腾讯云

企业创新在线学堂

互联网暴露面风险趋势与能力建设

关于暴露面

本产品孵化自腾讯安全实验室，历经多年攻防实战的锤炼，专注于在大型攻防演练和日常安全运营中精准发现风险，最终为企业实现降本增效。

讲师介绍

暴露面产品负责人

梁国锋

多年大型攻防演练经验，对攻与防有深入的实战理解，负责暴露面的产品设计与技术规划，从0到1的落地与建设。

企业创新在线学堂

目录 Menu

企业创新在线学堂

互联网暴露面风险趋势

攻击趋利化，自动化，成主流攻击手段

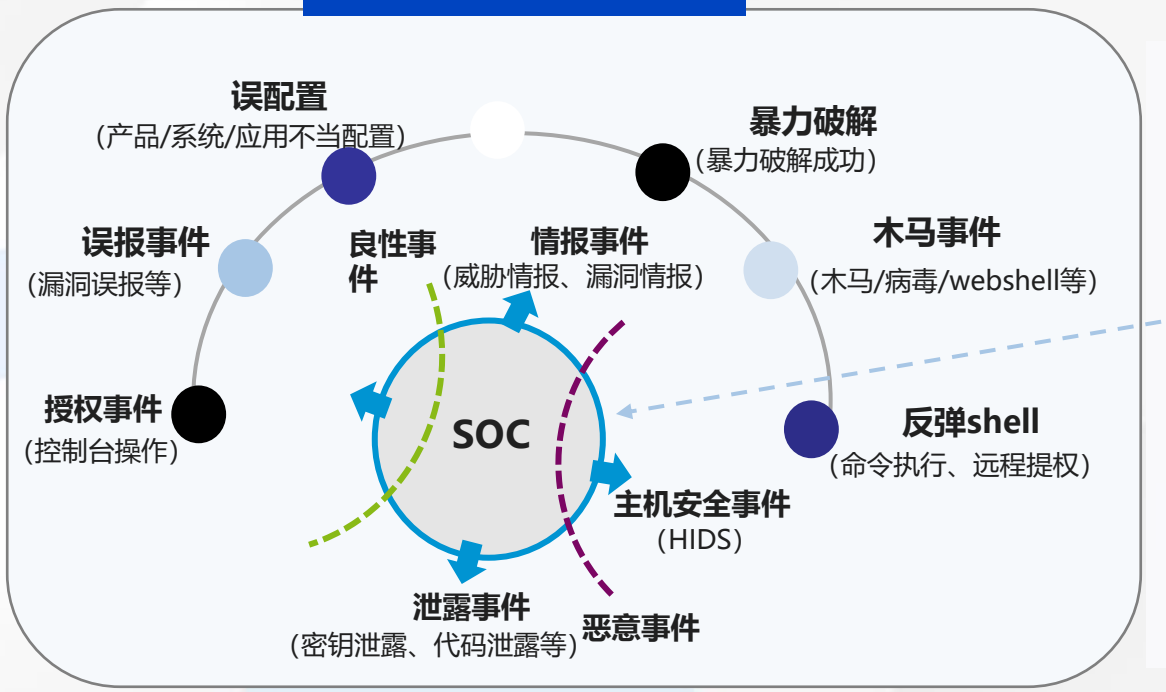
威胁主体	利用技术趋势	受攻击目标	
National Governments “国家级”攻击力量	0Day研究 / APT 供应链攻击 硬件/固件攻击 物理设施/设备攻击	Classified information 分类(涉密)信息： 政府及军事领域的涉密信息和系统	保密法 分级保护 军工保密 FAA 1600.2 DOD SRG ITAR/FIPS
Terrorists / Hacktivists 恐怖分子/无政府主义黑客	Botnet DDOS **勒索软件** **挖矿软件** 邮件/钓鱼/恶意软件 0Day利用/APT 针对AI的攻击 AI辅助攻击	National critical infrastructure 国家关键基础设施： 能源、交通、金融、通信等关键领域的机密性和可用性	信息安全法 等级保护 4+ FISMA FedRAMP High
Industrial Spies and Organized Crime Groups 商业间谍和有组织犯罪（黑灰产）		Controlled Unclassified Information 受控未分类信息： 政府和重要企事业单位的非涉密信息	网络安全法 等级保护 3+ FISMA FedRAMP Low+
Hackers 一般黑客	邮件/钓鱼/恶意软件 0Day利用/扫描 弱口令 Web漏洞	Commercial data 一般商业数据： 一般企业的商业和业务经营数据 Personally identifiable information (PII) 个人敏感信息： 个人身份、隐私相关的敏感数据	SOX HIPAA PCI-DSS
Insiders 内部无意识/恶意用户	邮件/钓鱼/恶意软件 弱口令/无意识信息泄露 越权访问		HIPAA GDPR 个人信息 保护法 数据安全法

Botnet控制者
Foreign intelligence services
Bot-network operators
Spyware/malware controller
Phishers/Spammers

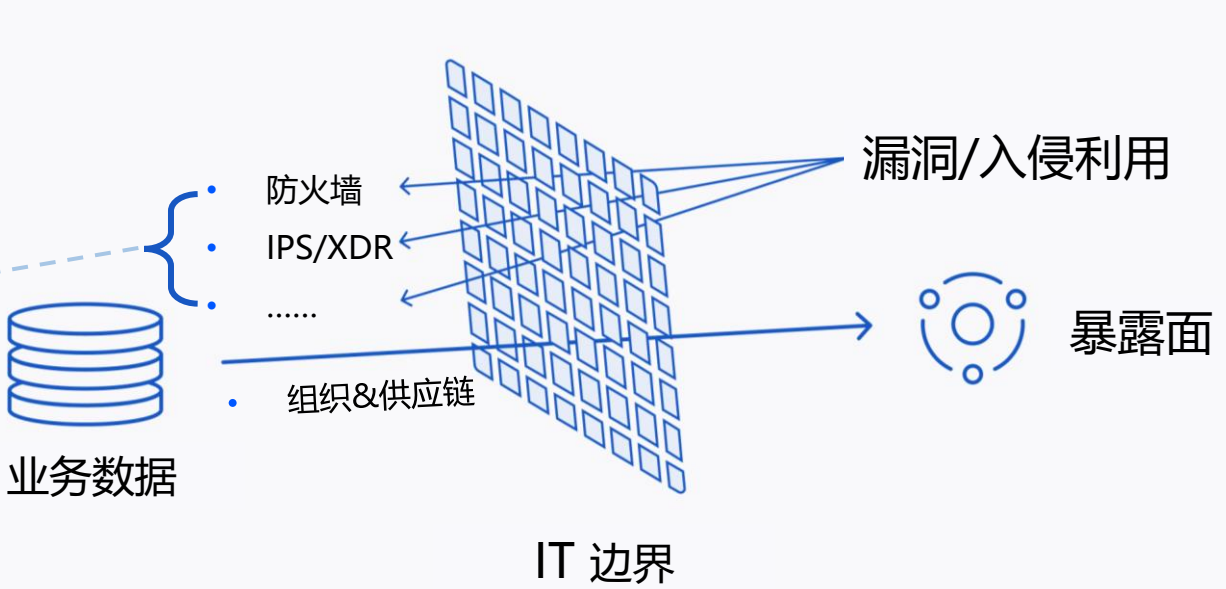
- 针对企业和重要机构的高危害攻击案例每年增加约27%。
- 2025年国际国内政企行业勒索事件、数据窃取事件，层出不穷。

产品告警驱动向暴露面管理驱动转变

产品告警驱动



威胁暴露面驱动



从 产品告警 驱动向 攻击视角威胁暴露面 转变

企业创新在线学堂

互联网隐匿攻击案例

存储桶盗刷

隐私泄露

因权限设置不当被恶意上传引流。导致存储桶被盗刷流量、造成财产损失、损害域名信誉、被通报。

API接口泄露

信息泄露

被入侵风险

利用API接口的未授权、越权等问题，低速非法获取数据、敏感token、密钥等

Stealer泄露

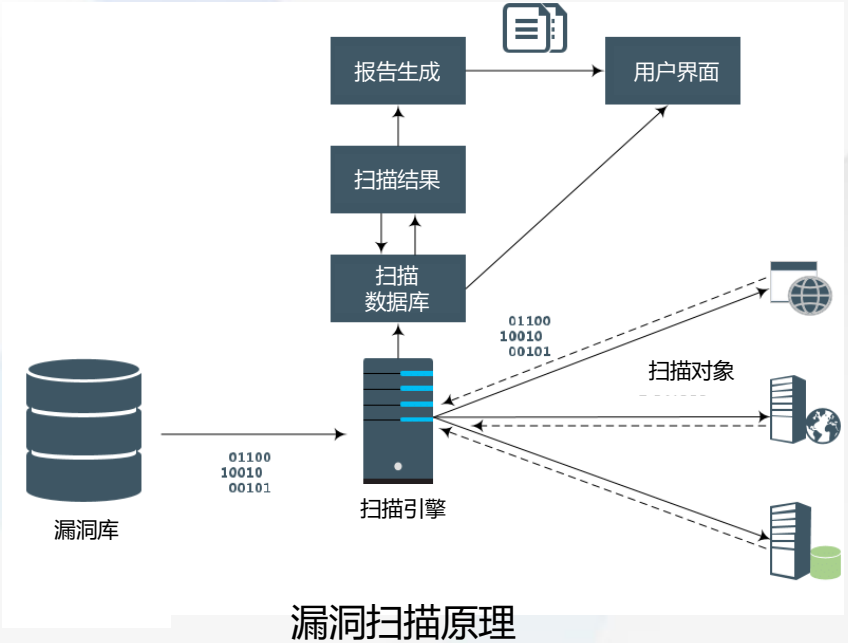
直接访问核心系统

利用暗网泄露的凭据直接绕开认证登录系统

传统扫描VS渗透存在的局限性

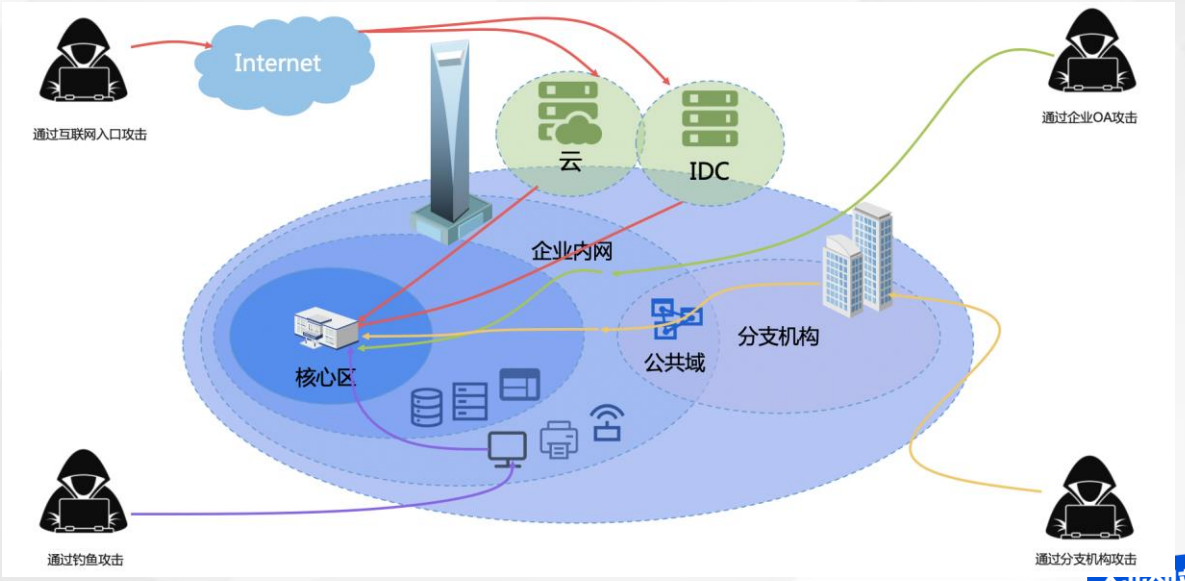
- 业务对外暴露面持续增加，可以被攻击者利用的风险点增加，往往在没有意识到的地方出现安全风险，导致业务被入侵
- 架构复杂度持续增加，使用的业务组件和服务应用往往导致不可控的风险，疏漏之处往往是被入侵的突破点

漏扫聚焦已知漏洞，存在局限性



漏洞扫描原理

渗透测试可识别暴露面，但实施成本较高



渗透测试及红蓝原理

企业创新在线学堂

攻强防弱—攻防演练常态化下的运营困境

差距点：攻击方往往占据攻防主动权，开展**持续、深度的风险面管理**，才能化被动为主动

以前的攻防演练（14天高频对抗）

	攻击方	防守方
人员	✓ 技术精湛，各单位优秀渗透人员 ✓ 团队作战，各人才分工明确高效	✗ 缺攻防经验，负责人以项目经理为主 ✗ 缺乏磨合，临时组建无实战配合
武器	✓ 大量0day漏洞储备 ✓ 专业攻防协作平台及工具集	✗ 已有安全厂商设备，IP封堵为主 ✗ 设备能力层次不齐
资金	✓ 多团队投入，形成A/B多联队 ✓ 外网专家储备	✗ 价低者中标 ✗ 部分单位租借或友情支持
情报	✓ 精良部队，各单位优秀渗透人员 ✓ 团队作战，分工专业	✗ 情报滞后，响应较晚 ✗ 虚假情报满天飞，干扰分析精力

现在的攻防演练（持续且深入的较量）

人员	✓ 技术精湛，各单位优秀渗透人员 ✓ 团队作战，各人才分工明确高效	✗ 缺攻防经验，负责人以项目经理为主 ✗ 缺乏磨合，临时组建无实战配合
武器	✓ 专业攻防协作平台及工具集 ✓ 更多攻防数据挖掘平台（社工、云等）	✗ 防护手段以漏扫、配置检查为主，缺乏攻击者视角风险发现能力 ✗ 缺乏云服务、员工社工钓鱼风险发现能力
天时	✓ 持久战，随意选择攻击时间、以逸待劳	✗ 黑白交替、拉锯战容易导致身心俱疲
地理	✓ 战场主动权，随意选择攻击目标	✗ 仅了解已知资产，供应链、分子公司等风险覆盖不全

解决思路——暴露面管理服务

CTEM 官方定义

持续威胁暴露面管理（CTEM）– Continuous Threat Exposure Management

即持续不断评估企业数字和物理资产的可访问性、暴露性和可利用性

腾讯实践

威胁暴露面管理 = 攻击面管理+风险验证+自动化修复改进

对比项	持续威胁暴露面（需具备的能力）	腾讯 服务解决方案（落地手段）
范围界定	✓	腾讯 EM 暴露面管理平台
持续发现	✓	
优先级划分	✓	
风险验证	✓	
动员修复	✓	

世界TOP企业安全实践

Microsoft

漏洞管理行业正在从有针对性的漏洞识别和修复发展为更全面的暴露管理方法，Gartner 将其称为持续威胁暴露管理（CTEM）

来源：https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/exposure-management-the-evolution-of-vulnerability-management/ba-p/4084587

企业创新在线学堂

漏洞扫描 VS 暴露面管理

	漏洞扫描	暴露面管理
关注范围	**查看组织系统、配置和软件中的弱点** 漏洞（CVEs）	**攻击者可能可见和访问的所有内容**，包括但不限于： 漏洞（CVEs or non-CVEs）、**云配置错误、凭据被盗、钓鱼风险**等
攻击面	端点（系统、应用）	内部、**外部、云、物联网设备、用户和供应链**
实施方式	周期扫描，每周1-2次	**近实时监测及扫描**、**原生集成各种API（测绘、数据泄露、子公司、情报等）**
评估方法	严重度	严重度、威胁等级、安全措施有效性、利用实施难度、业务影响
风险量化	无法量化	风险量化方式（**VPT**），基于情报动态评估，联动业务团队对齐
风险修复	补丁	补丁、**控制措施（策略、MFA等）**、配置修改等
运营价值	单向依赖 CMDB，通常资产易过期	双向集成，EM 平台能 **帮助更新 CMDB 资产**

案例1：漏洞扫描 VS 暴露面管理

实战案例：XX集团 存在API或敏感数据泄露场景

- 开发商不小心把测试的相关数据写在JS代码文件的问题
- 红队在Web网站的JS文件检测出相关的敏感数据与API接口，包含了账号密码、各种云的密钥，Saas化产品等各种各样的凭据、敏感信息
- 直接通过密钥渗透进入企业内部系统，获得业务生产数据

漏扫原理（基于“漏洞库”的“应试思维”）

- 基于**指纹**的漏洞扫描：可识别组件，但无法识别数据泄露及API
- 基于**PoC**的漏洞扫描：可识别漏洞，但无法识别数据泄露及API

漏洞名称	出现次数	详情和解决方法
检测到目标服务器启用了TRACE方法	1	
检测到目标服务器存在有可直接查看文件列表的目录	4	
检测到目标URL存在内部IP地址泄露	7	
发现目标存在永久性Cookie	1	
检测到目标网站robots文件网站结构信息泄露	1	
合计	**14**	

暴露面管理原理（基于“种子挖掘”的“发散式思维”）

- 暴露面管理通过 **主动爬虫+被动模糊匹配+AI分析** 获取到敏感信息以及系统入口，利用 js 中账号凭据（Admin/888888)成功登陆系统，获取大量摄像头、物联网设备控制权限

企业创新在线学堂

案例2:漏洞扫描 VS 暴露面管理

实战案例：XX集团出现多个类似名称小程序和公众号，导致用户信息泄露、监管机构通报

- 有攻击者以“XXX”品牌特征注册小程序和公众号，通过活动促销的文章收集用户信息，被用户投诉导致品牌声誉受损
- HW期间，某集团子公司私自注册了“XX”小程序，演练期间发现API鉴权不当导致集团客户信用卡信息泄露

漏扫的目的（“系统有没有已知漏洞？怎么修复”）

- **关注点：**
- ✓ 自身系统有没有 **漏洞**？
- ✓ 有哪些漏洞？
- ✓ 哪些事高危的漏洞？

暴露面管理的目的（“攻击者能不能进来？怎么进来？”）

- **关注点：**
- ✓ 系统本身、涉及的平台、人员、策略、供应链有没有 **风险**？
- ✓ 风险有哪些？
- ✓ 哪些风险可以直接进到内网来？

- *弱口令*
- *Nday漏洞*
- *……*

- *敏感信息〔员工邮箱、管理后台...〕*
- *登录凭据〔RDP、API key...〕*
- *0/1Day攻击情报*
- *小程序/公众号仿冒*
- *……*

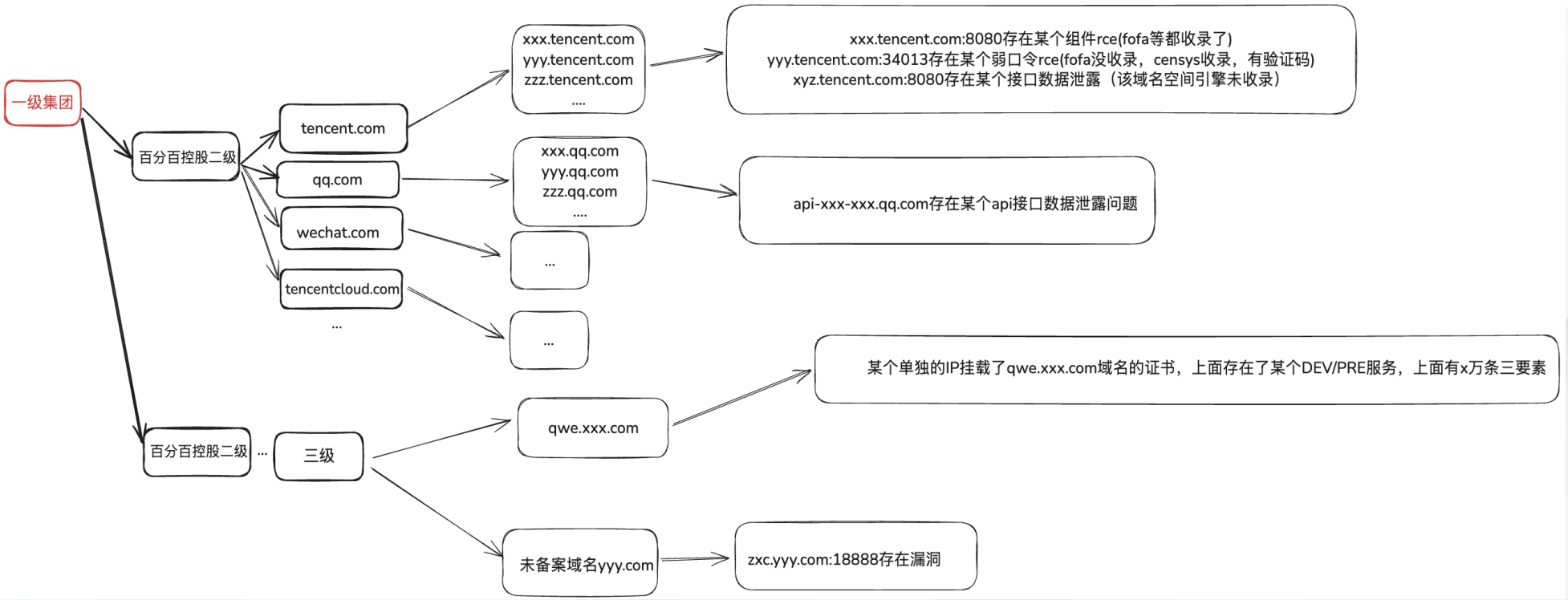
- *社工钓鱼*
- *主机失陷*
- *加密勒索*
- *数据泄露*
- *品牌声誉*
- *供应链攻击*
- *……*

企业创新在线学堂

构建持续的暴露面收敛能力

企业创新在线学堂

思考：实战案例



For攻击者

1、是否能全自动覆盖?

2、需要多久的时间?

For防守者

1、所有主机被入侵了都能发现吗?

2、新增一个子域名 是否可知?

3、发现问题多久能联系到负责人?

...

企业创新在线学堂

暴露面管理服务设计思路

暴露面监测 (Discovery)

测绘工具集（如云暴露面、暗网暴露面等）
识别资产暴露面、攻击向量和风险

暴露面分析（Prioritization）

以T-VPT为助力，提升风险识别精准度
基于历史漏洞行为，进行风险优先级划分

监测运营中心 （ Validation+Mobilization)

人工+工具平台深度验证漏洞影响，提供更精准修复建议

企业创新在线学堂

暴露面管理-服务内容

暴露面管理服务

服务内容

工具 | 监测分析

暴露面动态监测运营

- **资产测绘**（IP、域名、服务、证书等）
- **暴露面识别**（供应链、服务、凭据等）
- **脆弱性探测**（漏洞、配置等脆弱性风险）

算法 | 优先级评估 & 验证

暴露面关联分析及人工验证

- **关联分析** 资产与暴露面数据分析
- **路径验证** 验证暴露面潜在攻击路径
- **优先级研判**（VPT、过滤规则算法）

风险 | 修复&缓解

重点事件的统计分析，策略改进

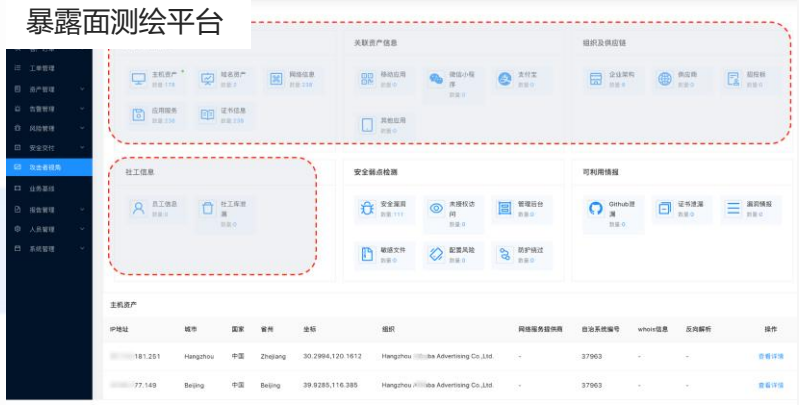
- **输出暴露面测绘报告**
- **输出安全运营改进建议**

暴露面监测指纹及策略优化

暴露面管理-服务能力构成和核心能力分布

暴露面监测系统（发现能力）

暴露面测绘平台



基础能力

- 互联网/暗网资产测绘
- 网站指纹分析
- 漏洞及基线检查
- 供应链风险挖掘
- 社工信息挖掘

核心能力

- 数据泄漏风险挖掘
- 云暴露面风险管理

数据联动

暴露面分析（分析能力）

情报字段丰富

- 国内外多方商业化情报
- 腾讯红队攻击情报
- ……

VPT优先级分析模型

- 情报自动化过滤
- 漏洞修复研判
- ……

可编排引擎交互

- 内置7大发现工作流
- 暴露面自定义编排能力
- ……

规则优化
能力扩展

辅助研判
风险告警

服务运营中心（运营能力）

人员组成

- 安全漏洞推修团队
- 腾讯安全服务蓝军

动员组织修复（Mobilization）

- 漏洞流程优化
- 研判标准优化
- 防护策略优化
- 自动化处置能力提升
- 安全运营实践分享
- ……

动员修复

暴露面分析及验证（Validation）

细节分析（运营）
风险核查（运营）

渗透测试（红队）
攻击模拟（BAS）

是否受影响

- 影响业务?
- 影响范围?
- 风险等级?
- 利用难度?
- 攻击路径?
- 检测方案?
- 修复方案?
- 缓解方案?

暴露面监测发现与运营能力

暴露面发现（技术）

企业主体	主域名
子域名	IP地址
网站后台	API服务
小程序	公众号
证书	云服务/容器
Github代码	邮箱账号

资产发现

×

域名解析	开放端口
服务指纹	操作系统
网络设备	安全设备
网站指纹	应用服务
网站接口	IoT系统
API接口	……

暴露面识别

发现工作流（流程）

漏洞情报	配置安全
数据泄露	提权利用
应用安全	社会工程
云安全	钓鱼攻击
配置安全	近源攻击
供应链攻击	……

攻击路径发现

运营能力优化（人员）

商业化软件漏洞挖掘	
WAF绕过技术研究	
网络攻击检测绕过	
云平台及服务攻击利用	
主机安全防御绕过	
虚拟化逃逸研究	……

发现能力强化

平台与资源支撑

数百个计算节点	数万个 精准指纹库	4600+黑产渠道
700+漏洞情报渠道	供应链挖掘渠道	多种DNS查询数据
移动应用发现平台	失陷账号监测平台	代码仓库泄漏分析
自动化渗透平台		

战术经验与人员储备

HW PoC库	0day漏洞库	云鼎实验室	玄武实验室
动静态数据	密钥数据特征库	虚拟化安全	行业研究团队
话术剧本库	云配置风险库	攻防情报联动	

企业创新在线学堂

基于大型互联网企业攻防实战能力沉淀

平台能力优势

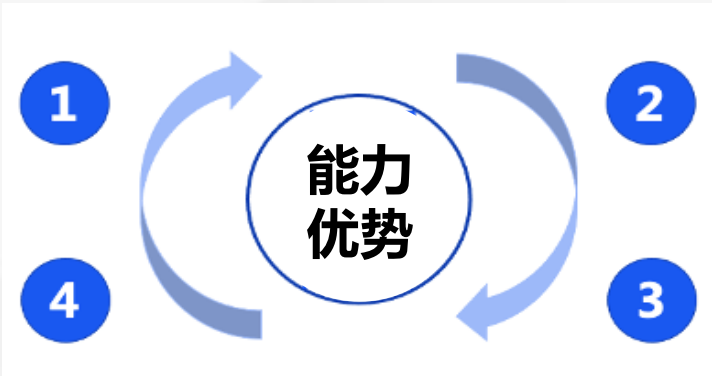
引入自动化工作流、整合腾讯T-VPT优先级算法、工具库及安全最佳实践，最高效率识别高优暴露面风险

基础引擎

- 灵活 **工作流引擎**
- 挖掘 **过程可编排**

通用功能

- 精准 **管理后台** 识别
- 深度 **目录爆破** 能力



运营能力

- 领先 **攻防对抗** 经验
- 高效 **风险验证** 平台

重点能力

- 广泛 **泄露监测网络**
- 独有 **云暴露面测绘**

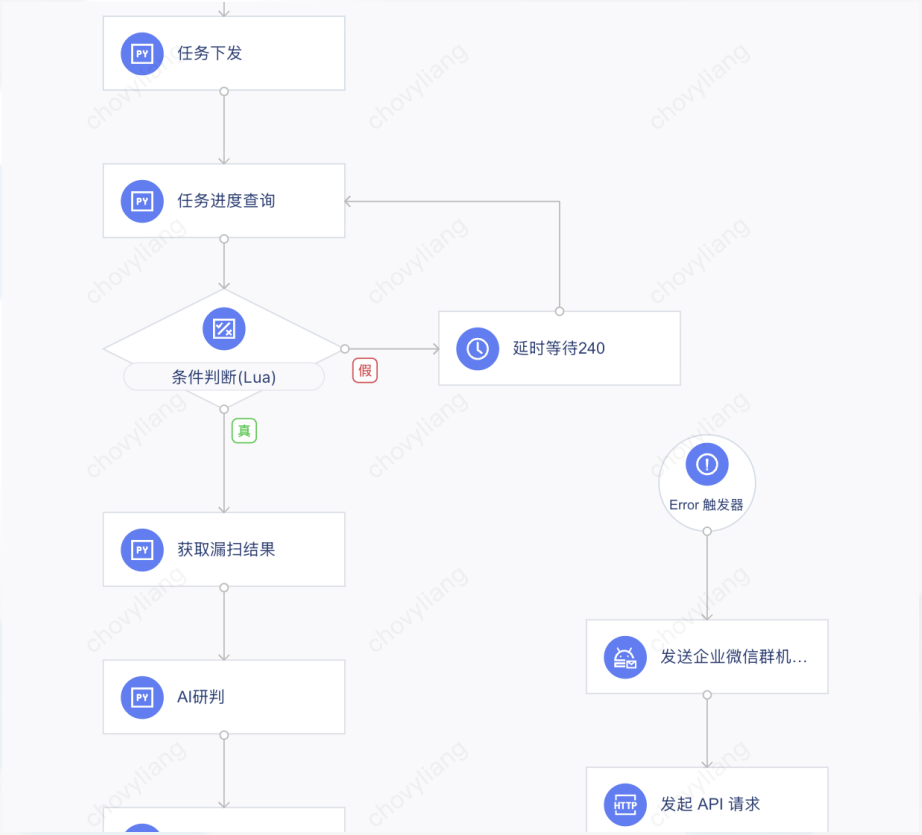
企业创新在线学堂

测绘工具自主运营，支持第三方工具集成

企业创新在线学堂

测绘工具自主运营，支持第三方工具集成

测绘流程 （可自主编排）



测绘结果 （ 清晰可看见）

功能亮点

1. 与企业现有安全产品或工具 **无缝融合**
2. 暴露面发现流程 **按需编排、更加灵活**
3. 基于自动化工作流构建，**过程可视可管理**
   - 清晰了解属于哪家子公司
   - 提供更多技术细节供分析
   - 为下发通报提供证据佐证

企业创新在线学堂

及时的资产变动感知+灵活的实施细节控制

自研 **资产变动监控** 能力

资产变动细节

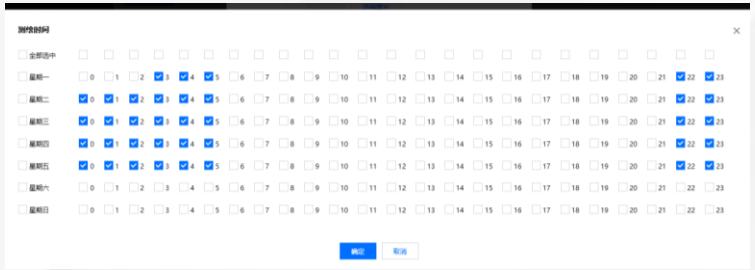
变更类型	变更情况	变更时间
指纹变动	新增Nginx指纹	2024-08-21 11:40:06
标题变动	-变为404 Not Found	2024-08-21 11:40:06

共 2 条　　10 条 / 页　　1 / 1 页

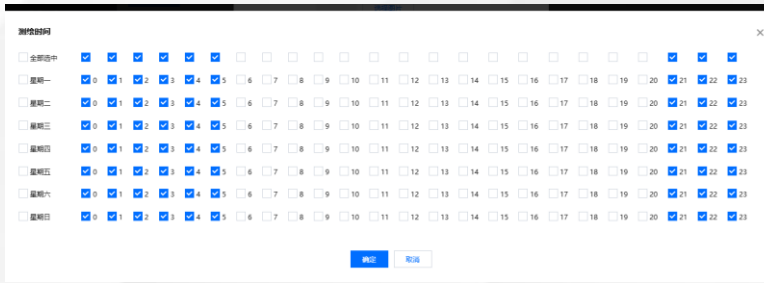
精细的扫描 **时间颗粒度控制**

精细的扫描时间颗粒度控制，满足各种客户个性化扫描需求

某智能硬件客户配置



某金融客户配置



功能亮点

- **资产变动监控**：持续监测业务变更，**动态捕捉**变更导致的**新增或遗漏风险**
- **精细扫描时间控制**：**满足客户复杂业务场景安全需求**，错开客户业务高峰期

企业创新在线学堂

精准的管理后台识别能力

精准的 管理后台识别 能力

抛弃传统误报漏报率高的正则识别方式，采用多种方式进行识别

功能亮点

- 场景丰富，基于金融、教育、交通、文旅、政务等多种业务场景实战
- 多识别方式，除正则外，含关键字库等方式

独有的 目录爆破分析 能力

- **目录暴露技术的困境**

目录爆破相关的开源技术都有 10 年，但 为何友商不全自动化集成?

—行业目录识别技术手段依靠状态码判断，存在大量误报导致无法运营

- **典型案例**

404状态码迷惑攻击队　　实际为数据泄露的未授权接口

- **腾讯自研目录爆破能力**

基于相似度识别算法，极大减少自定义404页面、伪200页面噪音干扰

功能亮点

- 低误报、低漏报
- 深层的敏感信息、影子资产识别

数据泄漏风险挖掘能力

引发数据泄露的“导火索”

数据泄露监测系统

账号泄露风险挖掘

功能亮点

- 监测**范围超过4000+黑产渠道**，其中付费、非公开渠道100+个
- 监控超过**200+勒索组织动态**，基于**资产自动关联**企业资产泄露风险

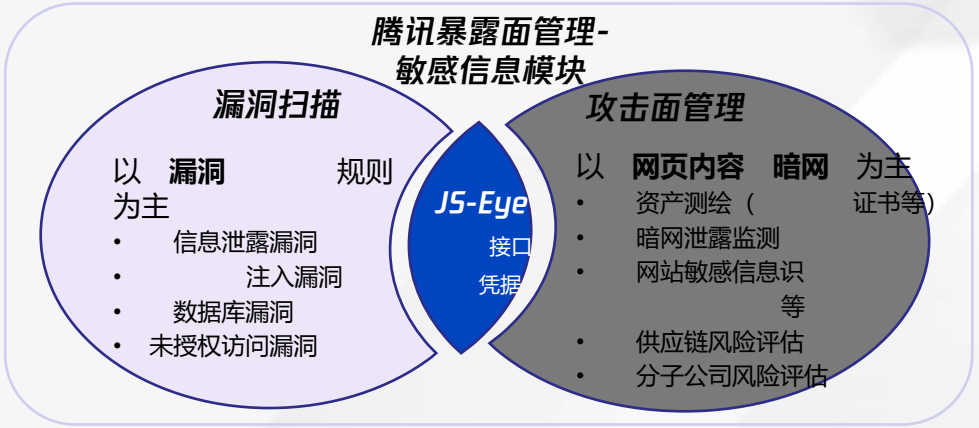
自研 JS 敏感信息检测/API发现能力

传统漏洞扫描等存在的不足

大量误报功能不可用，人工运营频繁漏报

腾讯暴露面管理“JS-Eye”模块

- 漏扫、ASM基础功能+ 网站动态脚本JS语法树解析
- 管理后台识别准确度达98%以上（远超主流友商）



功能亮点

- 深入**动态代码**层面
- 持续运营的 **JS 语法树解析库**
- **3000 +业务**管理后台积累

场景 ： 资产识别能力

传统扫描无法识别 接口，缺乏 识别能力

↓

JS API 特征规则库

场景 ： 敏感信息识别能力

漏扫无法识别业务敏感信息，或仅限于网页静态内容，未对 代码信息进行解析分析

↓ **JS 敏感信息特征规则库** ↓

用户名、密码

密钥

企业创新在线学堂

云暴露面风险管理能力

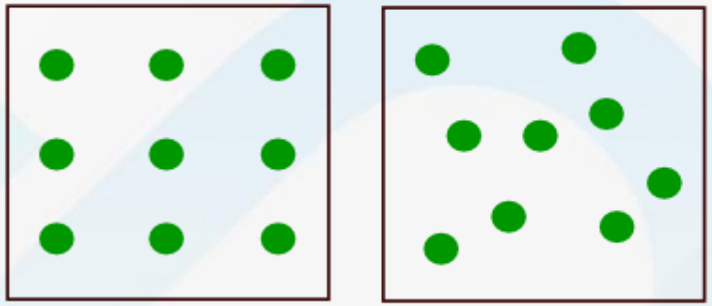
云暴露面发现难点

多云环境下，传统安全厂商缺乏云上安全运营实践，对云服务及产品特性了解不清晰，较难识别

场景 ： 段检测对云资产失效

传统 段扫描，可以很好识别 资产，但云资产 分配分散，无法通过 段扫描到

IP SCANNER

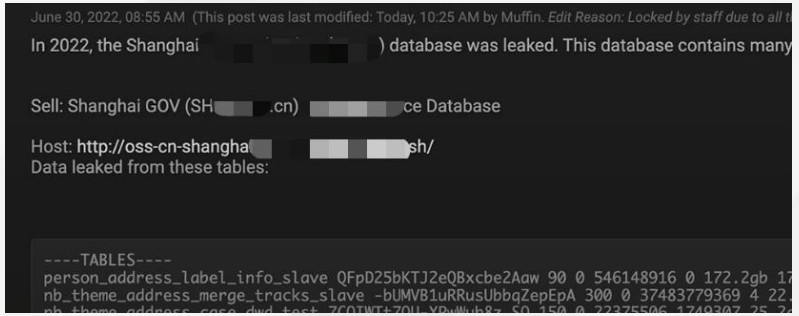


IDC Cloud

场景 ：云服务域名难扫描发现

云服务往往采用云厂商域名（ 网关、 、代码管理平台等），传统安全厂商依靠域名扫描，难以识别云暴露面风险

SERVICE DOMAIN

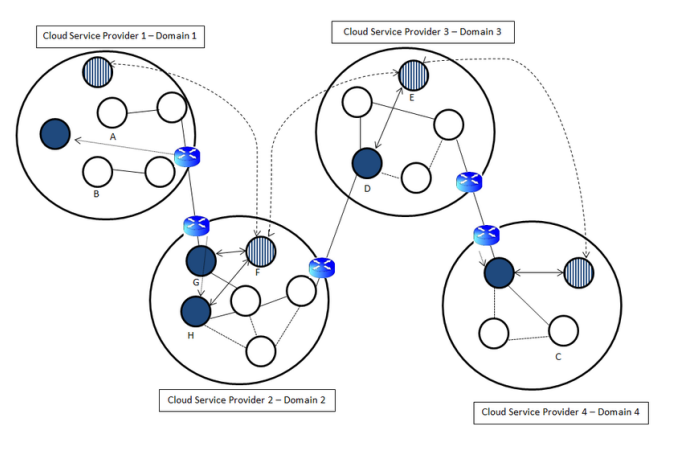


云厂商域名

场景 ：云访问控制暴露面识别较

云网络包含 网关、 、专线、负载均衡和 等复杂网络，没有外网 的云资产可能也会对外暴露

CLOUD NETWORK



云暴露面风险管理能力

云暴露面场景案例：阿里云　　（　　种）

多云环境下的安全风险，传统安全厂商较难识别

企业创新在线学堂

云暴露面风险管理能力

联动 多云安全治理平台 识别多云暴露路径

阿里云　　（　　种）阿里云数据库服务（10 种）

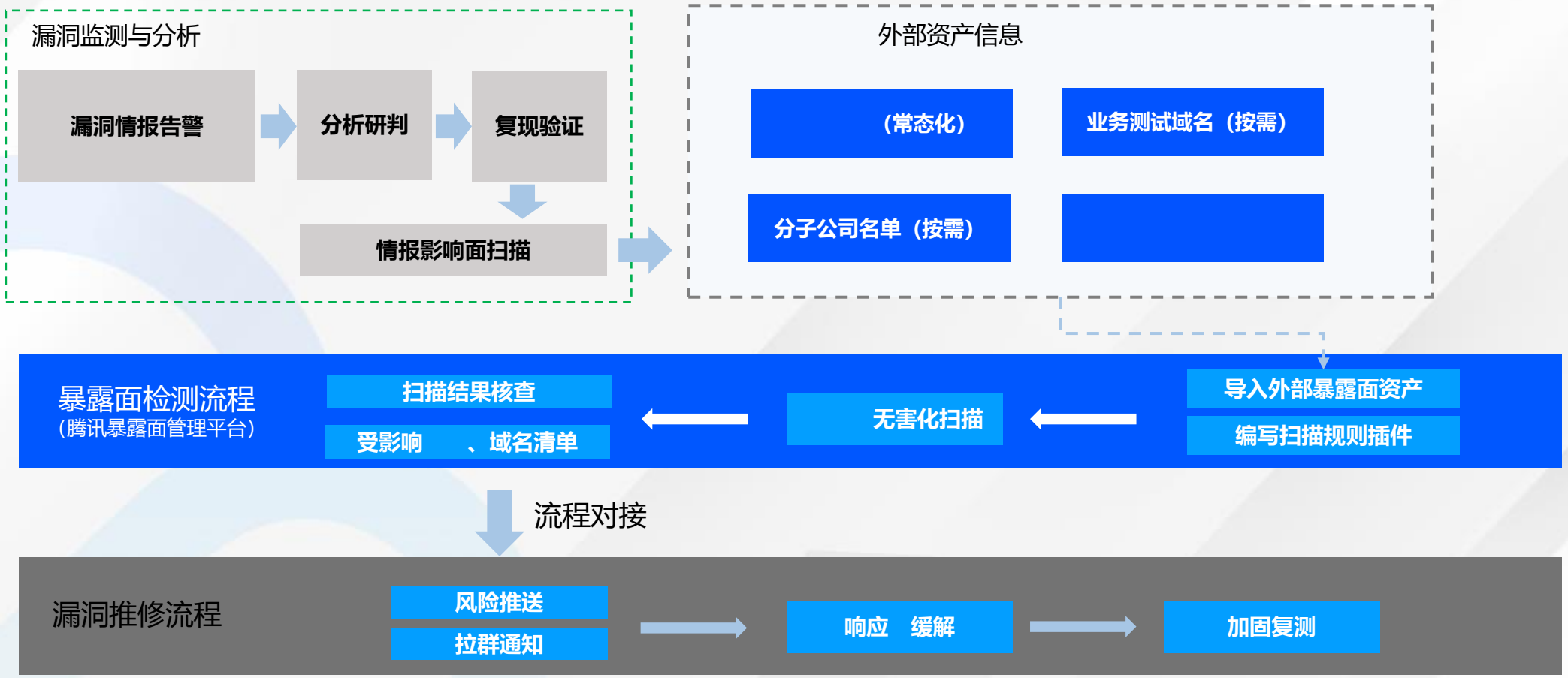
腾讯云CVM（53 种）　　……

功能亮点

- 源于多云安全治理经验，**基于云攻防矩阵ATT&CK，更全面**覆盖云暴露面
- 可识别**漏扫等无法识别的云服务资产、云API、云控制措施**等暴露面

企业创新在线学堂

腾讯漏洞情报 X 暴露面安全运营实践



企业创新在线学堂

支持的交付方式

服务报告

面向对象：所有客户

交付物：定期提供暴露面服务报告（每周/月）

运营场景：

1、日常运营场景，实时了解外部风险

2、重保或业务上线，了解自身暴露面

控制台权限

面向对象：公有云客户

交付物：暴露面管理控制台权限

运营场景：

1、公有云客户，想要了解自身暴露面

2、合规风险管理场景，需要大屏或者风险扫描措施

订阅式API

面向对象：所有客户，金融居多

交付物：提供暴露面数据接口文档、密钥

运营场景：

暴露面数据对接SOC或自身运营平台

腾讯云

企业创新在线学堂

感谢观看！

Thank you