数世咨询
Digital World Consulting

暗网情报（DWI）能力白皮书

数世咨询
Digital World Consulting

暗网情报（DWI）

能力白皮书

（2026 年 8 月）

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

数世咨询 **刘宸宇**

数世智库 数字安全能力研究院

目 录

关键发现

暗网情报（Dark Web Intelligence，DWI）正处于从「专业小众」走向「主流标配」的关键转折期。对于中国企业和安全产业而言，2026 年是一个标志性的拐点——五个变量的叠加正在将暗网威胁从「可被忽视的远虑」变为「必须正视的近忧」。

第一，AI 拆除了语言屏障。 大语言模型使全球勒索组织和黑客团伙能够快速理解中文数据的商业价值和合规风险，中国市场从「性价比不高」变为「必须拿下的增量池」。2026 年 7 月，国内勒索和商业黑客攻击受害者数量首次进入全球前列——这很可能不是偶发波动，而是一个长期趋势的开端。

第二，合规监管进入强周期。 新《网络安全法》于 2026 年 1 月施行，违法处罚上限从 100 万元跃升至 1,000 万元，直接责任人可终身禁业。暗网数据泄露事件的合规后果已发生质变，暗网情报从「可选的附加能力」变为「合规风险管理的必要组件」。

第三，暗网≠Tor。 当前「轻暗网」（Telegram 等加密社群）与「传统暗网」（Tor 网络中的暗网社群及衍生访问）同样承载着大规模数据泄露贩卖、勒索通知发布和入侵工具流通的主体流量。任何只关注传统暗网或轻暗网中的一个方向，而忽视双生态并行的方案，都存在结构性盲区。同时，中文暗网「混乱邪恶」的独特生态——高噪音、构陷机制、「过程即惩罚」——是国际主流 DWI 框架未曾覆盖的本土特有维度。

第四，IAB 和 Stealer 日志是当前最具预警价值、但在国内认知近乎空白的情报类型。 初始访问权限（IAB）的暗网交易均价在一年内暴涨超 40 倍，且其

出现通常领先实际勒索攻击数周。Stealer 窃密日志中的 Session Cookie 可绕过 MFA，是大多数企业防御体系的结构性盲区。对这两类情报的系统性忽视，意味着企业在攻击链的最上游就已经失守。

第五，从「借船出海」到「护航出海」是中国企业全球化必须跨越的能力门槛。 当供应链暗网数据泄露波及中国 OT 核心资产、当海外分支机构的凭据在暗网流通、当数据跨境合规监管进入深水区——暗网情报不再是可有可无的侦察哨，而是全球化企业安全基础设施的标配组件。

一、背景

长期以来，暗网内中国的数据泄露规模稳居全球前列，但勒索软件受害者数量却始终排在二十名开外，这使得国内企业存在「我们不在靶心」的侥幸心理。**2026 年，三个变量的叠加正在打破这一格局。**

- **AI 拆除了语言屏障。** 大语言模型使勒索组织和黑客团伙能够快速理解中文数据的商业价值和合规风险，中国市场从「性价比不高」变为「必须拿下的增量池」。2026 年 7 月，中国勒索和商业黑客攻击受害者数量首次进入全球前列。
- **合规监管进入强周期。** 新《网络安全法》于 2026 年 1 月施行，违法罚款上限从 100 万元跃升至 1,000 万元，直接责任人可终身禁业。国家安全部于 2026 年 3 月首次就暗网发布专题安全提示。暗网数据泄露的合规后果已发生质变。
- **勒索攻击完成本土化适配。** 「三重勒索」模式——加密赎金+数据泄露威胁+利用《数据安全法》《个人信息保护法》的合规举报杠杆——已在中国落地。企业即使有完备备份体系，也无法摆脱数据泄露带来的合规和声誉双重打击。

从全球范围来看，暗网情报正从「专业小众」走向企业安全能力体系的主流组件。几个典型的例证：

- 传统威胁情报厂商（Recorded Future、Mandiant 等）纷纷增加暗网模块
- Google Threat Intelligence 将 Gemini 大模型同时用于明网和暗网监

控，统一输出（此处特指在谷歌威胁情报平台内部运行的 Gemini 智能体，而非普通的聊天对话式 Gemini）。

- 暗网数据的商业价值——尤其是 IAB 和 Stealer 日志——已被证明是勒索攻击的最早预警信号之一
- 合规监管对数据泄露「证据链」的需求，将暗网情报从「可选」推升为「必选」

与此相对的，暗网情报这一细分领域在国内的能力发展现状到底如何呢?

数世咨询于 2026 年 4 月发布的《暗网情报技术能力框架及参考指标体系》给出了初步判断：**我国在该领域较国际水平存在约 10 年的代差。** 差距体现在三个主要维度：数据覆盖上，国内厂商在非中文论坛的覆盖广度和历史深度上与国际领先水平有明显差距;分析能力上，Flashpoint 等专业公司、Google Gemini 等情报分析 AI 模型的暗网分析准确率均在 90% 以上，而国内仍然依靠个别安全企业的人工经验，少数大模型驱动的语义理解仍属前沿探索阶段；认知上，行业整体将 DWI 等同于「对几个关键站点的关键词告警」，对暗网情报整体能力建设仍然匮乏，例如对 IAB 市场、Stealer 日志、专家谈判等闭环方法论还存在普遍性空白。

当然，差距的另一面是机遇。**国内 DWI 领域具备三个后发优势：** 本土化深度——中文暗网的独特生态是国际厂商难以穿透的天然壁垒；合规驱动——新法实施为 DWI 创造了由法律责任直接传导的刚性需求；AI 赋能——大模型技术为跨越式发展提供了可能，不必重复国际厂商「先积累十年数据、再培养百人团队」的传统路径。

因此笔者认为，可以说 2026 年中国暗网情报这一细分市场开始迎来拐点。

基于此，数世咨询撰写并发布本白皮书，希望提供一份从概念认知到能力框架、从落地方法论到产业全景的暗网情报指南，旨在为中国企业的安全决策者和安全产业的从业者，在这个拐点之年提供清晰的能力坐标和行动参考。

勘误与进一步交流，请联系主笔分析师：刘宸宇 liuchenyu@dwcon.cn。

二、概念描述

2.1 什么是暗网

2.1.1 互联网的「三层结构」

互联网并非一个扁平的整体。按照可访问性和索引状态，通常将互联网划分为三个层次：

- **明网（Surface Web / Clear Web）**：可通过标准搜索引擎索引和直接访问的公开网络空间，构成普通用户日常使用的互联网。约占互联网信息总量的 4-5%。
- **深网（Deep Web）**：无法被通用搜索引擎索引、但可通过标准浏览器直接访问的网络空间。包括企业内部系统、学术数据库、付费内容、医疗档案等合法场景下的非公开资源。深网的规模远超明网。
- **暗网（Darknet / Dark Web）**：需要通过专门软件、配置或授权才能访问的匿名加密网络空间。其核心特征是「隐匿」——既隐匿用户的身份与位置，也隐匿服务器的部署信息。

需要指出的是，「深网」与「暗网」在中文语境中常被混用，但二者有本质区别：深网的核心属性是「不可索引」，暗网的核心属性是「匿名加密」。本报告所讨论的范畴聚焦于**暗网**及其衍生生态。

2.1.2 暗网的协议与技术谱系

暗网并非单一网络，而是由多种匿名通信协议构成的加密网络集合。目前全

球暗网中，常见协议分布大致如下：

协议	占比	特征
Tor （The Onion Router）	98%以上	洋葱路由，多层加密中继。承载绝大多数暗网站点（.onion），包括黑客论坛、数据交易市场、勒索组织站点、匿名图片板等
I2P （Invisible Internet Project）	1-2%	大蒜路由，去中心化设计。主要用于文件分发和内部通讯，暗网站点数量较少
ZeroNet / Freenet	不足 1%	基于 P2P 的去中心化网络。ZeroNet 使用比特币加密和 BitTorrent 分发，Freenet 侧重抗审查的信息存储

Tor 凭借其成熟的洋葱路由机制和相对完善的生态，已成为暗网事实上的标准协议。全球绝大多数暗网威胁活动（黑客论坛交易、勒索软件运营、数据泄露贩卖等）均发生在 Tor 网络之上。

2.1.3 暗网的双生态

随着加密通讯工具的普及与地下产业形态的演进，暗网情报的监测范畴已远超传统 Tor/I2P 网络的边界。数世咨询提出暗网**「双生态」**概念，将暗网情报的覆盖范围划分为两个并行的威胁生态：

Traditional Dark Web（传统暗网）

基于 Tor/I2P 等匿名网络协议构建的「原生」暗网站点。典型载体包括：

- 黑客技术论坛（如 Exploit、XSS 等）
- 勒索软件组织的泄露站（Data Leak Site）

- 数据交易市场
- 匿名图片板（如 6chan 等 chan 系社区）
- MaaS（Malware-as-a-Service）生态平台
- RaaS 与加盟商（affiliate）相关生态系统

传统暗网是核心攻击组织与数据贩卖的策源地，持续输出威胁能力与交易规则。其特点是强匿名、高隐蔽、相对固定的站点结构，访问门槛较高。

Dark Web Lite（轻暗网）

基于加密通讯软件（Telegram、Discord、Signal 等）的封闭社群、私密频道和群组形成的次生地下生态。其访问方式无需传统匿名网络工具，但具备封闭、加密、邀请制、隐蔽交易等特征。

轻暗网与传统暗网互相补充，互有交集，人员结构相互交叉流窜，当前侵公查档、黑灰产协作等交易信息大部分发生在轻暗网中。相对于传统暗网，轻暗网具有以下特征：

- **规模庞大**：Telegram 单一平台即存在数千个威胁相关频道/群组
- **传播快速**：信息可被瞬间转发至数百个关联社群
- **迭代迅速**：频道/群组可被快速创建、废弃、迁移
- **门槛更低**：参与者无需掌握 Tor/I2P 等技术工具

「双生态」的核心判断：传统暗网与轻暗网并非相互替代，而是共同构成规模化、产业化、链条化的地下产业体系。有效的暗网情报能力必须同时覆盖两个生态，任何只关注其一的方案都存在结构性盲区。

2.2 什么是暗网情报（Dark Web Intelligence / DWI）

2.2.1 定义

暗网情报（Dark Web Intelligence，简称 DWI）是指：**从传统暗网及轻暗网的隐藏、加密空间中，通过系统化采集、对抗、分析、研判，将原始数据转化为具备上下文、可支撑业务决策和行动响应的成品情报的完整过程与能力体系。**

这一定义包含三个关键要素：

- **系统化**：DWI 不是偶发性的「逛暗网搜集信息」，而是具备持续采集、标准流程、质量管控和闭环响应的系统工程。
- **转化**：DWI 的核心价值不在于「原始数据量」，而在于将海量碎片化信息转化为经过验证、富上下文、可指导行动的高质量情报。
- **闭环**：DWI 的终点不是「发现威胁」，而是将情报转化为风险压降的实际行动——包括确认威胁真伪、完成证据固定、支撑合规上报、指导整改处置。

2.2.2 DWI 的层级区分

为避免概念泛化，需对暗网情报进行三个层级的区分：

层级	定义	典型产出	价值
暗网信息（Dark Web Information）	从暗网直接采集的原始信息	论坛帖子原文、Telegram 消息截图、数据交易列表	低——未经验证、缺乏上下文
暗网监测（Dark Web Monitoring）	对暗网数据的关键词匹配与	企业域名出现在某论坛、员工邮箱出现在某数据包	中——发现信号但无研判

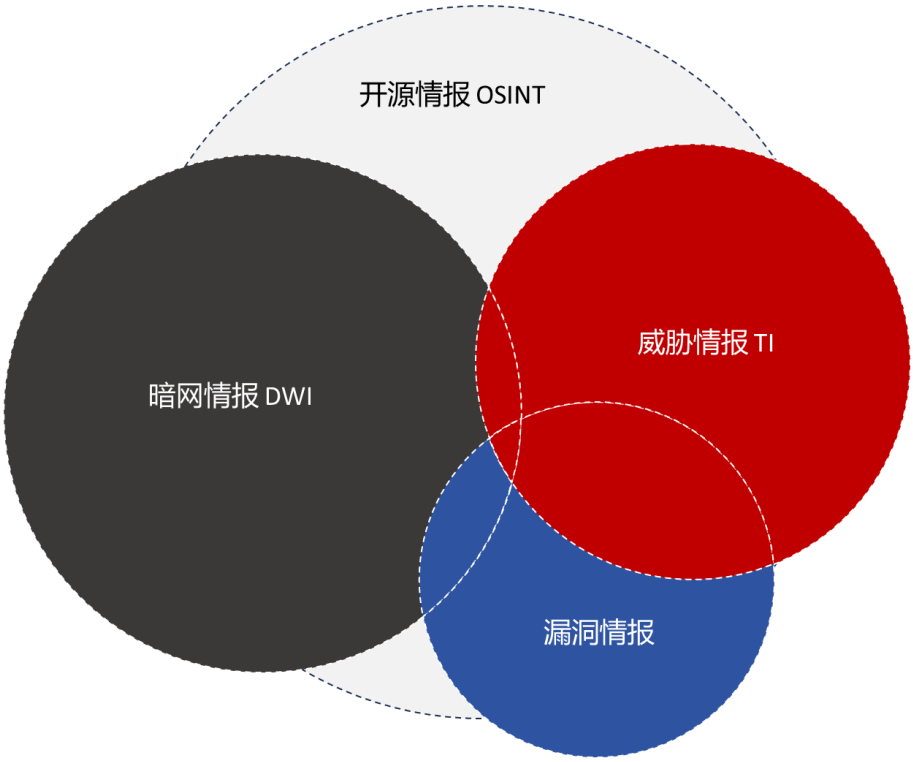
	告警		
暗网情报（Dark Web Intelligence）	经专业研判后的成品情报	完整事件研判报告、归因分析、处置建议、证据包	高——可指导决策与行动

大量声称具备「暗网情报能力」的产品和服务，本质上仍处于「暗网监测」层——能够发现信号，但缺乏验证、分析和闭环处置能力。真正的 DWI 能力必须穿透到第三层。

2.3 DWI 与相关情报概念的区别

暗网情报并非孤立存在，它与开源情报（OSINT）、漏洞情报（Vulnerability Intelligence）和威胁情报（TI）存在紧密又各有边界的关系。准确理解这些情报领域的定位差异，是正确构建情报能力体系的前提。

注：如无特别说明，本报告中所述“威胁情报（TI）”均指“狭义威胁情报”，即：恶意 IP、哈希、样本、流量和终端威胁数据等 IOCs（入侵指标）情报。



- **OSINT 是基础环境**：覆盖面最广、门槛最低，DWI、TI 和漏洞情报均可从公开来源部分获取素材，但各自拥有 OSINT 不可达的独有数据空间。DWI 尤其如此——暗网中的 IAB 交易、Stealer 日志、勒索组织内部讨论均落在 OSINT 范畴之外。
- **DWI、TI、漏洞情报三者并列交叉**：三者的两两交集构成了情报融合的核心价值区。DWI×漏洞情报，覆盖暗网漏洞交易与 Exploit 流通；DWI×TI，覆盖攻击者虚拟身份追踪与归因线索；TI×漏洞情报，覆盖攻击者正在利用的具体漏洞及 TTPs 映射。
- 三者的共同交集则代表了**最高价值的情报融合场景**：某攻击团伙（TI）正在暗网（DWI）出售针对特定漏洞（漏洞情报）的完整 Exploit，且目标行业与企业资产清单匹配。
- **OSINT 包裹但不替代**：OSINT 虚线外框包裹三者，表示公开来源为所有情报活动提供基础数据环境，但核心的差异化价值产生于 OSINT 不

可达的交叉地带。

下面我们来看 DWI 与相关情报概念的具体区别。

2.3.1 DWI 与开源情报

开源情报（Open Source Intelligence，OSINT）是指从公开可用来源（公开网站、社交媒体、新闻报道、学术论文、公共数据库等）系统性收集和分析信息的情报学科。其核心特征是「公开可获取」——情报来源不涉及非法访问或突破访问控制。

DWI 与 OSINT 的核心差异在于**数据源的访问属性**：

维度	OSINT	DWI
数据源性质	公开，无需特殊工具	隐藏/加密，需 Tor 等专用工具
典型来源	社交媒体、公开网站、GitHub	.onion 站点、Telegram 私密频道、I2P 网络
覆盖内容	品牌提及、公开漏洞信息、暴露面资产	泄露凭据/会话、IAB 列表、勒索通告、地下交易
法律边界	完全合法	数据采集需严格合规操作

核心关系：OSINT 覆盖面最广，但深度不足。暗网和轻暗网中流通的关键威胁信息——数据售卖/交易/发布、IAB 出售的企业访问权限、Stealer 日志中的 Session Cookie、勒索软件的泄露数据——均无法通过 OSINT 获取。DWI 填补了 OSINT 在「隐蔽威胁空间」中的情报空白。

2.3.2 DWI 与威胁情报

威胁情报（Threat Intelligence，TI）收集、分析和传播有关攻击者的特征信息，涵盖攻击者身份、动机、能力、技战术（TTPs）及攻击指标（IOCs）等内容。TI 回答的核心问题是「谁在攻击、为什么攻击、用什么手法攻击」。

DWI 与 TI 之间存在**显著且双向的交集**：

维度	TI（攻击者情报）	DWI
核心关注	攻击者是谁、TTPs、动机、归因	暗网/轻暗网中所有与威胁相关的信号
典型数据源	公开威胁报告、恶意软件分析、蜜罐、行业共享	暗网论坛、Telegram 私密频道、地下市场、勒索站点
对另一方的价值	提供分析框架（MITRE ATT&CK、钻石模型）为暗网追踪提供结构化认知坐标	提供 OSINT 不可达的攻击者行为数据——虚拟身份、交易记录、招募帖、攻击成果炫耀

DWI 是 TI 的关键上游供给。攻击者在暗网论坛中的活动——如虚拟身份注册与维护、TTPs 讨论、攻击工具交易、勒索成果炫耀、招募加盟商——构成了攻击者画像最丰富的数据来源之一。尤其是「暗网人格→现实身份」的映射追踪，高度依赖对暗网虚拟身份的长期监控和跨平台关联分析。但完整的 TI 还需融合更多一线情报源，例如：

- 内部遥测：EDR/NDR/SIEM 产生的内部威胁信号
- 技术情报（TECHINT）：恶意软件逆向分析、漏洞研究
- 人力情报（HUMINT）：行业信息交换、攻击者访谈

2.3.3 DWI 与漏洞情报

漏洞情报（Vulnerability Intelligence）是对已知和潜在安全漏洞的系统性收集、分析和预警，涵盖 CVE 漏洞公告、PoC（概念验证代码）、Exploit（利用代码）、漏洞利用趋势和 0day 交易动向等。

DWI 与漏洞情报的核心差异在于**覆盖的漏洞类型和信息层级**：

维度	漏洞情报	DWI
主要来源	公开漏洞库（NVD/CVE）、安全研究、厂商公告	暗网论坛、Telegram 私密频道、地下交易市场
覆盖重点	已披露漏洞的全生命周期管理、CVSS 评分、资产影响面分析	暗网中流通的 0day/NDay 交易、漏洞利用工具买卖、Exploit 租赁服务
时间特征	以漏洞披露日为基准的持续跟踪	以暗网首次出现为基准的早期发现
核心价值	支撑漏洞优先级（VPT）和补丁管理	发现尚未公开或未受关注的「在野」漏洞利用

两者的交叉与互补。 暗网是漏洞交易——0day 漏洞交易和 Nday 自动化攻击工具——的重要流通渠道。漏洞情报体系如果缺乏 DWI 输入，将存在一个明显的盲区：无法感知那些尚未进入公开漏洞库、但已在暗网中明码标价的漏洞利用。反过来，DWI 中发现的漏洞交易信号，也需要漏洞情报体系提供 CVSS/EPSS 评分、受影响产品和版本范围等上下文，才能完成从「暗网发现一个漏洞在卖」到「这个漏洞对企业意味着什么」的研判闭环。

2.3.4 DWI 与其他易混概念

舆情监控

舆情监控关注公开社交媒体、新闻资讯等渠道的品牌声誉、舆论动向和负面信息传播，主要面向 PR、品牌和合规部门。DWI 与舆情监控在数据源上有少量交叉（如 Telegram 公开频道），但本质截然不同：舆情监控发现的是「人们在公开说什么」，DWI 发现的是「攻击者在暗处做什么」——数据泄露交易、勒索通告发布、IAB 权限挂牌、侵公查档服务。前者关注品牌形象，后者关注实质性安全威胁。将 DWI 等同于「暗网版的舆情监控」是常见的认知错误。

网络空间测绘

网络空间测绘关注互联网资产的主动发现与拓扑映射——IP、域名、端口、服务、组件版本、证书等——核心回答「我有什么暴露在外面」。测绘是攻击者视角的资产清点，DWI 则是攻击者行为的情报感知。两者互补：测绘表明攻击面长什么样，DWI 表明攻击面中哪些部分已经在暗网上被挂牌出售或讨论。但测绘不构成 DWI 成立的前提，一个企业即便没有完整的资产测绘，暗网上出现的以其域名为关键词的泄露数据依然是有效情报。

攻击暴露面管理（EASM）

攻击暴露面管理（External Attack Surface Management）关注互联网暴露资产的持续发现、风险评估与收敛，外延比网络空间测绘更广——涵盖云资产、影子 IT、第三方暴露、证书透明日志等。EASM 与 DWI 的关系可以概括为：EASM 表明「哪些门开着」，DWI 表明「哪些门已经被撬过」。两者是独立但可互补的能力域：EASM 不依赖暗网数据即可运作，DWI 的闭环处置也不以 EASM 为前提。实践中，EASM 发现的暴露面清单可以为 DWI 的资产关联匹配提供上下文，但两者的能力建设路径和评估标准应各自独立。

2.4 中文暗网的特殊性

全球暗网生态并非铁板一块。不同语言区、不同文化背景的暗网社区，呈现出截然不同的生态特征和行为逻辑。理解中文暗网的独特性，是构建有效本土 DWI 能力的关键前提。

2.4.1 混乱邪恶，而非秩序邪恶

借鉴角色扮演游戏中的阵营体系，可将暗网社区的生态特征分为两极：

秩序邪恶（Lawful Evil）

以 Exploit、XSS、RAMP/Tier1 等俄语/英语高信任度黑客论坛或邀请制平台，以及勒索组织生态为代表。核心特征：

- 存在明确的**信誉体系**：交易评价、担保人制度、卖家等级
- 有**层级化组织**：管理员、版主、认证卖家、普通用户
- 行为**可预期**：遵循社区规则，追求长期商业利益
- **可直接画像**：通过交易记录、互动模式、语言风格构建攻击者数字档案

「秩序邪恶」社区更接近有组织犯罪的「企业化」运作——有规则、有信誉、有层级。国际主流 DWI 厂商（Flashpoint、DarkOwl）的分析方法论很大程度上建立在此类生态之上。

混乱邪恶（Chaotic Evil）

以串子会、6chan、夜上海等中文匿名图片板和大量无规则 Telegram 黑灰产社群为代表。核心特征：

- **无信誉体系**：不在乎评价，每个账户可能只发一条信息
- **碎片化**：信息高度离散，缺乏结构化组织形式

- **强情绪驱动**：以发泄、构陷、极端言论为主要行为模式，商业逻辑弱
- **高噪音**：约 90%内容为无价值或虚假信息

中文暗网社区整体偏「混乱邪恶」。显然这种生态具备其独特性，在国际主流 DWI 框架中缺乏对应分析维度。当然，如前言所说，这也是中国 DWI 厂商的机会所在。

2.4.2 过程即惩罚

中文暗网「混乱邪恶」生态中，一种独特的危害机制值得特别关注，单独阐述——**「过程即惩罚」**。

其运作模式如下：攻击者（或构陷者）在匿名平台发布极端言论、虚假威胁，或以他人名义宣称实施危害行为。即使被构陷者最终自证清白，调查过程中已承受实质性代价：被监管部门约谈、电子设备被检查取证、所在单位知情、社会关系受损。

这一机制的核心危害不在于「最终定罪」，而在于 **「从被举报到自证清白」这一过程本身就是惩罚**。它是一种低成本、高伤害、利用监管反应机制实施的匿名攻击手段。

此类威胁超出了传统网络安全的分析框架——它不涉及漏洞利用、恶意代码或数据加密，却可能对个人和企业造成严重的人身安全、声誉影响。识别和应对这一类威胁，需要 DWI 能力具备对中文匿名社区亚文化、语言习惯和攻击模式的深度理解。

2.4.3 建立有限路径，而非全部根除

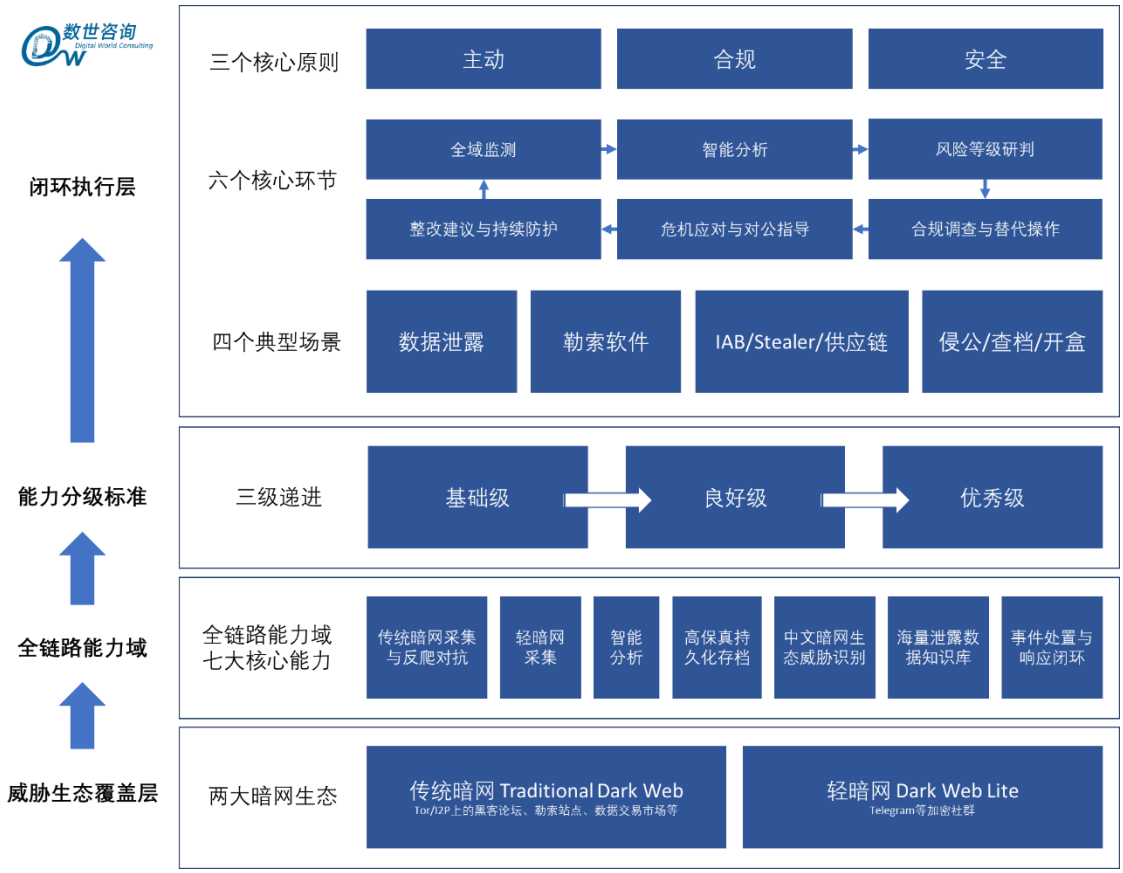
面对中文暗网「混乱邪恶」生态，情报工作的目标不应该是「根除」（技术上不可能，操作上不现实），而应该建立**有限路径**：

- **持续高频采集**：对关键匿名社区的 7×24 不间断监测
- **高保真持久化存档**：原始内容的完整镜像保存，确保可追溯
- **实体提取与关联**：从碎片化信息中提取发布者标识、关联账号、时间序列等可分析要素
- **AI 辅助分级分类**：利用大模型对海量噪音进行自动化筛选，识别高价值信号

中文暗网情报工作的核心，不在于追求「全部处置」或「彻底清除」，而在于在高噪音环境中建立可依赖的识别、存档、关联与分类能力——让有限的研判资源聚焦于真正的威胁信号。

三、能力框架与要点

暗网情报（DWI）作为一项系统工程，需要一套从采集到闭环、从技术到方法论的全链路能力体系。



3.1 能力框架全景图

暗网情报能力框架的设计遵循三项核心原则：**系统性**——覆盖「采集—对抗—分析—存档—治理—响应」的完整闭环；**实战性**——聚焦数据泄露、IAB 交易、勒索软件、RaaS、侵公威胁等本土高发风险；**独立性**——明确暗网情报专属技术边界，区别于通用威胁情报分析框架。

基于上述原则，框架由四个层次构成：

第一层：威胁生态覆盖层。 能力构建的起点是明确「覆盖什么」。暗网情

报需要同时覆盖两大威胁生态——Traditional Dark Web（Tor/I2P 上的黑客论坛、勒索站点、数据交易市场）与 Dark Web Lite（Telegram 等加密社群）。双生态并非相互替代关系，而是共同构成产业化、链条化的地下威胁体系。本报告第二章已对双生态进行了概念层面的阐述，此处不重复展开。

第二层：全链路能力域。框架文档将暗网情报能力划分为七大核心能力域：传统暗网采集与反爬对抗、轻暗网采集、智能分析、高保真持久化存档、中文暗网生态威胁识别、海量泄露数据知识库、事件处置与响应闭环。

第三层：能力分级标准。框架文档为每项能力域设定了基础级→良好级→优秀级的三级递进标准，为能力评估和建设提供可量化的参考基准。

第四层：闭环执行层。能力框架的最终落脚点是「落地」。闭环执行层定义了从发现到处置的完整工作流：六环节（全域监测→智能分析→风险等级研判→合规调查与替代操作→危机应对与对公指导→整改建议与持续防护）× 三原则（主动、合规、安全）× 四场景（数据泄露、勒索软件、IAB/Stealer/供应链、侵公/查档/开盒）。

阅读指引：框架文档与本白皮书的关系

数世咨询联合行业多家机构发布的《暗网情报技术能力框架及参考指标体系》（下称「框架文档」）已对暗网情报的技术能力域划分、分级标准、指标体系做了系统性阐述。框架文档侧重回答**「体系长什么样」**——构建能力评估的完整标尺。

本白皮书在此基础之上，侧重回答**「怎么落地」**——聚焦闭环方法论、被忽视的实战要点和行业认知偏差。两者互补衔接：框架文档提供全景坐标系，本白皮书在此坐标系中标注关键路径和常见陷阱。

因此，本章对已在框架文档中详述的内容仅做概要回顾与索引（3.2 节），将主要篇幅留给闭环方法论（3.3 节）和被业内长期忽视的关键要点（3.4 节）。

3.2 能力框架核心要素

以上四层框架的完整定义和技术指标，框架文档已有详尽阐述。本节仅就其中与「落地」密切相关的几个核心要素做概要回顾。

3.2.1 双生态覆盖的落地挑战

双生态覆盖在落地层面各有不同的技术难题。**传统暗网采集**的核心挑战在于反爬对抗——核心论坛（Exploit、XSS 等 Tier1 站点）部署的多层验证和封禁机制要求采集方具备跨协议爬虫引擎、浏览器指纹伪装和分布式节点轮换等对抗能力。采集能力的核心衡量指标是 **New Post 每日采集量**，反映的不是「采集了多少历史数据」，而是「对当下正在发生的讨论和交易的感知能力」。**轻暗网采集**（以 Telegram 为核心）则面临规模、速度、隐蔽、格式四重挑战：数千个频道/群组的优先级筛选、毫秒级转发扩散的时效压力、私密群组的审核门槛、文本/图片/文件/语音的多模态处理需求。

3.2.2 七大能力域及其落地定位

能力域	在落地中的定位	关键落地挑战
传统暗网采集与反爬对抗	全链条起点，Tier1-3 站点分级覆盖	反爬对抗持续升级、核心站点波动频繁、虚拟身份长期维护
轻暗网采集	体量最大、实时性最强的威胁信息流	账号风控、私密群组准入、海量消息优先级筛选、多模态解析
智能分析	「看得懂」：实体提取、分级分类、知识图谱、趋势预测	知识图谱国际顶级也仅半自动化；暗网黑话与代码词是 AI 的硬挑战

持久化存档	暗网信息易失性极高，取证溯源和合规上报的刚性需求	页面渲染态保存、关联上下文完整保留、加密存储与审计追踪
中文暗网生态识别	最具本土特色，应对中文暗网亚文化独有挑战	混乱邪恶社区识别、「过程即惩罚」机制理解、构陷与真实威胁交叉验证
泄露数据知识库	判断「新/旧/真/假」直接影响事件优先级和响应方式	历史数据积累规模、跨源去重准确率、资产关联精度
事件处置与响应闭环	框架的最终指向——将情报转化为实际风险压降	行业认知偏差普遍（详见 3.3 节）

3.2.3 能力分级的设计意图

框架文档提出的三级分级标准（基础级→良好级→优秀级），其设计意图不在于罗列技术指标，而是为行业提供两重价值：**对于采购方**，可以基于自身风险状况和预算合理设定能力建设目标，不必追求「一步到位」；**对于服务提供方**，拥有清晰的进阶路线图，每一级的跃升对应明确的能力增量——以传统暗网采集为例，从 Tier3 到 Tier2 再到 Tier1 的覆盖升级，背后是反爬对抗、虚拟身份维护、分布式节点调度等能力的逐级跃升，而非简单的「多爬几个站」。完整的分级指标和评估细则请参阅框架文档。

参考来源：七大能力域的完整定义、技术架构、各层级能力指标和评估细则，详见《暗网情报技术能力框架及参考指标体系》（数世咨询，2026 年 4 月发布）。

3.3 闭环落地方法论

闭环是暗网情报能力框架的最终指向，也是当前行业认知偏差最严重的环节。

3.3.1 两个常见认知偏差

偏差一：将「采集广度」等同于「全部能力」。 部分厂商以「覆盖了多少个暗网站点」「采集了多少 TB 数据」作为能力衡量的核心指标。但采集量不等于情报质量，数据体量不等于行动价值。真正决定 DWI 能力水平的，是「从海量数据中提取高价值信号并转化为行动」的完整链条——采集只是起点，而非终点。

偏差二：将「闭环」等同于「系统对接」。 一种普遍的误解是：暗网情报的闭环就是「把暗网监测平台与客户内部资产管理系统、漏洞扫描器、SIEM 打通」。实际上，暗网情报的领域独立性决定了：资产测绘、漏洞扫描、网络空间测绘等能力不构成闭环成立的前提条件。闭环的本质，是帮助客户在零风险前提下完成**「威胁确认→研判→证据固定→合规上报→整改」全过程**，并以完整证据链与监管可上报为交付标准。

3.3.2 闭环的六环节与三原则

一个完整的暗网情报处置闭环由六个环节串联而成：

全域监测，覆盖传统暗网与轻暗网，持续发现与客户资产关联的威胁信号。

智能分析，对监测信号进行实体提取、情报分级和真伪初判。

风险等级研判，这是闭环的真正起点，对信号进行深度验证：真还是假？新还是旧？来源是哪？据此确定风险等级和处置优先级。

合规泄露源调查与替代操作，在合法合规框架内完成对暗网情报源的进一步

调查；如果涉及需要主动接触暗网主体（如确认数据真实性需联系交易方），由专业团队替代客户完成所有高危操作，客户全程零接触。

危机应对与全流程对公指导，在勒索、数据泄露等高紧迫场景中，提供从谈判策略到监管上报的全流程指导。

整改建议与持续防护，基于事件根因提出整改建议，并将该事件涉及的威胁实体纳入持续监控范围。

贯穿这六个环节的是闭环的三项核心原则：

主动原则，不是「发现信号→甩给客户自行处置」，而是情报方主动承担研判和处置的专业工作；

合规原则，所有操作必须在法律框架内进行，不要求客户注册暗网账号、不引导客户访问高危环境、不代理客户进行缴费或交易；

安全原则，客户全程「零接触、零风险、零暴露」，所有涉及高危环境的操作由专业团队在隔离环境中替代完成。

3.3.3 四类场景的差异化处置

不同威胁类型需要不同的闭环策略，不可一概而论：

场景	核心问题	处置重点	特殊考量
数据泄露	真假？新旧？来源？	数据样本验证、新旧比对、泄露源头追溯	涉及个人信息时需同步评估个保法/数安法合规风险
勒索软件	是否已加密？数据是否已外泄？	勒索组织身份确认、谈判策略建议、监管上报指导	高紧迫性+合规敏感性，需第一时间启动对公指导

IAB/Stealer/供应链	哪些凭据被泄露？影响范围？	凭据有效性研判、资产关联匹配、重置/撤销指导	批量性、隐蔽性、长期性——需建立持续监控而非单次响应
侵公/查档/开盒	真伪？是否属于构陷？	内容真伪验证、负面影响评估、对公响应指导	中文暗网特有场景，合规与舆情双风险，需谨慎处置

3.4 被业内忽视的关键要点

暗网情报领域存在若干在国内安全行业中长期被忽视、但在国际实践中已被证实具有核心价值的议题。本节聚焦四个最值得关注的方向。

3.4.1 Stealer

传统安全行业习惯将 Stealer（窃密木马）归类为「终端恶意软件」的一种，属于木马大类，与病毒、蠕虫并列。但在暗网情报的视角下，这一归类掩盖了 Stealer 的真正本质。**Stealer 并非只是传统意义上的终端恶意软件，而是暗网凭据经济的标准化商品生产基础设施。** 其产物——「窃密日志」（Stealer Logs）——包含浏览器保存的密码、Cookie、会话令牌、密码管理器数据、加密钱包信息等，是后续账号接管（ATO）、初始访问代理（IAB）、勒索攻击的关键上游入口。

Stealer 已形成 **MaaS（恶意软件即服务）的专业产业化生态**：开发者以订阅为主、买断为辅的方式出售 Stealer 工具（主流版本月费上百美元，低门槛版本低至数十美元），运营者通过恶意广告、SEO 投毒、破解软件分发等方式部署，

产出的窃密日志在暗网市场和 Telegram 频道中批量交易，购买者从中提取企业 VPN 凭据、SSO 会话令牌等并转售给 IAB 或下游勒索组织。这一生态的关键拐点在于 MaaS 化——它将 Stealer 的攻击门槛从「需要改造恶意代码」降低到「需要一张信用卡」。

企业传统防御体系对窃密日志在暗网中的持续流通存在**结构性盲区**，主要体现在三个层面：第一，**Session Cookie 可绕过 MFA**——Session Cookie 是用户完成全流程认证后的已生效会话凭证，攻击者将其导入反检测浏览器，伪造浏览器指纹并搭配对应地区代理 IP，直接访问企业 SaaS 应用即可跳过登录环节、不触发任何 MFA 提示，传统检测系统会将此类访问识别为正常用户行为。第二，**直接感染对象往往是员工个人设备**——Stealer 通常通过员工个人设备（家用电脑、个人手机）感染，企业安全团队对这类感染往往无感知。第三，**常规密码轮换策略无法覆盖**——即使企业实施了严格的密码轮换策略，窃密日志中的 Session Cookie 在有效期内仍可被直接利用。将 Stealer 日志纳入暗网情报的持续监控范围——从 TB 级原始日志中提取与企业资产关联的凭据信号——是弥合这一盲区的关键步骤。

3.4.2 IAB

IAB（Initial Access Broker，初始访问经纪人）是暗网犯罪供应链中专门出售企业网络访问权限的中间商。他们通过 Stealer 日志购买、漏洞利用、钓鱼攻击、弱口令爆破等手段获取企业网络的初始入口，然后在暗网论坛上将这些访问权限打包出售给勒索软件加盟商（Affiliate）或其他攻击者。IAB 之所以被称为「最具预警价值的信号」，原因在于其**时间差**——IAB 列表的出现通常领先实

际勒索软件攻击数周，如果企业能在暗网 IAB 交易帖中发现自己的访问权限被挂牌出售，就获得了宝贵的响应窗口。

然而，**IAB 在国内信息安全行业中的关注度极低**。多数安全团队对勒索软件的认知停留在「备份」「隔离」「MFA」「EDR」等通用最佳实践层面，但这些措施对于阻止一个手握合法访问凭据的已登录用户几乎没有意义。了解 IAB 生态的运作逻辑、建立对 IAB 交易帖的持续监控，是弥合这一认知空白的起点。

3.4.3 谈判、证据固定与对公指导

国内安全行业对「事件处置」的认知模式，很大程度上来自病毒/恶意软件时代的经验积累——杀毒、隔离、清除、恢复。但**暗网情报处置的逻辑与此完全不同**。处置对象不再是恶意代码，而是已发生的入侵事实和已外泄的数据；核心动作不是清除和恢复，而是谈判、研判、证据固定和上报；时间窗口也不再是「发现后立即执行」，而是需要策略性判断——有时「等待评估和研判结果」比「立即实施处置行动」更有利于控制损失。

以勒索软件为例，2025-2026 年的勒索攻击已从「双重勒索」（加密赎金+泄露威胁）升级为**「三重勒索」**：第一层是加密赎金；第二层是数据泄露威胁（拒绝支付则公开发布）；第三层是利用《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》等法规，以「向监管部门举报数据泄露」为杠杆，对企业施加额外的合规和声誉打击。这第三层压力是中国特有的合规环境赋予勒索组织的额外杠杆，而国内多数应急响应预案尚未覆盖这一维度。

真正有价值的暗网情报处置闭环，应该能够系统性地回答一系列实战问题：被勒索的数据是否真实？是否涉及个人信息和监管上报义务？人力情报实施策

略和时机如何选择？如何在不访问暗网、不直接接触攻击者的情况下完成证据固定？向监管机构上报的材料和流程是怎样的？能够回答这些问题——并在操作层面支撑客户完成全流程——才是 DWI 闭环能力的真正体现。

3.4.4 从威胁信号到有效行动

暗网情报领域存在一个看似矛盾的现象：**企业并非缺乏威胁信号，而是面对大量信号时无法有效转化为行动**。这种「行动鸿沟」——信息已到达但行动未发生——可能比「数据缺失」更致命。

鸿沟的根源在于攻击方与防御方之间严重的**节奏错配**。攻击方一侧，Stealer 感染→日志提取→暗网市场上架，全流程可在 24-48 小时内完成工业化流转；防御方一侧，收到情报→内部验证→确认有效性→讨论方案→启动行动，决策周期以天甚至周计。这一节奏错配的根源不是技术问题，而是四类系统的认知偏差：**将威胁情报等同于漏洞验证**，要求「证明凭据还能登录」才认可情报价值，将情报降维为渗透测试；**过度追求确定性**，排斥概率性判断，在等待「100%确认」的过程中错失响应窗口；**价值标准错位**，用「即时可利用性」替代「早期风险暴露」作为评价标准，忽视情报的预警价值；**对 Session Cookie 等强信号认知不足**，注意力仍集中在「密码是否正确」，忽视有效会话令牌可绕过 MFA 这一事实。弥合行动鸿沟需要三个层面的同步调整——认知层面从「验证有效才行动」转向「基于风险信号快速响应」，能力层面补齐对窃密日志的持续可见性与企业资产关联匹配能力，服务层面明确情报方与客户方的责任边界：情报方负责发现、关联、优先级排序，客户方负责基于信号启动内部处置。

四、代表企业

全球暗网情报领域已形成差异化竞争的格局。本章选取四家具有代表性的企业进行介绍——美国两家（Flashpoint、DarkOwl）、韩国一家（S2W）、中国一家（零零信安）——分别覆盖全域情报平台、暗网数据引擎、AI 多域交叉分析和本土化深度洞察四种典型模式。选型依据是技术路线的代表性和区域覆盖的完整性，不构成任何形式的排名或推荐。

4.1 Flashpoint：全域风险情报的黄金标准

Flashpoint 成立于 2010 年，总部位于纽约，2021 年被 Audax Private Equity 收购多数股权，目前以私募股权旗下公司形式运营。总融资超 8000 万美元，当前（2026 年）估值约 5.25 亿美元，约 350-414 名员工，年度 ARR（经常性订阅收入）约 9500 万美元。在全球暗网情报领域，Flashpoint 被公认为行业黄金标准。

核心模式：技术与人力情报的混合体。 Flashpoint 的核心方法论不是单纯的数据采集，而是「技术自动化+人类分析师」的双引擎驱动。其数据引擎覆盖 3.6PB 以上的暗网、欺诈和漏洞数据，同时配备覆盖超 40 种语言的 100 多名专业情报分析师，7×24 小时驻守暗网论坛和市场。这些分析师的核心价值在于：识别黑话、确认身份、追踪资金流向，以及最关键的能力——将技术层面的威胁发现（「某论坛在倒卖你公司的数据库」）翻译成业务主管理解的风险语言（「这可能导致品牌声誉受损、客户流失和监管罚款」），并提供可执行的处置建议。

产品矩阵。 旗舰平台 Ignite 定位为一体化的全域风险情报平台，横跨网络

威胁情报（CTI）、漏洞情报、欺诈情报、物理安全情报、品牌保护和国家安全六大领域。通过 2022 年收购 Risk Based Security（获得漏洞数据库 VulnDB）和 Echosec Systems（获得 OSINT 与地理空间情报能力），Flashpoint 完成了从纯暗网情报向「全域风险情报」的战略跃迁。

市场地位。 服务于 800 多家企业和政府机构客户，覆盖金融服务、科技、能源、医疗和国防等关键行业。多家行业分析机构将其评为领域领导者。核心竞争壁垒在于多域融合的广度——能将网络威胁、物理安全、欺诈和地缘政治等不同维度的情报交叉关联，产出单一领域情报无法提供的洞察。

在能力框架中的参照意义。 Flashpoint 代表的是 DWI 的「天花板」——全域覆盖、分析师驱动、成品情报交付。其能力的核心不在于数据体量，而在于「翻译」能力：将海量暗网原始数据经严格研判转化为支撑业务决策和物理行动的成品情报。

4.2 DarkOwl：暗网原始数据引擎

DarkOwl 成立于 2009 年，总部位于科罗拉多州丹佛，是独立运营的精干型企业（员工约 31 人，分布在四大洲）。总融资超过 1600 万美元，当前（2026 年）估值约 3300 万美元，年度 ARR 370 万美元。与 Flashpoint 的「情报平台」定位形成鲜明对照，DarkOwl 走的是「数据引擎」路线。

核心模式：纯数据驱动。 DarkOwl 不配备分析师团队，不输出成品情报。其核心产品 Vision 本质上是一个暗网搜索引擎——索引了超过 10 亿份文档，提供 8 年以上的历史暗网归档数据，支持布尔/正则查询和 47 种语言的全文检索。用户（通常是威胁猎人、数字取证专家和执法调查人员）通过 Vision 自行检索

和研判暗网数据。另有 DarkMart 数据库追踪 81 个暗网市场的 38.7 万个商品列表，Vision API 供 SOC 和安全工具直接集成暗网数据。

与 Flashpoint 的互补关系。 Flashpoint 提供的是「经专家加工后的精炼情报」，DarkOwl 提供的则是「最大体量的原始暗网底层数据」。两者的关系并非竞争而是互补——在典型的安全能力堆栈中，Flashpoint 适合战略决策和态势感知场景，DarkOwl 适合深度取证、事件响应和威胁狩猎等需要原始数据支撑的实战场景。

在能力框架中的参照意义。 DarkOwl 代表的是 DWI 的「基础设施层」——不输出判断、只提供数据。这种模式的价值在于：在暗网信息高度易失的环境下，持续稳定地提供可检索的历史数据本身就是一种稀缺能力。对于具备自建分析能力的大型安全团队，这种「原始数据许可」模式比「黑箱式情报订阅」更具灵活性。

4.3 S2W：亚洲唯一的上市暗网情报公司

S2W（原名 S2W Lab）成立于 2018 年，总部位于韩国京畿道城南市，2025 年 9 月在韩国 KOSDAQ 创业板上市（股票代码：488280），是亚洲唯一以暗网情报为核心业务的上市公司。IPO 发行价 13,200 韩元，公开认购竞争率高达 1,972:1，上市首日股价暴涨约 80%，最高市值 1.76 亿美元，当前市值 6000~8000 万美元，员工约 100 人，年收入 708 万美元。

核心模式：AI 驱动的多域交叉分析。 S2W 的技术路线以知识图谱为核心，将暗网、Telegram 加密社群、社交媒体和虚拟资产交易所四个数据域进行跨域关联分析。这种技术路线在理念上接近 Palantir 的 Ontology 方法论——将不同

维度的实体（暗网账户、Telegram ID、区块链地址、社交媒体账号）编织成可追溯的关系网络。S2W 还开发了专门针对暗网内容训练的 AI 模型 DARK-BERT，用于暗网文本的语义理解和实体识别。

产品与营收。 旗舰产品 XARVIS 面向政府、执法、国防和情报机构，是 AI 驱动的网络犯罪情报平台，在 2020 年韩国「N 号房」事件中发挥了关键技术支持作用。企业级产品 QUAXAR 集数字风险保护（DRP）、威胁情报（TI）和攻击面管理（ASM）于一体，定位为「现金牛」业务。2025 年营收约 100.9 亿韩元，海外营收占比从 2022 年的 0.2%快速攀升至约 21%，日本分公司已于 2025 年成立。

在能力框架中的参照意义。 S2W 代表的是 DWI 的「跨界融合」方向——不仅覆盖暗网和轻暗网，还将区块链资金流纳入关联分析。这种多域交叉能力在追踪勒索软件赎金流向、虚拟资产洗钱和国家级攻击组织等方面具有独特优势。从企业发展的角度，S2W 的上市也标志着暗网情报作为一个独立赛道获得了公开资本市场的认可。

4.4 零零信安：中国暗网情报的实战派

零零信安成立于 2020 年，总部位于北京，2021 年获奇安基金千万级人民币天使轮独家投资。作为中国暗网情报领域的先行者，零零信安的定位是「本土化深度洞察 + 闭环落地」的实战派。

核心模式：本土化+AI 双轮驱动。 零零信安的核心技术能力体现在三个层面。采集层，「视界」跨协议蜘蛛爬虫引擎是国内首个能同时爬取高防黑客社群（XSS/Exploit 等）、勒索组织站点、黑客论坛和暗网交易市场、Telegram 频道

/群组、互联网暴露面、APP/小程序和 GitHub 等的跨协议爬虫系统。分析层，「风筝」（KITE）系统是专门处理暗网非结构化数据的 AI 知识分析引擎，结合神经网络驱动的自动化标签系统和专业人工审核。数据层，截至报告期已积累暗网情报 325 万条以上、Telegram 消息 13 亿条以上、泄露数据 216 亿条以上。

行业贡献。 零零信安是《暗网情报技术能力框架及参考指标体系》的主要起草单位，在闭环方法论、暗网监测实战、暗网威胁行为者画像和归因、Stealer 与 IAB 的专题研究、中文暗网亚文化分析等领域输出了系统性内容。其坚持的「客户零接触、零风险、零暴露」闭环原则——由专家团队替代客户完成所有高危操作——为行业提供了一套可参照的专业伦理标准。

差异化优势。 在国际竞争维度下，零零信安的核心壁垒在于对中文暗网生态的深度洞察——国际厂商难以穿透的中文暗网特有语境、术语、俚语和行为模式，是零零信安的天然护城河。在国内竞争维度下，其先发优势体现在数据的持续积累、闭环方法论的系统性和行业标准的话语权三个方面。

市场表现。 已服务上百家头部单位，覆盖政府、监管机构、金融、运营商、能源、制造、科技、互联网等行业。入选 Gartner《Hype Cycle for Security in China》代表厂商（2022 年）、IDC Innovator《中国攻击面管理技术》代表厂商（2023 年），并获数世咨询《新质・数字安全专精百强（2026）》「暗网情报」新赛道收录。

五、未来展望

暗网情报产业的未来走向，取决于监管环境、技术演进和全球化进程三个变量的交汇。

5.1 法律法规的健全与合规驱动

新《网络安全法》于 2026 年 1 月施行。 处罚力度的数量级大幅跃升（一般违法 5-50 万，特别严重后果最高 1,000 万），个人责任终身追溯（刑事处罚者终身禁业），其与《数据安全法》《个人信息保护法》的协同联动，共同推高了违法成本。在这一环境下，暗网情报从「可选的能力建设」变为「合规风险管理的必要组件」——企业是否能够证明已尽到合理的安全监测义务，将直接影响处罚认定。国家安全部 2026 年 3 月首次就暗网发布专题安全提示（「不访问、不自曝、不交易、不轻信」），标志着暗网威胁已从行业议题上升为国家安全关注维度。数据跨境合规执法同步进入深水区，出海企业面临的「一带一路」沿线国家法规高度分化，进一步增加了合规的不确定性。**国内监管收紧是 DWI 需求增长最确定的驱动力，出海安全的最终爆发不靠企业自觉，而靠合规压力。**

5.2 AI 双刃剑，攻击武器化与防御智能化

AI 对 DWI 的影响是双向深化且同步加速的。

先看攻击侧。首先，大模型拆除了语言壁垒。过去暗网上中文、日文等非英语数据因天然的语言门槛提升了交易成本，AI 彻底改变了这一格局，攻击面在全球范围内被抹平。其次，暗网专用 AI 走向工业化。Nytheon AI 等 800 亿参数混

合大模型通过 Tor 托管和 Telegram 订阅制销售，月费低至 30-200 美元，已形成至少 3 家供应商、超 1,000 名付费用户的规模。第三，越狱版 ChatGPT、Claude、Gemini 等商业大模型在功能上远超专用恶意 AI——每一次基础模型的能力跃升，都以近乎零成本惠及攻击侧。

再看防御侧。 2026 年 RSAC 大会上，Google 展示的基于 Gemini 的暗网威胁情报系统日处理近千万条帖子，准确率 98%（传统关键词工具仅 10-20%）。这标志着从「关键词匹配」到「语义理解」的范式转换——大模型能够识别暗网上的隐晦黑话和代码词，实现从发现信号到触发自动化响应（如检测到 Session Cookie 泄露→自动轮换令牌）的分钟级闭环。

核心判断：「AI 辅助+人工研判」是长期配置。 攻击者用 AI 降低攻击成本，防御方必须用 AI 获得对等能力——不具备 AI 分析能力的 DWI 方案在未来 2-3 年内将失去实用价值。但暗网环境的复杂性决定了 AI 输出仍需人类研判作为最终决策关口。

5.3 从「借船出海」到「护航出海」

过去十年中国企业出海以重工业和制造业为主，IT 安全投入有限，且形式多以打包出售为主，这一模式数世咨询称之为「借船出海」。近年来，这一趋势正在发生改变：出海主体开始变为比亚迪、工商银行等全球头部企业，海外资产攻击面远超以往，更何况，暗网中的供应链攻击黑灰产并不区分「发展中市场」和「发达市场」，同时，国内新《网络安全法》对数据出境的合规要求同样适用于海外分支机构。

对此，暗网情报将承担起「护航出海」的重要角色。

首先，**供应链暗网风险监控**——2026 年印度塔塔电子遭攻击事件中，中国企业生产的 OT 核心资产作为供应链一环被连带曝光，此类威胁只有通过暗网情报的持续监控才能及时发现。其二，**海外凭据泄露预警**——海外分支员工的 VPN 凭据和 Session Cookie 在暗网流通，可能在攻击者部署勒索软件数周前被情报捕捉。第三，**出海合规的证据支撑**——证明「未在暗网发现企业数据泄露」本身即是合规举证，而及早发现和处置的证明是减轻处罚的关键依据。

「护航出海」是一条长期曲线，但方向确定。DWI 将从「可选的小众能力」成为安全基础设施的标配组件。

Reference

- 中华人民共和国网络安全法

  https://www.cac.gov.cn/2025-12/29/c_1768735112911946.htm

- 数世咨询发布《暗网情报技术能力框架及参考指标体系》

  https://www.dwcon.cn/post/4792

- Google unleashes Gemini AI agents on the dark web

  https://www.theregister.com/special-features/2026/03/23/google-unleashes-gemini-ai-agents-on-the-dark-web/5228490

- Stealer：被低估的暗网威胁源——从窃密日志到暗网情报闭环

  https://blog.51cto.com/u_15551024/14802896

- 混乱邪恶：从“6 铲”观察中文暗网亚文化

  https://0.zone/article/20260727

- Flashpoint

  https://flashpoint.io

- DarkOwl

  https://www.darkowl.com/

- S2W

  https://s2w.inc/en/

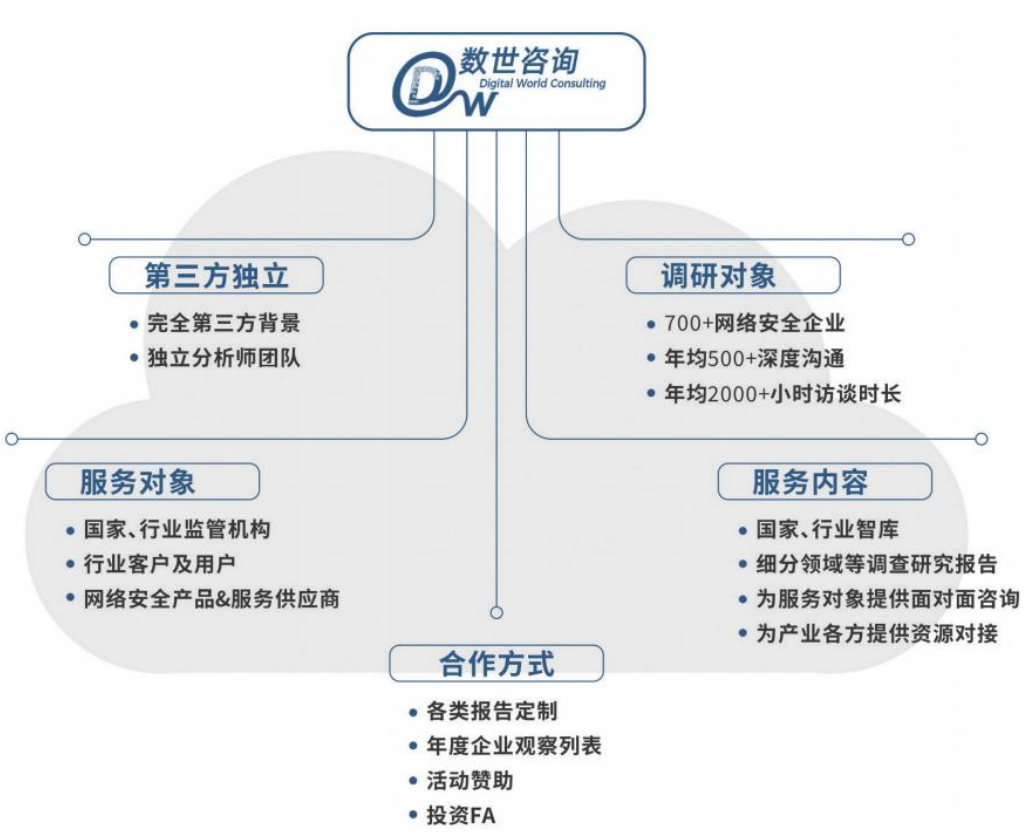
- 零零信安

  https://00sec.com/

- Dark Web Data Pricing 2026

https://www.stingrai.io/blog/dark-web-data-pricing-2026

如果您对报告有任何问题或意见，包括引用、指正或合作，请通过电子邮件 liuchenyu@dwcon.cn 与我们联系。



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800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