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

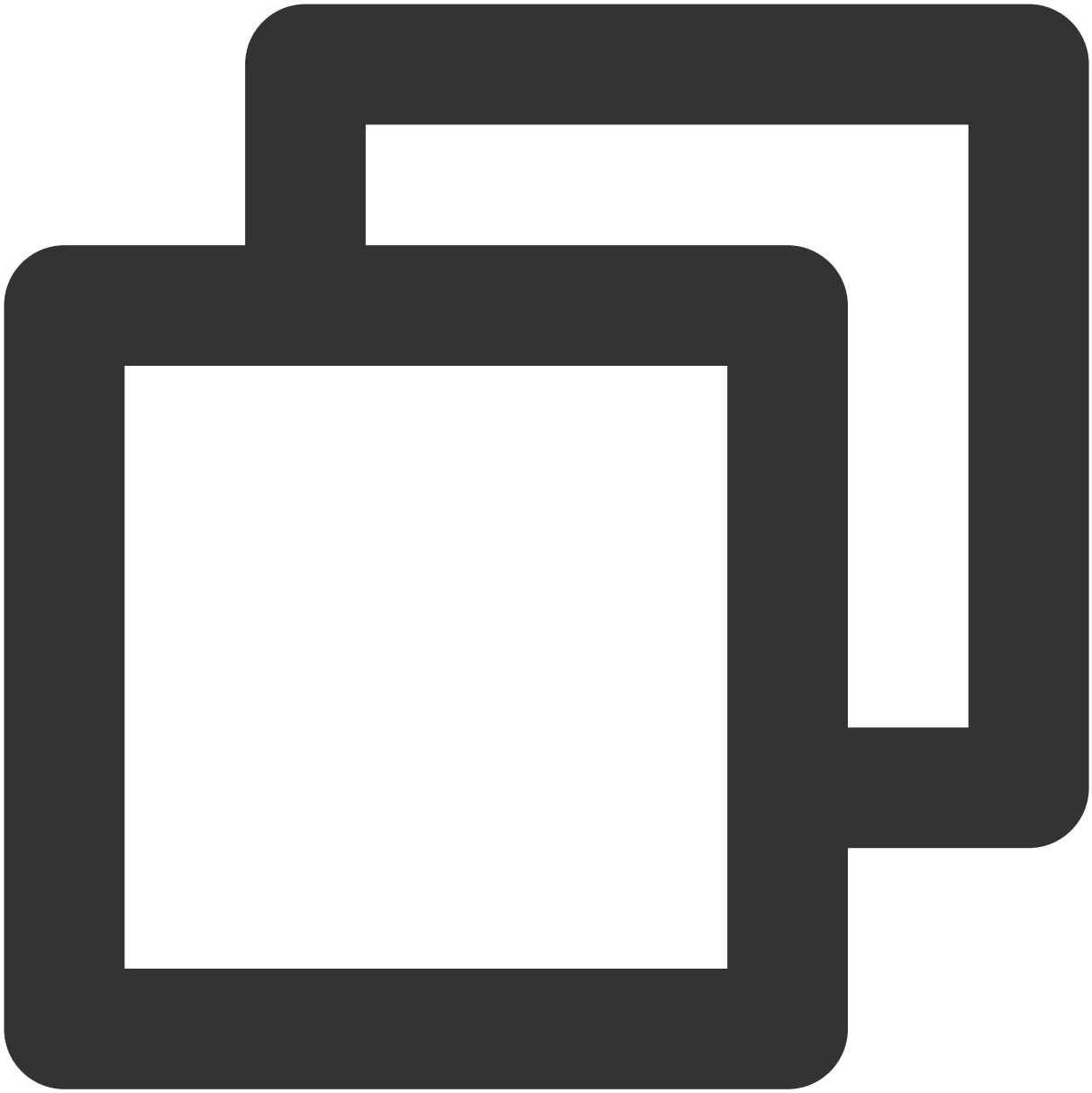
Last updated：2023-12-26 16:39:23

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.

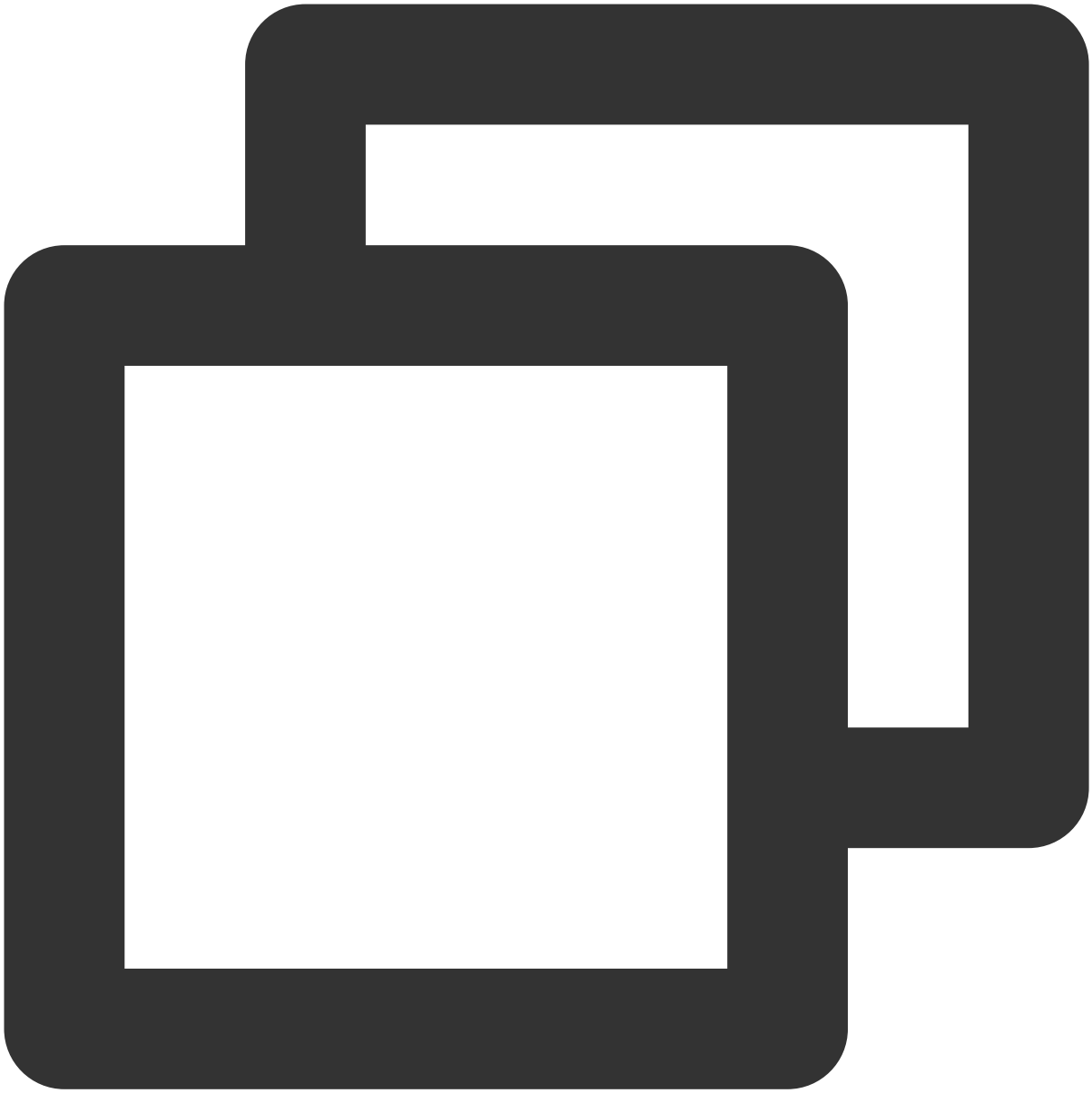
Agent restart commands (Linux)

1.1 Stop the agent program:



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

1.2 Restart the agent:

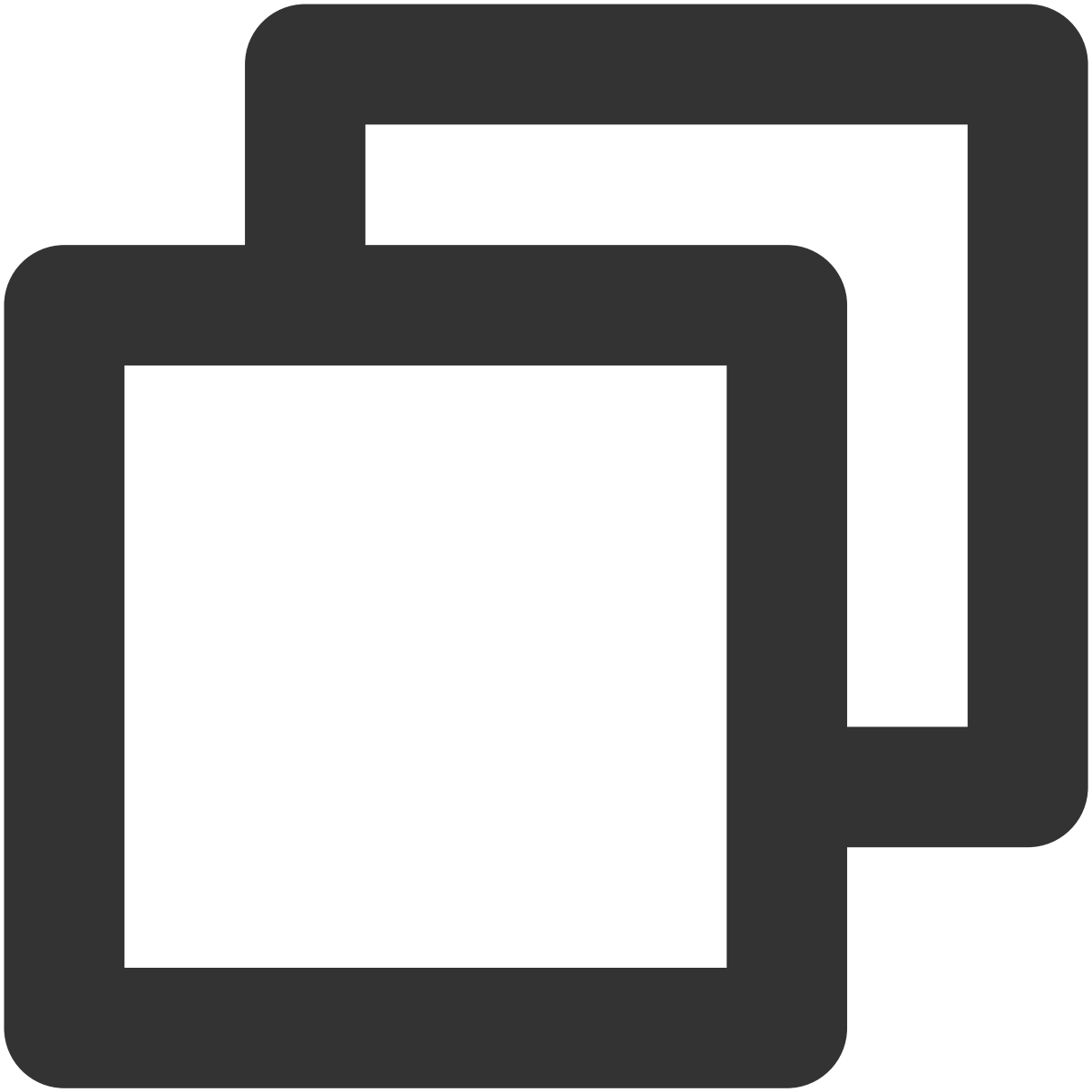


```
/usr/local/qcloud/YunJing/startYD.sh
```

Agent restart commands (Windows)

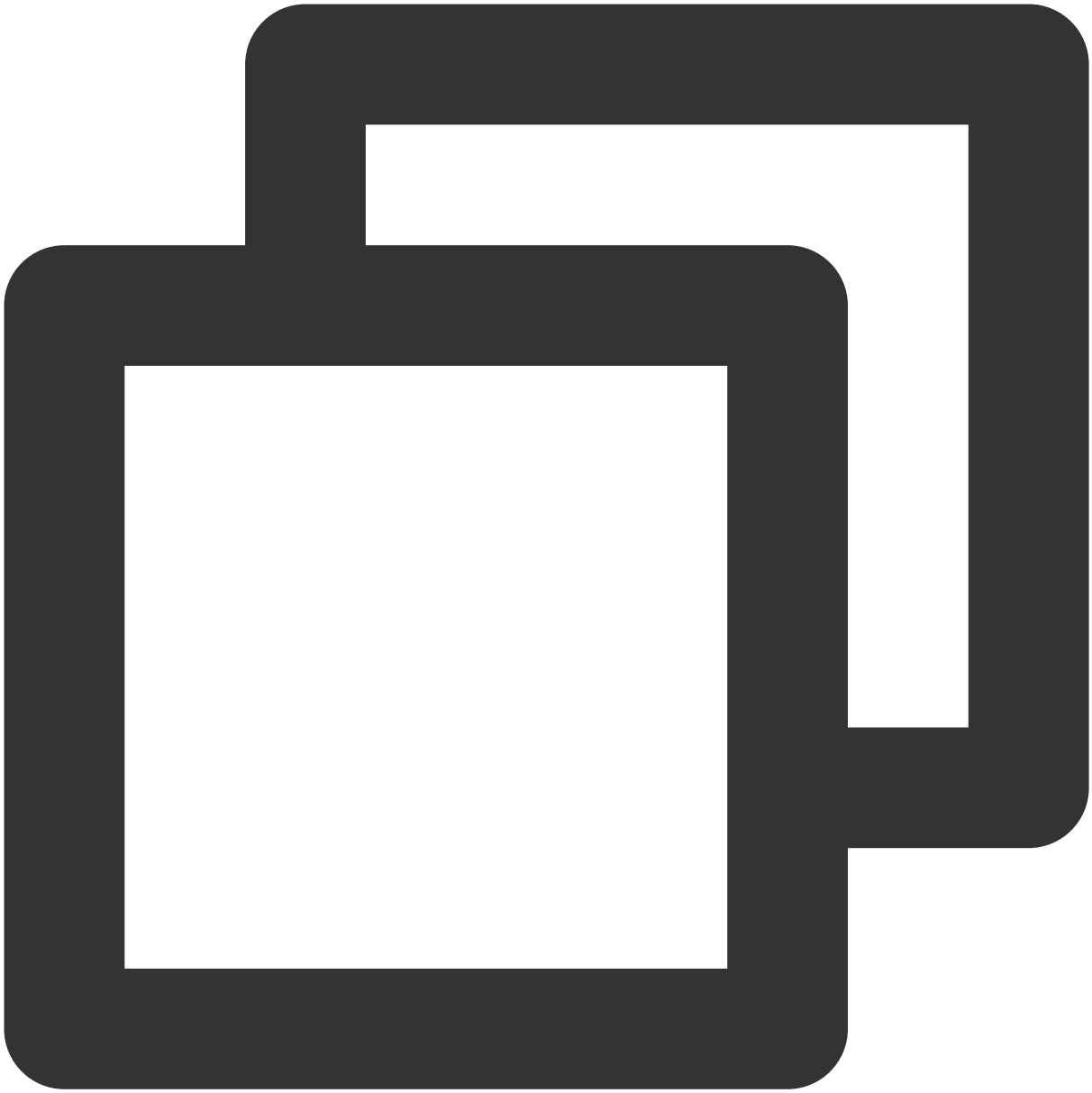
Enter the following commands or open Task Manager, locate YDService, and right-click to restart the agent.

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**.

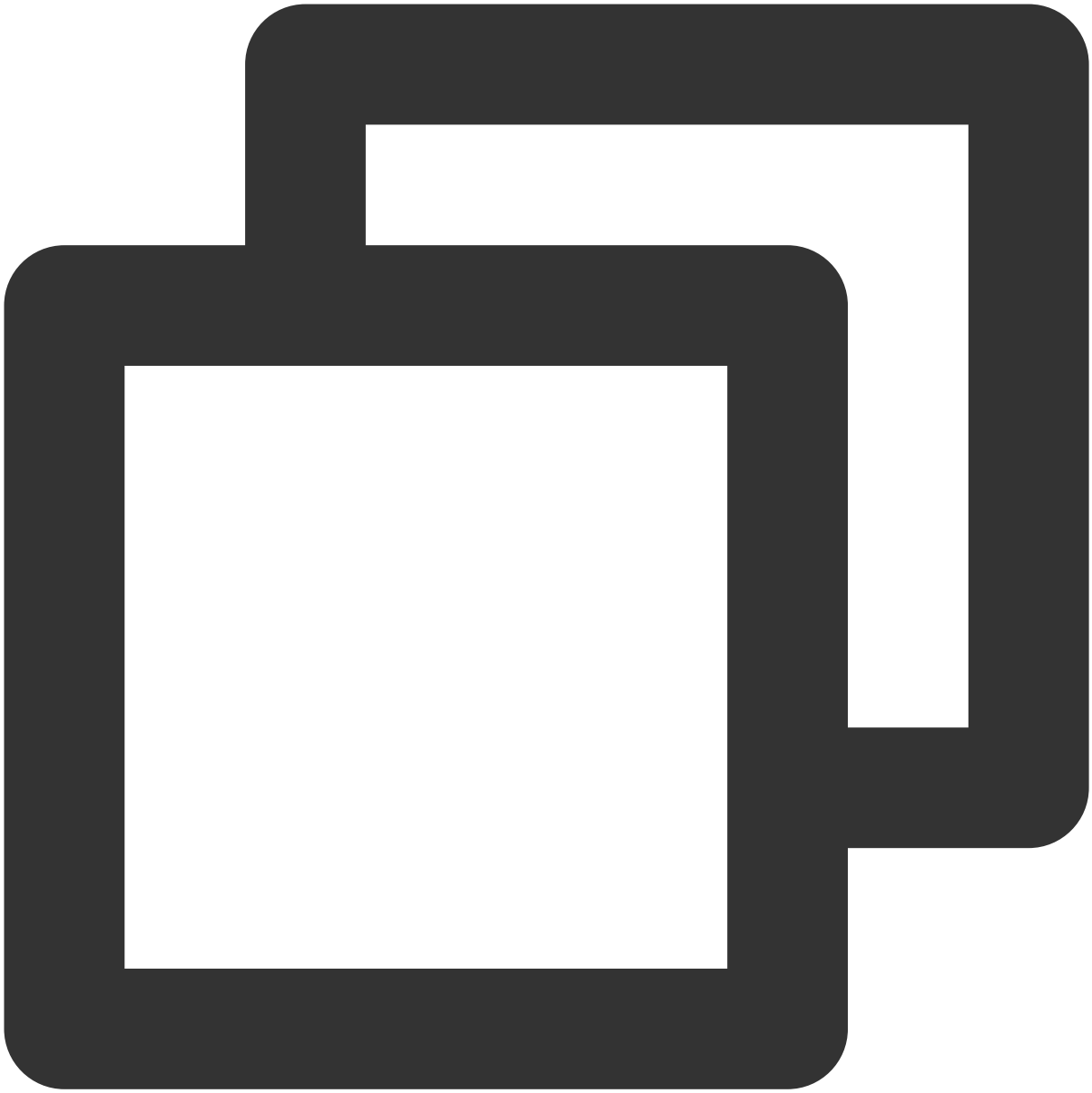
Note

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



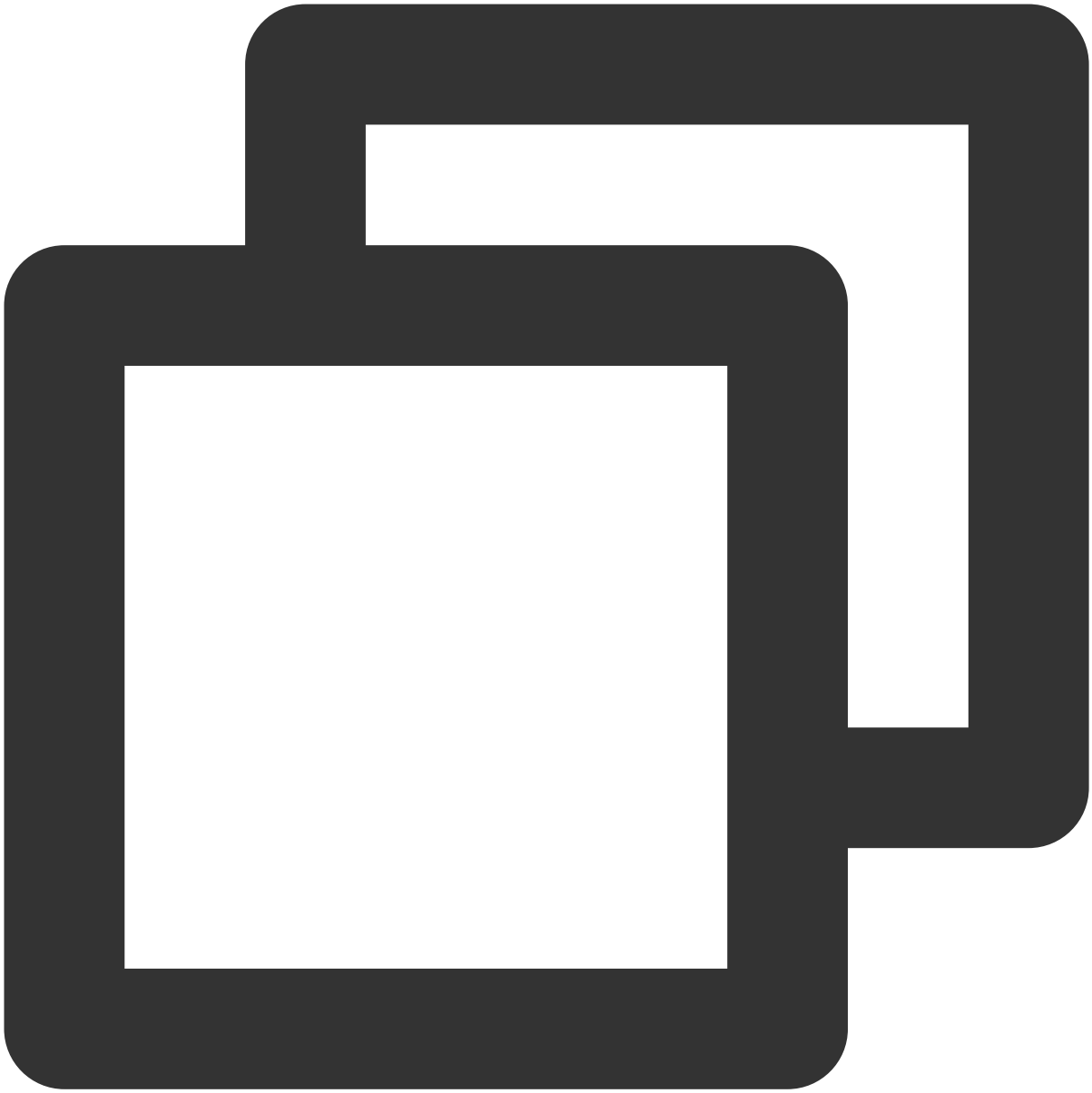
```
{
    "uin": "1000xxxxxx21",
    "nickname": "Test Account",
    "server": "172.x.x.41 [Test Machine]",
    "instance_id": "ins-xxxxxxxx",
    "region": "Southwest China (Chengdu)",
    "time": "October 30, 2023 09:24:20"
}
```

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"
}
```

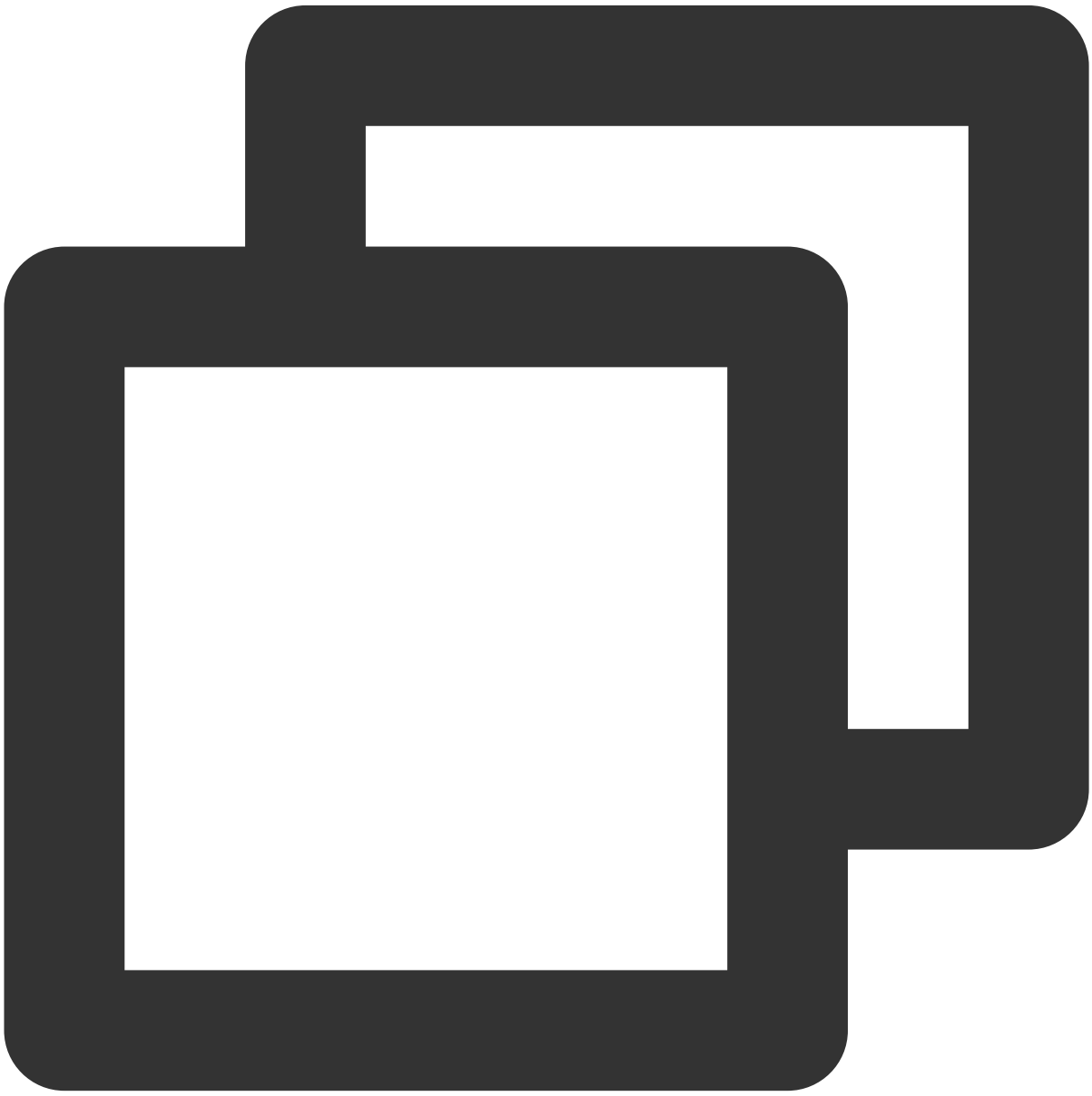
Field Description

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"
}
```

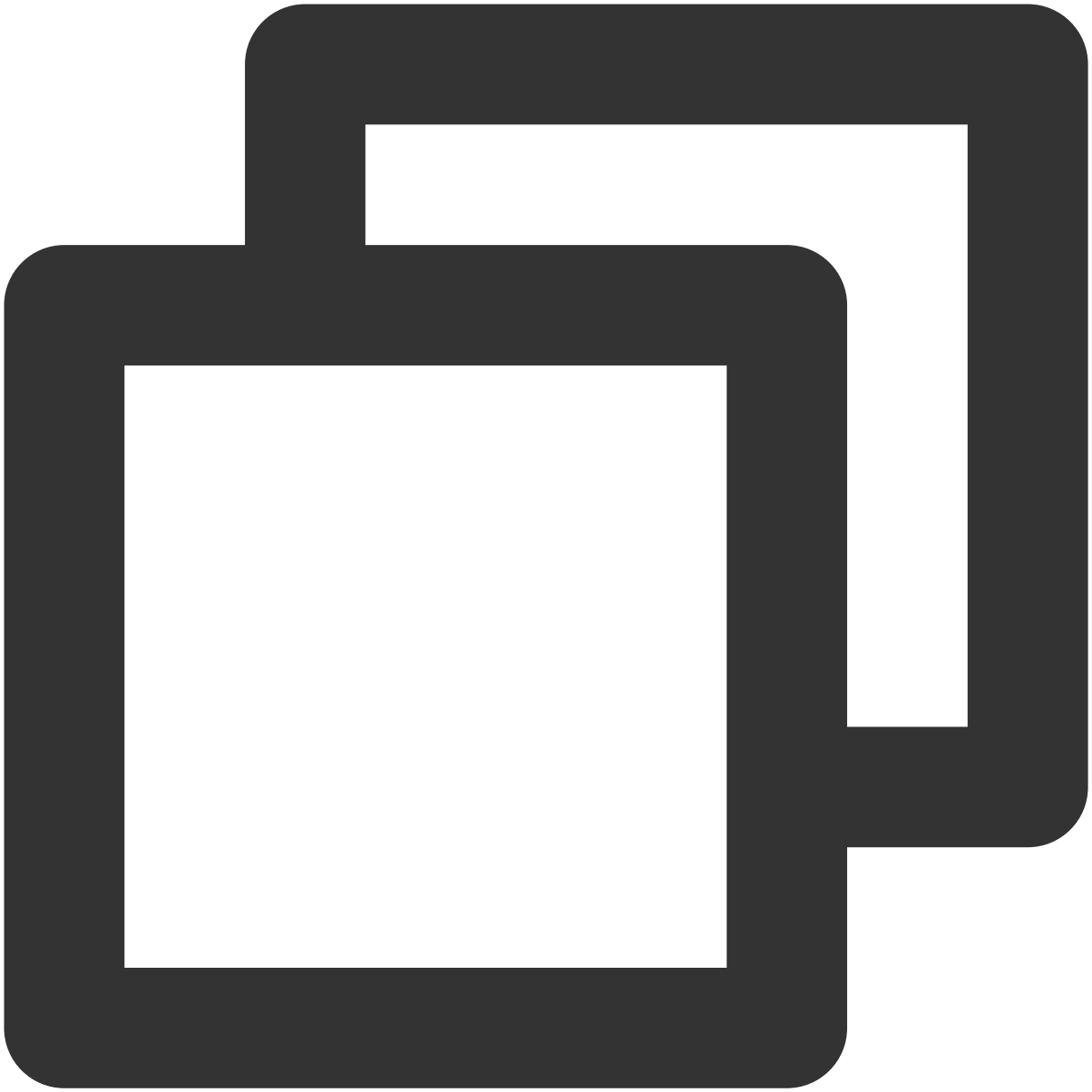
Field Description

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
}
```

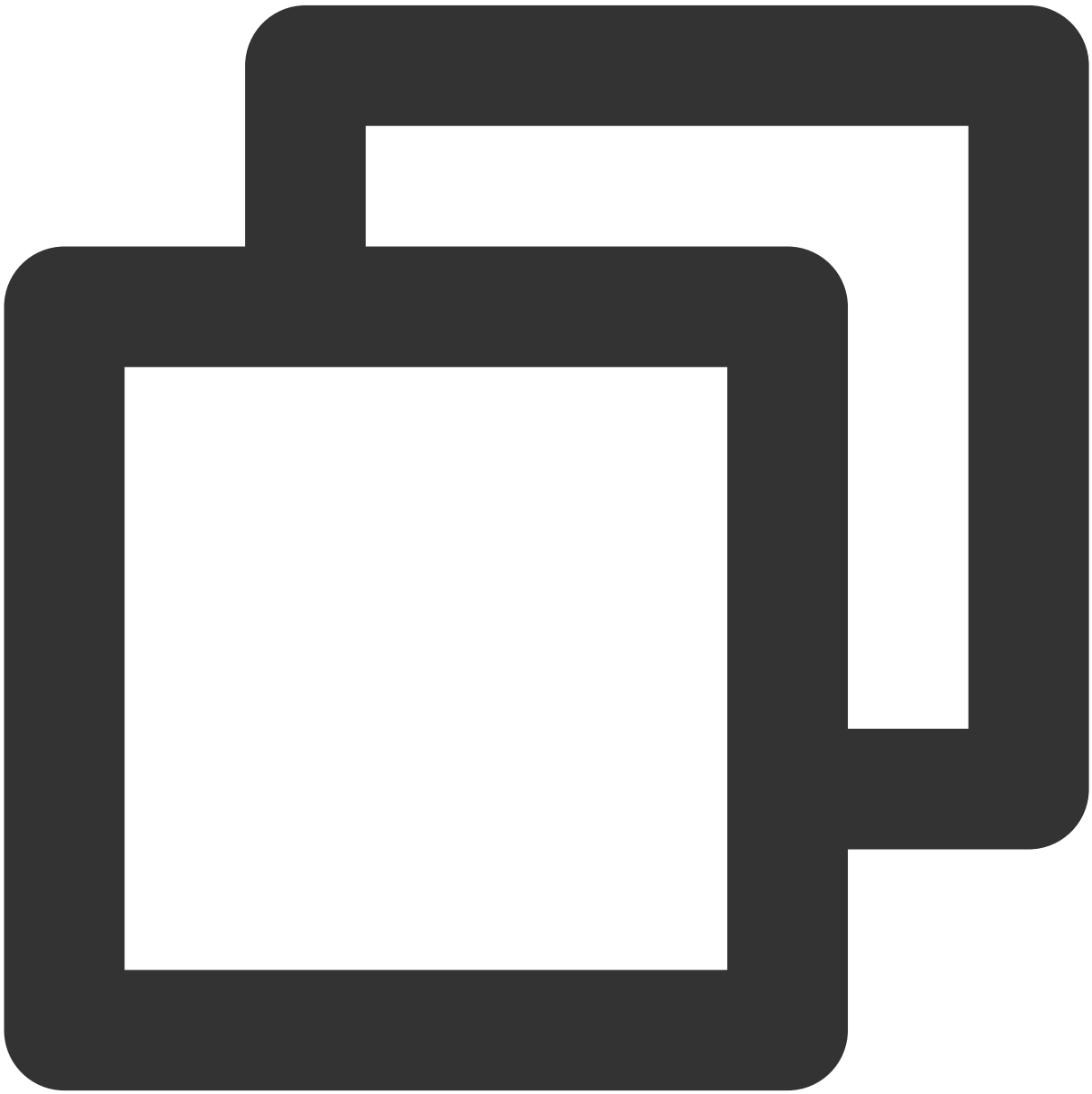
Field Description

Field name	Description

file_type	File type
path	File path
level	Danger level

Exceptional Processes

Sample



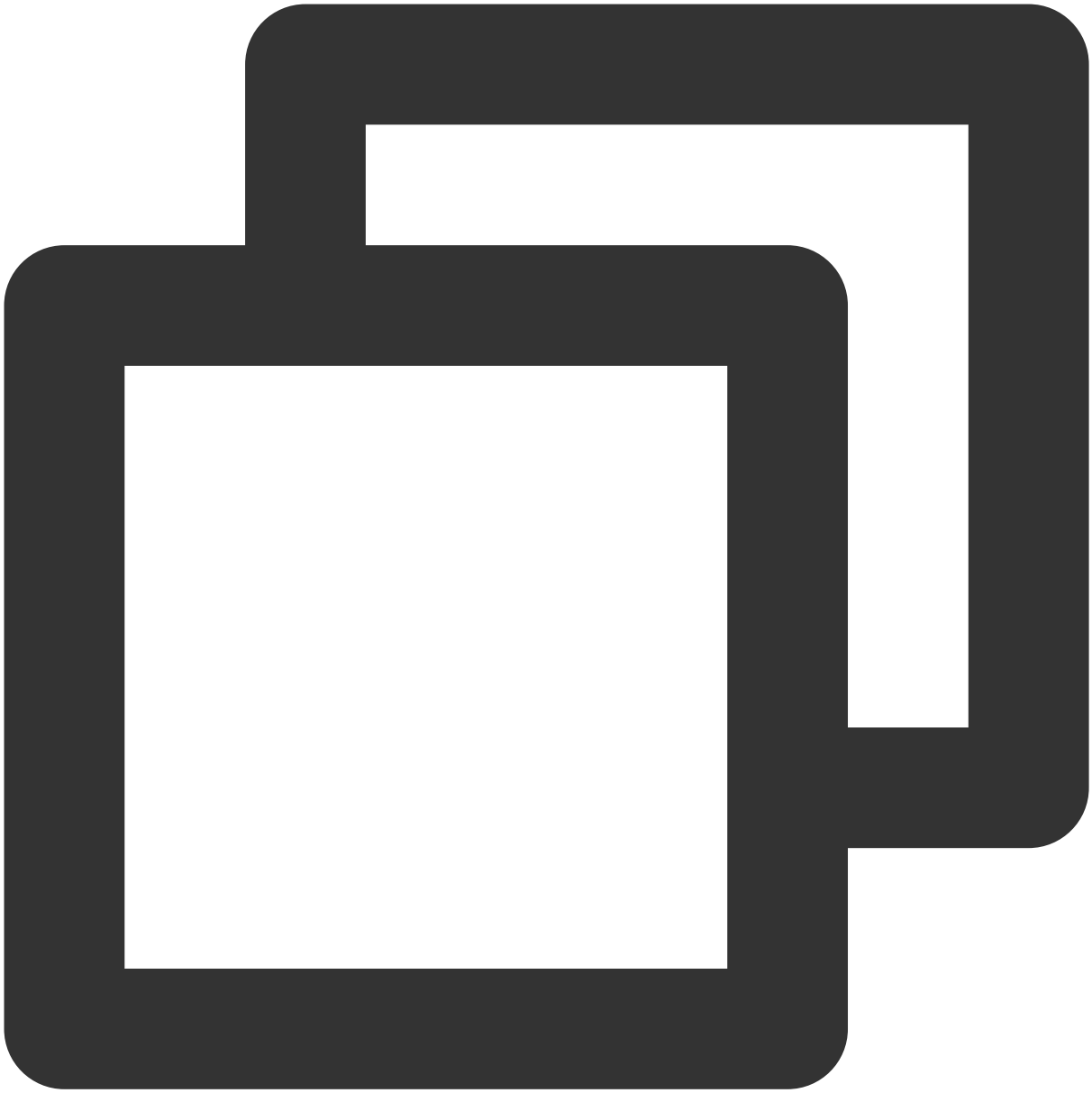
```
{
    "event_type": "Exceptional Processes",
    "pid": "5916",
    "path": "/root/2/ISHELL-v0.2/ishd"
}
```

Field Description

Field name	Description
pid	Process ID
path	Process path

Malicious Requests

Sample



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

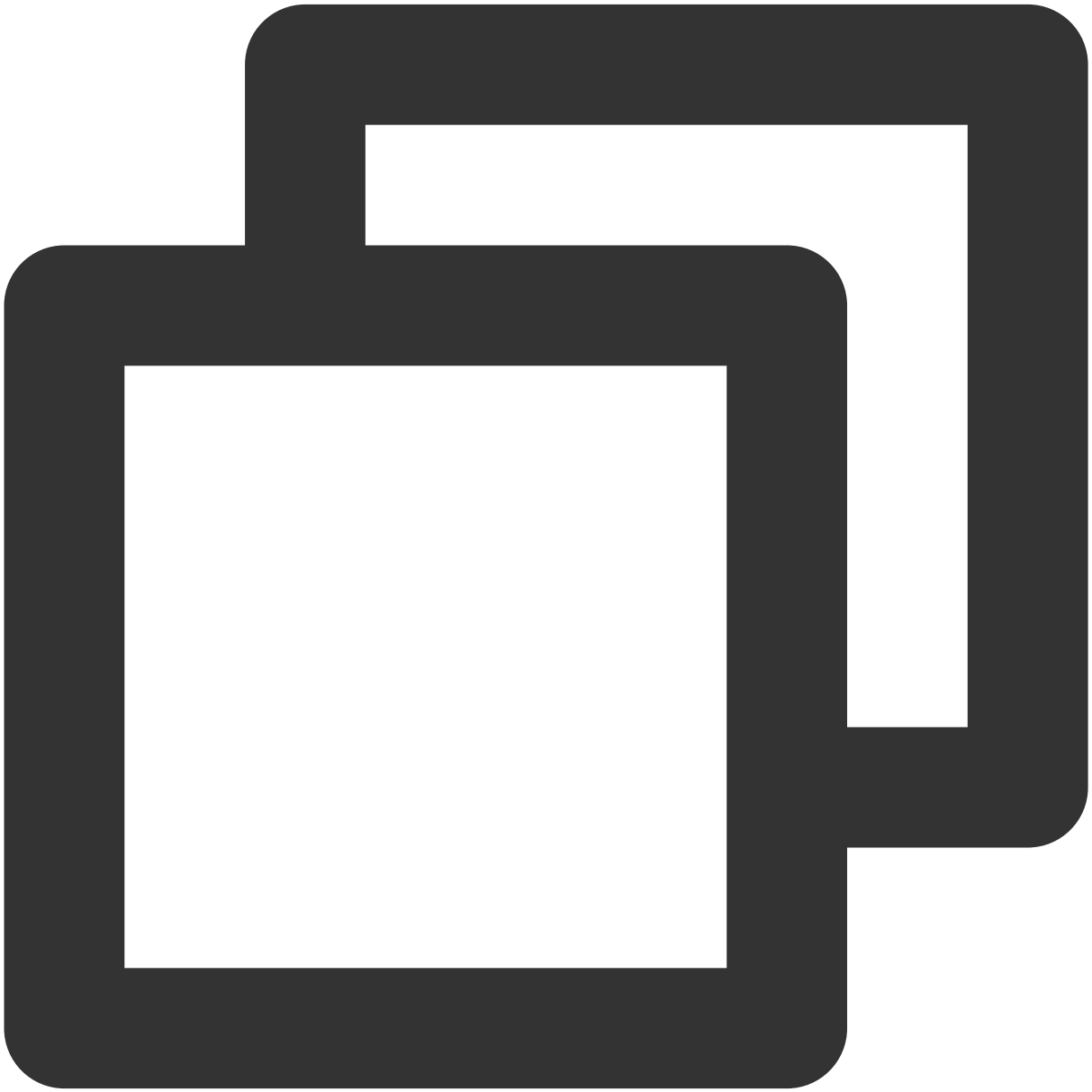
Field Description

Field name	Description

url	Malicious domain
count	Number of requests

High Risk Commands

Sample



```
{
```

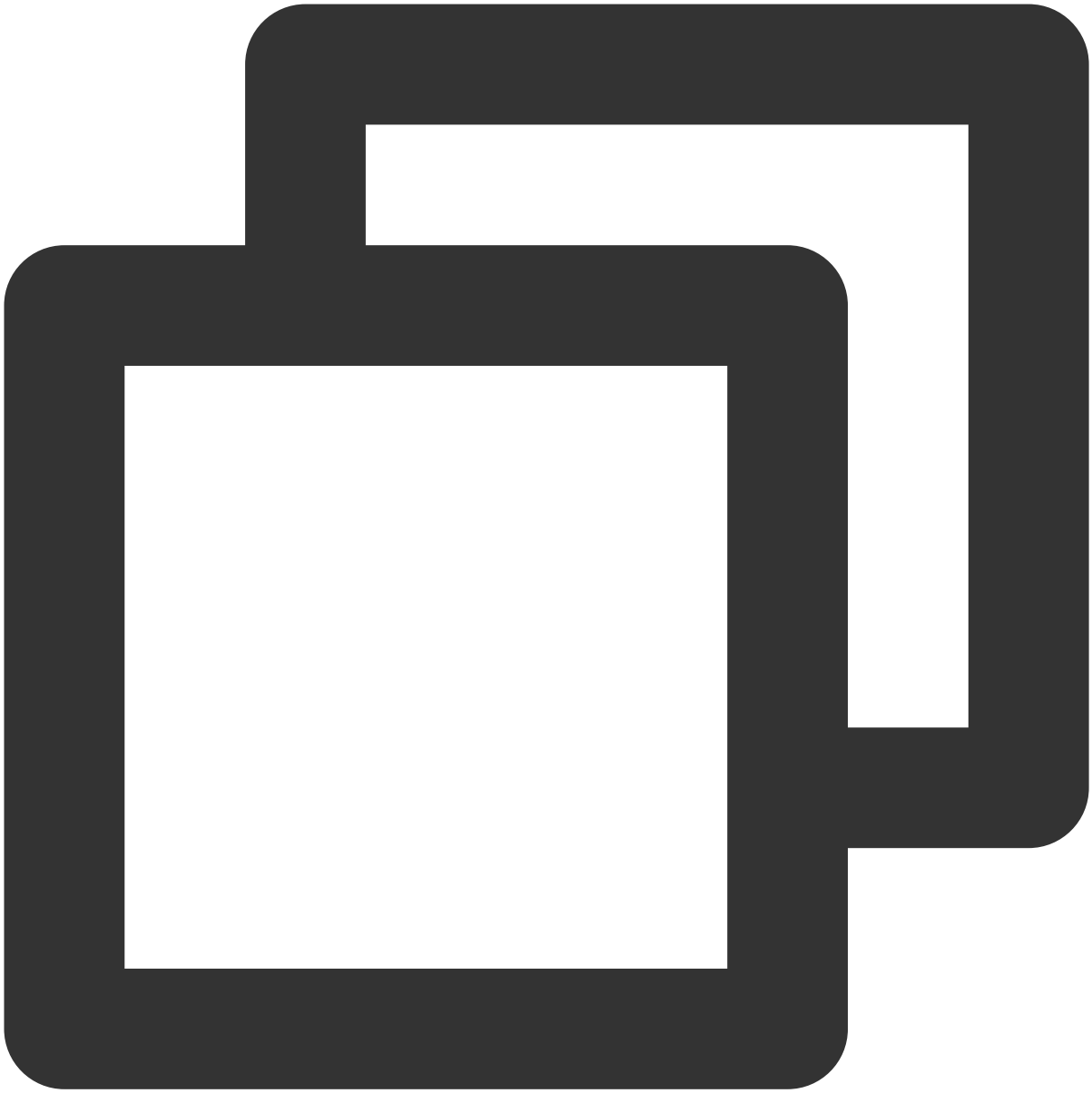
```
    "event_type": "High Risk Commands",
    "cmd": "iptables-restore -w 5 --noflush",
    "level": "High-risk",
    "status": "Processing"
}
```

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"
}
```

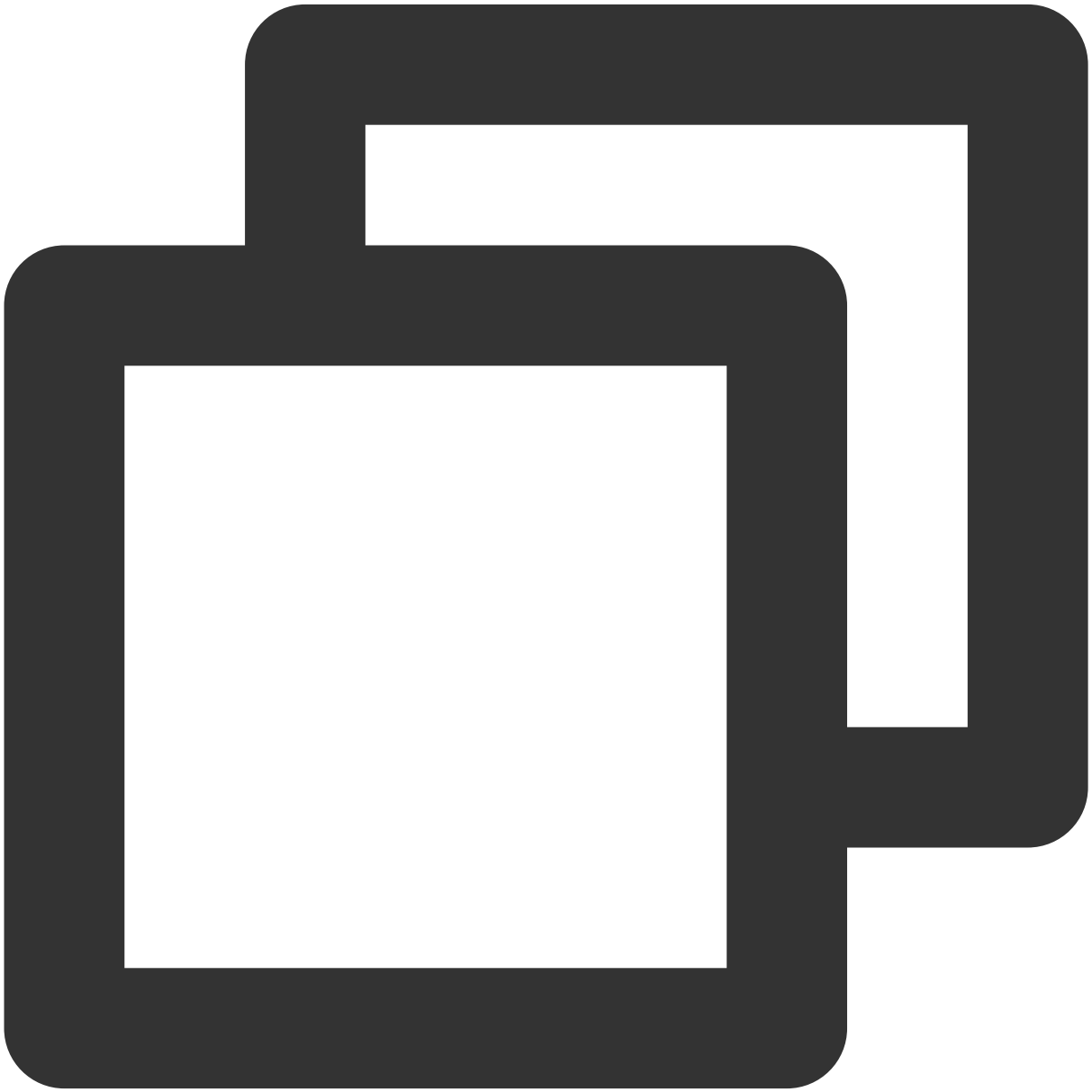
Field Description

Field name	Description

user	Privilege escalation user
process	Privilege escalation process

Reverse Shell

Sample



```
{
```

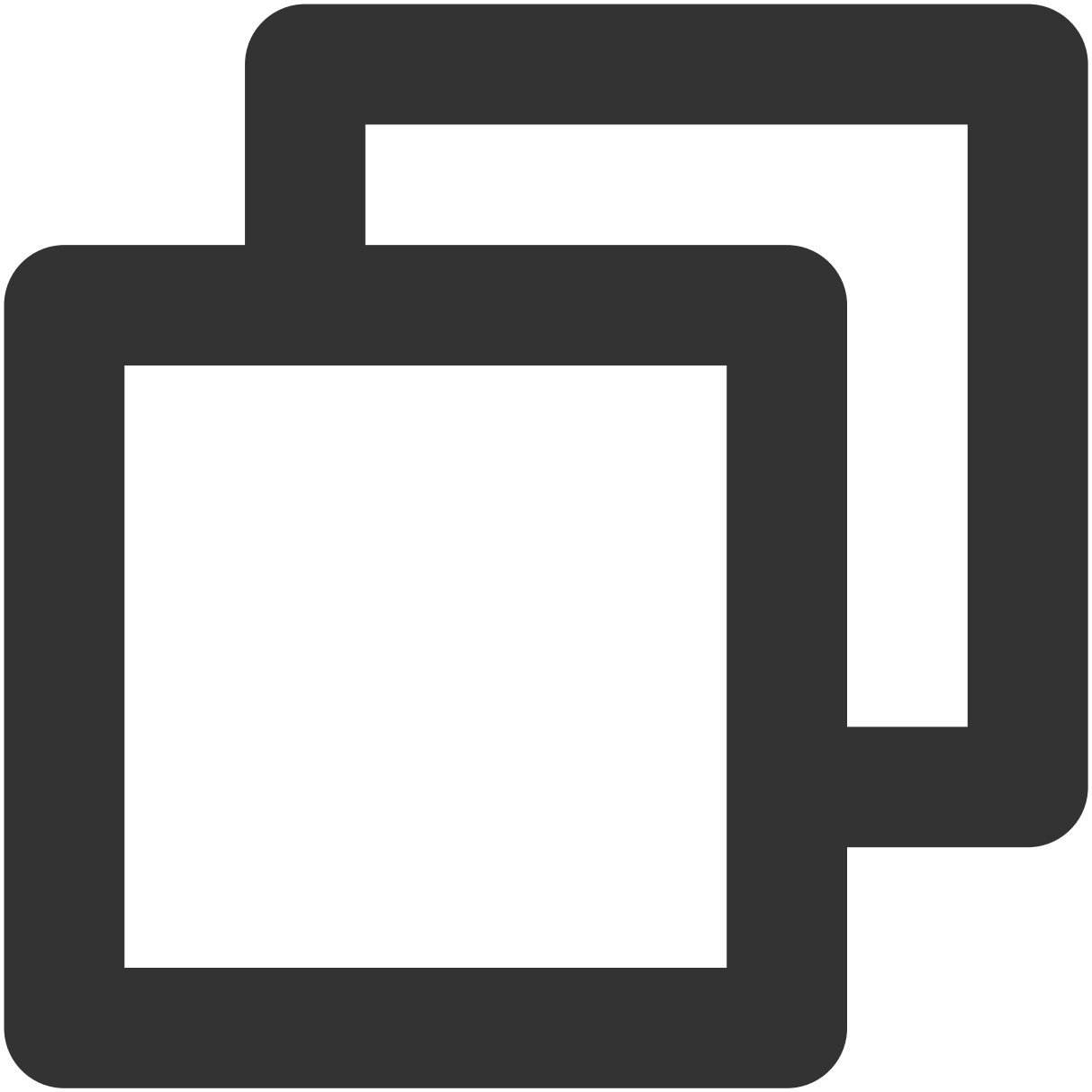
```
    "event_type": "Reverse Shell",
    "process": "mass_0",
    "dst_ip": "125.x.x.220",
    "dst_port": "8888"
}
```

Field Description

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

Java Webshell

Sample



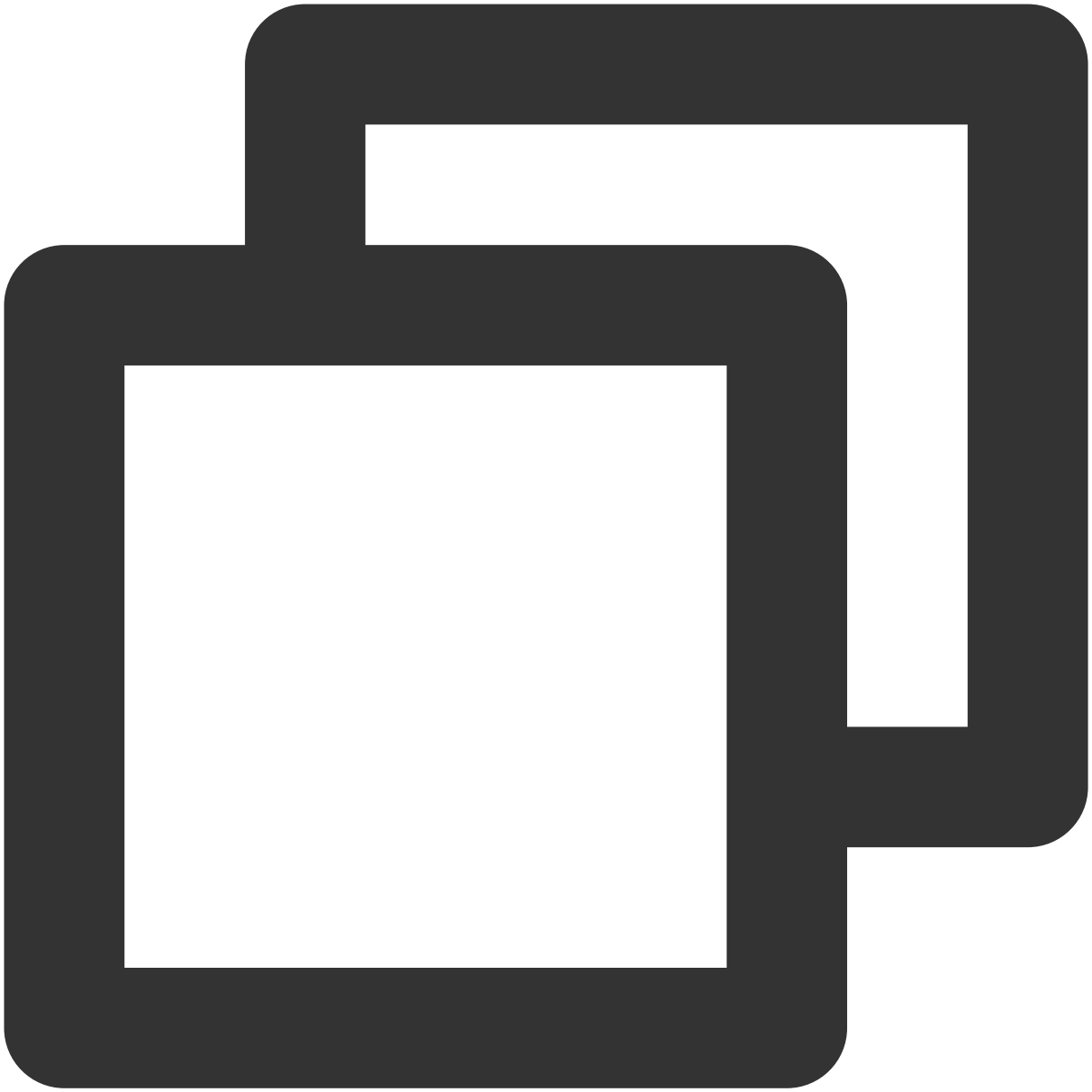
```
{
    "event_type": "Java Webshell",
    "type": "Java Webshell - Servlet",
    "pid": "3333",
    "argv": "masstest",
    "class_name": "massTest"
}
```

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



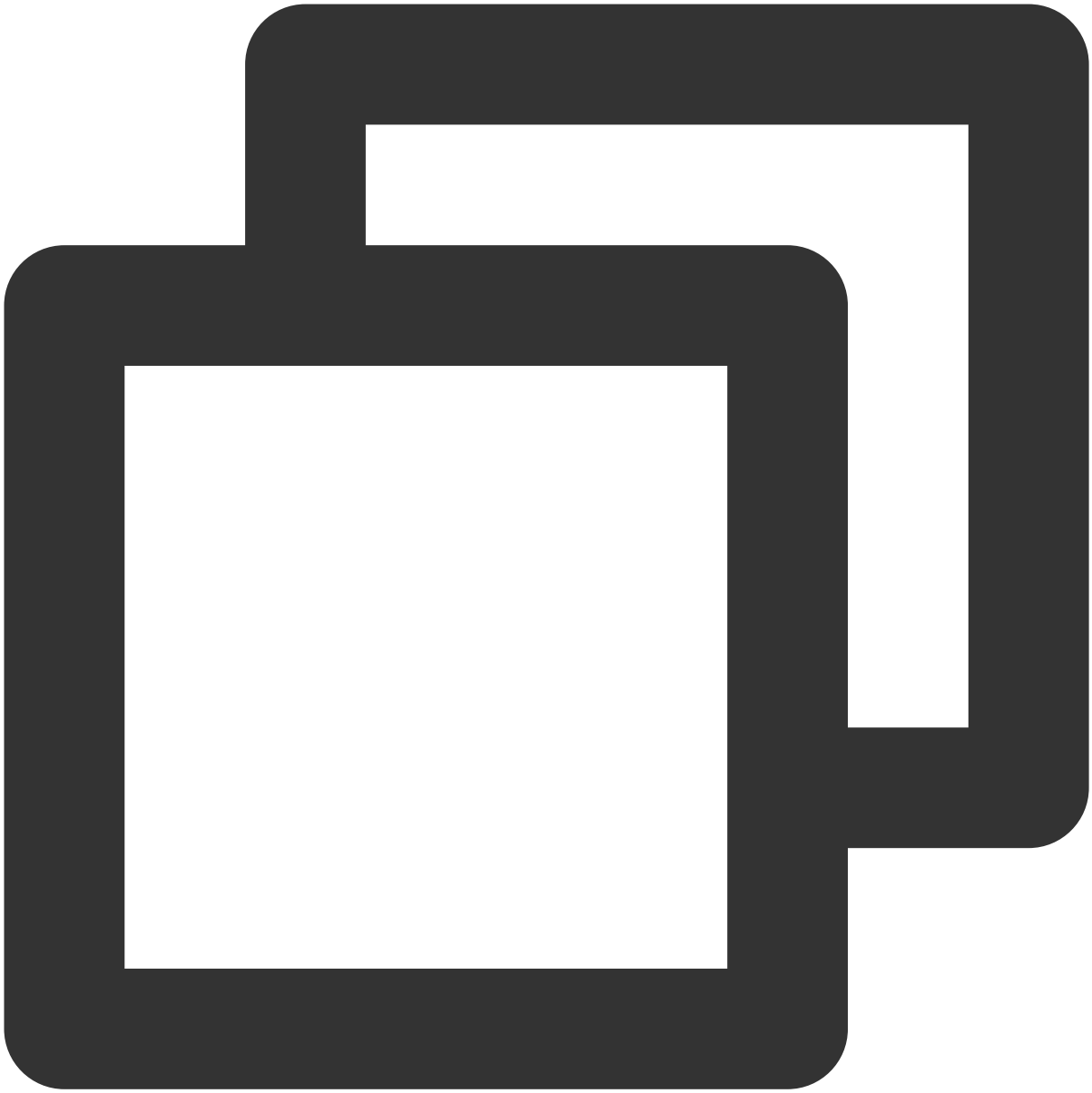
```
{
    "event_type": "CoreFiles",
    "rule_name": "adwqdadwqd",
    "exe_path": "/usr/bin/systemd-tmpfiles",
    "file_path": "/home",
    "count": "1",
    "level": "High-risk"
}
```

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



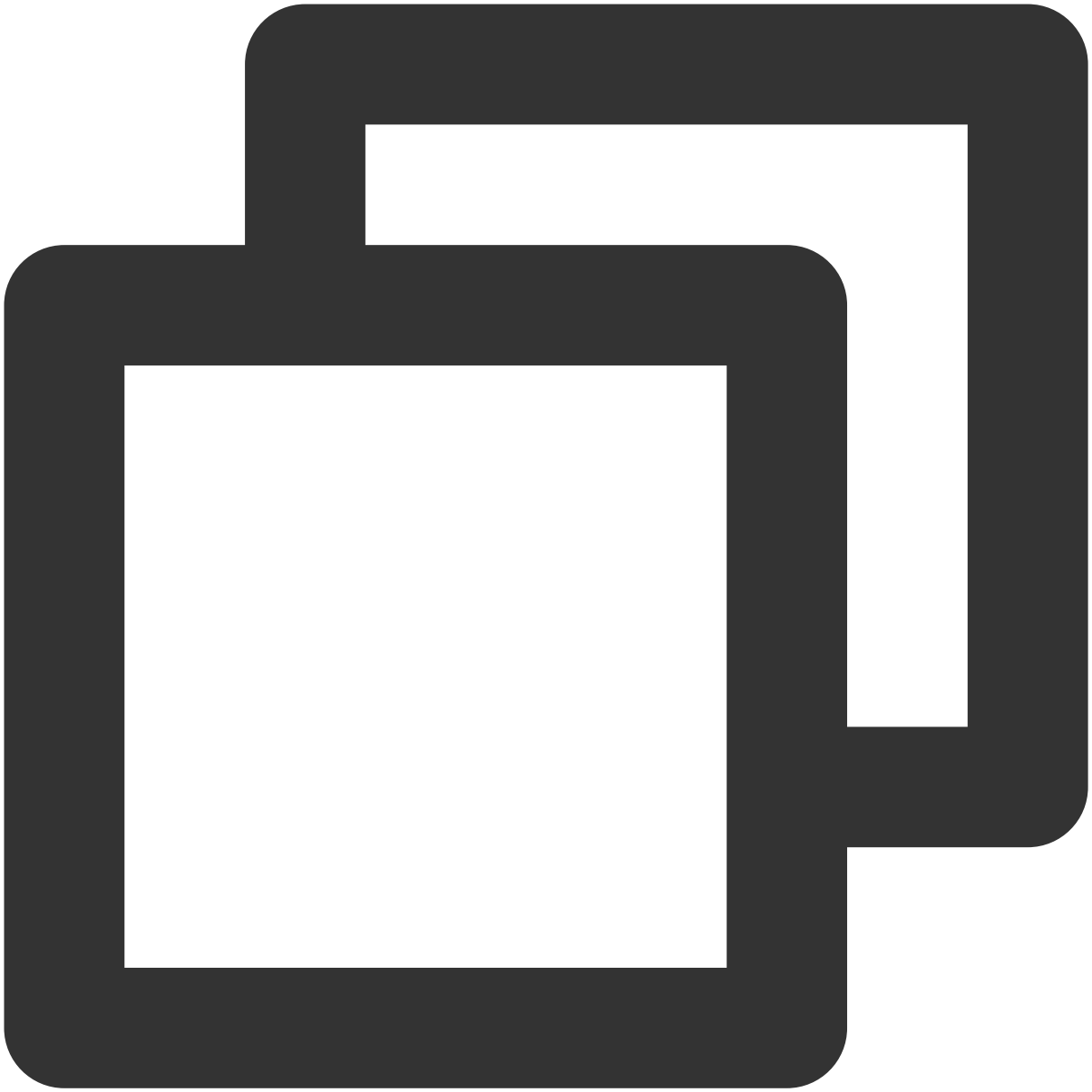
```
{
    "event_type": "Network Attacks",
    "src_ip": "129.x.x.166",
    "city": "Nanjing City, Jiangsu Province",
    "vul_name": "showdoc File Upload Vulnerability",
    "dst_port": "80",
    "status": "Attempted Attacks"
}
```

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

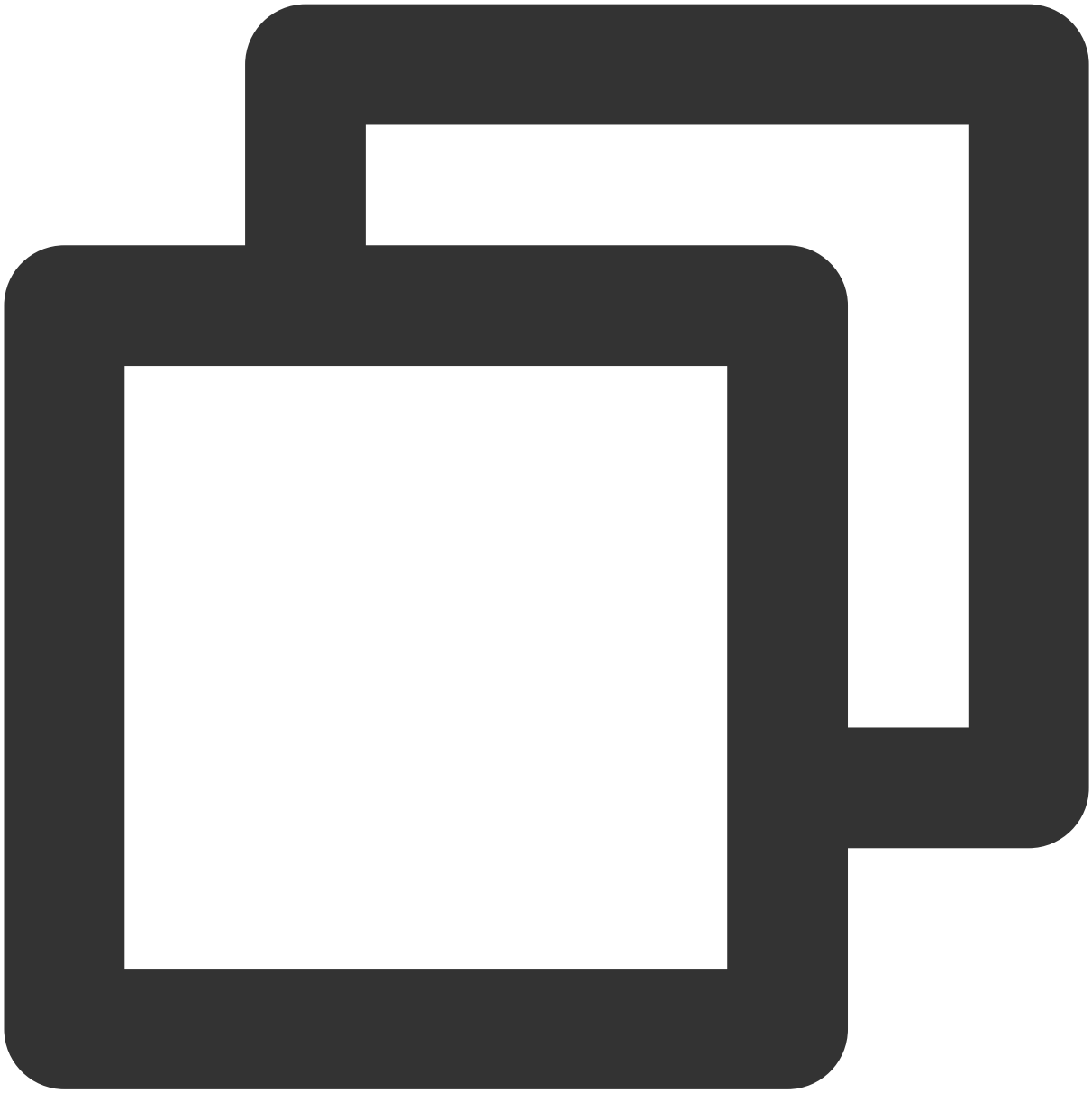


```
{
    "event_type": "Offline Client",
    "offline_hour": "1"
}
```

Field Description

Field name	Description
offline_hour	Client offline duration

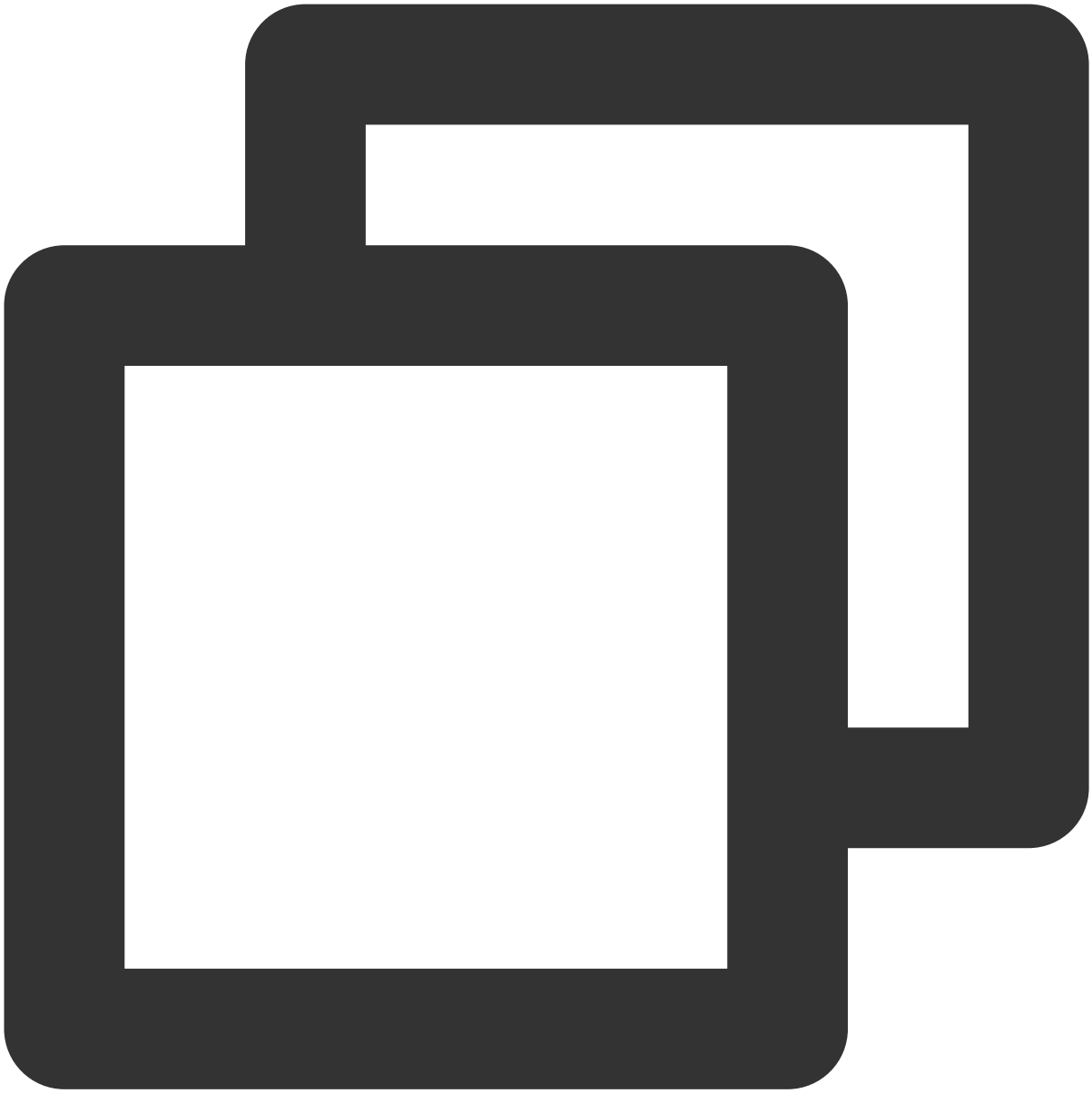
##Client Uninstallation



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

Vulnerability Notification

Sample



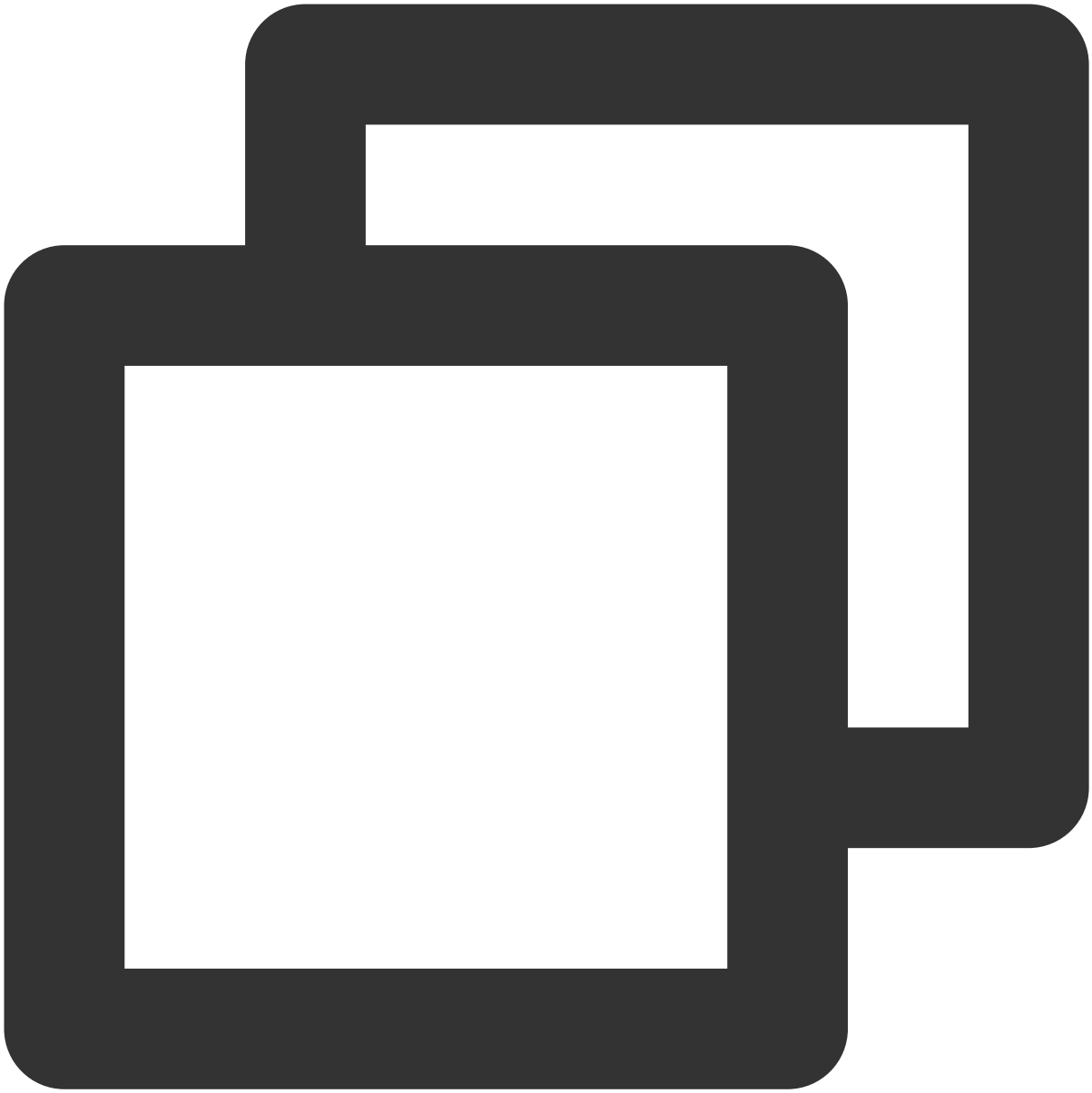
```
{
    "event_type": "Vulnerability",
    "category": "Linux Software Vulnerabilities",
    "vul_name": "libexpat Code Execution Vulnerability (CVE-2022-40674)",
    "level": "Critical"
}
```

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"
}
```

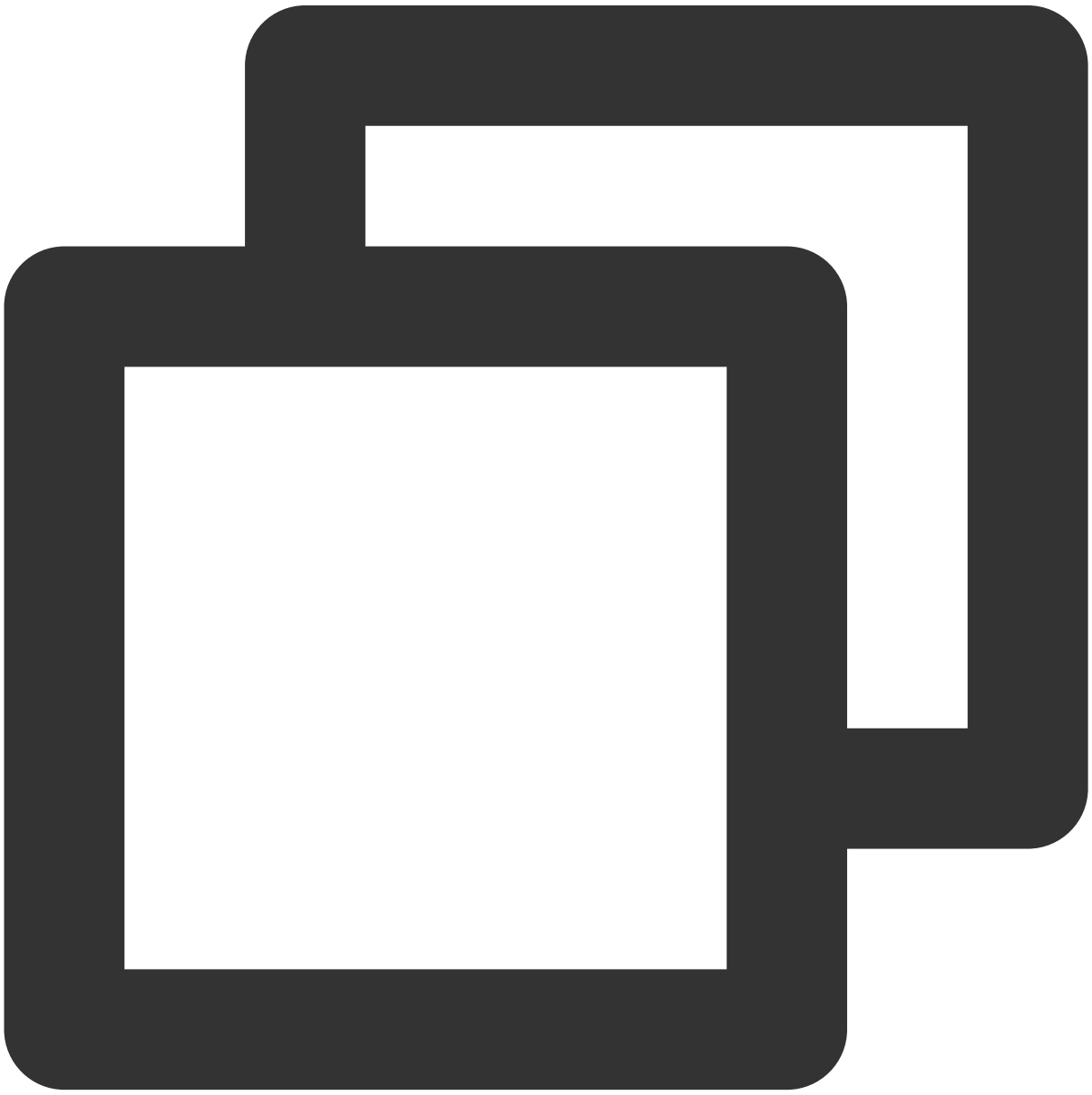
Field Description

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"
}
```

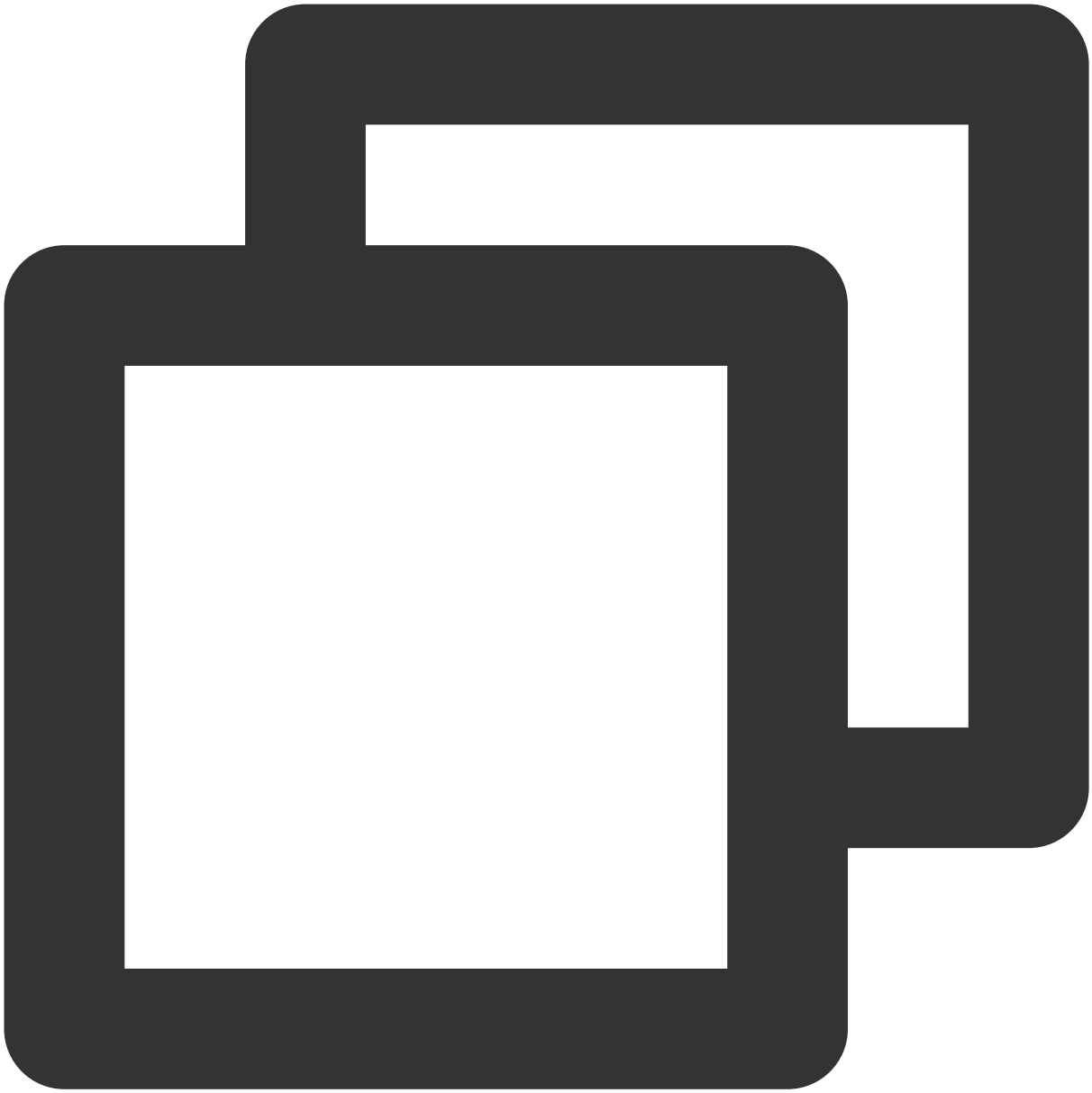
Field Description

Field name	Description
file_path	File directory

Web Tamper Protection

Successful Tampering

Sample



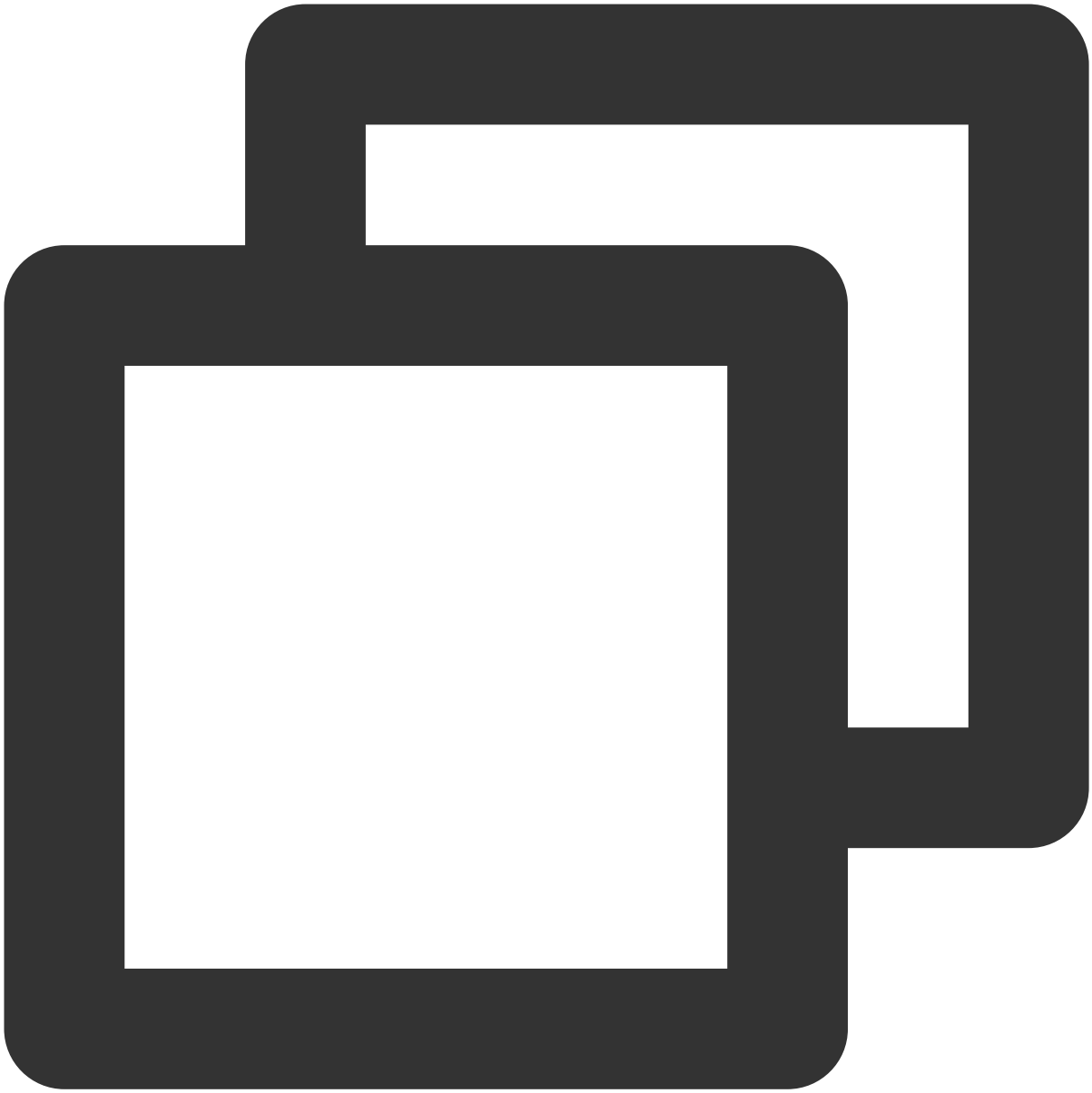
```
{
    "event_type": "Web Tamper Protection (Successful Tampering)",
    "protect_name": "Important File",
    "protect_path": "/tmp",
    "recover_type": "New File Creation",
    "recovered_status": "Not Recovered",
}
```

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

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.

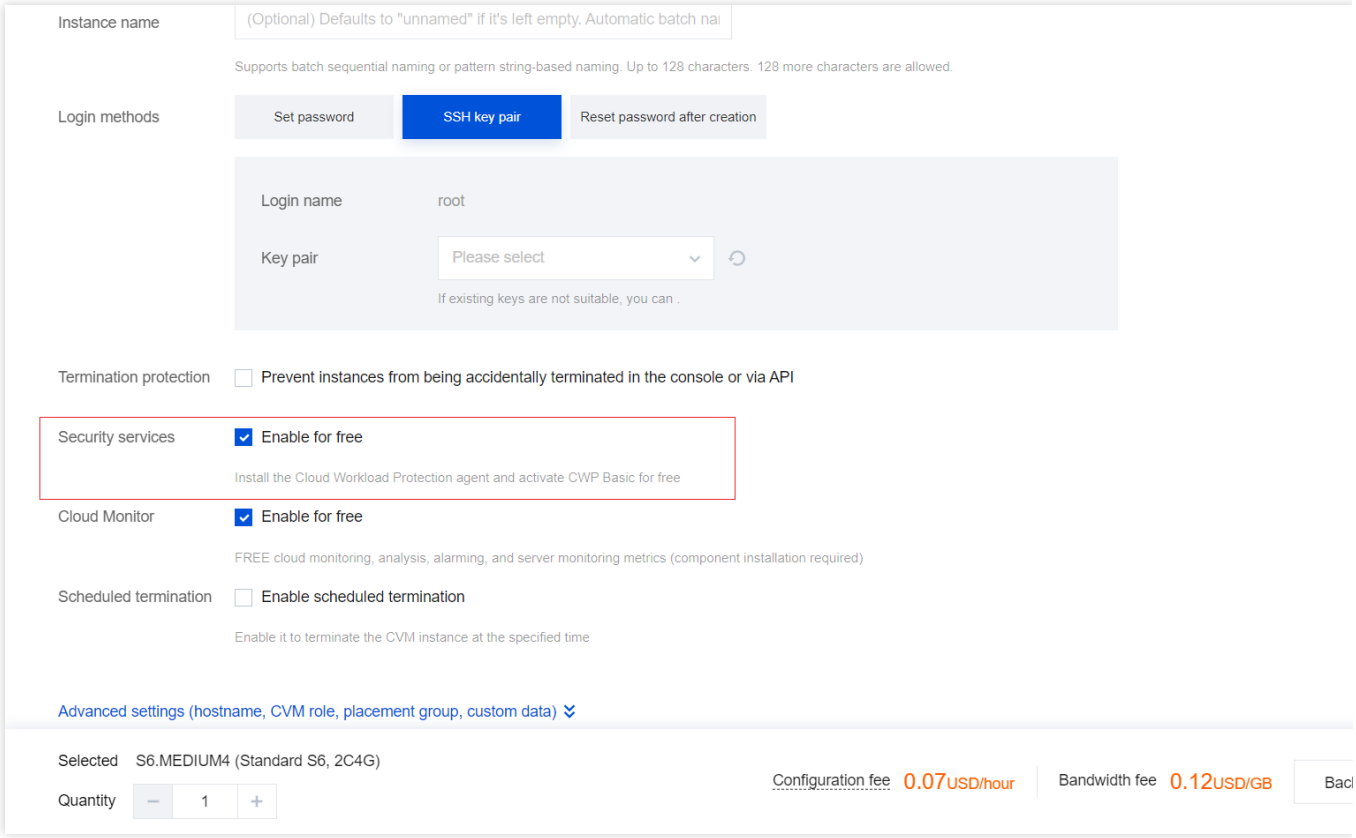
Conditions	Description
Server type	CWPP supports servers running in a hybrid cloud. Tencent Cloud: CVM, Lighthouse, and ECM Non-Tencent Cloud servers: third-party cloud vendor servers and IDC servers
Server OS	Linux CentOS: 6, 7, 8 (64-bit) Ubuntu: 9.10 - 20.10 (64 bit) Debian: 6, 7, 8, 9, 10, 11 (64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

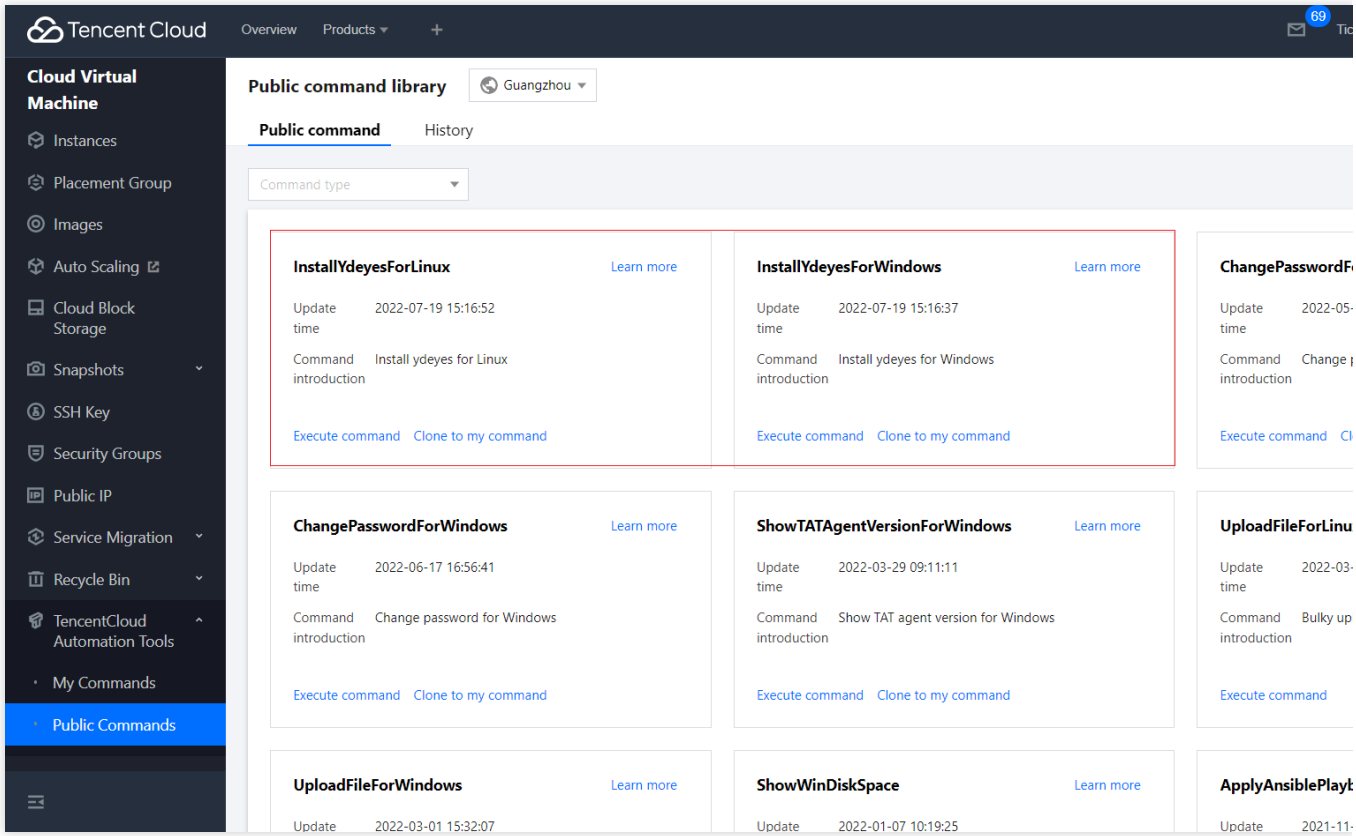
When purchasing the above servers, select **Security Reinforcement** to automatically install the CWPP Agent.



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

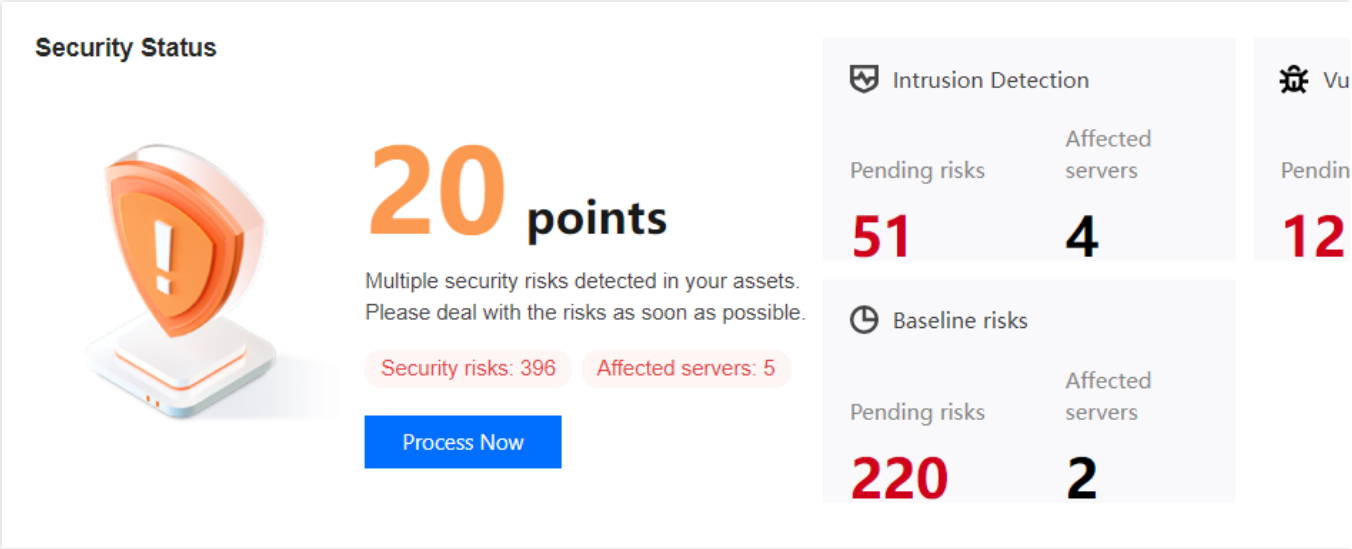
Security Score Overview

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.