数世咨询
Digital World Consulting

漏洞情报选型指南

数世咨询
Digital World Consulting

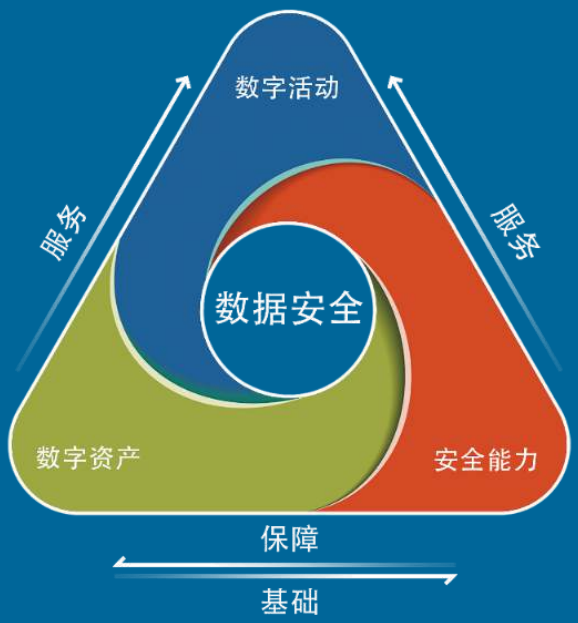
漏洞情报选型指南

数字安全是指，在全球数字化背景下，合理控制个人、组织、国家在各种活动中面临的数字风险，保障数字社会可持续发展*的政策法规、管理措施、技术方法等安全手段的总和。

这里的风险，不再局限于围绕数字化资产的攻防对抗，还包括了数字资产所承载业务的稳定性、连续性和健康性。这里的安全不再特指有意还是无意，天灾还是人祸，保安还是保险，而是更为广义的安全状态（SecSafe）。

*“世界环境与发展委员会出版的《我们共同的未来》报告中，将可持续发展定义为：“既能满足当代人的需要，又不对后代人满足其需要的能力构成危害的发展。”

——数世咨询，2023 年 11 月



以安全能力、数字资产和数字活动为三元素，以数据安全为核心目标，即三元一核的“数字安全三元论”。

“数字安全三元论”由“网络安全三元论”（数世咨询于 2020 年提出）更新迭代而来，旨在匹配数字中国建设的进程，保障数字基础设施稳定、可持续运行，保障数据有效流动、激发数据要素价值。

数世咨询作为国内独立的第三方调研咨询机构，为监管机构、地方政府、投资机构 ．网安企业等合伙伙伴提供网络安全产业现状调研，细分技术领域调研、投融资对接、技术尽职调查、市场品牌活动等调研咨询服务。

报告编委

报告类别：选型报告

报告名称：漏洞情报选型指南

主笔分析师：刘宸宇 数世咨询·高级分析师

分析团队：数世咨询·数字安全研究院

报告审核：李少鹏 数世咨询·首席分析师 闫志坤 数世咨询·市场分析师

目　录

一、 漏洞情报相关概念

1.1 威胁情报、漏洞、漏洞情报

◆ 威胁情报（Threat Intelligence）

威胁情报是一种基于证据的知识体系，描述已存在或潜在的威胁来源、攻击意图、手法（TTPs）、目标及应对建议，用于指导安全决策和响应行动。

◆ 漏洞（脆弱性 Vulnerability）

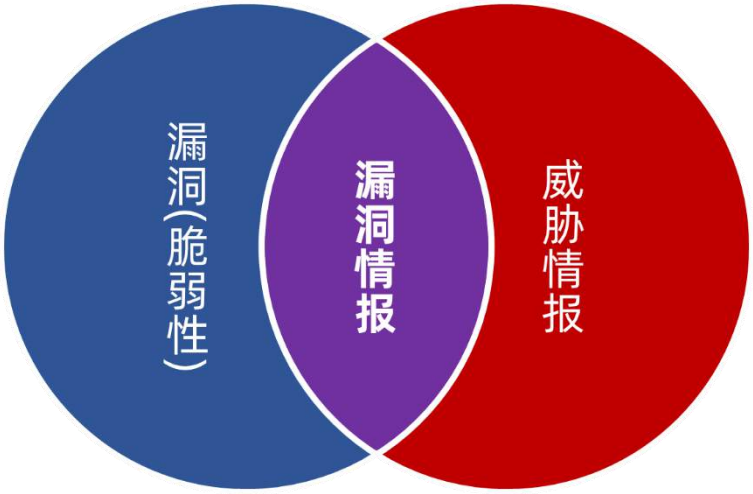
漏洞是指计算机、应用程序或网络设备等信息系统中由于自身代码缺陷、配置不当或业务逻辑等原因导致的安全脆弱性，可能存在被攻击者潜在利用的风险。

◆ 漏洞情报

漏洞情报是通过威胁情报技术对漏洞数据进行采集、深度分析和结构化处理后形成的知识体系，聚焦漏洞的利用方式（POC/EXP）、影响范围及修复方案。

◆ 三者的关系

首先，漏洞是原始数据，漏洞情报是漏洞的深度延伸，是漏洞数据加工后的知识。其次，威胁情报包含漏洞情报，但漏洞情报不等同于威胁情报。漏洞情报聚焦的是自身“脆弱性”，而威胁情报聚焦的是外部“攻击者”。但漏洞情报结合威胁情报（例如分析漏洞的可利用性与在野利用情况），知己知彼，攻防协同，可以发挥更大价值。



1.2 漏洞情报的组成

不同的漏洞情报发布平台，漏洞情报的组成项目不尽相同，各有优先与侧重，但主要的项目由以下内容组成：

项目	说明
漏洞名称	一般由产品名称、大版本号、漏洞类型、CVE 编号（若有）构成的简短组合
发布时间	一般包括公开日期、更新日期
漏洞类型	漏洞利用的类型，例如远程命令执行（RCE）、注入攻击、信息泄露、拒绝服务攻击等
漏洞编号	漏洞发布平台的编号，或是 CVE/CNVD/CNNVD 等共享平台的漏洞编号，帮助多个不同平台漏洞信息归一化的重要指标
影响产品与版本	详细的受影响产品与版本号，最严重的是“所有版本均受影响”
漏洞评级/评分	CVSS、EPSS 等参考评分，或是情报发布方参考 CVSS 评分、在野利用、可利用性等维度后给出的综合评分
技术细节	对漏洞细节的描述
POC/EXP	POC 即漏洞证明，用于检测证明漏洞的存在；EXP 即漏洞利用，使用代码或脚本利用漏洞的整个过程。仅有少部分

	漏洞有 POC/EXP，且往往不直接公开，避免被恶意攻击者利用
修复建议	临时补丁、安全更新包、版本升级等
相关链接	包括官网地址、披露地址

示例：

1.3 漏洞情报的披露、传递途径

大部分未公开漏洞，在 alpha、beta 以及灰度测试等阶段，已经由软件供应链上游厂商发现并修复。正式上线运行后的公开/半公开漏洞信息，则由个人白帽子、安全厂商的漏洞挖掘团队（安全实验室）、商业化漏洞情报社区（众测平台）等主体发现后，通过原厂安全响应中心（SRC）、漏洞上报平台、社区、群组等形式进行提交。

常见的漏洞情报披露、传递途径有：

漏洞情报披露、传递途径	举例
各国家级漏洞信息共享平台	如 NVD、CNVD、CNNVD、工业和信息化部网络安全威胁和漏洞信息共享平台（NVDB）、车联网产品安全漏洞专业库（CAVD）
开源技术社区&安全社区	如 GitHub、vulhub.org、Stack Overflow、看雪、itpub.net、CSDN、掘金、threatbook-x
社交软件群组	如 Facebook、Telegram、QQ 群、微信群
匿名/隐秘传播途径	如暗网

二、 漏洞情报需求场景

2.1 国家安全

在面对国家级安全威胁的自检自查场景中，漏洞情报是构建主动防御能力的重要数据来源之一。

场景标签：特种行业、0day 漏洞、APT 攻击、主动防御

特种行业所面临的国家级持续高级威胁（APT），多利用未公开的 0day 漏洞实现攻击渗透。威胁的隐蔽性高，潜伏时间长。针对这一场景，特种行业用户可利用漏洞情报，为关键单位和部门，针对关键设备、关键系统，实现主动防御性质的自检自查，先“敌”发现，先“敌”修复。

2.2 应急响应

在通用型漏洞应急响应场景中，漏洞情报是团队得以第一时间做出响应的最重要安全数据要素之一。

场景标签：头部用户、1day 漏洞、应急响应、安全能力成熟度较高

面对影响范围广泛的通用型漏洞，应急响应团队与潜在攻击者之间打响“抢时间”战斗，谁能先掌握漏洞的详细信息，利用 PoC/Exp 定位、控制漏洞资产，谁就能赢得这场战斗的制高点。巧合的是，近十年来，影响范围巨大的通用型漏洞（WannaCry、Struts2、Log4j 等），都是在周五晚上爆出来的，这相当于给刚刚进入周末放松状态的安全团队，来了一场“偷袭战”，因此，只有安全能力成熟度较高的头部用户，才能较为从容地应对，相应的，这对漏洞情报的及时性、准确性、完整性要求也会更高。

2.3 漏洞通报

在漏洞通报场景中，漏洞情报是行业监管、软件开发商通知重要用户尽快缓解、修复的重要依据之一。

场景标签：行业监管、软件开发商、Nday 漏洞、重要用户

关键信息基础设施行业中的重要用户，其业务的正常平稳运行关系国计民生，行业监管需要以漏洞情报为抓手，发现、通报关基行业 IT 环境中的漏洞并加以通报，落实安全责任；从软件供应链的角度，关基行业 IT 环境中被广泛使用的操作系统、软件、应用、中间件等一旦出现漏洞，直接、间接影响数百万乃至数亿台设备，其软件开发商也需要漏洞情报作为依据，为重要用户提供及时的漏洞通报与修复建议服务。

2.4 攻防演练

在攻防演练场景中，漏洞情报是自建“武器库”、锻炼安全团队、为自有安全产品赋能的重要组成部分。

场景标签：攻防演练、团队能力提升、Nday 漏洞

用户通过网络靶场、实训平台等方式搭建攻防演练环境，多用于安全技能培训、漏洞细节研究，实网攻防模拟等场景。该场景下，漏洞情报（特别是与用户自身资产特征相匹配的漏洞情报）的持续引入与更新，用于增加攻防演练环境的仿真度与对抗烈度，为安全团队提供有针对性的能力提升，同时也为用户的安全运营体系提供赋能。

三、 漏洞情报选购要点

3.1 情报及时性

- **合规角度**

2025 年 9 月 11 日，国家互联网信息办公室发布了《国家网络安全事件报告管理办法》[1]，对网络安全事件报告的最短时限提出了明确要求，根据网络安全事件的不同级别，最短上报时限不得超过半小时至 4 小时不等。《办法》将于 2025 年

[1] 《**国家网络安全事件报告管理办法**》全文详见 https://www.cac.gov.cn/2025-09/15/c_1759583017717009.htm

11 月 1 日起施行。

05 问：网络安全事件报告的流程和时限要求是什么？

涉及关键信息基础设施的，网络运营者应当第一时间向保护工作部门、公安机关报告，最迟不得超过1小时。属于重大、特别重大网络安全事件的，保护工作部门在收到报告后，应当第一时间向国家网信部门、国务院公安部门报告，最迟不得超过半小时。

网络运营者属于中央和国家机关各部门及其直属单位的，应当及时向本部门网信工作机构报告，最迟不得超过2小时。属于重大、特别重大网络安全事件的，各部门网信工作机构在收到报告后，应当第一时间向国家网信部门报告，最迟不得超过1小时。国家网信部门收到报告后及时向有关部门通报。

其他网络运营者应当及时向属地省级网信部门报告，最迟不得超过4小时。属于重大、特别重大网络安全事件的，省级网信部门在收到报告后，应当第一时间向国家网信部门报告，最迟不得超过1小时，并同时向同级有关部门通报。

由此，如果网络安全事件的主要构成因素包含漏洞，漏洞情报是否及时，就成为网络运营者是否能第一时间向相关主管部门上报事件的核心标准。

- **实战角度**

在漏洞技术细节逐渐被披露的过程中，网络运营者与潜在攻击者的对抗，关键就在于“谁更快”。漏洞情报更早传递到安全团队手中，就越能帮助安全团队先于攻击者定位漏洞资产、缓解漏洞影响。

3.2 信息完整度

前文“漏洞情报相关概念”中提到的漏洞信息组成内容中，除了漏洞名称等基本信息外，很多项目若包含以下更为丰富的关键信息，可视为具备较全面的信息完整度，帮助用户改善关注优先级：

- **漏洞的可利用性**

漏洞的危险等级并不直接代表漏洞对用户带来的危害，漏洞信息应当告诉用户，漏洞是否轻易可被攻击者利用。若是需要高权限执行、特殊身份交互、或者物理接触等条件才能利用的漏洞，对大部分用户来说，哪怕漏洞定级评分再高，也不

是需要优先关注的漏洞。因此，漏洞的可利用性，是基础漏洞信息之外要优先包含的内容。

- **漏洞的在野利用情况**

漏洞信息中若包含了在野利用的情况，如目前在某行业、某区域中已经被利用的大致数量、已被公开或通报的安全事件，这对于同行业、同区域的用户，将具有很高的参考价值，可以增加其优先进行处置的权重。

- **有针对性的修复建议**

在官方修复方案出来之前，漏洞情报若能够针对用户的业务优先级、IT 环境，提供有针对性的缓解措施，将为用户在最短时间内找到相对最优解——特别是供安全团队与业务、产研、网络运维等部门沟通协调下一步的动作——提供更具可操作性的选项。

3.3 与资产的匹配度

通用的漏洞情报作为全集，直接推送给用户的效果并不直观。海量情报的告警，等同于没有告警。因此，针对用户的业务优先级对应的资产环境，要有针对性的漏洞情报。即资产指纹与漏洞情报相匹配，具体来说，建议以用户订阅+情报商补充两者结合：

- **用户订阅**

一方面用户可以“订阅”方式，主动获取与自身 IT 资产相关的漏洞情报，此时需要情报提供方对资产的描述、定义、格式等进行标准化、归一化（如 CPE），保证资产指纹与用户的实际资产匹配度相一致。

- **情报商补充**

另一方面，由于用户的行业属性与业务场景在实施层面也需要落在具体的系统、软件、应用等 IT 资产，所以情报提供方也可以基于用户所在的行业属性、业务场景、软件供应链，为用户提供订阅之外的、间接匹配的情报。这种间接的漏洞情报，也可以为用户有效提供额外的情报补充。

3.4 漏洞优先级技术 VPT

以漏洞优先级技术 VPT 为优先采购立项的用户，建议重点关注前文提到的漏洞可利用性、漏洞在野利用情况、与资产的匹配度，除此之外，还建议考察漏洞情报的行业/合规、外部威胁两个方面。

- **漏洞可利用性**

见前文

- **漏洞在野利用情况**

见前文

- **与资产的匹配度**

见前文

- **行业/合规**

漏洞情报是否具备行业/合规属性。例如用户行业属于金融行业，有着“安全事件一票否决”这样的合规要求，又例如近期用户所在地区正在进行“两高一弱”的专项排查。诸如此类需求，漏洞情报商应当有针对性的提供专项情报，增加情报数量，或进行专项增量推送。

- **外部威胁**

当国际局势持续动荡，地缘冲突此起彼伏时，“关基”行业用户面临的潜在外部威胁风险增加，因此漏洞情报供应商若具备能力，可从“威胁”角度，以相关国家、地区的 APT 组织及其 TTPs 为研究目标，针对其习惯利用的漏洞与恶意软件家族，为“关基”用户提供专项情报。

3.5 漏洞验证 PoC

Exp 本报告不涉及，这里只讨论漏洞验证 PoC，建议用户采购时关注两个方面：

- **高质量 PoC 的数量**

用户采购漏洞情报时，请勿简单以 PoC 绝对数量为比较标准，要在去重、保留高危、去掉简单版本比对、与用户资产不匹配等低质量的 PoC 之后，综合以高质量 PoC 的数量为情报采购时的参考依据。

- **非破坏性**

漏洞验证 PoC 的执行，不应当对业务或 IT 环境有任何不良影响。当然，漏洞安全事件爆发的第一时间，为了“抢时间“，仓促编写好的 PoC 无法在模拟仿真环境中充分验证其对各种业务环境的影响，但在正式采购中，至少对批量交付的存量 PoC，应当有较为严格的非破坏性要求。

3.6 交付

- **格式、接口标准化**

漏洞情报应当兼容 CNVD、CNNVD 等国内主要的漏洞共享平台信息格式 ，具备标准化的 API 接口，能够与主流的攻击面管理、漏洞管理平台等产品对接。

- **支持多种交付形式**

漏洞情报的交付应当支持 Web 在线查询订阅、API 接口、SDK 等多种交付形式，且针对重大安全漏洞，或应用户要求，能够提供专项分析报告。此外，漏洞情报的预警通知渠道，也应当支持多种渠道，例如 API、邮箱、微信、Web 在线订阅查询等。

四、 选购前的问题

4.1 需要的是漏洞扫描器还是漏洞情报？

漏洞扫描器是工具型产品，而漏洞情报属于数据型产品。

—— 数世咨询

漏扫并非漏洞情报的消费场景。若团队已经建立起漏洞管理平台或攻击面管理平台，漏洞情报是一个必要且有力的数据补充。但倘若尚未具备此类平台，而是希望通过基于漏洞扫描器的方式引入漏洞情报，很可能事与愿违。漏洞扫描器中的漏洞信息与本报告中的漏洞情报主要区别在于：

- **时效性不同**

漏洞情报时效性更快，所谓 0day、1day 漏洞，才算漏洞情报；但漏扫中更新的漏洞信息，则要慢得多，一般最快更新也要在漏洞披露一个月以后。大部分的漏扫信息库更新都在三个月到半年。

- **流通范围不同**

漏洞情报的流通仅在极小范围，由商用情报商付费提供，或是技术小圈子内私密流通。在漏洞情报逐渐大范围传播后，漏洞技术细节逐步补充完整，各大漏洞库也均已收录，此时漏洞情报属性已转为公开的漏洞信息。

- **应用场景不同**

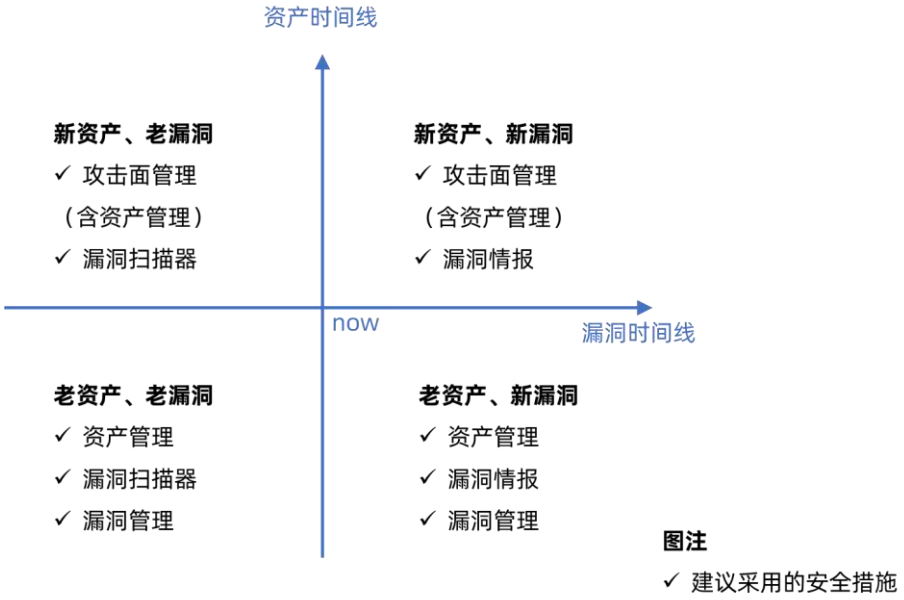
漏洞情报的应用场景如前文所述，一般用于商业客户对受漏洞影响资产的快速定位，或是特种行业 0day 漏洞的自检自查；而漏洞信息作为存量数据，批量存在于漏洞扫描器或漏洞管理平台中，使用方式也以版本匹配为主，不像漏洞情报多以 PoC 方式进行漏洞验证。

- **使用条件不同**

漏洞情报的使用条件较为苛刻，例如特种行业安全优先于业务，使用 0day 漏洞情报自检自查时，甚至可以接受短期的工作业务中断；又例如头部超大型互联网企业，有超强的应急处置能力，在 1day 漏洞情报定位风险资产后，可以组织多个不同部门的自有技术团队协同处置；相比之下，漏扫厂商定期更新的漏洞信息，已经在模拟仿真或真实的主流 IT 环境中进行了适配，以保证漏洞信息的准确、稳定、适配性强，因此，漏扫的使用条件会低很多，初、中级的安全工程师即可胜任。

4.2 资产管理工作是否做到位？

众所周知，风险=资产×漏洞×威胁。如果就资产、漏洞这两个维度进行分析，很容易得出结论，漏洞情报要发挥出更大价值，资产管理是必备的基础工作。如下图所示：



- **老资产，老漏洞**

存在多年的资产，如果还有很多老旧漏洞尚未修复，说明基础的安全工作尚未做好，这不是漏洞情报的目标场景。需要先以资产管理为基础，建立资产台账，然后辅以漏洞扫描器、漏洞管理等安全产品提升安全基线。

- **老资产，新漏洞**

存在多年的资产，如果新爆出一个漏洞，这是典型的漏洞情报应用场景，即前文提到的漏洞安全事件应急响应，可以利用漏洞情报快速定位存在漏洞的风险资产。设想如果没有做好资产管理，存在着盲点资产，即便是非常高质量的漏洞情报也没有了用武之地。

- **新资产，老漏洞**

这种场景一般是 IT 环境变化（例如新员工或访客的 BYOD）带来的新资产。新的 IT 环境中所有形态的新资产，都需要由安全团队第一时间发现、纳管，这些新资

产中经常存在极易被利用的 RCE 漏洞，此时安全控制措施的首选，建议采用具备持续新资产发现能力的攻击面管理（例如强制下线）。

- **新资产，新漏洞**

该场景中可能会综合出现上文提到的多种情况，但基本逻辑不变，都需要先以攻击面管理类型的产品，持续进行资产发现，同时辅以高质量的漏洞情报，对新出现的漏洞进行验证、缓解、修复等工作。该场景中的漏洞情报需要以 API 的方式与攻击面管理或漏洞管理平台进行自动化对接，以提高响应时效。

综上四个场景，只有将资产与漏洞情报相结合，才能有效收敛这两者带来的攻击暴露面，降低潜在的威胁风险。

此外，新业务、新系统、新应用，这些新资产在上线前的开发过程中，会存在产品研发团队代码编写导致的漏洞，因此在上线前，安全团队需要开展大量的安全测试工作，这属于开发安全或应用安全的范畴，本报告暂不展开论述。

五、 典型供应商代表

（排名不分先后，以公司简称首字母排序）

5.1 360 数字安全

差异化特点

1. 专属情报订阅：基于用户资产信息，提供定制化的精准情报推送，帮助用户聚焦于高可利用性、高危害性且需优先修复的漏洞。
2. 行业供应链情报订阅：覆盖金融、能源等重点行业的常用系统和软件。一旦出现相关 0day 或 1day 漏洞，可第一时间生成漏洞情报并推送至对应行业用户。同时支持历史行业漏洞的追溯，助力用户全面排查风险。
3. 标准化情报内容：推送的漏洞情报不仅便于人工阅读，也支持机器精准解析，告别杂乱无规则的数据格式，助力用户实现漏洞威胁处理的系统化与工程化。
4. 通俗化情报解读：除常规专业术语外，情报内容中额外加入通俗释义，使网络安全运营、研发、管理及普通员工均可轻松理解漏洞危害，有效降低运营

以及沟通成本，提升防御措施落地效率。

5. 0day 漏洞挖掘服务：经用户授权，可对用户自研并对外发布的软件系统进行漏洞挖掘，发现风险后转化为结构化情报及时上报，助力先于攻击者发现并修复漏洞。

部分用户

光大银行　建设银行

联系方式

网址：https://vi.loudongyun.360.net

邮箱：360VRI@360.cn

5.2 安恒信息

差异化特点

1. 安恒漏洞情报监测平台集成数十种实时爬虫，整合超百万条元数据公告，快速获取并更新全网公开的安全漏洞信息。
2. 平台具备 AI 能力，可自动对漏洞数据进行高效筛选、分类、完善，显著提升数据整理与分析效率，全自动化实现漏洞档案字段补全。
3. 具有安恒研究院全生命周期数据特性，涵盖策略处置、指纹处置及漏洞分析研究等内容，为用户提供深度洞见与研究支持。
4. 基于恒脑 3.0 能力，平台实现漏洞个性化，自动化打标，协助用户从众多漏洞中筛选出需要重点关注的漏洞，其标签种类包括但不限于影响领域（如 AI）、产品、厂商及关联 APT 事件等，实现漏洞资产的自动化个性标记。
5. 平台支持结合客户资产部署环境、资产重要性和漏洞本身的危害程度，重新调整漏洞危害评分，从而实现漏洞优先级的动态调整和个性化定制。

联系方式

https://www.dbappsecurity.com.cn

5.3 绿盟科技

差异化特点

1. 7x24 小时不间断的全网情报监控雷达，覆盖厂商公告、安全社区、漏洞文库、暗网论坛等多渠道数据源，实时采集安全漏洞、漏洞 EXP、安全事件、木马后门等情报信息。基于 CVSS 评分，综合漏洞 PoC 情况、在野利用状态、产品影响范围等维度评估漏洞风险，聚焦高风险漏洞运营，避免用户漏洞信息过载。
2. 多样的情报数据源与产品覆盖能力，涵盖操作系统、数据库、中间件、框架组件、终端软件、应用软件、安全设备等上百国内外厂商主流产品，最大化保障漏洞情报覆盖面，同时提供丰富且详尽的漏洞情报信息，针对重要漏洞提供深度分析复现报告，满足用户漏洞管理各阶段工作所需。
3. 整合公司多个团队资源，联动各产线协调配合；研究专家提供分析指导，攻防专家开展漏洞复现，产品专家编写规则，工程专家排查处置，多方协作为漏洞提供强有力的支撑，保障漏洞从监测预警到落地修复的全流程闭环。
4. 依托绿盟科技多年的漏洞研究与情报数据积累，针对漏洞输出的处置手册包含官方修复方法、临时防护措施和全系产品解决方案等内容，且针对不同的场景单独进行情况说明，确保整改工作落地。同时利用情报工作平台，动态跟踪情报处理状态，及时跟进产品规则迭代、情报推送等环节，确保漏洞闭环管理。
5. 自建漏洞场景 AI 深度研究 Agent，基于风云卫安全大模型与工作流框架自动收集与挖掘漏洞数据，汇总生成结构化漏洞报告与多格式 PoC 检测插件，极大提高信息收集与漏洞处置效率。

部分用户

某国有大行与商业大行、头部券商与保险集团、国家多个部委与事业单位、头部国有与私营能源企业、多家运营商省公司

联系方式

邮箱：cert@nsfocus.com

5.4 奇安信

差异化特点

1. 漏洞情报关键信息更加全面，涵盖更多的技术细节、检测规则、自研及多个公共 PoC/Exp、补丁文件及更多缓解/修复方案；
2. 打通 API、Web、微信、邮件等多个通知方式，重要漏洞实时推送，快于潜在攻击者启动漏洞缓解动作；
3. 支持 AI 总结情报。基于奇安信安全大模型 Q-GPT 的能力汇总多源漏洞情报，省去安全团队大量的基础资料搜集时间，提升漏洞响应时效；
4. 基于奇安信多年 APT 威胁防护与分析能力，漏洞情报高级分析报告包含漏洞利用分析、完整过程复现、攻击流量包分析、安全设备检测与防护规则策略等深度内容，协助用户对重要漏洞情报信息全掌控；

部分用户

天翼云、华为、大疆、华晨宝马

联系方式

网址：https://ti.qianxin.com/vulnerability

邮箱：ti_support@qianxin.com

5.5 盛邦安全

差异化特点

1. 拥有 DayDayPoc 漏洞社区，该社区集漏洞情报搜集、漏洞挖掘、漏洞收录、漏洞研究为一体，通过凝聚社区的安全技术力量，打造覆盖面广、检测能力强、漏洞扫描高效的检测、验证性平台，形成以漏洞检测与漏洞共性技术研发的研究生态圈。
2. 自研 AI 自动化漏洞挖掘工具 codeqlpy，可基于大语言模型能力进行自动化漏洞挖掘。
3. 作为烽火台情报联盟的首批成员单位，参与了联盟的发起和建设。其自主研发的“RayTBD 多源威胁情报融合分析平台”具备动态信誉评价与多级协同能

力，在 APT 资产拓线，攻击 IP 画像等方面具备独特优势；

4. 旗下的烽火台实验室以漏洞研究和攻防对抗为能力基石，持续为以上社区、工具和系统提供技术支撑，形成“实战驱动安全”的技术闭环。

部分用户

国家多个部委与事业单位、头部央国企、头部运营商、头部银行和券商、头部电力能源企业等

联系方式

https://www.ddpoc.com/

5.6 摄星科技

差异化特点

1. 资产驱动：以软硬件/开源组件视角，给出其漏洞及威胁变化趋势，及其最新版本、历史版本、安全版本、版本生命周期 EOL、高风险版本（包含两高一弱、APT、勒索软件、CISA KEV、关键漏洞目录、PoC/ExP 漏洞）。以及 jar 包漏洞查询、恶意开源组件包查询。
2. 运营视角：多年来专注漏洞管理平台和漏洞情报运营，持续为中国人民银行金融网络安全态势感知平台提供漏洞情报服务。深刻理解监主管机构、运营单位不同视角下的需求和痛点，形成具备独有优势的漏洞情报知识库，具备扎实的漏洞情报底座。赋能解决软硬件/组件命名不一致问题、解决海量漏洞管理问题、优先级评估和合规排查、提供“非接触”式漏洞发现能力。特别是在总部及下属机构间的联防联控场景中，可显著提升全局性资产漏洞管理能力。
3. 情报普惠：可根据软硬件/开源组件数量、时间（月、年）购买服务，购买成本低至传统漏洞情报的 1%；无需专业网络安全人员和本地系统或平台对接，使用浏览器、邮件、微信即可享受专业的定向漏洞情报。适合中小微企业、安全团队、大型机构的分支机构使用；24 小时全球漏洞情报监测，分钟级量定向漏洞预警。漏洞风险早知道、先知道、全知道。助力用户在网络安全合规、攻防对抗中获得先手优势和主动权。

部分用户

中国人民银行、东莞银行、中国联通、锐捷网络

联系方式

网址：https://xm.vulinsight.com.cn/

电话：010-62410018

5.7 腾讯安全

差异化特点

作为云安全、零信任、边界防护、漏洞管理、攻击面管理等安全产品的数据支撑型生态合作伙伴，腾讯安全以腾讯的运营商级海量威胁情报数据为基础，结合腾讯云自身安全需求与腾讯管家海量反病毒样例库，形成覆盖由云到端的高质量漏洞知识库，交付众多头部用户与广大安全厂商。

部分用户

天融信、锐捷网络

联系方式

tix@tencent.com

5.8 微步在线

差异化特点

1. 大型情报社区加持，漏洞情报更及时完整。依托国内用户规模领先、持续多年运营的威胁情报社区——“X 情报社区”，微步在线实时收集高价值漏洞信息及全网高质量漏洞源数据，持续补充微步自有产品发现的漏洞在野攻击数据的同时，为漏洞情报提供时效性更高、信息完整度更高的社区化支撑。

2. 自研漏洞风险评级，聚焦真正高风险漏洞。微步在线自研漏洞风险评估方法——漏洞评估模型（VPT），深度融合微步深耕多年威胁情报能力，对漏洞严重性、利用难度、潜在影响、在野利用情况等多个维度进行评估，发现真正高危漏洞，降噪率达到 95%，企业只需优先关注 5%的高风险漏洞告警。
3. 10%以上漏洞早于各大公开漏洞库，且提供全面准确漏洞详情。针对多渠道及时获取到的漏洞情报，微步在线漏洞分析师会对漏洞进行全方位深度剖析，涵盖漏洞原理、代码层详尽分析以及攻击特征的精准研判，为企业自查与提前防御提供有力支持。此外，微步漏洞情报提供自研无损 PoC，为企业漏洞排查提供高效、可靠工具，并为企业及时提供切实可行的临时修复方案，帮助企业迅速应对威胁，保障业务稳定运行。
4. 自动化漏洞资产匹配。微步在线漏洞情报可无缝对接企业资产平台，基于微步 XGPT 安全大模型能力，解决资产命名不一致的核心卡点，实现资产与漏洞智能精准且自动化匹配，快速定位受漏洞影响资产范围，并为企业后续漏洞处置提供明确指引，提升漏洞响应效率和效果，完成漏洞情报闭环。

部分用户

金融（银行、证券、交易所）、国央企、制造业、快消、运营商及教育行业

联系方式

https://x.threatbook.com/v5/vulIntelligence

（扫码一键试用微步漏洞情报）

5.9 知道创宇

差异化特点

1. 知道创宇的智脑漏洞情报速递产品，以多源高精度情报为核心驱动，以网络空间测绘为评估工具，以专业应急支撑经验为交付标准的全球漏洞情报能力产品，目标是为客户提供先发、精准、全维度的漏洞风险管控能力。
2. 快速的漏洞情报推送服务。依托于知道创宇 404 安全研究团队与 Seebug 平台

多年来在漏洞应急、漏洞分析、漏洞挖掘的经验，能够在第一时间内对漏洞进行分析，最快速同步至客户手中，为客户迅速进一步评估影响风险范围提供重要依据。

3. 准确的漏洞影响评估服务。知道创宇 404 安全研究团队将结合数十年的网络空间测绘能力与丰富的行业情报积累，能够迅速评估漏洞的影响范围和影响深度，确保客户在最短时间内具备先发预警与高效应急响应能力。

部分用户

国内商业大行、保险集团、头部券商、国有大行、国内某大型能源企业等。

联系方式

https://www.knownsec.com/#/contact

六、 附录：漏洞情报应用案例

某银行漏洞情报建设管理方案

（本案例由 360 数字安全提供）

案例背景

随着数字化转型的深入，金融业务与信息系统的耦合已达到前所未有的深度，云原生、分布式、AI 等新技术的广泛应用，极大地拓展了我们的业务边界。然而，这也同步急剧放大了我们的攻击面。

当前，网络安全威胁正呈现专业化、产业化态势。**尤其是与金融业务强相关的应用漏洞、第三方组件缺陷以及高危 0day 漏洞的持续爆发，使得我们传统的被动防御模式面临巨大挑战。**由于银行直接涉及海量的用户资金与敏感数据，一旦未能提前获知与自身相关的关键漏洞情报，导致防护措施滞后，遭受攻击的后果将不堪设想。这不仅会直接造成巨大的财务损失，更会引发客户信任危机、监管严厉处罚，对企业积累的声誉造成毁灭性打击。

因此，建立一套精准、及时、可行动的漏洞情报能力，不再是一种选择，而是构筑金融系统（例如银行、证券）主动、弹性安全防御体系的战略性必需品，对于保障业务连续性和维护金融稳定至关重要。

解决方案

- 为银行建立以情报驱动的漏洞快速响应机制

为应对日益严峻的第三方软件漏洞和 0day 威胁，本方案通过为，某银行部署 360 漏洞情报服务，增强全行对外部威胁感知与快速响应能力。服务提供 API 接口集成与 SaaS 化在线平台两种模式，满足银行不同场景下的使用需求。通过将漏洞情报能力无缝对接到银行现有的安全运营流程中，实现对高危漏洞的分钟级感知、小时级响应，彻底改变以往依赖公开信息导致的响应滞后局面，最大程度压缩攻击者可利用的时间窗口。

- 多渠道实时预警，抢占应急响应先机

本方案的核心优势在于情报的及时性与触达率。除了通过 API 和 SaaS 平台主动获取情报外，我们建立了多渠道实时预警机制。一旦有符合银行预设风险等级（如高危、紧急）或与银行资产相关的新漏洞情报产生，系统将自动触发短信与邮件推送，确保安全负责人即使在非工作时间也能第一时间获取预警信息，立即启动应急响应流程，为修复工作赢得宝贵时间。

- “精准制导”、“行业视图”、“全景视图”三图模式情报供给

1) 人工精编情报：我们的安全专家团队 7x24 小时监控全球漏洞动态，并从中筛选出客户真正需要关注的高风险、可被利用、影响广泛的漏洞，进行深度分析与加工。加工内容包括但不限于：精准的漏洞标签、可立即使用的 POC、详尽的修复方案、风险影响评估等。此模式直接为您呈现“需要立即行动”的短名单，将海量噪音降至几十条关键情报，帮助银行安全团队聚焦关键风险，避免精力分散

2) 全量漏洞知识库：同时，我们提供包含 30 万+条漏洞记录的完备知识库，涵盖您所需要的全部数据字段（如 CVE/CNVD/CNNVD 全编号、CVSS 全版本评分向量、供应商与产品信息、补丁链接等）。此举旨在为银行安全研究人员提供“一站式”查询平台，满足其对历史漏洞、特定组件漏洞的深度调研需求，解决大而全的知识储备问题。

3) 行业漏洞情报：我们为每条漏洞数据都打上了行业标签属性，银行用户

可以根据提供的刷选条件，选择金融行业漏洞，可快速筛选出本行业内出现的高频漏洞，为银行后续的软件采购、现有漏洞的查漏补缺以及供应链的管理提供精准的信息来源。

- 标准化漏洞数据提供了数据智化，漏洞风险可量化的基础条件

360 漏洞情报数据均为可机读可人读的标准化漏洞，所有字段均可对接程序自动化使用。在本案例中，360 漏洞情报对接某银行的 CMDB，漏洞情报平台将标准化、精准化的漏洞情报与银行资产库进行自动化匹配。系统不仅快速定位受影响资产，更结合漏洞公开状态、漏洞利用条件、补丁状态、0day 状态、严重性等级以及银行内部资产重要性标签，自动计算出真正属于本银行的、个性化的漏洞修复优先级。这将帮助银行将紧急修复的漏洞数量科学地控制在极少的范围内，实现从“修复所有漏洞”到“修复关键风险”的战略转变，大幅降低运维工作量。

- 提供信创漏洞应急响应解决方案

随着国产化软件的快速普及，信创软件的安全问题也逐渐凸显重要性。尤其在银行等金融体系中，安装有大量的信创软件。360 漏洞情报在为某银行的漏洞情报服务中，通过漏洞知识库提供了大量信创软件的历史安全风险问题，帮助企业在安全巡检过程中，发现了不少历史版本的漏洞威胁问题。尤其是在某些内部演练过程中，是信创软件漏洞的爆发期，360 漏洞情报以其精准的漏洞情报收集能力以及从海量数据库捕获漏洞情报的能力，快速精准的输出了许多关键情报，针对未知威胁，还提供出了虚拟补丁方案，成功帮助客户抵御了来自各方的安全攻击风险。

用户价值

- 主动防御能力构筑： 将银行的安全姿态从“被动响应”升级为“主动预警”。通过精准、及时的情报供给，建立起对外部威胁的早期发现和快速处置能力，显著提升对 0day 漏洞和新爆发漏洞的免疫力。
- 运营效率倍增与成本节约：“精准制导”情报将安全团队从海量漏洞告警中解放出来，预计可减少 80%以上的漏洞筛选与分析时间，使其能专注于真正的

关键威胁。快速的响应机制能有效降低安全事件发生的概率，每年预计可为银行避免数百万潜在的经济与声誉损失。

- 合规与品牌影响力提升：完善的漏洞情报监测与响应机制，是满足国家及行业监管要求的有力证明。本方案的成功实施，可成为银行在数字化安全领域的最佳实践，助力银行塑造“技术领先、安全可靠”的卓越品牌形象。

案例点评

360 漏洞情报服务，为银行建立了漏洞威胁情报的快速响应长效机制。它不仅仅是一个数据源，更是一个融合了专家智慧、先进平台与高效流程的安全运营核心。通过“三模式”情报供给与多渠道实时推送，该方案确保了从情报感知到预警触发的极致效率。尤为关键的是，它通过精准的风险评估与资产关联，将全局威胁转化为本地化、可执行的修复工单，真正实现了“风险驱动响应”的现代安全运营模式，极大降低了业务系统因已知漏洞而被攻击的风险，为银行业务的连续性与稳定性提供了关键保障。

北京数字世界咨询有限公司（以下简称“数世咨询”）是国内数字化领域独立第三方调研咨询机构，主营业务为网络安全产业领域的调查研究、资源对接与行业咨询。在国内网络安全产业的调查研究领域，无论是专业性还是资源丰富性，均处于业界领先地位。

调查研究方面，撰写发布《中国数字安全大事记》、《中国数字安全能力图谱》、《中国数字安全100强》、《中国数字安全产业年度报告》等业内影响力巨大的公开报告。同时，还为监督机构、国家部委、大型国企等单位提供各种定制化的内部调研报告。

资源对接方面，数世咨询目前已对接国内网络安全企业700余家，以及150余家网络安全投资业务的资本方，建立了频繁且良好的沟通合作关系，包括共同举办会议活动、投资对接，安全产品与企业推荐，企业资源整合等

行业咨询方面，经常性的为监管部门、国家部委、安全企业、安全用户、一二级市场投资机构提供建议、企业培训及专家评审等咨询服务。

公司地址：北京市东城区天鼎218文化金融园东外110号 网安小酒馆
官方网站：www.dwcon.cn
联系邮箱：dw@dwcon.cn

小酒馆

数世咨询
Digital World Consulting
数字安全领域独立第三方调研机构