主机安全

软件相关说明

产品文档

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2024 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【商标声明】

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

文档目录

软件相关说明
- 功能行为描述
- 客户端进程说明
- 安全基线检测列表
- JSON 格式告警数据解析
- 日志字段数据解析
- 客户端安装指引
- 安全评分说明

版权所有：腾讯云计算（北京）有限责任公司

软件相关说明
功能行为描述

最近更新时间：2023-12-26 15:26:49

Webshell 检测

Webshell 是黑客入侵过程中常用工具，主机安全客户端会对服务器上新创建的 Web 程序文件进行可疑风险判断，对于少量疑似 Webshell 文件，需要上报到云端，通过云端的机器学习检测引擎模块做进一步检测，检测完成后会实时删除该样本文件。主机安全默认提供每天全盘扫描服务，检测过程不会提取任何涉及用户隐私的数据。

登录异常提醒

登录异常提醒功能可以帮助用户识别异常的管理员登录行为，需要采集登录日志中的来源 IP、时间、登录用户名、登录状态数据到云端进行风险计算，登录日志数据需在云端保存一个月。

密码破解提醒

密码破解提醒功能可以告诉用户当前遭受的密码破解事件和破解结果，需要采集登录日志中的来源 IP、时间、登录用户名、登录状态数据到云端进行风险计算，登录日志数据需在云端保存一个月。

恶意木马和病毒检测

恶意木马和病毒程序通常会窃取用户数据或者对外攻击，消耗大量系统资源导致业务不能正常提供服务。客户端会采集可疑恶意程序的 哈希指纹 到云端，通过云查杀模块对哈希指纹进行检测，若云端哈希库无该文件记录，需要上报可执行文件到云端，通过云端杀毒引擎进行检测，检测完后会实时删除该样本文件。主机安全默认提供每天全盘扫描服务，检测过程中不会提取任何涉及用户隐私的数据。

漏洞提醒

目前主机安全支持检测影响面较大的 Linux 和 Windows 双平台的漏洞，以及符合腾讯云安全要求的基线检测。漏洞管理功能会显示当前主机上的漏洞风险情况，同时提供修复方案供用户参考。该模块执行时会从云端下载漏洞策略库在本地执行检测，对于存在漏洞风险的主机，会上报应用软件的名称、版本号、路径、发现时间。主机安全默认提供每天漏洞扫描服务，这个过程不会提取任何涉及用户隐私的数据。

升级维护

升级维护功能主要提醒用户对客户端进行升级，以获得最新的安全防护服务，客户端软件需要采集主机安全版本号、操作系统配置信息、安全规则版本号到云端进行判断和提醒，该过程不会提取任何涉及用户隐私的数据。

版权所有：腾讯云计算（北京）有限责任公司

客户端进程说明

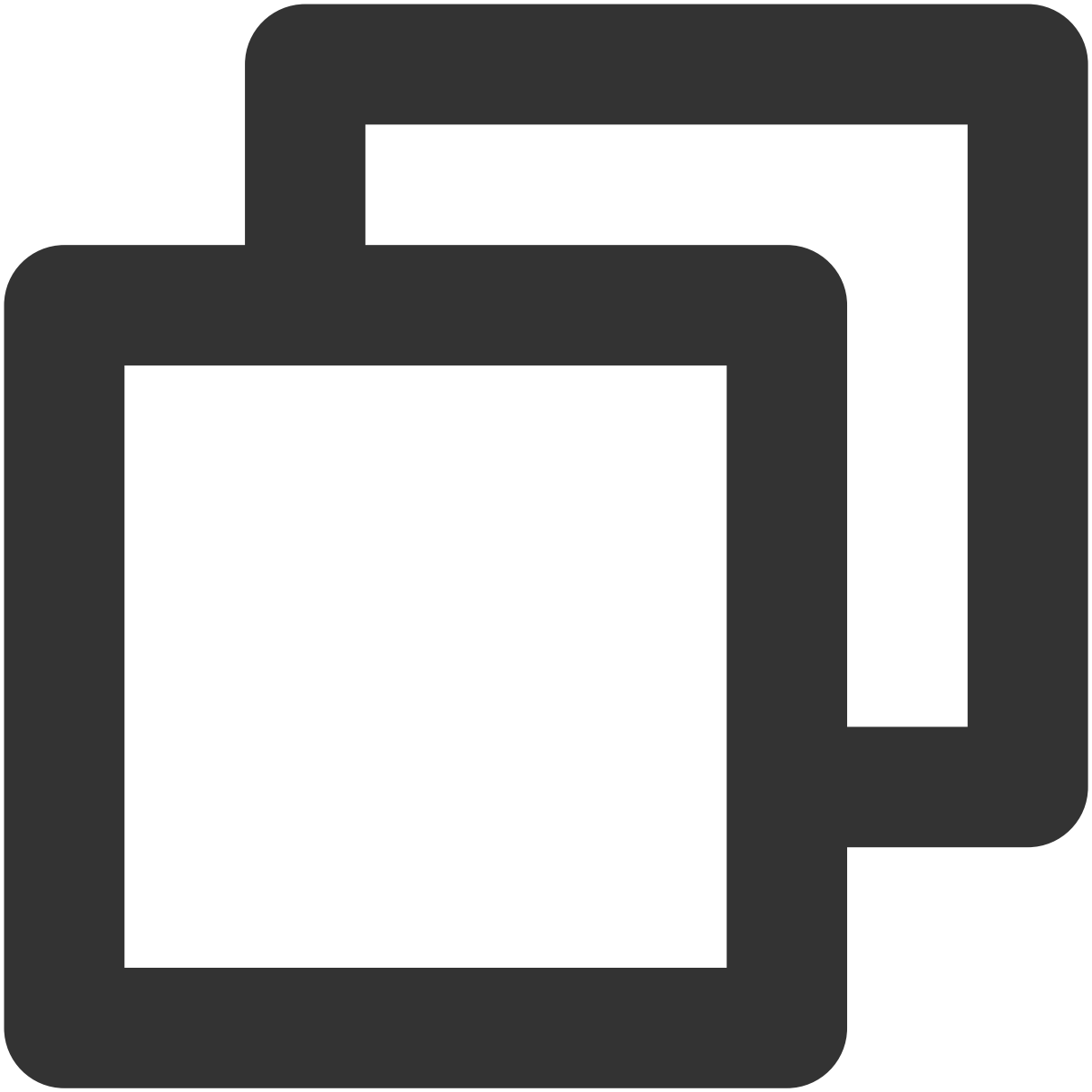
最近更新时间：2023-12-26 15:26:58

名称	Windows 系统	Linux 系统
程序安装目录	C:\\program files\\qcloud\\yunjing\\ydeyes C:\\program files\\qcloud\\yunjing\\ydlive	/usr/local/qcloud/YunJing/
进程名称	YDService 云镜主服务进程 YDLive 守护进程 YDPython 漏洞&基线扫描插件 YDQuaraV2 木马隔离插件 qtflame 资产采集插件	YDService 云镜主服务进程 YDLive 守护进程 YDPython 漏洞&基线扫描插件 YDUtils 进程扫描插件 YDQuaraV2 木马隔离插件 qtflame 资产采集插件 tcss-agent 容器基线扫描插件 tcss-scan 容器镜像扫描插件
注册服务名称	YDService YDLive YDEdr	-

客户端程序所占用端口是系统随机返回的，无固定端口范围，若占用端口与用户业务端口冲突，重启客户端程序即可。

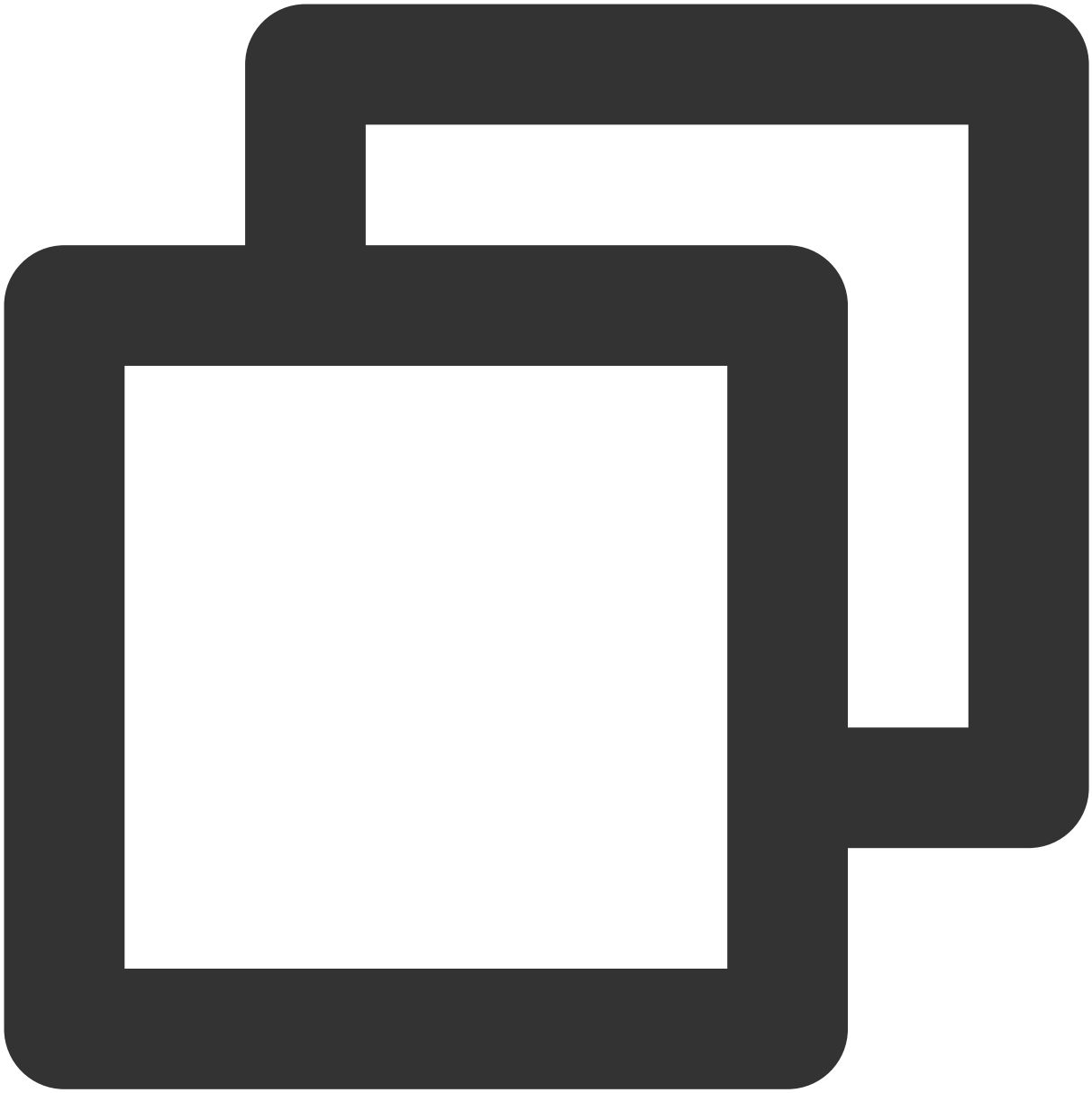
客户端重启命令（Linux系统）

1.1 暂停客户端程序服务



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

1.2 重新启动客户端

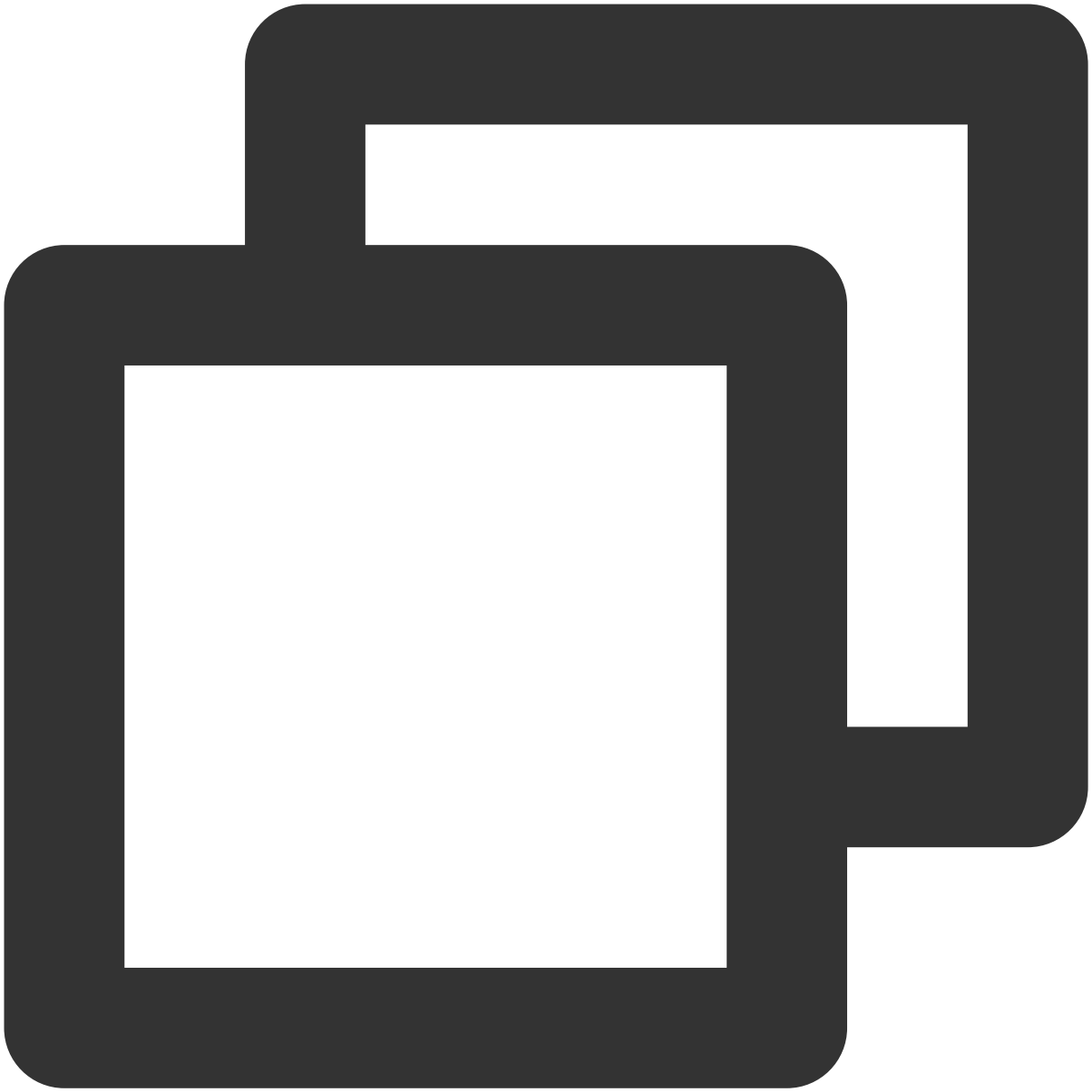


```
/usr/local/qcloud/YunJing/startYD.sh
```

客户端重启命令（Windows系统）

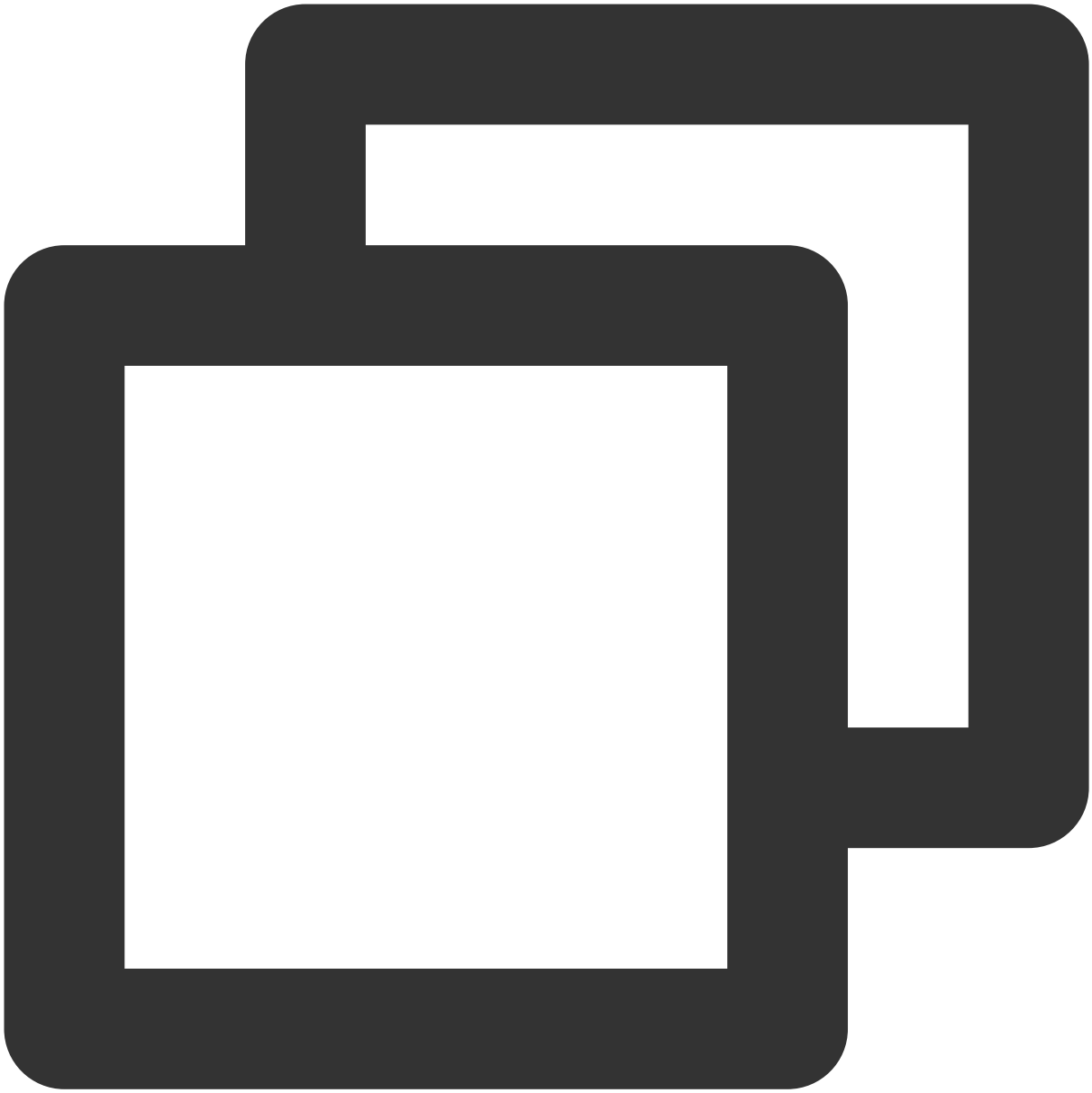
输入以下命令，或打开任务管理器的服务，找到 YDService 服务，右键重启。

1.1 暂停客户端程序服务



```
net stop YDService
```

1.2 重新启动客户端



```
net  start YDService
```

安全基线检测列表

最近更新时间：2024-08-13 16:31:25

本文档将为您介绍主机安全的安全基线检测列表。

注意：

安全基线在产品设置后，将即时生效。

Name	Level	Vul_type
CouchDB 未授权访问	高	配置不当
Docker Daemon 2375 管理端口开启	高	远程代码执行
Elasticsearch 未授权访问	高	配置不当
JavaRMI 远程代码执行	高	远程代码执行
Jenkins 未开启认证可导致命令执行	高	远程代码执行
Kubelet 未授权访问	高	安全基线
Linux 系统弱口令检测	高	远程代码执行
MongoDB 未授权访问	高	配置不当
MySQL 弱口令检测	高	弱口令
NFS 错误配置导致可挂载敏感目录	高	配置不当
Redis 基线合规检测	高	远程代码执行
RPCBind 配置不当检测	高	安全基线
Rsync 弱口令检测	高	弱口令
Rsync 无密码访问	高	配置不当
Tomcat 弱口令检测	高	弱口令
Windows 用户弱口令检测	高	弱口令
Xampp 默认 FTP 密码	高	信息泄露
网站目录存在备份文件	高	信息泄露
FTP 匿名登录检测	中	信息泄露

版权所有：腾讯云计算（北京）有限责任公司

IIS 配置错误导致存在解析漏洞	中	配置不当
Memcached UDP 端口可被利用为 DDOS 放大攻击	中	信息泄露
PHP-FPM 错误配置	中	安全基线
PostgreSQL 合规检测	中	远程代码执行
Web 目录存在 .git 文件夹导致信息泄露	中	信息泄露
Web 目录存在 .svn 文件夹导致信息泄露	中	信息泄露
Windows 隐藏账户检测	中	安全基线
Windows 影子账户检测	中	远程代码执行
ZooKeeper 未授权访问	中	配置不当
Hadoop未授权访问	低	远程代码执行
sudo 无密码用户检测	低	安全基线
Tomcat 样例目录检测	低	安全基线
Web 目录存在 phpinfo 文件	低	信息泄露
Windows 来宾账户状态检测	低	安全基线

版权所有：腾讯云计算（北京）有限责任公司

JSON 格式告警数据解析

最近更新时间：2024-08-13 16:33:02

本文档将为您介绍在 告警设置 > **机器人通知**设置接收 JSON 格式告警数据后，用户将收到的各类告警的传输字段及说明。

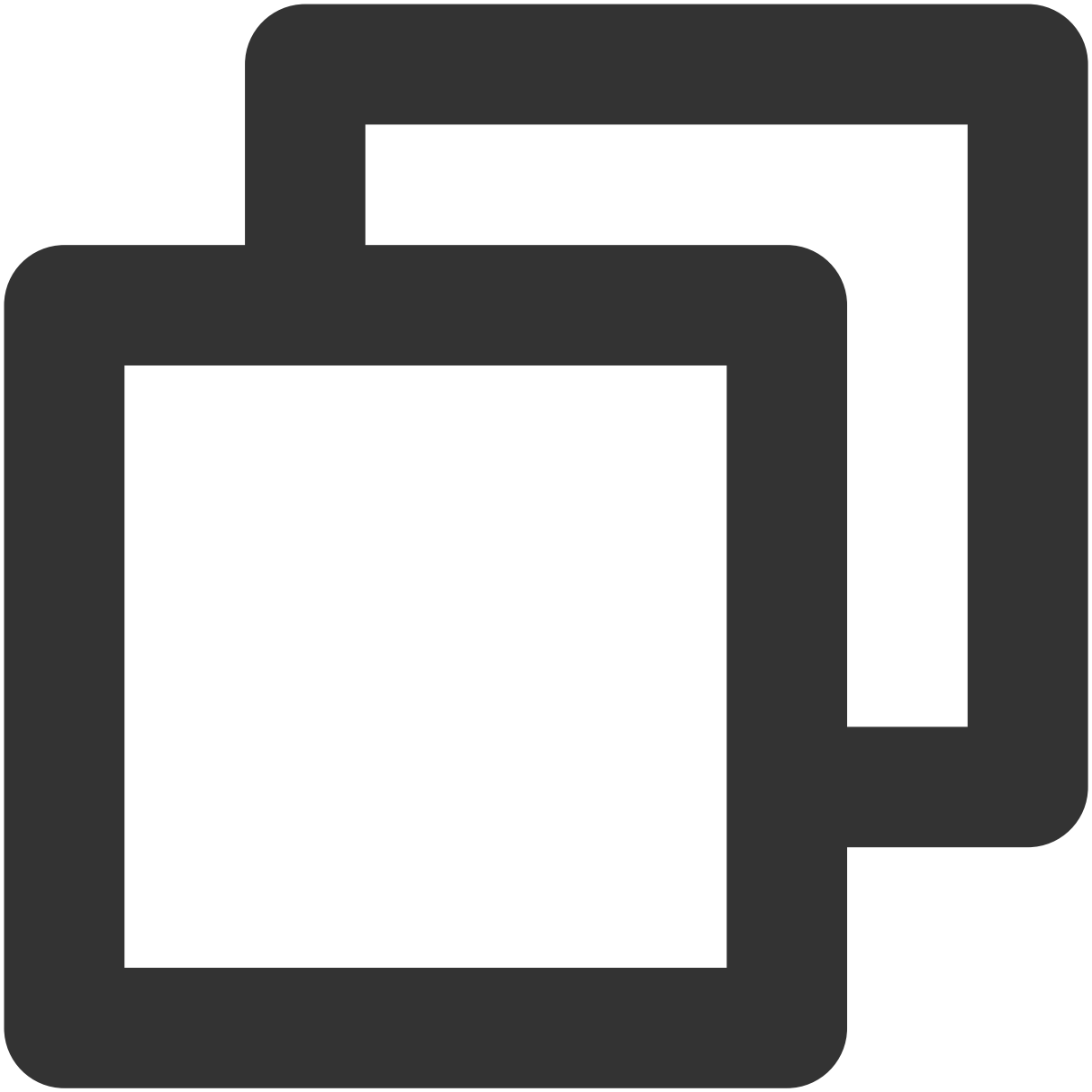
说明

目前机器人通知处于灰度状态，仅对明确有该需求的客户开放，若您希望实时接收主机安全 webhook 机器人告警，请 联系我们 申请使用。

告警设置 > **机器人通知**与消息中心的机器人相互独立，没有关联。

公共字段

示例



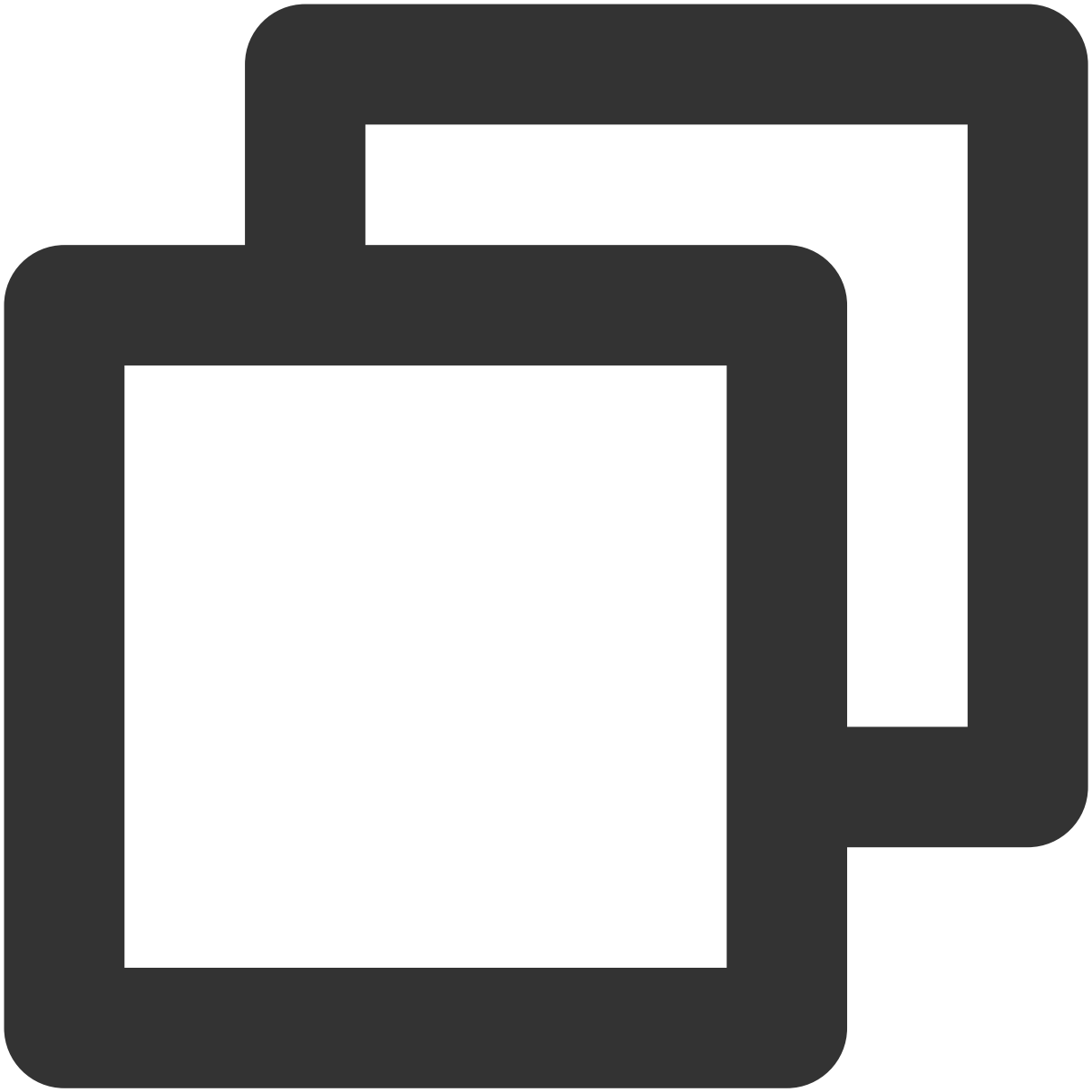
```
{
    "uin": "1000xxxxxx21",
    "nickname": "测试号",
    "server": "172.x.x.41 [测试机器]",
    "instance_id": "ins-xxxxxxxx",
    "region": "西南地区（成都）",
    "time": "2023-10-30 09:24:20"
}
```

字段说明

字段名称	说明
uin	用户 uin
nickname	用户昵称
server	机器 ip [机器别名]
instance_id	机器实例 id
region	机器所在区域
time	事件时间

异常登录

示例



```
{
    "event_type": "异常登录",
    "src_ip": "43.x.x.41",
    "area": "中国香港",
    "level": "高危"
}
```

字段说明

字段名称	说明

src_ip	来源 ip
area	来源地
level	危胁等级

密码破解

示例

```
{
    "event_type": "密码破解",
    "src_ip": "43.x.x.41",
    "area": "中国香港",
    "count": "3",
    "banned": "阻断成功"
}
```

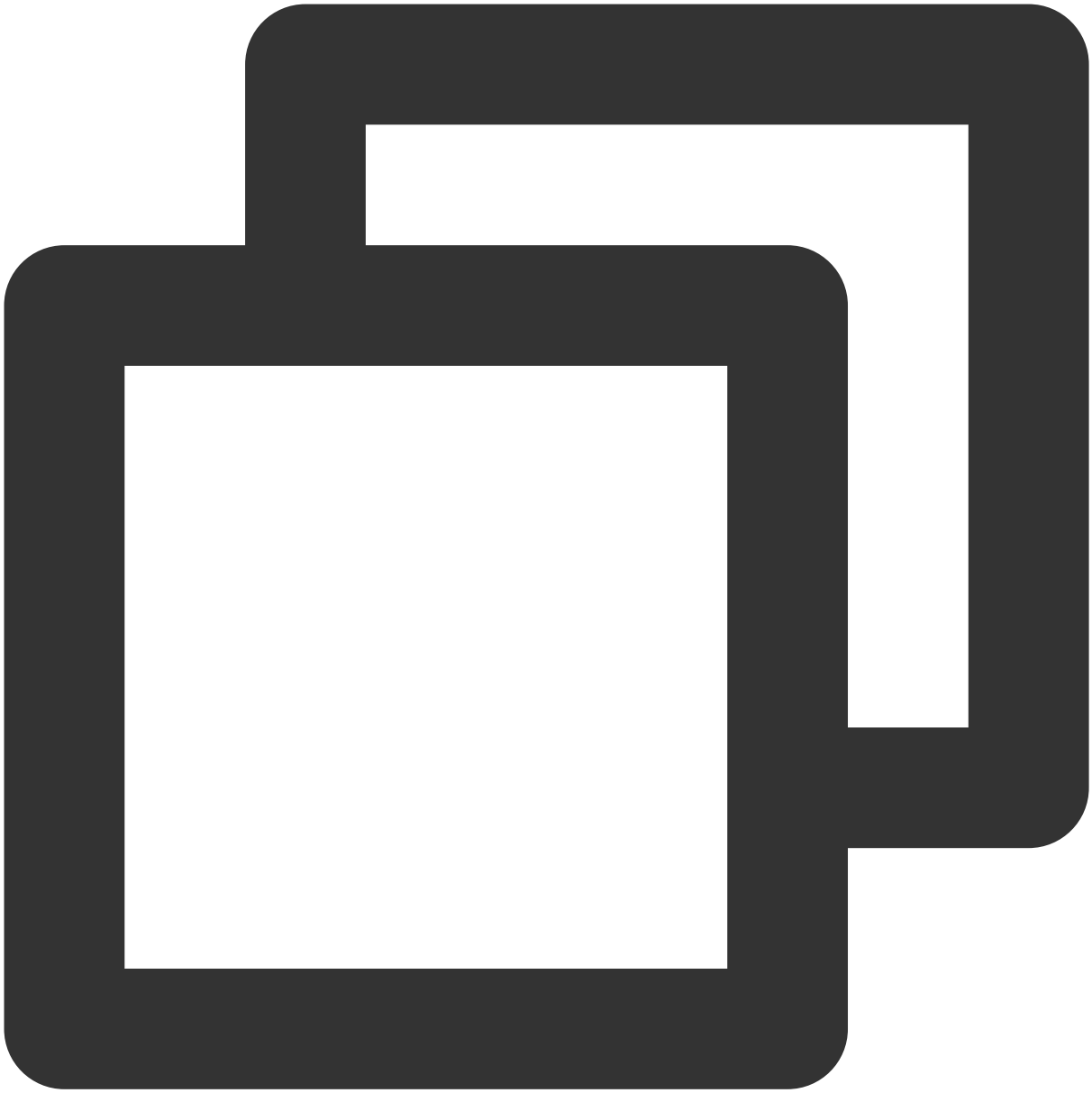
字段说明

字段名称	说明
src_ip	来源 ip
area	来源地
count	尝试次数
banned	阻断状态

文件查杀

恶意文件

示例



```
{
    "event_type": "恶意文件",
    "file_type": "恶意",
    "path": "/root/bebinder_shell.jsp",
    "level": "严重，您的服务器疑似被黑客入侵，建议您及时确认，避免造成严重损失"
}
```

字段说明

字段名称	说明

file_type	文件类型
path	文件路径
level	危险等级

异常进程

示例

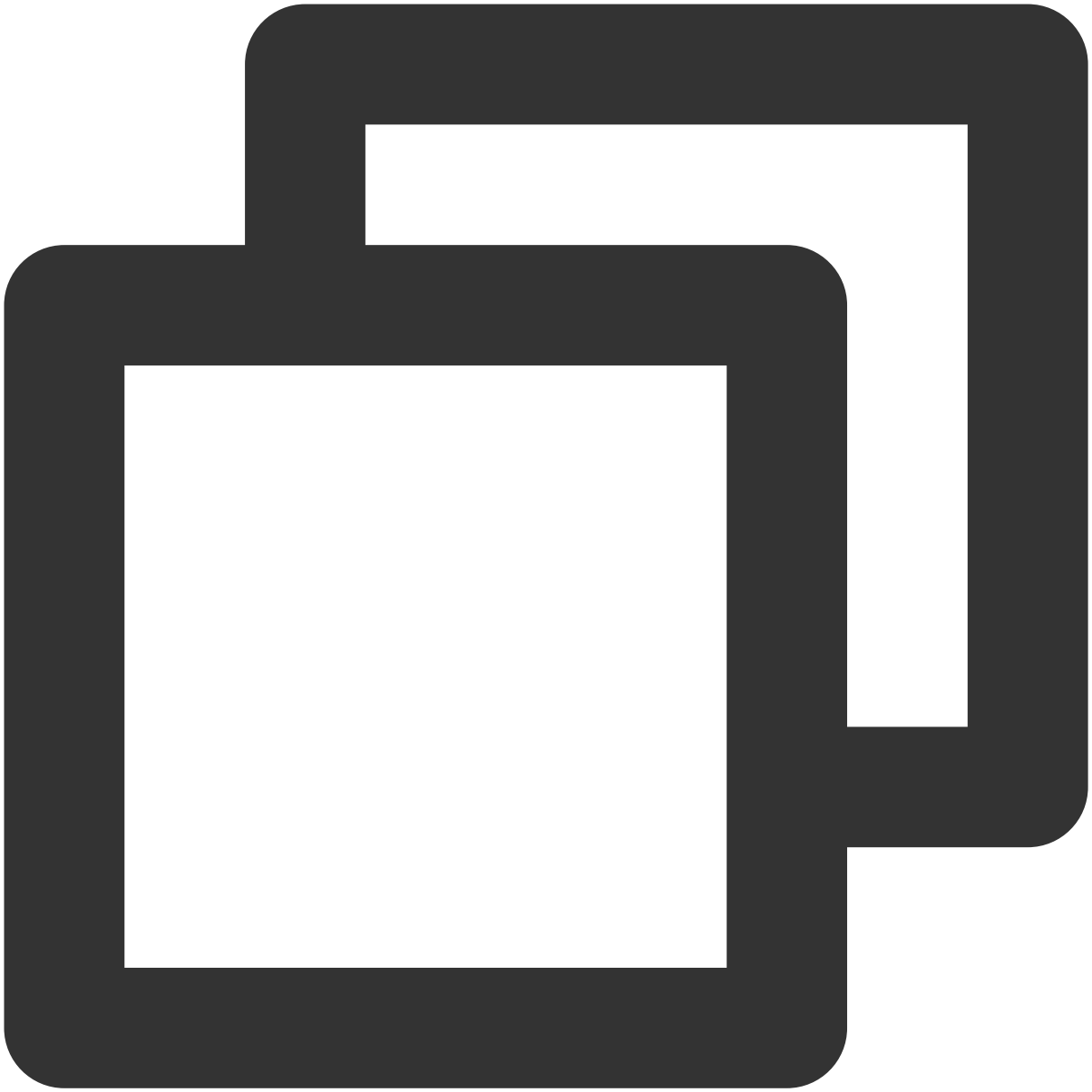
```
{
    "event_type": "异常进程",
    "pid": "5916",
    "path": "/root/2/ISHELL-v0.2/ishd"
}
```

字段说明

字段名称	说明
pid	进程 id
path	进程路径

恶意请求

示例



```
{
    "event_type": "恶意请求",
    "url": "massdns.ran6066.com",
    "count": "1"
}
```

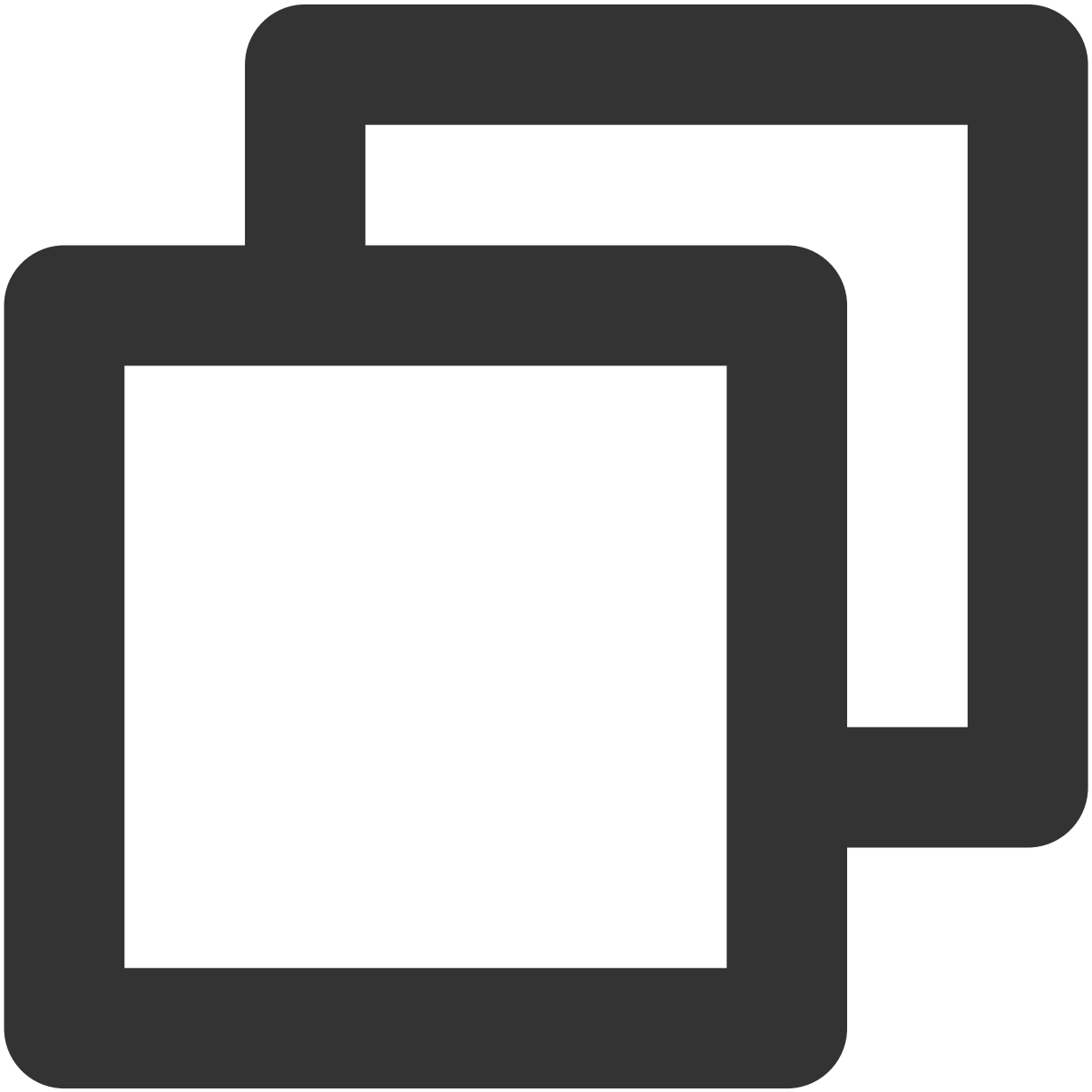
字段说明

字段名称	说明

url	恶意域名
count	请求次数

高危命令

示例



```
{
```

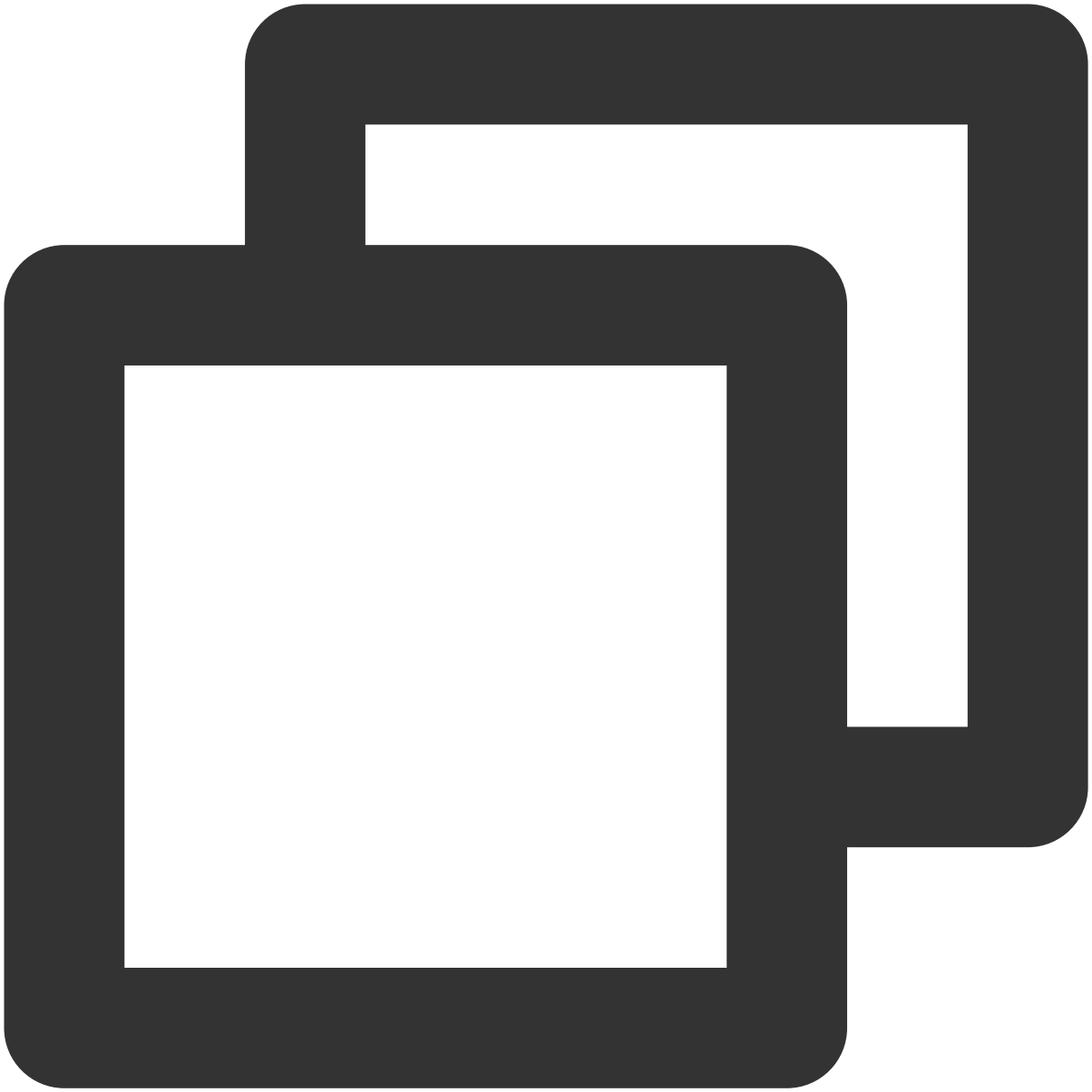
```
    "event_type": "高危命令",
    "cmd": "iptables-restore -w 5 --noflush",
    "level": "高危",
    "status": "待处理"
}
```

字段说明

字段名称	说明
cmd	命令内容
level	威胁等级
status	处理状态

本地提权

示例



```
{
    "event_type": "本地提权",
    "user": "0",
    "process": "privilege"
}
```

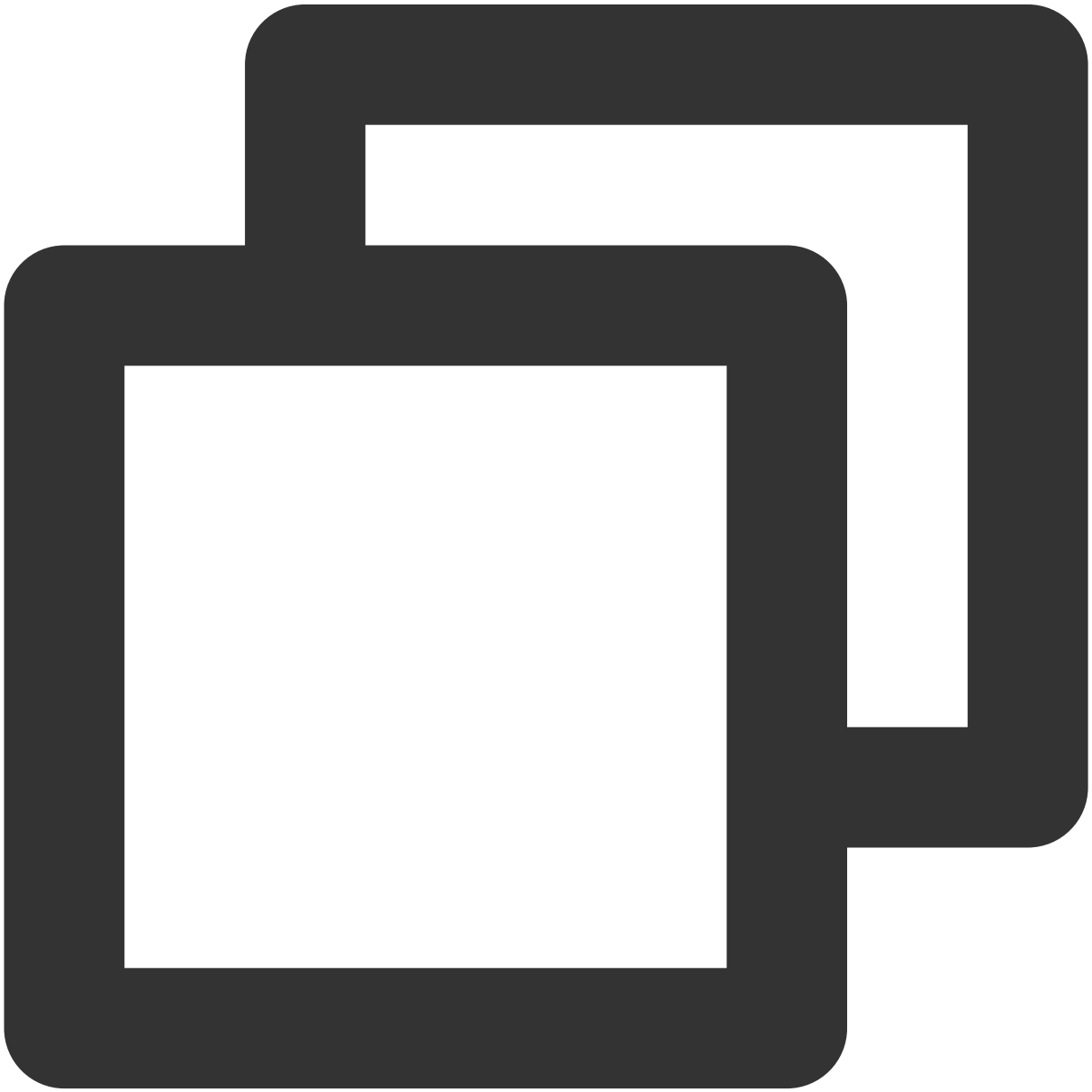
字段说明

字段名称	说明

user	提权用户
process	提权进程

反弹 Shell

示例



```
{
```

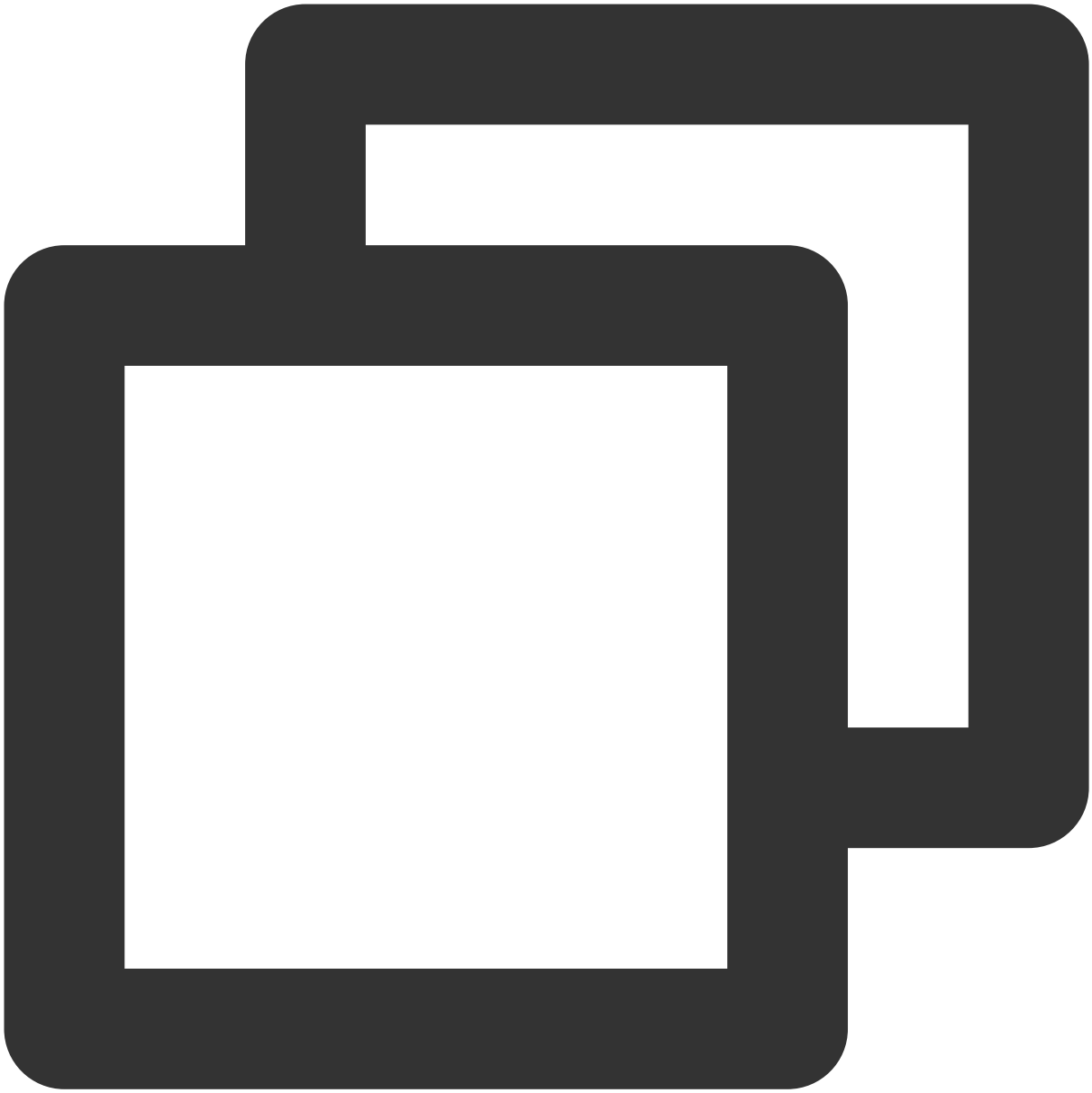
```
    "event_type": "反弹Shell",
    "process": "mass_0",
    "dst_ip": "125.x.x.220",
    "dst_port": "8888"
}
```

字段说明

字段名称	说明
process	进程名称
dst_ip	目标主机
dst_port	目标端口

java 内存马

示例



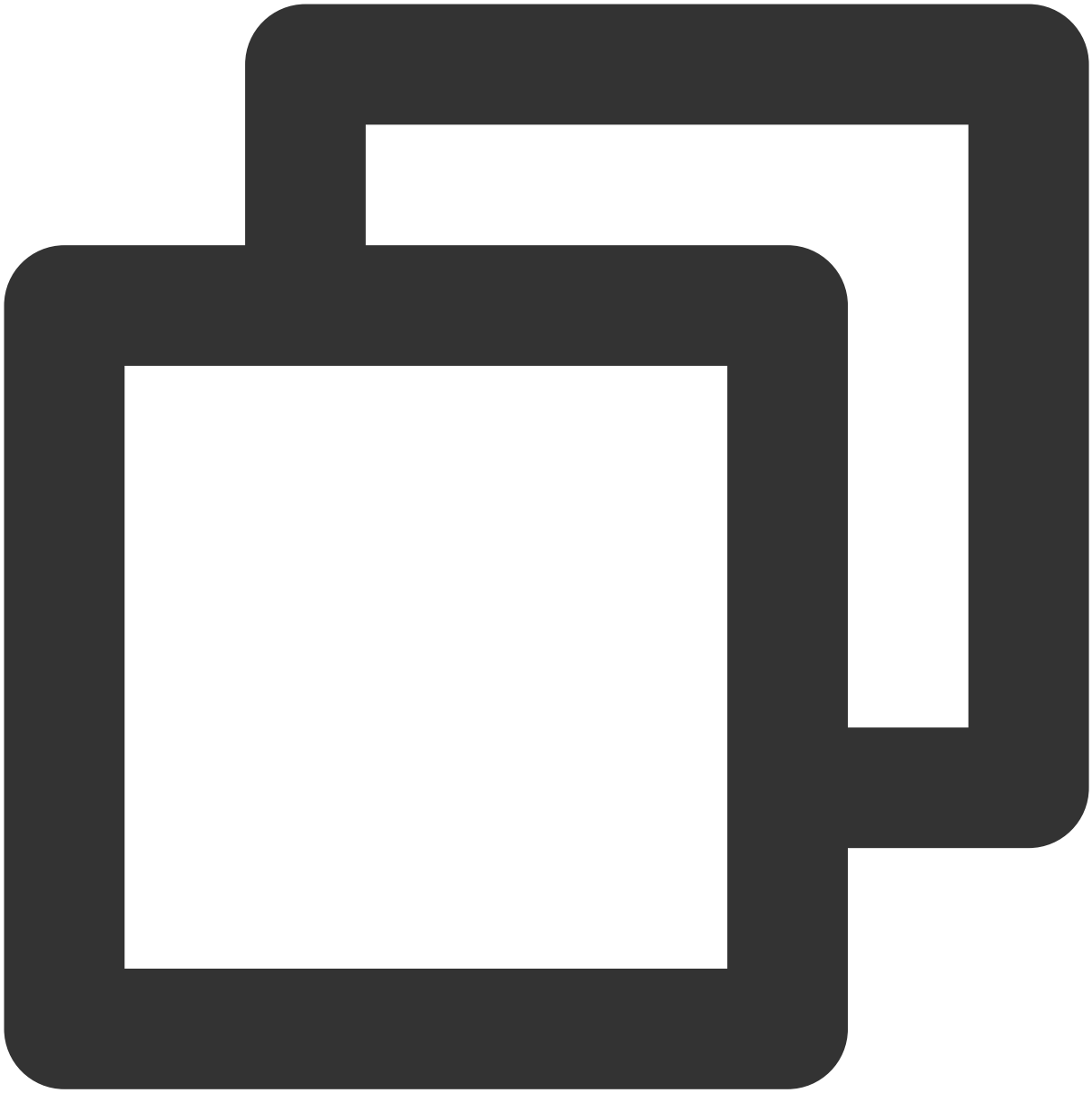
```
{
    "event_type": "java内存马",
    "type": "Java内存马-Servlet",
    "pid": "3333",
    "argv": "masstest",
    "class_name": "massTest"
}
```

字段说明

字段名称	说明
type	内存马类型
pid	进程 id
argv	进程参数
class_name	内存马 class 名称

核心文件监控

示例



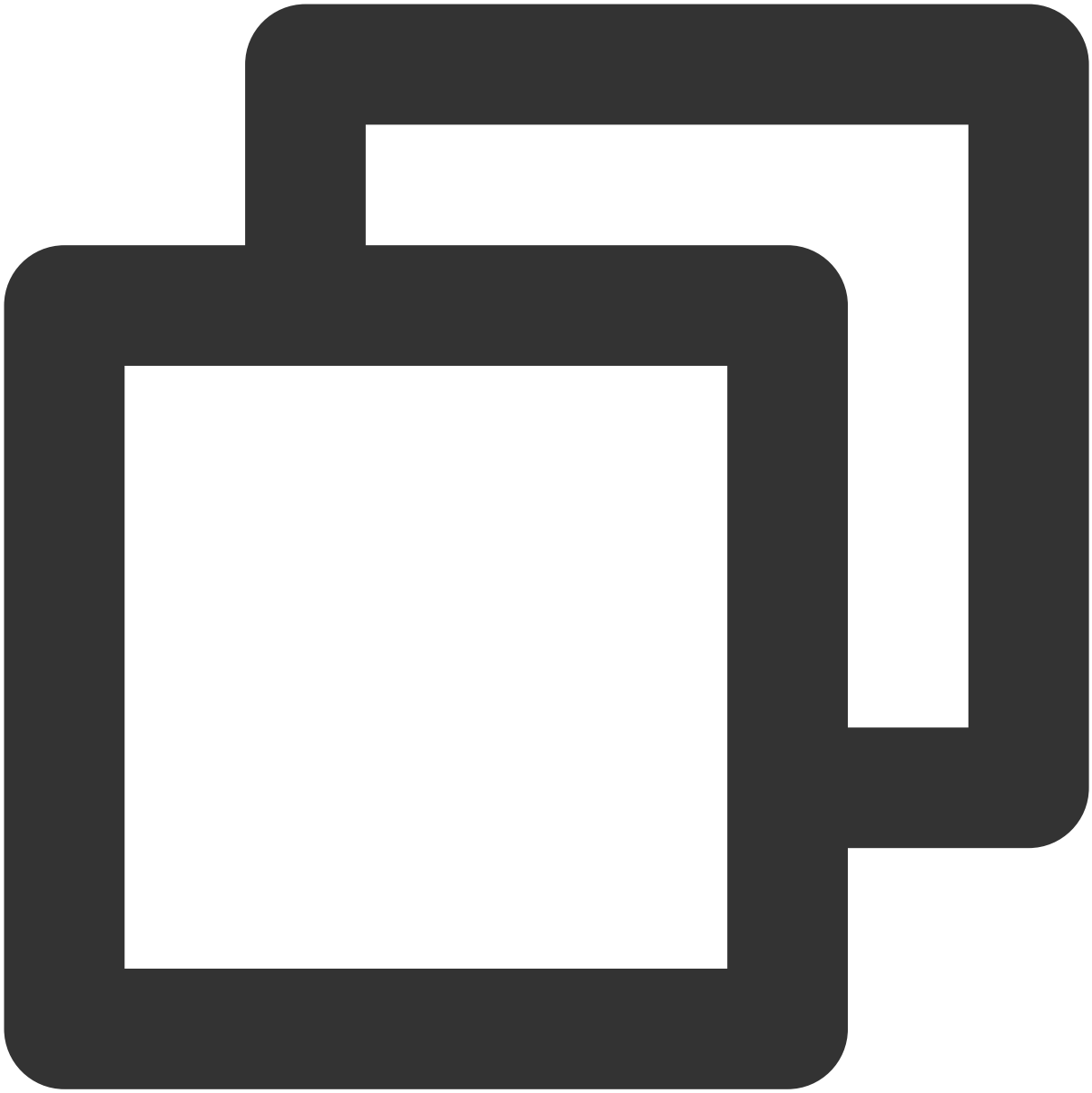
```
{
    "event_type": "核心文件",
    "rule_name": "adwqdadwqd",
    "exe_path": "/usr/bin/systemd-tmpfiles",
    "file_path": "/home",
    "count": "1",
    "level": "高危"
}
```

字段说明

字段名称	说明
rule_name	命中规则名称
exe_path	进程路径
file_path	文件路径
count	事件数量
level	威胁等级

网络攻击

示例



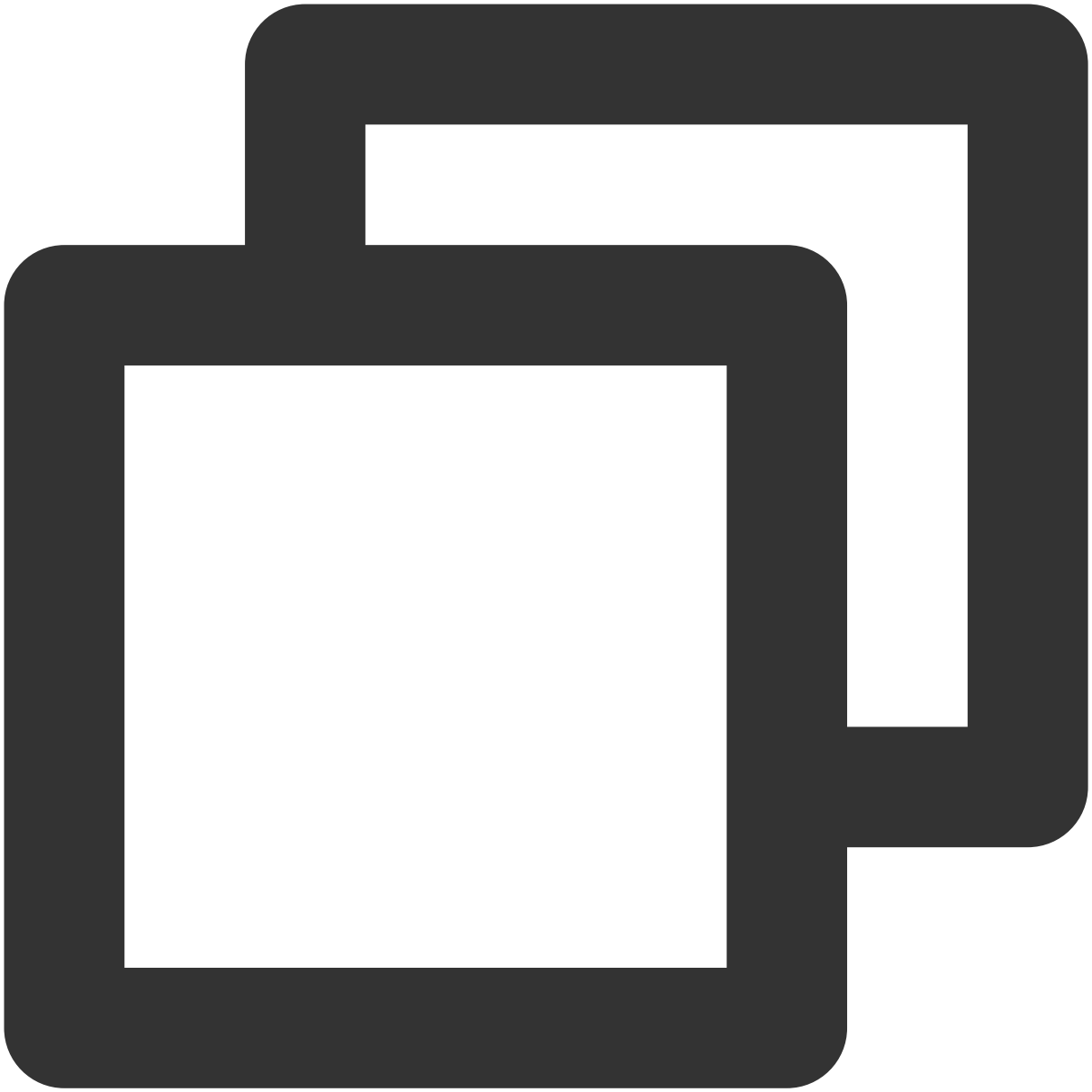
```
{
    "event_type": "网络攻击",
    "src_ip": "129.x.x.166",
    "city": "江苏省-南京市",
    "vul_name": "showdoc 文件上传漏洞",
    "dst_port": "80",
    "status": "尝试攻击"
}
```

字段说明

字段名称	说明
src_ip	来源 ip
city	来源城市
vul_name	漏洞名称
dst_port	目标端口
status	攻击状态

客户端离线

示例

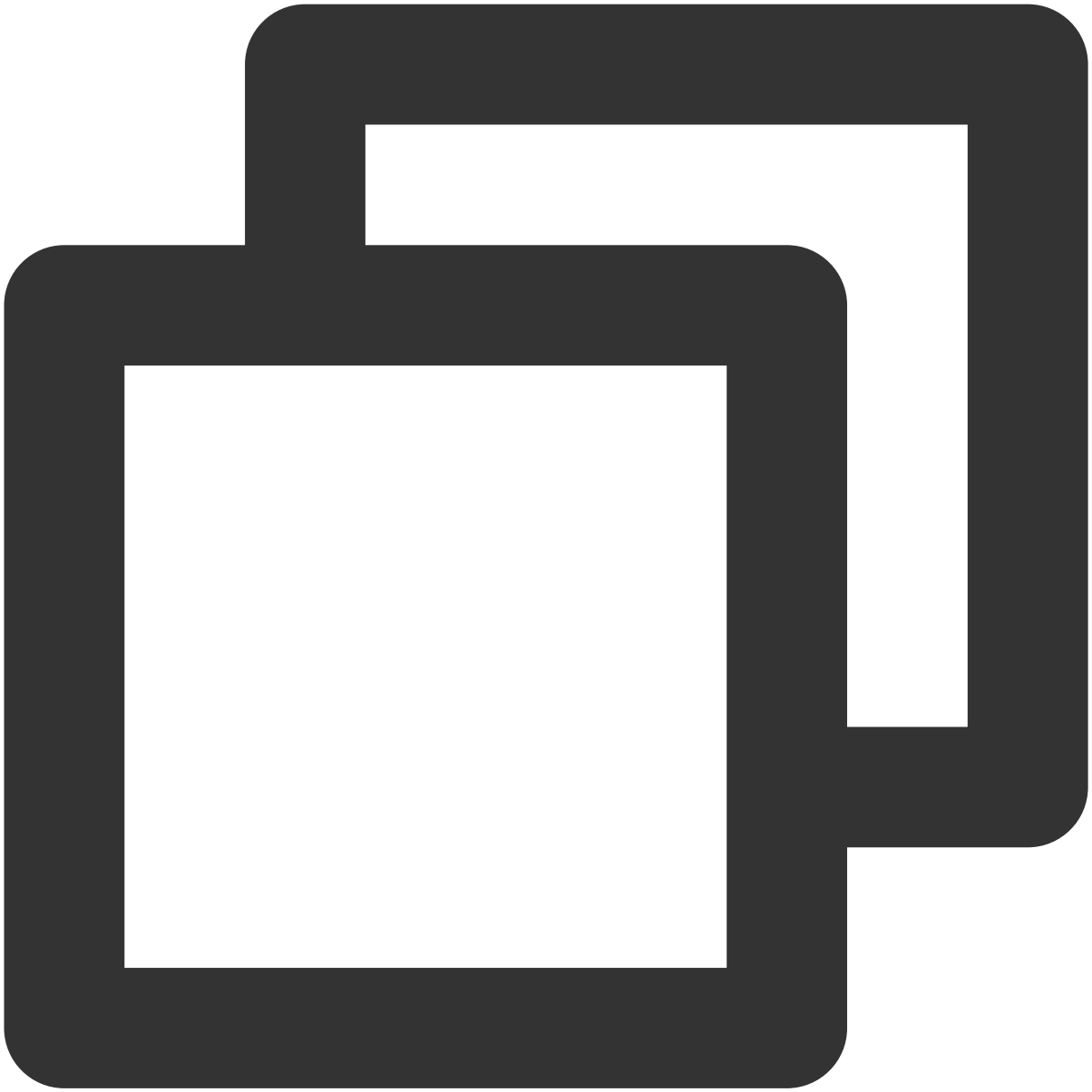


```
{
    "event_type": "客户端离线",
    "offline_hour": "1"
}
```

字段说明

字段名称	说明
offline_hour	客户端离线时长

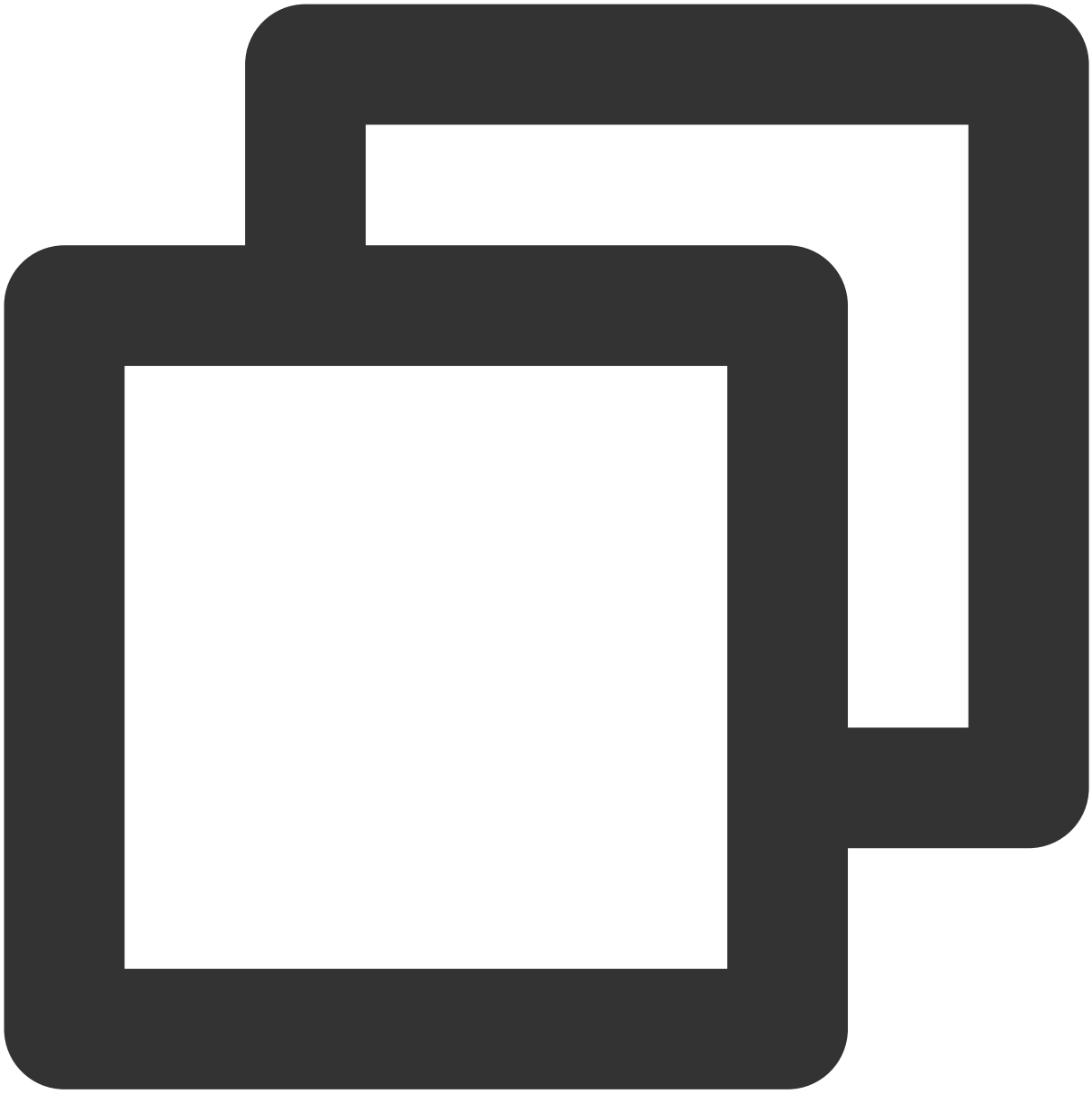
客户端卸载



```
{
    "event_type": "客户端卸载"
}
```

漏洞通知

示例



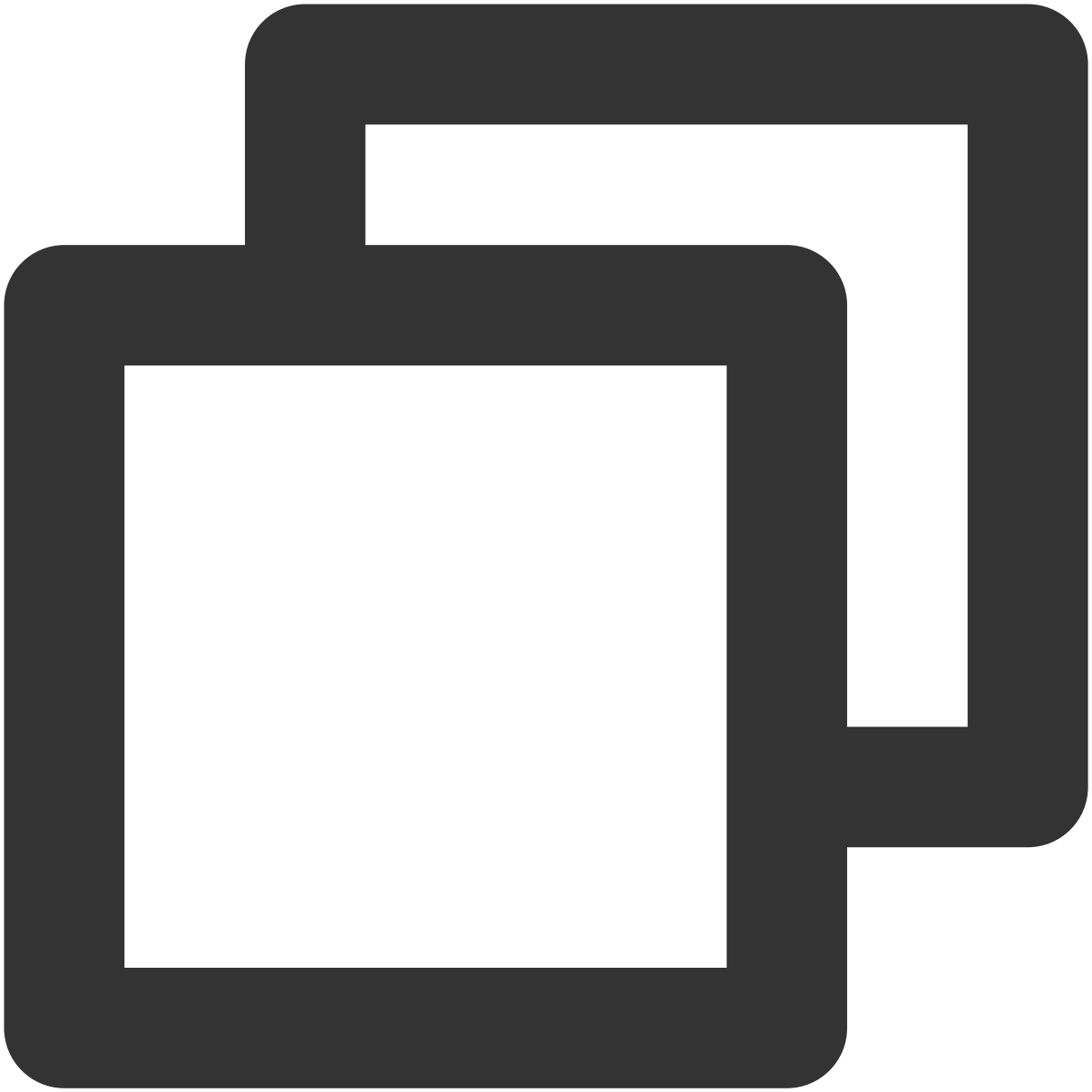
```
{
    "event_type": "漏洞",
    "category": "Linux软件漏洞",
    "vul_name": "libexpat 代码执行漏洞（CVE-2022-40674）",
    "level": "严重"
}
```

字段说明

字段名称	说明
category	漏洞分类
vul_name	漏洞名称
level	威胁等级

基线通知

示例



```
{
    "event_type": "基线",
    "category": "Linux系统弱口令检测",
    "rule_name": "Linux系统弱口令检测",
    "level": "高危"
}
```

字段说明

字段名称	说明

category	基线分类
rule_name	规则名称
level	威胁等级

勒索防御

示例

```
{
    "event_type": "勒索防御",
    "file_path": "/usr/bin/vi"
}
```

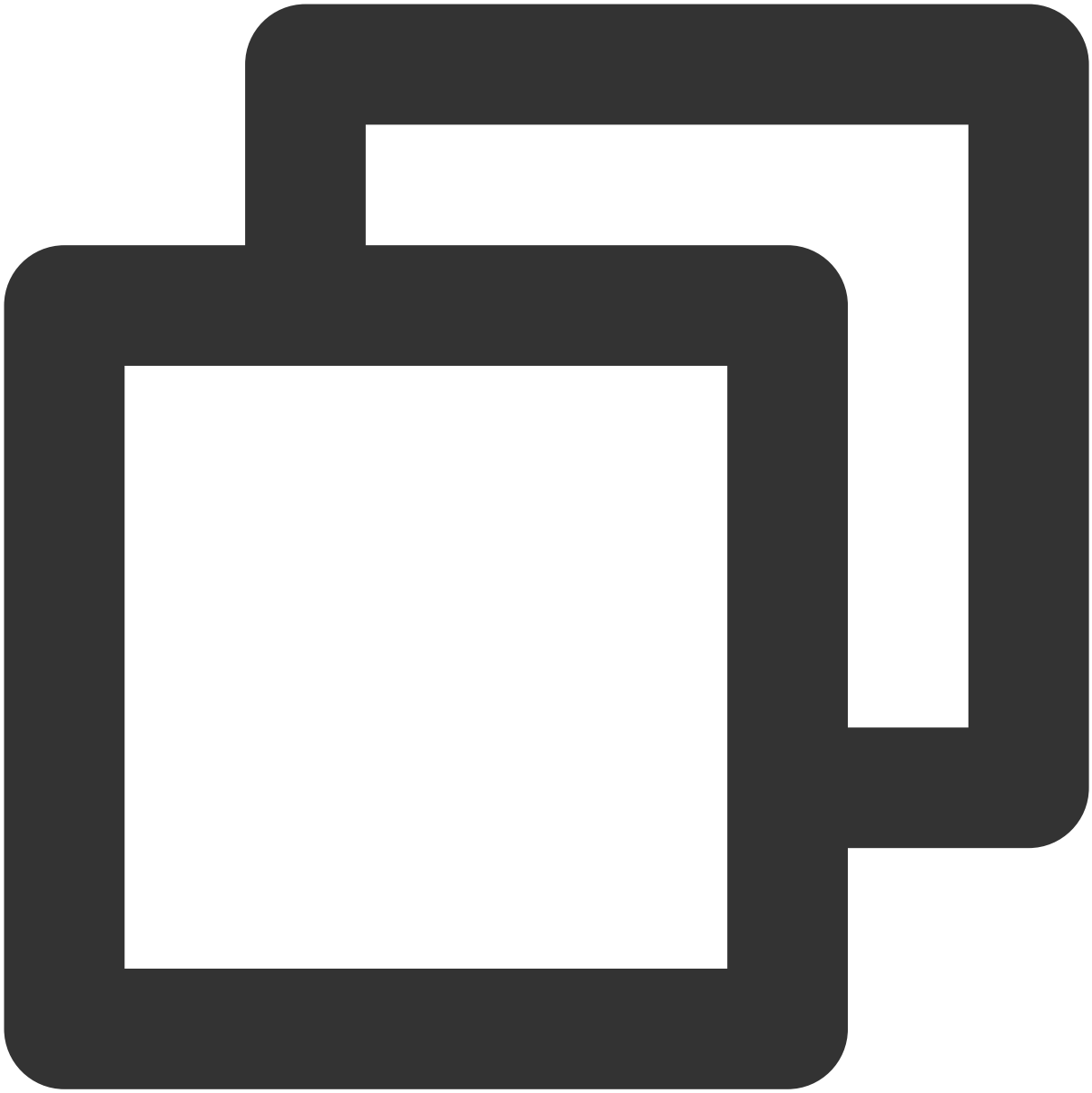
字段说明

字段名称	说明
file_path	文件目录

网页防篡改

篡改成功

示例



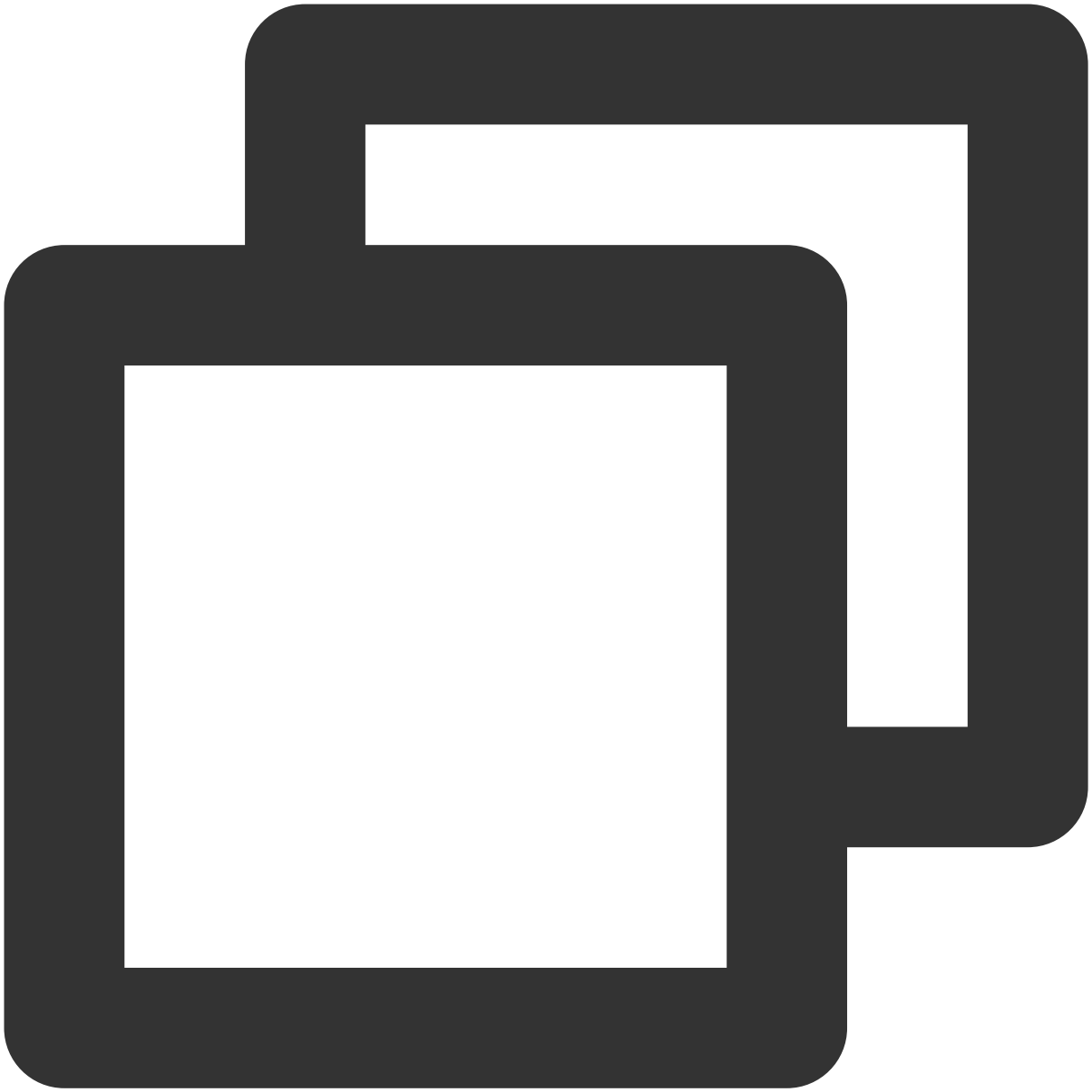
```
{
    "event_type": "网页防篡改（篡改成功）",
    "protect_name": "重要文件",
    "protect_path": "/tmp",
    "recover_type": "新增文件",
    "recovered_status": "未恢复",
}
```

字段说明

字段名称	说明
protect_name	防护名称
protect_path	防护目录
recover_type	事件类型
recovered_status	事件状态

恢复失败

示例



```
{
    "event_type": "网页防篡改（恢复失败）",
    "protect_name": "重要文件",
    "protect_path": "/tmp",
    "exception": "客户端离线"
}
```

字段说明

字段名称	说明

protect_name	防护名称
protect_path	防护目录
exception	失败原因

版权所有：腾讯云计算（北京）有限责任公司

日志字段数据解析

最近更新时间：2024-08-16 17:39:58

全局规范

日志内容信息采用 JSON 格式。
日志字符编码统一为 utf-8 格式。
日志包含公共字段和各类型独有字段，详见字段说明。
日志目前分为事件日志、资产日志、客户端日志三种类型。

日志类型

日志类型由公共字段 cls_event_type 确定，目前包含日志类型值说明如下：

事件日志

cls_event_type	日志类型值
malware	文件查杀
risk_process	异常进程
hostlogin	异常登录
bruteattack	密码破解
risk_dns	恶意请求
bash	高危命令
privilege_escalation	本地提权
reverse_shell	反弹 Shell
emergency_vul	应急漏洞
linux_app_vul	Linux 系统漏洞
windows_sys_vul	Windows 系统漏洞
Web-CMS_vul	Web-CMS 漏洞

版权所有：腾讯云计算（北京）有限责任公司

application_vul	应用漏洞
baseline	基线
attack_logs	网络攻击
java_shell	Java 内存马
file_tamper	核心文件监控
tamper_protect_logs	网页防篡改事件
tamper_protect_exceptions	网页防篡改异常
agent_uninstall	客户端卸载
agent_offline	客户端离线

资产日志

cls_event_type	日志类型值
machines	主机列表
asset_system	资源监控
asset_account	账号
asset_netstat	端口
asset_process	进程
asset_app	软件应用
asset_database	数据库
asset_web_app	Web 应用
asset_web_service	Web 服务
asset_web_frame	Web 框架
asset_web_location	Web 站点
asset_jar	jar 包
asset_init_service	启动服务
asset_scheduled_task	计划任务

版权所有：腾讯云计算（北京）有限责任公司

asset_env	环境变量
asset_core_module	内核模块
asset_package	系统安装包

客户端上报日志

cls_event_type	日志类型值
client_log	主机原始日志
dns_log	DNS 日志
process_snapshot	进程快照日志
net_log	网络五元组日志
file_log	文件监控日志
login_log	登录流水日志

事件日志字段说明

公共字段说明

字段	类型	说明
id	string	数据库记录 id
appid	string	用户 appid
create_time	string	事件创建时间
modify_time	string	事件修改时间
cls_event_type	string	事件类型
event_status	string	事件状态（create 创建、modify 修改、delete 删除）

文件查杀字段说明

字段	类型	说明
uuid	string	机器 uuid

hostip	string	主机 IP
file_path	string	文件路径
md5	string	文件 md5
filesize	string	文件大小
file_create_time	string	文件创建时间
file_modify_time	string	文件修改时间
file_access_time	string	文件访问时间
status	string	状态（待处理、已信任、已隔离、白文件、文件已删除、隔离中、恢复中、事件记录已删除）
virus_name	string	病毒名
bwtype	string	样本属性（10：白；20~29：黑）
path_md5	string	文件路径 md5

异常进程字段说明

字段	类型	说明
uuid	string	机器 uuid
hostip	string	主机 IP
pid	int	进程 ID
exe_path	string	进程路径
exe_md5	string	进程 md5
exe_desc	string	进程详情
exe_argv	string	进程参数
exe_create_time	string	进程创建时间
exe_modify_time	string	进程修改时间
exe_access_time	string	进程访问时间
status	string	状态（待处理、已信任、已清理、已退出）

版权所有：腾讯云计算（北京）有限责任公司

start_time	string	进程启动时间
virus_name	string	病毒名
latest_scan_time	string	最近扫描时间
pstree	string	进程树详情，json 格式
risk_level	string	风险等级（提示、低、中、高、严重）
pay_version	string	机器版本（基础版、专业版、旗舰版、普惠版）
rss	int	进程内存
permission	string	进程权限

异常登录字段说明

字段	类型	说明
uuid	string	机器 uuid
hostip	string	主机 IP
username	string	登录用户名
count	string	登录次数 （1分钟聚合一次）
src_ip	string	登录来源 IP
dst_port	string	登录端口
src_machine_name	string	登录源机器名称
login_time	string	登录时间
status	string	状态（正常登录、异常登录、已加白、已删除、确认入侵登录、已处理、已忽略）
location	string	位置

密码破解字段说明

字段	类型	说明
uuid	string	机器 uuid
hostip	string	主机 IP

username	string	用户名
count	string	尝试次数
event_type	string	事件类型 （爆破失败、爆破成功、爆破不存在的账号）
src_ip	string	来源 IP
dst_port	string	来源端口
src_machine_name	string	来源机器名称
status	string	状态（待处理、已忽略 、误报、已删除、命中白名单、已处理 、已加白名单）
location	string	位置
banned	string	阻断状态（未阻断、已阻断、未阻断（未开启阻断）、未阻断（非专业版）、未阻断（已加白名单）、未阻断（未绑定公网 IP）、阻断失败（接口异常）、阻断失败（内网不支持）、阻断失败（可用区不支持））

恶意请求字段说明

字段	类型	说明
uuid	string	机器 uuid
hostip	string	主机 IP
url	string	域名
pid	string	进程 ID
process_name	string	进程名称
cmd_line	string	命令行
status	string	状态（待处理、已删除、已加白、用户已取消信任、已处理、已忽略）
access_count	string	请求次数
query_time	string	首次请求时间
merge_time	string	最近请求时间

高危命令字段说明

字段	类型	说明
uuid	string	机器 uuid
hostip	string	主机 IP
user	string	执行的用户
platform	string	平台
exec_time	string	命令执行时间
bash_cmd	string	执行的命令
status	string	状态（待处理、危险命令、正常命令、已忽略、已删除）
rule_name	string	命中的规则名
rule_level	string	命令危险等级 （高危、中危、低危）

本地提权字段说明

字段	类型	说明
uuid	string	机器 uuid
hostip	string	主机 IP
process_name	string	进程名称
full_path	string	文件路径
pid	string	进程 ID
cmd_line	string	命令行
user_name	string	执行的用户
user_group	string	执行用户所属组
proc_file_privilege	string	进程文件权限信息
ppid	string	父进程 ID
parent_proc_name	string	父进程名称
parent_proc_user	string	执行父进程的用户
parent_proc_group	string	执行父进程用户所属组

版权所有：腾讯云计算（北京）有限责任公司

parent_proc_path	string	父进程路径
find_time	string	执行时间
proc_tree	string	进程树
sid	string	用户 sessionid，目前默认为0
uid	string	用户 ID
gid	string	用户组 ID
euid	string	有效用户 ID
egid	string	有效用户组 ID
status	string	状态（待处理、提权事件、白名单、已处理、已忽略、已删除）

反弹 Shell 字段说明

字段	类型	说明
uuid	string	机器 uuid
hostip	string	主机 IP
dst_ip	string	目的 IP
dst_port	string	目的端口
process_name	string	执行的进程
full_path	string	进程路径
pid	string	进程 ID
cmd_line	string	执行的命令
user_name	string	执行的用户
user_group	string	执行用户所属组
ppid	string	父进程 ID
parent_proc_name	string	父进程名称
parent_proc_user	string	执行父进程的用户

版权所有：腾讯云计算（北京）有限责任公司

parent_proc_group	string	执行父进程用户所属组
parent_proc_path	string	父进程路径
find_time	string	执行时间
proc_tree	string	进程树
status	string	状态（待处理、反弹 Shell 事件、白名单、已处理、已忽略、已删除）

漏洞字段说明

字段	类型	说明
uuid	string	机器 uuid
hostip	string	主机 IP
status	string	漏洞状态（待处理、已忽略、已修复、检测中、修复中、回滚中、修复失败、已失效、已下线）
vul_category	string	漏洞分类（Web 应用漏洞、系统组件漏洞、Linux 系统漏洞、Windows 系统漏洞）
descript	string	漏洞事件详情
path	string	漏洞文件路径
remark	string	漏洞备注
name	string	漏洞名称
fix	string	修复说明
cve_id	string	cve 编号
reference	string	参考说明
level	string	漏洞级别（低危、中危、高危、提示）
is_emergency	string	是否紧急

基线字段说明

字段	类型	说明
name	string	基线名称

uuid	string	机器 uuid
hostip	string	主机 IP
status	string	状态（未通过、已忽略、通过、已删除、检测中）
level	string	级别（低危、中危、高危、严重）
descript	string	描述
remark	string	备注
rule_id	string	所属基线分类 ID
category_name	string	基线分类名称
item_id	string	基线规则 ID
fix	string	修复建议

网络攻击字段说明

字段	类型	说明
uuid	string	机器 uuid
dst_port	int	目的端口
src_ip	string	来源 IP
type	string	类型，尝试攻击/攻击成功
status	string	事件状态，待处理/已处理/已加白名单/已忽略/已删除/已开启防御
count	int	事件合并计数次数
svc_ps	string	服务进程详情，json 格式
net_payload	string	攻击数据包（明文格式）
merge_time	string	事件合并时间（最近检测时间）
host_op_type	string	异常行为类型，无失陷行为/rce(命令执行)/dnslog/writefile
host_op_pstree	string	异常行为进程树，json 格式
host_op	string	异常行为内容
hostip	string	主机 IP

Java 内存马字段说明

字段	类型	说明
uuid	string	机器 uuid
type	string	木马类型（Filter 型、Listener 型、Servlet 型 、Interceptors 型、Agent 型、其他）
exe	string	Java 进程路径
argv	string	Java 进程命令行
pid	string	Java 进程 ID
class_name	string	内存马 class_name
loader_class_name	string	内存马 loader_class_name
super_class_name	string	内存马父类 super_class_name
interfaces	string	内存马 interfaces
recent_found_time	string	最近检出时间
status	string	状态（待处理、已加白、已删除、已忽略、已手动处理）
file_exist	string	文件是否存在（文件不存在、文件存在）
class_file	string	class 所在文件路径

核心文件监控字段说明

字段	类型	说明
uuid	string	机器 uuid
hostip	string	主机 IP
hostname	string	主机名称
process_exe	string	进程路径
process_argv	string	进程命令行参数
target	string	目标文件路径
status	string	状态（待处理、已加白、已删除 、已忽略、已手动处理）

版权所有：腾讯云计算（北京）有限责任公司

event_count	string	事件产生次数
rule_name	string	规则名称
event_detail	string	事件详情，json 格式
pstree	string	进程树
rule	string	规则组详情，json 格式
level	string	级别（无、高危、中危、低危）

网页防篡改事件字段说明

字段	类型	说明
uuid	string	机器 uuid
path	string	文件路径
recover_type	string	恢复类型（内容被修改恢复、权限被修改恢复、归属被修改恢复、被删除恢复、新增删除）
has_recovered	string	是否恢复（未恢复、已恢复）
recover_time	string	恢复时间
is_manual_recover	string	是否用户手动恢复（否、是）
is_deleted	string	是否已删除（未删除、已删除）
status	string	状态（待处理、确认恶意、确认误报）
file_type	string	文件类型（常规文件、目录、软链接）

网页防篡改异常字段说明

字段	类型	说明
quuid	string	机器 uuid
exception	string	异常类型（无异常、超出限制、Agent 离线、超时、磁盘不足、机器已销毁、备份时文件变化、备份时文件不存在、超出限制，监控路径不是一个目录、超出限制，文件类型不支持、超出限制，文件数量超出限制、超出限制，路径太长、超出限制，文件太大、超出限制，文件读取失败、超出限制，防护目录、子目录数量过多、其他）
exception_message	string	异常提示

版权所有：腾讯云计算（北京）有限责任公司

客户端卸载字段说明

字段	类型	说明
uuid	string	机器 uuid
pstree	string	进程树
uninstall_time	string	卸载时间

客户端离线字段说明

字段	类型	说明
uuid	string	机器 uuid
offline_time	string	机器离线时间

资产日志字段说明

公共字段说明

字段	类型	说明
id	string	数据库记录 ID
appid	string	用户 appid
host_name	string	主机名称
host_ip	string	主机内网 IP
wan_ip	string	主机外网 IP
instance_id	string	实例 ID
os_name	string	操作系统名称
os_type	string	操作系统类型（Unknow、CentOS、Debian、Gentoo、RedHat、Ubuntu、WindowsServer、TencentOS、CoreOS、FreeBSD、SUSE）
create_time	int	创建时间，时间戳格式

update_time	int	资产更新时间，时间戳格式
cls_event_type	string	事件类型
event_status	string	事件状态（create、modify、delete）

主机列表字段说明

字段	类型	说明
quuid	string	机器 quuid
machine_type	string	机器类型（CVM、LH、Other、ECM）
region	string	地域
project_id	int	实例所属项目 ID
instance_id	string	实例 ID
instance_state	string	实例状态（PENDING、LAUNCH_FAILED、RUNNING、STOPPED、STARTING、STOPPING、REBOOTING、SHUTDOWN、TERMINATING、TERMINATED）
restrict_state	string	业务状态（NORMAL、EXPIRED、PROTECTIVELY_ISOLATED、TERMINATED_PRO_VERSION）
instance_name	string	实例名称
private_ip_addresses	string	实例内网地址
public_ip_addresses	string	实例外网地址
ipv6_addresses	string	实例 IPv6 地址
vpc_id	string	vpc id
os_name	string	操作系统名称
os_type	string	操作系统类型（Unknow、CentOS、Debian、Gentoo、RedHat、Ubuntu、WindowsServer、TencentOS、CoreOS、FreeBSD、SUSE）
installed_cwp	int	是否安装主机安全客户端（0：未安装、1：已安装）
latest_sync_time	string	最近同步时间

资源监控字段说明

字段	类型	说明
core_version	string	内核版本
boot_time	int	系统启动时间，unix 时间戳
cpu_info	string	CPU 信息
cpu_size	int	CPU 数量
cpu_load	float	CPU 使用率
memory_size	int	内存数量：单位 MB
memory_load	float	内存使用率
disk_size	int	硬盘数量：单位 MB
disk_load	float	硬盘使用率

账号字段说明

字段	类型	说明
group_name	string	账号 GroupName
status	string	账号状态（禁用、启用）
is_root	string	是否有 root 权限
name	string	账号名称
type	string	账号类型（访客用户、标准用户、管理员用户）
home_path	string	Home 目录
shell	string	Shell 路径
password_change_time	string	密码修改时间
password_due_days	int	密码多少天后到期，-1为永不过期
password_lock_days	int	密码锁定时间，单位天，-1为无限
password_warn_days	int	密码过期提醒，单位天
password_change_type	string	密码修改设置（不可修改、可修改）
password_status	string	密码状态（正常、即将过期、已过期、已锁定）

版权所有：腾讯云计算（北京）有限责任公司

login_type	string	登录方式（不可登录、只允许 key 登录、只允许密码登录、允许 key 和密码）
last_login_time	int	上次登录时间
last_login_terminal	string	最近登录终端
last_login_ip	string	最近登录 IP
disable_time	string	账号到期时间

端口字段说明

字段	类型	说明
name	string	进程名称
version	string	进程版本
path	string	进程路径
parent_process_name	string	父进程名称
pid	string	进程 ID
user	string	运行用户
group_name	string	所属用户组
start_time	int	启动时间，unix 时间戳
param	string	启动参数
tty	string	进程 TTY
port	string	端口
ppid	string	父进程 ID
proto	string	端口协议

软件应用字段说明

字段	类型	说明
name	string	应用名称

type	string	应用类型（运维工具、数据库、安全应用、可疑应用、系统架构、系统应用、WEB 运维、其他）
bin_path	string	二进制路径
config_path	string	配置文件路径
process_count	int	关联进程数
version	string	版本号

进程字段说明

字段	类型	说明
name	string	进程名称
group_name	string	进程用户组
desc	string	进程描述
path	string	进程路径
pid	string	进程 ID
ppid	string	父进程 ID
parent_process_name	string	父进程名称
user	string	运行用户
start_time	int	启动时间
param	string	启动参数
tty	string	进程 TTY
version	string	进程版本
status	string	进程状态（无、可执行、可中断、不可中断、暂停状态或跟踪状态、僵尸状态、将被销毁、空闲、等待分配内存）
package_name	string	软件包名

数据库字段说明

字段	类型	说明

版权所有：腾讯云计算（北京）有限责任公司

name	string	数据库名
version	string	版本
port	string	端口
proto	string	协议
user	string	运行用户
ip	string	绑定 IP
config_path	string	配置文件路径
log_path	string	日志文件路径
data_path	string	数据路径
permission	string	运行权限
error_log_path	string	错误日志路径
plugin_path	string	插件路径
bin_path	string	二进制路径
param	string	启动参数

Web 应用字段说明

字段	类型	说明
name	string	应用名
desc	string	应用描述
version	string	版本
root_path	string	根路径
service_type	string	服务类型
domain	string	站点域名
virtual_path	string	虚拟路径
plugin_count	int	插件数

版权所有：腾讯云计算（北京）有限责任公司

Web 服务字段说明

字段	类型	说明
name	string	框架名
version	string	版本
bin_path	string	二进制路径
service_type	string	服务类型
user	string	启动用户
install_path	string	安装路径
config_path	string	配置路径
process_count	int	关联进程数

Web 框架字段说明

字段	类型	说明
name	string	框架名
version	string	版本
lang	string	语言
service_type	string	服务类型
path	string	应用路径

Web 站点字段说明

字段	类型	说明
name	string	域名
port	string	站点端口
proto	string	站点协议
service_type	string	服务类型
path_count	int	站点路径数

版权所有：腾讯云计算（北京）有限责任公司

user	string	运行用户
ip	string	绑定 IP
command	string	启动命令

Jar 包字段说明

字段	类型	说明
name	string	名称
type	string	类型（应用程序、系统类库、Web 服务自带库、其他）
status	string	是否可执行
version	string	版本
path	string	路径

启动服务字段说明

字段	类型	说明
name	string	名称
type	string	类型
status	string	默认启用状态（启用、未启用）
user	string	启动用户
path	string	路径

计划任务字段说明

字段	类型	说明
status	string	默认启用状态（启用、未启用）
cycle	string	执行周期
command	string	执行命令或脚本
user	string	启动用户
config_path	string	配置文件路径

版权所有：腾讯云计算（北京）有限责任公司

os_info	string	操作系统

环境变量字段说明

字段	类型	说明
name	string	名称
type	string	类型（用户、系统）
user	string	启动用户
value	string	环境变量值

内核模块字段说明

字段	类型	说明
name	string	名称
desc	string	描述
path	string	路径
version	string	版本
size	int	大小

系统安装包字段说明

字段	类型	说明
name	string	安装包名
desc	string	描述
version	string	版本
install_time	int	安装时间，unix 时间戳
type	string	类型

客户端上报日志字段说明

原始日志字段说明

字段	类型	说明
appid	int	用户 appid
uuid	string	机器 uuid
path	string	日志文件路径
tag	string	标签(将来用户定义)
time	string	日志时间
log	string	日志内容

DNS 日志字段说明

字段	类型	说明
appid	int	用户 appid
quuid	string	机器 quuid
uuid	string	机器 uuid
recv_time	int	时间戳
domain	string	域名
hostip	string	主机 IP
platform	string	平台：Linux，Windows
pid	int	进程 ID
process_path	string	进程路径
cmdline	string	进程命令行参数
count	int	上报周期内访问次数

进程快照日志字段说明

字段	类型	字段描述
appid	string	账户 appid

quuid	string	主机 quuid（对应 cvm uuid）
uuid	string	主机 uuid
hostip	string	主机 ip（与后台连接 ip）
instance_id	string	实例 id
event_name	string	事件类型：process - 进程事件
pid	int	进程 ID
ppid	int	父进程 ID
sid	int	进程会话 ID（仅 Linux 支持）
uid	int	进程 uid（仅 Linux 支持）
gid	int	进程 gid（仅 Linux 支持）
euid	int	进程 euid（仅 Linux 支持）
egid	int	进程 egid（仅 Linux 支持）
report_type	int	上报类型：0-实时进程 1-进程快照
parent_proc_name	string	父进程名
process_name	string	进程名
process_path	string	进程路径
cmdline	string	进程命令行
user_name	string	进程启动用户
process_md5	string	进程 md5
platform	string	平台：Linux，Windows
time	int	事件采集时间戳
timestamp	string	事件入库时间日期
insert_time	int	事件入库时间戳

网络五元组日志字段说明

字段	类型	字段描述

appid	string	账户 appid
quuid	string	主机 quuid（对应 cvm uuid）
uuid	string	主机 uuid
hostip	string	主机 ip（与后台连接 ip）
instance_id	string	实例 id
event_name	string	事件类型：net - 网络五元组
pid	int	进程 pid
proc_path	string	进程路径
argv	string	进程执行参数
username	string	进程所属用户:用户组
src_ip	string	源 ip
src_port	int	源端口
dst_ip	string	目的 ip
dst_port	int	目的端口
first_time	int	上报周期内第一次触发时间
last_time	int	上报周期内最后一次触发时间
count	int	上报周期内触发次数
time	int	事件采集时间戳
timestamp	string	事件入库时间日期
insert_time	int	事件入库时间戳

文件监控日志字段说明

字段	类型	字段描述
appid	string	账户 appid
quuid	string	主机 quuid（对应 cvm uuid）
uuid	string	主机 uuid

hostip	string	主机 ip（与后台连接 ip）
instance_id	string	实例 id
event_name	string	事件类型：file - 文件操作事件
pid	int	进程 ID
ppid	int	父进程 ID
session_id	int	进程会话 ID（仅 Linux 支持）
uid	int	进程 uid（仅 Linux 支持）
gid	int	进程 gid（仅 Linux 支持）
file_path	string	操作文件路径
cwd	string	进程当前执行路径
proc_path	string	进程路径
argv	string	进程命令行
username	string	文件操作用户
parent_proc_name	string	父进程名
proc_name	string	进程名
proc_md5	string	进程 md5
proc_perm	string	进程文件执行权限
proc_mtime	int	进程文件 modify time
proc_ctime	int	进程文件 change time
proc_atime	int	进程文件 access time
operation	string	文件操作类型: write-写 rename-重命名
file_size	int	文件大小
file_mtime	int	操作文件 modify time
file_ctime	int	操作文件 change time
file_atime	int	操作文件 access time

版权所有：腾讯云计算（北京）有限责任公司

file_perm	string	操作文件权限
file_owner	string	操作文件用户归属
time	int	事件采集时间戳
timestamp	string	事件入库时间日期
insert_time	int	事件入库时间戳

登录流水日志字段说明

字段	类型	字段描述
appid	string	账户 appid
quuid	string	主机 quuid（对应 cvm uuid）
uuid	string	主机 uuid
hostip	string	主机 ip（与后台连接 ip）
instance_id	string	实例 id
event_name	string	事件类型：login - 登录事件
src_ip	string	登录源 ip
dst_port	int	登录目标端口
protocol	string	登录协议
count	int	登录次数
event_type	string	事件状态：success：登录成功 fail：登录失败
time	int	事件采集时间戳
insert_time	int	事件入库时间戳

版权所有：腾讯云计算（北京）有限责任公司

客户端安装指引

最近更新时间：2023-12-26 15:27:07

本文将为您介绍如何安装主机安全客户端。

限制说明

服务器须满足以下两个条件，才可正常安装和使用主机安全客户端。

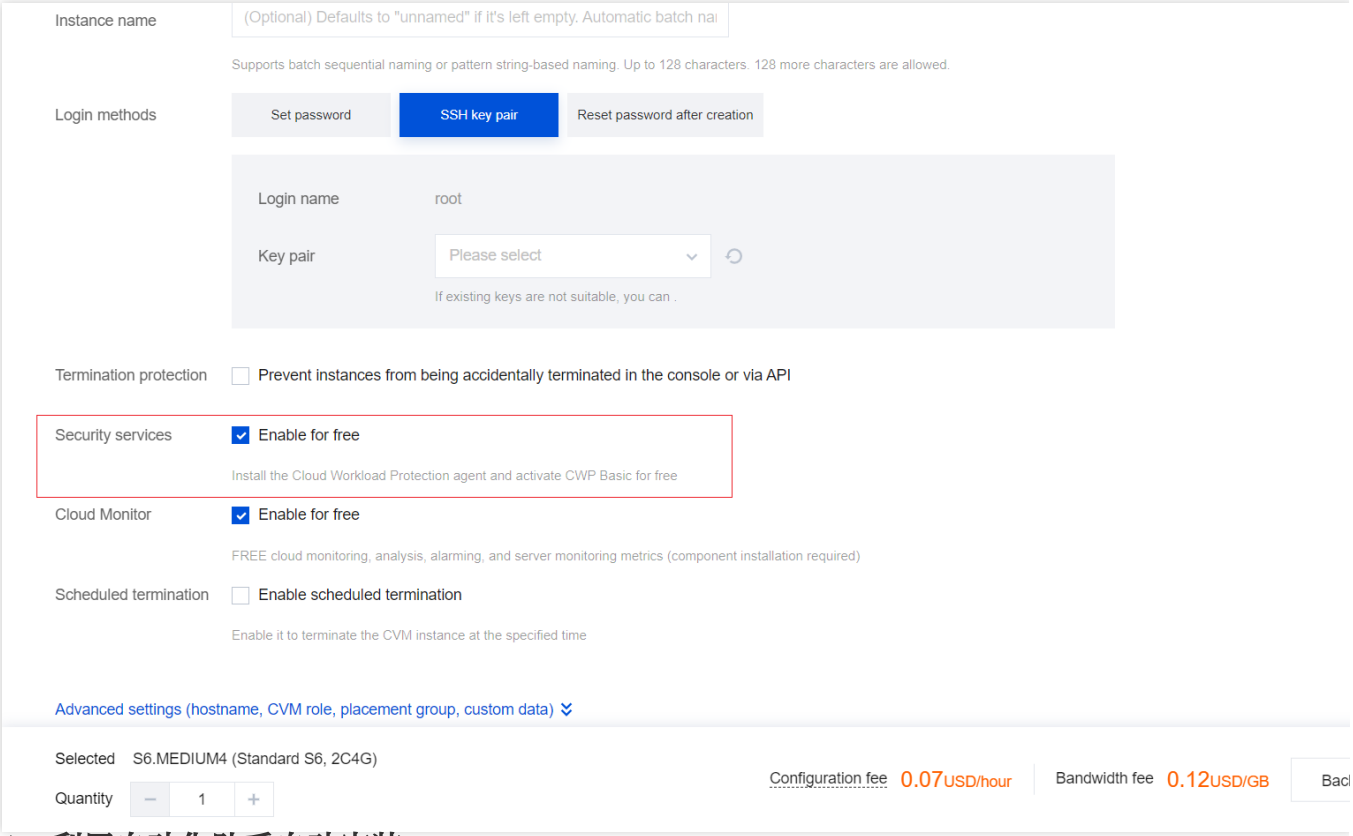
条件	说明
服务器类型	主机安全已支持混合云主机接入。 腾讯云：云服务器（CVM）、轻量应用服务器（Lighthouse）、边缘计算机器（ECM） 非腾讯云：第三方云厂商服务器、IDC服务器
服务器系统	Linux系统 CentOS: 6, 7, 8(64 bit) Ubuntu: 9.10 - 20.10(64 bit) Debian: 6, 7, 8, 9, 10, 11(64 bit) RHEL: 6, 7(64 bit) Windows系统 Windows server 2012, 2016, 2019 Windows server 2008 R2 Windows server 2003 (limited support)

安装方式

方式一：购买服务器时直接安装

适用于：云服务器（CVM）、轻量应用服务器（Lighthouse）、边缘计算机器（ECM）

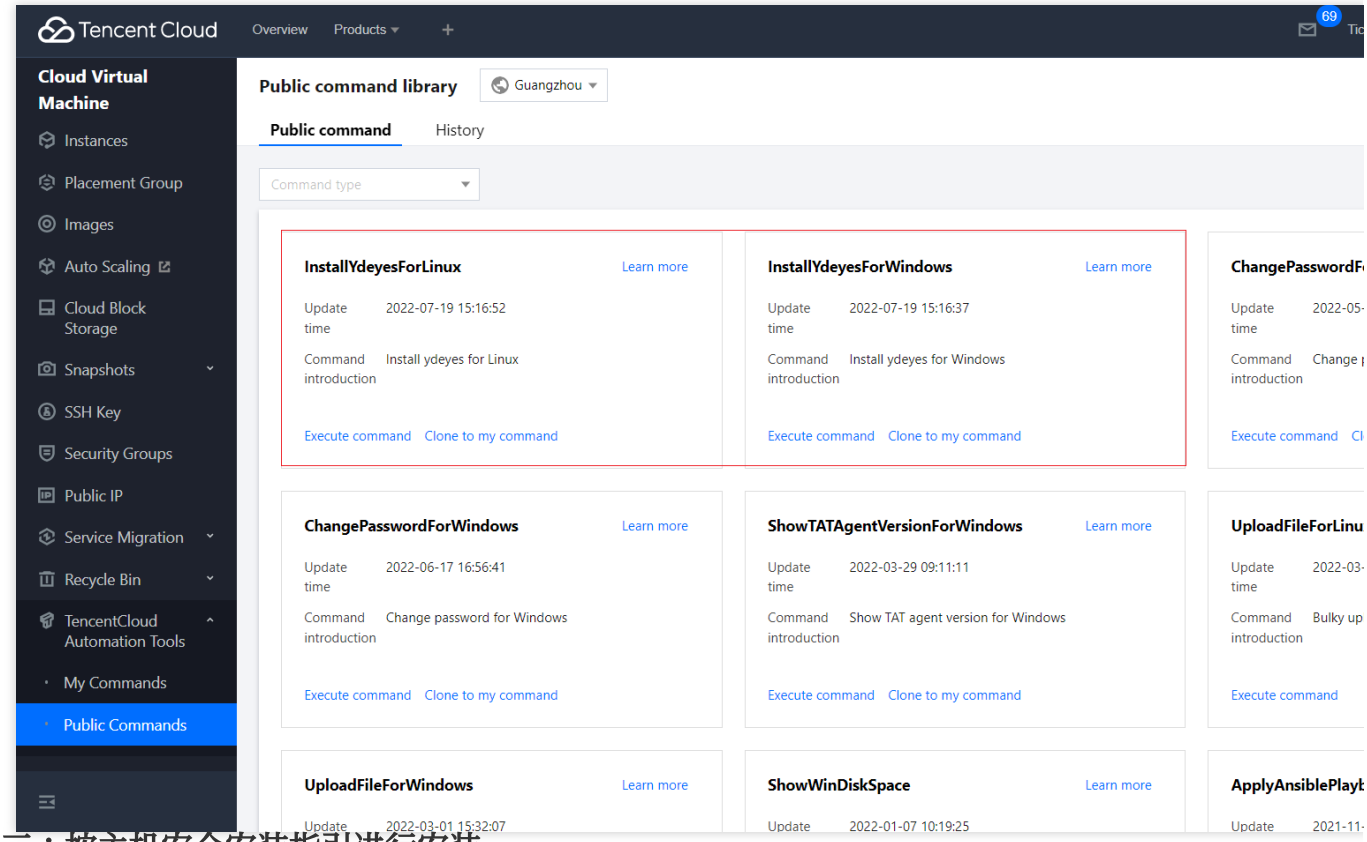
在选购上述服务器时，勾选**安全加固**项即自动安装主机安全客户端。



方式二：利用自动化助手自动安装

适用于：云服务器（CVM）、轻量应用服务器（Lighthouse）

在云服务器或轻量应用服务器的**自动化助手>公共命令库**中，找到主机安全客户端的安装命令，点击**执行命令**，选择服务器进行安装即可。



方式三：按主机安全安装指引进行安装

1. 登录主机安全控制台。
2. 单击左侧导航中的**主机列表**，点击**安装主机安全客户端**按钮，打开安装指引弹窗，根据服务器不同特性，选择合适的安装方式进行安装。

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

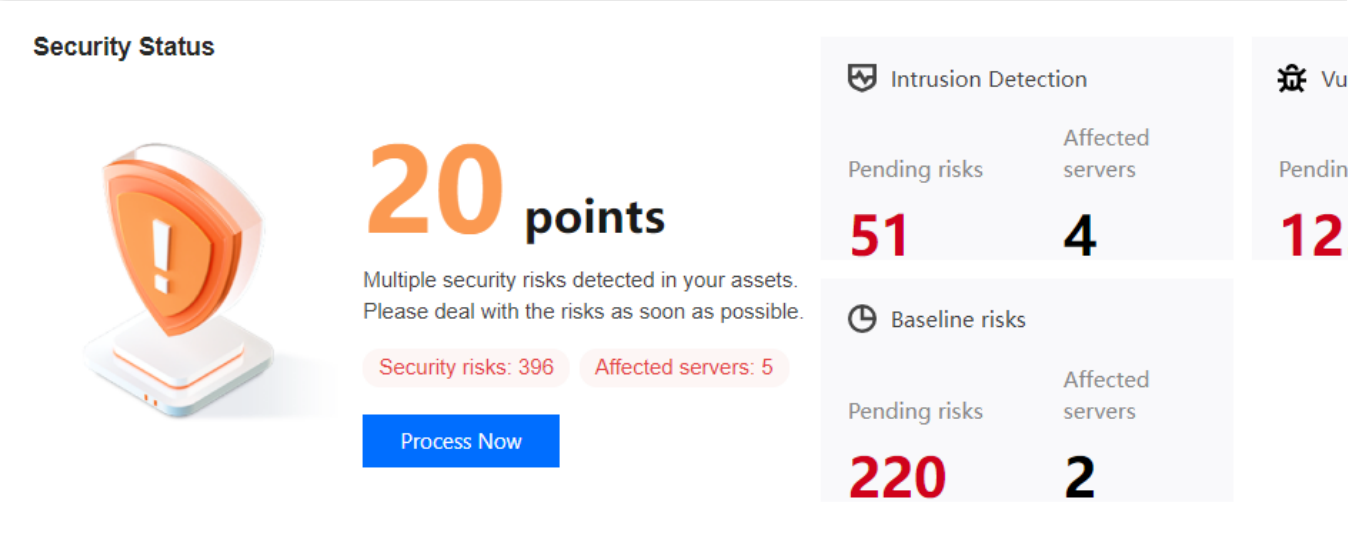
安全评分说明

最近更新时间：2023-12-26 15:27:17

本文将为您介绍安全评分细则。

安全评分

安全评分满分100，底分20。依据安全事件类型、安全事件数量、事件威胁等级进行扣分，以最终分数来划分安全等级。



扣分规则

等级	安全事件（按事件数计算）	扣分/个	叠加最大扣分
严重	木马文件、暴破成功、恶意请求	-40分	-50分
高危	严重漏洞、高危漏洞、严重基线、高危基线、异常登录（高危）、本地提权、反弹Shell	-10分	-20分
中危	中危漏洞、中危基线	-3分	-10分
低危	低危漏洞、低危基线	-2分	-5分
其他	基础版防护、未安装主机安全客户端	-1分	-5分

版权所有：腾讯云计算（北京）有限责任公司

安全等级

等级	体检评分	字体颜色	状态说明
优	90分 - 100分	绿色	资产安全状态较好，需继续保持，定期巡检。
中危	60分 - 89分	橙色	资产存在较多安全风险，建议您及时处理安全事件。
高危	20分 - 59分	红色	资产存在严重安全风险，请您尽快处理安全事件。

版权所有：腾讯云计算（北京）有限责任公司