安 全 智 能　　情 报 驱 动

微步在线

ThreatBook

TDP

TDPS

OneDNS 安全DNS服务

OneDNS DNS防火墙

TIP

微步情报API

MDR

S云沙箱

X社区

www.threatbook.cn

邮箱：　contactus@threatbook.cn

电话：　010-57017961

公司介绍

Company Introduction

微步在线
ThreatBook

微步在线成立于2015年7月，是专注威胁情报能力输出的安全企业，也是国内威胁情报领军品牌，提供专业的威胁检测/响应类产品与威胁情报订阅服务。公司主要成员来自于亚马逊、微软、BAT、美团等公司。微步在线从成立初始便专注于威胁情报领域，积累了深厚的威胁分析能力，已将情报数据能力和分析能力以专业检测设备/情报管理产品的方式赋能给客户，帮助客户落地威胁情报能力、建立全方位的威胁监控体系。微步在线在2017–2018年多次入选全球网络安全500强(CyberSecurity 500)，并在2017、2019年连续两次成为唯一入选Gartner《全球威胁情报市场指南》的中国公司。

产品一览：

2019.06 参与制定《信息安全技术网络安全等级保护评测要求》标准发布

2019.02 Gartner《2019全球威胁情报市场指南》唯一入选中国厂商

2018.11 2018中国国际进口博览会安保单位

2018.07 2018 IDC Innovator 入选企业

2018.06 2018–2019年度中国互联网网络安全威胁治理联盟威胁情报共享工作组组长

2018.06 2018人工智能安全解决方案提供商Top10（Enterprise Security Magazine）

2018.05 2018世界网络安全（Cyber Security Ventures）500强企业

2018.04 2018 Cyber Defense Magazine 威胁情报最佳创新奖

2018.01 2017中国金融科技创新创业大赛新锐企业Top30

2017.10 2017世界网络安全（Cyber Security Ventures）500强企业

2017.10 2017全球网络安全领导者Top50（Cyber Defense Magazine）

2017.07 Gartner《2017全球威胁情报市场指南》唯一入选中国厂商

2017.06 2017达沃斯论坛安保技术支撑单位

2016.07 中国网络安全产业联盟会员单位

2016.04 IDC中国首届“互联网+”产业创新企业100强

典型客户

现有数百家客户，行业覆盖能源、证券、银行、政府、互联网、制造业等。

威胁检测平台

Threat Detection Platform - TDP

微步在线威胁检测平台 (Threat Detection Platform, TDP) 基于对网络流量的实时分析检测，发现内网威胁事件，精准定位已失陷主机。提供丰富的威胁上下文和联动的终端处置工具，帮助安全团队实现内网威胁”检测–分析–处置”的闭环。

核心功能：

精准定位“失陷”主机

定位遭受恶意软件感染，已被黑客直接控制的内网主机。

全面绘制攻击者内网活动地图

围绕攻击链进行纵深防御，及时发现内网恶意样本下载和传播、主机受控反连、内网横向渗透、数据窃取、黑产牟利等一系列恶意活动，防止攻击者造成进一步破坏。

网络+端点的联动处置，消除威胁

安全团队可通过网络告警中丰富的威胁情报上下文辅助处置决策，并使用和平台联动的终端工具定位恶意进程，阻断网络访问，自动化清理流行恶意软件。

产品特性：

分钟级同步微步在线专业的威胁情报数据

清晰的威胁事件归类，并提供丰富的威胁事件上下文信息

以攻击链的角度绘制一个主机的行为地图

提供联动终端工具，定位恶意进程和阻断威胁

旁路流量接入，支持接入组织边界的南北向流量和内网东西向流量，配置简单，可在两小时内可实现上架部署

攻击感知平台

Threat Detection Platform for Servers - TDPS

攻击感知平台 (Threat Detection Platform for Servers, TDPS) 依托微步在线全球领先的高可信威胁情报数据，通过旁路监听出入站双向流量，实现攻击行为准确感知、攻击过程完整追溯、攻击团伙自动聚合，攻击成功精准告警，暴露资产全面梳理和数据泄露及时发现。

核心功能：

攻击行为准确感知

基于规则和机器算法模型，准确发现攻击杀伤链各阶段攻击威胁。

攻击过程完整追溯

通过关联分析及数据还原技术完整呈现攻击过程，并将告警数据以攻击杀伤链和时间顺序展示。

攻击团伙自动聚合

通过攻击路径、特征和技术细节，结合威胁情报，对攻击者进行黑客团伙聚类分析和背景信息的丰富。

攻击成功精准告警

利用攻击载荷与响应数据相互印证，对攻击成功与否进行精准判定。

暴露资产全面梳理

对暴露的域名、IP、端口、应用、接口进行全面发现和梳理。

数据泄露及时发现

针对撞库和敏感信息泄露等关键场景，提供完整感知、分析、处置方案。

产品特性：

聚焦真实威胁，提高安全运维效率

双向互联网流量交叉检测，实现完整溯源取证

快速梳理潜在攻击面，清晰呈现企业攻防边界

全球情报驱动，定位攻击者资产，实现精准报警

OneDNS
安全DNS服务

OneDNS Cloud

OneDNS Cloud是 SaaS化的 DNS解析和管控服务，实时拦截网络设备与恶意地址间的通信，避免后续攻击行动的发生。安全管理团队可以在 OneDNS Cloud控制台灵活配置策略，进行内容访问控制和上网行为管理。SaaS化产品形态适配各类IT架构，使企业总部、分支机构、漫游设备和云端应用获得统一的安全防护。

核心功能：

高速、稳定的DNS云解析服务

OneDNS Cloud 有遍布全国各地的递归加速节点，高速响应DNS解析请求，提升企业网络访问速度。

精准、全面的网络威胁防护

实时同步高价值威胁情报，精准阻断恶意软件通信行为，拦截钓鱼、欺诈、挂马网站浏览，避免进一步损失发生。

灵活、精细的网络访问行为管理

可根据企业安全策略，配置允许/禁止访问的内容分类，或需要拦截/放行的网络地址，策略粒度精细到接入点级别。

提供全局安全视野

OneDNS Cloud 后台提供多视角的数据报表，呈现企业内部安全威胁和不合规浏览情况。可选择在本地部署虚拟化探针，精准定位内部主机行为。

产品特性：

多 >>>> 适合多点办公场景，防护企业总部、分支机构和漫游网络设备

快 >>>> 无需安装硬件设备，十分钟即可完成企业全网部署

好 >>>> 精准拦截威胁，防止损失发生

省 >>>> 费用低，价格仅为同类硬件产品十分之一

OneDNS
DNS防火墙

OneDNS DNS Firewall

由微步在线与互联网域名系统北京市工程研究中心联合推出的国内首款专业的安全 DNS防火墙，集微步在线专业的威胁情报数据与威胁分析能力和互联网域名系统北京市工程研究中心高效稳定的域名递归解析解决方案为一体，为客户提供最轻量有效的安全防护产品，有效推动监管合规。

核心功能：

高效的DNS递归解析功能

利用互联网域名系统北京市工程研究中心新一代递归/缓存系统，按需对解析结果进行优选并应答，促进链路均衡、提高访问速度、兼顾dns服务的稳定性和安全性，让现有网络持续运营于最佳状态。

专业威胁情报防护

依托微步在线分钟级同步全球最新威胁情报，实时阻断恶意软件连接，防范安全威胁事件发生。

企业安全威胁全监控

精准定位“失陷”主机，提供可视化实时监控报表，展示详细威胁事件详情，指导安全团队进行威胁事件评估与响应。

产品特性：

基于微步在线完善的情报生产体系和覆盖全球高质量情报，提供精准的威胁阻断能力

灵活定制阻断机制，推动监管合规

多种递归结果选择策略，实现最优解析

多种联动机制，保证动态解析秒级调优

威胁情报管理平台

Threat Intelligence Platform - TIP

微步在线威胁情报管理平台 (Threat Intelligence Platform,TIP) 是国内首个威胁情报管理平台。主要用于帮助企业整合多源情报实现统一管理与共享；进行情报关联分析与深度挖掘；与现有安全系统集成提升威胁感知与响应能力。

核心功能：

多源情报整合与共享

整合微步机读情报、开源情报、自定义情报、第三方商业情报，标准化情报格式实现多源威胁情报融合，从多角度评估情报源质量，实现情报的统一管理，方便企业内部情报共享和使用。

本地化威胁情报API

基于微步在线业内领先的威胁情报数据，提供本地高质量情报查询，内置微步X社区查询接口，协助企业安全团队评估业务线威胁，进行有情报数据佐证的业务领域重点防护。

对接SIEM、SOC、态势感知平台

基于特有模块实现TIP与SIEM、SOC、态势感知平台对接，帮助企业安全团队实现数据关联分析、情报深度挖掘以及告警优先级排列，提高整个安全运营体系的情报检测与分析能力。

安全设备联动

通过自定义策略和插件与下游防火墙、WAF、IDS/IPS等安全设备联动联防，提升自动化响应能力和边界防护能力。

赋能情报生产能力

TIP已内置小型化的微步领先的威胁情报生产算法和流程，可根据用户环境原始数据附加微步基础数据全自动实时生产针对该用户的定向威胁情报。

产品特性：

覆盖全球高价值情报，确保优质情报产出

每秒处理情报查询数量达万级

支持SaaS和本地化部署，满足云战略需求和企业数据隐私

提供定制化联动插件，满足威胁实时阻断需求

微步情报 API

ThreatBook SaaS API

微步 API–灵活、轻量级的SaaS接口 (ThreatBook SaaS API) 安全设备、SIEM平台、大数据平台、态势感知中心，可选择直接调用，可按次数按类型进行收费，灵活接入全球最新威胁情报数据。

出站威胁情报 API

用于出站流量检测或者安全设备出站类告警的分析与筛选

包括远控或者恶意下载站的各类IP、域名和URL

提供丰富的上下文信息，例如关联的样本、注册人信息、是否APT、针对行业等

入站威胁情报 API

用于入站流量、web日志的分析，安全设备如WAF/IPS等告警的分析

包括全球42亿IP数据的画像信息，对每个IP提供了丰富的基础信息和威胁标签。

可提供围绕IP的丰富上下文

恶意样本分析 API

实时检测可疑文件，增强企业内部即时检测能力

通过反病毒引擎检出结果对文件进行预过滤，提升检测效率

敏感信息隔离保护，全面保护客户信息安全，无需担心内部文件外泄

检测及响应服务

Managed Detection and Response - MDR

基于微步在线的团队、技术与产品的支持，为企业客户提供高级应急响应服务和企业网络威胁的持续监控服务。由资深专家团队提供专业支持，对企业内、外部威胁线索及时告警、处置、响应、攻击者画像分析。

服务内容：

- 网络威胁检测、告警
- 安全事件响应、分析
- 攻击溯源、处置及修复建议
- 定期威胁发掘及安全巡检

微步云沙箱

ThreatBook Cloud Sandbox - S

微步云沙箱–情报驱动的恶意软件分析平台 (ThreatBook Cloud Sandbox)与传统的反恶意软件检测不同，微步云沙箱提供完整的多维检测服务，通过模拟文件执行环境来分析和收集文件的静态和动态行为数据，结合微步威胁情报云，分钟级发现未知威胁。

核心功能：

反病毒引擎检测

基于多款反病毒引擎检测，快速检测已知威胁。

精准定位恶意行为

利用虚拟化沙箱深度分析技术，实现恶意文件自动化、可定制化的行为分析，检测未知威胁。

高级情报判定系统

集成微步多个核心的高级情报分析系统，对文件运行过程中的网络、主机行为进行智能化的威胁判定，产出可直接用于失陷检测和应急分析的 IOC。

检测反沙箱恶意软件

支持识别和检测反沙箱恶意软件，防止恶意软件逃避虚拟机检查。

产品特性：

汇集 25 款源于不同国家的顶级反病毒引擎，帮助提高对已知威胁的检测能力

结合 700 多个高质量行为签名，提升识别和分类恶意软件的关键行为

持续通过遍布全球范围的蜜罐网络等多个渠道实时捕获全球上百万最新新增恶意样本，实现全球范围内威胁的全覆盖

提供定制化联动插件，满足威胁实时阻断需求

威胁情报社区

Threat Intelligence Analysis Community - X

微步在线X情报社区（Threat Intelligence Analysis Community,X）是以威胁数据查询、分析及情报数据共享为基础创建的，网络安全行业人员聚集的垂直类安全社区。旨在帮助社区的用户通过实时返回的分析检测结果及已分享的情报样本、黑客资源、攻击手法、线索、事件等，辅助安全人员快速定位及排除安全隐患，同时提供强大的在线API帮助企业设备对接，开启“上帝视角”。

核心功能：

开放的社区用户情报及可视化的数据展示

除公开的用户共享情报外，X情报社区运营着价值千万的情报奖励计划，重视优质情报的发掘，诚意回馈社区成员。

丰富的威胁数据查询与分析结果

深耕威胁数据精度与宽度，提供丰富数据源及可视化关联分析结果，辅助用户快速、及时排除网络安全隐患。

- **基础数据：8年Passive DNS信息、17年whois信息、每日百万新增域名**
- **威胁情报数据：40 W高可信IOC，全球42亿IP信誉与标签**
- **多引擎与沙箱：20+知名杀毒引擎，每日百万级新增样本、千万级新增URL**

强大的场景化API功能

为企业应用场景打造的Private API，可获取微步在线威胁分析平台的所有数据，支持与您的产品或服务做深度整合。辅助您现有的安全设备开启“上帝视角”。

- **入站IP信誉**
- **出站失陷检测**
- **文件分析与信誉检测**

安全智能 情报驱动

ThreatBook 微步在线

邮箱：contactus@threatbook.cn

电话：010-57017961

北京：北京市海淀区苏州街49-3盈智大厦3层

上海：上海市浦东新区盛荣路88弄盛大天地源创谷6号楼306室

深圳：深圳市南山区海岸大厦东座B区15层CR07