	Event identifier	Example: "coengine|104008"
device_info	object	Device information	
source	string	Data source	The default value is Cyber Command.
apikey	string	-	This field is empty by default and does not need to be concerned.
deviceId	string	Device ID	Example: F99EAAF0
deviceVersion	string	Device version	Example: SIS3.0.12.20180919110523 Build20180919

Error (No access permission)

HTTP / 1.1 403 Forbidden

{

"code":13, // Error code ACCES

"message" : "Permission denied!"

}

Error (Data obtaining failed)

{

"code": 301,// The error code indicates a failure no matter whether data obtaining fails partially or fully.

"message" : "Invalid argument"

}

3.8 Vulnerabilities Details

API method: GET

API address:

https://IP:7443/sangforinter/v1/data/hole?token=xxx&fromActionTime=xxx&toActionTime=xxx&maxCount=xxx

fromActionTime: Start timestamp, for example, 1528747735.

toActionTime: End timestamp.

maxCount: Maximum number of data records pulled at a time. The maximum value is 5,000.

#Response:

True

HTTP / 1.1 200 OK

{

"code":0,

"message":"success",

"data":

{

"sendTime":,

"items":

[{

"ip":,

"appCrc":,

"protocol":,

"branchName":,

"branchId",

"type":,

"groupId":,

"groupName":,

"dstPort":,

"firstTime":,

"holeId":,
"dealDetail":,
"dealStatus":,
"branchType":,
"dealTime":,
"level":,
"sipHoleType":,
"recordDate":,
"ruleId":,
"holeName":,
"desc":,
"impact":,
"solution":,
"proof":,
"lastTime":,
"event_key":
}],
"count": Actual quantity of obtained data records
"message": Prompt indicating whether data is completely obtained
"device_info": Device information
{
"source": "SIP",
"apikey": "ED199EDB4A48CABC241D2FF6FAA18BF5",
"deviceId": "F99EAAF0",
"deviceVersion": "SIS3.0.12.20180919110523 Build20180919"
},
}
}

Field	Type	Meaning	Rule
ip	string	Server IP address (destination IP address)	"1.1.1.3"
appCrc	int	Related to the weakness details	Used to determine the protocol to which a vulnerability belongs.
protocol	string	Protocol to which a vulnerability belongs	
branchName	string	Branch	
branchId	string	Branch ID	Example: "1"
groupId	string	ID of the corresponding type	If no group is configured, **groupName** is set to the ID.
groupName	string	Group name	
dstPort	int	Destination port	

firstTime	int	First discovery timestamp	
holeId	int	Available only to vulnerabilities (vulnerability ID)	
dealDetail	string	Fixing details	
dealStatus	int	Fixing status	**0**: Not fixed **1**: Fixed
branchType	Int	Branch type	**0**: User-based **1**: Device-based
dealTime	int	Fixing timestamp	
level	Int	Weakness level	**1**: Low **2**: Medium **3**: High
sipHoleType	String (Available only to vulnerabilities)	Vulnerability category	
recordDate	List	Recording date	Example: [20180801, 20180813]
ruleId	string	Weakness rule ID	**504001**: Vulnerability
holeName	string	Vulnerability name	/home/fantom/apps/seclib/local/fw.unzipped/4.7/pvs/patch0/rules_des_ini_cn/ Find the file with the corresponding holeId.
desc	string	Vulnerability description	The source is same as above.
impact	string	Possible impact	The source is same as above.
solution	list	Solution	["Solution 1", "Solution 2", ...]
proof	Vulnerability proof	string	
lastTime	int	Latest occurrence timestamp	
eventKey	string	Event identifier	Example:

			"coengine|104008"
device_info	object	Device information	
source	string	Data source	The default value is Cyber Command.
apikey	string	-	This field is empty by default and does not need to be concerned.
deviceId	string	Device ID	Example: F99EAAF0
deviceVersion	string	Device version	Example: SIS3.0.12.20180919110523 Build20180919

3.9 Unencrypted Traffic

API method: GET
API address:
https://IP:7443/sangforinter/v1/data/plaintexttransmission?token=xxx&fromActionTime=xxx&toActionTime=xxx&maxCount=xxx

fromActionTime: Start timestamp, for example, 1528747735.
toActionTime: End timestamp.
maxCount: Maximum number of data records pulled at a time. The maximum value is 5,000.

#Response:
True
HTTP / 1.1 200 OK
{
"code":0,
"message":"success",
"data":
{
"sendTime":,
"items":
[{
"ip":,
"appCrc":,
"branchName":,
"branchId",
"type":,
"groupId":,
"groupName":,

```
            "dstPort":,
            "firstTime":,
            "dealDetail":,
            "dealStatus":,
            "branchType":,
            "dealTime":,
            "level":,
            "recordDate":,
            "ruleId":,
            "url":,
            "proof":,
            "lastTime"
        }],
        "count":                                    Actual quantity of obtained data records
        "message":                  Prompt indicating whether data is completely obtained
        "device_info":                                  Device information
        {
            "source": "SIP",
            "apikey":   "ED199EDB4A48CABC241D2FF6FAA18BF5",
            "deviceId":   "F99EAAF0",
            "deviceVersion":   "SIS3.0.12.20180919110523 Build20180919"
        },

    }
}
```

Field	Type	Meaning	Rule
ip	string	Server IP address (destination IP address)	"1.1.1.3"
appCrc	int	Related to the weakness details	
branchName	string	Branch	
branchId	string	Branch ID	Example: "1"
groupID	string	ID of the corresponding type	If no group is configured, **groupName** is set to the ID.
groupName	string	Group name	
dstPort	int	Destination port	
firstTime	int	First discovery timestamp	
dealDetail	string	Fixing details	
dealStatus	int	Fixing status	**0**: Not fixed **1**: Fixed

branchType	Int	Branch type	
dealTime	int	Fixing timestamp	
level	Int	Weakness level	**1**: Low **2**: Medium **3**: High
recordDate	List	Recording date	Example: [20180801, 20180813]
ruleId	string	Weakness rule ID	502001: Web unencrypted login
url	string	Unencrypted domain name/URL	
proof	json	Data packet proof	
lastTime	int	Latest occurrence timestamp	
eventKey	string	Event identifier	Example: "coengine|104008"
device_info	object	Device information	
source	string	Data source	The default value is Cyber Command.
apikey	string	-	This field is empty by default and does not need to be concerned.
deviceId	string	Device ID	Example: F99EAAF0
deviceVersion	string	Device version	Example: SIS3.0.12.20180919110523 Build20180919

Error (No access permission)

HTTP / 1.1 403 Forbidden

{

"code":13, // Error code ACCES

"message" : "Permission denied!"

}

Error (Data obtaining failed)

{

"code": 301, // The error code indicates a failure no matter whether data obtaining fails partially or fully.

"message" : "Invalid argument"

}

3.10 Branch Information

https://IP:7443/sangforinter/v1/data/branch?token=xxx

API method: GET

Response:

```
{
   "message": "Invalid argument",
   "code": 301
}
{
   "message": "Permission denied",
   "code": 13
}
```

Success

```
{
      "code":0,
      "message":"success",
      "data":{
            // Key is the branch ID.
            "1":{
                  "name":          string ,          // Branch name, for example: "Branch 1"
                  "priority":      string ,          //
                  "address":       string,           // Address
                  "position":      dic,              // Location (longitude and latitude)
                  {
                        "longitude": 114.009129,
                        "latitude": 22.59815
                  }
                  "found":         bool,             //
                  "point_id":                        // Not used
                  "update_time": int,                // Update timestamp
                  "status":        int,              // Status. Example: 0: Not deleted, 1: Deleted
                  "author":        string,           // Owner
                  "email":         string,           // Email address
                  "ip_group":      list,             // IP groups in a branch. Example:
                  [
                        {
                              "start_ip": string    // Start IP address, for example, 1.1.1.1
                              "end_ip": string      //End IP address, for example, 1.1.1.1
                        },
                        ... ...
                  ]
            },
```

```
        ... ...
        "record_cnt":{
            "total":    int,                // Total
            "auto_id": int,                 // Number used as the key
        }
    }
}
```

JSON content in the branch configuration file is returned, and fields are not converted.

Field	Type	Description
name	string	Branch name.
priority	string	The options are as follows: **branch** **headquarters**
address	string	Address
position	json	Location information (longitude and latitude).
found	bool	Not used.
point_id	Reserved (Null)	Not used.
update_time	int	Update timestamp.
status	int	Status. **0**: Not deleted **1**: Deleted
author	string	Owner.
email	string	Email address.
ip_group	list	IP groups contained in a branch.
start_ip	string	Start IP address, for example, 1.1.1.1.
end_ip	string	End IP address, for example, 1.1.1.1. If there is only one IP address, the end IP address is the same as the start IP address.