暗网情报技术能力框架及参考指标体系

—— 指导性技术文件 ——

（2026 版）

版本编号：DW-TI-CF-2026

发布时间：2026 年 4 月

发布方：

数世咨询

联合发布方：

中关村华安关键信息基础设施安全保护联盟（关保联盟）

奇安信威胁情报中心

绿盟科技鹰眼安全运营中心

北京微步在线科技有限公司

PCSA（行业云安全能力者联盟）智御未来安全研究院

厦门慢雾科技有限公司

北京赛博英杰科技有限公司

数说安全

主要起草单位：

北京零零信安科技有限公司

特别鸣谢：正奇学院

目录

摘要

本框架由数世咨询发布，北京零零信安科技有限公司作为主要起草单位，与中关村华安关键信息基础设施安全保护联盟（关保联盟）、奇安信威胁情报中心、绿盟科技鹰眼安全运营中心、北京微步在线科技有限公司、PCSA（行业云安全能力者联盟）智御未来安全研究院、厦门慢雾科技有限公司、北京赛博英杰科技有限公司、数说安全等机构联合发布。

框架聚焦网络安全领域**暗网情报**能力，全面覆盖 **Traditional Dark Web（传统暗网）**与 **Dark Web Lite（轻暗网）**双生态，构建包含**威胁源采集与反爬对抗、智能分析、高保真存档、中文生态识别、海量泄露数据治理、事件处置与响应闭环**在内的**七大核心能力域**，形成全链路、可量化、可落地的技术能力评估体系。

框架立足国内暗网威胁实战特征，针对数据泄露、勒索软件、IAB 交易、侵公威胁等本土高发风险，明确统一分级标准与量化指标参数，解决当前行业能力定义模糊、评估主观化、标准不统一、本土化适配不足等突出问题。本框架为指导性参考文件，**不设强制性标准与固定权重**，可灵活适配安全厂商、政企机构、监管与研究单位在能力自评、供应商选型、产品研发、安全运营、行业对标等场景使用。

随着暗网威胁持续迭代演化，本框架旨在为行业提供统一、科学、实战化的能力标尺，推动国内暗网情报能力向**体系化、专业化、实战化**方向高质量发展。

鉴于我国暗网情报技术领域与国际水平存在约 10 年代差，本框架当前设计主要参考国际已成熟的技术体系。为前瞻性应对暗网犯罪生态的演进，报告最后特别增加“未来展望”章节，基于国际前沿技术与趋势进行预研，以提升框架对于我国暗网情报能力建设的战略指导性和长期适用性。

关键词

暗网情报；Traditional Dark Web；Dark Web Lite；中文暗网；数据泄露监测；勒索软件；反爬对抗；高保真存档；应急响应；能力框架

第一章 绪论

绪论部分主要阐述本框架的研究背景、现实意义、国内暗网威胁生态现状、当前行业存在的突出问题、编制依据与参考标准，以及框架的适用对象与使用场景，为后续能力体系设计提供整体逻辑与定位支撑。

1.1. 研究背景与意义

近年来，全球网络犯罪持续向暗网迁移，勒索软件攻击、数据泄露交易、RaaS 产业化、黑客组织协作、IAB 买卖与侵公类威胁在暗网生态内呈规模化、常态化、组织化趋势，已成为危害关键信息基础设施、企业数据安全与社会公共利益的突出风险。传统威胁情报体系对暗网威胁覆盖不足、采集能力参差不齐、分析标准不统一、评估维度缺乏共识，导致政企机构在暗网情报能力建设、供应商选型、服务质量判定、安全运营闭环等方面缺少统一、可量化、可落地的参考依据。

在此背景下，构建一套覆盖**暗网情报威胁源采集、反爬对抗、智能分析、高保真存档、中文暗网识别、海量泄露数据治理、事件应急响应**的全链路技术能力框架，具有重要的现实意义与行业价值。本框架通过统一评估标准、明确能力等级、量化关键指标，可为安全厂商、政企单位、监管机构提供可参照、可核验、可落地的技术标尺，助力提升暗网威胁发现、预警、溯源与处置能力，完善数据泄露与勒索软件攻击的事前监测、事中响应、事后闭环体系，推动国内暗网威胁情报领域向标准化、专业化、实战化方向发展。

1.2. 国内暗网威胁生态现状

为清晰界定框架覆盖范围，先对两类核心暗网形态进行定义：

1. **Traditional Dark Web（传统暗网）**

   指基于 Tor、I2P 等匿名网络搭建，需专用浏览器与特殊网络配置才可访问的封闭网络空间。典型形态包括黑客论坛、勒索软件数据泄露站点、数据交易市场、IAB 交易平台、RaaS 服务站点等，具有强匿名、高隐蔽、长期存续、结构固定等特征。

2. **Dark Web Lite（轻暗网）**

   指基于加密通讯软件、封闭社群、私密频道 / 群组形成的次生地下生态。无需传统匿名网络即可访问，但具备封闭、加密、邀请制、隐蔽交易等特征，是当前数据泄露贩卖、勒索通知、入侵工具流通、侵公查档、黑灰产协作的主要载体，具有传播快、波动大、迭代快、规模庞大等特点。

当前，国内网络犯罪与地下黑灰产已形成 **Traditional Dark Web 与 Dark Web Lite 并行、相互协同、全域覆盖** 的复杂威胁生态。Traditional Dark Web 作为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；Dark Web Lite 则承担大规模数据流通、实时交易、攻击协作与扩散分发功能，二者共同构成规模化、产业化、链条化的地下产业体系。

受反爬策略、地址轮换、平台封禁、执法行动、加密机制等影响，两类威胁源均呈现**高波动、高对抗、高隐蔽**特性，传统监测与情报手段难以实现稳定采集、及时分析与有效闭环，对政企机构安全防御与行业监管治理构成显著挑战。

1.3. 现有评估体系存在的问题

当前国际暗网情报技术领域正处于快速发展阶段，我国尚处于萌芽阶段，行

业标准、技术边界、能力定义、评估体系均未统一，在实践中存在诸多突出问题：

一是**暗网情报技术领域界定模糊，易与传统威胁情报混淆**。行业常将暗网情报（DWI/DWTI）与网络威胁情报（CTI）、漏洞情报、高级持续性威胁（APT）情报、开源情报（OSINT）、互联网舆情等概念混用，未能清晰区分其监测对象、覆盖范围、技术路径与应用场景，导致能力建设方向不明确。

二是**暗网情报的领域独立性未被充分认知**。暗网情报虽常被交叉纳入数字风险保护（DPRS）、外部攻击面管理（EASM）、扩展威胁情报（XTI）、网络空间测绘、黑灰产威胁等其他网络安全领域，但因其所面向环境的封闭性、高对抗性、生态化特征，且更聚焦于入侵既成事实后的及时发现、溯源与处置，具备显著的领域独立性，现有评估体系未能体现这一核心特点。

三是**暗网研究方向不清晰，易出现范畴错位**。全球范围内对暗网的研究已分化为多条技术路线：一类以暗网基础设施、节点与流量为研究对象；一类以执法打击毒品、人口贩卖等犯罪为目标；第三类则聚焦网络安全领域，研究非法数据交易、IAB 攻击情报、企业与国家机密泄露、ATO 威胁、RaaS 产业化等内容。当前行业评估未明确界定研究范畴，易造成对象错位、标准失焦。

四是**能力定义不统一，边界模糊**。不同机构对 Traditional Dark Web 与 Dark Web Lite 两类生态的覆盖范围、监测重点、评价维度缺乏共识，能力描述主观化、碎片化，难以形成统一对标。

五是**缺乏量化指标，评估偏主观**。现有评价多以 “覆盖广”“时效性强”“分析精准” 等定性描述为主，缺少可核验、可对比、可落地的量化标准，无法客观衡量采集规模、响应时延、数据质量、对抗能力、处置闭环效果。

六是**国内外标准脱节，本土化适配不足**。国际通用评估体系未充分考虑中文暗网生态、IAB 交易、数据贩卖、侵公威胁等国内高发威胁形态，直接套用难以满足实战需求。

七是**能力碎片化，未形成全链路视角**。多数评估仅聚焦单一环节，缺少对“采

集 — 对抗 — 分析 — 存档 — 溯源 — 应急” 全流程的体系化设计，无法支撑政企机构构建完整的暗网威胁治理闭环。

1.4. 本框架编制依据与参考标准

本框架在编制过程中，充分对标全球暗网情报领域成熟评估体系，结合国内网络安全监管要求与本土化暗网威胁特征，形成兼顾国际先进性、行业实用性与场景针对性的技术能力标尺，主要编制依据如下：

一是**国际权威行业研究与评估框架**。框架参考 Javelin Strategy & Research《Dark Web Threat Intelligence Vendor Scorecard 2025》、Gartner《Market Guide for Threat Intelligence Products and Services 2024》、Forrester《The State of Threat Intelligence 2025》《External Threat Intelligence Service Providers Landscape 2025》等全球主流机构的研究方法论、能力维度与评估逻辑，借鉴国际先进的暗网情报能力划分、指标设计与实践经验，确保框架体系完整、维度科学。

二是**国内网络安全监管与实战需求**。立足我国网络安全法律规范、数据安全管理要求及关键信息基础设施保护需求，聚焦中文暗网生态、IAB 交易、数据泄露贩卖、勒索软件、RaaS 产业化、侵公类威胁等本土高发场景，强化对 Traditional Dark Web 与 Dark Web Lite 双生态的覆盖，突出可落地、可量化、可核验的实战导向。

三是**国内暗网情报领域产业实践**。综合国内主流安全厂商、政企安全运营单位、威胁情报服务机构的技术能力现状与建设痛点，围绕采集、对抗、分析、存档、溯源、应急等全流程环节，形成符合国内产业发展阶段、可普遍适用的能力分级与指标体系。

四是**领域专属技术特性**。严格遵循暗网情报的独立性、生态性、封闭性、高对抗性特征，聚焦 “入侵既成事实后的及时发现、溯源与处置” 核心定位，明确本框架仅面向网络**安全领域范畴**的暗网情报能力，即针对非法数据交易、IAB 攻击情报、国家 / 企业机密泄露、ATO 威胁、RaaS 服务等相关威胁的监测、分

析与处置能力，不包含暗网基础设施研究及非网络安全类执法研究方向，确保框架边界清晰、定位精准。

1.5. 框架适用对象与使用场景

本框架聚焦**网络安全领域内的暗网威胁情报能力**，面向全行业提供统一、可量化、可落地的技术评估标准，具备广泛的适用性与实践价值。

1.5.1. 适用对象

1. **安全产品与服务厂商：**用于暗网情报相关产品研发、能力迭代、服务标准化与对外能力展示。

2. **政企及关键信息基础设施运营单位：**用于暗网情报能力自查、建设规划、安全运营评估与供应商选型对标。

3. **监管与研究机构：**用于行业态势分析、技术标准制定、领域研究参考及产业规范化指导。

4. **测评与认证机构：**用于暗网情报产品 / 服务的测试、检验、评估与定级依据。

1.5.2. 主要使用场景

1. **能力自评与规划：**机构可对照指标体系开展全面自检，明确短板，制定分阶段建设路线。

2. **供应商选型与验收：**以量化指标为标尺，客观对比厂商能力，规范项目需求与验收标准。

3. **产品设计与研发：**为暗网监测、采集、分析、存档、溯源、应急响应等系统开发提供能力蓝图。

4．**安全运营与实战处置**：指导建立 “发现 — 分析 — 研判 — 溯源 — 闭环” 的暗网威胁应急处置流程。

5．**行业交流与对标**：为行业内能力对比、技术交流、实践分享提供统一口径与共识基础。

第二章 总体设计

本章明确框架的核心设计原则、整体能力结构、统一分级标准与评估边界，是全文的纲领性章节，用于规范后续所有能力维度的定义、划分与评价口径。

2.1. 设计原则

本框架遵循**科学性、系统性、实战性、独立性、本土化**五大核心设计原则，确保体系完整、逻辑严谨、可落地、可核验。

1．**科学性原则**：对标国际权威评估体系，采用可量化、可验证、可对比的指标设计，避免主观定性描述。

2．**系统性原则**：覆盖暗网情报全技术链条，形成 “采集 — 对抗 — 分析 — 存档 — 治理 — 响应” 的完整闭环。

3．**实战性原则**：聚焦真实威胁场景，以数据泄露、IAB 交易、勒索软件、RaaS、侵公威胁等本土高发风险为核心导向。

4．**独立性原则**：明确暗网情报专属技术边界，突出其生态封闭性、高对抗性、事后发现与快速处置的领域特性。

5．**本土化原则**：深度适配中文暗网生态、Traditional Dark Web 与 Dark Web Lite 双域并行特征，贴合国内监管与运营需求。

2.2. 框架整体结构

本框架围绕暗网情报全生命周期能力构建，共设 **7 大核心能力域**，全面覆盖技术实现、运营效能与服务闭环：

1. **Traditional Dark Web 威胁源采集和反爬对抗能力**
2. **Dark Web Lite 威胁源采集能力**
3. **暗网情报智能分析能力**
4. **暗网情报高保真复制和持久化存档能力**
5. **中文暗网生态环境威胁识别能力**
6. **海量泄露数据知识库能力**
7. **事件处置与响应闭环能力**

各能力域下设二级指标项，统一采用**基础、良好、优秀**三级评定标准，形成层次清晰、维度完整、可量化评估的技术能力体系。

2.3. 能力分级定义

本框架对所有指标统一划分为**三级能力水平**：

1. **基础级**：具备核心功能与基本覆盖，满足最低可用要求，以人工或半自动化方式实现主要流程。
2. **先进级**：具备较高自动化水平与规模化处理能力，时效性、稳定性、完整性明显提升，可支撑常态化运营。
3. **优秀级**：具备全流程自动化、高对抗性、高保真、高时效与全域覆盖能

力，达到行业领先与实战化标杆水平。

2.4. 评估范围与边界说明

1. **领域边界**：本框架仅针对**网络安全领域的暗网情报能力**，聚焦非法数据交易、IAB 攻击情报、企业 / 机构机密泄露、ATO 威胁、勒索软件、RaaS 等相关威胁；不包含暗网基础设施研究、流量分析、非网络安全类犯罪打击等其他研究方向。

2. **生态边界**：同时覆盖 **Traditional Dark Web** 与 **Dark Web Lite** 两类核心威胁生态。

3. **对象边界**：聚焦黑客论坛、勒索泄露站点、数据交易市场、加密通讯群组、封闭交易频道等网络犯罪相关载体，不含合法匿名网络使用场景。

4. **功能边界**：以**监测、采集、分析、存档、溯源、研判、应急处置**为主，不涉及入侵、攻击、控制等违法违规技术能力。

5. **合规性边界**：本框架为技术能力参考文件，相关能力的建设与使用应遵循**《中华人民共和国网络安全法》《数据安全法》《个人信息保护法》**等法律法规要求。使用方在具体实施过程中，应自行确保各项操作符合适用法律及监管规定。

第三章 Traditional Dark Web 威胁源采集和反爬对抗能力

Traditional Dark Web 是基于 Tor、I2P 等匿名网络构建的高隐蔽、高对抗性地下生态空间，主要承载黑客论坛、勒索软件数据泄露站点、数据交易市场、IAB 交易平台、RaaS 服务等网络犯罪相关载体。本章从采集广度、采集深度、反爬对抗、时效性、波动应对、引擎安全六个维度，构建 Traditional Dark Web 威胁源采集与对抗能力的量化评估体系。

3.1. 威胁源采集广度

3.1.1. 设计目的

威胁源采集广度是暗网情报技术能力体系建设的**基础性核心指标**。其核心设计目的在于：**最大限度降低暗网威胁事件的漏检风险**，保障数据泄露监测的**全面性与及时性**。

在实际网络安全攻防场景中，攻击者在完成数据窃取后，通常会在多个暗网威胁源进行数据流通与贩卖。若监测体系的采集范围有限，未能实现对核心暗网生态的全覆盖，则极有可能出现相关暗网情报未被监测到的情况。这将直接导致相关单位在数据泄露发生后，无法在**威胁早期阶段**获取有效预警，进而错失**阻断威胁传播、控制泄露影响范围**的最佳时机。

因此，威胁源采集广度直接决定了暗网情报体系的**发现窗口与响应前置性**。只有具备足够的采集广度，才能确保在数据泄露事件发生后，相关敏感信息在暗网流通的第一时间实现**及时发现与响应**，为后续开展风险评估、事件研判、溯源取证及应急处置提供全面、可靠的**情报支撑**。

3.1.2. 设计依据

本指标主要参考 Javelin Strategy & Research《Dark Web Threat Intelligence Vendor Scorecard（2025）》中关于“**Source Collection（威胁源采集能力）**”的评估维度，并结合全球暗网威胁源的实际分布特征与国内网络安全实战需求进行设定。

全球暗网站点数量庞大，但绝大多数为毒品、违禁物品、虚假证件等**非网络安全类犯罪内容**，与网络安全直接相关的**网络犯罪生态站点**（含黑客论坛、勒索软件泄露站点、数据交易市场、IAB 交易平台等）数量相对集中。从全球实战监测情况来看，真正具备高情报价值、持续活跃的核心威胁源根域，通常集中在数十至数百个范围内。

因此，本框架以**威胁源根域数量**作为核心量化标准，并结合行业能力现状划分三级阈值：

- **200 个以上**：代表具备**行业领先的采集覆盖能力**，可覆盖绝大多数高价值网络安全类威胁源，包括主流黑客论坛、活跃勒索组织站点及核心数据交易市场，监测范围达到国际一线暗网情报厂商水平，具备全面的暗网威胁发现能力。

- **50 个以上**：代表具备**良好的监测覆盖能力**，可有效掌握主要高价值威胁源，能够满足各类机构常态化风险预警与安全运营需求。

- **5 个以上**：代表满足**基础监测能力要求**，可覆盖当前最活跃的核心黑客论坛及少量关键泄露站点，能够支撑最基本的暗网威胁关注与发现。

该指标设计充分贴合暗网威胁源的真实分布规模，同时合理划分能力梯度，确保指标具备**可操作性、可对比性与行业普遍适用性**。

3.1.3. 指标参数

威胁源采集广度以**威胁源根域数量**作为核心量化指标，具体分级标准如下：

指标项	指标参数	评判等级
威胁源采集广度	威胁源根域数量 > 5	基础
	威胁源根域数量 > 50	良好
	威胁源根域数量 > 200	优秀

指标说明

威胁源根域数量指可**稳定监测并持续采集**的网络安全相关**网络犯罪生态暗网根域总数**。该指标重点关注**高价值威胁源覆盖范围**，而非暗网站点总体数量。

通过该量化标准，可客观评估在 Traditional Dark Web 领域的**采集覆盖能力**，为后续采集深度、反爬对抗及情报分析能力奠定基础支撑。

3.2. 威胁源采集深度

3.2.1. 设计目的

威胁源采集深度是评估暗网情报**采集能力**的重要指标。其核心设计目的在于衡量能否**及时、全面地获取暗网威胁源中新发布的高价值内容**。

在实际威胁场景中，攻击者窃取相关单位数据后，往往会通过暗网论坛、泄露站点或交易市场发布相关情报。若对新帖的采集深度不足，则可能无法及时发现此类高价值事件，导致相关单位在数据泄露发生后错失**早期预警窗口**，无法有效采取阻断传播、降低损失的应对措施。

因此，威胁源采集深度直接关系到能否在威胁情报出现的关键阶段实现**及时发现**，从而为后续风险评估、事件研判和应急处置提供可靠的数据支撑。该指标以 New Post 每日采集量作为量化依据，重点考察对高价值新内容的**抓取能力**。

3.2.2. 设计依据

本指标主要参考 Javelin Strategy & Research《Dark Web Threat Intelligence Vendor Scorecard（2025）》中“**Source Collection（威胁源采集能力）**”的评估维度，并结合 Traditional Dark Web 威胁源的实际发布特征与国内网络安全实战需求进行设定。

Traditional Dark Web 威胁源中，**高价值情报**主要以 New Post（新主帖）的形式发布，涵盖数据贩卖帖、数据库泄露帖、勒索软件通告、IAB 交易帖等核心内容。此类新帖的出现频率与数量，直接反映了暗网网络犯罪活动的活跃程度，也是采集能力需重点覆盖的核心对象。因此，本框架以 **New Post 每日采集量** 作为核心量化标准，用以评估对高价值情报的抓取深度。

指标分级设计综合考虑三大核心因素：一是全球主要黑客论坛和勒索组织泄露站点的实际发帖规模；二是高价值情报在暗网的分布特点与传播规律；三是不同能力层级在实战中的差异化表现。通过设定科学合理的量化阈值，确保该指标既具备**科学性与合理性**，又能清晰体现不同采集能力在抓取深度上的实际差距，满足行业评估与实战应用需求。

3.2.3. 指标参数

威胁源采集深度以 **New Post 每日采集量** 作为核心量化指标，重点评估对高价值新内容的抓取能力，具体分级标准如下：

指标项	指标参数	评判等级
威胁源采集深度	New Post 每日采集量 > 100	基础
	New Post 每日采集量 > 200	良好
	New Post 每日采集量 > 1000	优秀

指标说明

New Post 指暗网威胁源中新发布的主帖，核心涵盖**数据贩卖帖、数据库泄露帖、勒索软件通告、IAB 交易帖**等高价值内容，是反映暗网威胁动态的核心载体。

该指标通过量化每日新增主帖的采集数量，客观反映采集能力的深度与全面性 —— 采集量越多、覆盖越全面，越能及时捕捉到暗网中的高价值威胁信息，为后续的情报分析、风险预警以及应急处置，提供真实、有效的数据支撑，避免因遗漏关键新帖而导致的风险防控滞后。

3.3. 防御策略 / 反爬对抗能力

3.3.1. 设计目的

防御策略与反爬对抗能力是 **Traditional Dark Web 威胁源采集** 的关键技术保障。其核心设计目的在于评估针对黑客论坛、勒索组织泄露站点等高价值目标所具备的**反爬对抗与突破能力**，保障情报采集工作能够稳定、持续开展。

Traditional Dark Web 中的高价值威胁源普遍采用严格的**会员准入审核、异常行为检测、IP 与设备指纹限制、JS 动态渲染、Cloudflare 等多层级防护机制**。若反爬对抗能力不足，将难以有效突破上述防御措施，极易出现采集中断、内容缺失或采集不稳定等问题，直接影响暗网情报的**及时性与完整性**。

从能力分级来看：

- **优秀级**要求可稳定采集 **Tier1 级别高壁垒威胁源**（如 XSS、Exploit 类核心站点），体现顶尖的反爬对抗技术实力；
- **良好级**要求可稳定采集 **Tier2 级别威胁源**（如 RansomHub、Qilin、Akira 等活跃勒索组织站点），具备成熟的实战对抗能力；
- **基础级**要求可稳定采集 **Tier3 级别威胁源**（如 Breachforums、Darkforums 等公开度较高站点），满足基础采集可用要求。

因此，该指标直接决定暗网情报采集的**可靠性与持续性**，为后续风险预警、事件研判和应急处置提供坚实的技术支撑。

3.3.2. 设计依据

本指标主要参考 Javelin Strategy & Research《Dark Web Threat Intelligence Vendor Scorecard（2025）》中“**Source Collection（威胁源采集能力）**”的评估维度，并在编制过程中充分借鉴全球暗网情报领域顶尖机构的技术分析成果，包

括：

- Flashpoint《Technical Analysis of High-Wall Underground Forums: XSS and Exploit（2025）》

- Recorded Future《Defense Mechanisms in Russian Cybercrime Forums: XSS.is and Exploit.in Case Study（2025）》

结合 Traditional Dark Web 威胁源的**实际防御策略特征**与国内网络安全实战需求进行设定。

Traditional Dark Web 中的高价值威胁源普遍部署**多层次、高复杂度的防御机制**，不同难度等级的威胁源，在**防护强度、技术复杂度及采集对抗成本**上存在显著差异，结合行业实战共识与技术特征，具体分级说明如下：

- **Tier 1 级别**（以 XSS、Exploit 等为代表）：通常部署**最高等级防护体系**，涵盖**企业级 Cloudflare 防护、严格会员制审核、邀请制注册、深度行为指纹检测、高强度 JS 动态渲染、多重 CAPTCHA 验证及复杂异形网站结构**。此类威胁源构成暗网中**防御壁垒最高**的场景，采集难度极大，需具备**极为成熟、全面的反爬对抗技术**，才能实现稳定采集。

- **Tier 2 级别**（以 RansomHub、Qilin、Akira 等为代表）：多采用**标准 Cloudflare 防护**，同时搭配大量**异形网站结构、特殊技术栈、访问速率限制及会话验证**等防御手段。相较于 Tier 1 级别，其整体防御强度有所降低，但仍具备**较高的采集对抗成本**，尤其在适配异形结构、兼容特殊技术栈方面，需具备较强的**技术适配与突破能力**。

- **Tier 3 级别**（以 Breachforums、Darkforums 等为代表）：虽已普遍配备 Cloudflare 防护，但均为**基础级服务**，搭配**常规 IP 封禁、简单验证码及标准反爬规则**，整体防御强度相对较低，采集对抗成本也处于较低水平，基础反爬对抗技术即可实现有效突破与稳定采集。

基于上述威胁源防御特征的分级设计，本指标可**客观反映针对不同防御强度威胁源的反爬对抗水平**，清晰区分不同能力层级的技术差距，为暗网情报采集对抗能力的量化评估，提供**科学、可对比、可落地的核心依据**。

3.3.3. 指标参数

防御策略与反爬对抗能力以对不同难度威胁源的**稳定采集能力**作为核心量化指标，具体分级标准如下：

指标项	指标参数	评判等级
防御策略/反爬对抗能力	稳定采集 Tier3 级别威胁源（Breachforums、Darkforums 等）	基础
	稳定采集 Tier2 级别威胁源（RansomHub、Qilin、Akira 等）	良好
	稳定采集 Tier1 级别威胁源（XSS、Exploit 等）	优秀

指标说明

本指标重点评估针对不同防御强度威胁源的**反爬对抗水平**。其中 Tier 1 级别代表**最高对抗难度**，Tier 2 级别代表**中高对抗难度**，Tier 3 级别代表**中低对抗难度**。

通过该分级标准，可客观反映在 Traditional Dark Web 领域突破目标站点防御策略的技术实力，为后续情报采集的**可靠性与持续性**提供重要技术支撑。

3.4. 情报采集时效性

3.4.1. 设计目的

情报采集时效性是 **Traditional Dark Web 威胁源采集能力** 的重要评估维度。其核心设计目的在于衡量在不同难度威胁源上，从情报发布到完成采集的**响应速度与效率**。

在实际威胁场景中，**高价值情报**（如新数据泄露帖、勒索软件通告、IAB 交易信息等）往往在暗网威胁源中呈现**短暂流通、快速扩散**的特征。若采集时效性不足，将可能错过此类情报的关键窗口期，导致相关单位无法及时发现自身数据已在暗网流通或攻击活动正在发生，进而错失**最佳的风险阻断和应急应对时机**。

因此，该指标通过区分 Tier 1、Tier 2、Tier 3 不同难度威胁源的采集时效要求，客观评估在实战环境下的情报采集响应能力，为后续风险预警、事件研判和应急处置提供**及时、可靠的情报支撑**，确保威胁情报能够发挥前置预警、快速响应的核心价值。

3.4.2. 设计依据

本指标主要参考 Javelin Strategy & Research《Dark Web Threat Intelligence Vendor Scorecard》（2025）中“**Source Collection（来源采集能力）**”的评估维度，并结合 **Traditional Dark Web** 威胁源的**实际发布特征**与**采集时效要求进行设定**。

Traditional Dark Web 中的高价值情报通常以 **New Post** 或 **New Leak** 的形式快速涌现，其核心价值随时间呈**指数级衰减**特征。鉴于不同难度等级的威胁源在采集技术门槛与响应时效要求上存在显著差异，本指标体系严格按照威胁源的**对抗强度**，将采集时效性划分为 **Tier 1、Tier 2、Tier 3** 三个梯度进行量化评估。

具体而言：

- **Tier 1 级别威胁源**（以 XSS、Exploit 等为代表）：因部署**最高等级防御体系**，采集对抗成本与技术难度最大，对引擎的并发处理与实时抓取能力要求极高，因此设定**最严苛的时效标准**，以确保高价值情报不被遗漏。

- **Tier 2 级别威胁源**（以 RansomHub、Qilin、Akira 等为代表）：防御强度与采集复杂度次之，时效要求相应**适度降低**，重点评估引擎突破常规防护后稳定获取情报的速度。

- **Tier 3 级别威胁源**（以 Breachforums、Darkforums 等为代表）：防御机制相对基础，时效要求也**更为宽松**，主要考察采集覆盖的广度与及时性。

通过这种**分级差异化**的设计，本指标能够精准、客观地反映引擎在不同对抗环境下对高价值情报的**快速响应能力**，确保评估结果具备**科学性、针对性**，并能直接指导实战中的风险预警与应急处置。

3.4.3. 指标参数

情报采集时效性以不同难度威胁源的**稳定采集延迟**作为核心量化指标，具体分级标准如下：

指标项	指标参数	评判等级
情报采集时效性	威胁源：Tier1 无，Tier2 无，Tier3 < 24 小时	基础
	威胁源：Tier1 无，Tier2 < 6 小时，Tier3 < 12 小时	良好
	威胁源：Tier1 < 6 小时，Tier2 < 2 小时，Tier3 < 1 小时	优秀

指标说明

本指标重点评估对不同难度威胁源的**响应速度**。其中 Tier 1 级别代表**最高对抗难度**，Tier 2 级别代表**中高对抗难度**，Tier 3 级别代表**中低对抗难度**。

通过量化采集延迟，可客观反映引擎在实战环境下的情报获取及时性，为后续风险预警、事件研判和应急处置争取关键时间窗口，提供重要时效支撑。

3.5. 暗网波动对抗能力

3.5.1. 设计目的

暗网波动对抗能力是 **Traditional Dark Web 威胁源采集** 的重要保障性指标。其核心设计目的在于评估在面对威胁源波动时的**快速恢复能力与应急适配能力**，确保采集工作不中断、情报获取不脱节。

Traditional Dark Web 中的高价值威胁源易受多种因素影响产生波动，包括**执法打击行动、站点查封、域名 / 地址更换、防护机制升级**等，这些因素均可能直接导致采集中断。若缺乏有效的波动对抗能力，将可能出现长时间无法获取暗网情报的情况，进而影响相关单位对暗网威胁的**及时发现、快速响应与风险处置**，导致威胁预警滞后、处置被动。

因此，该指标通过量化从发现威胁源波动到恢复稳定采集的时间，客观反映在复杂对抗环境下的**持续采集能力**，为暗网情报采集工作的**稳定性与可靠性**提供重要技术支撑，保障情报采集工作的连续性与实战可用性。

3.5.2. 设计依据

本指标的设计依据主要参考 Javelin Strategy & Research《Dark Web Threat Intelligence Vendor Scorecard》（2025）中“**Source Collection（来源采集能力）**”的评估维度，并结合 Traditional Dark Web 威胁源的**实际波动特征**进行设定。

Traditional Dark Web 中的高价值威胁源具有**较高的波动性**，经常因**执法行动、站点查封、地址更换、防护升级或站点主动迁移**等因素导致**采集中断**。这种波动直接影响情报采集的**连续性和及时性**。因此，本框架以“发现波动至恢复稳定采集的时间”**作为主要量化标准**，并按照**恢复速度**划分为三个等级。

优秀级要求在 **48 小时**内恢复稳定采集，体现具备较强的**自动发现和新源适配能力**；**良好级**要求在 **7 天内**恢复，表明具备基本的**波动应对机制**；**基础级**要求在 **30 天内**恢复或具备一定处置措施，达到**最低可用要求**。

通过这种分级设计，本指标能够客观反映在面对暗网威胁源波动时的**恢复能力**，为评估采集**稳定性和实战韧性**提供可靠依据。

3.5.3. 指标参数

暗网波动对抗能力以**发现波动至恢复稳定采集的时间**作为核心量化指标，具体分级标准如下：

指标项	指标参数	评判等级
暗网波动对抗能力	发现波动至恢复 < 30 天	基础
	发现波动至恢复 < 7 天	良好
	发现波动至恢复 < 48 小时	优秀

指标说明

本指标重点评估在面对**执法行动、地址更换、防护升级**等威胁源波动情况下的**恢复能力**。通过量化恢复时间，可客观反映在复杂对抗环境下的**持续采集韧性**，为情报采集的**稳定性和长期可用性**提供重要技术支撑。

第四章 Dark Web Lite 威胁源采集能力

Dark Web Lite 是以加密通信工具为依托、由封闭社群与私密频道 / 群组构成的次生地下威胁生态，无需依托传统匿名网络即可接入，兼具开放接入与邀请制封闭运行双重形态，具有传播速率快、地址更迭频繁、结构动态演化、总体规模庞大等典型特征。该生态是当前暗网环境中数据泄露交易、勒索通告发布、入

侵工具流转、侵公查档活动、黑灰产协同作业与实时情报交互的主要承载空间，在网络犯罪产业化链条中占据高频交互、快速扩散的核心地位。本章立足该生态的动态化、规模化、高对抗性特征，从威胁源采集广度、威胁源内容解析度、威胁源采集规模、采集效果优化效率四个维度，构建 Dark Web Lite 威胁源采集能力量化评估体系，用以全面评估针对加密社群类威胁情报的全域覆盖能力、深度解析能力、规模化获取能力与快速适配能力，为暗网情报全链路采集体系提供轻量化地下生态的能力支撑与可量化评估依据。

4.1. 威胁源采集广度

4.1.1. 设计目的

威胁源采集广度是 **Dark Web Lite 威胁源采集能力**的**基础性核心指标**。其核心设计目的在于：**评估网络安全相关网络犯罪生态中 Dark Web Lite 威胁源的覆盖范围与覆盖规模**，最大限度降低威胁情报漏检风险，保障情报监测的全面性与稳定性。

Dark Web Lite 生态中的高价值威胁情报主要依托**群组与私密频道**开展传播与交易活动。若采集广度不足，则无法实现对足量威胁源的有效覆盖，极易造成**重要数据泄露、IAB 交易、窃密日志**等关键情报漏报，直接导致相关机构在威胁发生早期阶段难以实现有效发现与快速响应，错失风险处置的最佳时机。

因此，威胁源采集广度**直接决定能否全面、及时发现 Dark Web Lite 生态内的网络安全相关威胁活动**，为后续情报分析、风险预警与应急处置提供充足、可靠的数据支撑。

4.1.2. 设计依据

本指标的设计依据主要结合 **Dark Web Lite 威胁源**的实际分布特征与采集需求进行设定。

Telegram 作为 Dark Web Lite 的**主要承载载体**，其社群与频道总体规模极为庞大，全球范围内总量已达数亿级别。但聚焦至网络安全相关网络犯罪生态（含数据泄露贩卖、勒索通告、IAB 交易、窃密日志等）的有效威胁源，其实际数量远低于总体规模。依据行业研究成果与实战监测数据，该领域内具备持续活跃属性的群组与频道数量，**总量处于数千至数万区间**。

本框架以**威胁源群组和频道数量**作为核心量化标准，用以评估对 Dark Web Lite 威胁源的采集覆盖广度。指标分级设计综合考虑三大核心要素：一是 Dark Web Lite 生态中网络安全相关威胁源的**真实规模分布**；二是不同能力层级在覆盖范围上的**差异化表现**；三是该生态所具备的**高波动、快速迭代特征**。通过设定科学合理的量化阈值，保障指标兼具科学性与可操作性，能够客观体现引擎在采集广度层面的实际能力差距。

本指标主要参考依据包括：Flare Systems《Telegram Cybercrime Ecosystem Report》（2025）、Chainalysis《Crypto Crime Report 2025》中关于地下通讯社群威胁源规模的测算与统计数据。

4.1.3. 指标参数

威胁源采集广度以**威胁源群组和频道数量**作为核心量化指标，具体分级标准如下：

指标项	指标参数	评判等级
威胁源采集广度	威胁源群组和频道数量 > 100	基础
	威胁源群组和频道数量 > 1000	良好
	威胁源群组和频道数量 > 5000	优秀

指标说明

本指标重点评估对网络安全相关网络犯罪生态中 **Dark Web Lite 威胁源的覆盖范围**。通过量化**威胁源群组和频道数量**，可客观反映在 Dark Web Lite 领域的采集覆盖能力，为后续内容解析、情报分析与风险预警提供重要的数据支撑。

4.2. 威胁源采集内容解析度

4.2.1. 设计目的

威胁源采集内容解析度是 **Dark Web Lite 威胁源采集能力**的**重要评估维度**。其核心设计目的在于：**衡量对采集所得情报内容的处理深度，尤其针对多媒体元素的获取与解析能力。**

Dark Web Lite 生态内的高价值威胁情报，常以**消息、图片、附件**等多元形态发布。若仅能采集文本消息，无法对附件或多媒体内容开展有效解析与提取，将直接造成**情报完整性缺失**，难以全面掌握威胁核心细节，进而影响后续风险评估与响应决策的科学性与准确性。

因此，本指标重点考察采集环节对**多媒体内容**的处理能力，该项能力**直接关系到情报的可用性与分析深度**，可为安全运营工作提供更全面、更具实战价值的数据支撑。

4.2.2. 设计依据

本指标的设计依据主要结合 **Dark Web Lite 威胁源**的内容发布特征与实际采集需求进行设定。

Dark Web Lite 中的高价值情报常以**消息、图片、Excel、压缩包**等附件形式发布，此类非结构化多媒体载体中往往包含大量**受影响主体的实体信息**，如域名、邮箱、账号等关键内容。但在实际采集作业中，全量下载所有附件难以落地执行，原因在于部分合集打包文件体积庞大，可达数十 GB、上百 GB 乃至 TB 级别，不仅会大幅提升存储成本，还会显著提高被社群管理者发现并封禁的风险。

因此，本框架以**多媒体内容解析深度**作为量化标准，重点评估对小文件与附件的自动采集能力，以及对超大附件的**地址记录与精准定位能力**。通过该分级设计，既可保障情报获取的完整性，又能兼顾实际采集的可行性与安全性，为后续**向量检索、知识图谱构建及风险预警**提供可靠的数据支撑。

4.2.3. 指标参数

威胁源采集内容解析度以**多媒体内容的处理深度**作为核心量化指标，具体分级标准如下：

指标项	指标参数	评判等级
威胁源采集内容解析度	采集消息	基础
	采集消息，识别和定位消息附件	良好
	采集消息，自动下载小附件，识别和定位超大附件	优秀

指标说明

本指标重点评估对 Dark Web Lite 威胁源中多媒体内容的采集处理能力。**优秀级**要求能够**自动下载小附件并识别定位超大附件，良好级**要求能够**识别和定位消息附件，基础级**则仅能**采集消息文本**。通过该量化标准，可客观反映采集过程中的内容完整性，为后续情报分析和风险预警提供重要支撑。

4.3. 威胁源采集量

4.3.1. 设计目的

威胁源采集量是 **Dark Web Lite 威胁源采集能力**的**核心量化指标**。其核心设计目的在于：**评估对网络安全相关网络犯罪生态中 Dark Web Lite 威胁源的每日**

情报获取规模。

Dark Web Lite 生态内的高价值威胁情报以**消息形态**高速产生与传播。若采集量不足，则难以覆盖足够规模的威胁源，极易造成**重要数据泄露、IAB 交易、窃密日志**等关键情报漏报，直接影响相关主体在威胁发生早期阶段的发现与响应能力。

因此，威胁源采集量**直接决定能否全面、及时掌握 Dark Web Lite 中的网络安全威胁动态**，为后续情报分析、风险预警与应急处置提供**充足、可靠的数据基础**。

4.3.2. 设计依据

本指标的设计依据主要结合 **Dark Web Lite 威胁源**的消息发布特征与实际采集需求进行设定。

Dark Web Lite 中的网络安全相关网络犯罪生态威胁源以 **Telegram 群组与频道**为主要承载载体，具备消息产生速率快、总体规模庞大的特征，高价值情报通常以高频消息形式出现。因此，本框架以**每日消息数量**作为核心量化标准，用以评估对 Dark Web Lite 威胁源的采集规模。

指标分级设计综合考虑 Dark Web Lite 生态中网络安全相关威胁源的实际消息产出规模，以及不同能力层级在采集总量上的差异化表现。通过设定科学合理的量化阈值，确保指标兼具科学性与可操作性，能够客观体现采集能力在消息处理规模上的真实差距。

4.3.3. 指标参数

威胁源采集量以**每日消息数量**作为核心量化指标，具体分级标准如下：

指标项	指标参数	评判等级

威胁源采集量	每日消息数量 > 10,000	基础
	每日消息数量 > 100,000	良好
	每日消息数量 > 1,000,000	优秀

指标说明

本指标重点评估对 Dark Web Lite 威胁源的每日情报获取规模。通过量化每日消息采集数量，可客观反映在 Dark Web Lite 领域的采集能力，为后续情报分析、风险预警和应急处置提供重要数据支撑。

4.4. 威胁源采集效果优化

4.4.1. 设计目的

威胁源采集效果优化是 **Dark Web Lite 威胁源采集能力**的**重要保障性指标**。其核心设计目的在于：**评估在面对威胁源波动或新源发现时的快速适配与优化能力**。

Dark Web Lite 生态内的威胁源具备**高波动性**特征，群组与频道频繁出现迁移、封禁及新源创建等情形。若无法快速完成采集适配与优化，将直接引发情报采集中断或覆盖缺失，进而影响对网络安全相关威胁的及时发现与持续监测。

因此，本指标通过量化**旧源波动或新源发现后的采集优化时间**，客观反映动态环境下的适配能力与采集稳定性，为 Dark Web Lite 威胁源采集的**长期可靠性与连续性**提供重要技术支撑。

4.4.2. 设计依据

本指标的设计依据主要结合 **Dark Web Lite 威胁源**的高波动性特征与实际采集需求进行设定。

Dark Web Lite 中的群组与频道迭代迅速，频繁因执法行动、管理封禁、地址迁移或新源创建而产生波动。若无法及时开展采集优化，将直接导致情报覆盖中断或数据缺失。因此，本框架以**旧源波动或新源发现时的采集优化时间**作为核心量化标准，用以评估动态环境下的适配能力。

指标分级设计综合考虑以下因素：一是 **Dark Web Lite 威胁源快速迭代与波动频率**；二是不同能力层级在采集优化速度上的**差异化表现**；三是该项能力对整体采集**连续性与稳定性**的支撑作用。通过设定科学合理的量化阈值，确保指标兼具科学性与可操作性，能够客观体现采集效果优化层面的真实能力差距。

4.4.3. 指标参数

威胁源采集效果优化以**旧源波动或新源发现时的采集优化时间**作为核心量化指标，具体分级标准如下：

指标项	指标参数	评判等级
威胁源采集效果优化	旧源波动或新源发现时，采集优化时间 < 24 小时	基础
	旧源波动或新源发现时，采集优化时间 < 6 小时	良好
	旧源波动或新源发现时，采集优化时间 < 1 小时	优秀

指标说明

本指标重点评估在面对 Dark Web Lite 威胁源波动或新源出现时的快速适配能力。通过量化采集优化时间，可客观反映动态环境下的采集稳定性和连续性，为 Dark Web Lite 威胁源采集的长期可靠性和实战效能提供重要技术支撑。

第五章 暗网情报智能分析能力

暗网情报智能分析是暗网威胁情报全链路体系中的核心能力环节，承接前端多源威胁情报采集成果，面向 Traditional Dark Web 与 Dark Web Lite 双生态的海量异构数据，实现威胁识别、实体提取、分类分级、关联挖掘与知识化呈现。该环节以人工智能、自然语言处理、向量检索与知识图谱技术为支撑，解决暗网情报非结构化、碎片化、高噪声、强隐蔽等难题，是提升威胁研判精准度、响应时效性与溯源完整性的关键支撑。本章立足暗网生态数据特征与实战化研判需求，从关键实体信息提取、情报分级分类、情报分析时效性、多维度向量检索、情报知识图谱构建五个维度，建立暗网情报智能分析能力量化评估体系，全面衡量对暗网威胁数据的自动化处理、深度挖掘、精准研判与智能关联能力，为暗网威胁预警、事件溯源与安全运营提供标准化、可量化的分析能力依据。

5.1. 关键实体信息提取

5.1.1. 设计目的

关键实体信息提取是**暗网情报智能分析能力**的**基础性核心指标**。其核心设计目的在于：**评估从海量原始情报中自动识别与提取关键实体的能力**。

暗网威胁源中蕴含大量分散的实体信息，主要包括**发布者、组织标识、Telegram 账号、邮箱地址、事件标题、事件内容、发布时间、威胁源**等。若无法有效提取上述关键实体，将难以把零散的原始数据转化为**结构化、可关联**的情报成果，进而影响后续情报分级分类、知识图谱构建以及风险预警的准确性与处置效率。

因此，本指标重点考察对关键实体的自动提取能力，以及在威胁源波动场景下的**自动关联与更新能力**，该项能力**直接决定暗网情报从原始数据向可行动情报转化的效率**，为风险评估与响应决策提供可靠的基础支撑。

5.1.2. 设计依据

本指标的设计依据主要结合**暗网情报**的实际数据特征与分析需求进行设定。

暗网威胁源普遍存在**波动频繁**的特征，各类黑客论坛、勒索组织泄露站点等高频次因执法行动、主动迁移、地址轮换等原因发生域名或访问路径变更。当威胁源出现波动时，若无法实现波动前后的**实体自动关联**，将产生大量重复数据与冗余信息，严重影响情报质量与后续分析效率。

因此，本框架以**关键实体信息提取的完整性与自动化程度**作为量化标准，重点评估从多源原始情报中自动识别与提取关键实体的能力，并着重强调威胁源波动场景下的**自动关联更新**能力。通过设定科学合理的分级阈值，确保指标能够客观体现情报分析基础能力层面的真实差距。

5.1.3. 指标参数

关键实体信息提取以**关键实体的自动提取能力和关联能力**作为核心量化指标，具体分级标准如下：

指标项	指标参数	评判等级
关键实体信息提取	可自动提取部分威胁源或部分关键实体信息	基础
	自动提取全部威胁源中的关键实体（发布者、Telegram 账号、邮箱地址、事件标题、事件内容、发布时间、威胁源）	良好
	自动提取全部威胁源中的关键实体（发布者、Telegram 账号、邮箱地址、事件标题、事件内容、发布时间、威胁源），并支持威胁源波动时的自动关联	优秀

指标说明

本指标重点评估从暗网原始情报中自动识别和提取关键实体的能力。通过量化实体提取的完整性和在威胁源波动时的关联更新能力，可客观反映在情报分析基础环节的处理水平，为后续分级分类、向量检索和知识图谱构建提供重要数据支撑。

5.2. 情报分级分类

5.2.1. 设计目的

情报分级分类是**暗网情报智能分析能力**的**核心指标之一**。其核心设计目的在于：**评估对海量暗网情报进行系统化分级与分类的能力**，实现情报价值的精准区分与高效流转。

暗网情报具有**数量庞大、类型繁杂、价值不均**的特征，若无法对情报开展有效的分级分类，将难以区分不同情报的紧急程度、影响范围与威胁等级，极易导致高价值关键威胁被淹没在海量冗余数据中，无法为相关主体提供精准的风险预警与决策支撑。

因此，本指标重点考察对情报**价值等级、受影响国家、受影响主体、归属行业、事件类型**等多维度的分级分类能力，该项能力**直接决定情报分析的效率与准确性**，为后续风险评估、事件研判与应急处置提供清晰的优先级指引，保障威胁响应的针对性与时效性。

5.2.2. 设计依据

本指标的设计依据主要结合**暗网情报**的实际数据特征与分析需求进行设定。

从行业实际应用现状来看，全球范围内半数以上涉足暗网情报领域的相关机构，尚未对情报开展有效的分级分类工作，大部分机构仅能完成受影响国家与受影响主体的粗浅分类；仅有少数行业头部机构，能够实现情报的细致、规范、可操作的分级分类，这一现状充分体现了情报分级分类工作的实操难度。

造成该工作难度较高的核心原因，在于暗网情报本身具备**海量性、非结构化、碎片化**的显著特征，采用人工分类或简单规则匹配的方式，难以达到理想的分类效果，且效率低下、误差较大。唯有**成熟运用人工智能相关技术**，才能实现对情报**价值等级、受影响国家、受影响主体、归属行业、事件类型**等多维度的精准、高效分级分类。

因此，本框架以**情报分级分类的自动化程度与多维度覆盖完整性**作为核心量化标准，通过科学设定分级阈值，确保指标能够客观、真实地反映在情报分析核心能力上的实际差距。

5.2.3. 指标参数

情报分级分类以**分级分类的自动化程度和维度覆盖范围**作为核心量化指标，具体分级标准如下：

指标项	指标参数	评判等级
情报分级分类	未进行系统化或明确的分级分类	基础
	进行部分情报的分级分类，主要包括受影响国家、受影响企业	良好
	成熟运用 AI 技术实现全自动化暗网情报分级分类，支持情报价值、受影响国家、受影响企业、归属行业、事件类型等多维度评估	优秀

指标说明

本指标重点评估对暗网情报进行系统化分级与分类的能力。通过量化分级分类的自动化程度和维度覆盖范围，可客观反映情报分析环节的智能化水平，为后续的风险评估、事件研判以及应急处置工作，提供清晰的优先级指引，确保研判工作高效、精准开展。

5.3. 情报分析时效性

5.3.1. 设计目的

情报分析时效性是暗网情报智能分析能力的**关键指标之一**。其核心设计目的在于**评估对暗网情报进行分析处理的响应速度**。

暗网中的**高价值情报**具有**极强的时效性**，若分析处理延迟过长，可能导致相关主体在威胁出现的**关键窗口期**无法获得有效预警，错失**阻断威胁传播、降低安全损失**的最佳时机。

因此，该指标重点考察对**高价值情报的分析时效**，这一能力**直接关系到情报从原始采集到可行动成果的转化效率**，为风险评估和应急响应提供及时、可靠的决策支撑。

5.3.2. 设计依据

本指标的设计依据主要结合暗网情报的**时效性特征**与实际分析需求进行设定。

暗网中的高价值情报具有极强的时效性，其核心价值会随着时间推移快速衰减，若无法及时分析处理，将错过最佳的风险处置时机。同时，暗网数据存在显著特点 ——**海量性、非结构化、碎片化且伴随高噪音**，这使得实时全自动分析在技术层面存在较高难度。即便在国际范围内，一流的暗网情报分析机构，对高价值情报的自动化分析平均时长也多在 15 分钟至 2 小时之间，难以实现真正的秒级实时响应。

因此，本框架以**情报分析的自动化程度和响应延迟**作为核心量化标准，通过设定科学合理的分级阈值，确保该指标能够客观、准确地反映出情报分析的效率与水平，清晰呈现不同能力层级的差距，为后续的风险研判和应急处置提供可靠依据。

5.3.3. 指标参数

情报分析时效性以**高价值情报的分析响应延迟**作为核心量化指标，具体分级标准如下：

指标项	指标参数	评判等级
情报分析时效性	未进行系统化或明确的情报分析	基础
	半自动化对高价值暗网情报进行分析，延迟 < 24 小时	良好
	成熟运用 AI 技术，对高价值暗网情报自动化分析，延迟 < 1 小时	优秀

指标说明

本指标重点评估对高价值暗网情报的分析响应速度。通过量化分析延迟，可客观反映情报分析环节的时效性，为后续风险评估、事件研判和应急处置提供及时、可靠的决策支撑。

5.4. 多维度向量检索

5.4.1. 设计目的

多维度向量检索是暗网情报智能分析能力的**重要支撑指标**。其核心设计目的在于**评估对海量情报数据进行高效、精准检索的能力**。

暗网情报具有**海量性、碎片化、多源分散**的特点。若无法实现多维度向量检索，则难以在复杂数据中快速定位相关情报，导致情报利用效率低下，无法满足风险预警和事件溯源的实时需求。

因此，该指标重点考察**基于关键实体、分级分类、情报价值等多维度条件的向量检索能力**，直接关系到情报分析的便捷性和实用性，为后续知识图谱构建和风险决策提供快速、准确的数据支撑。

5.4.2. 设计依据

本指标的设计依据主要结合暗网情报的数据特征与实际分析需求进行设定。

暗网情报具有**海量性、碎片化、多源分散**的特点，传统关键词检索难以满足复杂查询需求。**向量检索技术**能够基于语义相似性实现高效定位。其中，单一维度向量检索主要依赖单一条件进行匹配，而**多维度联合查询向量检索**则可同时融合关键实体、分级分类、情报价值等多类条件，实现**更精准、更全面的关联检索**，其价值在于显著提升情报**定位效率和分析深度**。

因此，本框架以**向量检索的维度覆盖范围和查询能力**作为量化标准，通过设定合理的分级标准，确保该指标能够客观反映情报分析支撑能力上的实际差距。

5.4.3. 指标参数

多维度向量检索以**向量检索的维度覆盖范围和查询能力**作为核心量化指标，具体分级标准如下：

指标项	指标参数	评判等级
多维度向量检索	仅支持基于原始情报关键词的传统检索	基础
	支持基于关键实体和分级分类的向量检索	良好
	支持多维度联合查询条件向量检索（基于情报关键实体+分级分类）	优秀

指标说明

本指标重点评估对暗网情报进行多维度向量检索的能力。通过量化检索的维度覆盖范围和查询复杂度，可客观反映情报分析支撑环节的智能化水平，为后续知识图谱构建和风险决策提供高效、精准的数据支撑。

5.5. 情报知识图谱构建

5.5.1. 设计目的

建立**情报知识图谱**是暗网情报智能分析能力的**最高阶核心指标之一**。其核心设计目的在于：**评估将分散的原始情报转化为结构化、关联化知识体系的能力**。

暗网情报具有**高度碎片化、多源分散**的显著特征，原始数据往往分散在不同来源、不同场景中，缺乏系统性关联。若无法实现跨威胁源、跨事件、跨实体的知识图谱构建，将难以形成完整的威胁视图，导致各类情报相互孤立，无法有效支撑复杂威胁的溯源、深度研判及趋势预测，进而影响风险应对的及时性和准确性。

因此，本指标重点考察对知识图谱的**自动化构建与关联能力**，这一能力直接决定了暗网情报从 **“原始数据” 到 “可用知识” 的转化深度**，为威胁分析、风险评估及战略决策提供系统化、智能化的核心支撑，助力实现对暗网威胁的全面掌控和精准应对。

5.5.2. 设计依据

本指标的设计依据主要结合暗网情报的数据特征与分析实际需求进行设定。

建立**情报知识图谱**是暗网情报分析的**最高阶核心指标之一**，技术实现**难度极高**，主要源于暗网数据的**海量性、非结构化特性、碎片化分布以及威胁源的频繁波动**。即使是国际顶级的暗网情报分析机构，目前也仅能实现半自动化构建，仍需大量人工干预方可完成跨威胁源、跨事件、跨实体的关联整合。

因此，本框架以知识图谱构建的**自动化程度和关联范围**作为量化标准，通过设定合理的分级标准，确保该指标能够客观反映情报分析高阶能力上的实际差距。

5.5.3. 指标参数

建立以**知识图谱构建的自动化程度和关联范围**作为核心量化指标，具体分级标准如下：

指标项	指标参数	评判等级
建立情报知识图谱	未建立系统化或明确的知识图谱关联	基础
	支持半自动化知识图谱构建，可基于人工引导进行跨事件关联	良好
	实现全自动跨威胁源、发布者、威胁事件、实体的知识图谱构建与关联	优秀

指标说明

本指标重点评估将分散的原始情报转化为结构化、关联化知识体系的能力。通过量化知识图谱构建的自动化程度和关联范围，可客观反映在暗网情报分析最高阶环节的智能化水平，为复杂威胁溯源、研判和战略决策提供系统化支撑。

第六章 暗网情报高保真复制和持久化存档能力

暗网情报高保真复制和持久化存档能力是暗网威胁情报全链路能力体系中的关键支撑环节。其核心在于将采集到的原始情报以高保真方式完整保留，并实现长期安全存档，从而有效解决暗网站点频繁波动、查封或下线带来的访问难题。

Traditional Dark Web 和 Dark Web Lite 中的威胁源具有极高的不稳定性，论坛、泄露站点和群组经常因执法行动、运营商迁移或主动下线而消失。若无法对原始内容进行高保真复制和持久化存档，将会造成大量情报永久丢失，导致历史轨迹无法追溯，风险评估和事件研判缺乏完整依据。

因此，本章从高保真复制、多媒体解析、多媒体向量检索、持久化存档稳定性以及风险控制与便利性五个维度，构建暗网情报高保真复制和持久化存档能力的量化评估体系，旨在提供稳定、安全且便捷的原始情报访问能力，支撑长期历史分析和证据保全工作。

6.1. 高保真复制

6.1.1. 设计目的

暗网情报高保真复制是持久化存档能力的**基础性核心指标**，其核心设计目标在于**评估对暗网原始内容的完整复制能力**，是支撑暗网情报全流程处理、实现数据价值转化的重要基础。

暗网威胁源具备极强的**不稳定性**，各类论坛页面、泄露信息站点及群组消息，常因执法管控、地址迁移或主动关停等因素出现存续中断，导致**原始情报数据极易丢失**。若未能实现对原始内容的高保真复制，将造成大量核心情报**永久流失**，使得威胁历史轨迹无法追溯，进而导致风险评估与事件研判工作缺乏完整的数据支撑，影响研判结果的准确性与全面性。

因此，该指标核心聚焦于**对威胁源原始内容的完整复制能力**，重点考察对**文字信息、页面布局、附属文件、图像等各类多媒体元素**的完整复刻能力，其能力水平直接决定暗网情报的**原始性与可用性**，为后续持久化存档、多媒体解析及历史数据回溯分析等工作，提供坚实且可靠的基础支撑，是暗网情报从原始数据向可用信息转化的核心前提。

6.1.2. 设计依据

本指标的设计依据，主要结合暗网威胁源的实际特征与高保真复制的技术需求开展设定，确保指标设计的科学性、实用性与针对性，贴合暗网情报分析的实际工作需求。

暗网情报高保真复制工作面临显著的技术难点，核心在于暗网威胁源具备高度的**动态性与对抗性**：暗网网站页面结构复杂且多变，JS 动态渲染技术应用普遍，多媒体附件类型繁杂且体积差异悬殊，同时，暗网威胁源常因执法管控、运营商迁移或主动关停等因素，出现频繁的地址变更与内容删除情况。上述多重因素相互叠加，导致传统采集方式难以实现对暗网原始内容的完整、高保真复刻，无法满足后续情报分析与数据留存的核心需求。

因此，本评估框架以高保真复制的**完整性与覆盖范围**作为**核心量化标准**，重点评估对暗网威胁源原始内容的复制能力，涵盖**文字信息、页面布局、附属文件、图像等各类多媒体元素**的完整复刻。通过设定科学合理的分级标准，客观反映在暗网高对抗环境下的复制能力水平，为后续持久化存档、多媒体解析及历史数据回溯分析等工作，提供可靠、完整的基础数据支撑，保障整个暗网情报分析工作的有序推进。

6.1.3. 指标参数

高保真复制以对威胁源原始内容的**复制完整性**作为核心量化指标，具体分级标准如下：

指标项	指标参数	评判等级
高保真复制	仅获取威胁信息或消息文本，未对原始情报进行结构化复制	基础
	对威胁源原始内容进行部分复制，主要包含	良好

	文字和布局，但未完整复制多媒体元素	
	对威胁源原始内容进行高保真完整复制，保留文字、布局、附件、图像等多媒体元素	优秀

指标说明

本指标核心评估对暗网威胁源原始内容的复制完整性，通过量化复制的覆盖范围与保真程度，客观反映暗网原始内容的复刻能力水平，为后续多媒体解析、持久化存档及历史情报追溯等工作，提供坚实、可靠的技术支撑，确保原始情报的完整性与可用性，为后续风险研判和事件溯源提供基础数据支撑。

6.2. 多媒体解析与向量检索

6.2.1. 设计目的

多媒体解析与向量检索是暗网情报高保真复制和持久化存档能力的**重要支撑指标**。其核心设计目的在于**评估对非结构化多媒体内容的解析深度以及后续检索支持能力**。

暗网原始情报中包含大量**图片、附件等非结构化多媒体元素**，这些内容往往承载着**关键的威胁信息**。如果无法对多媒体内容进行有效解析并纳入向量检索范围，则难以充分利用原始情报中的深层价值，导致情报分析的完整性和准确性受到限制。

因此，该指标重点考察对**图片、附件等多媒体内容的深度解析能力及其与向量检索**的结合程度，直接关系到原始情报的可用性和后续分析效率，为风险评估和事件研判提供更全面的技术支撑。

6.2.2. 设计依据

本指标的设计依据，主要结合暗网原始情报的实际数据特征与实际分析需求

进行设定，确保指标的实用性与针对性。

多媒体解析与向量检索在暗网情报分析中具有**核心支撑价值**：通过对暗网原始情报中样例文件的深度解析，结合向量检索技术，可有效梳理暗网数据泄露的历史轨迹与跨平台传播路径，为威胁溯源、风险研判提供关键数据支撑，是连接原始数据与实用情报的**核心环节**。

需明确的是，该技术的实现高度依赖高保真内容复制作为前置条件，**技术落地难度较高**。从当前行业现状来看，全球范围内能够实现该技术能力的暗网情报相关机构，占比不足一半。

因此，本评估框架以**多媒体内容的解析深度**，以及解析结果与向量检索的结合程度作为核心量化标准，确保该指标能够客观、真实地反映平台在高保真复制后续环节的实际支撑能力，为暗网情报的深度分析提供可靠依据。

6.2.3. 指标参数

多媒体解析与向量检索以对非结构化多媒体内容的解析深度及其与向量检索的结合程度作为主要量化指标，具体分级标准如下：

指标项	指标参数	评判等级
多媒体解析与向量检索	不提取或不处理多媒体信息，无法进行向量检索	基础
	仅提供多媒体原始地址链接，不进行解析，无法支持向量检索	良好
	利用 OCR 和智能格式化技术，对图片、附件等非结构化多媒体内容进行深度解析，并支持多维度向量检索	优秀

指标说明

本指标重点评估平台对暗网情报中非结构化多媒体内容的解析深度，以及解析结果与向量检索的结合能力。通过量化解析的完整性、检索的精准性，可客观反映平台在高保真复制后续环节的实际支撑水平，为后续知识图谱构建、威胁溯源及风险决策提供高效的技术基础，确保暗网情报的深层价值得到充分挖掘与利用。

6.3. 持久化存档稳定性

6.3.1. 设计目的

持久化存档稳定性是暗网情报高保真复制和持久化存档能力的**重要保障性指标**。其核心设计目的在于**评估平台对高保真复制后的原始情报进行长期安全存档的能力**。

暗网威胁源具有极高的不稳定性，论坛页面、泄露站点和群组消息经常因**执法行动、地址迁移或主动下线**而消失。如果无法对原始情报进行**长期稳定的持久化存档**，则会造成大量**历史情报永久丢失**，导致无法追溯事件完整轨迹，影响后续的**风险评估、事件研判和证据保全**。

因此，该指标重点考察在高保真复制基础上的**长期存档稳定性和抗风险能力**，直接关系到情报的长期可用性和连续性，为历史分析和合规要求提供可靠的技术支撑。

6.3.2. 设计依据

本指标的设计依据，主要结合**暗网威胁源的波动特征**与**长期存档实际需求**进行设定。

由于暗网威胁源波动频繁，一旦出现**地址迁移、查封或下线，原始信息尤其是多媒体内容**极难找回。因此，本框架以**持久化存档的稳定性**和**对原始情报源的依赖程度**作为核心量化标准，重点评估在高保真复制基础上的**长期存档效果**。通

过设定合理的分级标准，确保该指标能够客观反映**情报长期可用性**上的实际差距。

6.3.3. 指标参数

持久化存档稳定性以**对原始情报的长期存档稳定性**和**对原始情报源的依赖程度**作为主要量化指标，具体分级标准如下：

指标项	指标参数	评判等级
持久化存档稳定性	仅对威胁信息或消息文本进行基本存档，详细内容依赖原始情报源	基础
	对原始情报的文本和消息内容进行长期持久化存档，多媒体部分依赖原始情报源	良好
	对高保真复制的原始情报进行长期稳定持久化存档，有效应对威胁源波动、查封或下线风险	优秀

指标说明

本指标重点评估对高保真复制后的原始情报进行长期安全存档的能力。通过量化存档稳定性和对原始情报源的依赖程度，可客观反映应对暗网威胁源波动时的持久化能力，为情报的长期可用性和历史追溯提供重要技术支撑。

6.4. 风险控制与使用便利性

6.4.1. 设计目的

风险控制与便利性是暗网情报高保真复制和持久化存档能力的**重要应用**，其核心设计初衷是**为用户提供安全便捷的情报分析环境**。

暗网原始情报的访问通常需要**使用 Tor 网络、注册暗网账号或进行其他高**

风险操作，这不仅增加了用户自身的**风险**，还显著降低了情报使用的便捷性。若无法有效平衡风险控制与使用便利，会限制情报的实际应用价值，影响安全团队的日常研判和响应效率。

因此，该指标重点考察通过高保真复制技术实现的**用户零暴露、零注册访问能力**，直接关系到情报使用的**安全性和实用性**，为暗网情报应用提供**低风险、高便利**的技术支撑。

6.4.2. 设计依据

本指标的设计依据主要结合**暗网情报使用的实际环境**与**用户需求**进行设定。

该技术的重要性体现在两个方面。首先，由于 Tor 网络本身的**不稳定性**，以及大量黑客论坛、交易市场等威胁源均需要**注册会员**或**缴纳会费**才能访问核心情报内容，导致传统情报分析工作面临**极大的不便**。其次，暗网环境充斥着**巨大风险**，无论是注册时的**身份暴露**、缴费过程中**个人隐私泄露**，还是暗网中可能存在的**病毒、恶意程序**等，都可能让直接访问者面临**严重的潜在威胁**。

因此，本框架以**风险控制与便利性**作为量化标准，重点评估通过高保真复制技术实现的用户**零暴露、零注册访问能力**，从而为暗网情报应用提供**低风险、高便利**的技术支撑。

6.4.3. 指标参数

风险控制与便利性以用户访问原始情报的**安全性和便捷程度**作为主要量化指标，具体分级标准如下：

指标项	指标参数	评判等级
风险控制与便利性	用户仅能获取基本消息，查看具体原始情报内容时需登录原始地址	基础

	用户无需使用 Tor 网络或 APP 即可查看主要情报内容，但查看附件或多媒体元素时需登录原始地址	良好
	用户无需使用 Tor 网络或任何其他 APP、无需注册或购买账号，即可安全、便捷地查看原始情报	优秀

指标说明

本指标重点评估通过高保真复制技术为用户提供的风险控制与便利性水平。通过量化用户访问原始情报的**安全性和便捷程度**，可客观反映在实际应用场景中的可用性，为暗网情报分析提供低风险、高效率的技术支撑。

第七章 中文暗网生态环境威胁识别能力

中文暗网生态是以**中文**为核心交互语言，依托传统匿名网络与加密通信工具构建，具备**本土化、圈层化、高指向性**特征的地下威胁生态，是国内数据泄露交易、IAB 买卖、侵公类活动、勒索软件通告、黑灰产协同运作的主要承载场景。该生态呈现**中文 Traditional Dark Web** 与**中文 Dark Web Lite** 并行共生、境内外联动的格局，威胁行为更贴合本土监管环境与机构运行特征，识别难度与治理价值显著高于通用暗网生态。

本章立足中文暗网生态的**语言专属特性、本土威胁场景**与**侵公类风险高发**等核心特征，从中文 Traditional Dark Web 识别、中文 Dark Web Lite 识别、侵公威胁源识别三个维度，构建中文暗网生态环境威胁识别能力量化评估体系，用以全面衡量对本土地下威胁的精准发现、专属适配与深度研判能力，为暗网情报体系的本土化落地、全域威胁感知与合规治理提供**专属化、可量化、可核验**的能力依据。

7.1. 中文 Traditional Dark Web 识别

7.1.1. 设计目的

中文 Traditional Dark Web 识别能力，是**中文暗网生态环境威胁识别能力**的**基础性核心指标**。本指标核心设计目的，在于对面向中国境内的网络安全相关网络犯罪生态范畴内 Traditional Dark Web 威胁源的**识别能力**与**覆盖程度**开展评估。

相较于国际通用暗网生态，中文 Traditional Dark Web 具备显著的**本土化特征**与**复杂语境属性**。若无法对该类本土化威胁源实现有效识别与全域覆盖，则难以发现针对中国境内主体的定向威胁活动，易形成情报覆盖盲区，进而削弱风险预警工作的**及时性**与**完整性**。

因此，本指标重点考察对中文 Traditional Dark Web 主要威胁源的**识别深度**，该项能力直接决定本土化暗网威胁场景下情报获取的有效性，可为后续威胁分析、风险预警与应急处置工作提供**具备针对性**的数据支撑。

7.1.2. 设计依据

本指标的设计依据，主要结合**中文 Traditional Dark Web** 威胁源的实际分布特征与情报价值进行设定。

在英文体系黑客论坛及勒索组织载体中，面向中国境内的泄露事件发布行为通常较为零散且非定期，缺乏**系统性**与**持续性**。而中文暗网交易市场呈现**大量、高频**发布境内相关数据的显著特征，已成为境内网络安全相关网络犯罪生态的重要**集散地**。

因此，本框架以面向中国境内的网络安全相关网络犯罪生态范畴内 Traditional Dark Web 威胁源的**识别深度**作为量化标准，重点评估对本土化暗网威胁源的**覆盖能力**。通过设定科学合理的分级标准，确保该指标能够客观反映主体在中文 Traditional Dark Web 识别维度的实际能力差异。

7.1.3. 指标参数

中文 Traditional Dark Web 识别以面向中国境内的网络安全相关网络犯罪生态暗网威胁源的**覆盖深度**作为主要量化指标，具体分级标准如下：

指标项	指标参数	评判等级
中文暗网 Traditional Dark Web 的识别	不支持专门面向中文 Traditional Dark Web 威胁源监测	基础
	覆盖至少 2 个主要中文 Traditional Dark Web 平台	良好
	深度监测并覆盖至少 5 个主要中文 Traditional Dark Web 平台	优秀

指标说明

本指标重点评估对中文 Traditional Dark Web 威胁源的**识别能力**与**覆盖能力**。通过量化覆盖深度，可客观反映主体在本土化暗网生态中的识别水平，为后续情报分析与风险预警提供**具备针对性**的数据支撑。

7.2. 中文 Dark Web Lite 识别

7.2.1. 设计目的

中文 Dark Web Lite 识别能力，是**中文暗网生态环境威胁识别能力**的**重要构成指标**。本指标核心设计目的，在于对网络安全相关中文 Dark Web Lite 威胁源的**识别能力**与**覆盖程度**开展评估。

Dark Web Lite 为当前数据泄露贩卖、勒索通告、IAB 交易及侵公查档等威胁活动的**主要承载载体**，其中中文相关群组与频道具备**传播速率快、迭代频次高、总体规模大**的典型特征。若无法对该类本土化威胁源实现有效识别与全域覆盖，

则难以及时发现面向中国境内主体的定向威胁活动，易形成情报覆盖盲区，进而削弱风险预警工作的**及时性**与**完整性**。

因此，本指标重点考察对中文 Dark Web Lite 威胁源的**采集规模**与**识别深度**，该项能力直接决定本土化暗网威胁场景下情报获取的有效性，可为后续威胁分析、风险预警与应急处置工作提供**具备针对性**的数据支撑。

7.2.2. 设计依据

本指标设计依据主要结合**中文 Dark Web Lite** 威胁源的实际分类特征与监测需求进行设定。

中文 Dark Web Lite 生态内的网络安全相关威胁源主要可划分为三类：其一为**数据发布与交易类**群组，对应境外数据泄露与窃密日志交易类频道；其二为黑灰产**数据专卖类**群组，涵盖电商消费数据、交通出行实时数据等境内敏感数据交易载体；其三为**侵公类**数据相关群组，包含个人信息挖掘、定向查档类服务载体。

对上述类型威胁源实施有效监测具备重要价值：一方面，监测广度直接决定面向中国境内主体定向威胁活动的**及时发现能力**；另一方面，唯有实现三类威胁源的全面识别，方可构建完整的本土化威胁视图，消除情报覆盖盲区，为风险预警与应急处置提供可靠支撑。

因此，本框架以威胁源**采集数量**作为量化标准，通过设定科学合理的分级阈值，确保指标可客观反映主体在中文 Dark Web Lite 识别维度的实际能力水平。

7.2.3. 指标参数

中文 Dark Web Lite 识别以威胁源**采集数量**作为主要量化指标，具体分级标准如下：

指标项	指标参数	评判等级

中文暗网 Dark Web Lite 的识别	不支持专门面向中文 Dark Web Lite 威胁源监测	基础
	采集网络安全相关中文 Dark Web Lite 威胁源数量 > 500	良好
	采集网络安全相关中文 Dark Web Lite 威胁源数量 > 2000	优秀

指标说明

本指标重点评估对中文 Dark Web Lite 威胁源的**识别能力**与**覆盖能力**。通过量化威胁源群组与频道的采集数量，可客观反映主体在本土化暗网生态中的**覆盖广度**，为后续情报分析、风险预警与应急处置提供重要的数据支撑。

7.3. 侵公威胁源识别

7.3.1. 设计目的

侵公威胁源识别是**中文暗网生态环境威胁识别能力**的**重要专项指标**。本指标核心设计目的，在于对侵公、查档类本土化威胁源的**识别能力**与**预警能力**开展评估。

侵公威胁属于中文暗网生态中具备**高度本土化特征**的典型风险形态，核心指向通过非法渠道侵害公民个人隐私数据的相关行为。若无法对该类威胁源实现有效识别，则难以及时发现面向中国境内主体的隐私数据贩卖活动，致使相关风险长期处于隐匿状态，无法为境内主体提供具备针对性的预警与防护支撑。

因此，本指标重点考察对侵公、查档类威胁源的**采集能力、识别能力与预警能力**，该项能力直接决定本土化隐私泄露威胁的早期发现水平，可为境内主体隐私保护及合规风险管理提供关键技术支撑。

7.3.2. 设计依据

本指标设计依据主要结合**侵公威胁源**的实际特征与情报价值进行设定。

侵公类数据具备**实时性强、完整性高、合法获取难度大、信息要素全面**等显著特征，其主要来源为**内部权限主体**或**上下游数据权限提供方**的**非法查询服务**，少量来源于应用程序编程接口漏洞等技术层面缺陷。该类数据与传统暗网环境中发布的数据集，在**获取途径、持续危害程度、研判处置难度**等方面存在本质差异。

传统暗网数据集多呈现一次性泄露特征，而侵公类数据通常具备**持续更新、精准查询**的能力，对公民个人隐私与机构内部信息安全构成**长期且直接**的威胁。因此，本框架以侵公威胁源的**识别深度**与**预警能力**作为量化标准，重点评估对该类本土化高风险威胁的监测水平。通过设定科学合理的分级标准，确保指标可客观反映主体在中文暗网生态环境中的专项识别能力。

7.3.3. 指标参数

侵公威胁源识别以对侵公、查档类威胁源的**采集与识别深度**作为主要量化指标，具体分级标准如下：

指标项	指标参数	评判等级
侵公威胁源识别	不支持专门面向侵公、查档类威胁源识别	基础
	能采集并识别较多侵公、查档类威胁源	良好
	深度识别并预警侵公、查档类威胁源，对附件、图像等多媒体元素进行 OCR 分析并提供向量检索	优秀

指标说明

本指标重点评估对侵公、查档类威胁源的**识别能力**与**预警能力**。通过量化识

别深度与覆盖范围，可客观反映主体在本土化隐私泄露威胁监测中的实际水平，为境内主体隐私保护及合规风险管理提供关键技术支撑。

第八章 海量泄露数据知识库能力

海量泄露数据知识库是暗网情报体系中**数据资产汇聚、价值提炼、长期复用**的核心支撑载体，承载全域历史泄露数据与新增泄露数据的标准化治理、规模化存储、智能化检索功能。该知识库以**高保真、去重化、结构化、安全化**为建设准则，面向全域数据泄露事件提供全周期数据支撑，是实现威胁溯源、风险预警、事件核验、态势分析的关键基础。本章立足海量数据的**治理难度、响应速度、扩展能力**等核心特征，从历史知识库积累规模、新增数据扩展速度、数据库响应速度三个维度，构建海量数据知识库能力量化评估体系，用以全面衡量数据治理、知识沉淀、快速检索与动态扩展的综合水平，为暗网威胁研判与数据泄露治理提供**规模化、标准化、可量化**的底层能力支撑。

8.1. 历史知识库积累规模

8.1.1. 设计目的

历史知识库积累规模是**海量泄露数据知识库能力**的**基础性核心指标**。本指标核心设计目的，在于对长期积累的风险情报数据集的**积累规模**与**数据质量**开展评估。

暗网威胁情报具备显著的**历史积累价值**。若历史知识库规模不足或数据质量未达标准，则难以支撑长期历史轨迹追溯与跨事件关联分析，无法为全域风险画像构建与趋势研判提供有效支撑。

因此，本指标重点考察历史知识库的**积累规模**与**数据处理水平**，该项能力直接决定情报分析的**深度**与**广度**，为全域风险预警机制构建提供坚实的数据基础。

8.1.2. 设计依据

本指标设计依据主要结合暗网情报的**长期积累价值**与**实际处理难度**进行设定。

暗网情报历史知识库总量规模可达千亿级以上，但受暗网数据**碎片化显著、结构差异巨大、重复度偏高**等特征影响，实施统一结构化清洗、去重与格式化处理的技术难度较高。因此，本框架以历史知识库的**积累规模**与**数据处理水平**作为量化标准，重点评估长期积累的风险情报数据集的体量与质量。通过设定科学合理的分级标准，确保指标可客观反映主体在知识库基础能力维度的实际差异。

8.1.3. 参数指标

历史知识库积累规模以知识库**数据规模**作为主要量化指标，具体分级标准如下：

指标项	指标参数	评判等级
历史知识库积累规模	历史知识库规划中	基础
	已建立历史知识库，但未进行严格清洗、去重与格式化处理	良好
	已积累经严格清洗、去重、格式化并进行安全处理的知识库数据 > 100 亿	优秀

指标说明

本指标重点评估长期积累的风险情报数据集的**规模**与**处理水平**。通过量化知识库数据规模，可客观反映主体在历史数据治理能力上的实际差异，为后续情报分析、风险预警与事件研判提供重要的数据基础。

8.2. 新增数据扩展速度

8.2.1. 设计目的

新增数据扩展速度是**海量泄露数据知识库能力**的**重要动态指标**。本指标核心设计目的，在于对知识库的**持续增长能力**与**动态更新能力**开展评估。

暗网威胁情报具备显著的**时效性**与**动态性**，新泄露事件、新增数据交易及攻击活动每日持续产生。若新增数据扩展速度不足，则难以适配暗网威胁的演化节奏，易造成知识库时效性衰减，无法为及时、有效的风险预警与趋势研判提供支撑。

因此，本指标重点考察每日新增入库数据的**规模**与**稳定性**，该项能力直接决定知识库的**时效性**与**长期应用价值**，为全域风险预警机制构建提供持续性的数据支撑。

8.2.2. 设计依据

本指标设计依据主要结合暗网威胁情报的**动态性**与知识库持续更新需求进行设定。

知识库增量水平，是判别知识库能否保持**时效性**与**长期有效性**的重要依据。事件驱动型扩展通常呈现爆发式增长特征，但**稳定性**相对不足；常态化运营可实现每日稳定、持续的增量更新，更有利于知识库**长期价值**的沉淀与积累。

因此，本框架以每日新增入库数据的**规模**与**稳定性**作为量化标准，通过设定科学合理的分级标准，确保指标可客观反映主体在知识库动态更新能力维度的实际差异。

8.2.3. 参数指标

新增数据扩展速度以每日新增入库数据的**规模**与**稳定性**作为主要量化指标，具体分级标准如下：

指标项	指标参数	评判等级
新增数据扩展速度	知识库更新规划中	基础
	随事件不定期扩展	良好
	每天稳定新增入库数据量在数千万量级以上	优秀

指标说明

本指标重点评估知识库的**持续增长能力**与**动态更新能力**。通过量化每日新增入库数据的规模与稳定性，可客观反映主体在知识库动态更新能力上的实际差异，为保障知识库**时效性**与**长期价值积累**提供重要支撑。

8.3. 数据库响应速度

8.3.1. 设计目的

数据库响应速度是**海量泄露数据知识库能力**的**关键效能指标**。本指标核心设计目的，在于对知识库在数据检索、订阅、输出等全流程操作中的**响应效率**开展评估。

海量泄露数据知识库面向超大规模非结构化数据开展查询与订阅操作，数据体量庞大、关联维度复杂，响应时延直接决定威胁研判、风险核验与预警推送的**实时性**。若响应速度不足，将导致情报获取滞后、研判效率降低，无法满足暗网威胁**快速发现、快速核验、快速处置**的实战需求。

因此，本指标重点考察从指令输入至结果全量返回的**耗时水平**，该项能力直接决定知识库的**实战可用度**与**运营效能**，为全域风险预警与事件快速研判提供**高效率、低时延**的底层支撑。

8.3.2. 设计依据

本指标设计依据主要结合海量泄露数据知识库的**数据规模、检索复杂度**与**实战化响应**需求进行设定。

海量暗网泄露数据知识库具备**体量巨大、结构异构、关联关系复杂**等特征，全量检索与多条件联合查询对算力、索引结构、数据治理水平提出较高要求。响应速度是衡量知识库**底层架构合理性、索引优化能力、数据治理成熟度**的核心外在表现。在实战场景中，情报检索与订阅的时延直接影响威胁闭环效率，**低时延响应**是实现威胁早发现、早处置的重要前提。

因此，本框架以指令输入至结果全量返回的**完成耗时**作为量化标准，通过设定科学合理的分级阈值，确保指标可客观反映主体在知识库高性能支撑能力维度的实际差异。

8.3.3. 参数指标

数据库响应速度以指令输入至结果全量响应完成的**耗时**作为主要量化指标，具体分级标准如下：

指标项	指标参数	评判等级
数据库响应速度	输入-全部响应完成 > 15 秒	基础
	输入-全部响应完成 < 15 秒	良好
	输入-全部响应完成 < 5 秒	优秀

指标说明

本指标重点评估知识库的**响应效率**。通过量化指令输入至全量结果返回的耗时，可客观反映主体在海量数据处理与高性能查询方面的实际能力，为保障情报研判实时性与威胁处置高效率提供关键支撑。

第九章 事件处置与响应闭环能力

事件处置与响应闭环是暗网情报从**威胁发现**向**风险消除**转化的最终落地环节，贯穿事件研判、溯源调查、危机应对、合规报送全流程，是实现暗网威胁**早发现、早研判、早处置、早闭环**的核心保障。该能力以**真实性核验、全链条溯源、全流程指导、风险压降**为核心目标，面向各类暗网数据泄露与威胁通告提供标准化处置路径，直接决定威胁治理的最终成效与影响控制水平。本章立足暗网威胁事件的**突发性、隐蔽性、扩散性、合规性**等核心特征，从暗网事件风险等级研判、协助泄露源调查、危机应对指导三个维度，构建事件处置与响应闭环能力量化评估体系，用以全面衡量威胁研判精准度、调查支撑力度与危机应对专业度，为暗网威胁事件的**全流程闭环治理、合规化处置、风险最小化**提供可量化、可落地的能力标尺。

9.1. 暗网事件风险等级研判

9.1.1. 设计目的

暗网事件风险等级研判是**事件处置与响应闭环能力**的**核心基础性指标**。本指标核心设计目的，在于对暗网泄露事件的**真实性判定、新旧程度区分、威胁轨迹追溯、风险综合定级**能力开展评估。

暗网威胁事件具有**来源混杂、真伪难辨、历史跨度大、影响范围广**等特征，若缺乏系统化研判机制与历史数据支撑，将无法准确判定事件危害等级与扩散态势，难以形成科学处置优先级，进而延误响应时机、扩大风险危害。

因此，本指标重点考察事件**真实性核验能力、历史轨迹追溯时长、全维度研判完整性**，该项能力直接决定威胁事件的**判定精准度**与**处置优先级合理性**，为全域风险管控与应急响应提供**可靠、权威、可落地**的研判依据。

9.1.2. 设计依据

本指标设计依据主要结合暗网威胁事件的**隐蔽性、扩散性、溯源难度**与实战化处置需求进行设定。

暗网数据泄露事件普遍存在重复发布、旧闻新发、部分伪造、分段泄露等现象，单一时间点信息无法完整反映事件真实状态。长期历史数据积累与跨威胁源关联追溯，是区分**新发事件与历史事件、真实泄露与虚假通告、完整泄露与片段泄露**的关键依据。追溯时长越长、覆盖维度越全，研判结论可信度越高。

因此，本框架以事件**真实性研判能力、威胁轨迹完整性、历史追溯时长**作为量化标准，通过设定科学合理的分级阈值，确保指标可客观反映主体在暗网事件风险定级与深度研判维度的实际能力水平。

9.1.3. 参数指标

暗网事件风险等级研判以事件**研判完整性、真实性核验能力、历史轨迹追溯时长**作为主要量化指标，具体分级标准如下：

指标项	指标参数	评判等级
暗网事件风险等级研判	仅可进行部分暗网泄露事件真实性、新旧等维度研判，无历史积累用于研判	基础
	可对任意暗网泄露事件进行真实性、新旧等维度研判，暗网轨迹追溯时间 > 1 年	良好

	可对任意暗网泄露事件进行真实性、新旧等维度研判，可输出事件全部暗网轨迹，追溯时间 > 3 年	优秀

指标说明

本指标重点评估对暗网泄露事件的**真实性判定、风险定级、全轨迹追溯**能力。通过量化追溯时长与研判完整性，可客观反映主体在威胁事件深度分析与风险评估方面的实战水平，为应急处置、优先级排序与风险压降提供关键支撑。

9.2. 协助泄露源调查

9.2.1. 设计目的

协助泄露源调查是**事件处置与响应闭环能力**的关键实操指标。本指标核心设计目的，在于评定针对泄露事件源头排查、链路溯源工作的全程支撑效能，规避实操环节各类合规风险与违规操作行为。

暗网相关溯源场景存在大量高风险实操环节，涉资金往来、匿名访问、私密社群准入、违规数据获取等行为均存在合规隐患。若相关支撑力度不足，易导致落地排查流程中必须介入高危操作，放大整体风险边界。

因此，本指标重点核验溯源支撑环节对**违规操作的规避能力**，直接决定排查工作的合规安全性与落地可行性，为泄露源头清查与链路研判提供合规化实操依据。

9.2.2. 设计依据

本指标设计依据主要结合泄露溯源场景的**合规红线、实操风险、业务支撑边界**综合确立。

泄露溯源的作业环境全程处于暗网生态，该场景匿名性强、风险触点密集、法律边界模糊，且溯源本身存在极大不确定性，最终成功率受多方客观因素影响，

技术层面无法做到绝对保障。因此开展所有溯源工作，**首要核心绝非追求溯源结果，而是全程优先保障用户人身安全与操作合规**。

常规溯源动作中，涉及私下谈判转账、搭建匿名链路、入驻黑客社群、下载敏感泄露数据等行为，均触碰高风险红线；一旦由用户自主操作，极易引发安全隐患与合规风险。

故此本指标评判暗网情报支撑能力，核心标准聚焦一点：**能否依托自有能力隔绝高危操作，让用户全程零触碰、零风险参与溯源**。以此划定分级梯度，客观体现不同服务层级下，对用户安全与合规的兜底保障能力。

9.2.3. 参数指标

协助泄露源调查以溯源工作中**违规操作的全流程替代支撑能力**为核心量化指标，具体分级标准如下：

指标项	指标参数	评判等级
协助泄露源调查	对用户不提供实操类调查支撑，仅可输出理论咨询内容	基础
	可协助用户完成部分调查工作，剩余环节需用户自主推进，完整排查流程无法完全规避违规操作	良好
	可协助用户完成生态级全链条调查，全程用户无需开展支付、谈判、匿名访问、圈层注册、匿名介质使用、原始数据获取等各类违规操作	优秀

指标说明

本指标重点评定泄露源头调查工作的**合规支撑能力**与**实操替代水平**。通过明确违规操作的规避边界，可客观界定溯源支撑的安全层级，为泄露事件合规化排

查、风险溯源及闭环处置提供标准化判定依据。

9.3. 危机应对指导

9.3.1. 设计目的

危机应对指导是**事件处置与响应闭环能力**的**重要组成部分**。本指标核心设计目的，在于评估**针对暗网事件输出全流程合规应对支撑的专业能力**。

暗网相关事件爆发后，往往将面临**数据泄露扩散、品牌声誉受损、合规追责承压**等多重风险。若无系统化、可落地的危机应对支撑，难以规范完成事件研判报告编制、涉案证据归集提交、监管与公安单位协同配合等关键动作，易长期处于被动处置状态，进而加剧事件影响范围与损失程度。

因此，本指标重点考核**协助对接网络安全监管部门及公安机关**，完成**分析报告编撰、证据材料规整报送、全程配合调查取证**等全链条实操工作的能力，直接决定事件能否由被动补救转为主动处置，为最大限度压降**经济损失、声誉风险与合规隐患**提供关键支撑。

9.3.2. 设计依据

本指标设计依据，结合暗网事件爆发后的**合规处置要求、取证规范标准、对公对接流程**综合确立。

暗网相关泄露事件涉及监管核查与公安取证流程，相关材料撰写、证据固化、流程对接均有严格规范；若无专业支撑，极易出现材料不合规、证据链路断裂、对接流程疏漏等问题，直接影响整体处置成效。

实战场景中，能否全程协助完成报告编撰、证据规整、取证配合等对公全流程工作，是实现**主动控险、压降影响**的核心关键；仅能按需提供局部协助，无法实现全流程闭环支撑；仅提供口头咨询，则无法落地实际对公对接与材料报送。

以此分级划定标准，可客观体现对应的**对公协助能力、材料支撑能力与取证配合能力**，贴合实战中合规报备与风险止损的核心需求。

9.3.3. 参数指标

危机应对指导以对公协助、材料支撑与取证配合的**全流程落地能力**为核心量化标准，具体分级如下：

指标项	指标参数	评判等级
危机应对指导	仅提供咨询服务	基础
	针对暗网事件进行响应，基于用户需求进行协助，无法进行全流程主动推进和提供危机应对指导	良好
	针对暗网事件，可协助用户向网络安全监管单位或公安机关撰写分析报告、提交证据材料、配合调查取证等全流程工作，化被动为主动，最大限度降低事件带来的影响和损失	优秀

指标说明

本指标重点评估暗网事件发生后的**对公对接、材料整编、取证协同**实操能力，通过量化全流程协助落地效果，客观体现危机阶段主动控险、合规报备、压降损失的实际支撑水平。

第十章 2026 版框架体系结语

本框架系统梳理了暗网威胁情报从**采集、对抗、分析、存档到响应闭环的全链路技术能力维度**，配套完善量化判定标准与分级参数，旨在形成一套可落地、可对标、可复盘的统一评估依据。

通过对 Traditional Dark Web 与 Dark Web Lite 的双生态暗网场景全面覆盖，同时针对原始情报采集、深度研判分析、历史数据归档、本土化威胁识别、溯源调查支撑、危机合规引导等关键环节完成精细化指标设计，可直观厘清能力短板、明确优化方向，为后续针对性补强提供清晰可行的落地思路。

本框架为指导性参考文件，无强制约束要求，不固定评分权重与执行细则。可结合实际业务场景、风险管控需求与现有资源条件，灵活调整、适配优化相关指标内容。

当前暗网威胁情报领域技术迭代迅速、威胁形态持续演变，攻防对抗节奏不断升级。期望本框架能够为行业提供务实参考，共同推动暗网威胁情报相关能力，朝着**体系化、专业化、实战化**方向稳步精进，夯实常态化风险防控与应急处置支撑能力。

第十一章 未来展望

暗网情报技术是我国网络安全所有细分技术领域中发展最为滞后的技术领域，与国际前沿技术存在 10 年以上的代差。本框架指标中已提出的技术领域和量化参数，均围绕当前国际主流和成熟的技术分类与能力要求进行设计，旨在为国内行业提供统一、可量化、可落地的能力建设标尺。而本章节则主要基于国际暗网情报领域的前沿技术和演进趋势，对未来国内暗网情报能力建设进行前瞻性预研，为行业后续的技术迭代、能力提升和战略规划提供方向指引。

11.1. 设计目的

本章旨在对暗网情报技术能力框架进行前瞻性展望，系统分析暗网威胁生态的未来演变趋势、情报技术能力的演进方向，以及本框架的迭代优化建议。随着人工智能、量子计算、Web3.0、自动化攻击链等新兴技术的深度融合，以及 Traditional Dark Web 与 Dark Web Lite 双生态的进一步交织融合，暗网威胁呈现出更强的组织化、智能化、跨域化特征。传统被动采集与分析模式将难以满足实战

需求，本框架需主动适应这一趋势，为行业提供可落地、可迭代、可扩展的战略指引，推动国内暗网情报能力向预测性、自动化、全域闭环方向高质量发展，助力关键信息基础设施、企业数据安全与社会公共利益的长期韧性建设。

11.2. 暗网威胁生态未来演变趋势

未来 3—5 年内，暗网威胁生态将呈现以下核心演进特征：

1. **双生态深度融合与边界模糊化：**Traditional Dark Web 的核心攻击组织与数据策源功能将更多通过 Dark Web Lite 实现实时分发与协同，Telegram 等加密社群将成为 IAB 交易、勒索通告、窃密日志的主要流通渠道，威胁源迁移速度进一步加快，采集与反爬对抗难度指数级上升。

2. **侵公类威胁向多元化和国际化发展：**犯罪分子通过更广泛的地下招募渠道，实现更深层次的内外勾结，能够提供和出售类型更加丰富多样的公民隐私数据；同时，其业务范围已不再局限于境内市场，正逐步向新加坡、香港、澳门、台湾、马来西亚、印度尼西亚等海外地区扩张，侵公类交易呈现明显的国际化趋势。

3. **威胁智能化与自动化升级：**RaaS 服务将深度集成 AI 辅助攻击工具，infostealer 日志与浏览器指纹数据将实现自动化清洗与交易；数据泄露与 IAB 交易将更多呈现“低噪声、高频次、小批量”的流通特征。

4. **跨域与 cyber-kinetic 风险凸显：**暗网情报不再局限于数据泄露，而是与物理世界基础设施（如能源、金融、交通）形成联动，勒索软件攻击将更多指向供应链与关键信息基础设施，数据泄露事件的影响面从“信息资产”扩展至“物理-网络融合”风险。

5. **监管与执法反制下的高动态波动：**国际合作执法行动、平台封禁、加密协议升级将持续推动威胁源地址轮换与加密层级提升，Dark Web Lite 的邀请制、临时群组特征将更加突出，传统采集手段的时效性窗口进一步

压缩。

11.3. 暗网情报技术能力未来发展方向

为应对上述趋势，暗网情报技术能力需在现有七大核心能力域基础上实现以下突破：

1. **采集能力向全域自动化与自适应演进：**Traditional Dark Web 的反爬对抗将引入 AI 驱动的动态指纹伪装与自适应爬虫；Dark Web Lite 采集将实现多模态（消息、图片、附件、视频）全自动解析与向量嵌入，支持 TB 级超大附件智能定位与风险预判。

2. **智能分析能力向预测性与因果推理升级：**基于大模型与知识图谱的因果推理引擎将成为标配，实现“威胁者 TTP 预测”“潜在泄露风险链路推演”“攻击路径自动化模拟”；同时需强化对多元化公民隐私数据及跨区域国际化交易模式的语义理解与实体关联能力，支持多语言、跨司法管辖区的精准研判。

3. **高保真存档与知识库能力向量子安全与分布式演进：**采用后量子加密算法实现高保真情报的长期存档；海量泄露数据知识库将构建联邦学习机制，支持跨机构隐私保护下的联合建模，提升事件处置与响应闭环的协同效率。

4. **事件处置与响应闭环向自动化编排与闭环反馈演进：**实现“采集—分析—研判—溯源—阻断—反馈”的全流程自动化编排，结合 SOAR 平台形成秒级响应能力；中文暗网生态环境威胁识别将融入实时行为画像与风险评分模型，支持侵公威胁的自动化等级研判与应急指导。

5. **能力评估体系向动态量化与 AI 辅助评估演进：**本框架的量化指标将引入实时自适应阈值，支持 AI 驱动的能力成熟度自动评估；新增“预测性情报输出准确率”“自动化响应覆盖率”等新兴指标，实现框架与实战的

动态对齐。

11.4. 本框架未来迭代方向

本框架作为指导性技术文件，将保持开放迭代属性，构建暗网情报技术共享，预期每 12—18 个月进行一次版本更新，重点纳入以下内容：

1. 新增能力域或指标项（如量子安全采集对抗、多模态 AI 分析、联邦学习知识库等）。

2. 动态调整量化阈值，参考全球最新报告（Javelin、Gartner、Forrester 等）与国内实战数据进行校准。

3. 强化与国家网络安全监管政策、数据安全法、个人信息保护法的深度适配，增加合规性边界指标。

4. 构建配套评估工具与参考实现指南，支持政企机构开展能力自评与供应商选型。

通过持续迭代，本框架将始终保持科学性、实战性与前瞻性，成为国内暗网情报领域标准化、专业化、实战化的参考标尺。

11.5. 结语

暗网情报能力建设是一场没有终点的持久战。未来，唯有坚持技术创新与生态协作并重，构建“采集—分析—存档—响应—反馈”的智能化闭环，才能在复杂对抗环境中始终占据主动。本框架的发布与迭代，目的正是为行业提供统一、科学、可落地的能力标尺，助力国内网络安全产业向高质量发展迈进，共同守护数字中国的网络空间安全与数据主权。

参考文献

1. *Javelin Strategy & Research, Dark Web Threat Intelligence Vendor Scorecard, 2025*

2. *Gartner, Market Guide for Security Threat Intelligence Products and Services, 2024*

3. *Forrester, The State of Threat Intelligence, 2025*

4. *Forrester, External Threat Intelligence Service Providers Landscape, 2025*

5. *Flashpoint, Technical Analysis of High-Wall Underground Forums: XSS and Exploit, 2025*

6. *Recorded Future, Defense Mechanisms in Russian Cybercrime Forums: XSS.is and Exploit.in Case Study, 2025*

7. *Flare Systems, Telegram Cybercrime Ecosystem Report, 2025*

8. *Chainalysis, Crypto Crime Report 2025*