工信安全智库
洞察系列报告

报告编号：2021-dc-24

网络安全威胁情报行业发展报告
（2021 年）

国家工业信息安全发展研究中心
北京微步在线科技有限公司
2021 年 12 月

“工信安全智库”系列报告编委会

编写组

撰　稿： 陈羽凡 叶晓亮 李晓婷

审　稿： 孙倩文

序

国家工业信息安全发展研究中心经过 60 余年的发展与积淀，在智库研究方面形成了丰硕的积累。2018 年 9 月，中心推出“工信安全智库”品牌，立足深化供给侧结构性改革和加快建设创新型国家战略需求，围绕制造强国和网络强国建设任务，聚焦网络安全、数字经济、信息技术产业、战略前沿等重点领域，开展基础性、战略性、先导性智库研究，为工业和信息化部、中央网信办、国家发展改革委等提供智力支持。

“工信安全智库”自 2019 年开始陆续推出“研判”“洞察”“瞭望”“指数”“案例”“编译”等系列研究报告，围绕党和政府决策急需的相关重大课题和关键问题，开展形势研判、专题调研、国际跟踪、景气测度、案例分析、报告翻译等方面的持续研究，为主管部门预见走势、把握机遇、应对挑战、谋划战略提供参考。

本次推出的洞察报告《网络安全威胁情报行业发展报告（2021 年）报告》对网络安全威胁情报相关概念进行系统梳理，对国内外网络安全威胁情报发展情况进行总结分析，结合对我国网络安全威胁情报产业发展现状的调研，提出威胁情报服务能力评价框架，并就未来发展趋势及建议展开探讨，旨在为更好发挥威胁情报价值、促进威胁情报落地应用、推动威胁情报产业发展提供参考。

本报告得到北京微步在线科技有限公司的大力支持，产业调研还得到 360 政企安全集团、奇安信科技集团股份有限公司、绿盟科技集团股份有限公司、杭州安恒信息技术股份有限公司等企业的支

持，在此一并感谢。

由于成稿仓促，加之水平有限，报告中难免有疏漏和错误之处，恳请批评指正。

编写组

2021 年 12 月

摘　要

随着网络威胁的数量和复杂性不断增长，构建基于威胁情报的网络安全主动防御体系势在必行。2014 年起，威胁情报逐渐成为网络安全的热点领域之一，2018 年更是出现爆发性增长。各国政府、企业对威胁情报的重视程度不断提高，各类产业主体积极围绕威胁情报技术及商业模式开展探索，同时大力推动威胁情报标准化和共享机制的建立。威胁情报于 2015 年前后正式进入我国市场，威胁情报的价值在近几年的发展过程中逐渐被接受和认可，各行各业对威胁情报的需求也不断增长，据估计 2021 年我国威胁情报市场规模约在 10.69 亿元左右。

报告在产业深度调研的基础上提出威胁情报服务能力评价框架，为更加科学全面评价地评价供应商能力提供参考。该框架面向威胁情报供应商能力成熟度和市场发展潜力两方面目标，围绕情报数据、业务流程、产品服务、企业竞争力等四个基本维度，对供应商威胁情报服务能力的评价。针对典型网络安全威胁情报供应商的能力评价及优势分析随文附后。

为更好发挥威胁情报赋能作用，应进一步夯实威胁情报对网络安全发展的基础支撑作用，促进威胁情报开发利用以覆盖多元化情报需求，加快标准化建设以实现更大范围情报共享，以更加广阔的威胁情报视野驱动各类网络安全技术、服务、产业协同，实现推进网络安全产业高质量发展的目标。

目　录

随着网络环境日益复杂化，网络攻击行为趋于产业化，攻击手段也愈发多样化，根据经验构建防御策略、部署产品的传统方式在面对层出不穷的新型、持续性、高级威胁时，难以及时有效的检测、拦截、分析和响应。在此背景下，网络安全威胁情报应运而生。作为一种重要的网络安全基础知识，可支撑构建更加主动的网络安全防御模式，基于全方位的情报感知、多维度的融合分析，研判网络安全整体态势并合理预判威胁动向，实现动态精准的网络安全威胁应对。

一、威胁情报概述

情报(Intelligence)一词，源于军事领域，指“获得的他方有关情况以及对其分析研究的成果”，多带机密性质，目前在不同的领域内均有应用。以威胁情报为中心的信息安全保障框架对于生活和生产关键基础设施的稳定运行、军事作战指挥能力保障及国际社会的和平稳定具有重大意义，它受到了来自各国政府、学术界以及全球大型互联网企业的高度重视。

（一）威胁情报的定义

2013 年，Gartner 首次提出关于威胁情报的**定义**：威胁情报是关于现有或即将出现的针对资产有威胁的知识，包括场景、机制、指标、启示和可操作建议等，且这些知识可为主体提供威胁的应对策略。简单来讲，威胁情报就是通过各种来源获取环境所面临的威胁的相关知识，主要描述现存的、即将出现的针对资产的威胁或危险。Forrester 认为威胁情报是内部和外部威胁参与者动机、意图和能力的

详细信息。威胁情报包含这些攻击者的战术、技术手段和攻击过程的详细信息。2014 年，SANS 提出威胁情报是收集、评估和应用的关于安全威胁、恶意行为者、漏洞利用、恶意软件、漏洞和危害指标的数据集。总结来说，**威胁情报主要指**通过各种来源获取环境所面临的威胁的相关知识，来描述现存的、即将出现的针对资产的威胁或危险。高质量的威胁情报具有时效性、准确性、适用性、丰富性、可操作性等特点。

（二）威胁情报的分类

目前，可按照威胁情报的来源、内容、形式和应用价值四个不同维度对威胁情报进行分类。

1. 来源角度分类

根据情报产生的来源角度可分为内部情报、外部情报。内部情报是由组织内部产生的，其目的是“知己”，用于反映内部系统安全状态。外部情报是由组织外部输入的，其目的是“知彼”，用于反映外部网络空间安全状态。

2. 内容角度分类

从网络威胁情报内容属性来看，威胁情报可分为基础信息类、威胁类、资产类、事件类等。基础信息类包括 IP 基础情报、域名基础情报、URL 基础情报、邮箱基础情报等。威胁类情报包括攻击者、攻击模式、基础设施、漏洞、样本、恶意软件、威胁指示器等内容。资产类情报主要对网络空间中的 IP、域名、URL、邮箱等资产的安全性进行描述，包括安全状态、威胁状态、恶意历史、相关的样本、

事件等。事件类情报具体描述时间、参与方、损失类型、影响的资产、影响程度等。

3. 形式角度分类

可读性是从情报使用者和使用方法的角度进行划分的，通常分为“机读”情报和“人读”情报。机读情报(Machine Readable Threat Intelligence, MRTI)是可被计算机软硬件系统理解和使用的方式提供的情报，通常格式符合特定的规范标准，比如 OpenIOC 格式、STIX 格式的指示器等。人读情报以人可理解和使用的方式提供的情报。例如各种安全分析报告、漏洞详情、威胁通告等。

4. 价值角度分类

威胁情报价值，最重要的体现就是与行动/决策的相关程度。根据行动/决策的执行对象和应用维度，可以将其分为**战略级情报、运营级情报和战术级情报**三个层面。**战术级情报**是威胁情报最基础，也是应用最广的类型。战术执行层面的行动或决策需要的是与具体的资产、漏洞、威胁、风险、事件相关的可机读情报，大多直接作用于具体的检测与响应工作。**运营级情报**是指运营管理层面的行动或决策需要的基于一定情境和机制的具有较丰富上下文信息的情报，其侧重于根据分析结果掌握某类威胁、漏洞、资产或事件的情况，并制定针对性的整体防御、检测和响应策略。又可细分为基础情报、威胁对象情报、IOC 情报（Indicators of Compromise，攻击指示器）、事件情报等。**战略情报**是指战略、策略制定层面的行动或决策需要的经由综合性分析得出的，带有建议的战略级情报。战略级情报侧

重于对安全态势的整体性描述，并借助与之相关的战术级和运营级情报作为相关观点和建议的佐证，大多以报告、指南或框架文件等形式供高层管理人员和战略制定者阅读，以辅助其制定相应的企业战略和决策。

（三）威胁情报的作用

威胁情报既是知识，也是载体，既是输入，也是输出。作为新一代网络安全能力建设的核心，通过赋能各类网络设备、安全产品，实现全网安全检测、响应、分析能力的联动。

一是可用于安全模式突破和完善。基于威胁情报的防御思路是以威胁为中心的，因此，需要对关键设施面临的威胁做全面的了解，建立一种新型高效的安全防御体系。这样的安全防御体系往往需要安全人员对攻击战术、方法和行为模式等有深入的理解，全面了解潜在的安全风险，并做到有的放矢。威胁情报可提供最新的恶意威胁信息情报、漏洞信息情报、安全事件情报、安全资讯，攻击组织情报、攻击手法情报、最新前沿技术分析报告等，情报可与现有的防火墙、入侵检测、入侵防御、Web 应用防护防火墙（WAF）、终端安全设备、安全运营中心（SOC）、态势感知平台结合，更新规则库、矫正检测模型，可以预防和检测更多攻击，具有“看见威胁的能力”，发现最新威胁、隐藏的威胁、甚至未知威胁，并对其进行有效应急处置。

二是可用于应急检测和主动防御。在战术和战略层面威胁情报是对高级威胁进行防护的关键。随着黑客攻击的专业化和组织化，

要想更好的抵御黑客攻击（尤其是高级威胁），需要掌握攻击者的 TTP（战术、技术手段和过程）及攻击趋势，确定重点防御方向，制定合理的防御策略。只有走在攻击者前面，才能占据攻防先机。另一方面，各种安全控制措施通过共享可机读的威胁情报，及时触发相关的防护和告警规则。此外，通过企业内或行业间的高级威胁情报共享，可以做到一点发现、全面布防，实现更大范围的高级威胁防御生态。

三是可用于安全分析和事件响应。威胁情报成为提升整体网络安全防护效率的重要措施，采用多种技术手段，通过采集大规模、多渠道的碎片式攻击或异常数据，集中地进行深度融合、归并和分析，形成与网络安全防护有关的威胁信息线索，并在此基础上进行主动、协同式的网络安全威胁预警、检测和响应，有效降低平均威胁检测时间（MTTD）、平均威胁响应时间（MTTR），缩短自由攻击时间，降低网络安全威胁的防护成本，提升整体的网络安全防护效率。

二、国外威胁情报发展现状分析

2014 年起，威胁情报逐渐成为网络安全的热点领域之一。目前各国政府部门、网络安全企业愈加重视威胁情报的发展，各行各业对威胁情报的需求也在不断增长。据全球企业咨询公司 Frost & Sullivan 预测，到 2022 年仅威胁情报平台的全球市场规模相比较于 2019 年将增长约 77%。

（一）国家和战略层面重视程度不断提高

近几年，在威胁情报全球市场中，以美国为代表的北美国家持续占据主导地位，对全球威胁情报技术及产品的发展发挥着不可忽视的影响。

美国是全球最早开展威胁情报工作的国家。2003 年发布《网络空间安全国家战略》提出建立信息共享与分析中心，以确保能够接收实时的网络威胁和漏洞数据。2010 年，发布《国土安全网络和物理基础设施保护法案》进一步突出威胁情报的重要性。2015 年 2 月，建成全国性的网络威胁情报中枢——网络威胁与情报整合中心，以对网络攻击相关情报进行综合分析，并向国内机构提供分析结果，提升网络攻击的防范和处置能力。另外，美国依托其不断发展完善的威胁情报共享技术，通过构建“网络天气地图”（Cyber Weather Map）威胁情报管理体系，将国家网络安全保护系统与互联网中相关的探测器关联，收集相关的威胁情报信息，利用大数据分析技术，并结合外部的其他威胁情报来源，并形成针对性的安全策略。

欧盟网络与信息安全局于 2018 年 3 月发布《探索威胁情报平台机遇与挑战》强调了威胁情报平台的重要性，并针对欧盟威胁情报平台存在的情报分析能力欠缺、缺乏技术支持以及情报共享缺乏实时动态功能等不足，提出了诸多建议。2019 年 1 月欧盟网络与信息安全局发布《2018 年 ENISA 威胁全景报告》，探讨了开发内部威胁情报的紧迫性，并要求欧盟各成员国必须开发更强大的内部网络威胁情报系统，扩大网络威胁情报收集范围，提升欧盟网络威胁情报

能力，提高网络威胁情报的独立性和质量。2019 年 11 月发布的《增强欧盟未来网络安全战略价值链分析》，强调建立网络安全威胁风险及实践信息等的共享利用体系。2020 年 9 月，爱沙尼亚和美国启动了为期 5 年的网络威胁情报共享项目，以提升网络威胁情报共享的自动化水平。

英国更加注重网络安全威胁情报的汇聚与共享。英国国家网络安全中心负责威胁情报的收集和分析，该中心搭建了允许来自不同行业和组织的成员在安全和动态的环境中实时交换网络威胁信息的 CiSP 社区。2020 年 4 月，英国投资协会推出网络威胁情报平台 IATITAN，以帮助投资经理保护本公司免受网络攻击。该平台接入了来自执法部门、政府机构的威胁情报数据，可实时显示涉及投资管理社区的恶意软件、勒索软件和软件漏洞等威胁信息。

（二）威胁情报描述、交换和共享等环节标准逐渐完善

虽然目前国际上暂未形成统一的威胁情报标准，但是欧美国家积极围绕威胁情报描述、交换和共享等环节的标准化进行探索，IBM、思科、美国国防部等机构已形成了丰富的实践经验。

威胁情报描述环节，由美国非营利性组织 MITRE 联合美国国土安全部发布的结构化威胁信息表达式（STIX）标准，提供了威胁情报的描述方法，并可表示威胁情报中的多方面特征，包括威胁因素、威胁活动、威胁属性等。网络可观察表达式（CybOX）标准提供了一套用来描述计算机相关操作和内容的方法，可用于威胁评估、日志管理、恶意软件特征描述、指标共享和事件响应等。VERIS 事件

记录和事故共享词汇定义了一个用于描述安全事件的词汇表，它与网络可观察表达式 CybOX 的部分内容虽然有一些重叠，但是 VERIS 却扩展了针对一些特定场景的相关描述方法。

威胁情报交换和共享环节，2016 年 4 月，美国国家标准技术研究院发布的《美国联邦网络威胁信息共享指南（第二版）》，为美国联邦政府网络威胁信息共享工作指明了基本方向。指标信息的可信自动化交换（TAXII）标准规范了威胁情报交换和传输过程。使用 TAXII 规范，不同的组织机构之间可以通过定义对应的 API 来共享威胁情报。由美国网络安全公司 MANDIANT 发布的开放威胁指示器（OpenIOC）标准，通过将威胁信息转变为机器可读形式，实现威胁情报的快速共享。属性枚举和特征描述（MAEC）标准是一种共享恶意软件结构化信息的标准化语法，可去除恶意软件描述中的不确定问题。IODEF 安全事件描述转换格式是一种计算机安全事件响应组用来在其本身、他们的支持者及其合作者之间交换事件信息的格式，可以为互操作工具的开发提供基础。

（三）威胁情报自身多环节以及与多业务逐步融合

目前，国外网络安全企业在威胁情报的生产、分析及应用环节以及与多业务呈现不断融合趋势。

一方面，威胁情报的生产及分析环节的界限逐渐消失。原先具备丰富威胁情报数据来源的网络安全企业纷纷由仅提供数据向提供分析业务转变，包括思科、IBM 等市场占有率较高的网络安全硬件厂商，以及赛门铁克、红帽、卡巴斯基等拥有大量用户的杀毒软件

厂商。其中，IBM 通过整合其威胁研究数据和技术，包括 Qradar 安全情报平台、上万的客户和 IBM 安全管理服务的安全分析，发布集聚超过 700T 数据的 X-Force Exchange 威胁情报共享平台，面向全球提供对 IBM 及第三方威胁数据资源的访问，帮助网络安全分析人员和研究人员筛选出有价值的威胁情报信息。此外，卡巴斯基通过 Kaspersky Expert Security framework 对外提供威胁情报服务。该框架拥有数十亿字节的丰富威胁数据可供挖掘、先进的机器学习技术以及独特的全球专家库，还包括卡巴斯基反针对性攻击平台和终端检测响应 EDR 解决方案，可实现威胁发现和检测、调查和及时的事件响应处置。

另一方面，威胁情报业务逐渐与安全企业自身的安全解决方案、软硬件设备等多个业务融合。**俄罗斯厂商 Group-IB** 的威胁情报服务与能力已经被融合进其高复杂性的软硬件生态系统解决方案中，通过“打包”形式为客户提供网络攻击的监测、识别和处置服务。**美国 FireEye** 公司同样如此，其客户可以在购买 FireEye 设备后，进一步订购其威胁情报服务。其威胁情报主要从 FireEye 全球传感器中进行识别和提取，并通过与其旗下的 Mandiant 公司的网络安全事件响应数据进行融合，提供战术、战略和运营级威胁情报。**美国 CrowdStrike 公司**的 Falcon 威胁情报平台，可对企业日常数据进行监测。另外还可以通过学习攻击行为特征，形成相应的应急处置方案。

三、我国威胁情报产业调研分析

2015 年前后，威胁情报正式进入国内市场，以网络安全企业与互联网公司为主的产业主体积极围绕威胁情报技术及商业模式开展探索，同时大力推动威胁情报标准化和共享机制的建立。随着各行业对威胁情报的认识不断深入，威胁情报能力作为网络安全基础能力的重要价值得到进一步认可，市场需求持续扩大，且有望保持较快增长。据国家工业信息安全发展研究中心对涉及“威胁情报”能力网络安全产品的测算，我国威胁情报市场规模约在 10.69 亿元左右。

（一）我国威胁情报行业正处于初级发展阶段

2017 年 WannaCry 勒索病毒的大规模爆发，暴露出传统网络安全产品及防御体系缺乏对未知威胁识别以及应对能力，也一定程度上推动了以威胁情报、安全大脑等为代表的主动防御型网络安全产品的快速发展。近年来，奇安信、360、安恒信息、绿盟科技等传统大型网络安全企业，与阿里、腾讯等互联网公司利用自身技术及资源优势纷纷布局威胁情报领域。同时，微步在线、天际友盟等威胁情报初创企业，也凭借着自身核心技术竞争力与独特的商业模式，成为威胁情报领域生态链条中的重要参与者。从产品形态来看，我国威胁情报主流产品可分为以下三种：一是数据交付模式，即通过 API 查询、或订阅规则库的方式交付威胁情报数据；二是服务交付模式，可进一步分为结合威胁情报能力的检测、评估、测试、应急等网络安全服务包和面向专业安全技术人员提供威胁情报搜索、分析等服务；三是产品交付模式，包括集成威胁情报模块的网络安全设

备，以及为企业搭建具备情报运营能力的定制化威胁情报平台。

标准制定方面，2018 年 10 月 10 日，我国正式发布威胁情报的国家标准——《信息安全技术网络安全威胁信息格式规范 Information security technology — Cybersecurity threat information format》(GB/T36643-2018)。标准从可观测数据、攻击指标、安全事件、攻击活动、威胁主体、攻击目标、攻击方法、应对措施等八个组件进行描述，并将这些组件划分为对象、方法和事件三个域，最终构建出一个完整的网络安全威胁信息表达模型。其中，对象域包括威胁主体和攻击目标，二者构成攻击者与受害者的关系；事件域包括攻击活动、攻击指标、安全事件和可观测数据，以上组件构成完整的攻击事件流程；方法域包括攻击方法，即攻击方所使用的方法、技术和过程（TTP），以及应对措施，即防御方所采取的防护、检测、响应、回复等行动。此外，在组件属性的格式方面，与 STIX 2.x 版本一致，采用了更便于理解和阅读的基于 JavaScript 的 JSON 数据格式，JSON 格式有良好的自我描述性，结构简单，生成和解析都更为方便。

威胁情报共享方面，政企合作、平行机构共享、开源社区等不同层次的威胁共享机制初步建立。2021 年 9 月 1 日，工业和信息化部网络安全威胁和漏洞信息共享平台正式上线运行，面向电信主管部门、基础电信企业、互联网企业、网络安全企业、网络安全专业机构等，统一汇集、存储、分析、通报、发布网络安全威胁信息，并实现与相关单位网络安全监测平台实现对接。奇安信威胁情报中心联合国内知名网络安全企业共同发起建立网络安全威胁情报生态

联盟，搭建行业内威胁情报信息共享、数据运营、情报分发、威胁情报消费的行业闭环，以情报的共享交换促进网络安全产业协同发展。此外，微步在线推出国内首个综合性的威胁分析平台和情报分享社区——X 情报社区，并发布千万情报奖励计划，促进威胁情报共享与优质情报发掘。目前该社区注册用户达到 12 万以上，日活跃用户最高达 2 万以上。

（二）网络安全企业积极推动威胁情报产品化

我国网络安全企业围绕威胁情报的理念、技术、应用开展积极探索，从建设自身网络安全威胁情报体系，到开发威胁情报平台产品，再到构造模块化威胁情报能力，持续推动威胁情报产品化进程。

一是建立企业威胁情报共享中心，提升自身网络安全能力并对外开放威胁情报服务。网络安全企业依托部署在网络中的防火墙等安全设备、网络空间测绘系统、蜜罐蜜网捕获系统、开源情报采集系统、暗网监测系统等，基于对全网安全数据、开源情报的收集积累，综合运用静态分析、动态分析、大数据关联分析、深度学习、多源情报聚合等先进技术，结合技术专家团队丰富的一线实战攻防经验和安全研究能力，汇聚形成种类丰富的高质量威胁情报信息集合。同时，对外开放基于威胁情报能力的部分服务，如实时在线查询服务、在线沙箱样本分析服务等。

二是推出威胁情报平台产品，协助企业构建威胁情报全生命周期管理能力。威胁情报平台（TIP）是集情报汇聚、情报分析、情报检索、情报协同、情报分发等功能于一体的本地化威胁情报管理系

统，主要解决因高级威胁或未知威胁导致漏洞利用、主机失陷、病毒感染、钱财勒索等威胁定位问题，协助企业建设、完善、优化威胁溯源、关联分析、攻击画像、事件通告、共享赋能等威胁情报运营能力。威胁情报平台具备与其他网络安全设备联动的能力，通过赋能监测探针类、威胁感知类、分析溯源类、安全运营类产品服务，协助构建基于情报驱动的纵深防御体系，实现漏洞和入侵行为的快速研判和全网共享，提升威胁检测、响应处置、安全运营、事件分析、态势预警等安全能力。为更好服务于企业数字化转型，目前的威胁情报平台类产品均能够提供本地化平台和 SECaaS 服务[1]两种集成方式，以适配不同的业务环境。

三是集成威胁情报数据模块，推动威胁情报能力普及。为进一步提升威胁防护能力，网络安全企业开发独立的威胁情报数据模块，并将其集成至多种网络安全产品与服务中，实现终端安全防护设备与威胁情报中心之间的“云地联动”，以全网威胁情报能力驱动本地网络安全威胁监测与响应，提升威胁发现和威胁处置效率，实现小时级别威胁识别与防御。现阶段，安全检测类、分析类服务中已实现了威胁情报能力的深度集成。例如，在网络流量检测中，基于 IP 地址、域名、URL、文件 Hash 等 IOC 情报指标对流量载荷进行深度研判，实现攻击判定，并自动阻断后续攻击；在互联网接入服务中，基于恶意软件远控地址、钓鱼地址和矿池地址、非法网站数据，实现对恶意访问的过滤拦截；在终端检测中，充分利用“云上”威

[1] 安全即服务（Security as a Service，SECaaS)）即以软件即服务（Software as a Service，SaaS）的模式提供网络安全服务。

胁数据、恶意样本数据、攻击特征数据、黑客组织画像信息等关键数据，以及病毒引擎检测、智能沙箱分析与攻击链路行为分析等技术手段，对终端的进程、网络、文件等系统行为日志进行综合分析，实现对主机入侵的精准发现、自动化告警关联、攻击链路可视化展示与高效溯源、入侵事件响应及阻断等。

（三）行业企业需求主要集中于威胁情报订阅

在市场中，订阅模式一直是企业获取威胁情报服务的主流方式，然而以 SECaaS 服务的形式直接获取威胁情报能力的企业仍占少数，其威胁情报需求更多聚焦于订阅情报数据或情报查询服务的层面。

一是 API 查询服务。行业企业多倾向于在现有网络安全建设的基础上，以最小的成本投入扩展威胁情报的能力。面向网络安全产品和设备的威胁情报查询服务，即 API 查询服务，凭借其“性价比”优势赢得市场青睐。威胁情报 API 查询服务依托海量威胁情报库，支持对 IP 地址、域名、URL、文件 Hash 等多种信标进行高速递归检测，快速输出威胁判定结果、威胁名称、威胁组织、威胁类型等相关情报信息，直接服务于防火墙、入侵检测、入侵防御、Web 应用防护防火墙（WAF）、防病毒、终端检测响应（EDR）等安全设备。

二是在线查询服务。对于网络安全分析人员、研究人员来说，威胁情报能够帮助其快速了解新的 IOC 及相关信息，基于上下文信息更全面地分析攻击模式、攻击路径，预判有可能遭受攻击的应用、系统和用户群，从而优先保护这些高风险目标。各网络安全企业的威胁情报共享中心均支持在线情报搜索，可通过交互式查询方式获

取 IP 威胁、Web 威胁、恶意文件、漏洞威胁信息，并可对查询结果进行统计分析，展示威胁态势。

三是订阅推送服务。机读情报方面，行业企业可通过订阅高质量可同步的明文威胁情报规则集合，将其直接添加到现有安全产品和安全设备的规则库中，实现威胁情报能力的集成。订阅的方式能够使企业及时获取最新、最流行、高危情报规则，按需增减更新规则库，保证威胁情报能力持续优化更新。人读情报方面，网络安全分析人员、研究人员为更全面地掌握全球网络安全态势，更快了解最新的网络安全动态，通常会订阅专业威胁情报分析机构最新生产的威胁情报内容，例如高级威胁分析报告、重要趋势性分析报告、威胁通报预警、前瞻性研究成果与技术文献翻译等。RSS（Really Simple Syndication，简易信息聚合）订阅是目前较为主流的订阅方式。RSS 是一种网站之间共享内容的简易方式，使用 XML 作为彼此共享内容的标准方式，可根据用户选择的关键词和标签条件，将定制化的威胁情报信息以邮件等形式定期推送。

四、威胁情报服务能力框架

为更加科学全面地评价威胁情报供应商的服务能力，面向能力成熟度和市场发展潜力两类目标，围绕情报数据、业务流程、产品服务、企业竞争力等四个基本维度，构建 2 横 4 纵的服务能力评价框架。

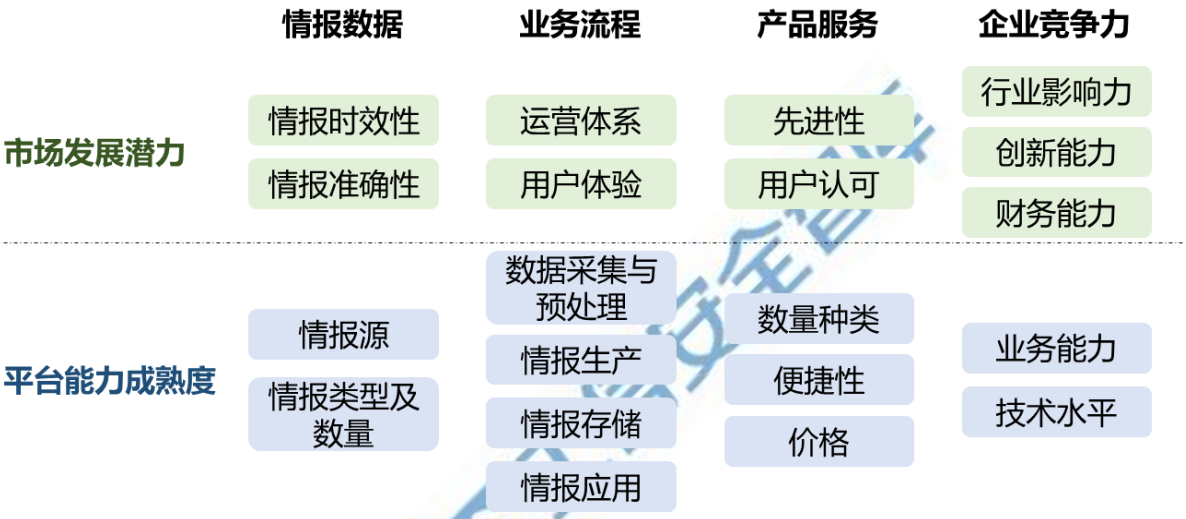


图 1 威胁情报服务能力框架

（一）情报数据

情报数据是威胁情报能力的基础，也是开展各类网络安全服务所必需的数据支撑。

从现有能力角度出发，对威胁情报数据的评价主要关注其全面性。**一是威胁情报来源。**数据来源的广泛程度说明了供应商威胁情报的获取能力，一般包括供应商内部自有产品体系记录及生成的数据、安全分析或研究过程中产生的情报数据，行业联盟的共享情报，来自外部的安全社区、社交媒体、第三方平台等的开源数据以及暗

网情报等。**二是威胁情报类型。**一个好的威胁情报平台应涵盖尽可能多的威胁情报类型，包括恶意域名、IP 信誉、恶意 URL、文件 Hash 等 IOC 情报，以及网络空间测绘数据、漏洞情报、黑客组织情报等。**三是威胁情报数量。**当前可供使用的威胁情报实际数量是反映供应商威胁情报服务能力的定量指标，但情报规模大小并不能准确体现其对用户需求的满足程度，还涉及情报适用性相关因素。

从市场发展来看，威胁情报数据的时效性与准确性决定了供应商威胁情报相关业务未来的发展潜力。**时效性**强是情报的重要特点，威胁情报的价值伴随时间的推移而下降，其内容也可能产生变化。威胁情报的时效性可通过情报的日常更新频率、过时或失真情报的处理频率，以及面对突发事件的威胁情报生产效率来评估。情报**准确性**决定了决策的效果，情报准确率或情报误报率通常作为度量威胁情报质量的重要指标。

（二）业务流程

围绕威胁情报运营的闭环流程是技术手段、管理措施、人员经验能力的集合。

从现有能力角度出发，可从数据采集与预处理、情报生产、情报存储与情报应用等各方面对威胁情报技术服务能力开展评价。**数据采集与预处理方面，**应考虑平台支持的数据接入设备种类及范围，还应包括对各类原始数据的抽取、清洗、归并等技术方法的性能评估，关注流程上如何实现统一的结构化处理，验证数据准确性并为情报标注置信度，以及类同情报数据的合并。**情报生产方面，**主要

关注威胁情报团队从海量低价值信息中提取高价值威胁特征的技术能力，包括在数据分类整理、关联融合分析过程中采用了何种大数据分析和人工智能技术等先进技术，对提升威胁情报生产效率和质量取得的积极成效等。**情报存储方面**，重点关注威胁情报数据库在存储架构、数据管理与处理技术的应用，以及在解决情报数据的可存储、可表示、可处理、可靠性及有效传输等几个关键问题方面取得的良好效果。**情报应用方面**，应考虑威胁情报平台能够对外提供的服务能力，一方面是与行业用户内部网络安全体系的联动能力，比如支持的接口形式和协议类型等，另一方面是其在线平台开放的服务能力，比如在线情报搜索、交互式查询、统计分析与动态展示等。此外，威胁情报共享方式共享范围和共享频率也是情报应用能力的重要体现。

从市场发展来看，威胁情报运营体系自身的完备性及行业用户对威胁情报服务的体验反馈可反映出企业威胁情报相关业务未来的发展潜力。一个好的**威胁情报运营体系**应具有完整的威胁情报生命周期管理闭环，覆盖威胁情报规划、威胁情报收集、威胁情报处理与分析、威胁情报分发以及应用、评价与反馈等全流程，并实现威胁情报运营的全闭环循环。目前，大多数供应商仍在探索建立与行业用户之间的威胁情报评价与反馈机制。**用户体验**方面，需着重关注情报的适用性，即提供的威胁情报服务与行业用户网络安全需求结合的紧密程度，对辅助安全决策发挥的作用如何，以及是否提供可定制化的情报订阅、共享交换方式等。此外，对于情报查询服务

而言，响应时间也是用户体验的重要方面，通常使用并发数、吞吐量（TPS）、每秒查询率（QPS）等指标来衡量。

（三）产品服务

产品服务是供应商威胁情报能力输出的载体，也是行业用户实现威胁情报赋能网络安全防御的必要途径。

从现有能力角度出发，立足于行业用户的网络安全威胁情报需求对威胁情报产品服务的供给能力进行评价。丰富的**产品服务数量与类别**为行业用户提供充足的选择空间，也刻画出供应商的产业供给能力。**产品服务的便捷性**取决于能否提供与行业用户实际威胁情报需求相匹配的产品形态、交付方式以及情报质量。例如，面向情报内生需求，是否具备威胁情报平台建设能力，或针对直接消费的要求，能否提供可定性、可研判、可拦截、可溯源的高质量威胁情报。此外，**价格**是行业用户在采购产品服务中重点考虑的因素之一，尤其是在网络安全预算有限的情况下会更加倾向于获得性价比更高的威胁情报产品或服务。

从市场发展来看，威胁情报产品服务的先进性与行业用户的认可程度决定了供应商威胁情报相关业务未来的发展潜力。一方面，威胁情报产品服务的**先进性**可表现为取得权威机构的相关资质认证，或通过具有广泛影响力的行业评选结果来体现。另一方面，**用户的认可**一般可通过相关威胁情报服务的续订情况、以及在线开放部分服务的威胁情报中心（社区）的用户活跃度来体现。

（四）企业竞争力

企业竞争力主要包括业务能力、技术能力和资本能力，是保障当下威胁情报能力建设及未来业务发展所需的产业基础资源。

对**企业现阶段**在威胁情报细分领域竞争力主要评估业务能力、技术能力两方面，一方面通过当前的业务营收规模或市场占有率来评估**威胁情报业务能力**，另一方面通过威胁情报相关的知识产权数量、威胁情报团队技术人员比重、威胁情报相关研发投入等指标衡量企业**威胁情报技术水平**。

从市场发展来看，供应商在网络安全行业的影响力、自主创新能力、资本能力等共同决定了供应商威胁情报相关业务未来的发展潜力。**行业影响力**的评估可参考供应商网络安全产品服务的市场占有情况、用户满意度和重大活动支撑情况等指标进行衡量。**自主创新能力**的评估可参考知识产权数量、研发人员的学历构成、研发投入占业务营收的比例等指标进行衡量。**财务能力**包含的评估可参考资产负债率、资产回报率、现金流、现金和现金等价物等指标进行衡量。

五、威胁情报行业发展趋势及建议

在网络攻击日趋复杂多样的背景下，企业网络安全建设逐步从被动的威胁应对模式转向发展内生网络安全能力，威胁情报在企业安全建设中的参考权重不断上升。面向未来，威胁情报应充分发挥网络安全基础知识支撑作用，覆盖多元化情报需求、实现更广范围情报共享，带动网络安全技术、服务、产业协同联动，推进网络安

全产业高质量发展。

（一）结合知识图谱技术，推动威胁情报开发利用

当前面向网络威胁情报领域所开展的工作多聚焦于 IOC 的获取与利用，日益严峻的网络安全态势要求企业具备更广阔的威胁情报视野、更丰富的威胁实体信息。未来，威胁情报数据来源的完善将成为安全厂商竞争的关键，开源威胁情报的收集、整理、分析或将成为威胁情报技术的制高点。然而，开源威胁情报主要来自网络安全白皮书、博客、供应商公告、社交媒体以及黑客论坛等公共资源数据，大多是文本类的非结构化数据，而且数据质量可能良莠不齐。为加强海量多源异构威胁数据的整合、提取和分析，提升网络威胁情报的质量和准确性，可基于网络安全知识图谱技术，实现关键威胁要素的融合与关联分析，形成统一高质量的威胁基础知识库，构建威胁情报能力。

知识图谱将客观世界中大规模碎片化知识转换成直观的结构化链接表达，实现了对知识的有效组织和管理，便于更加智能的访问操作，并在一定程度上实现智能辅助决策。在网络安全领域，知识图谱技术可优化威胁情报融合和关联分析方法，实现网络安全态势的整体感知和预测，进一步提升威胁狩猎的效率和准确性。**知识表示技术**以统一的逻辑框架开展威胁语义建模，将分散的大规模、碎片化的多源异构网络威胁情报数据转化为结构化的链接数据，并通过对文本的语义挖掘，进一步对网络威胁实体信息集成和链接，**形成统一的威胁情报知识体系**。**知识融合与推理技术**根据威胁情报知

识间的语义联系，通过公理和规则补全知识，基于深度学习方法进行有效的隐含知识挖掘和推理等，构建完善**威胁情报全景图**，为网络安全态势感知提供知识库资源。**语义搜索技术**可实现对单个威胁情报相关全部信息的检索，协助安全分析师高效准确的从大量碎片化的网络安全大数据中定位所需信息，服务于**网络攻击场景重构**。

（二）威胁情报需求分化，分层发展趋势初显

在数字化转型、企业上云的大潮下，网络安全需求加速释放，威胁情报能力作为“知己知彼”的下一代网络安全建设的基础支撑，将迎来更广阔的应用前景。

一方面，大型集团积极建设内部威胁情报基础设施，构建自身威胁情报能力。由于不同网络安全厂商面对的攻击者群体和攻击技术具有差异，其提供的威胁情报服务可能无法契合企业对于安全情报的需求。因此，具有一定技术基础和专业人才储备的大型集团企业为确保威胁情报能够真正服务于自身业务，更倾向于建设内部威胁情报能力，实现对多源威胁情报采集、处理、分析、生产，结合自身业务需求构建网络安全威胁情报运营的闭环。面向大型集团企业，网络安全厂商不仅要提供基础的威胁情报数据，更要注重输出威胁情报平台建设能力与定制化服务，协助企业建设既关注外部网络安全威胁，也关注内部数字资产风险；既服务于企业网络安全运营，也服务于日常经营管理活动的情报能力。

另一方面，中小企业要求可直接使用的威胁情报，青睐内嵌威胁情报能力的集约化安全服务。威胁情报生产和运营过程中，从数

据采集到数据分析，从情报验证到情报富化。从威胁建模到样本分析，大量工作都要求较高的专业知识技能，然而大多数企业往往并不具备基本的威胁情报认知和理解能力，更没有将威胁情报数据转化为威胁情报能力的专业人才储备。因此，面向中小企业直接交付威胁情报的生产和运营是不可行的，而应该以威胁情报服务能力输出为主，即依托威胁检测、响应处置、安全运营、事件分析等安全服务提供可定性、可研判、可拦截、可溯源的高质量威胁情报。同时，还应注重威胁情报能力下沉至生产业务及基础应用环境中，第一时间识别和检测网络中的攻击事件或异常行为。例如，通过邮箱数据比对自动识别钓鱼攻击威胁，通过对外网站来源检测自动识别暴力破解或 DDoS 攻击，通过 DNS 日志数据分析自动识别失陷资产，通过负载均衡数据分析自动定位恶意链接等等。此外，各大威胁情报中心面向网络安全从业人员、科研人员等免费开放部分功能的现象将更加普遍，在推广服务、提升影响力的同时，也一定程度上促进了威胁情报的共享。

（三）加快标准化建设，促进威胁情报共享融合

随着威胁行为体的规模、范围和复杂程度的增加，网络安全防御难度不断增大，仅靠单个企业的防御能力可能不足以应对，应逐步建立网络安全威胁情报共享机制，打破各自为战，实现协同联防。

一方面，标准化是威胁情报共享的必要前提。可借鉴美欧相关经验，从国家战略高度部署和推进威胁情报标准化工作，为标准的管理、更新和推广提供政策指导与制度保障。**威胁情报描述方面，**

鉴于我国威胁情报技术仍处在发展应用的初期，不同网络安全厂商以及行业组织的使用场景不尽相同，可在《信息安全技术网络安全威胁信息表达模型》(GB/T36643－2018)基础上逐步细化，实现威胁信息的结构化、系统化的表征从无到有、从实用化再到自动化。**传输协议方面，可**参考以 TAXII 为代表的威胁情报共享与传输规范的情报表达模式，并充分考虑基于威胁情报的共享机制、共享平台、智能化应用等需要，切实做好网络威胁情报生态环境的底层支持。结构化的规范情报描述标准和统一的传输协议可降低参与情报共享机构、存储库进行情报交换和数据格式转化的成本，提高情报交换的效率和准确性，促进各参与主体间资源共享、交流协作。

另一方面，机制建设是威胁情报共享的基础保障。2021 年 7 月，《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》公开征求意见，在“专栏 4　网络安全产业生态培育工程”中明确提出“**完善网络安全威胁信息共享服务体系和机制。**建立驱动漏洞、恶意程序、恶意地址、攻击行为等威胁信息挖掘、披露、流转和利用的规则机制，鼓励网络安全企业、行业用户、科研机构、高校积极参与信息共享，提升威胁信息要素聚集水平与服务能力。”，可借鉴欧盟信息共享与分析中心（ISAC）、公私合作伙伴（PPP）等共享合作经验，加强网络安全管理部门与行业、企业的合作与支持，扩展威胁情报共享路径，扩大威胁情报共享的参与主体范围，促进参与主体间网络安全能力合作协同。此外，应充分保障情报共享者的权益，设立行之有效的奖惩制度，调动各方共享情报的积极性，

并严厉打击“搭便车”行为以防止其对健康共享环境造成的负面影响，制定威胁情报合作共享长效机制。

（四）夯实威胁情报基础，赋能安全协同生态建设

在网络安全内生化趋势下，威胁情报的基础性、重要性作用不断凸显，日益成为新一代企业网络安全体系建设的核心。未来，威胁情报基础能力有望驱动基础网络设备、网络安全设备、终端安全产品和网络安全运营平台的协同联动，实现威胁检测、威胁分析、威胁处置、威胁溯源、威胁感知等的闭环。

一是情报融合分析。《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》在“加强共性基础支撑”重点任务中，也明确将“威胁信息”作为“**网络安全基础知识库**”的重要组成部分。建立网络安全基础知识库要求更广泛全面地收集防火墙、入侵检测、入侵防御等网络安全设备以及防病毒、终端检测响应（EDR）等终端安全管理产品产生的日志及告警数据，并构建多级情报联动管理能力，将进一步促进企业内部网络安全基础数据的关联分析与共享融合。在此基础上，依托对威胁情报、网络原始日志、终端日志、告警日志的关联分析，能够从攻击者视角还原攻击路径、呈现威胁全貌。

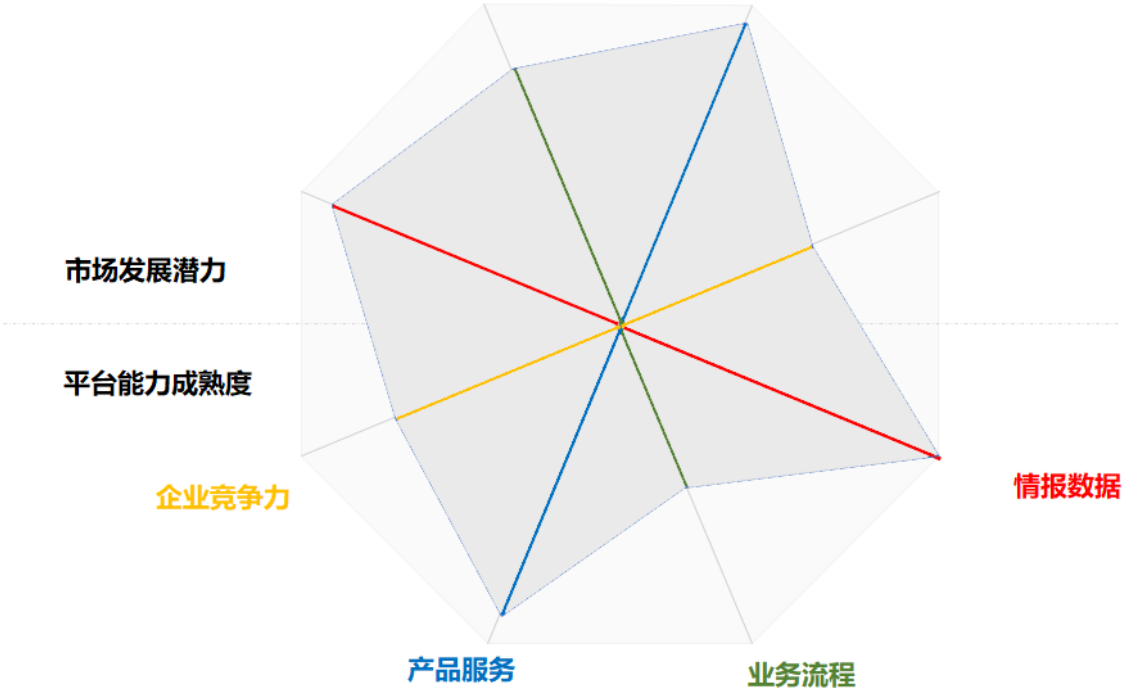
二是处置能力协同。威胁情报能力将驱动安全编排与自动化响应（SOAR）等安全运营平台更加快速地识别威胁并实施自动化处置。基于海量威胁情报构建动态更新的威胁特征库，赋能安全设备实施网络流量和主机日志的实时监控，有助于提升网络安全检测能力及

效率，尽早识别渗透行为并开展干预。以 TTP（战术、技术手段和过程）类情报为基础知识支持，利用攻击链模型或 ATT&CK 模型等进行威胁狩猎分析，实现攻击过程的精准定位以及对潜在威胁和攻击路径等的预判。更重要的是，结合网络安全攻防实践经验，建立与威胁特征相对应的安全响应指令集和响应策略集，编排各类网络安全、主机安全、终端安全设备协同开展威胁处置工作。例如，采取网络封堵、隔离等措施的同时，定位失陷主机并实施相应自动化处置策略。

三是安全态势研判。多源威胁情报信息的有效整合利用有助于激活企业安全信息和事件管理平台（SIEM）、网络安全运营中心（SOC）或网络安全态势感知平台等“安全大脑”的分析能力，助力企业实现从被动防御到主动防御的转变。充足的威胁情报数据将有效支撑对复杂多维的安全事件和网络流量的深度关联分析，从更加丰富的维度进行威胁分析，不仅能够更加全面地检测内部及外部的网络安全威胁，还能在威胁溯源分析中更加精准定位攻击来源及特征，并生成威胁预警能力，服务于后续安全运营。此外，在威胁情报分析中深入应用大数据分析、深度学习、人工智能等新技术，有效提升整体威胁态势综合研判能力，实现网络安全策略的动态调整，推动企业安全运营能力向智能化发展，实现更加精确主动的防御。

附录：典型网络安全威胁情报供应商的能力评价及优势分析

北京微步在线科技有限公司



●专注于威胁情报细分领域，以威胁情报数据为核心，结合云端与本地化产品以及专业安全服务，为各行业提供创新性解决方案。

●不断拓展基础网络数据监测范围，构建 PB 级威胁情报知识图谱，持续开展对全球近 300 个黑客组织的画像和追踪，确保对威胁、资产、风险场景更全面的覆盖。

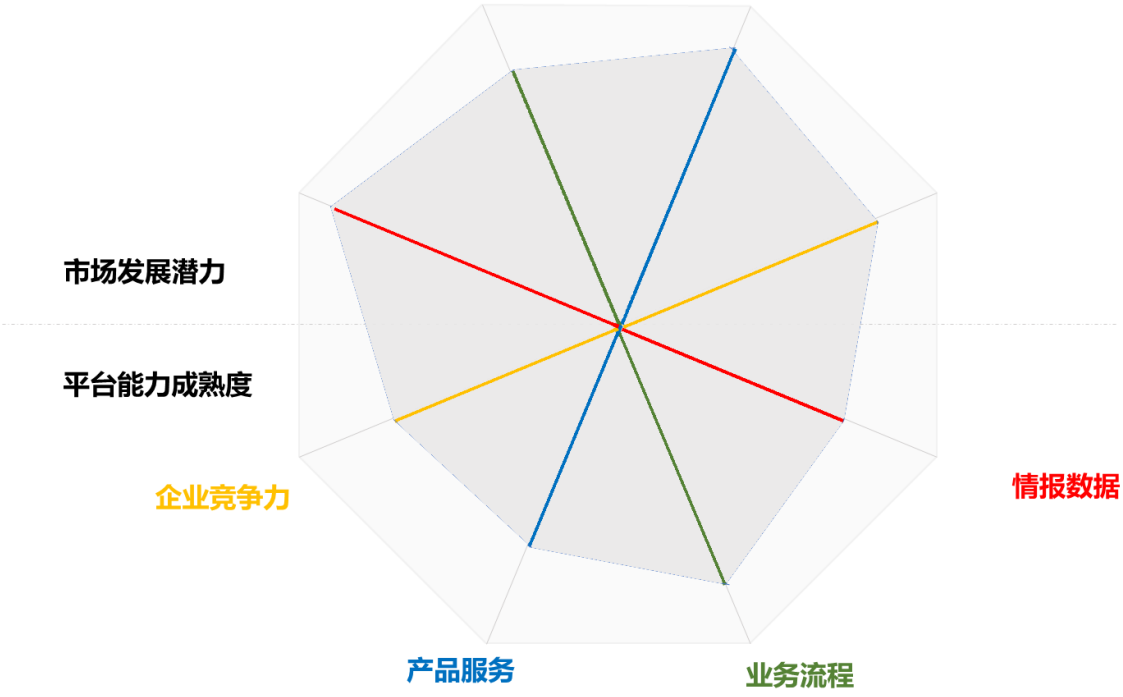
●深入应用 AI 技术，综合多种先进数据分析方法，支持多种场景下的情报提取和分析研判，实现了自动化生产高可信情报。

●采用规则+AI 模型的方式，对不同资产类型的 IOC 设置精细化的去误报机制，并结合情报告警反馈及时更新和优化去误报机制，实现高达 99.99%的情报准确率，以精准的情报数据驱动网络安全防

御。

●打造“检测—响应”产品矩阵，突出 SaaS 订阅模式+产品化的优势，实现从威胁情报衍生至全栈能力。其中威胁感知平台（TDP）、本地威胁情报管理平台（TIP）和 OneDNS 互联网安全接入服务三大主打产品覆盖了全流量威胁检测、本地化威胁情报管理和互联网安全接入等多个安全检测场景。此外，还推出了威胁情报检测与分析 API、开放威胁情报社区 X、恶意软件分析平台 S、企业安全服务 MDR、外部威胁监控服务 OneRisk、终端威胁检测与响应平台 OneEDR 等。

奇安信科技集团股份有限公司



●利用国内庞大的安全终端产生的海量基础数据，直接赋能自身安全体系产品，形成威胁情报驱动的联动防御体系。

●持续跟踪分析的主要 APT 团伙超过 46 个，独立发现 APT 组织 13 个，持续发布 APT 组织的跟踪报告超过 90 篇。

●威胁情报检测引擎支持细粒度的规则设置，具备微秒级威胁情报查询能力，准确率可达 99.9%。

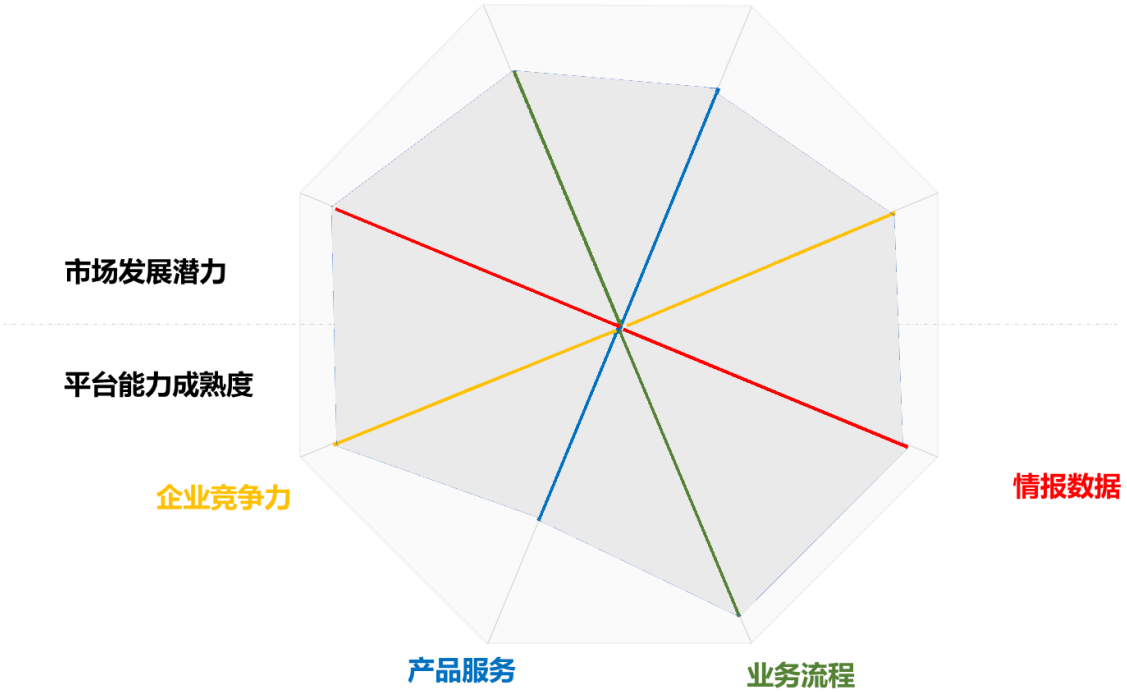
●自主研发基于大数据分析的多源威胁情报采集及查询技术、基于 KV 可扩展高性能数据处理引擎的威胁情报存取技术、基于图关系模型和大数据分布式关联引擎的威胁情报自动化分析技术等创新技术。

●发布包括威胁情报平台、ALPHA 威胁分析平台、威胁雷达、奇安信威胁情报运营系统（TIOS 解决方案）等威胁情报产品，覆盖

主流威胁情报服务模式，并提供定制化的行业解决方案。

●发起网络安全威胁情报生态联盟，面向联盟成员免费的失陷（受害）主机检测能力、告警日志富化能力。发布“TI INSIDE 计划”，把威胁情报中心多年来的数据积累、技术、能力、专家，尤其是威胁情报实战经验固化形成开发 SDK，服务于行业客户和生态合作伙伴，让威胁情报应用的行业生态合作也快一步。

360 政企安全集团



●建立大范围、长时间、多维度的存量和实时全网安全大数据库，安全大数据总存储数量超 2EB。建立攻防对抗知识库、APT 组织知识库、漏洞知识库、病毒库等多维度全景安全知识库。

●具备 APT 威胁情报的快速关联溯源能力，发现并追踪了 46 个 APT 组织及黑客团伙，独立发现了多起境外 APT 组织使用“在野”0day 漏洞针对我国境内目标发起的 APT 攻击。

●打造智能化情报生产流程，及时高效的生产 IOC 数据，并通过智能分析和人工运营提高情报的准确性。

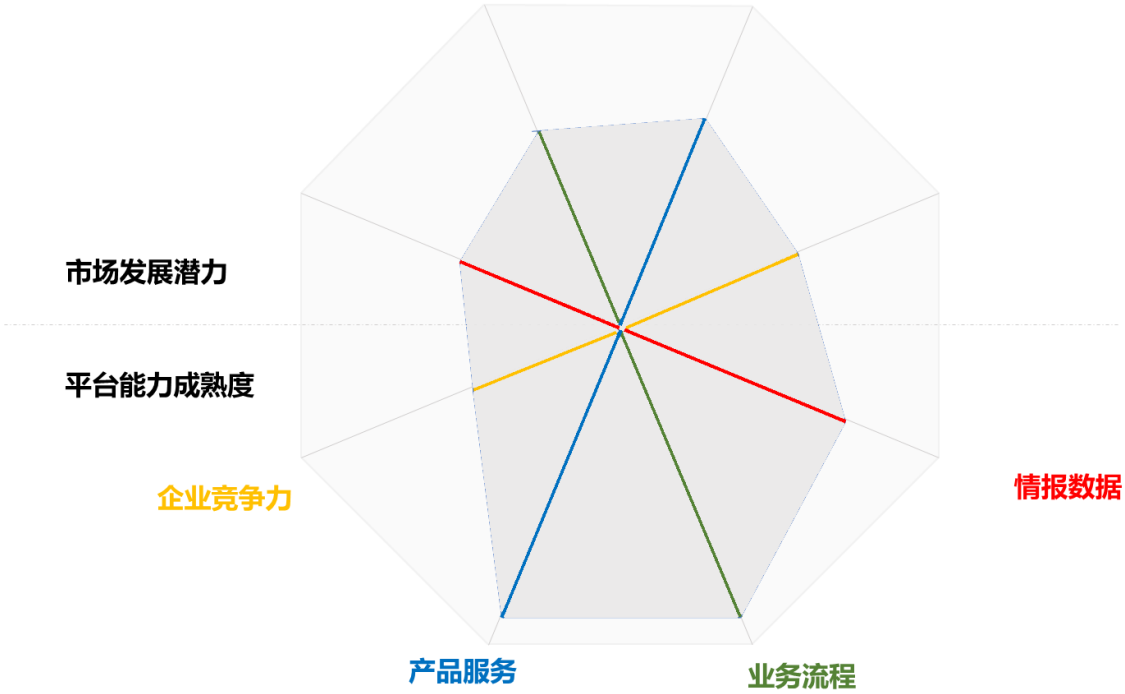
●研发基于 KV 引擎的威胁情报高速数据存储和查询技术、面向海量威胁情报数据的 ETL 性能优化技术、多源异构威胁情报动态评估与聚合技术、面向多粒度威胁情报数据的威胁研判分析技术、基于深度学习的自动化威胁情报提取分析技术和面向多源多维威胁情

报数据的情报图谱构建技术等创新技术。

●360 威胁情报平台可查询众多与恶意行为或威胁事件相关的基础与关联数据，如域名的历史解析记录信息、属主情况与变更信息、数字证书记录信息等，并提供了进一步的智能化分析预判结果，更全面地展示威胁全貌。

●发布威胁情报平台（TIP）提供一体化情报管理、赋能、评价、分享能力，以及威胁态势监控（TSM）提供云端威胁态势监控服务。

绿盟科技集团股份有限公司



●综合产品探针和 SaaS 服务、公网数据和第三方情报为用户提供全面优质的情报服务。

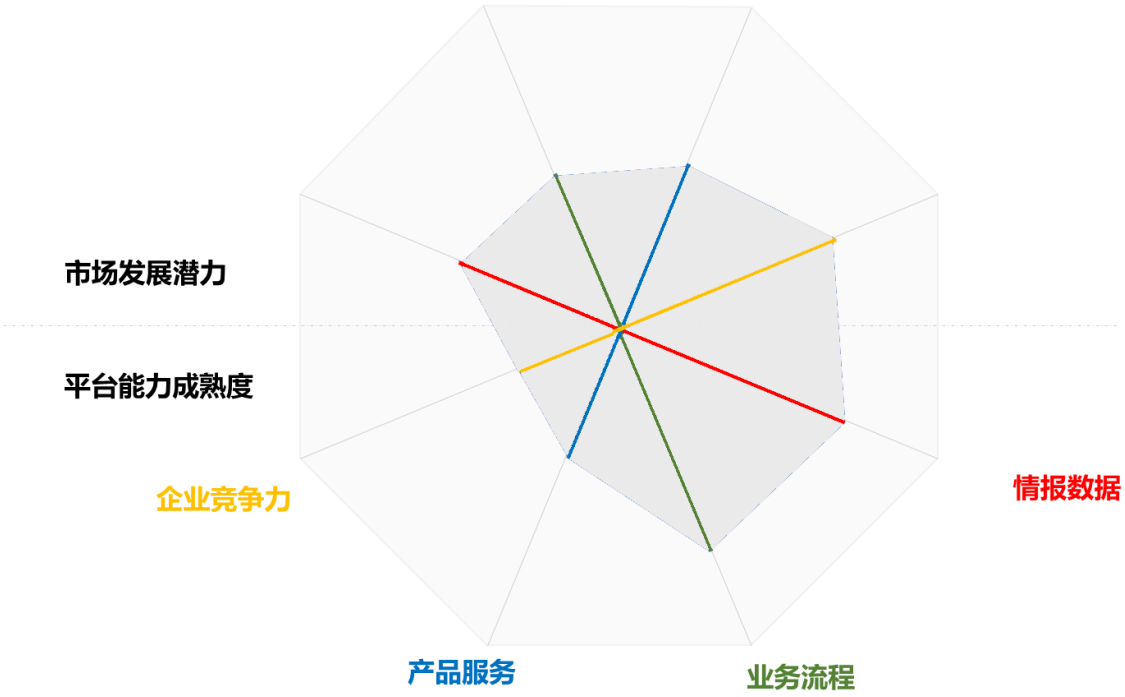
●基于持续的资产监测能力，将威胁情报与资产准确关联，以主动推送的方式为用户提供持续的资产安全性监测服务。

●自主研发基于知识图谱建模的威胁推理技术、威胁自适应诱捕与追踪技术、大数据关联分析与威胁挖掘技术等创新技术，助力未知威胁的发现。

●提供多种威胁情报输出和使用模式，以满足不同用户和业务的应用需求。面向安全人员，提供全球威胁情报云查询服务和定制化情报的 email 推送服务；针对第三方安全产品和软件，提供基于 API 访问接口的机读情报数据订阅服务。此外，面向专属威胁情报能力建设需求，提供本地威胁情报平台或用于安全产品或安全平台的威

胁情报数据模块；面向互联网资产管控的需求，衍生出基于情报的互联网资产核查服务。

杭州安恒信息技术股份有限公司



●基于网络空间探测雷达 Sumap 的全球网络空间资产探测能力提供最丰富的基础数据支撑能力。

●拥有多维度的情报库，包括高精准情报、IOC 情报、白名单情报、信誉情报、whois 数据、家族情报、近 4000 篇威胁事件情报、与 200 多个黑客组织相关的情报、230 多个分析报告和验证工具的漏洞情报等。

●威胁情报平台具备任一情报源接入能力，并能快速对情报进行处理、聚合、分析及评价情报质量等。

参考文献

[1]赵宁,李蕾,刘青春,叶锐.基于网络开源情报的威胁情报分析与管理.情报杂志.2021 年.

[2] 何志鹏,刘鹏,王鹤.网络威胁情报标准化建设分析.信息安全研究.2021 年.

[3] 李留英.欧盟网络威胁情报共享进展及启示研究.情报杂志.2021 年.

[4] 石志鑫,马瑜汝,张悦,等.威胁情报相关标准综述.信息安全研究.2021 年.

[5] 董聪,姜波,卢志刚,刘宝旭,李宁,马平川,姜政伟,刘俊荣.面向网络空间安全情报的知识图谱综述.信息安全学报.2020 年.

[6] 林玥,刘鹏,王鹤,等.网络安全威胁情报共享与交换研究综述.计算机研究与发展,2020 年.

[7] 王秉,郭世珍.安全情报服务能力评价指标体系构建.科技情报研究.2020 年.

[8] 张雷,宋栋,刘红.基于 AHP 的威胁情报网站价值评估方法.信息技术与网络安全.2020 年.

[9] 霍珊珊,李宁,周丽娜等.网络安全态势感知数据评价方法研究.2019 年.

[10]杨沛安,武杨,苏莉娅等.网络空间威胁情报共享技术综述.计算机科学.2018 年.

[11]王晨璐,胡敏,刘春阳等.基于威胁情报的安全指标量化技术研究与

应用.通信技术.2017 年.

[12]单琳.网络威胁情报发展现状综述.保密科学技术.2016 年.

[13]王滢波.网络安全企业核心竞争力指标初探.信息安全与通信保密.2015 年.

[14]Xu, Y., Yang, Y. and He, Y. A Business Process Oriented Dynamic Cyber Threat Intelligence Model. Proceedings of 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation. 2019 年 8 月.

[15]Dong, Cong & Chen, YuFan & Zhang, YunJian & Jiang, Bo & Han, DongXu & Liu, BaoXu. An Approach for Scale Suspicious Network Events Detection. 2019 年.

[16] Tounsi, Wiem & Rais, Helmi. A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & Security. 2017 年.

2021 年“工信安全智库”系列研究报告

报告编号	报告名称	发布时间
2021-yp-01	2020-2021 年度工业信息安全形势分析	2021 年 1 月
2021-yp-02	2020-2021 年数字经济形势分析	2021 年 1 月
2021-yp-03	2020-2021 年度信息技术产业形势分析	2021 年 1 月
2021-yp-04	2020-2021 年度全球网络空间形势分析	2021 年 1 月
2021-dc-01	2020-2021 年我国工业互联网产融合作发展报告	2021 年 2 月
2021-dc-02	2020 年我国网络安全产业产融合作发展报告	2021 年 2 月
2021-lw-01	拜登政府网络安全政策走向及影响研判	2021 年 2 月
2021-lw-02	数字税的概念详解、全球进展和有关影响	2021 年 3 月
2021-dc-03	网络安全保险发展现状研究及展望	2021 年 3 月
2021-dc-04	数字中国建设扎实推进——解读《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 远景目标纲要》第五篇“加快数字化发展 建设数字中国”	2021 年 3 月
2021-dc-05	全球跨境数据流动相关问题研究	2021 年 4 月
2021-lw-03	欧盟《数字市场法案》《数字服务法案》的影响、趋势和建议	2021 年 4 月
2021-lw-04	2020 年东盟数字经济发展情况报告	2021 年 5 月
2021-lw-05	“小院高墙”下美国产业政策走向及我国应对措施	2021 年 5 月
2021-by-01	全球趋势 2040 一个竞争更加激烈的世界	2021 年 5 月
2021-dc-06	国内外个人信息保护政策和立法探究	2021 年 5 月
2021-yp-05	2021 年工业信息安全半年形势分析	2021 年 6 月
2021-yp-06	2021 年数字经济半年形势分析	2021 年 6 月
2021-yp-07	2021 年信息技术产业半年形势分析	2021 年 6 月

报告编号	报告名称	发布时间
2021-dc-07	2021 年上半年我国工业互联网产融合作发展报告	2021 年 7 月
2021-dc-08	2021 年我国网络安全产业产融合作半年形势分析	2021 年 7 月
2021-dc-09	智能网联汽车数据安全研究	2021 年 7 月
2021-dc-10	我国智慧农业发展情况及对策建议	2021 年 8 月
2021-dc-11	中国—东盟数字经济合作白皮书	2021 年 8 月
2021-dc-12	2020 年我国企业数字化转型进程报告	2021 年 8 月
2021-lw-06	主要工业国家和地区推动制造业数字化转型的做法和启示	2021 年 8 月
2021-dc-13	我国网络安全产业调研报告	2021 年 9 月
2021-dc-14	我国《数据安全法》构建的数据安全治理框架及政策趋势研究	2021 年 9 月
2021-dc-15	新一代人工智能算力基础设施发展研究	2021 年 9 月
2021-dc-16	面向数字基建的网络安全监管体系构建研究	2021 年 9 月
2021-dc-17	人工智能安全风险及治理研究	2021 年 9 月
2021-dc-18	我国数据开放共享报告 2021	2021 年 9 月
2021-dc-19	美国加大科技遏制对我国工业和信息化重点领域的影响	2021 年 10 月
2021-zs-01	2021 长三角数字经济发展报告	2021 年 10 月
2021-dc-20	共同富裕：企业社会责任助力工业和信息化大中小企业融通发展	2021 年 10 月
2021-dc-21	算力：数字经济发展的基石	2021 年 11 月
2021-dc-22	新形势下我国工业互联网+智能制造产业发展研究	2021 年 11 月
2021-lw-07	国外数据信托制度研究	2021 年 11 月

联系人：赵铭晨　　19800323351