实体安防威胁行为知识库：基础字典表（v0.3 可推理升级版）

> 版本：v0.3 可推理升级版
> 更新日期：2026年6月
> 文件名：实体安防威胁行为知识库_基础字典表_v0.3_可推理升级版_JSON附录版.md
> 基础版本：v0.2 国际化升级版
> 用途：用于实体安防风险评估工具、案例自动匹配工具、攻击路径分析工具、安防措施有效性评价工具、AI 辅助研判和知识图谱建设。
> 格式说明：本版已将正文中的 JSON 示例全部移至文末附录。正文用于人工阅读和业务评估；附录 A、B、C 用于工具开发、数据库建模和规则引擎调用。

版本说明与主要更新摘要

v0.3 在 v0.2 的“威胁主体—目标资产—攻击战术—攻击技术—攻击路径—脆弱性—防范措施—案例映射” ATT&CK 式结构基础上，进一步补齐工具化、可观测、可评分、可验证、可推理所需的数据层。v0.2 已经完成国际化主体、资产、路径、措施和案例扩展，本版不推倒重来，而是在原有编号体系上增加行为指标、主体能力、控制效果、证据置信和行业画像。

本次补齐的五大缺口

1. **新增行为指标库（Indicators）**：将原来散落于技术条目中的检测指标独立编码为 `IND-` 条目，使监控、门禁、访客系统、工单系统、人工报告可以被统一匹配。
2. **新增威胁主体能力模型（Capabilities Model）**：用组织化、资源、情报、技术、暴力、接近权、持续性、规避能力八个维度对 `T-` 主体评分。
3. **新增技术—控制效果映射矩阵（Control Effectiveness Matrix）**：把 `TEC-` 技术与 `M-` 措施映射为 Deter / Detect / Delay / Respond / Recover 功能、效果等级、证据要求和剩余风险。
4. **新增证据与置信度模型（Evidence & Confidence）**：定义 `EVD-` 证据类型和 `C0-C5` 置信度规则，避免 AI 或人工研判只凭单一线索下结论。
5. **新增行业画像库（Industry Profiles）**：将通用知识库映射到学校、医院、制造业、数据中心、零售、能源、政务、仓储物流等常见行业。

正文与附录分工

- 正文：保留完整知识库结构、条目、表格、解释、评估要点。
- 附录A：工具开发字段示例，包括技术、指标、案例、控制矩阵的结构化字段。
- 附录B：JSON 数据结构模板，用于后续拆分为独立 JSON 文件或 API 返回格式。
- 附录C：数据库字段建议，用于 SQLite、PostgreSQL、Streamlit、知识图谱或轻量 Web 工具开发。

1. 总体数据结构（更新后的八类 + 新增类字典表）

v0.3 建议采用“基础字典表 + 关联表 + 事件表”的结构。原有八类基础表继续保留，同时新增五类工具化表。

类别	前缀	类型	作用	状态
威胁主体库	**T**	主表	描述攻击方角色、动机、能力、接近权和约束条件	保留并升级
目标资产库	**A**	主表	描述被保护资产及其关键性	保留并升级
攻击战术库	**TAC**	主表	描述攻击阶段和目的	保留
攻击技术库	**TEC**	主表	描述具体攻击手法	保留并增加指标映射
行为指标库	**IND**	主表	描述可观察事件、异常和前兆	新增
威胁主体能力模型	**CAP**	主表	对主体能力向量量化评分	新增
攻击路径库	**PATH**	主表	描述多步骤攻击链	保留并升级
脆弱性库	**V**	主表	描述可被利用的弱点	保留并升级
防范措施库	**M**	主表	描述控制措施和控制功能	保留并升级
技术–控制效果矩阵	**MAT**	关联表	描述 TEC 与 M 的效果映射	新增
证据与置信度模型	**EVD / C**	主表	描述证据类型和置信度规则	新增
行业画像库	**IP**	主表	描述行业威胁优先级和模板	新增
案例映射库	**CASE**	主表	描述案例、技术链、指标命中、控制缺口和复盘结论	保留并升级

基本推理关系

```
威胁主体 T
↓
主体能力 CAP + 动机 + 接近权
↓
攻击战术 TAC
↓
攻击技术 TEC
↓
行为指标 IND
↓
证据 EVD + 置信度 C
↓
攻击路径 PATH
↓
利用脆弱性 V
↓
影响目标资产 A
↓
防范措施 M
↓
技术—控制效果矩阵 MAT
↓
剩余风险 / 优先整改 / 案例入库
```

---

2. 威胁主体库（增加能力模型）

威胁主体库不再只按“外部、内部、访客”静态分类，还应记录其动机（Motive）、能力（Capability）、接近权（Access）、持续性（Persistence）、约束条件（Constraint）和攻击前行为（Pre-Incident Behavior）。

代码	威胁主体	英文	核心描述	常见目标资产	常见战术	能力模型	升级说明
T001	**外部机会型违法人员**	Opportunistic Offender	临时起意、能力较低、资源有限，主要选择低阻力目标。	A002/A003/A010	TAC-02/TAC-03/TAC-09	CAP-T001	本地化建议：用于普通盗窃、顺手牵羊、低门槛尾随等场景。
T002	**外部职业犯罪人员**	Professional Criminal	有预谋、有踩点、有工具和一定反侦察意识，可能重复作案。	A002/A003/A011	TAC-01/TAC-03/TAC-05/TAC-09	CAP-T002	新增国际经验：可结合 hostile reconnaissance 识别反复观察、测试门禁、试探报警等行为。
T003	**有组织犯罪团伙**	Organized Crime Group	分工明确、资源较强、可持续作案，可能存在内外勾结。	A002/A011/A008	TAC-01/TAC-03/TAC-08/TAC-14	CAP-T003	新增国际经验：与 ORC、cargo theft、供应链犯罪存在交叉，应关注人车货单关联。
T004	**在职内部人员**	Current Insider	合法进入、熟悉制度流程、知道盲区并可能拥有较高权限。	A003/A005/A006/A010	TAC-04/TAC-07/TAC-10	CAP-T004	本地化建议：不宜简单标签化人员，应纳入岗位权限、审计和离职调岗流程。
T005	**离职人员**	Former Employee	熟悉原单位环境、人员和流程，可能仍掌握旧权限、钥匙或流程信息。	A003/A005/A008	TAC-01/TAC-03/TAC-11	CAP-T005	本地化建议：重点核查离职权限、钥匙、访客例外和熟人放行。
T006	**承包商 / 外包人员**	Contractor / Outsourced Staff	半内部身份，阶段性进入权限，现场熟悉度较高，管控强度常低于员工。	A005/A006/A009	TAC-02/TAC-03/TAC-06/TAC-10	CAP-T006	新增国际经验：长期承包商权限漂移是 insider risk 的重要来源。
T007	**供应商 / 物流 / 维保人员**	Supplier / Logistics / Maintenance	高频进出，接触后勤、仓储、设备或装卸区域，合法理由充分。	A002/A005/A011	TAC-02/TAC-03/TAC-12	CAP-T007	新增国际经验：结合虚假承运商、虚假工单、供应商远程维护风险管理。
T008	**访客**	Visitor	短时进入，目的多样，依赖预约、前台、被访人确认和陪同管理。	A001/A006/A010	TAC-02/TAC-03	CAP-T008	本地化建议：从登记管理升级为访客生命周期风险管理。
T009	**极端个人 / 报复人员**	Grievance-driven Individual	情绪驱动、目标明确，可能不计后果，常与矛盾纠纷升级相关。	A001/A008/A006	TAC-01/TAC-08/TAC-11	CAP-T009	新增国际经验：应纳入 grievance、threat assessment 和冲突降级机制。
T010	**聚集性事件参与者**	Disorder / Protest Participant	群体行为、情绪传导快，目标可能从表达诉求转向冲击秩序。	A008/A012/A007	TAC-02/TAC-03/TAC-11/TAC-14	CAP-T010	本地化建议：重点看外围缓冲、出入口韧性、公安联动和非对抗处置。
T011	**激进组织 / 恐怖主义主体**	Extremist / Terrorist Cell	目标指向社会影响，可能使用暴力、危险物或车辆，低频高后果。	A001/A012/A007	TAC-01/TAC-08/TAC-11/TAC-14	CAP-T011	新增国际经验：与 soft target、HVM、active assailant preparedness 强关联。
T012	**高能力主体 / 国家支持主体**	High-capability / State-backed	资源强、长期潜伏，目标多为关键技术、关键设施和高价值信息。	A003/A005/A007/A013	TAC-01/TAC-06/TAC-10/TAC-14	CAP-T012	新增国际经验：关注网络—实体融合、供应链接近、网络化安防系统破坏。
T013	**内部威胁人员**	Insider Threat Actor	包括恶意、疏忽、受胁迫、被收买或被外部操纵的内部或半内部人员。	A003/A009/A013	TAC-07/TAC-08/TAC-10	CAP-T013	新增国际经验：Insider Threat；建议建立跨 HR、保卫、法务、信息化的人员风险治理。

代码	威胁主体	英文	核心描述	常见目标资产	常见战术	能力模型	升级说明
T014	**有组织零售 / 货运犯罪团伙**	ORC / Cargo Theft Group	以获利为目的，分工明确，可能结合网络冒充、虚假承运商、虚假提货和调包。	A002/A011/A010	TAC-02/TAC-03/TAC-08/TAC-09/TAC-12	CAP-T014	新增国际经验：Organized Retail Crime / Cargo Theft；适合零售、仓储、物流和制造成品库。
T015	**议题型行动者**	Issue-motivated Actor	以环保、劳工、消费者、政治或社会议题为动机，重视传播效果。	A008/A012/A007	TAC-11/TAC-13/TAC-14	CAP-T015	新增国际经验：Activist / Protest-Oriented Actor；重点关注象征性目标、外围堵控和直播传播。
T016	**孤狼 / 怨恨型攻击者**	Lone Actor / Grievance Actor	单人或小范围行动，受个人怨恨、极端情绪或意识形态驱动，突发性强。	A001/A012/A008	TAC-01/TAC-08/TAC-11	CAP-T016	新增国际经验：Lone Actor；重点纳入威胁言论、异常徘徊、车辆冲撞和主动暴力准备。
T017	**国家支持型实体行动主体**	Nation-State Physical Operator	高情报、高规避，可结合商务访问、供应链、网络化安防系统和长期接近。	A013/A005/A007/A009	TAC-01/TAC-06/TAC-10/TAC-14	CAP-T017	新增国际经验：Nation-State Physical Operations；适用于关键基础设施、科研单位、数据中心和高价值制造。

3. 目标资产库

目标资产从人员、财物、资料、设备、区域、业务、声誉扩展到安防系统自身、身份凭证、供应链物流资产、公共开放空间和科研技术资产。资产既可能是被保护对象，也可能成为攻击路径中的中间资源。

代码	资产	英文	典型内容	建议关键性维度
A001	**人员**	People	员工、高管、学生、医护人员、患者、访客、公众、特定岗位人员。	伤害严重性、密度、可疏散性、被针对性。
A002	**财物**	Property	现金、贵重物品、物资、产品、仓储资产、零售商品。	单位价值、易搬运性、可变现性、盘点难度。
A003	**信息资料**	Information	纸质文件、研发资料、客户资料、经营数据、个人信息、平面图。	敏感性、合规性、泄露后果、可复制性。
A004	**危险品**	Hazardous Materials	危化品、易燃易爆物、管制物品、放射源、特殊药品。	滥用后果、监管要求、接触控制等级。
A005	**关键设备**	Critical Equipment	生产设备、控制设备、电力设备、通信设备、医疗设备、安防设备。	可替代性、停机损失、恢复时间、外部依赖。
A006	**关键区域**	Critical Area	机房、实验室、仓库、财务室、控制室、档案室、危险品库。	进入后果、路径暴露度、分层防护数量。
A007	**关键业务**	Critical Operations	连续生产、医疗服务、教学秩序、政务运行、金融服务、物流履约。	业务中断损失、恢复时间目标、替代能力。
A008	**声誉与秩序**	Reputation & Order	社会影响、舆情、单位形象、公共秩序、客户信任。	扩散速度、社会敏感性、媒体关注度。
A009	**安防系统自身**	Physical Security Systems	CCTV、门禁、报警、访客系统、停车场系统、安防平台和远程维护通道。	可观测性、单点失效影响、网络暴露面。
A010	**身份与权限凭证**	Credentials	门禁卡、钥匙、访客证、临时证、二维码、车辆通行证、工单、账号。	可复用性、撤销速度、绑定强度、转发风险。
A011	**供应链与物流资产**	Supply Chain & Logistics	货物、单据、承运商账户、车辆、装卸区、提货码、封签、交接记录。	可调包性、验证成熟度、运输可视性。
A012	**公共开放空间 / 软目标**	Public Realm / Soft Target	大堂、门前广场、医院候诊区、学校门口、活动现场、落客区。	开放度、人群密度、车辆接近界面、疏散难度。
A013	**科研、技术与知识产权资产**	Research / Technology / IP Assets	研发样品、实验数据、技术图纸、代码、原型设备、关键工艺。	战略价值、长期竞争影响、国家安全相关性。

4. 攻击战术库

继续采用类似 ATT&CK 的战术—技术模型。战术表示攻击者在某一阶段希望达成的目的，技术表示具体实现方式。

代码	战术	英文	目的
TAC-01	**情报收集**	Reconnaissance	了解目标位置、布局、人员、流程和防护弱点。
TAC-02	**接近目标**	Approach	获得靠近单位、建筑、人员、车辆或目标区域的机会。
TAC-03	**获得进入**	Initial Access	进入单位、园区、建筑、车辆通道或受控区域。
TAC-04	**扩展通行**	Lateral Movement	从低敏区域进入高敏区域，或从公共空间进入核心区。
TAC-05	**规避发现**	Evasion	避免被人防、技防、物防发现或降低被怀疑程度。
TAC-06	**绕过控制**	Bypass Controls	绕过门禁、访客、审批、巡逻、安检、物流、权限等控制。
TAC-07	**接触目标资产**	Access Objective	实际接触人员、物品、设备、信息、凭证或系统。
TAC-08	**获取 / 破坏 / 影响目标**	Actions on Objectives	盗窃、破坏、泄露、伤害、纵火、冲撞、业务中断。
TAC-09	**撤离 / 逃逸**	Egress	带离资产、转运调包、混入人流或掩盖痕迹离场。
TAC-10	**持续接近 / 长期滥用**	Persistence	适用于内部人员、外包人员、供应商等长期接触主体。
TAC-11	**制造影响**	Impact Generation	扩大社会影响、舆论影响、业务影响或恐慌效果。
TAC-12	**建立攻击资源**	Resource Development	准备身份、车辆、工具、服装、工单、二维码、无人机或内部协助。
TAC-13	**诱导 / 操纵授权**	Abuse of Trust / Social Engineering	利用礼貌、熟人、领导名义、紧急维修、假监管、假检查等诱导放行。
TAC-14	**破坏响应能力**	Inhibit Response / Response Impairment	遮挡摄像机、破坏报警、制造多点事件、干扰通信或占用安保注意力。

5. 攻击技术库（增加行为指标映射）

本章保留原有 TEC 编号体系，并增加“主要指标”和“主要控制”字段。完整指标定义见第 6 章，控制效果见第 11 章。

代码	技术	战术	简要说明	主要指标	主要控制
TEC-0101	**公开信息收集**	TAC-01	网站、招聘、地图、社交媒体、公告、供应商资料等公开信息收集。	IND-0101-01	M-05/M-08
TEC-0102	**现场观察 / 踩点**	TAC-01	在单位周边观察出入口、巡逻规律、人员流量、车辆通行。	IND-0102-01/IND-0102-02	M-01/M-02/M-11
TEC-0103	**伪装询问**	TAC-01	以办事、求职、送货、维修、咨询名义获取流程信息。	IND-0103-01	M-05/M-13
TEC-0104	**内部信息获取**	TAC-01	通过熟人、员工、承包商、供应商获得内部布局、权限和流程信息。	IND-0104-01	M-09/M-15
TEC-0105	**影像记录**	TAC-01	拍摄出入口、安防设施、通行流程、敏感区域。	IND-0105-01	M-02/M-05
TEC-0106	**网络化安防系统暴露面收集**	TAC-01	收集摄像机、门禁、NVR、访客系统、远程维护入口等暴露面。	IND-0106-01	M-10/M-08
TEC-0107	**无人机观察**	TAC-01	使用 UAS 对园区、屋顶设备、活动现场、安保部署进行观察。	IND-0107-01/IND-0107-02	M-02/M-16/M-17
TEC-0201	**正常访客接近**	TAC-02	以合法访客身份靠近目标。	IND-0201-01	M-05/M-14
TEC-0202	**供应商 / 物流接近**	TAC-02	利用送货、取件、配送、装卸进入单位。	IND-0202-01	M-12/M-14
TEC-0203	**施工 / 维保接近**	TAC-02	借施工、检修、保洁、运维等身份进入。	IND-0203-01	M-05/M-12
TEC-0204	**车辆接近**	TAC-02	利用车辆进入停车场、装卸区、地下车库或靠近建筑。	IND-0204-01	M-03/M-16
TEC-0205	**人群混入**	TAC-02	利用上下班高峰、会议、活动、开放日混入。	IND-0205-01	M-02/M-11
TEC-0206	**公共开放空间接近**	TAC-02	通过大堂、门前广场、候诊区、校门、落客区等开放空间接近。	IND-0206-01	M-11/M-16
TEC-0207	**线上预约诱导线下接近**	TAC-02	通过伪造预约、假会议、假接待需求诱导线下准入。	IND-0207-01	M-05/M-14
TEC-0301	**尾随进入**	TAC-03	跟随授权人员通过门禁、闸机、门岗或电梯厅。	IND-0301-01/IND-0301-02/IND-0301-03	M-02/M-03/M-14
TEC-0302	**冒充访客**	TAC-03	伪造访问目的或冒用预约进入。	IND-0302-01/IND-0302-02	M-05/M-14
TEC-0303	**冒充供应商 / 维修人员**	TAC-03	以送货、维修、检测、弱电维护等理由进入。	IND-0303-01/IND-0303-02	M-05/M-12/M-14
TEC-0304	**使用他人证件 / 借卡**	TAC-03	使用员工卡、访客卡、临时证件或他人二维码进入。	IND-0304-01/IND-0304-02	M-02/M-14
TEC-0305	**伪造证件**	TAC-03	使用伪造工作证、访客证、监管证、供应商证。	IND-0305-01	M-05/M-14
TEC-0306	**翻越围界**	TAC-03	通过围墙、围栏、绿化带、低矮边界进入。	IND-0306-01/IND-0306-02	M-02/M-03
TEC-0307	**破门 / 破窗进入**	TAC-03	通过门、窗、卷帘、通风口等薄弱点进入。	IND-0307-01	M-03/M-04
TEC-0308	**利用未关闭入口**	TAC-03	利用未上锁门、消防通道、侧门、货梯门进入。	IND-0308-01	M-02/M-03
TEC-0309	**利用合法权限进入**	TAC-03	内部人员或授权人员进入目标区域并偏离业务必要性。	IND-0309-01	M-09/M-14/M-15
TEC-0310	**二维码 / 访客码转发进入**	TAC-03	访客码截图转发、多设备使用、重复使用或被盗用。	IND-0310-01	M-14/M-05
TEC-0311	**车辆冲卡 / 强行突破入口**	TAC-03	车辆未停车核验即冲闸、撞杆、突破临时隔离。	IND-0311-01	M-03/M-04/M-16

代码	技术	战术	简要说明	主要指标	主要控制
TEC-0401	**从公共区进入受控区**	TAC-04	从大厅、走廊、办公区进入机房、仓库、档案室。	IND-0401-01	M-14/M-11
TEC-0402	**利用电梯 / 楼梯通行**	TAC-04	通过电梯、楼梯、消防通道跨层进入。	IND-0402-01	M-14/M-02
TEC-0403	**利用后勤通道**	TAC-04	通过垃圾清运、餐饮、设备间、地下通道接近目标。	IND-0403-01	M-12/M-14
TEC-0404	**利用临时开放通道**	TAC-04	施工、活动、搬迁、会议期间利用临时开放通道。	IND-0404-01	M-05/M-03
TEC-0405	**内部协助通行**	TAC-04	由员工、外包、熟人带入或放行。	IND-0405-01	M-09/M-15
TEC-0406	**利用停车场到核心区通道**	TAC-04	从停车场、电梯厅、楼梯间进入核心办公或敏感区域。	IND-0406-01	M-11/M-16/M-14
TEC-0501	**利用视频盲区**	TAC-05	选择监控覆盖不足区域行动。	IND-0501-01	M-02/M-11
TEC-0502	**利用照明不足**	TAC-05	选择暗区、背光区、遮挡区行动。	IND-0502-01	M-11/M-02
TEC-0503	**利用巡逻间隙**	TAC-05	掌握巡逻规律，在间隙行动。	IND-0503-01	M-02/M-18
TEC-0504	**利用人员注意力分散**	TAC-05	在高峰、活动、交接班、突发忙乱时行动。	IND-0504-01	M-05/M-04
TEC-0505	**伪装为正常行为**	TAC-05	穿着、行为、工具与场景一致，降低怀疑。	IND-0505-01	M-02/M-05
TEC-0506	**避开报警探测**	TAC-05	选择无探测区域或探测失效区域行动。	IND-0506-01	M-02/M-03
TEC-0507	**遮挡 / 破坏监控**	TAC-05	遮挡、偏转、喷涂、断电、破坏摄像机或录像设备。	IND-0507-01/IND-0507-02	M-02/M-04/M-10
TEC-0508	**利用报警疲劳**	TAC-05	利用高误报区域导致值守人员忽视报警。	IND-0508-01	M-06/M-18
TEC-0601	**绕过访客流程**	TAC-06	不登记、不预约、冒用预约、借用访客证。	IND-0601-01	M-05/M-14
TEC-0602	**绕过物品出入控制**	TAC-06	夹带、混装、伪报或借物流通道带出物品。	IND-0602-01	M-12/M-05
TEC-0603	**绕过车辆管理**	TAC-06	利用套牌、借车、临时车、内部车辆进入。	IND-0603-01	M-16/M-12
TEC-0604	**绕过钥匙管理**	TAC-06	利用私配钥匙、未归还钥匙、通用钥匙。	IND-0604-01	M-05/M-14
TEC-0605	**绕过门禁权限**	TAC-06	利用共享卡、长期未清理权限、权限继承错误。	IND-0605-01	M-10/M-14
TEC-0606	**绕过安检 / 包裹检查**	TAC-06	利用忙乱、例外、VIP、熟人或低摩擦流程绕过检查。	IND-0606-01	M-05/M-04
TEC-0607	**供应商远程维护绕过实体控制**	TAC-06	利用远程维护账号修改门禁、视频或报警配置。	IND-0607-01/IND-0607-02	M-10/M-12
TEC-0701	**接触财物**	TAC-07	进入仓库、办公室、财务室、设备间接触财物。	IND-0701-01	M-02/M-03
TEC-0702	**接触文件资料**	TAC-07	进入档案室、办公桌、打印区、会议室接触文件。	IND-0702-01	M-05/M-09
TEC-0703	**接触危险品**	TAC-07	接近危险品库、实验室、药房、化学品柜。	IND-0703-01	M-05/M-04
TEC-0704	**接触关键设备**	TAC-07	接近配电、通信、控制、生产、安防设备。	IND-0704-01	M-03/M-10
TEC-0705	**接触人员**	TAC-07	接近特定人员实施伤害、纠缠、威胁、滋扰。	IND-0705-01	M-04/M-17
TEC-0706	**接触身份凭证**	TAC-07	拍摄、借用、复制、盗取门禁卡、访客证、二维码、钥匙。	IND-0706-01	M-14/M-09
TEC-0707	**接触安防系统**	TAC-07	接触门禁控制器、摄像机、报警主机、NVR、弱电间。	IND-0707-01	M-10/M-03

代码	技术	战术	简要说明	主要指标	主要控制
TEC-0801	**盗窃**	TAC-08	非法取得财物、物资、设备、商品。	IND-0801-01	M-02/M-03/M-04
TEC-0802	**泄密**	TAC-08	获取、拍摄、复制、带离敏感信息。	IND-0802-01	M-09/M-15/M-10
TEC-0803	**破坏设施**	TAC-08	损坏门禁、视频、报警、设备、门窗、供电等。	IND-0803-01	M-03/M-04
TEC-0804	**纵火**	TAC-08	对建筑、车辆、仓储、设备或外部依赖点实施纵火。	IND-0804-01/IND-0804-02	M-02/M-04/M-17
TEC-0805	**暴力伤害**	TAC-08	对人员实施攻击、威胁、伤害。	IND-0805-01/IND-0805-02/IND-0805-03	M-04/M-17
TEC-0806	**扰乱秩序**	TAC-08	堵门、冲击、聚集、滋扰、干扰业务运行。	IND-0806-01	M-04/M-17
TEC-0807	**危险品滥用**	TAC-08	非法获取或使用危险品造成伤害、破坏、污染。	IND-0807-01	M-05/M-04/M-17
TEC-0808	**安防系统干扰**	TAC-08	破坏、遮挡、断电、配置篡改或静默安防设备。	IND-0808-01/IND-0808-02	M-10/M-04
TEC-0809	**车辆冲撞**	TAC-08	使用车辆冲撞人群、门岗、大堂、活动区或建筑界面。	IND-0809-01/IND-0809-02	M-16/M-17
TEC-0810	**业务连续性攻击**	TAC-08	攻击供电、通信、物流、关键通道或单点依赖造成业务中断。	IND-0810-01	M-17/M-18
TEC-0901	**原路撤离**	TAC-09	沿进入路径离开。	IND-0901-01	M-02/M-04
TEC-0902	**另选出口撤离**	TAC-09	利用侧门、消防通道、货运通道离开。	IND-0902-01	M-02/M-04
TEC-0903	**借车辆撤离**	TAC-09	通过车辆携带人员或物品离开。	IND-0903-01	M-16/M-12
TEC-0904	**混入人流撤离**	TAC-09	利用高峰、活动、群体离开。	IND-0904-01	M-02/M-11
TEC-0905	**转运 / 调包撤离**	TAC-09	在物流、仓储、配送环节中转、调包、改变路线。	IND-0905-01	M-12/M-06
TEC-1001	**权限长期滥用**	TAC-10	内部人员长期利用合法权限实施违规行为。	IND-1001-01	M-14/M-15
TEC-1002	**低频多次小额盗取**	TAC-10	长期少量带出物品，规避盘点。	IND-1002-01	M-06/M-18
TEC-1003	**长期收集信息**	TAC-10	通过日常工作、拍摄、询问、复制长期积累敏感信息。	IND-1003-01	M-15/M-10
TEC-1004	**利用岗位轮换空档**	TAC-10	在人员调整、交接、离职期间利用权限空档。	IND-1004-01	M-09/M-18
TEC-1005	**长期承包商权限漂移**	TAC-10	承包商项目结束后权限未回收或权限逐步扩大。	IND-1005-01	M-12/M-14/M-15
TEC-1101	**扩大舆情**	TAC-11	通过拍摄、传播、网络发酵扩大事件影响。	IND-1101-01	M-17/M-06
TEC-1102	**制造恐慌**	TAC-11	通过威胁、虚假警情、可疑物、破坏行为制造恐慌。	IND-1102-01	M-17/M-04
TEC-1103	**业务中断**	TAC-11	针对关键设备、出入口、人员、系统造成运行中断。	IND-1103-01	M-17/M-18
TEC-1104	**象征性目标攻击**	TAC-11	针对具有象征意义的门牌、旗帜、标志建筑、公众空间实施攻击或破坏。	IND-1104-01	M-01/M-17
TEC-1201	**虚假工单 / 维修单**	TAC-12	伪造或冒用维修、施工、消防检测、设备巡检等工单。	IND-1201-01	M-05/M-12
TEC-1202	**虚假承运商 / 虚假提货**	TAC-12	冒充承运商、司机、提货人，利用伪造单据或盗用账号提走货物。	IND-1202-01/IND-1202-02	M-12/M-05
TEC-1203	**准备假身份 / 假证件**	TAC-12	准备假工牌、假访客证、假监管证件、假会议凭证等。	IND-1203-01	M-05/M-14
TEC-1204	**准备车辆 / 工具 / 服装**	TAC-12	准备场景匹配车辆、反光背心、工具箱、制服、推车等。	IND-1204-01	M-01/M-13

代码	技术	战术	简要说明	主要指标	主要控制
TEC-1301	**礼貌施压 / 熟人放行**	TAC-13	利用礼貌、人情、熟人、领导名义、紧急事务让人放弃核验。	IND-1301-01	M-05/M-14
TEC-1302	**紧急维修借口**	TAC-13	声称设备故障、漏水、断电、消防报警等要求快速进入。	IND-1302-01	M-05/M-12
TEC-1303	**假监管 / 假检查**	TAC-13	冒充监管、检查、审计、执法、上级单位或消防检测人员。	IND-1303-01	M-05/M-13
TEC-1401	**制造多点事件分散响应**	TAC-14	制造小纠纷、假警情、设备故障、门口拥堵等分散安保力量。	IND-1401-01	M-04/M-17
TEC-1402	**干扰通信 / 报警链条**	TAC-14	破坏对讲、断电、干扰网络、占线、误导报警信息。	IND-1402-01/IND-1402-02	M-10/M-17

6. 新增：行为指标库（Indicators）

行为指标库是 v0.3 的第一优先级新增模块。它回答的是“观察到什么现象”。每个指标应尽量具备可编码、可记录、可检索、可映射、可复核特征。

指标字段建议

字段	含义
indicator_id	**指标编号，如 IND-0301-01**
name	**指标名称**
related_technique	**关联攻击技术**
data_source	**数据来源，如 ACS、VMS、访客系统、工单、人工报告**
trigger_rule	**触发建议或阈值**
evidence_type	**推荐证据类型**
base_confidence	**基础置信度**

指标代码	指标名称	关联技术	主要数据源	触发建议	证据类型	基础置信度
IND-0101-01	**敏感平面图 / 组织名录被非常态查询**	TEC-0101	文件日志 / 网站分析	24h 内非常态下载或截图。	EVD-01/EVD-08	中
IND-0102-01	**同一人多次停留观察入口 / 巡逻 / 摄像机**	TEC-0102	视频 / 人工通报	7日内重复出现或停留超过阈值。	EVD-02/EVD-04	中
IND-0102-02	**以手机定向拍摄门禁、卸货口、围界弱点**	TEC-0102/TEC-0105	视频 / 巡检	针对性持续拍摄。	EVD-02	中高
IND-0103-01	**以问路 / 招聘 / 检查名义打探安保细节**	TEC-0103	前台记录 / 员工报告	问题涉及防护流程或薄弱点。	EVD-04/EVD-05	中
IND-0104-01	**内部人员无业务必要提供平面、名册或流程**	TEC-0104	邮件 / 访谈 / 审计	涉敏资料外传。	EVD-01/EVD-04/EVD-08	中高
IND-0105-01	**对机房、配电、安控室进行定向录像**	TEC-0105	视频 / 巡检	非授权摄录。	EVD-02/EVD-04	中高
IND-0106-01	**门禁 / CCTV / NVR 暴露面被异常扫描或登录测试**	TEC-0106	系统日志 / SIEM	扫描、爆破、异地登录。	EVD-01	高
IND-0107-01	**未授权无人机在边界上空盘旋或定向拍摄**	TEC-0107	UAS观察 / 视频	停留、悬停、反复复访。	EVD-02/EVD-03	中高
IND-0107-02	**无人机在敏感时段靠近屋顶设备或活动现场**	TEC-0107	UAS观察	近距离飞行或低空悬停。	EVD-02/EVD-03	中高
IND-0201-01	**访客目的与受访人、时段、区域不一致**	TEC-0201	访客系统	多字段不匹配。	EVD-05	中
IND-0202-01	**到场司机 / 车牌 / 单号与预约资料不符**	TEC-0202	YMS / 收货台	任一主验证失败。	EVD-05/EVD-02	高
IND-0203-01	**维保人员无有效工单或进入范围超出工单**	TEC-0203/TEC-1201	EAM / 工单系统	无票或越权。	EVD-05	高
IND-0204-01	**车辆高速接近、逗留敏感入口或反复驶离再接近**	TEC-0204	车牌识别 / 视频	可疑路径循环。	EVD-02/EVD-03	中高
IND-0205-01	**控制点前突发群聚与推挤**	TEC-0205	视频 / 现场回报	入口负载异常。	EVD-02/EVD-04	中高
IND-0206-01	**开放区人流向受控区边界异常聚集**	TEC-0206	视频热区	跨界密度异常。	EVD-02	中

指标代码	指标名称	关联技术	主要数据源	触发建议	证据类型	基础置信度
IND-0207-01	**预约建立者与到场人不一致且来源可疑**	TEC-0207	预约系统	异常邀请人、异常设备或异常联系方式。	EVD-05/EVD-01	中高
IND-0301-01	**单次刷卡多人通行**	TEC-0301	ACS + 视频	即时触发。	EVD-01/EVD-02	中高
IND-0301-02	**闸机方向逆行或第二人贴身通过**	TEC-0301	闸机 / 视频AI	即时触发。	EVD-01/EVD-02	中高
IND-0301-03	**员工为陌生人主动撑门**	TEC-0301	视频 / 人工通报	即时触发。	EVD-02/EVD-04	中
IND-0302-01	**访客证件、照片、受访信息不一致**	TEC-0302	前台 / OCR	任一要素不符。	EVD-05	中高
IND-0302-02	**访客离开前台后路径偏离授权陪同线**	TEC-0302	视频 / 室内定位	未陪同进入内区。	EVD-02/EVD-03	中高
IND-0303-01	**维修公司名称、工单、制服、车辆样式不一致**	TEC-0303	前台 / 收货 / 视频	任一关键项不符。	EVD-05/EVD-02	高
IND-0303-02	**承包商要求接触与工单无关设备**	TEC-0303	现场监工	越界工项。	EVD-04/EVD-05	中高
IND-0304-01	**卡证持有人与刷卡者人脸不匹配**	TEC-0304	ACS + 视频	即时触发。	EVD-01/EVD-02	高
IND-0304-02	**卡证在不合理时距内于相隔地点使用**	TEC-0304	ACS	不可能通行。	EVD-01	高
IND-0305-01	**卡片外观模板、条码、RF 行为异常**	TEC-0305	发卡审计 / 门禁	证件可疑。	EVD-01/EVD-05	中高
IND-0306-01	**围界震动 / 攀爬 / 切割告警**	TEC-0306	PIDS	即时触发。	EVD-03	高
IND-0306-02	**边界告警与盲区移动关联**	TEC-0306/TEC-0501	PIDS + 视频	关联后升级。	EVD-02/EVD-03	高
IND-0307-01	**门窗破坏、玻璃震动、异常开启**	TEC-0307	IDS / 门磁	即时触发。	EVD-03/EVD-07	高
IND-0308-01	**出入口长时间未关、门磁常开**	TEC-0308	ACS / 门磁	超时告警。	EVD-01/EVD-03	中高
IND-0309-01	**合法持证人进入与职责不符区域**	TEC-0309	ACS / HR	越权访问。	EVD-01/EVD-08	中高
IND-0310-01	**访客码重复使用、截图转发、多设备验证**	TEC-0310	访客系统	即时封锁。	EVD-01/EVD-05	高
IND-0311-01	**车辆未停车核验即撞击闸杆 / 连续闯关**	TEC-0311	车道闸机 / 视频	立即高优先。	EVD-02/EVD-03	高
IND-0401-01	**人员从公共区进入非授权受控区**	TEC-0401	门禁 / 视频	无权限越界。	EVD-01/EVD-02	中高
IND-0402-01	**访客或低权限人员到达非授权楼层**	TEC-0402	电梯权限 / 视频	楼层越权。	EVD-01/EVD-02	中高
IND-0403-01	**后勤人员偏离规定路线**	TEC-0403	视频 / 访客轨迹	路线异常。	EVD-02/EVD-03	中
IND-0404-01	**临时通道在活动/施工结束后未恢复控制**	TEC-0404	巡检 / 门磁	恢复缺失。	EVD-03/EVD-09	中
IND-0405-01	**内部人员陪同对象路径异常或敏感区停留过久**	TEC-0405	室内定位 / 视频	行程偏差。	EVD-02/EVD-03	中高
IND-0406-01	**地库到核心区缺少二次核验且出现陌生人员上行**	TEC-0406	地库视频 / 电梯门禁	停车区上行异常。	EVD-01/EVD-02	中高
IND-0501-01	**个体长时间停留在视频弱覆盖界面**	TEC-0501	视频AI	超过阈值。	EVD-02	中
IND-0502-01	**暗区或背光区反复出现异常停留**	TEC-0502	视频 / 巡检	夜间重复出现。	EVD-02/EVD-04	中
IND-0503-01	**异常行为总在巡逻间隔后出现**	TEC-0503	巡更 / 视频	与巡逻规律相关。	EVD-02/EVD-08	中
IND-0504-01	**交接班、活动高峰出现绕行或异常接近**	TEC-0504	视频 / 值班记录	注意力分散时段命中。	EVD-02/EVD-06	中

指标代码	指标名称	关联技术	主要数据源	触发建议	证据类型	基础置信度
IND-0505-01	**服装工具符合场景但无法说明任务**	TEC-0505	门岗询问 / 视频	身份可信但事由不清。	EVD-04/EVD-05	中
IND-0506-01	**多次避开探测器覆盖区移动**	TEC-0506	视频 / PIDS	路径刻意规避。	EVD-02/EVD-03	中高
IND-0507-01	**摄像机遮挡、偏转、失焦、黑屏**	TEC-0507	VMS 健康监控	即时触发。	EVD-01/EVD-02	高
IND-0507-02	**摄像机异常后邻近区域出现未授权移动**	TEC-0507	VMS + 视频	关联升级。	EVD-01/EVD-02	高
IND-0508-01	**同区重复误报导致警卫不再处置**	TEC-0508	IDS / 值班记录	误报疲劳。	EVD-01/EVD-06	中高
IND-0601-01	**访客未登记但出现在受控区**	TEC-0601	访客系统 / 视频	记录缺失与现场存在矛盾。	EVD-02/EVD-05	高
IND-0602-01	**出库商品、包裹或工具与出入单不一致**	TEC-0602	WMS / 收发台	任一关键字段不符。	EVD-05/EVD-02	高
IND-0603-01	**车牌权限与驾驶人/随车人不一致**	TEC-0603	LPR / 门岗	人车不绑定。	EVD-02/EVD-05	中高
IND-0604-01	**钥匙领用无审批、超期未还或通用钥匙异常使用**	TEC-0604	钥匙柜 / 台账	超时或越权。	EVD-05/EVD-08	中高
IND-0605-01	**门禁群组被非常态提升或临时授权未回收**	TEC-0605	IAM / ACS	超时未回收。	EVD-01/EVD-08	高
IND-0606-01	**包裹绕过安检或安检例外无审批**	TEC-0606	安检记录 / 视频	例外缺证据。	EVD-02/EVD-05	中高
IND-0607-01	**远程维护连接无工单、无监护、无录像**	TEC-0607	远维平台 / SIEM	任一条件缺失。	EVD-01/EVD-05	高
IND-0607-02	**远维账号在异常时间修改门禁/视频/报警配置**	TEC-0607	系统日志	异常时间 + 高风险操作。	EVD-01	高
IND-0701-01	**财物被接触或移动但无工单、无出库或无授权**	TEC-0701	RFID / WMS / 视频	异常流转。	EVD-01/EVD-02/EVD-05	高
IND-0702-01	**文件、样品、存储介质被集中带离或拍摄**	TEC-0702	视频 / 出入口 / 打印日志	涉敏资料外流迹象。	EVD-01/EVD-02	高
IND-0703-01	**危险品领用数量、人员、用途或时段异常**	TEC-0703	台账 / 视频	异常领用。	EVD-05/EVD-02	高
IND-0704-01	**关键设备柜门开启但无授权工单**	TEC-0704	门磁 / 工单 / 视频	即时触发。	EVD-03/EVD-05	高
IND-0705-01	**高风险人员接近特定人员并伴随纠缠或威胁**	TEC-0705	现场报告 / 视频	接触风险升级。	EVD-02/EVD-04	高
IND-0706-01	**卡证无人看管、被借用或持有人不在场期间使用**	TEC-0706	视频 / ACS	即时触发。	EVD-01/EVD-02	高
IND-0707-01	**安防主机、控制器、NVR 柜体被无授权开启**	TEC-0707	门磁 / 视频 / 工单	即时触发。	EVD-02/EVD-03	高
IND-0801-01	**高价值物品位移无交易、无工单、无授权**	TEC-0801	RFID / WMS / 视频	异常流转。	EVD-01/EVD-02/EVD-05	高
IND-0802-01	**纸本、样品、存储介质被集中带离或拍摄**	TEC-0802	视频 / 出入台	涉敏资料外流迹象。	EVD-02/EVD-05	高
IND-0803-01	**配电柜、控制箱、机柜被开启且无授权工作**	TEC-0803	门磁 / 工单 / 视频	即时触发。	EVD-02/EVD-03/EVD-05	高
IND-0804-01	**有加速剂气味、烟温异常、可疑容器遗留**	TEC-0804	消防 / 视频 / 巡检	即时高风险。	EVD-02/EVD-03/EVD-07	高
IND-0804-02	**外部依赖点附近出现可疑停留、点火或破坏痕迹**	TEC-0804/TEC-0810	视频 / 巡检	关键依赖点异常。	EVD-02/EVD-07	高
IND-0805-01	**抱怨升级、威胁语句、报复性行为与持械迹象并存**	TEC-0805	HR / 通报 / 视频	需要威胁评估。	EVD-04/EVD-09	高
IND-0805-02	**医疗或校园场域出现 escalating behavior 对人员逼近**	TEC-0805	现场回报 / 视频	中高优先。	EVD-02/EVD-04	中高
IND-0805-03	**人员携带异常包裹或工具进入开放区并拒绝说明**	TEC-0805	安检 / 视频	拒绝核验时升级。	EVD-02/EVD-05	中高

指标代码	指标名称	关联技术	主要数据源	触发建议	证据类型	基础置信度
IND-0806-01	**堵门、冲击、围堵人员或业务点位**	TEC-0806	现场报告 / 视频	秩序受影响。	EVD-02/EVD-04	中高
IND-0807-01	**危险品库存异常减少或用途不匹配**	TEC-0807	台账 / 审计	库存差异。	EVD-05/EVD-08	高
IND-0808-01	**CCTV / ACS 规则配置被未授权更改**	TEC-0808	审计日志	即时触发。	EVD-01	高
IND-0808-02	**多设备同步离线或异常静默**	TEC-0808/TEC-1402	健康监控	关联升级。	EVD-01	高
IND-0809-01	**车辆脱离正常车道向人群 / 建筑加速**	TEC-0809	视频 / 雷达	立即高危。	EVD-02/EVD-03	高
IND-0809-02	**车辆反复测试入口减速、道闸、隔离设施**	TEC-0809	LPR / 视频	前兆测试。	EVD-02/EVD-03	中高
IND-0810-01	**多个关键节点同时出现小事件造成实际停摆**	TEC-0810	事件关联	关联触发。	EVD-06/EVD-08	高
IND-0901-01	**异常人员沿原入口快速离场并回避询问**	TEC-0901	视频 / 门岗	离场异常。	EVD-02/EVD-04	中
IND-0902-01	**消防门、侧门、货运门异常开启后人员离场**	TEC-0902	门磁 / 视频	出口异常。	EVD-02/EVD-03	中高
IND-0903-01	**车辆离场携带异常包裹或货物**	TEC-0903	视频 / 车辆检查	物品异常。	EVD-02/EVD-05	中高
IND-0904-01	**人员混入高峰人流离场且访客证未回收**	TEC-0904	访客系统 / 视频	离场闭环失败。	EVD-02/EVD-05	中
IND-0905-01	**同批货在出场前后发生车辆 / 司机 / 封条替换**	TEC-0905	WMS / 视频 / 封条审计	高优先。	EVD-02/EVD-05/EVD-07	高
IND-1001-01	**同一内部人员长期夜间、小流量时段异常进入**	TEC-1001	ACS	30日趋势。	EVD-01/EVD-08	中高
IND-1002-01	**小额损耗集中于同一人员、班次或区域**	TEC-1002	盘点 / 排班	趋势异常。	EVD-08/EVD-05	中高
IND-1003-01	**非职责范围长期访问、复制或拍摄敏感信息**	TEC-1003	访问日志 / 视频	低频长期。	EVD-01/EVD-02/EVD-08	高
IND-1004-01	**岗位变更后旧权限仍可用**	TEC-1004	IAM / HR / ACS	变更后未同步。	EVD-01/EVD-08	高
IND-1005-01	**承包商凭证在项目结案后仍可用**	TEC-1005	IAM / ACS	结案即检查。	EVD-01/EVD-05	高
IND-1101-01	**现场出现同步直播、定向拍摄和舆情扩散**	TEC-1101	现场监测 / 舆情	事件传播启动。	EVD-02/EVD-12	中高
IND-1102-01	**可疑物、威胁信息或虚假警情造成恐慌**	TEC-1102	报警 / 现场报告	恐慌迹象。	EVD-04/EVD-06	中高
IND-1103-01	**关键通道、系统或设备故障导致服务停摆**	TEC-1103	运维 / 事件系统	业务中断。	EVD-01/EVD-06	高
IND-1104-01	**象征性标识、门牌、旗帜或公共界面被定向破坏**	TEC-1104	视频 / 巡检	象征性目标受损。	EVD-02/EVD-07	中
IND-1201-01	**工单编号无效、人员与工单不一致或要求进入非工单区域**	TEC-1201	工单系统 / 前台	立即复核。	EVD-05	高
IND-1202-01	**提货人公司名称与订单 / 合同不一致**	TEC-1202	TMS / ERP	高优先。	EVD-05	高
IND-1202-02	**临时改派提货且核验链不足**	TEC-1202	物流协同平台	二次核验。	EVD-05/EVD-04	高
IND-1203-01	**证件编号不存在、二维码无法验证或权威身份拒绝登记**	TEC-1203	前台 / 证件系统	阻断并升级。	EVD-05/EVD-04	高
IND-1204-01	**工具、车辆、服装与任务不匹配但试图进入**	TEC-1204	门岗 / 视频	场景不一致。	EVD-02/EVD-04	中高
IND-1301-01	**保安因语言压力 / 熟人关系直接放行**	TEC-1301	现场回报 / 视频	审计复盘。	EVD-02/EVD-04	中
IND-1302-01	**紧急维修理由无法由业主 / 设施方验证**	TEC-1302	工单 / 通联记录	即时阻断。	EVD-05/EVD-04	高

指标代码	指标名称	关联技术	主要数据源	触发建议	证据类型	基础置信度
IND-1303-01	**假监管 / 假检查人员要求快速通行或调阅资料**	TEC-1303	前台 / 通报	二次验证。	EVD-04/EVD-05	高
IND-1401-01	**远距多点同步事件造成值守资源稀释**	TEC-1401	PSIM / SOC	关联升级。	EVD-06/EVD-08	中高
IND-1402-01	**对讲、无线电、蜂窝信号异常中断**	TEC-1402	通信监测	高优先。	EVD-01/EVD-06	中高
IND-1402-02	**告警不上送、时间戳异常、监控大面积失联**	TEC-1402/TEC-0808	PSIM / VMS / ACS	立即处置。	EVD-01	高

7. 新增：威胁主体能力模型

能力模型采用 1—5 分制，分数越高代表该能力越强。八维向量如下：

维度	含义
O 组织化程度	**单人、临时团伙、职业团伙、组织化行动、国家支持**
R 资源能力	**资金、工具、车辆、设备、人员、外部支持**
I 情报能力	**踩点、公开信息收集、内部信息获取、长期观察**
T 技术能力	**门禁、视频、网络化安防系统、伪造材料、远程访问等能力**
V 暴力能力	**是否可能使用暴力、车辆、纵火、危险品或武器**
A 接近权	**外部、访客、承包商、员工、供应商、远程系统访问**
P 持续性	**单次机会型、重复进入、长期潜伏、持续滥用**
E 规避能力	**规避视频、报警、巡逻、访客流程、物流核验的能力**

分数定义

分数	含义
1	**极低，偶发或几乎不具备**
2	**低，仅能依赖简单手法**
3	**中，可在熟悉场景重复使用**
4	**高，具备计划、分工或专业支援**
5	**极高，可跨场景、长期、复合式运作**

模型	主体	O	R	I	T	V	A	P	E	典型说明
CAP-T001	**T001**	1	1	1	1	1	1	1	2	低准备、低持续，主要依赖机会。
CAP-T002	**T002**	3	3	3	2	2	1	3	4	有踩点、工具和一定规避能力。
CAP-T003	**T003**	5	4	3	3	3	2	4	4	有分工、资源调度和跨点协同。
CAP-T004	**T004**	2	2	4	3	1	5	4	4	高接近权，熟悉流程，低可见性。
CAP-T005	**T005**	2	2	3	2	2	2	2	3	熟悉旧流程和关系网络。
CAP-T006	**T006**	3	2	3	3	1	4	4	3	合法进场频繁，工单和区域权限可被滥用。
CAP-T007	**T007**	3	3	3	3	1	4	3	3	可利用物流、维修和交接流程。

模型	主体	O	R	I	T	V	A	P	E	典型说明
CAP-T008	**T008**	1	1	1	1	1	2	1	1	权限短时，依附性强。
CAP-T009	**T009**	1	1	2	1	4	1	2	2	情绪驱动，可升级暴力。
CAP-T010	**T010**	3	2	2	1	3	2	2	2	人数压力与秩序冲击。
CAP-T011	**T011**	4	4	4	3	5	1	4	4	追求象征性和高影响后果。
CAP-T012	**T012**	5	5	5	5	3	2	5	5	情报、技术、长期渗透能力强。
CAP-T013	**T013**	3	2	5	3	1	5	5	5	内部威胁典型高接近权、高持续、高规避。
CAP-T014	**T014**	5	4	3	2	3	2	4	4	快速变现、协同转运、重复作案。
CAP-T015	**T015**	3	2	3	2	2	2	3	2	重视镜头、舆情和象征性。
CAP-T016	**T016**	1	1	2	1	5	1	2	2	低组织化、高暴力能力。
CAP-T017	**T017**	5	5	5	4	3	3	5	5	高能力实体接近，可结合供应链和系统弱点。

计算建议

```
Threat Success Potential
= ActorCapabilityScore × PathFeasibility × AssetCriticality × VulnerabilityExposure × (1 - EffectiveControlCoverage)
```

---

8. 攻击路径库

攻击路径用于把技术点串联成真实事件过程。评估时应判断攻击者从外部到目标资产需要经过哪些空间、流程、身份、系统或第三方环节，以及每一环节的威慑、探测、延迟、响应和恢复能力。

路径	名称	典型阶段	高风险主体	关键评分点
PATH-01	**围界入侵路径**	外围观察 → 翻越/破坏围界 → 穿越外场 → 接近建筑/仓库 → 接触目标 → 撤离	T002/T003/T011	边界高度、PIDS、照明、巡逻、响应时限。
PATH-02	**正门访客路径**	门岗/前台 → 访客登记 → 接待区 → 办公区 → 敏感区域	T008/T013/T015	预约核验、被访人确认、陪同、区域授权。
PATH-03	**物流货运路径**	货运入口 → 装卸区 → 仓储区 → 内部通道 → 目标资产	T007/T014	人车货单一致性、装卸监管、封签和交接。
PATH-04	**地下车库路径**	车库入口 → 停车区 → 电梯厅/楼梯间 → 办公/核心区域	T002/T009/T016	车人绑定、地库视频、电梯权限、楼梯门状态。
PATH-05	**后勤服务路径**	后勤入口 → 保洁/餐饮/垃圾清运区 → 设备间/走廊 → 目标区域	T006/T007	后勤人员管理、动线隔离、监控覆盖。
PATH-06	**施工维保路径**	施工入口 → 临时作业区 → 设备/管井/弱电间 → 目标区域	T006/T013	工单核验、临时权限、作业陪同、完工复核。
PATH-07	**内部人员路径**	合法进入 → 正常工作区 → 权限滥用 → 接触目标 → 带离/泄露/破坏	T004/T013	权限最小化、审计追踪、异常行为识别。
PATH-08	**群体冲击路径**	外围聚集 → 出入口压迫 → 突破门岗 → 进入公共区 → 影响秩序/人员安全	T010/T015	外围缓冲、门岗加固、分区隔离、公安联动。
PATH-09	**企业办公尾随路径**	大堂高峰 → 跟随员工过闸机 → 电梯厅 → 办公楼层 → 会议室/打印区/机房	T001/T008/T013	反尾随、楼层权限、陌生人识别、员工挑战文化。
PATH-10	**供应链物理攻击路径**	线上冒充 → 获取提货信息 → 车辆司机到场 → 装货交接 → 改线/调包 → 虚假签收	T003/T014	承运商白名单、提货二次确认、封签、GPS、双人交接。
PATH-11	**停车场到核心区路径**	车辆进入停车场 → 人员下车 → 电梯厅/楼梯间 → 核心区域	T009/T016	地库直达风险、车人分流、二次门禁、人车权限分离。
PATH-12	**车辆冲撞路径**	外部道路 → 加速接近 → 突破道闸/门岗/临时隔离 → 冲撞人群/大堂/活动区	T009/T011/T016	车辆可达速度、缓冲距离、HVM、门岗避险、临时封控。
PATH-13	**安防系统网络化破坏路径**	识别供应商/设备 → 获取弱口令/远维账号 → 访问门禁/视频/报警 → 开门/静默/删录像	T012/T017/T013	资产清单、外网暴露、远维审批、日志、备份、网络分区。
PATH-14	**活动现场外围渗透路径**	开放人群 → 临时围栏/检票/安检 → 利用盲区/证件/车辆/高峰突破 → 贵宾/控制区	T015/T011	临时围界、证件分级、高点控制、外围观察、统一通信。
PATH-15	**无人机观察 / 干扰路径**	场外起飞 → 低空接近 → 拍摄布局/安保/屋顶设备 → 悬停/干扰/投送 → 离场	T012/T011/T016	UAS发现、屋顶防护、禁飞提示、报告联动。

9. 脆弱性库

脆弱性不再只限于围界、门禁、视频、报警，还包括空间设计、组织治理、第三方、内部威胁、业务连续性、网络化安防系统、物流验证和主动暴力事件准备。

代码	脆弱性类型	典型表现	建议评分轴
V-01	**物理边界类**	围界低矮、破损、无防攀爬、门窗抗破坏弱、非主入口防护弱。	可攀爬性、可破坏性、边界连续性。
V-02	**探测感知类**	视频盲区、夜间图像差、报警探测缺失、误报高、无人复核。	可观测性、告警质量、复核时效。
V-03	**延迟阻隔类**	门禁不分区、门锁等级低、敏感区域无二次隔离、地库直达办公区。	延迟时间、防护层数、单点失效后剩余能力。
V-04	**响应处置类**	保安响应慢、巡逻固定、夜间力量不足、预案不可操作、联动弱。	响应时限、到场质量、指挥链清晰度。
V-05	**身份与权限类**	访客核验弱、临时证件失控、门禁权限过宽、离职权限未回收。	身份可信度、权限生命周期、动态授权。
V-06	**外包与关联方类**	背景审核弱、供应商白名单缺失、维保审批弱、陪同制度不落实。	第三方验证成熟度、合同约束、监督质量。
V-07	**资产管理类**	资产台账不清、物品出门审批弱、危险品领用不严、库存异常不发现。	可追溯性、盘点周期、异常识别能力。
V-08	**组织管理类**	制度有但执行弱、职责不清、整改闭环不足、培训不足、复盘不足。	治理成熟度、责任闭环、绩效指标。
V-09	**CPTED 与空间设计类**	自然监视不足、边界感弱、人车流线混乱、暗角遮挡多。	自然监视、领域性、维护状态、人车分流。
V-10	**分层防护不足类**	一道门禁失效后可直达核心资产，缺少 Defense-in-Depth。	防护层数、每层 D-D-D-R-R 功能、最短攻击时间。
V-11	**低摩擦准入与安全控制失衡类**	为便利过度放宽访客、快递、车辆、承包商管理。	例外比例、核验率、便利与安全平衡。
V-12	**安防系统网络安全不足类**	默认口令、外网暴露、远维无审批、管理员共享、日志缺失。	CAPSS / cyber assurance、补丁、账号、分区、日志。
V-13	**响应链条断裂类**	报警有人看但无人判断，判断后无人到场，到场后无人指挥。	报警确认率、升级规则、联动演练、指挥链。
V-14	**第三方治理类**	供应商、承包商、维保、物流人员准入弱，合同缺少安全条款。	备案率、培训率、违规处置、远程维护审批。
V-15	**情绪、纠纷与行为风险识别类**	威胁言论、纠纷升级、异常徘徊缺乏记录和干预。	行为前兆报告、台账完整率、冲突降级能力。
V-16	**业务连续性耦合风险类**	单点电力、通信、安防平台、出入口、物流通道故障导致业务中断。	单点数量、替代路线、恢复时间、备用能力。
V-17	**高价值信息与科研资产保护不足类**	研发区、实验室、技术资料、原型设备访问控制不足。	敏感资产生命周期保护、禁拍、最小知悉。
V-18	**内部威胁治理不足类**	HR、保卫、法务、信息化、业务部门信息不通，高风险岗位无审计。	insider readiness、异常复核率、离职回收时效。
V-19	**物流交接与供应链验证不足类**	司机、车辆、货物、单据、预约未绑定，临时变更无复核。	人车货单一致率、封签异常率、路线可视性。
V-20	**主动暴力事件准备不足类**	主动攻击、车辆冲撞、持械伤害、纵火等低频高后果事件缺少预案。	演练覆盖率、一键报警、避险空间、HVM 评估。

10. 防范措施库（增加 D-D-D-R-R 映射）

防范措施从传统 Deter、Detect、Delay、Respond 扩展为 Deter、Detect、Delay、Deny、Respond、Recover、Govern，并强调控制措施必须可验证。

代码	措施	主功能	典型内容	建议证据
M-01	**威慑**	Deter	警示标识、可见安保、围界形象、禁拍标识、随机巡查。	EVD-05/EVD-09
M-02	**探测**	Detect	视频监控、入侵报警、门磁、巡逻、车辆异常识别、报警复核。	EVD-01/EVD-02/EVD-03
M-03	**延迟**	Delay	围栏、防盗门窗、分区门禁、防尾随设施、车辆阻挡、双门互锁。	EVD-10/EVD-11
M-04	**响应**	Respond	保安到场、一键报警、内部联动、公安联动、封控追踪、疏散控制。	EVD-06/EVD-07
M-05	**管理控制**	Deter/Detect	访客预约、被访人确认、陪同、权限审批、物品出门、外包管理。	EVD-05/EVD-09
M-06	**审计与复盘**	Detect/Recover	门禁记录分析、视频抽查、巡逻复核、事件复盘、案例入库。	EVD-08/EVD-09
M-07	**恢复**	Recover	安防系统恢复、业务恢复、证据保护、舆情恢复、备用通道、心理支持。	EVD-06/EVD-12
M-08	**治理**	Govern	风险评估、责任分工、制度体系、预算保障、第三方管理、管理层评审。	EVD-09
M-09	**人员风险管理**	Deter/Detect	背景核验、高风险岗位、权限矩阵、离职回收、行为异常报告。	EVD-05/EVD-09
M-10	**安防系统网络与设备韧性**	Detect/Delay/Recover	资产清单、网络分区、强认证、远维审批、日志、补丁、配置备份。	EVD-01/EVD-08/EVD-11
M-11	**CPTED 与空间治理**	Deter/Detect/Delay	自然监视、出入控制、领域感、环境维护、照明、人车分流。	EVD-10/EVD-11
M-12	**供应链与物流安防**	Detect/Delay	承运商白名单、人车货单绑定、封签、双人交接、异常路线预警。	EVD-05/EVD-01
M-13	**风险情报与联动**	Detect/Respond	与公安、园区、物业、供应商、同业共享风险信息。	EVD-09/EVD-12
M-14	**Zero Trust Physical Access**	Deter/Detect/Delay	基于身份、权限、场景、时间、区域、行为和风险动态验证。	EVD-01/EVD-05
M-15	**内部威胁管理**	Detect/Respond	内部威胁小组、行为异常报告、权限审计、离职交接、人员风险干预。	EVD-01/EVD-08/EVD-09
M-16	**Hostile Vehicle Mitigation**	Deter/Delay/Respond	车辆接近路径分析、人车分流、车辆减速、防冲撞设施、门岗避险。	EVD-10/EVD-11
M-17	**应急响应与业务连续性**	Respond/Recover	主动暴力预案、车辆冲撞预案、可疑物处置、BCP、备用电源。	EVD-06/EVD-12
M-18	**安防绩效与持续改进**	Detect/Recover/Govern	KPI、控制有效性测试、红队演练、隐患整改、管理层评审。	EVD-08/EVD-09

11. 新增：技术—控制效果映射矩阵（示例）

本矩阵用于回答：“某项措施对某项攻击技术到底有多大效果，需要什么证据验证，仍剩什么风险？”实际工具中可扩展为全量 `MAT-` 关联表。

MAT	技术	控制措施	功能	效果等级	主要证据	常见剩余风险
MAT-001	**TEC-0301 尾随进入**	M-14 + M-02 + M-03	Detect/Delay	高	ACS日志 + 视频	员工替人开门文化未改变。
MAT-002	**TEC-0302 冒充访客**	M-05 + M-14	Deter/Detect	中高	访客记录、证件扫描	前台忙碌时漏验。
MAT-003	**TEC-0303 冒充供应商/维修**	M-12 + M-05 + M-14	Detect/Delay	高	工单、车牌、陪同记录	急修情境下破口。
MAT-004	**TEC-0304 借卡/冒用卡**	M-14 + M-02	Detect	中高	ACS + 视频比对	未启用人卡绑定。
MAT-005	**TEC-0306 翻越围界**	M-02 + M-03 + M-11	Detect/Delay	高	PIDS、照明、围界检查	夜间盲区。
MAT-006	**TEC-0308 利用未关闭入口**	M-02 + M-03 + M-18	Detect/Delay	高	门磁、超时记录	习惯性撑门。
MAT-007	**TEC-0607 远维绕过实体控制**	M-10 + M-12 + M-15	Detect/Delay	高	远维日志、工单、会话录像	厂商例外账号未管控。
MAT-008	**TEC-0801 盗窃**	M-02 + M-03 + M-06	Detect/Delay/Recover	中高	视频、RFID、盘点	低频小额长期流失。
MAT-009	**TEC-0804 纵火**	M-02 + M-04 + M-17	Detect/Respond/Recover	中高	消防、视频、现场勘验	加速剂点位未发现。
MAT-010	**TEC-0805 暴力伤害**	M-04 + M-17 + M-09	Respond/Recover	中	通报、演练、威胁评估	事前前兆采集不足。
MAT-011	**TEC-0808 安防系统干扰**	M-10 + M-04 + M-18	Detect/Respond	高	配置变更日志、健康监控	备援未完全切换。
MAT-012	**TEC-0809 车辆冲撞**	M-16 + M-11 + M-17	Deter/Delay/Respond	高	HVM设计、VSB等级、演练	周界外公共道路限制。
MAT-013	**TEC-1001 权限长期滥用**	M-15 + M-14 + M-06	Detect	中高	权限审查、审计报告	低频行为难察觉。
MAT-014	**TEC-1202 假承运/假提货**	M-12 + M-05 + M-06	Detect/Delay	高	提货核验、封签、交接录像	紧急改单漏洞。
MAT-015	**TEC-1401 多点事件分散响应**	M-04 + M-17 + M-13	Respond/Recover	中高	指挥记录、通联、预案	人力池不足。
MAT-016	**TEC-1402 通信/报警链条干扰**	M-10 + M-17	Detect/Recover	中高	通信监测、备援测试	备援路径未常态测试。
MAT-017	**TEC-0107 / TEC-0808 UAS侦察/干扰**	M-02 + M-16 + M-17	Detect/Respond	中高	UAS侦测、视频、飞行事件记录	法规限制反制手段。
MAT-018	**TEC-0106 / TEC-0808 安防系统 cyber-physical 攻击**	M-10 + M-08	Detect/Delay	高	CAPSS/硬化证据、系统日志	旧设备无法升级。

矩阵评分建议

```
Control Effectiveness Score
= Function Coverage × Deployment Quality × Evidence Strength × Operational Readiness

Residual Risk
= Technique Severity × Actor Capability × Path Feasibility - Effective Control Score
```

12. 新增：证据与置信度模型

v0.3 将“看到什么”和“凭什么相信”拆开处理。行为指标命中后，应根据证据类型、证据数量、来源独立性和相互印证程度确定置信度。

代码	类型	内容	预设可信度
EVD-01	**系统事件证据**	ACS、VMS、IDS、PIDS、PSIM、SIEM 日志。	高
EVD-02	**视频 / 影像证据**	CCTV、行车记录、手机影像、UAS 观察。	高
EVD-03	**感测器证据**	门磁、震动、烟温、雷达、RFID、玻破。	中高
EVD-04	**人体观察证据**	保安、前台、主管、员工、访客回报。	中
EVD-05	**文件 / 流程证据**	工单、预约、交接单、合同、名册、钥匙台账。	中高
EVD-06	**应急处置证据**	通联、值班记录、到场时间、指挥记录、报警记录。	中高
EVD-07	**勘验与实物证据**	封签、破坏痕迹、工具、遗留物、损坏设备。	高
EVD-08	**审计 / 趋势证据**	权限审查、盘点差异、告警趋势、异常行为分析。	中高
EVD-09	**管理性证据**	制度、培训、演练、签核、责任矩阵、评审记录。	中
EVD-10	**设计 / 建置证据**	HVM 设计、围界等级、照明设计、CPTED 图纸。	中高
EVD-11	**验证 / 测试证据**	测试报告、CAPSS、红队、渗透测试、演练结果。	高
EVD-12	**外部情报 / 执法信息**	警方通报、行业预警、公开案件资料、同业情报。	中

置信度分级

等级	名称	判定规则
C0	**未知**	无可用证据
C1	**低**	单一来源，且为易误判来源
C2	**中**	两种来源，或单一高质量系统证据
C3	**中高**	至少两种独立来源，其中一种为系统、视频或勘验证据
C4	**高**	三种以上来源相互印证，且包含至少一种高完整性证据
C5	**极高**	已完成取证、审计或官方确认，可直接进入案例库

证据融合规则

1. 单一访谈或单一告警，不得直接映射为高置信技术判断。
2. 同一设备产生的多笔记录，只算一个独立来源。
3. 若存在视频 + 门禁 + 工单/预约三者一致，通常可升至 C4。
4. 若存在管理缺陷但无事件证据，可判为脆弱性成立，不可直接判为攻击已发生。
5. 对 AI 推理引擎，应保留 evidence_trace、confidence_score、contradictions 字段。

---

13. 新增：行业画像库

行业画像库用于避免通用知识库落回“一张表检查所有单位”。同一攻击技术在不同场景中的优先级不同，因此工具中应支持行业默认权重和本地化调整。

代码	行业	核心资产	高优先威胁主体	高频技术 / 路径	重点指标	重点控制	本地化建议
IP-01	**学校 / 校园**	A001/A006/A008	T008/T009/T016	TEC-0301/TEC-0302/TEC-0805；PATH-02/PATH-09	IND-0301-01、IND-0805-01、IND-0206-01	M-05、M-14、M-17、M-09	本地化建议：区分校门、教学楼、宿舍、实验室、接送区，建立学生、家长、外包、访客分类准入。
IP-02	**医院 / 医疗场域**	A001/A005/A007/A012	T009/T016/T013	TEC-0206/TEC-0705/TEC-0805/TEC-1401；PATH-02/PATH-11	IND-0805-02、IND-0206-01、IND-1401-01	M-04、M-17、M-09、M-05	本地化建议：急诊、门诊、住院、药房和财务窗口应差异化设置冲突降级与快速报警。
IP-03	**制造业 / 工厂 / 工控场域**	A005/A006/A007/A013	T006/T007/T013/T017	TEC-0203/TEC-0607/TEC-0704/TEC-0803；PATH-05/PATH-06/PATH-13	IND-0203-01、IND-0607-01、IND-0803-01	M-10、M-12、M-14、M-15	本地化建议：承包商、装卸区、危险品库、配电室、实验室和生产线应纳入统一路径评估。
IP-04	**数据中心**	A005/A003/A009/A007	T012/T013/T017	TEC-0106/TEC-0605/TEC-0808/TEC-1001；PATH-13	IND-0106-01、IND-0605-01、IND-0808-01	M-10、M-14、M-08、M-07	新增国际经验：对接 NPSA CAPSS / data centre security 思路，将安防系统自身作为关键资产。
IP-05	**商业零售 / 商场**	A002/A001/A010/A008	T001/T014/T010	TEC-0205/TEC-0301/TEC-0801/TEC-0904/TEC-1202；PATH-02/PATH-10	IND-0205-01、IND-0301-01、IND-0801-01、IND-0905-01	M-02、M-03、M-12、M-18	新增国际经验：ORC 不只发生在卖场，也可能发生在后仓、配送和退货环节。
IP-06	**能源设施 / 变电与供能场域**	A005/A006/A007/A001	T011/T012/T017/T009	TEC-0102/TEC-0306/TEC-0803/TEC-0809/TEC-0810；PATH-01/PATH-12/PATH-13	IND-0306-01、IND-0803-01、IND-0809-01、IND-0810-01	M-03、M-10、M-16、M-17	新增国际经验：将实体破坏、网络化安防系统风险、自然灾害和业务连续性联动评估。
IP-07	**政务 / 公共服务机关**	A001/A008/A006/A007	T015/T016/T009/T010	TEC-0206/TEC-0302/TEC-0805/TEC-1104/TEC-1401；PATH-02/PATH-08/PATH-12	IND-0206-01、IND-0805-01、IND-1104-01、IND-1401-01	M-01、M-04、M-17、M-16	本地化建议：接访、窗口、门前广场、停车落客区和舆情场景应联动设计。
IP-08	**仓储 / 物流 / 冷链**	A011/A002/A005	T007/T014/T003	TEC-0202/TEC-0602/TEC-0905/TEC-1202；PATH-03/PATH-10	IND-0202-01、IND-0602-01、IND-0905-01、IND-1202-01	M-12、M-05、M-06、M-17	本地化建议：建立人、车、单、货、封签、时间窗六要素核验。

14. 案例映射库（升级版）

案例映射不应只记录“发生了什么”，而应将案例拆解为主体、目标、战术、技术、路径、指标命中、脆弱性、控制缺口、证据、置信度和可转化评估指标。

案例字段建议

字段	含义
case_id	**案例编号**
case_name	**案例名称**
scenario	**场景描述**
actors	**威胁主体**
assets	**目标资产**
tactics	**攻击战术**
techniques	**攻击技术链**
path_refs	**攻击路径**
indicators_hit	**命中的行为指标**
vulnerabilities	**利用脆弱性**
controls_present	**已有控制**
controls_missing	**缺失或失效控制**
evidence	**证据类型**
confidence	**置信度**
lessons_learned	**复盘结论**
assessment_metrics	**可转化评估指标**

案例	场景	主体	资产	技术链	指标命中	关键脆弱性	建议措施	可转化指标
CASE-001	**外部人员冒充维修人员进入办公楼盗窃**	T001/T007	A002	TEC-0203 → TEC-0303 → TEC-0401 → TEC-0701 → TEC-0901	IND-0203-01/IND-0303-01	V-05/V-06/V-03/V-07	M-05/M-03/M-06	维保工单核验率、访客陪同落实率、异常进入复核率。
CASE-002	**Moore County 变电站破坏类关键设施外围攻击**	T002/T011/T016	A005/A007/A008	TEC-0102 → TEC-0306 → TEC-0803 → TEC-0810	IND-0102-01/IND-0306-01/IND-0810-01	V-01/V-02/V-16	M-02/M-03/M-17	关键设施周界探测覆盖率、报警到场时间、恢复时间。
CASE-003	**车辆冲撞公共开放空间事件**	T009/T011/T016	A001/A008/A012	TEC-0204 → TEC-0311 → TEC-0809 → TEC-1102	IND-0204-01/IND-0311-01/IND-0809-01	V-09/V-10/V-20	M-16/M-11/M-17	车辆可达速度、缓冲距离、防冲撞设施覆盖率。

案例	场景	主体	资产	技术链	指标命中	关键脆弱性	建议措施	可转化指标
CASE-004	**网络赋能货运盗窃 / 虚假提货**	T003/T007/T014	A002/A011	TEC-0202 → TEC-1202 → TEC-0602 → TEC-0905	IND-0202-01/IND-1202-01/IND-0905-01	V-14/V-19/V-07	M-12/M-05/M-06	人车货单一致率、 承运商临时变更复核率、封签异常率。
CASE-005	**有组织零售盗窃 ORC**	T003/T014	A002/A008	TEC-0205 → TEC-0504 → TEC-0801 → TEC-0904	IND-0205-01/IND-0801-01/IND-0904-01	V-07/V-11/V-13	M-02/M-03/M-13/M-18	高风险商品损耗率、 重复异常人员识别率、 视频证据完整率。
CASE-006	**主动暴力 / 工作场所暴力事件**	T009/T016	A001/A008/A012	TEC-0206 → TEC-0705 → TEC-0805 → TEC-1102	IND-0805-01/IND-0805-02	V-15/V-20/V-13	M-09/M-04/M-17	高风险纠纷台账完整率、 一键报警覆盖率、演练覆盖率。
CASE-007	**Tesla Berlin 疑似纵火导致供电中断类外部依赖点攻击**	T015/T002/T016	A005/A007/A008	TEC-0804 → TEC-0810 → TEC-1103	IND-0804-02/IND-0810-01	V-16/V-01/V-02	M-02/M-17/M-18	关键外部依赖点识别率、 备用能源支撑时间、恢复时间。
CASE-008	**Butler 集会安保失败类高风险活动外围控制**	T016/T011/T017	A001/A008/A012	TEC-0102 → TEC-0206 → TEC-0501 → TEC-1401/1402	IND-0102-01/IND-0501-01/IND-1401-01	V-04/V-13/V-20	M-04/M-17/M-13/M-18	责任矩阵完整率、高点排查覆盖率、 统一指挥响应时间。
CASE-009	**机场 / 关键设施周界闯入**	T001/T002/T009/T011	A001/A005/A007	TEC-0306 → TEC-0501 → TEC-0506 → TEC-0508	IND-0306-01/IND-0501-01/IND-0508-01	V-01/V-02/V-13	M-02/M-03/M-04/M-18	周界报警准确率、误报治理率、 报警到场时间。
CASE-010	**未授权无人机抵近侦察资料中心**	T012/T017	A005/A003/A009	TEC-0107 → TEC-0501 → TEC-1101	IND-0107-01/IND-0107-02	V-02/V-12/V-20	M-02/M-17/M-13	UAS事件发现率、报告链路、 空域联动时间。
CASE-011	**内部人员慢性滥用权限**	T004/T013	A003/A010/A013	TEC-1001 → TEC-1003 → TEC-0802	IND-1001-01/IND-1003-01/IND-0802-01	V-05/V-18/V-17	M-14/M-15/M-06	权限复核率、异常行为复核率、 离职权限回收时效。
CASE-012	**多点事件分散安保后趁机进入**	T003/T010/T015	A002/A006/A008	TEC-1401 → TEC-0308 → TEC-0403 → TEC-0801	IND-1401-01/IND-0308-01	V-04/V-13/V-08	M-04/M-17/M-18	多点事件指挥链、关键点不脱岗率、 复盘闭环率。

15. 主要更新点总结与后续扩展建议

15.1 本次主要更新点

1. **从“技术条目”升级为“技术 + 指标 + 证据 + 控制效果”**：每个技术不再只描述手法，还能映射可观察信号、证据来源和控制措施。
2. **从“威胁主体分类”升级为“主体能力向量”**：每类主体均可按组织化、资源、情报、技术、暴力、接近权、持续性、规避能力评分。
3. **从“措施清单”升级为“D-D-D-R-R 控制矩阵”**：可判断措施是威慑、探测、延迟、响应还是恢复，以及控制证据是否充分。
4. **从“案例叙述”升级为“案例知识图谱节点”**：案例可反向沉淀为主体、技术、路径、指标、脆弱性、措施和行业权重。
5. **从“通用安防字典”升级为“行业画像模板”**：支持学校、医院、制造、数据中心、零售、能源、政务、仓储物流等场景的差异化评估。

15.2 后续扩展建议

1. **建立指标事件表**：将 `IND` 与门禁、视频、访客、工单、物流、巡检、应急系统对接，形成 `indicator_event`。
2. **建立路径评分器**：为每条 `PATH` 的关键节点设置可行性、暴露度、延迟时间、响应时间和证据强度。
3. **建立控制覆盖率计算器**：从 `MAT` 中自动计算某项技术在当前单位是否被有效覆盖。
4. **建立行业权重模板**：如学校优先人员安全，医院优先暴力冲突和开放空间，数据中心优先安防系统网络韧性和供应商治理。
5. **建立案例反向学习机制**：每次事件复盘后反向更新 `IND`、`MAT`、`V`、`IP` 权重。
6. **保留人工复核机制**：AI 推理结果必须展示指标来源、证据链、置信度、矛盾证据和人工确认状态。

15.3 本版本定位

```
v0.1：基础字典
v0.2：国际化 ATT&CK 式实体安防知识库
v0.3：可观测、可评分、可验证、可推理的风险评估知识库
```

最终目标不是简单保存案例，而是将零散案例、检查问题、隐患整改、安防措施和风险评估结果，转化为可积累、可检索、可复用、可量化、可推理的实体安防威胁行为知识库。

附录A：工具开发字段示例

> 本附录集中存放所有 JSON 示例。正文阅读时可以跳过；开发风险评估工具、案例匹配工具、规则引擎或 AI 推理模块时使用。

A.1 攻击技术字段示例

```
{
  "id": "TEC-0301",
  "name_zh": "尾随进入",
  "name_en": "Tailgating",
  "tactic": "TAC-03",
  "actors": ["T001", "T008", "T013"],
  "assets": ["A001", "A006", "A010"],
  "indicators": ["IND-0301-01", "IND-0301-02", "IND-0301-03"],
  "controls": ["M-02", "M-03", "M-14"],
  "evidence_required": ["EVD-01", "EVD-02", "EVD-04"],
  "path_refs": ["PATH-02", "PATH-09"],
  "confidence_rule": ">=2个独立来源且含1个系统证据时，可升至中高置信",
  "residual_risk_logic": "若无反尾随设施与人工抽查，则剩余风险维持中高"
}
```

A.2 行为指标字段示例

```
{
  "indicator_id": "IND-0301-01",
  "name": "单次刷卡多人通行",
  "observable": "门禁一次合法开门后，第二人未刷卡跟入",
  "data_source": ["ACS日志", "视频AI", "巡更观察"],
  "related_techniques": ["TEC-0301"],
  "threshold": "5分钟内>=1次即可触发；30日内累计>3次升级",
  "evidence_type": ["EVD-01", "EVD-02"],
  "base_confidence": "中",
  "triage_severity": "中高"
}
```

A.3 主体能力模型字段示例

```
{
  "capability_id": "CAP-T013",
  "actor_id": "T013",
  "actor_name": "内部威胁人员",
  "dimensions": {
    "organization": 3,
    "resource": 2,
    "intelligence": 5,
    "technical": 3,
    "violence": 1,
    "access": 5,
    "persistence": 5,
    "evasion": 5
  },
  "typical_strength": "合法接近权、流程熟悉、低可见性、长期持续性",
  "typical_controls": ["M-09", "M-14", "M-15", "M-06"]
}
```

A.4 技术—控制效果矩阵字段示例

```
{
  "matrix_id": "MAT-001",
  "technique_id": "TEC-0301",
  "control_ids": ["M-14", "M-02", "M-03"],
  "control_function": ["Detect", "Delay"],
  "effectiveness_level": "高",
  "required_evidence": ["EVD-01", "EVD-02", "EVD-11"],
  "residual_risk": "员工替人开门文化未改变时，仍存在中等剩余风险",
  "test_method": "抽查门禁日志与视频，进行反尾随演练或红队测试"
}
```

A.5 案例映射字段示例

```
{
  "case_id": "CASE-010",
  "scenario": "未授权无人机抵近侦察资料中心",
  "actors": ["T012", "T017"],
  "assets": ["A005", "A003", "A009"],
  "tactics": ["TAC-01", "TAC-05"],
  "techniques": ["TEC-0107"],
  "path_refs": ["PATH-15"],
  "indicators_hit": ["IND-0107-01", "IND-0107-02"],
  "evidence": ["EVD-02", "EVD-03"],
  "confidence": "C3",
  "controls_present": ["M-02"],
  "controls_missing": ["M-16", "M-17"],
  "impact": "中",
  "lessons_learned": "需建立UAS事件升级流程与空域协调机制"
}
```

A.6 行业画像字段示例

```
{
  "industry_id": "IP-04",
  "industry_name": "数据中心",
  "core_assets": ["A005", "A003", "A009", "A007"],
  "priority_actors": ["T012", "T013", "T017"],
  "priority_techniques": ["TEC-0106", "TEC-0605", "TEC-0607", "TEC-0808", "TEC-1001"],
  "priority_paths": ["PATH-13", "PATH-07"],
  "priority_vulnerabilities": ["V-12", "V-18", "V-16"],
  "recommended_controls": ["M-10", "M-14", "M-08", "M-07"],
  "localization_note": "应结合等保、关基、数据安全、个人信息保护和视频图像信息管理要求。"
}
```

附录B：JSON 数据结构模板

B.1 知识库根结构模板

```
{
  "version": "v0.3",
  "updated_at": "2026-06",
  "knowledge_base_name": "实体安防威胁行为知识库",
  "tables": {
    "actors": [],
    "assets": [],
    "tactics": [],
    "techniques": [],
    "indicators": [],
    "capabilities": [],
    "paths": [],
    "vulnerabilities": [],
    "controls": [],
    "control_matrix": [],
    "evidence_types": [],
    "confidence_levels": [],
    "industry_profiles": [],
    "case_mappings": []
  }
}
```

B.2 攻击技术表模板

```
{
  "technique_id": "TEC-0000",
  "name_zh": "",
  "name_en": "",
  "tactic_id": "TAC-00",
  "description": "",
  "related_actor_ids": [],
  "related_asset_ids": [],
  "related_path_ids": [],
  "related_vulnerability_ids": [],
  "indicator_ids": [],
  "recommended_control_ids": [],
  "evidence_required": [],
  "typical_cases": [],
  "localization_note": "",
  "international_practice_note": ""
}
```

B.3 行为指标表模板

```
{
  "indicator_id": "IND-0000-00",
  "name": "",
  "observable": "",
  "related_technique_ids": [],
  "data_sources": [],
  "trigger_rule": "",
  "severity_hint": "低/中/中高/高",
  "base_confidence": "低/中/中高/高",
  "evidence_type_ids": [],
  "false_positive_notes": "",
  "response_hint": ""
}
```

B.4 证据与置信度模板

```
{
  "evidence_record_id": "EVR-000001",
  "event_time": "2026-06-01T10:30:00+08:00",
  "evidence_type_id": "EVD-01",
  "source_system": "ACS",
  "source_id": "door-3F-001",
  "related_indicator_id": "IND-0301-01",
  "raw_reference": "log_id_or_file_path",
  "integrity_status": "原始/复制/人工录入/待核验",
  "confidence_level": "C3",
  "reviewer": "",
  "review_status": "待复核/已复核/已排除/已入库"
}
```

B.5 技术—控制效果矩阵模板

```
{
  "matrix_id": "MAT-000",
  "technique_id": "TEC-0000",
  "control_ids": [],
  "control_functions": ["Deter", "Detect", "Delay", "Respond", "Recover"],
  "effectiveness_level": "低/中/中高/高",
  "deployment_quality_required": "",
  "required_evidence_ids": [],
  "test_method": "",
  "residual_risk_description": "",
  "recommended_improvement": ""
}
```

B.6 案例映射模板

```
{
  "case_id": "CASE-000",
  "case_name": "",
  "event_time": "",
  "industry_profile_id": "IP-00",
  "scenario": "",
  "actor_ids": [],
  "asset_ids": [],
  "tactic_ids": [],
  "technique_ids": [],
  "path_ids": [],
  "indicator_ids_hit": [],
  "vulnerability_ids": [],
  "controls_present": [],
  "controls_failed": [],
  "controls_missing": [],
  "evidence_records": [],
  "confidence_level": "C0-C5",
  "impact_level": "低/中/高/极高",
  "lessons_learned": "",
  "assessment_metrics": []
}
```

附录C：数据库字段建议

C.1 推荐建库方式

第一阶段建议使用 SQLite 或 PostgreSQL 的关系型结构，配合部分 JSON 字段保存多对多关系。工具成熟后，可进一步同步到图数据库。

阶段	推荐方式	适用场景
原型阶段	**Markdown + CSV + SQLite**	Streamlit、本机工具、轻量评估工具
业务应用阶段	**PostgreSQL + API**	多用户、权限管理、版本管理
AI 推理阶段	**PostgreSQL + 向量库 + 图数据库**	案例相似度、路径推理、自动推荐措施

C.2 主表字段建议

actors 威胁主体表

字段	类型	说明
actor_id	**TEXT PRIMARY KEY**	T001 等
name_zh	**TEXT**	中文名称
name_en	**TEXT**	英文名称
description	**TEXT**	主体描述
typical_assets	**TEXT / JSON**	常见目标资产
typical_tactics	**TEXT / JSON**	常见战术
capability_id	**TEXT**	CAP-T001 等
localization_note	**TEXT**	本地化建议

capabilities 主体能力表

字段	类型	说明
capability_id	**TEXT PRIMARY KEY**	CAP-T001 等
actor_id	**TEXT**	对应主体
organization_score	**INTEGER**	组织化程度 1-5
resource_score	**INTEGER**	资源能力 1-5
intelligence_score	**INTEGER**	情报能力 1-5
technical_score	**INTEGER**	技术能力 1-5
violence_score	**INTEGER**	暴力能力 1-5
access_score	**INTEGER**	接近权 1-5
persistence_score	**INTEGER**	持续性 1-5
evasion_score	**INTEGER**	规避能力 1-5
note	**TEXT**	说明

techniques 攻击技术表

字段	类型	说明
technique_id	**TEXT PRIMARY KEY**	TEC-0301 等
name_zh	**TEXT**	中文名称
tactic_id	**TEXT**	TAC-03 等
description	**TEXT**	技术描述
indicator_ids	**JSON**	关联 IND
control_ids	**JSON**	关联 M
evidence_required	**JSON**	关联 EVD
path_refs	**JSON**	关联 PATH
severity_default	**INTEGER**	默认严重性 1-5

indicators 行为指标表

字段	类型	说明
indicator_id	**TEXT PRIMARY KEY**	IND-0301-01 等
name	**TEXT**	指标名称
related_techniques	**JSON**	关联技术
data_sources	**JSON**	数据来源
trigger_rule	**TEXT**	触发规则
evidence_type_ids	**JSON**	证据类型
base_confidence	**TEXT**	基础置信度
severity_hint	**TEXT**	严重性提示

control_matrix 控制效果矩阵表

字段	类型	说明
matrix_id	**TEXT PRIMARY KEY**	MAT-001 等
technique_id	**TEXT**	技术编号
control_ids	**JSON**	控制措施
control_functions	**JSON**	Deter/Detect/Delay/Respond/Recover

字段	类型	说明
effectiveness_level	**TEXT**	低/中/中高/高
required_evidence_ids	**JSON**	所需证据
residual_risk	**TEXT**	剩余风险
test_method	**TEXT**	验证方式

evidence_records 证据记录表

字段	类型	说明
evidence_record_id	**TEXT PRIMARY KEY**	证据记录编号
evidence_type_id	**TEXT**	EVD-01 等
source_system	**TEXT**	ACS/VMS/IDS/工单等
source_id	**TEXT**	设备或系统编号
related_indicator_id	**TEXT**	命中指标
raw_reference	**TEXT**	原始记录路径或编号
confidence_level	**TEXT**	C0-C5
review_status	**TEXT**	待复核/已复核/已排除/已入库
reviewer	**TEXT**	复核人
created_at	**DATETIME**	记录时间

case_mappings 案例映射表

字段	类型	说明
case_id	**TEXT PRIMARY KEY**	CASE-001 等
case_name	**TEXT**	案例名称
industry_profile_id	**TEXT**	IP-01 等
actor_ids	**JSON**	威胁主体
asset_ids	**JSON**	目标资产
tactic_ids	**JSON**	战术
technique_ids	**JSON**	技术链
path_ids	**JSON**	路径

字段	类型	说明
indicator_ids_hit	**JSON**	命中指标
vulnerability_ids	**JSON**	脆弱性
controls_failed	**JSON**	失效措施
confidence_level	**TEXT**	置信度
lessons_learned	**TEXT**	复盘结论

C.3 关系表建议

表名	作用
actor_technique_map	**主体—技术常见关系**
technique_indicator_map	**技术—指标关系**
technique_control_map	**技术—控制关系**
technique_evidence_map	**技术—证据需求关系**
industry_technique_weight	**行业—技术权重**
path_technique_sequence	**路径—技术顺序**
case_indicator_hit	**案例—指标命中**

C.4 风险评分字段建议

字段	含义
actor_capability_score	**威胁主体能力综合分**
asset_criticality_score	**资产关键性分**
path_feasibility_score	**路径可行性分**
vulnerability_exposure_score	**脆弱性暴露分**
control_effectiveness_score	**控制有效性分**
evidence_confidence_score	**证据置信分**
residual_risk_score	**剩余风险分**
recommendation_priority	**整改优先级**

C.5 最小可用工具开发顺序

1. 先录入 `T / A / TAC / TEC / PATH / V / M` 基础字典。
2. 再录入 `IND` 行为指标库。
3. 建立 `TEC_IND`、`TEC_M`、`TEC_EVD` 三类映射。
4. 增加 `CAP` 主体能力评分。
5. 增加 `MAT` 控制效果矩阵。
6. 增加 `CASE` 案例映射和 `IP` 行业画像。
7. 最后开发自动推荐逻辑：指标命中 → 技术匹配 → 路径推断 → 主体可能性 → 脆弱性定位 → 措施推荐。