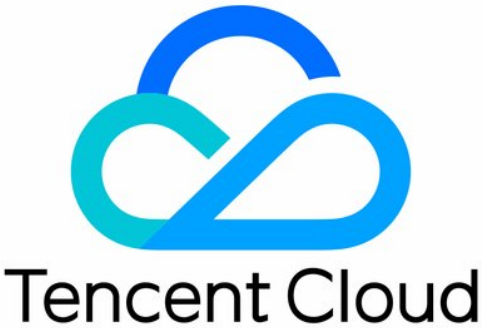
Cloud Workload Protection Platform

Cloud Workload Protection Description

Product Documentation



Contents

Cloud Workload Protection Description
Feature Description

Last updated：2023-12-26 16:39:11

Web shell detection

Web shells are common in hackers' attacks. The CWPP agent will scan newly created web program files on the server for suspicious risks. For a small number of files that are suspected to be web shells, CWPP reports them to Tencent Cloud, which then conducts further detection through the machine learning detection engine. After detection, the sample files will be deleted in real time. CWPP runs a full scan every day by default. No private data will be extracted in this process.

Abnormal login reminder

The abnormal login reminder allows you to identify abnormal admin logins. The source IP, time, login user name and login status data in the login log need to be collected for computing risks. The login log data is retained on cloud for one month.

Password cracking reminder

Detect password cracking attacks against your server and show you the log and result of the attacks. It collects and analyzes information in the logs, including source IP address, attack time, login username, and login status. The login logs will be retained in the cloud for one month.

Malicious Trojans and virus detection

Malicious Trojans and virus programs usually steal user data or launches attacks, which will consume a large amount of system resources and make your business unable to provide services normally. The CWPP agent will collect the hash values of suspicious programs to the cloud, and the cloud-based scanning and blocking module will inspect the values. If a value is not found in the cloud-based hash value library, the corresponding executable file will be reported to the cloud and inspected by the cloud-based anti-virus engine. After inspection, the sample file will be deleted in real time. CWPP runs a full scan every day by default. No private data will be extracted in this process.

Vulnerability alert

The current CWPP supports detecting Linux and Windows vulnerabilities and security baselines complying with Tencent Cloud requirements.
The vulnerability management feature presents the vulnerability risks on the current server and provides a repair solution to you for reference. This module downloads vulnerability policy library from the cloud to perform detection locally, and reports the name, version number, path, and discovery time of application for a server with vulnerability risk. No data related to user privacy is fetched during the process.

Upgrade and maintenance

The upgrade and maintenance feature mainly informs you of agent upgrades, so that you can obtain the latest security protection services in time. The agent needs to collect the CWPP version number, OS configuration information, security rule version number to the cloud for further judgment and prompt. No private data will be extracted in this process.

Agent Process Description

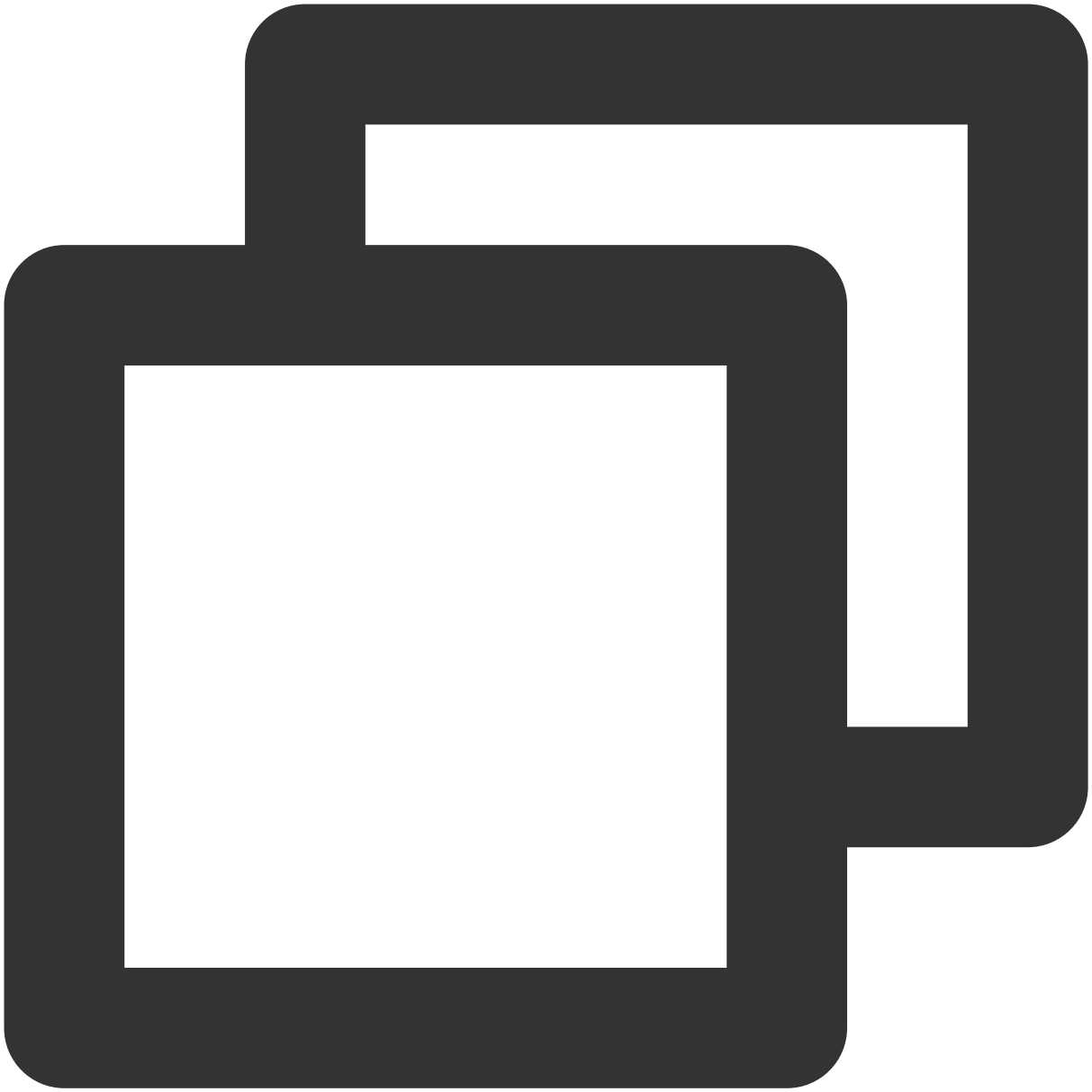
Last updated：2023-12-26 16:39:23

Item	Windows System	Linux System
Program installation directory	C:\\program files\\qcloud\\yunjing\\ydeyes C:\\program files\\qcloud\\yunjing\\ydlive	/usr/local/qcloud/YunJing/
Process name	YDService CWPP main service process YDLive daemon YDPython vulnerability & baseline scan plugin YDQuaraV2 Trojan isolation plugin qtflame assets collection plugin	YDService CWPP main service process YDLive daemon YDPython vulnerability & baseline scan plugin YDUtils process scan plugin YDQuaraV2 Trojan isolation plugin qtflame assets collection plugin tcss-agent container baseline scan plugin tcss-scan container image scan plugin
Registered service	YDService YDLive YDEdr	-

The port used by the agent program is randomly returned by the system, and there is no fixed port range. If the used port conflicts with the port for business, restart the agent program.

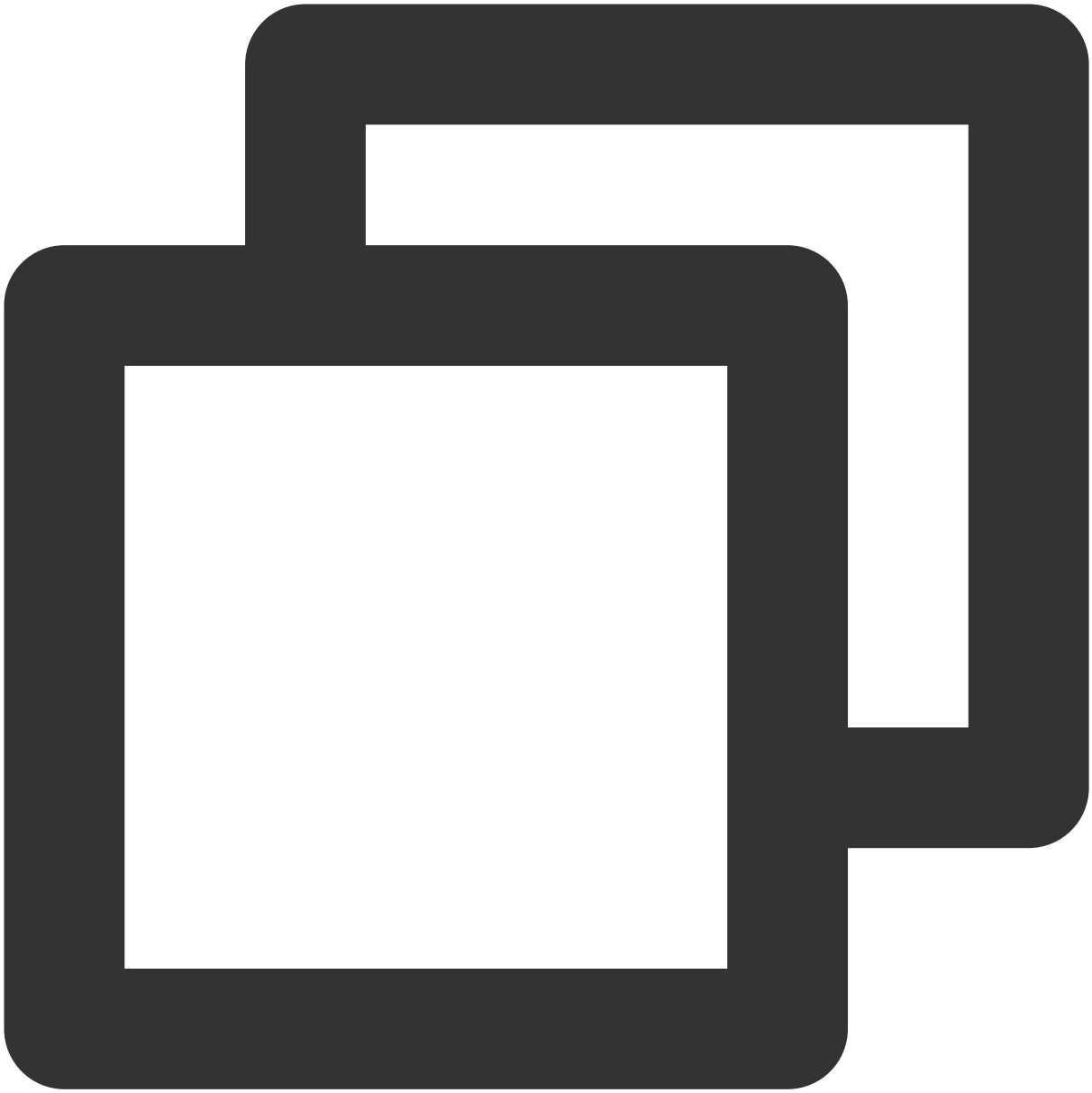
Agent restart commands (Linux)

1.1 Stop the agent program:



```
/usr/local/qcloud/YunJing/stopYDCore.sh
```

1.2 Restart the agent:

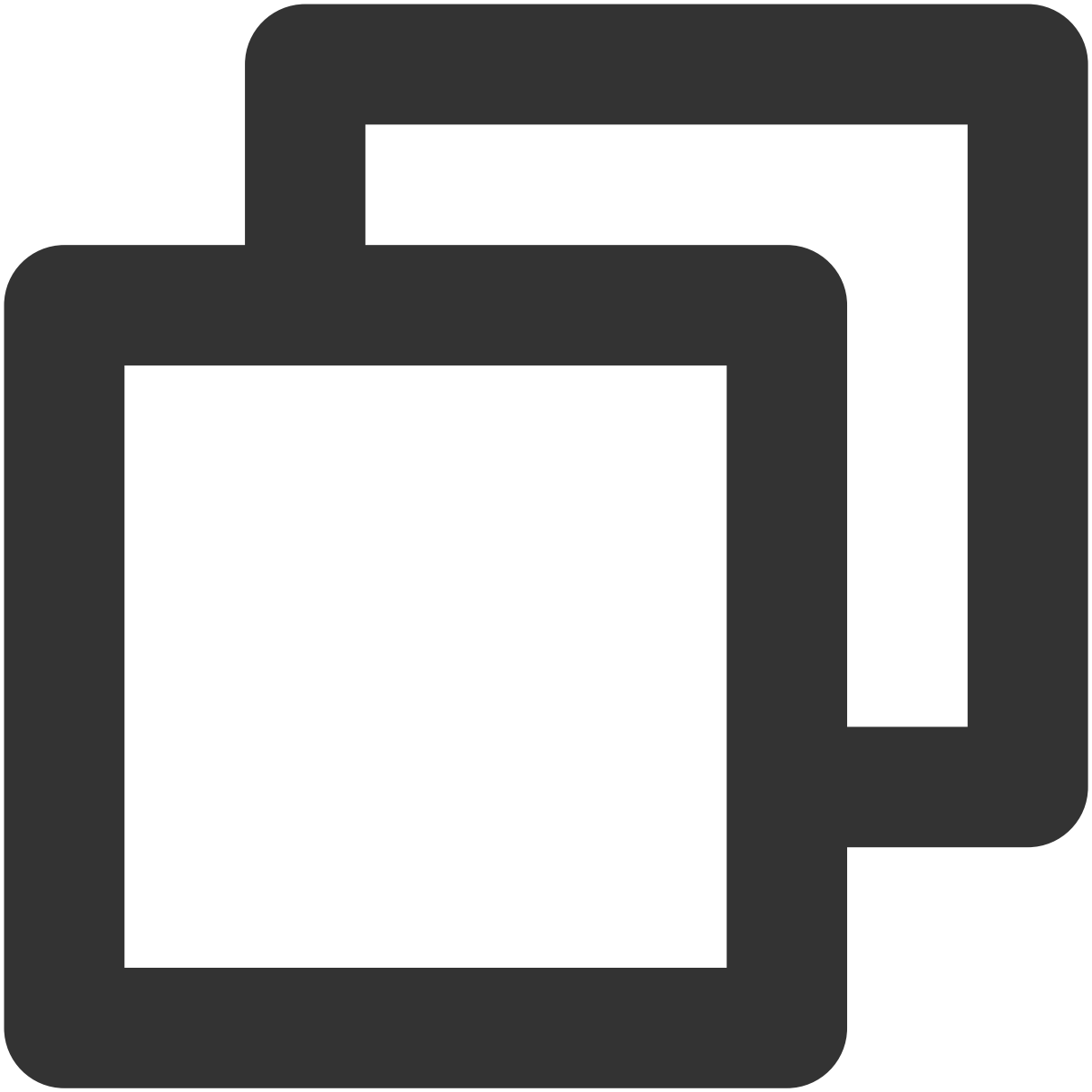


```
/usr/local/qcloud/YunJing/startYD.sh
```

Agent restart commands (Windows)

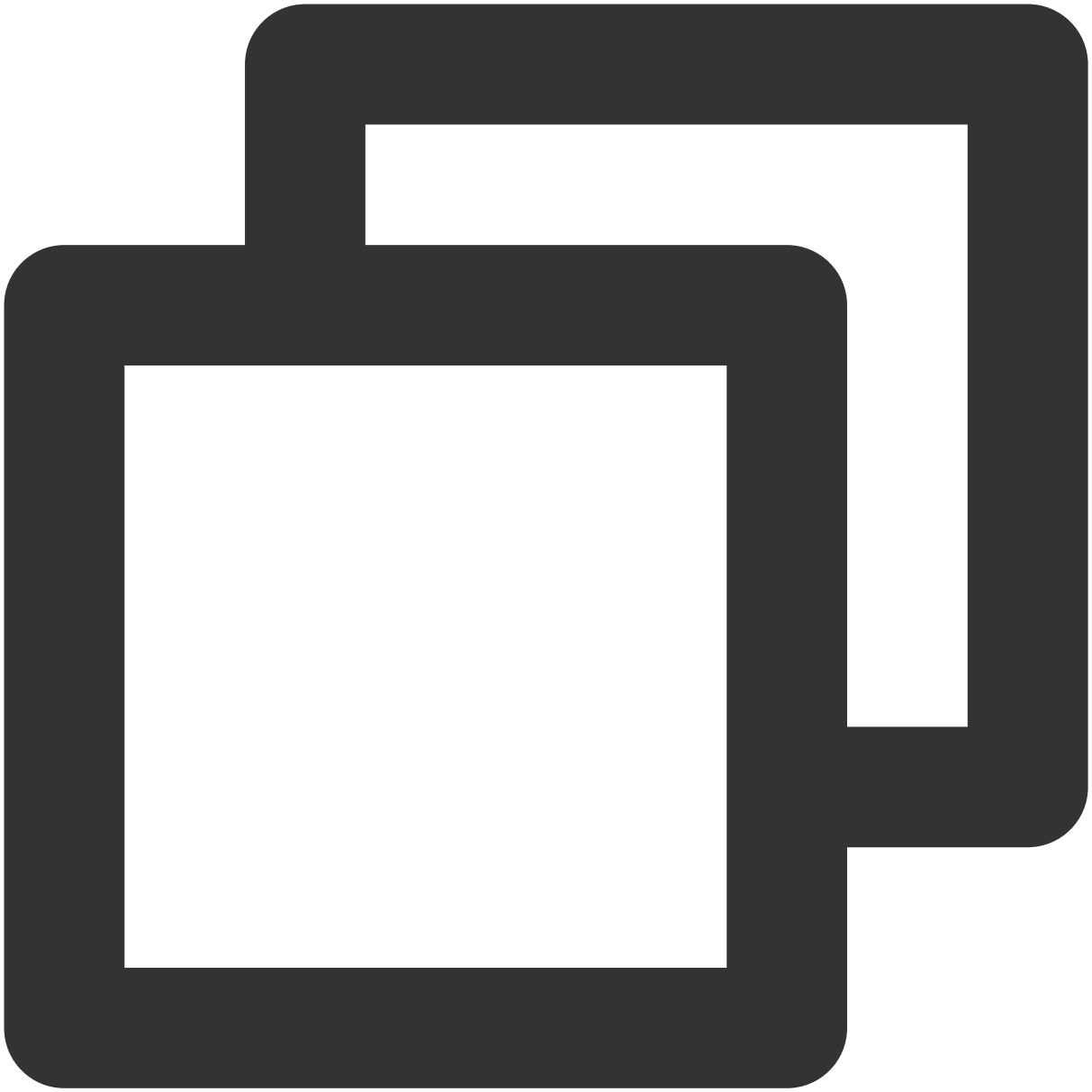
Enter the following commands or open Task Manager, locate YDService, and right-click to restart the agent.

1.1 Stop the agent program:



```
net stop YDService
```

1.2 Restart the agent:



```
net  start YDService
```

A Security Baseline Detection List

Last updated：2024-08-13 16:30:55

This document introduces the list of the security baseline detection in CWPP.

Note:

The security baselines will take effect immediately after product setup.

Name	Level	Vul_type
Unauthorized access to CouchDB.	High	Improper configuration
Docker Daemon 2375 management port is open.	High	Remote code execution
Unauthorized access to Elasticsearch.	High	Improper configuration
JavaRMI remote code execution	High	Remote code execution
The lack of authentication in Jenkins can lead to command execution.	High	Remote code execution
Unauthorized access to Kubelet.	High	Security baseline
Weak password detection of the Linux system	High	Remote code execution.
Unauthorized access to MongoDB.	High	Improper configuration
Weak password detection of MySQL	High	Weak password
NFS misconfiguration leads to mountable sensitive directory.	High	Improper configuration
Baseline compliance detection of Redis	High	Remote code execution
Improper configuration detection of RPCBind	High	Security baseline
Weak password detection of Rsync	High	Weak password
Rsync passwordless access	High	Improper configuration

Weak password detection of Tomcat	High	Weak password
Weak password detection of Windows users	High	Weak password
Xampp default FTP password	High	Information leakage
Backup files exist in the website directory.	High	Information leakage
Anonymous log-in detection of FTP	Medium	Information leakage
IIS misconfiguration leads to parsing vulnerability.	Medium	Improper configuration
Memcached UDP port can be exploited for DDOS amplification attacks.	Medium	Information leakage
PHP-FPM misconfiguration	Medium	Security baseline
Compliance detection of PostgreSQL	Medium	Remote code execution
Information leakage due to the presence of a .git folder exists in the Web directory.	Medium	Information leakage
Information leakage due to the presence of a .svn folder exists in the Web directory.	Medium	Information leakage.
Hidden account detection of Windows	Medium	Security baseline
Shadow account detection of Windows	Medium	Remote code execution
Unauthorized access to ZooKeeper.	Medium	Improper configuration
Unauthorized access to Hadoop.	Low	Remote code execution
Passwordless user detection of sudo	Low	Security baseline.
Sample directory detection of Tomcat	Low	Security baseline
A phpinfo file exists in the Web directory.	Low	Information leakage
Guest account status detection of Windows	Low	Security baseline

Parsing of JSON Format Alarm Data

Last updated：2024-08-13 16:31:31

This document will introduce the transmission fields and descriptions of various alarms received after you set JSON format alarm data reception in alarm settings > **Robot Notification**.

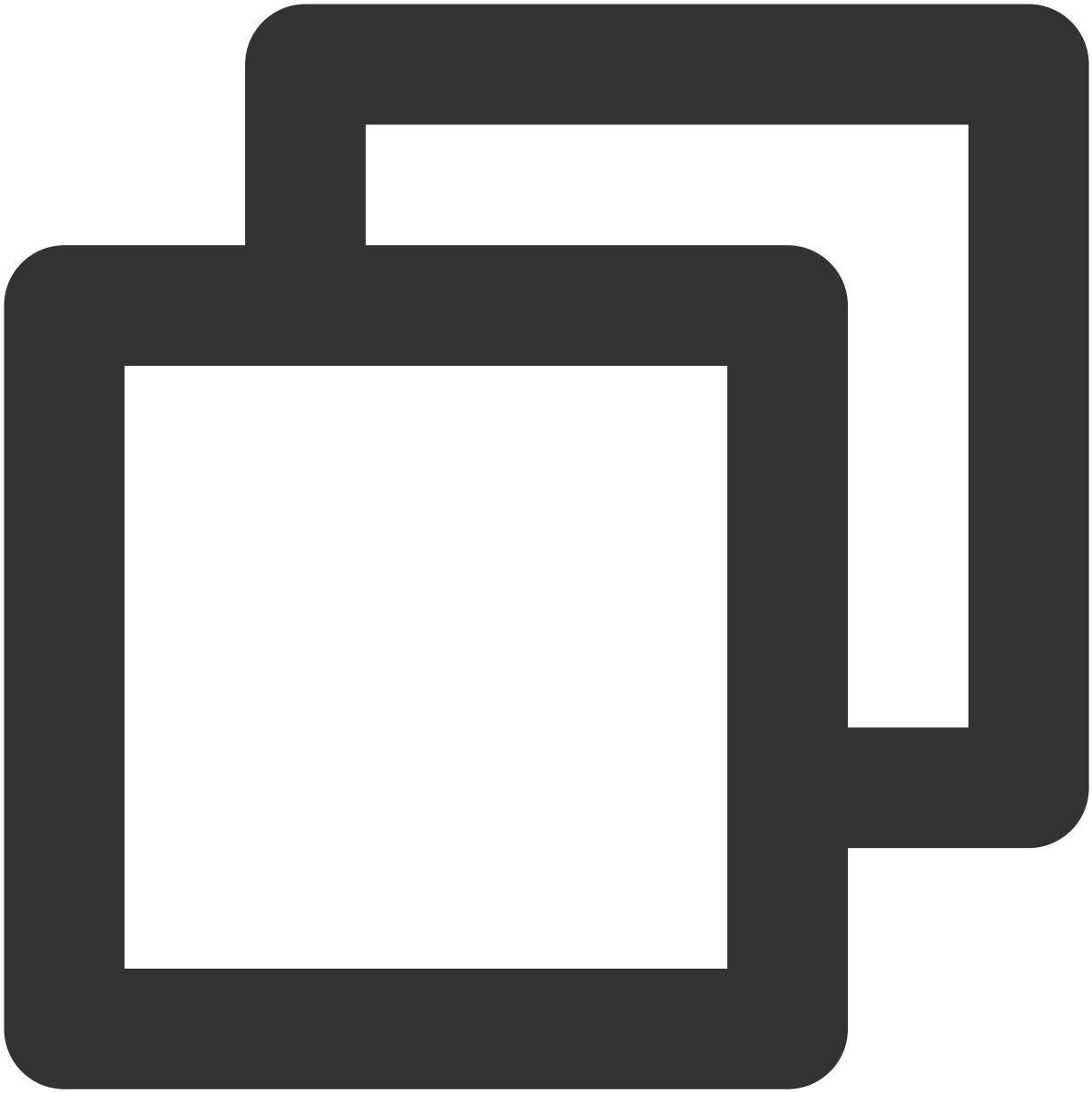
Note

Currently, robot notification is in a grayscale status and is only open to customers with a clear demand for it. If you want to receive CWPP webhook robot alarms in real-time, you can contact us to apply for use.

Alarm settings > **Robot Notification** is independent of the message center robot and is not related to it.

Public Fields

Sample



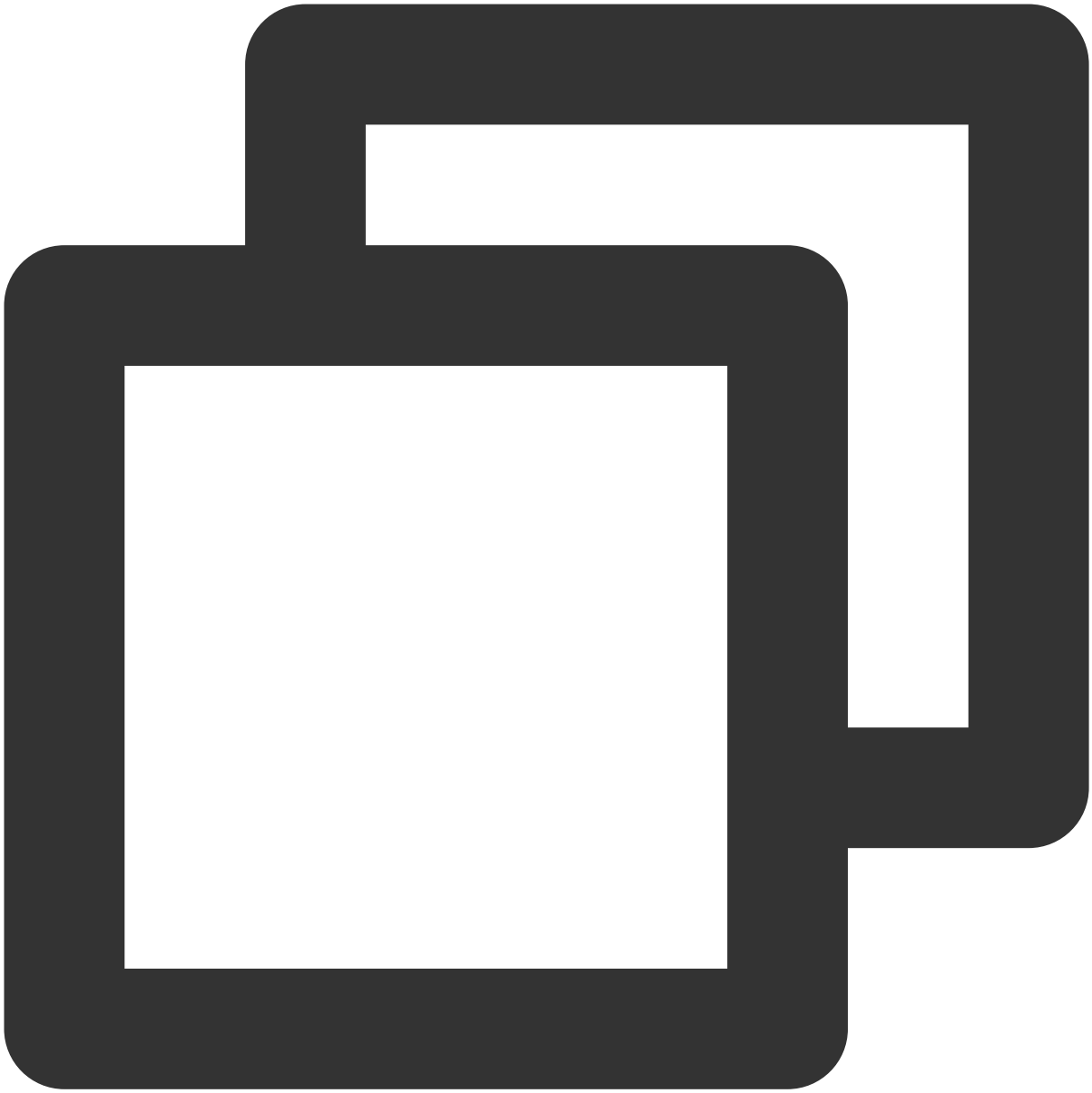
```
{
    "uin": "1000xxxxxx21",
    "nickname": "Test Account",
    "server": "172.x.x.41 [Test Machine]",
    "instance_id": "ins-xxxxxxxx",
    "region": "Southwest China (Chengdu)",
    "time": "October 30, 2023 09:24:20"
}
```

Field Description

Field name	Description
uin	User UIN
nickname	User's nickname
server	Machine IP [Machine alias]
instance_id	Machine instance ID
region	Region where the machine located
time	Event time

Exceptional Log-in

Sample



```
{
    "event_type": "Exceptional Log-in",
    "src_ip": "43.x.x.41",
    "area": "Hong Kong (China)",
    "level": "High-risk"
}
```

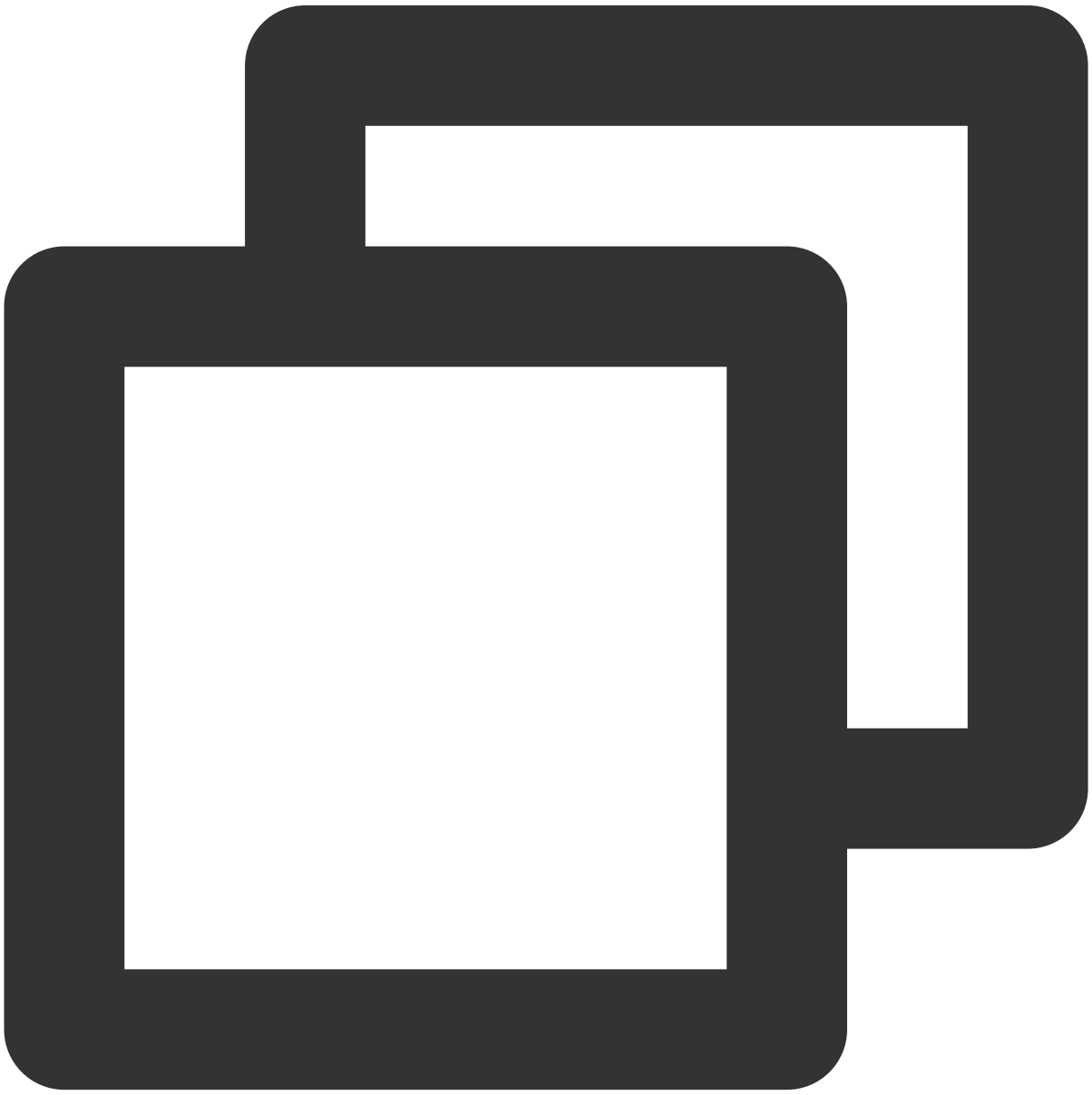
Field Description

Field name	Description

src_ip	Source IP
area	Source location
level	Risk level

Password Cracking

Sample



```
{
    "event_type": "Password Cracking",
    "src_ip": "43.x.x.41",
    "area": "Hong Kong (China)",
    "count": "3",
    "banned": "Block Success"
}
```

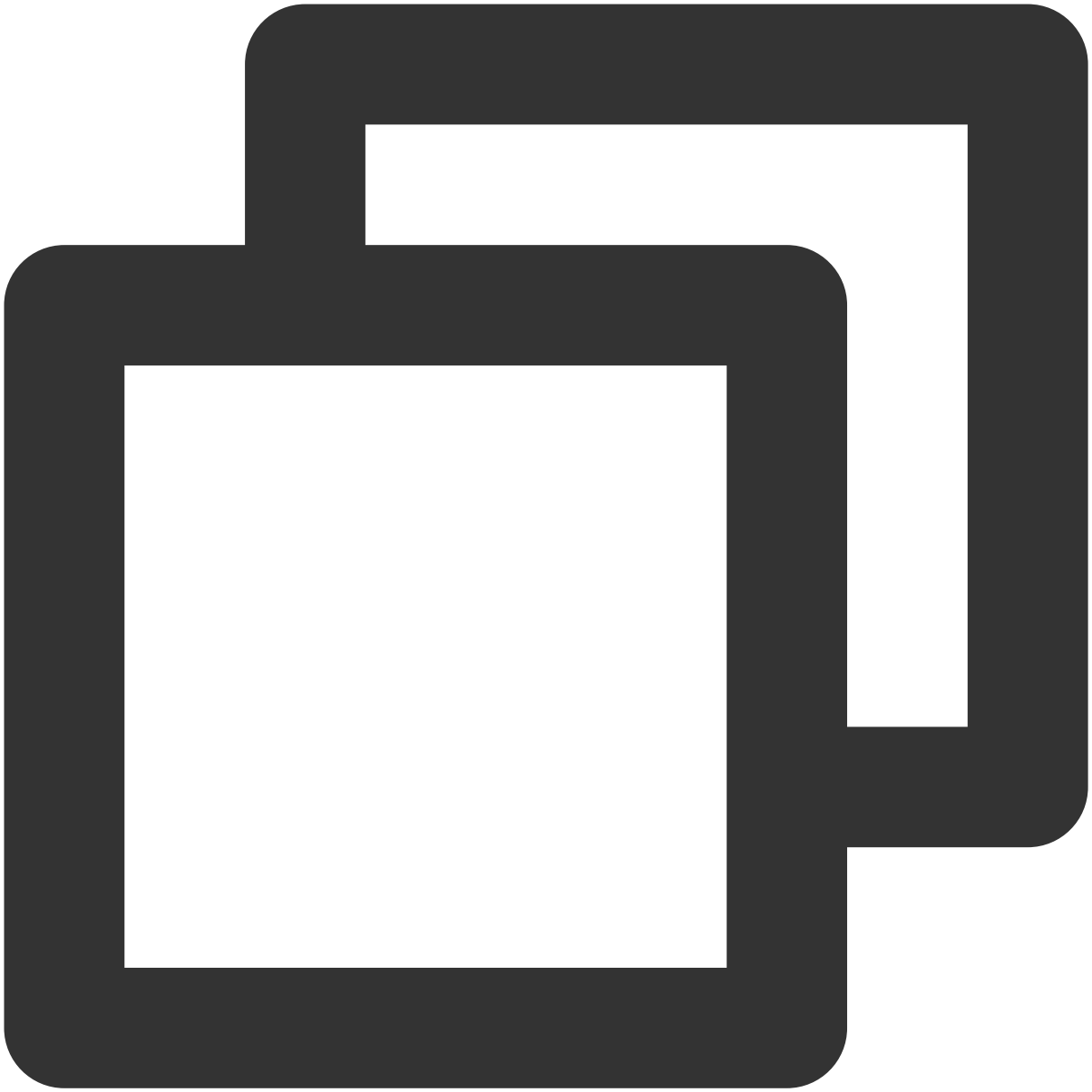
Field Description

Field name	Description
src_ip	Source IP
area	Source location
count	Number of attempts
banned	Blocking status

Malicious File Scan

Malicious Files

Sample



```
{
    "event_type": "Malicious Files",
    "file_type": "Malicious",
    "path": "/root/bebinder_shell.jsp",
    "level": "Severe. Your server may have been hacked. It is recommended to verify
}
```

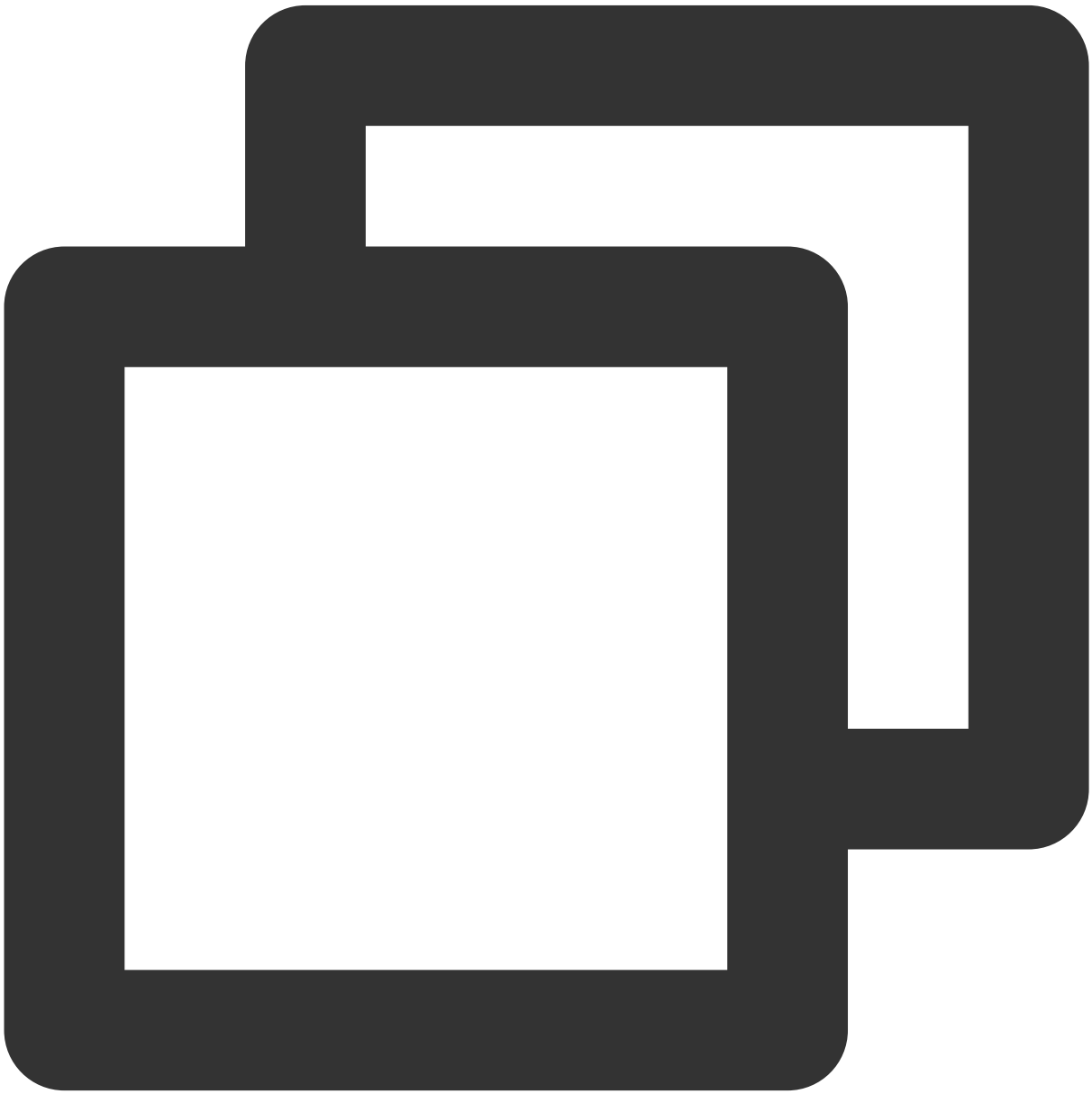
Field Description

Field name	Description

file_type	File type
path	File path
level	Danger level

Exceptional Processes

Sample



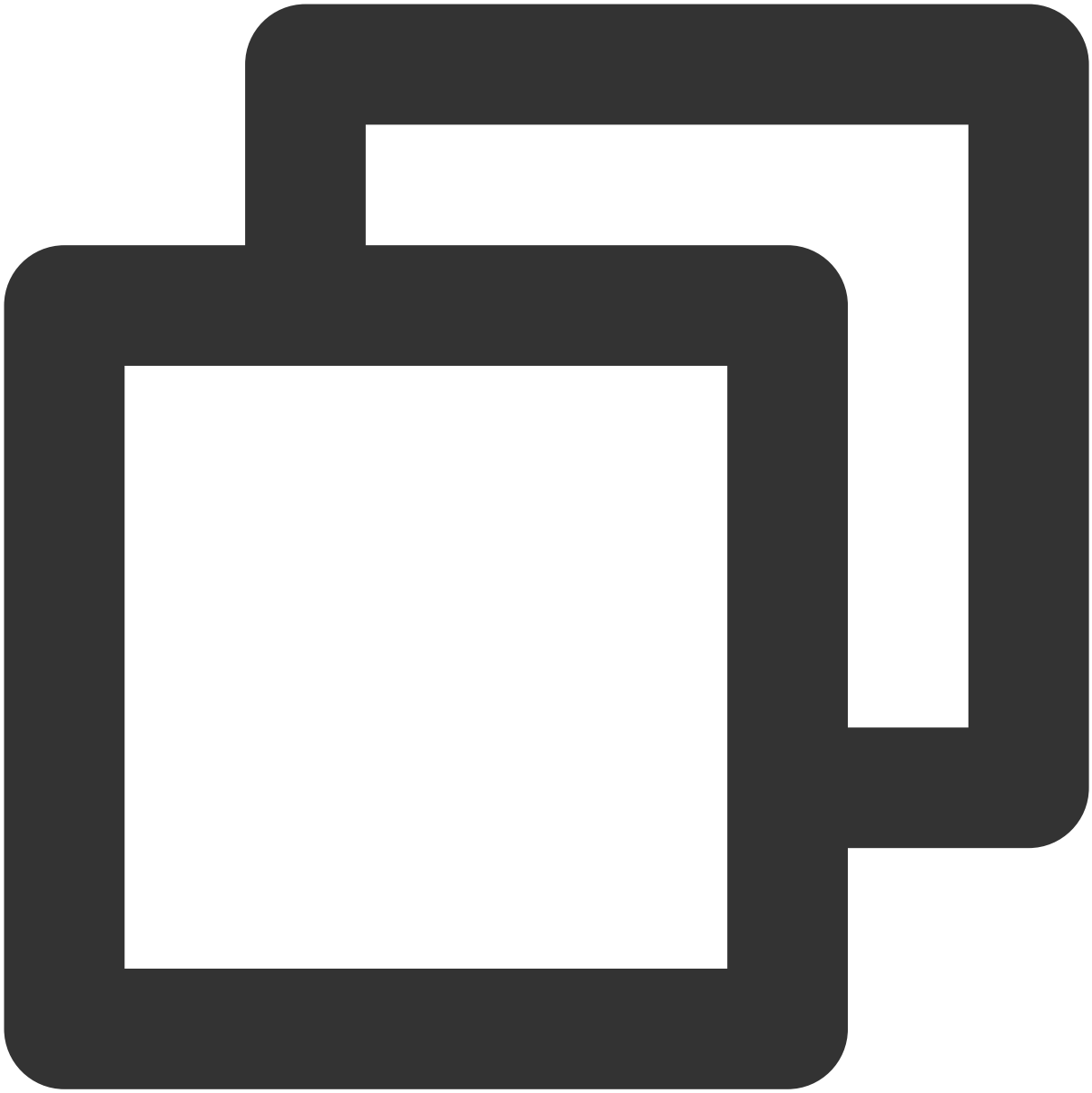
```
{
    "event_type": "Exceptional Processes",
    "pid": "5916",
    "path": "/root/2/ISHELL-v0.2/ishd"
}
```

Field Description

Field name	Description
pid	Process ID
path	Process path

Malicious Requests

Sample



```
{
    "event_type": "Malicious Requests",
    "url": "massdns.ran6066.com",
    "count": "1"
}
```

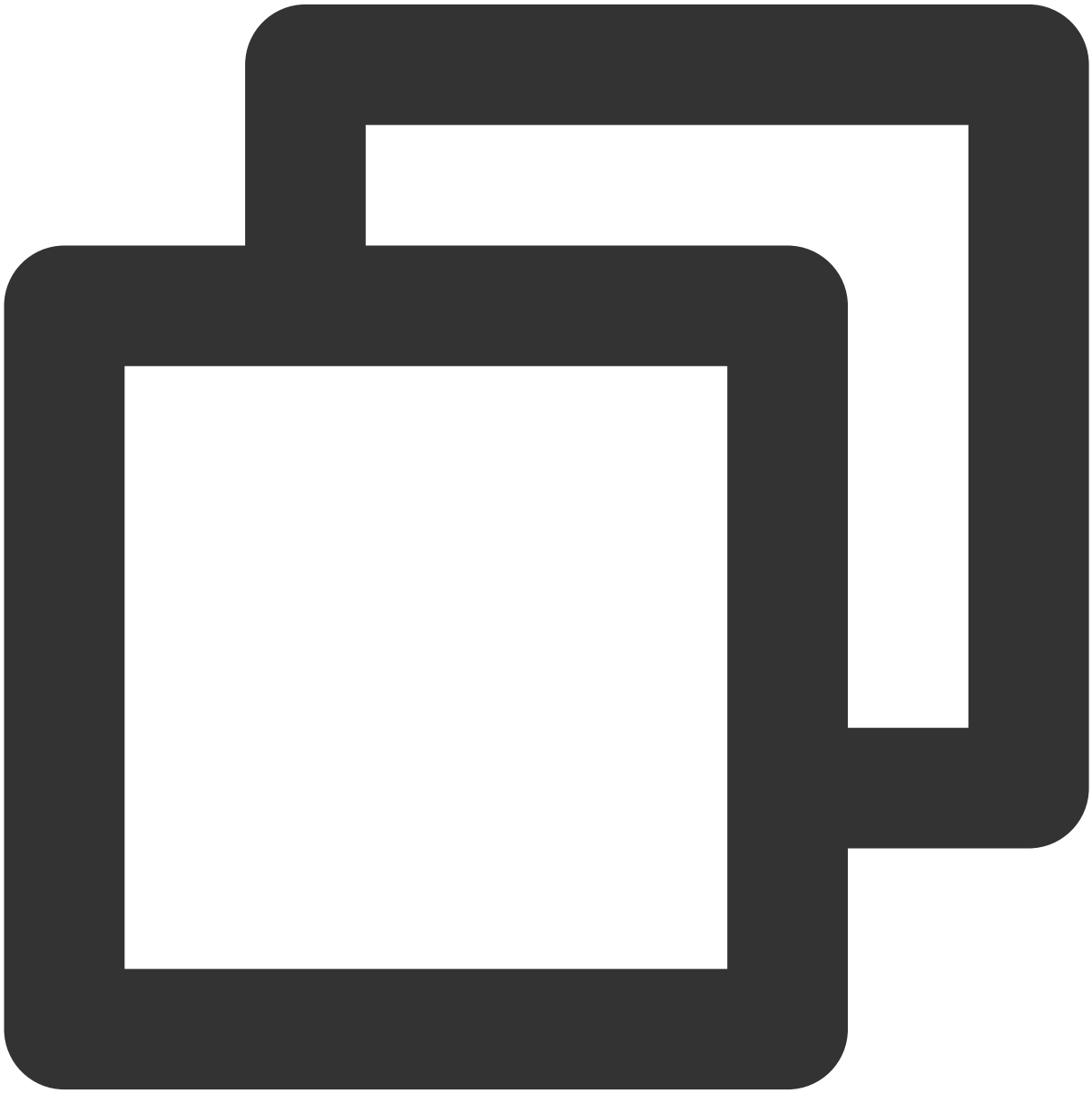
Field Description

Field name	Description

url	Malicious domain
count	Number of requests

High Risk Commands

Sample



```
{
```

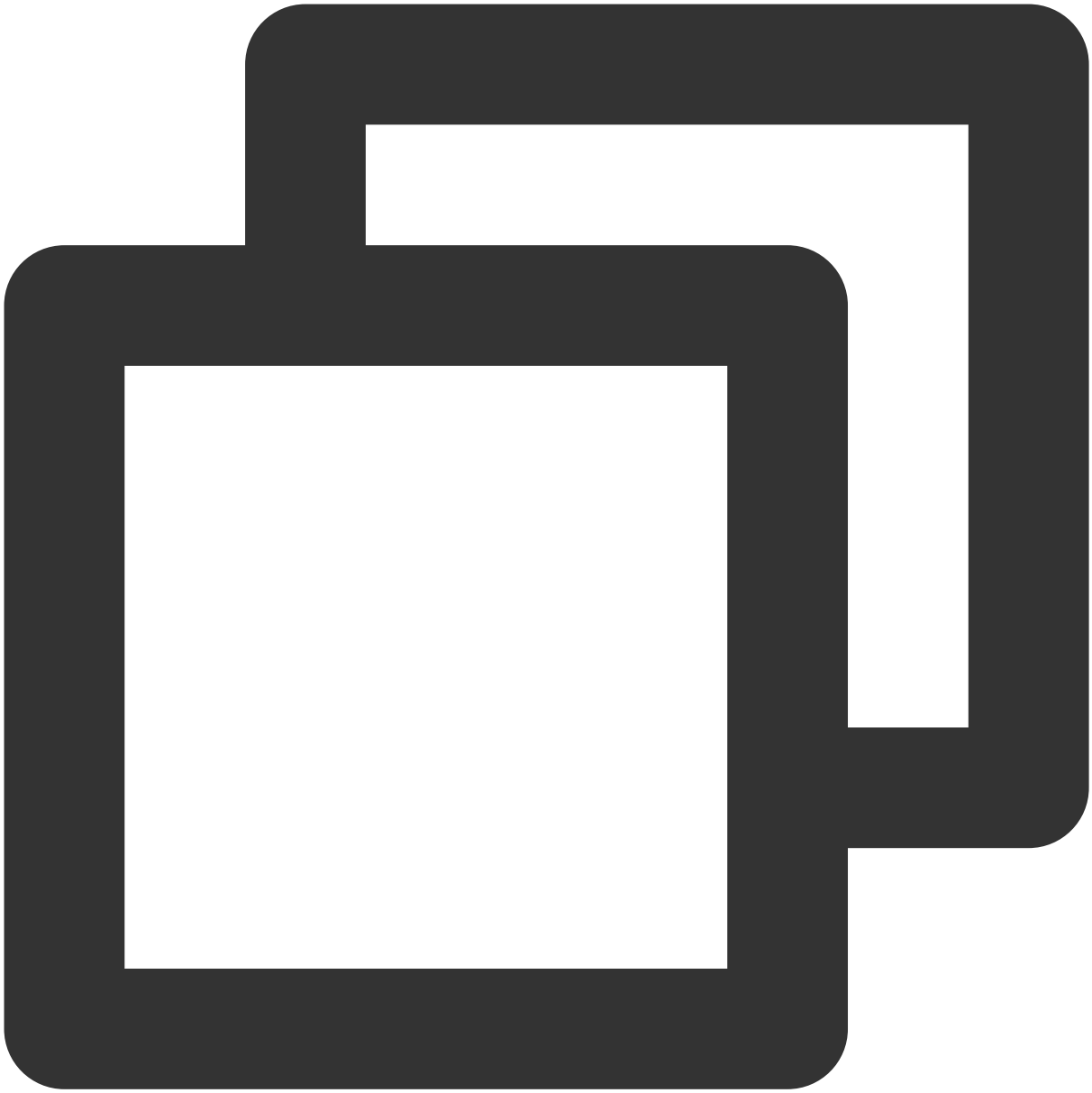
```
    "event_type": "High Risk Commands",
    "cmd": "iptables-restore -w 5 --noflush",
    "level": "High-risk",
    "status": "Processing"
}
```

Field Description

Field name	Description
cmd	Command content
level	Threat level
status	Processing status

Local Privilege Escalation

Sample



```
{
    "event_type": "Local Privilege Escalation",
    "user": "0",
    "process": "Privilege"
}
```

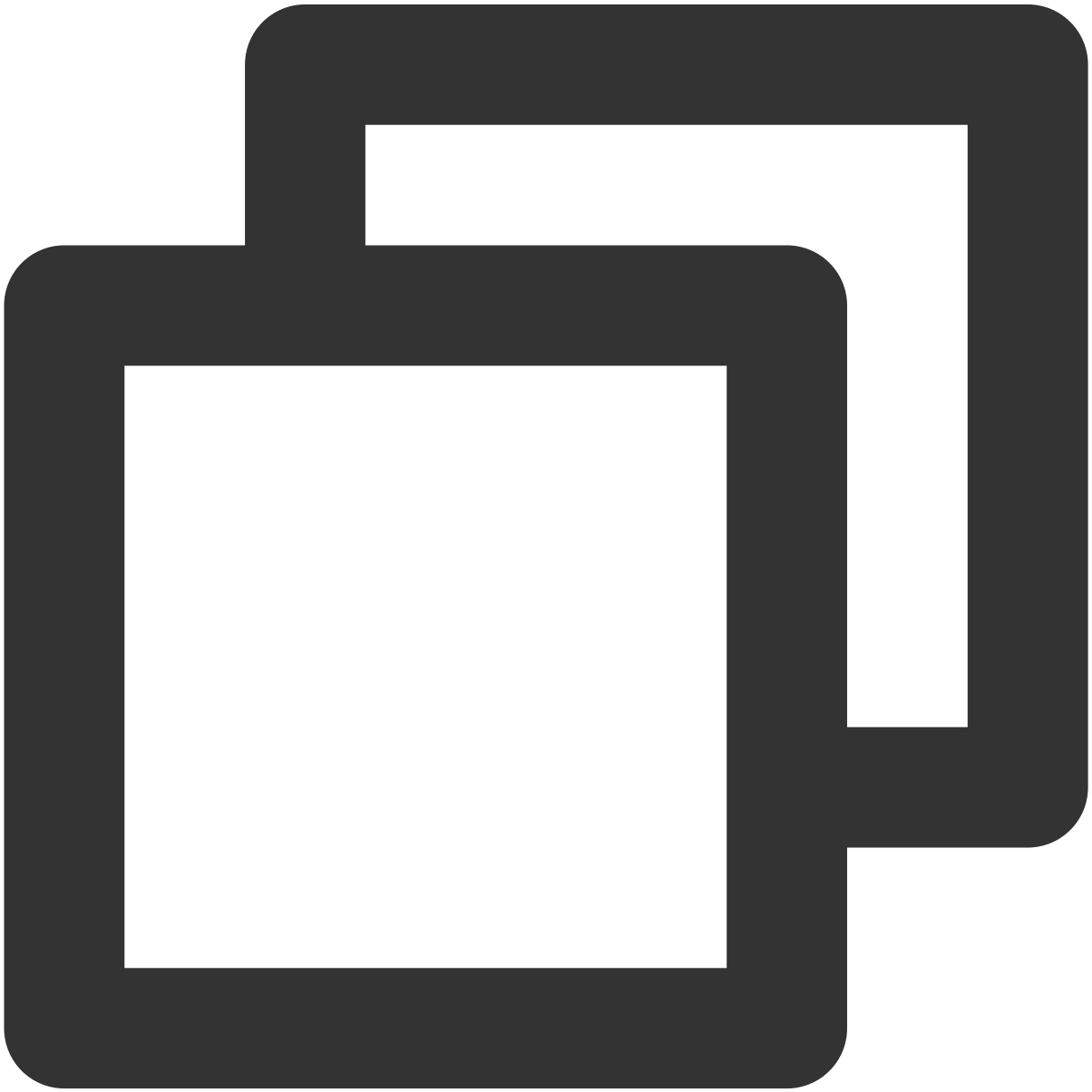
Field Description

Field name	Description

user	Privilege escalation user
process	Privilege escalation process

Reverse Shell

Sample



```
{
```

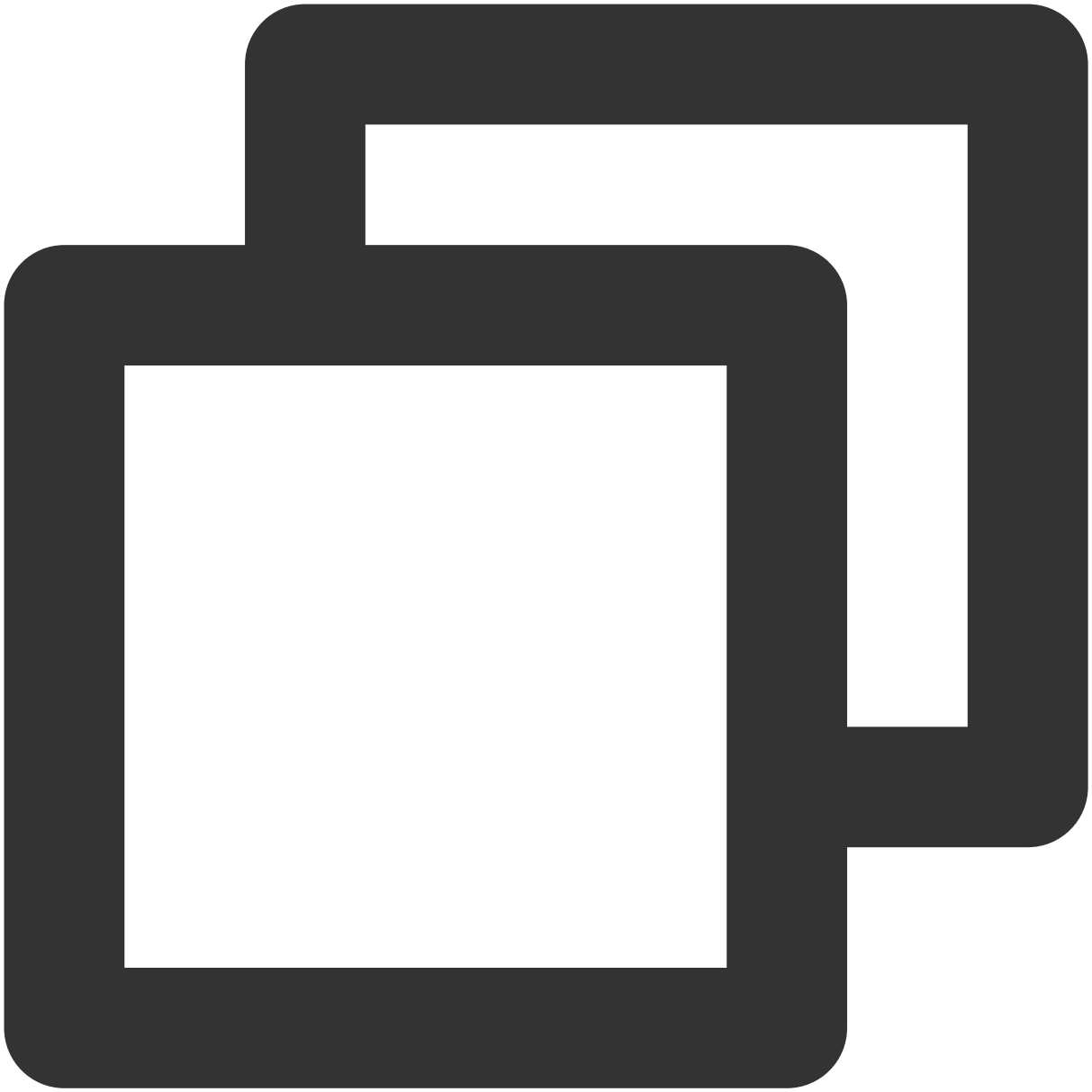
```
    "event_type": "Reverse Shell",
    "process": "mass_0",
    "dst_ip": "125.x.x.220",
    "dst_port": "8888"
}
```

Field Description

Field name	Description
process	Process name
dst_ip	Target host
dst_port	Target port

Java Webshell

Sample



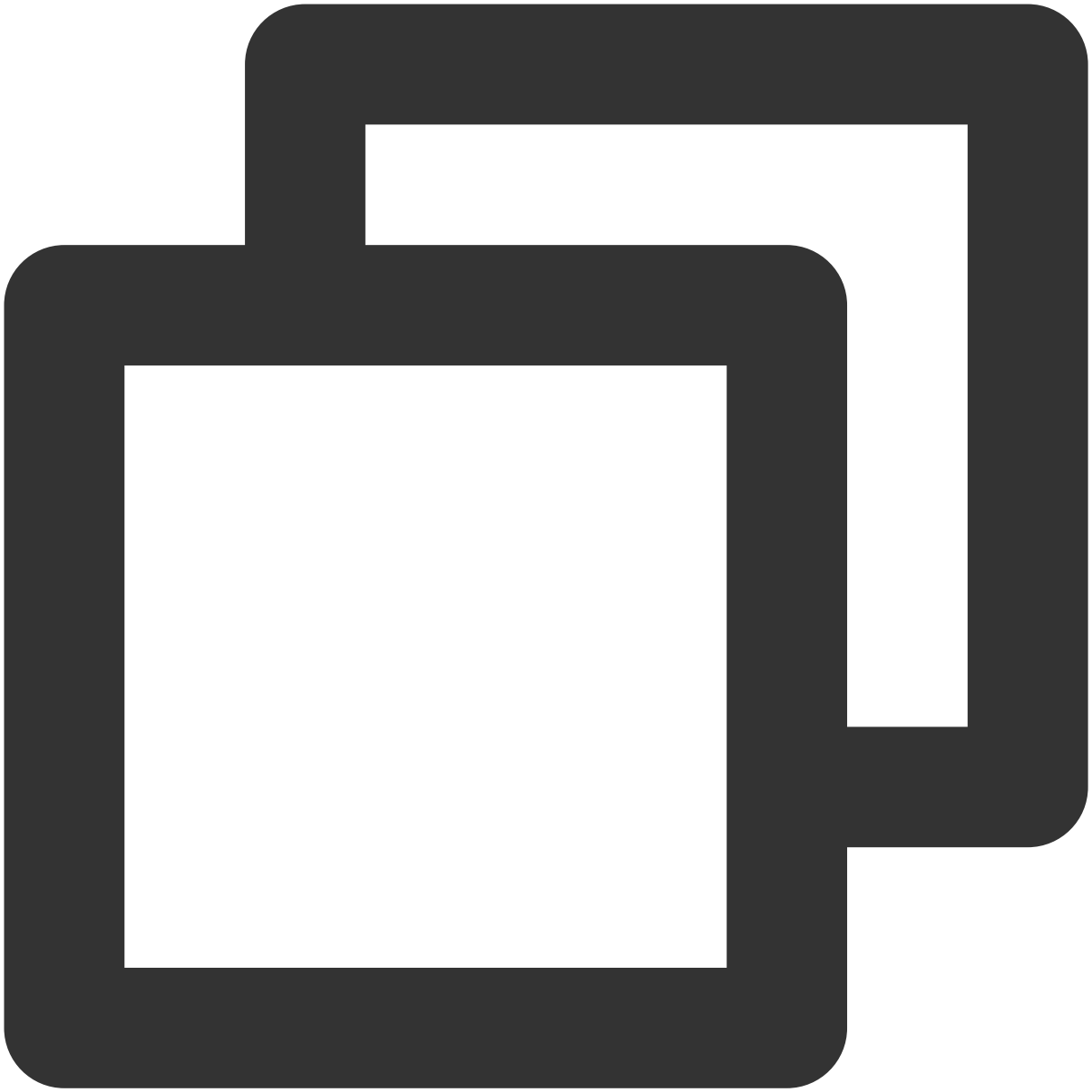
```
{
    "event_type": "Java Webshell",
    "type": "Java Webshell - Servlet",
    "pid": "3333",
    "argv": "masstest",
    "class_name": "massTest"
}
```

Field Description

Field name	Description
type	Java Webshell type
pid	Process ID
argv	Process parameters
class_name	Java Webshell class name

Core File Monitoring

Sample



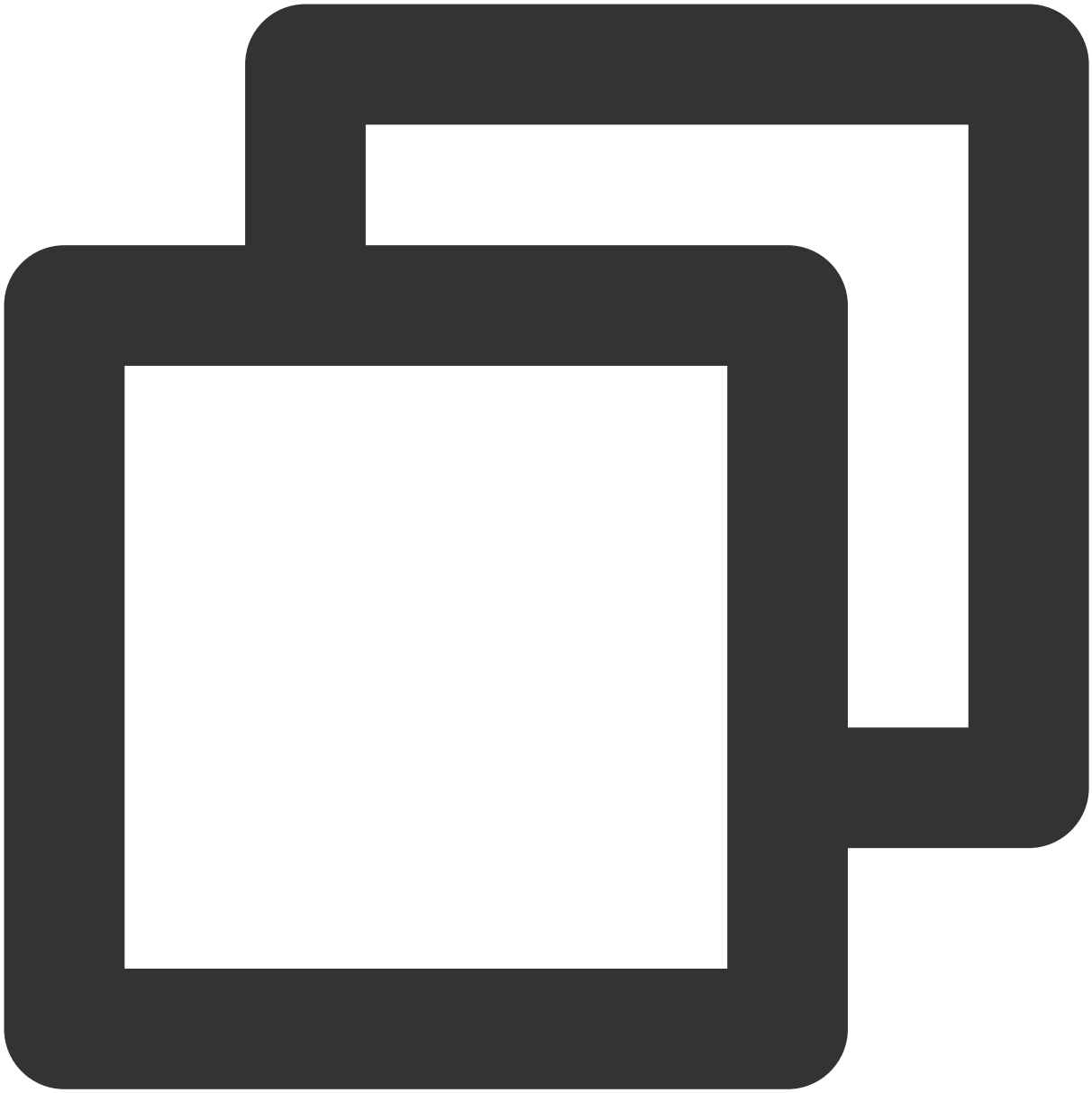
```
{
    "event_type": "CoreFiles",
    "rule_name": "adwqdadwqd",
    "exe_path": "/usr/bin/systemd-tmpfiles",
    "file_path": "/home",
    "count": "1",
    "level": "High-risk"
}
```

Field Description

Field name	Description
rule_name	Hit rule name
exe_path	Process path
file_path	File path
count	Event count
level	Threat level

Network Attacks

Sample



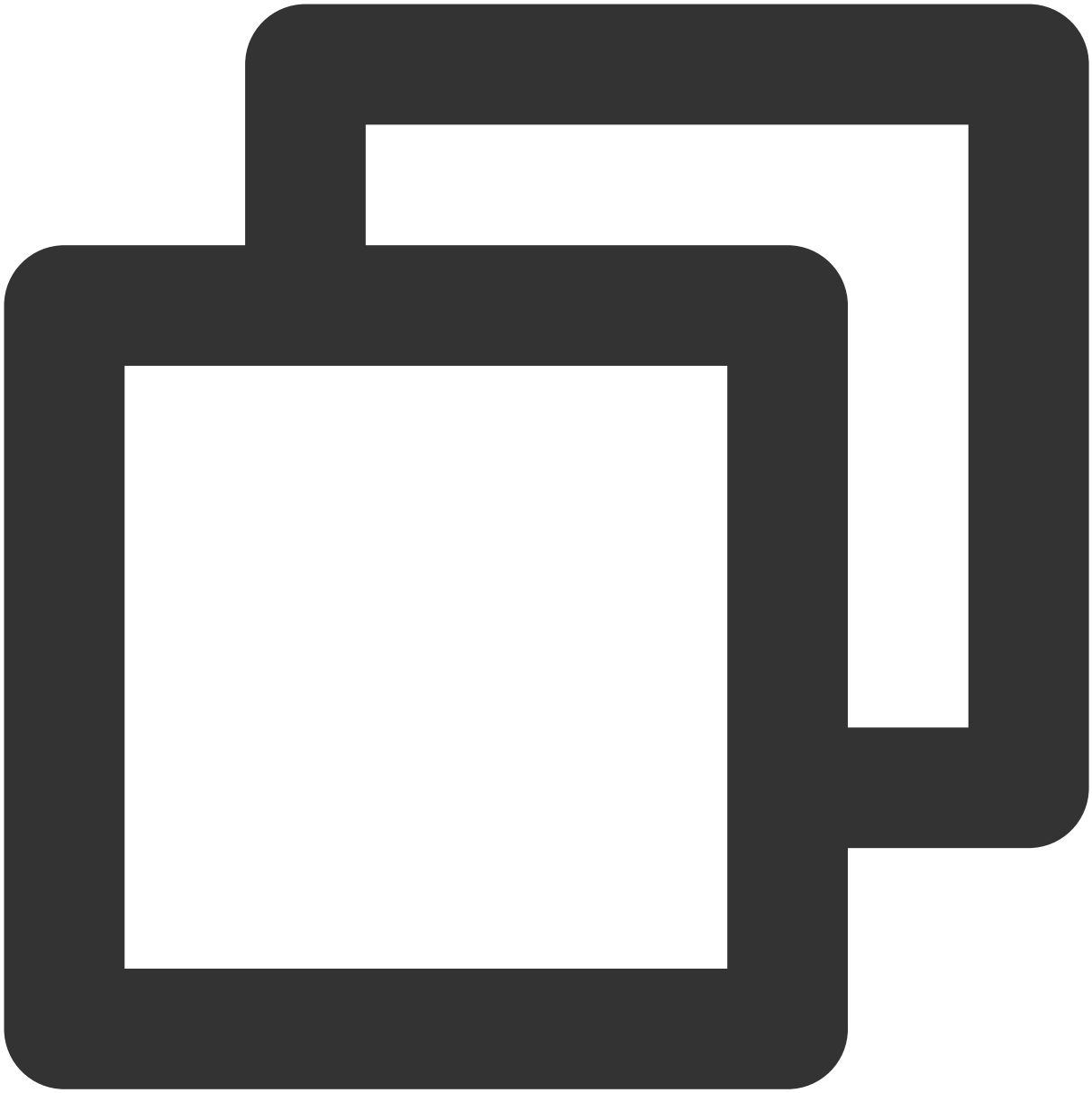
```
{
    "event_type": "Network Attacks",
    "src_ip": "129.x.x.166",
    "city": "Nanjing City, Jiangsu Province",
    "vul_name": "showdoc File Upload Vulnerability",
    "dst_port": "80",
    "status": "Attempted Attacks"
}
```

Field Description

Field name	Description
src_ip	Source IP
city	Source city
vul_name	Vulnerability name
dst_port	Target port
status	Attack status

Offline Client

Sample

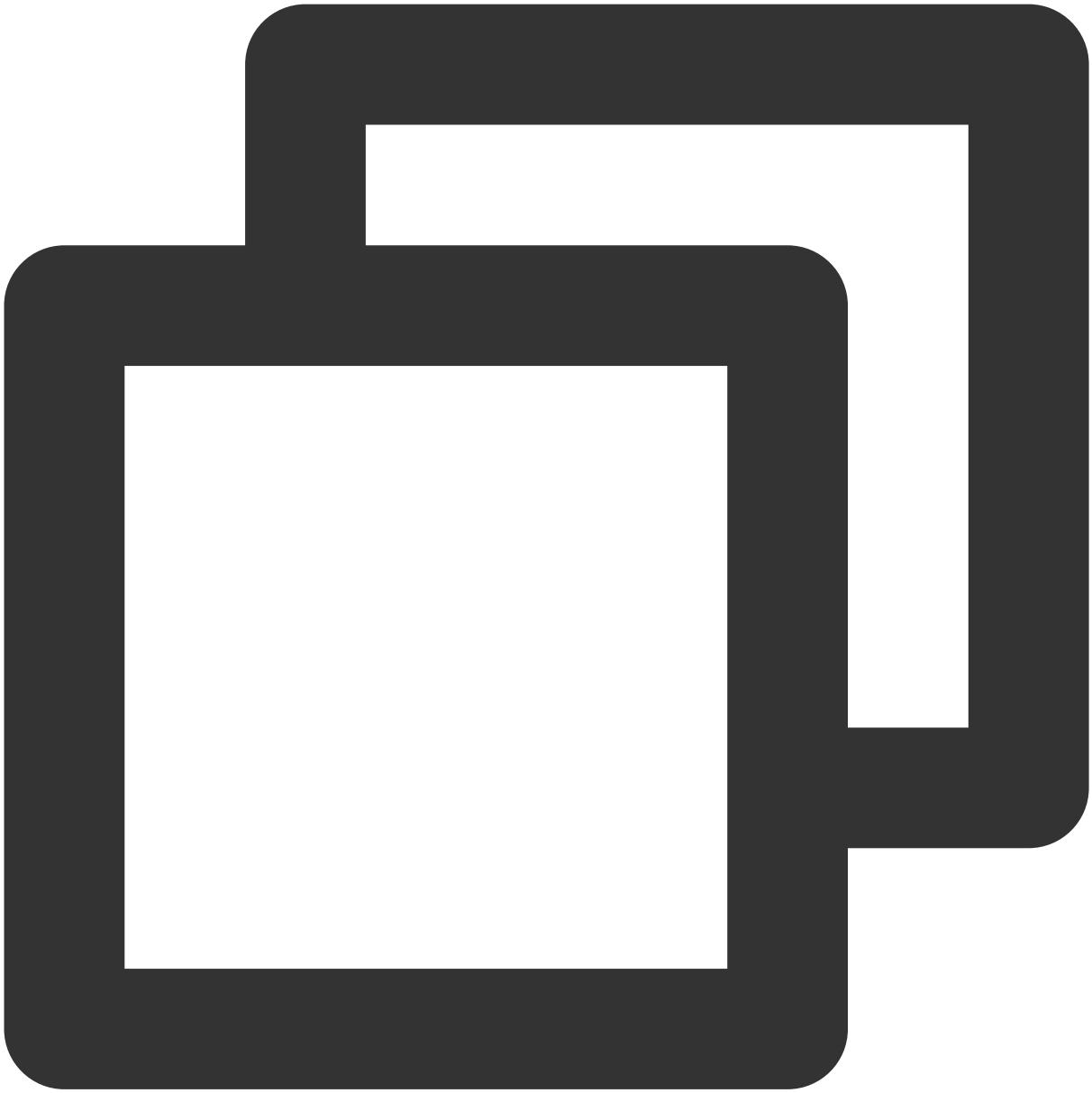


```
{
    "event_type": "Offline Client",
    "offline_hour": "1"
}
```

Field Description

Field name	Description
offline_hour	Client offline duration

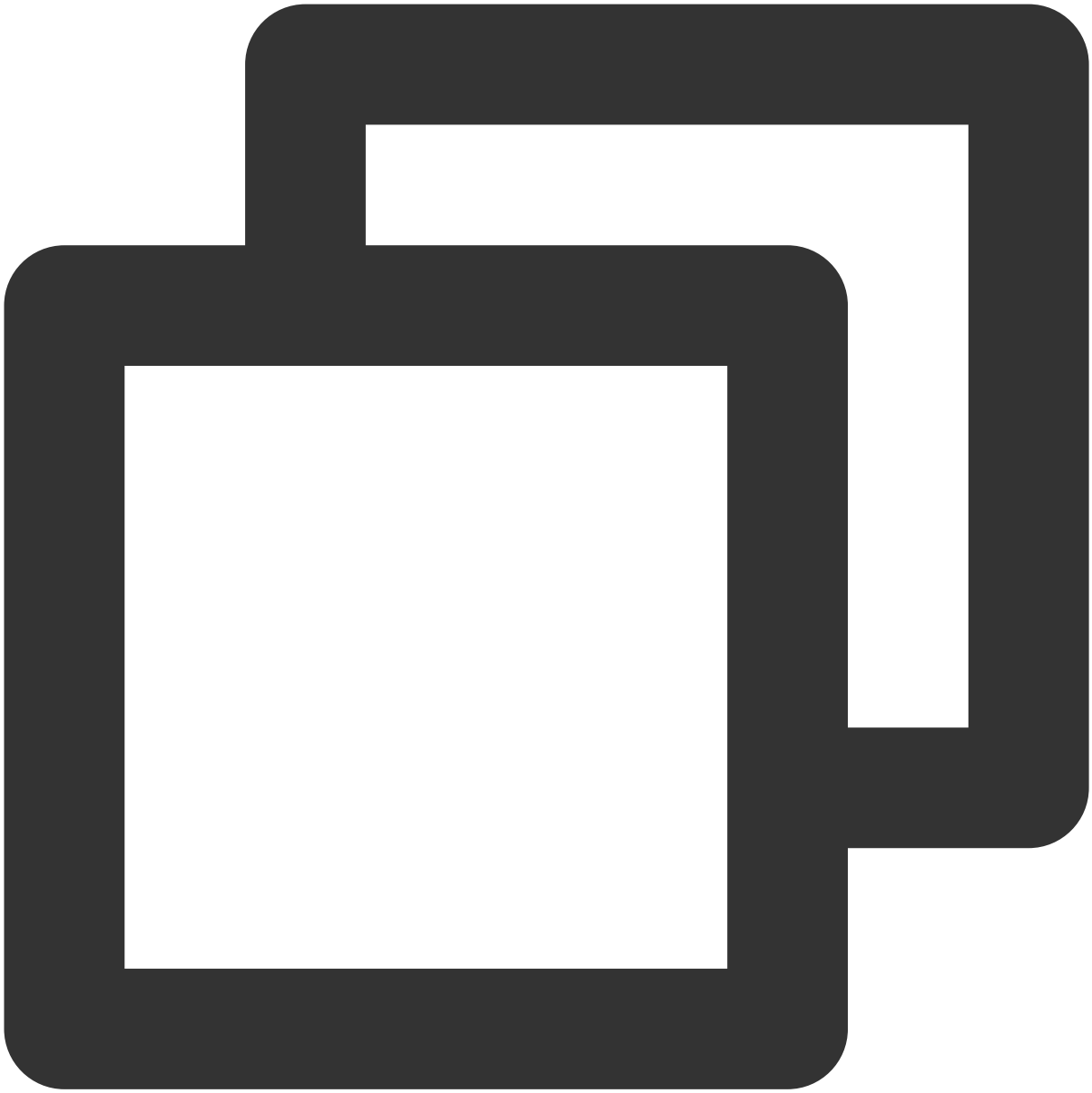
##Client Uninstallation



```
{
    "event_type": "Client Uninstallation"
}
```

Vulnerability Notification

Sample



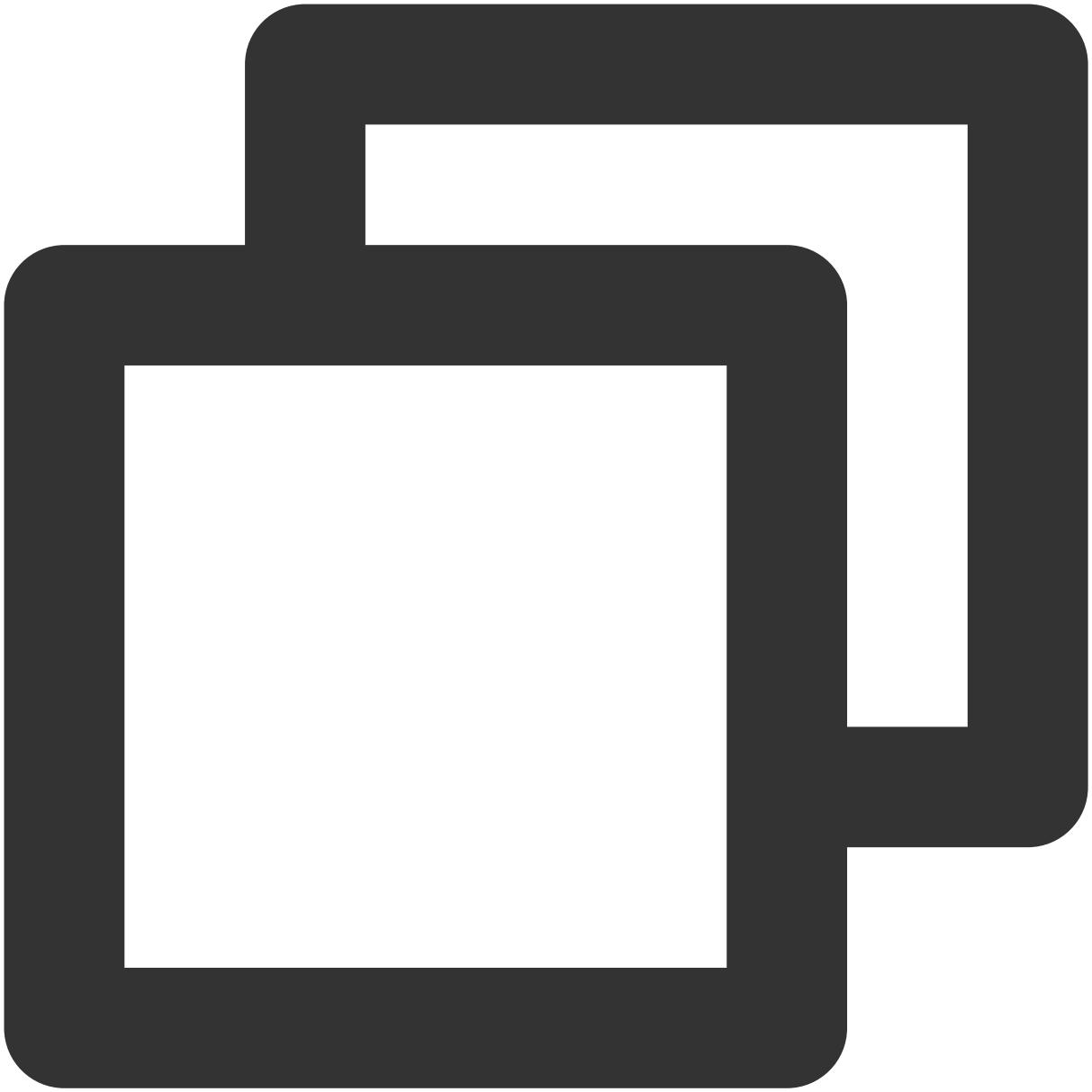
```
{
    "event_type": "Vulnerability",
    "category": "Linux Software Vulnerabilities",
    "vul_name": "libexpat Code Execution Vulnerability (CVE-2022-40674)",
    "level": "Critical"
}
```

Field Description

Field name	Description
category	Vulnerability category
vul_name	Vulnerability name
level	Threat level

Baseline Notification

Sample



```
{
    "event_type": "Baseline",
    "category": "Linux System Weak Password Detection",
    "rule_name": "Linux System Weak Password Detection",
    "level": "High-risk"
}
```

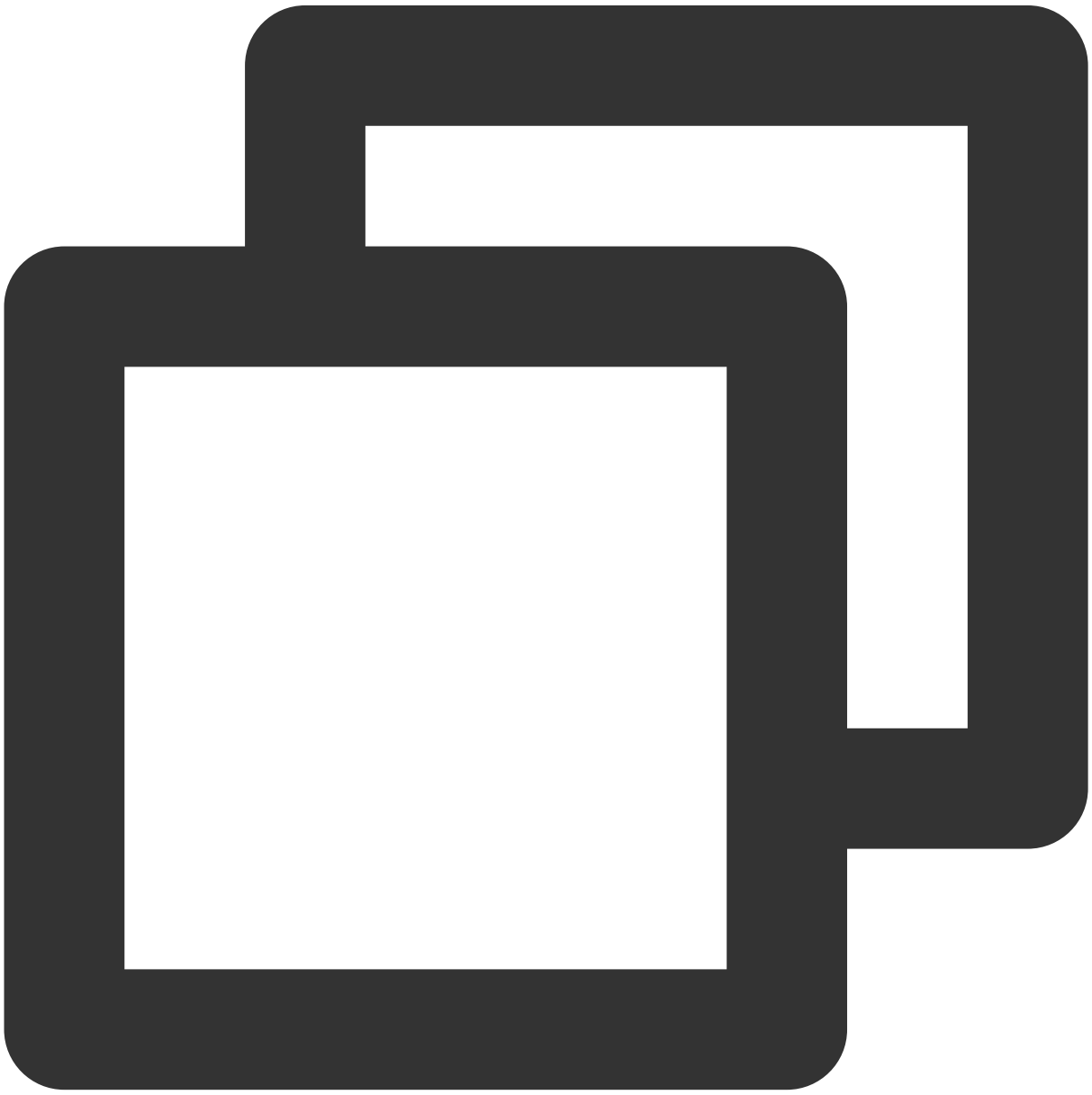
Field Description

Field name	Description

category	Baseline category
rule_name	Rule name
level	Threat level

Ransomware Defense

Sample



```
{
    "event_type": "Ransomware Defense",
    "file_path": "/usr/bin/vi"
}
```

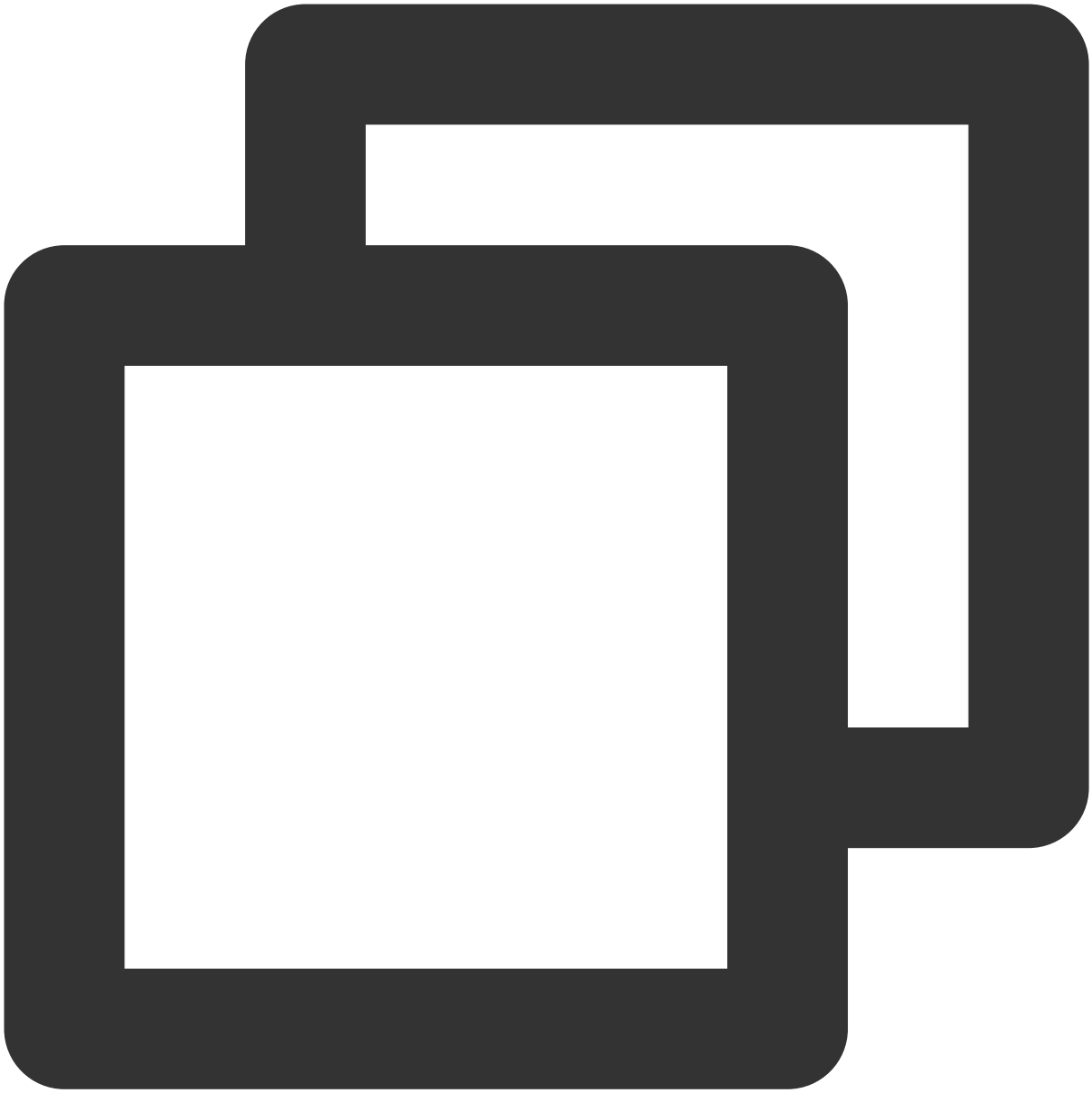
Field Description

Field name	Description
file_path	File directory

Web Tamper Protection

Successful Tampering

Sample



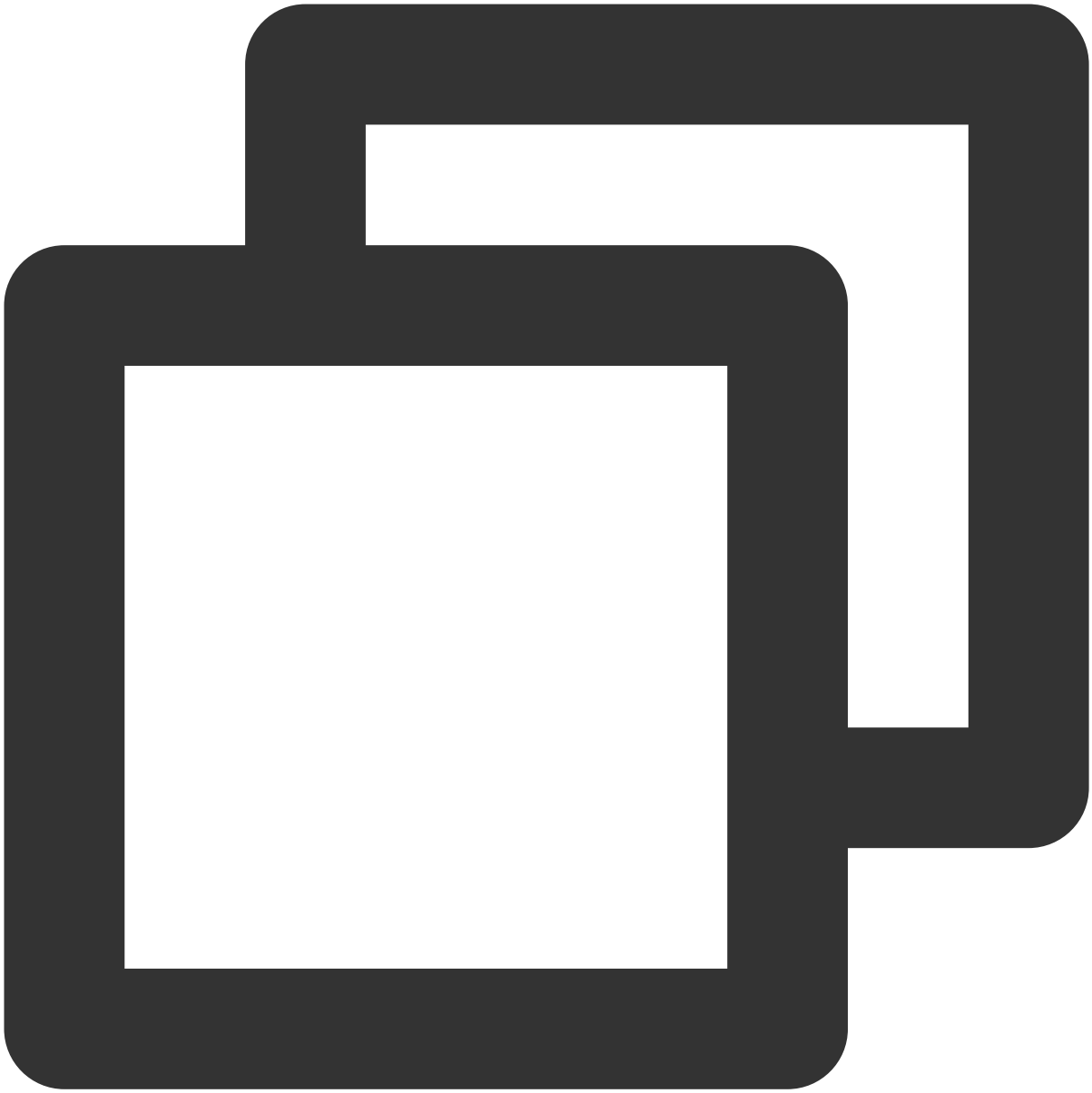
```
{
    "event_type": "Web Tamper Protection (Successful Tampering)",
    "protect_name": "Important File",
    "protect_path": "/tmp",
    "recover_type": "New File Creation",
    "recovered_status": "Not Recovered",
}
```

Field Description

Field name	Description
protect_name	Protection name
protect_path	Protection directory
recover_type	Event type
recovered_status	Event status

Recovery Failed

Sample



```
{
    "event_type": "Web Tamper Protection (Recovery Failed)",
    "protect_name": "Important File",
    "protect_path": "/tmp",
    "exception": "Client Offline"
}
```

Field Description

Field name	Description

protect_name	Protection name
protect_path	Protection directory
exception	Reason for failure

Log Field Data Parsing

Last updated：2024-08-16 17:34:08

Global Specification

Log contents are in JSON format.
Log character encoding is in UTF-8 format.
Logs contain common fields and type-specific fields. Refer to Fields Description for details.
Currently, logs are divided into three types: event logs, asset logs, and client logs

Log Type

The log type is determined by the common field cls_event_type, and currently, the log type values are defined as follows:

Event Logs

cls_event_type	Log Type Values
malware	Malicious File Scan
risk_process	Abnormal Process
hostlogin	Unusual Login
bruteattack	Password Cracking
risk_dns	Malicious Request
bash	High-risk Commands
privilege_escalation	Local Privilege Escalation
reverse_shell	Reverse Shell
emergency_vul	Emergency Vulnerability
linux_app_vul	Linux System Vulnerability
windows_sys_vul	Windows System Vulnerability
Web-CMS_vul	Web-CMS Vulnerability

application_vul	Application Vulnerability
baseline	Baseline
attack_logs	Network Attacks
java_shell	Java Webshell
file_tamper	Core File Monitoring
tamper_protect_logs	Web Tamper Protection Event
tamper_protect_exceptions	Web Tamper Protection Anomaly
client_uninstall	Client Uninstallation
client_offline	Offline Client

Asset Logs

cls_event_type	Log Type Values
machines	Host List
asset_system	Resource Monitoring
asset_account	Account
asset_netstat	Port
asset_process	Process
asset_app	Software Applications
asset_database	Database
asset_web_app	Web Applications
asset_web_service	Web Services
asset_web_frame	Web Frameworks
asset_web_location	Web Site
asset_jar	JAR package
asset_init_service	Start Service
asset_scheduled_task	Scheduled Tasks

asset_env	Environment Variables
asset_core_module	Kernel Modules
asset_package	System Installation Package

Client Report Logs

cls_event_type	Log Type Values
client_log	Original Host Logs
dns_log	DNS Logs
process_snapshot	Process Snapshot Logs
net_log	Network Quintuple Logs
file_log	File Monitoring Logs
login_log	Login to Transaction Logs

Event Log Fields Description

Common Fields Description

Field	Type	Description
id	string	Database Record id
appid	string	User appid
create_time	string	Event Creation Time
modify_time	string	Event Modification Time
cls_event_type	string	Event Type
event_status	string	Event Status (Create, Modify, and Delete)

Malicious File Scan Fields Description

Field	Type	Description
uuid	string	Machine uuid

hostip	string	Host IP
file_path	string	File Path
md5	string	File md5
filesize	string	File Size
file_create_time	string	File Creation Time
file_modify_time	string	File Modification Time
file_access_time	string	File Access Time
status	string	Status (Pending, Trusted, Isolated, Allowlisted File, File Deleted, In Quarantine, In Restoration, and Event Record Deleted)
virus_name	string	Virus Name
bwtype	string	Sample Attributes (10: Allowlisted; 20~29: Blocklisted)
path_md5	string	File Path md5

Abnormal Process Fields Description

Field	Type	Description
uuid	string	Machine uuid
hostip	string	Host IP
pid	int	Process ID
exe_path	string	Process Path
exe_md5	string	Process md5
exe_desc	string	Process Details
exe_argv	string	Process Parameters
exe_create_time	string	Process Creation Time
exe_modify_time	string	Process Modification Time
exe_access_time	string	Process Access Time
status	string	Status (Pending, Trusted, Cleaned Up, and Exited)

start_time	string	Process Start Time
virus_name	string	Virus Name
latest_scan_time	string	Latest Scan Time
pstree	string	Process Tree Details (json Format)
risk_level	string	Risk Level (Advisory, Low, Medium, High, and Critical)
pay_version	string	Machine Version (Basic Edition, Professional Edition, Ultimate Edition, and Universal Edition)
rss	int	Process Memory
permission	string	Process Permissions

Abnormal Log-in Fields Description

Field	Type	Description
uuid	string	Machine uuid
hostip	string	Host IP
username	string	Log-in Username
count	string	Log-in Attempts (Aggregated Once per Minute)
src_ip	string	Log-in Source IP
dst_port	string	Log-in Port
src_machine_name	string	Log-in Source Machine Name
login_time	string	Log-in Time
status	string	Status (Normal Log-in, Abnormal Log-in, Allowlisted, Deleted, Confirmed Intrusion Log-in, Processed, and Ignored)
location	string	Location

Password Cracking Fields Description

Field	Type	Description
uuid	string	Machine uuid

hostip	string	Host IP
username	string	Username
count	string	Attempt Count
event_type	string	Event Type (Brute Force Failure, Brute Force Success, and Brute Force on Non-existent Account)
src_ip	string	Source IP
dst_port	string	Source Port
src_machine_name	string	Source Machine Name
status	string	Status (Pending, Ignored, False Positive, Deleted, Hit Allowlist, Processed, and Allowlisted)
location	string	Location
banned	string	Blocking Status (Not Blocked, Blocked, Not Blocked (Blocking Not Enabled), Not Blocked (Non-Professional Edition), Not Blocked (Allowlisted), Not Blocked (No Public IP Bound), Blocking Failed (Interface Anomaly), Blocking Failed (Private Network Not Supported), and Blocking Failed (Available Zone Not Supported))

Malicious Request Fields Description

Field	Type	Description
uuid	string	Machine uuid
hostip	string	Host IP
url	string	Domain Name
pid	string	Process ID
process_name	string	Process Name
cmd_line	string	Command Line
status	string	Status (Pending, Deleted, Allowlisted, Trust Revoked by User, Processed, and Ignored)
access_count	string	Request Count
query_time	string	First Request Time

merge_time	string	Recent Request Time

High-risk Command Fields Description

Field	Type	Description
uuid	string	Machine uuid
hostip	string	Host IP
user	string	Executing User
platform	string	Platform
exec_time	string	Command Execution Time
bash_cmd	string	Executed Command
status	string	Status (Pending, Hazardous Command, Normal Command, Ignored, and Deleted)
rule_name	string	Hit Rule Name
rule_level	string	Command Hazard Level (High, Medium, and Low)

Local Privilege Escalation Fields Description

Field	Type	Description
uuid	string	Machine uuid
hostip	string	Host IP
process_name	string	Process Name
full_path	string	File Path
pid	string	Process ID
cmd_line	string	Command Line
user_name	string	Executing User
user_group	string	Group to Which the Executing User Belongs
proc_file_privilege	string	Process File Permission Information
ppid	string	Parent Process ID

parent_proc_name	string	Parent Process Name
parent_proc_user	string	User Executing the Parent Process
parent_proc_group	string	Group to Which the Executing User of Parent Process Belongs
parent_proc_path	string	Parent Process Path
find_time	string	Execution Time
proc_tree	string	Process Tree
sid	string	User sessionid (Currently Default to 0)
uid	string	User ID
gid	string	User Group ID
euid	string	Effective User ID
egid	string	Effective User Group ID
status	string	Status (Pending, Privilege Escalation Event, Allowlisted, Processed, Ignored, and Deleted)

Reverse Shell Fields Description

Field	Type	Description
uuid	string	Machine uuid
hostip	string	Host IP
dst_ip	string	Destination IP
dst_port	string	Destination Port
process_name	string	Executed Process
full_path	string	Process Path
pid	string	Process ID
cmd_line	string	Executed Command
user_name	string	Executing User
user_group	string	Group to Which the Executing User Belongs

ppid	string	Parent Process ID
parent_proc_name	string	Parent Process Name
parent_proc_user	string	User Executing the Parent Process
parent_proc_group	string	Group to Which the Executing User of Parent Process Belongs
parent_proc_path	string	Parent Process Path
find_time	string	Execution Time
proc_tree	string	Process Tree
status	string	Status (Pending, Reverse Shell Event, Allowlisted, Processed, Ignored, and Deleted)

Vulnerability Fields Description

Field	Type	Description
uuid	string	Machine uuid
hostip	string	Host IP
status	string	Vulnerability Status (Pending, Ignored, Fixed, Under Detection, Fix In Progress, Rolling Back, Fix Failed, Expired, and Offline)
vul_category	string	Vulnerability Classification (Web Application Vulnerability, System Component Vulnerability, Linux System Vulnerability, and Windows System Vulnerability)
descript	string	Vulnerability Event Details
path	string	The File Path of the Vulnerability
remark	string	Vulnerability Remarks
name	string	Vulnerability Name
fix	string	Remediation Description
cve_id	string	cve Number
reference	string	Reference Description
level	string	Vulnerability Severity Level (Low, Medium, High, and Advisory)
is_emergency	string	Urgent or Not

Baseline Fields Description

Field	Type	Description
name	string	Baseline Name
uuid	string	Machine uuid
hostip	string	Host IP
status	string	Status (Failed, Ignored, Passed, Deleted, and Under Detection)
level	string	Severity Level (Low, Medium, High, and Critical)
descript	string	Description
remark	string	Remarks
rule_id	string	Baseline Category ID
category_name	string	Baseline Category Name
item_id	string	Baseline Rule ID
fix	string	Suggestions for Fix

Network Attack Fields Description

Field	Type	Description
uuid	string	Machine uuid
dst_port	int	Destination Port
src_ip	string	Source IP
type	string	Type (Attack Attempt/Successful Attack)
status	string	Event Status (Pending, Processed, Allowlisted, Ignored, Deleted, and Defense Enabled)
count	int	Event Merging Count
svc_ps	string	Service Process Details (json Format)
net_payload	string	Attack Packet (Plaintext Format)

merge_time	string	Event Merging Time (Latest Detection Time)
host_op_type	string	Abnormal Behavior Type (No Compromised Behavior/rce (Command Execution)/dnslog/writefile)
host_op_pstree	string	Abnormal Behavior Process Tree (json Format)
host_op	string	Abnormal Behavior Content
hostip	string	Host IP

Java Webshell Fields Description

Field	Type	Description
uuid	string	Machine uuid
type	string	Trojan Type (Filter, Listener, Servlet, Interceptors, Client, etc.)
exe	string	Java Process Path
argv	string	Java Process Command Line
pid	string	Java Process Process ID
class_name	string	Memory Shellcode class_name
loader_class_name	string	Memory Shellcode loader_class_name
super_class_name	string	Memory Shellcode Parent Class super_class_name
interfaces	string	Memory Shellcode interfaces
recent_found_time	string	Last Detection Time
status	string	Status (Pending, Allowlisted, Deleted, Ignored, and Manually Processed)
file_exist	string	File Exists or Not (File Does Not Exist, File Exists)
class_file	string	The File Path of class

Kernel File Monitoring Fields Description

Field	Type	Description
uuid	string	Machine uuid

hostip	string	Host IP
hostname	string	Host name
process_exe	string	Process Path
process_argv	string	Process Command Line Parameters
target	string	The File Path of the Destination
status	string	Status (Pending, Allowlisted, Deleted, Ignored, and Manually Processed)
event_count	string	Event Occurrence Count
rule_name	string	Rule Name
event_detail	string	Event Details (json Format)
pstree	string	Process Tree
rule	string	Rule Group Details (json Format)
level	string	Severity Level (None, High, Medium, and Low)

Web Tamper Protection Event Fields Description

Field	Type	Description
uuid	string	Machine uuid
path	string	File Path
recover_type	string	Recovery Type (Recovery for Content Modification, Recovery for Permission Modification, Recovery for Ownership Modification, Recovery for Deletion, and Deletion for Addition)
has_recovered	string	Deleted or Not (Not Deleted, Deleted)
recover_time	string	Restoration Time
is_manual_recover	string	Whether Manually Restored by User (No, Yes)
is_deleted	string	Deleted or Not (Not Deleted, Deleted)
status	string	Status (Pending, Confirm Malicious, and Confirm False Positive)
file_type	string	File Type (Regular File, Directory, and Symbolic Link)

Web Tamper Protection Anomaly Fields Description

Field	Type	Description
quuid	string	Machine uuid
exception	string	Exception Type (No Exception, Beyond Limit, Client Offline, Timed Out, Insufficient Disk Space, Machine Destroyed, File Changed During Backup, File Not Found During Backup, Beyond Limit (Monitoring Path is not a Directory), Beyond Limit (File Type not Supported), Beyond Limit (Number of Files Exceeded the Limit), Beyond Limit (Path Too Long), Beyond Limit (File Too Large), Beyond Limit (Failed to Read File), Beyond Limit (Too Many Protected Directories/Subdirectories), etc.)
exception_message	string	Exception Prompt

Client Uninstallation Fields Description

Field	Type	Description
uuid	string	Machine uuid
pstree	string	Process Tree
uninstall_time	string	Uninstallation Time

Offline Client Fields Description

Field	Type	Description
uuid	string	Machine uuid
offline_time	string	Machine Offline Time

Asset Log Fields Description

Common Fields Description

Field	Type	Description
id	string	Database Record ID
appid	string	User appid

host_name	string	Host name
host_ip	string	Host Private IP
wan_ip	string	Host Public IP
instance_id	string	Instance ID
os_name	string	Operating System Name
os_type	string	Operating System Type (Unknow, CentOS, Debian, Gentoo, RedHat, Ubuntu, WindowsServer, TencentOS, CoreOS, FreeBSD, and SUSE)
create_time	int	Creation Time (Timestamp Format)
update_time	int	Asset Update Time (Timestamp Format)
cls_event_type	string	Event Type
event_status	string	Event Status (create, modify, and delete)

Host List Fields Description

Field	Type	Description
quuid	string	Machine quuid
machine_type	string	Machine Type (CVM, LH, Other, and ECM)
region	string	Region
project_id	int	Instance Project ID
instance_id	string	Instance ID
instance_state	string	Instance Status (PENDING, LAUNCH_FAILED, RUNNING, STOPPED, STARTING, STOPPING, REBOOTING, SHUTDOWN, TERMINATING, and TERMINATED)
restrict_state	string	Business Status (NORMAL, EXPIRED, PROTECTIVELY_ISOLATED, and TERMINATED_PRO_VERSION)
instance_name	string	Instance Name
private_ip_addresses	string	Instance Private IP Address
public_ip_addresses	string	Instance Public IP Address
ipv6_addresses	string	Instance IPv6 Address

vpc_id	string	vpc id
os_name	string	Operating System Name
os_type	string	Operating System Type (Unknow, CentOS, Debian, Gentoo, RedHat, Ubuntu, WindowsServer, TencentOS, CoreOS, FreeBSD, and SUSE)
installed_cwp	int	Whether or Not Installed CWPP Client (0: Not Installed; 1: Installed)
latest_sync_time	string	Last Synchronization Time

Resource Monitoring Fields Description

Field	Type	Description
core_version	string	Kernel Version
boot_time	int	System Boot Time (unix Timestamp)
cpu_info	string	CPU Information
cpu_size	int	Number of CPUs
cpu_load	float	CPU Utilization
memory_size	int	Memory Size (MB)
memory_load	float	Memory Utilization
disk_size	int	Disk Size (MB)
disk_load	float	Disk Utilization

Account Fields Description

Field	Type	Description
group_name	string	Account GroupName
status	string	Account Status (Disabled, Enabled)
is_root	string	Whether or Not Have Root Privilege
name	string	Account Name
type	string	Account Type (Guest User, Standard User, and Administrator

		User)
home_path	string	Home Directory
shell	string	Shell Path
password_change_time	string	Password Change Time
password_due_days	int	Password Due Days (-1 means that it never expires.)
password_lock_days	int	Password Lockout Duration in Days (-1 means that it is infinite.)
password_warn_days	int	Password Expiration Reminder in Days
password_change_type	string	Password Change Settings (Not Modifiable, Modifiable)
password_status	string	Password Status (Normal, Expiring Soon, Expired, and Locked)
login_type	string	Log-in Method (No Log-in Allowed, Key-only Log-in, Password-only Log-in, and Key and Password Allowed)
last_login_time	int	Last Log-in Time
last_login_terminal	string	Last Log-in Terminal
last_login_ip	string	Last Log-in IP
disable_time	string	Account Expiration Time

Port Fields Description

Field	Type	Description
name	string	Process Name
version	string	Process Version
path	string	Process Path
parent_process_name	string	Parent Process Name
pid	string	Process ID
user	string	Running User
group_name	string	Belonging User Group
start_time	int	Start Time (unix Timestamp)

param	string	Startup Parameters
tty	string	Process TTY
port	string	Port
ppid	string	Parent Process ID
proto	string	Port Protocol

Software Application Fields Description

Field	Type	Description
name	string	Application Name
type	string	Application Type (Ops Tool, Database, Secure Application, Suspicious Application, System Architecture, System Application, WEB Ops, etc.)
bin_path	string	Binary Path
config_path	string	The File Path of the Configuration
process_count	int	Associated Process Count
version	string	Version Number

Process Fields Description

Field	Type	Description
name	string	Process Name
group_name	string	Process User Group
desc	string	Process Description
path	string	Process Path
pid	string	Process ID
ppid	string	Parent Process ID
parent_process_name	string	Parent Process Name
user	string	Running User
start_time	int	Start Time

param	string	Startup Parameters
tty	string	Process TTY
version	string	Process Version
status	string	Process Status (None, Executable, Interruptible, Not Interruptible, Paused or Traced, Zombie, To Be Destroyed, Idle, and Waiting for Memory Allocation)
package_name	string	Software Package Name

Database Fields Description

Field	Type	Description
name	string	Database Name
version	string	Version
port	string	Port
proto	string	Protocol
user	string	Running User
ip	string	Bound IP
config_path	string	The File Path of the Configuration
log_path	string	The File Path of Logs
data_path	string	Data Path
permission	string	Running Permission
error_log_path	string	Error Log Path
plugin_path	string	Plugin Path
bin_path	string	Binary Path
param	string	Startup Parameters

Web Application Fields Description

Field	Type	Description

name	string	Application Name
desc	string	Application Description
version	string	Version
root_path	string	Root Path
service_type	string	Service Type
domain	string	Site Domain Name
virtual_path	string	Virtual Path
plugin_count	int	Plugin Count

Web Servie Fields Description

Field	Type	Description
name	string	Framework Name
version	string	Version
bin_path	string	Binary Path
service_type	string	Service Type
user	string	Starting User
install_path	string	Installation Path
config_path	string	Configuration Path
process_count	int	Associated Process Count

Web Framework Fields Description

Field	Type	Description
name	string	Framework Name
version	string	Version
lang	string	Language
service_type	string	Service Type

path	string	Application Path

Web Site Fields Description

Field	Type	Description
name	string	Domain Name
port	string	Site Port
proto	string	Site Protocol
service_type	string	Service Type
path_count	int	Site Path Count
user	string	Running User
ip	string	Bound IP
command	string	Startup Command

jar File Fields Description

Field	Type	Description
name	string	Name
type	string	Type (Application, System Class Library, Web Service Built-in Library, and Other)
status	string	Executable or Not
version	string	Version
path	string	Path

Startup Service Fields Description

Field	Type	Description
name	string	Name
type	string	Type
status	string	Default Enablement Status (Enabled, Not Enabled)

user	string	Starting User
path	string	Path

Scheduled Task Fields Description

Field	Type	Description
status	string	Default Enablement Status (Enabled, Not Enabled)
cycle	string	Execution Cycle
command	string	Execute Command or Script
user	string	Starting User
config_path	string	The File Path of the Configuration
os_info	string	Operating System

Environment Variable Fields Description

Field	Type	Description
name	string	Name
type	string	Type (User, System)
user	string	Starting User
value	string	Environment Variable Value

Kernel Module Fields Description

Field	Type	Description
name	string	Name
desc	string	Description
path	string	Path
version	string	Version
size	int	Size

System Installation Package Fields Description

Field	Type	Description
name	string	Installation Package Name
desc	string	Description
version	string	Version
install_time	int	Installation Time (unix Timestamp)
type	string	Type

Client Reporting Log Fields Description

Original Log Fields Description

Field	Type	Description
appid	int	User appid
uuid	string	Machine uuid
path	string	The File Path of Logs
tag	string	Tag (To be Defined by User)
time	string	Log Time
log	string	Log Content

DNS Log Fields Description

Field	Type	Description
appid	int	User appid
quuid	string	Machine quuid
uuid	string	Machine uuid
recv_time	int	Timestamp
domain	string	Domain Name

hostip	string	Host IP
platform	string	Platform: Linux, Windows
pid	int	Process ID
process_path	string	Process Path
cmdline	string	Process Command Line Parameters
count	int	Number of Accesses during Reporting Period

Process Snapshot Fields Description

Field	Type	Filed Description
appid	string	Account appid
quuid	string	Host quuid (Corresponding cvm uuid)
uuid	string	Host uuid
hostip	string	Host ip (ip Connected with the Backend)
instance_id	string	Instance id
event_name	string	Event Type: process - Process Event
pid	int	Process ID
ppid	int	Parent Process ID
sid	int	Process Session ID (Linux Only)
uid	int	Process uid (Linux Only)
gid	int	Process gid (Linux Only)
euid	int	Process euid (Linux Only)
egid	int	Process egid (Linux Only)
report_type	int	Report Type: 0: - Real-time Process; 1: - Process Snapshot
parent_proc_name	string	Parent Process Name
process_name	string	Process Name
process_path	string	Process Path

cmdline	string	Process Command Line
user_name	string	Process Starting User
process_md5	string	Process md5
platform	string	Platform: Linux and Windows
time	int	Event Collection Timestamp
timestamp	string	Event Storage Date and Time
insert_time	int	Event Storage Timestamp

Network Quintuple Log Fields Description

Field	Type	Filed Description
appid	string	Account appid
quuid	string	Host quuid (Corresponding cvm uuid)
uuid	string	Host uuid
hostip	string	Host ip (ip Connected with the Backend)
instance_id	string	Instance id
event_name	string	Event Type: net - Network Quintuple Logs
pid	int	Process pid
proc_path	string	Process Path
argv	string	Process Execution Parameters
username	string	User to Which the Process Belongs: User Group
src_ip	string	Source ip
src_port	int	Source Port
dst_ip	string	Destination ip
dst_port	int	Destination Port
first_time	int	First Trigger Time during Reporting Period
last_time	int	Last Trigger Time during Reporting Period

count	int	Number of Triggers during Reporting Period
time	int	Event Collection Timestamp
timestamp	string	Event Storage Date and Time
insert_time	int	Event Storage Timestamp

File Monitoring Log Fields Description

Field	Type	Filed Description
appid	string	Account appid
quuid	string	Host quuid (Corresponding cvm uuid)
uuid	string	Host uuid
hostip	string	Host ip (ip Connected with the Backend)
instance_id	string	Instance id
event_name	string	Event Type: file - File Operation Event
pid	int	Process ID
ppid	int	Parent Process ID
session_id	int	Process Session ID (Linux Only)
uid	int	Process uid (Linux Only)
gid	int	Process gid (Linux Only)
file_path	string	Operation File Path
cwd	string	Current Execution Path of the Process
proc_path	string	Process Path
argv	string	Process Command Line
username	string	File Operation User
parent_proc_name	string	Parent Process Name
proc_name	string	Process Name

proc_md5	string	Process md5
proc_perm	string	Process File Execution Permissions
proc_mtime	int	Process File modify time
proc_ctime	int	Process File change time
proc_atime	int	Process File access time
operation	string	File Operation Type: write; rename
file_size	int	File Size
file_mtime	int	Operation File modify time
file_ctime	int	Operation File change time
file_atime	int	Operation File access time
file_perm	string	Operation File Permissions
file_owner	string	Operation File Owner
time	int	Event Collection Timestamp
timestamp	string	Event Storage Date and Time
insert_time	int	Event Storage Timestamp

Log-in Activity Log Fields Description

Field	Type	Filed Description
appid	string	Account appid
quuid	string	Host quuid (Corresponding cvm uuid)
uuid	string	Host uuid
hostip	string	Host ip (ip Connected with the Backend)
instance_id	string	Instance id
event_name	string	Event Type: login - Log-in Event
src_ip	string	Log-in Source ip
dst_port	int	Log-in Target Port

protocol	string	Log-in Protocol
count	int	Log-in Count
event_type	string	Event Status: success: Log-in succeeded; fail: Log-in failed.
time	int	Event Collection Timestamp
insert_time	int	Event Storage Timestamp

Agent Installation Guide

Last updated：2023-12-26 16:39:31

This topic describes how to install CWPP Agent.

Limitations

CWPP Agent can only be installed and used on the servers that meet the following two conditions.

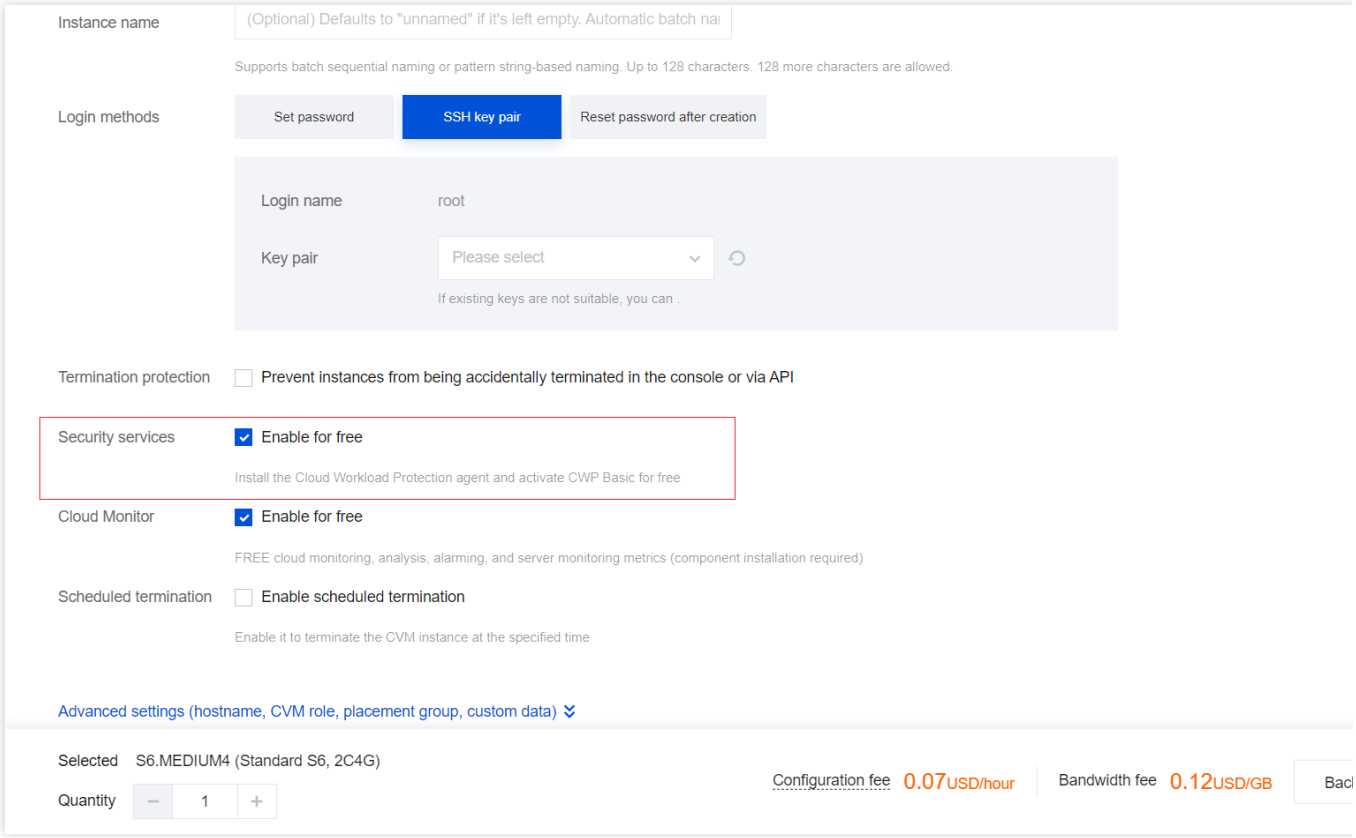
Conditions	Description
Server type	CWPP supports servers running in a hybrid cloud. Tencent Cloud: CVM, Lighthouse, and ECM Non-Tencent Cloud servers: third-party cloud vendor servers and IDC servers
Server OS	Linux CentOS: 6, 7, 8 (64-bit) Ubuntu: 9.10 - 20.10 (64 bit) Debian: 6, 7, 8, 9, 10, 11 (64 bit) RHEL: 6, 7 (64 bit) Windows Windows server 2012, 2016, 2019 Windows server 2008 R2 Windows server 2003 (limited support)

Installation

Option 1: Install directly upon purchase

Applicable to: CVM, Lighthouse, and ECM

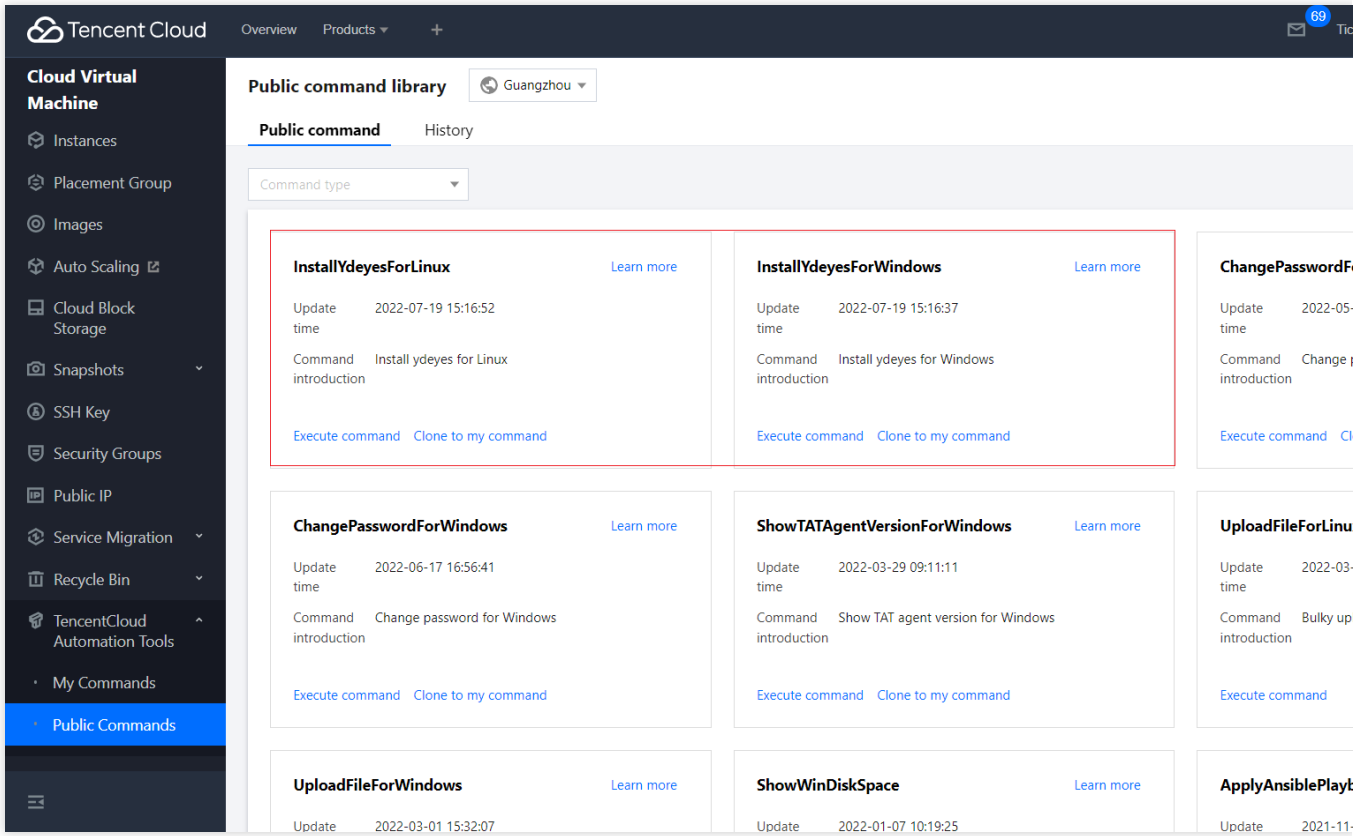
When purchasing the above servers, select **Security Reinforcement** to automatically install the CWPP Agent.



Option 2: Install automatically using Tencent Cloud Automation Tools (TAT)

Applicable to: CVM and Lighthouse

Go to **TAT**>**Public Command Library** of your CVM or Lighthouse server, locate the installation command of the CWPP Agent, click **Execute Command**, and select the server to install the agent.



Option 3: Install by following the installation guide

1. Log in to the CWPP Console.
2. Click **Server List** in the left navigation pane, click **Install CWPP Agent** to open the installation guide pop-up window, and select an installation method based on your server.

Install Cloud Workload Protection agent

Select a proper installation method

Server type	Tencent Cloud	Non-Tencent Cloud
Server System	Linux	Windows
Server Products	CVMs	
Server architecture	x86	arm
Network	VPC	Classic network

Copy and execute the command

```
wget http://uo.yd.tencentyun.com/ydeyes_linux64.tar.gz -O ydeyes_linux64.tar.gz && tar -zxvf ydeyes_linux6
```

Determines whether the installation is successful

Execute the command ps -ef | grep YD to view whether YDService and YDLive are running. If yes, the installa

```
[root@VM_90_131_centos conf]# ps -ef|grep YD
root     16216 21992  0 14:33 pts/3    00:00:00 grep --color=auto YD
root     32707     1  0 11:23 ?        00:00:09 /usr/local/qcloud/YunJing/YDEyes/Y
root     32724     1  0 11:23 ?        00:00:01 /usr/local/qcloud/YunJing/YDLive/Y
[root@VM_90_131_centos conf]# ps -ef|grep YD
```

Note: If the process does not start, you can execute the command manually as a root user to start the prograr
/usr/local/qcloud/YunJing/YDEyes/YDService

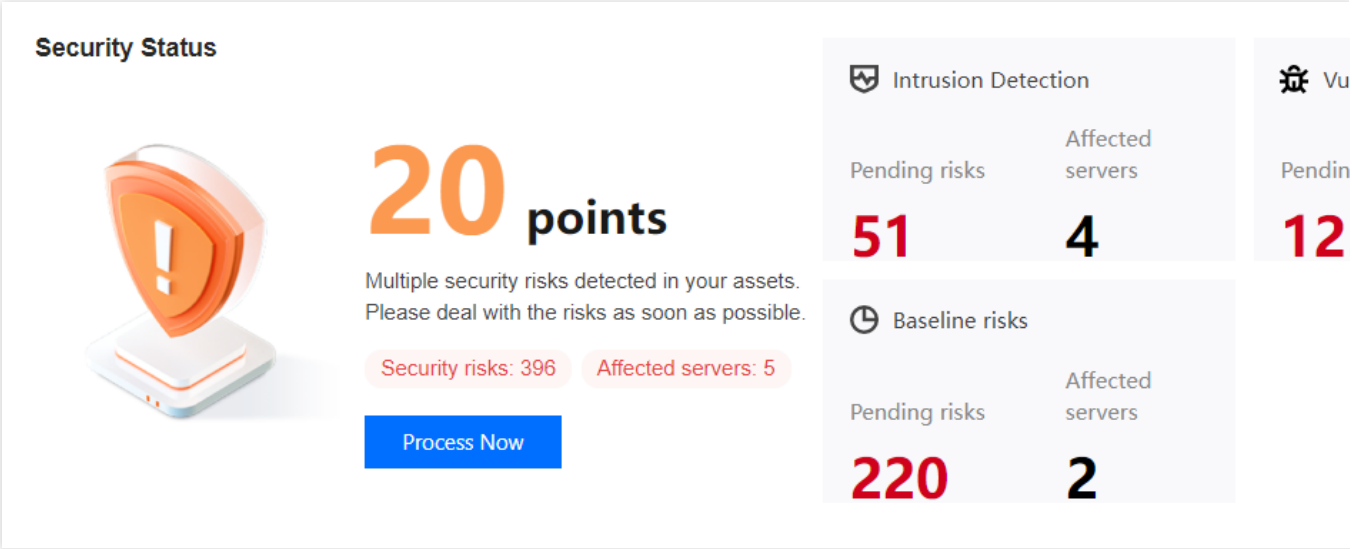
Security Score Overview

Last updated：2023-12-26 16:39:39

This topic describes how to calculate the security score for your assets.

Security Score

The highest security score is 100, and the lowest score is 20. The security level of a server is based on its security score, which is calculated by subtracting the points scored by the types, number, and threat level of security incidents from the total score of 100.



Scoring rules

Level	Security Incidents (by incident count)	Penalty per incident	Maximum total penalty
Critical	Trojan files, brute force attacks, and malicious requests	-40	-50
High	Critical vulnerabilities, high-risk vulnerabilities, critical baseline items, high-risk baseline items, unusual logins (high risk), local privilege escalation, and reverse shell	-10	-20
Medium	Medium-risk vulnerabilities and baseline items	-3	-10
Low	Low-risk vulnerabilities and baseline items	-2	-5

Other	Only CWPP Basic is implemented, or CWPP Agent is not installed	-1	-5

Security level

Level	Health check score	Text color	Description
Good	90-100	Green	The assets have a good security status. Regular inspection is recommended to maintain the good status.
Medium	60-89	Orange	Many security risks exist in the assets. It is recommended to handle the security incidents in a timely manner.
Bad	20-59	Red	Critical security risks exist in the assets. It is recommended to handle the security incidents as soon as possible.