



网络空间威胁对抗与防御技术研讨会
暨 第十一届安天网络安全冬训营

持续性API自动发现与风险防控

——基于API和应用视角推进执行体的治理

安天青竹智语实验室

执行体治理赋能与大模型辅助

北向守望



- 01 API安全背景
- 02 安天API风险监控实践
- 03 技术优势与用户价值
- 04 安天零配置安全工具APIRadar



网络空间威胁对抗与防御技术研讨会
暨 第十一届安天网络安全冬训营

北向守望

01

API安全背景

- 随着数字化转型的推进深入，API在移动APP，物联网，车联网，以及机器学习大模型中被广泛的应用。
- 统计数据显示，API请求已经占据所有互联网应用请求的83%。
- 针对API的攻击急剧增多，API安全受到广泛关注。

94%

Salt Security发现：94%的调查受访者在生产API中遇到了安全问题。48%的表示，API安全现在已成为高级管理层的讨论议题。

1061

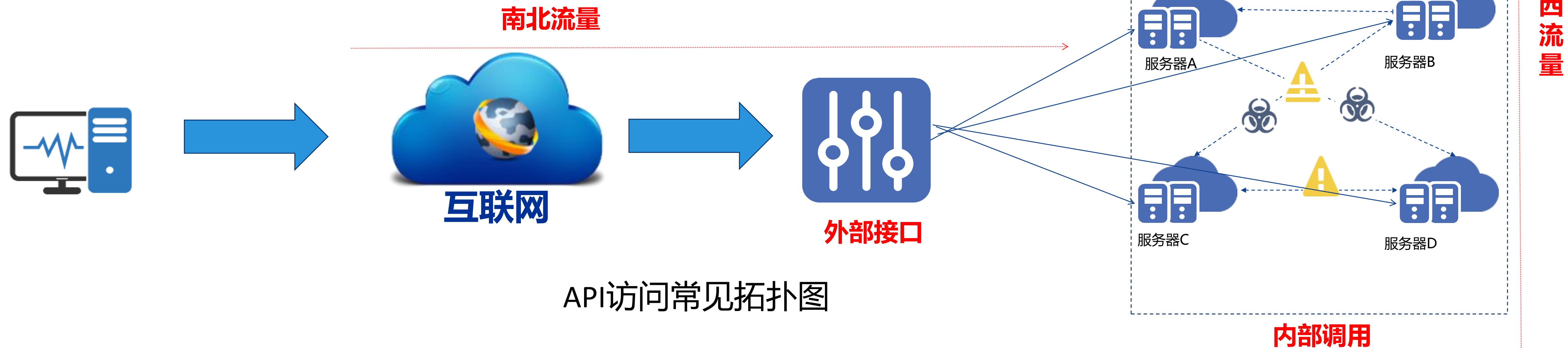
Akamai表示：随着组织继续朝着采用更多的Web应用程序来增强整体业务运营的方向发展，每个公司平均使用1061个应用程序，攻击面也在不断扩大。

681%

62%

Salt Labs发现恶意的API流量相比总体API流量增长了681%，而总体API流量增长了321%。可以理解的是，62%的调查受访者承认由于API安全问题而放慢了新应用程序的推出速度。

- API作为业务接口，对外提供外部公共接口，内部各个微服务之间，业务系统之间提供内部调用接口。
- API调用的后端是业务逻辑计算的应用环境，同时API作为网络接口也是数据的重要传输通道。
- 通过对外部接口的攻击，执行体经过南北流量进入系统。
- 通过攻击内部调用，经过东西流量，执行体完成内部的复制，提权等操作。



1 API资产不清

- 云，物联网，车联网等应用兴起，企业提供大量API应用服务。
- 小程序，微服务，oa系统，开源组件之间调用关系复杂，彼此之间接口不清晰，调用关系不明确。

2 API防护管控手段不足

- API属于WEB应用，但传统的WEB应用防护产品不理解用户业务逻辑，无法为用户提供有效的业务安全防护。攻击者利用API特点，绕过攻击特征，攻击用户业务，抢占大量的线上资源，盗取用户信息。
- API网关专注于流量分发，安全能力不足；基于提前配置，无法快速反应。

3 API基于上下文的追踪溯源困难

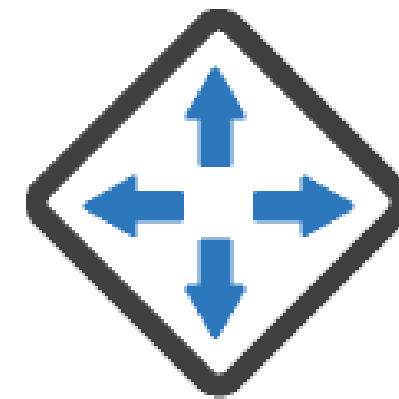
- 各种审计，风控系统通过收集业务系统日志，安全产品日志进行分析，缺乏应用和用户上下文，无法进行有效关联分析，追踪溯源困难。
- 日志系统数据有限，视角单一，无法发现深层次的业务问题。

4 API应用环境复杂度高

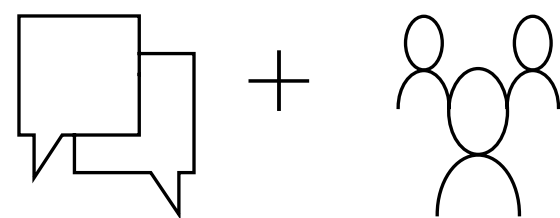
- 当前的API应用环境很多没有明显的网络边界，其广泛部署于内部，外部，多云环境，彼此调用关系复杂，分析防护难度大。
- API彼此之间加密通讯，分析困难。



Web应用防火墙 (WAF)：提供通用的Web安全防护；专注站点防护，站点入侵检测；缺乏针对API的防护功能。

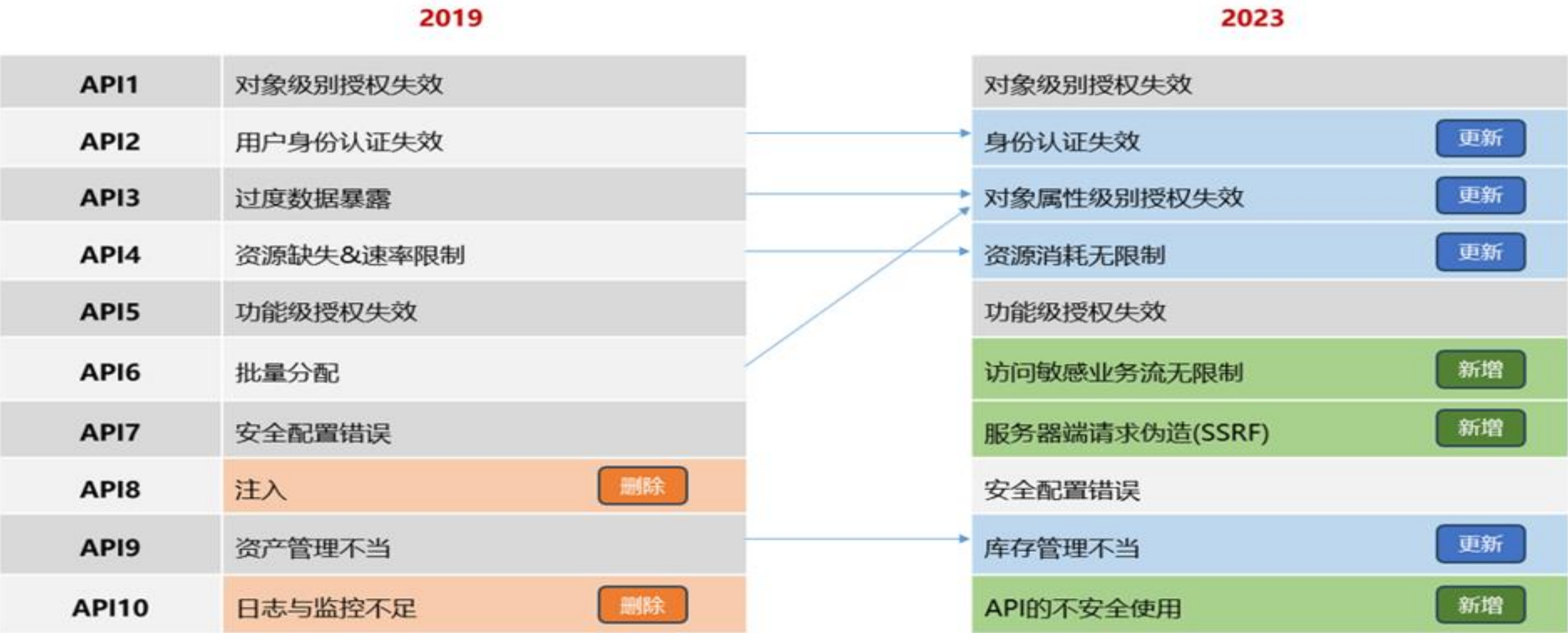


Web Application and API Protection (WAAP)：包含Web防护，DDos攻击防御，Bot检测和API防护；跟WAF一样，从**流量检测**出发，发现攻击和异常行为；缺乏对API资产业务的检测视角。



API安全防护：根据API特点，从**资产，业务和访问行为**出发，发现异常访问行为，保护资产和业务安全。

OWASP为强调API安全的重要性，在2019年首次提出了API Security Top 10。后随着安全产业实践加深，于2023年6月5日，又正式发布了2023年API Security Top 10。



OWASP API Security Top 10变更图



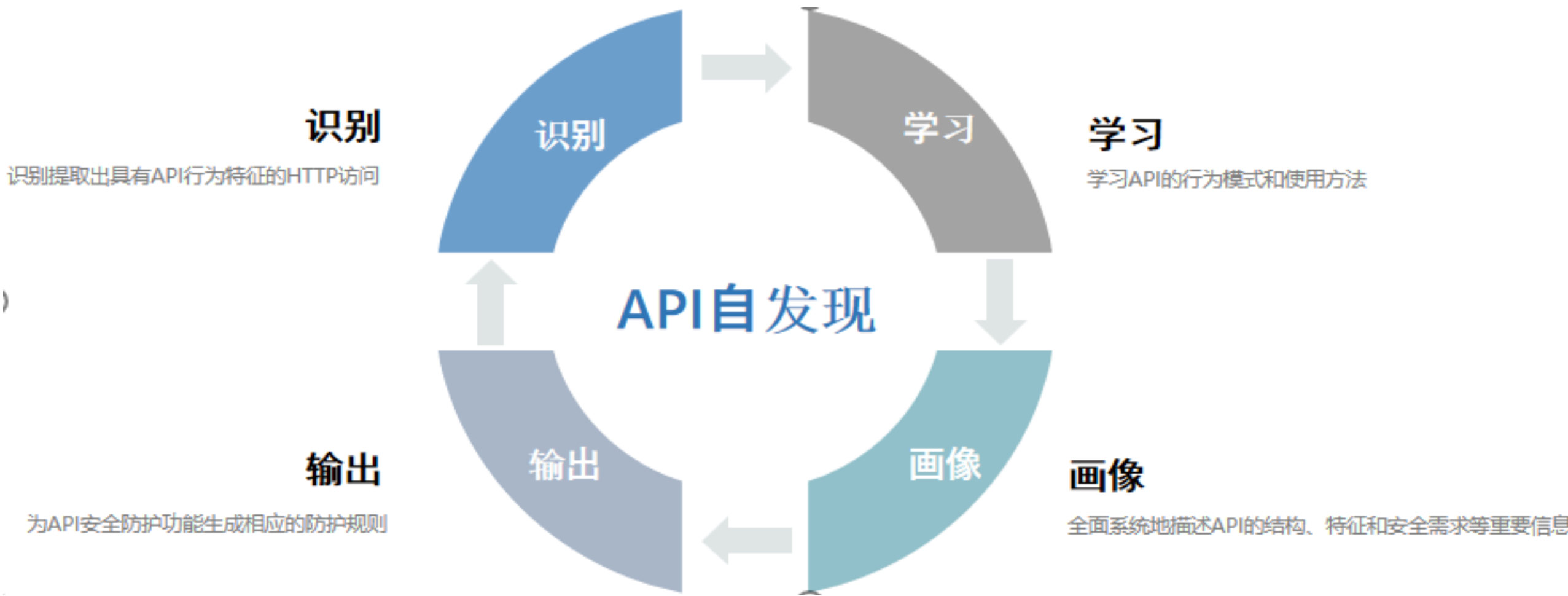
网络空间威胁对抗与防御技术研讨会
暨 第十一届安天网络安全冬训营

北向守望

02

安天API风险监控实践

- 通过自动识别，检测全网API资产，梳理API结构，简化部署复杂度。
- API、站点、业务三者相互关联，减轻运维复杂度，降低运维交互成本。
- 持续学习，自动发现，实时检测资产变化，跟踪资产生命周期



API数

36

API总数

API

36

活跃API数

0

废弃API数

0

复活API数

刷新

过滤器

重置过滤器

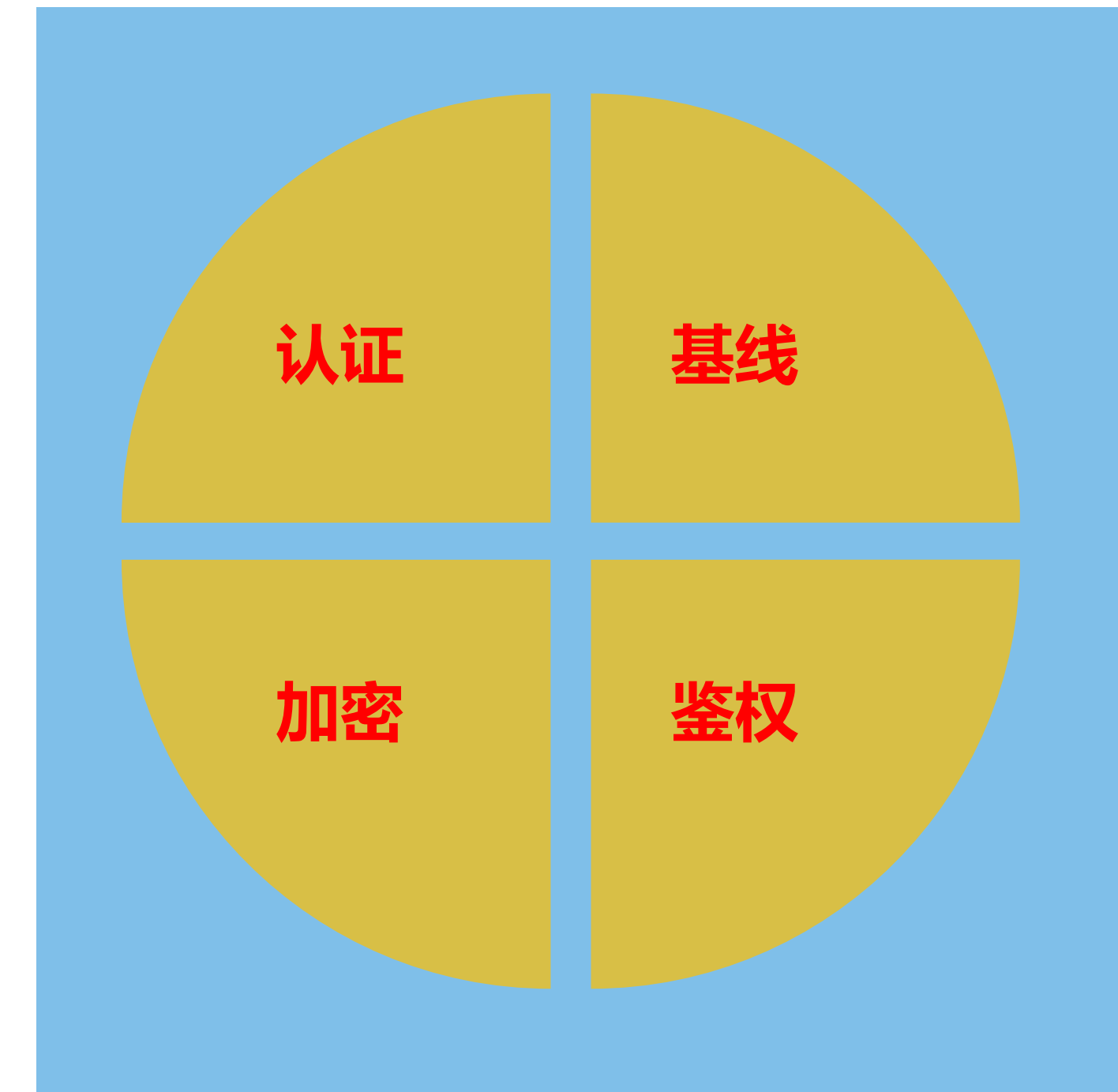
定制表头

操作

导出

	序号	Host	API路径	API方法	风险级别	可见范围	业务类型	数据标签	状态	活跃状态	OpenAPI规范	详细信息
☐	1	192.168.10...	/v1/config/l...	GET	中	内部	数据获取	无标签	有效	活跃		
☐	2	192.168.10...	/v1/config/i...	GET	中	内部	数据获取	无标签	有效	活跃		
☐	3	192.168.10...	/v1/config/c...	GET	中	内部	数据获取	无标签	有效	活跃		
☐	4	192.168.10...	/v1/config/r...	GET	中	内部	数据获取	用户名	有效	活跃		
☐	5	192.168.10...	/v1/config/l...	GET	中	内部	业务管理	密码 ...	有效	活跃		
☐	6	192.168.10...	/v1/system/...	GET	中	内部	登录	无标签	有效	活跃		
☐	7	192.168.10...	/v1/system/...	GET	中	内部	数据获取	无标签	有效	活跃		
☐	8	192.168.10...	/v1/system/...	GET	中	内部	数据获取	无标签	有效	活跃		
☐	9	192.168.10...	/v1/system/...	GET	中	内部	数据获取	无标签	有效	活跃		
☐	10	192.168.10...	/v1/system/...	GET	中	内部	数据获取	无标签	有效	活跃		
☐	11	192.168.10...	/v1/config/a...	GET	中	内部	业务管理	无标签	有效	活跃		

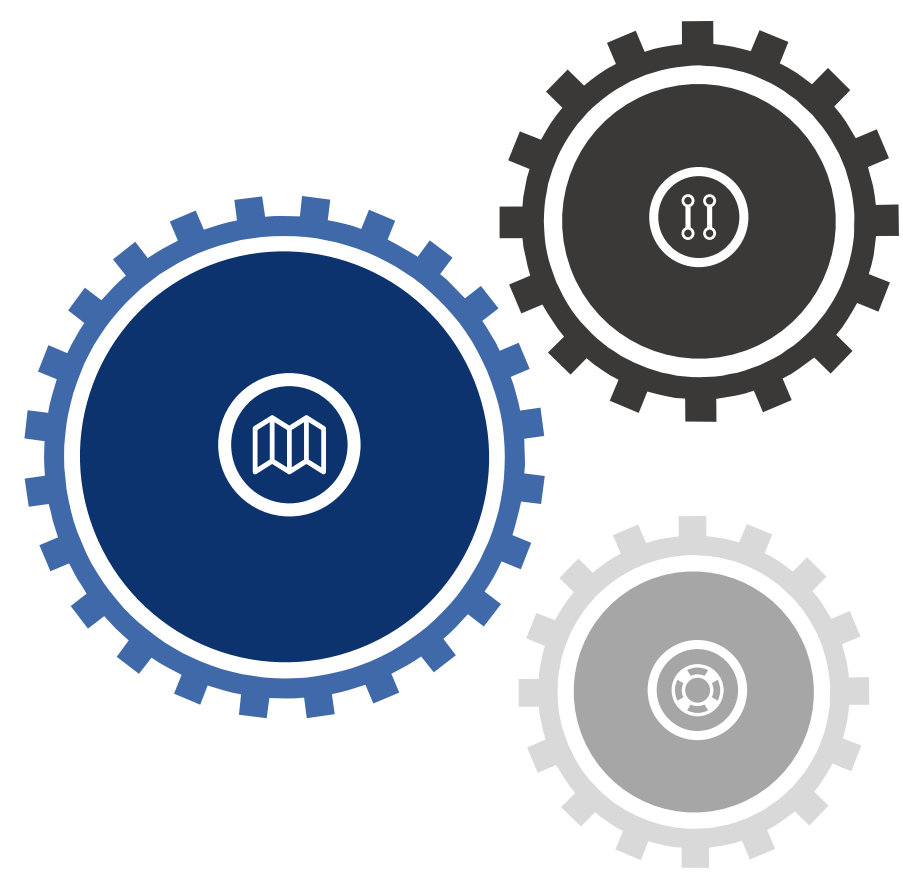
- 基于用户身份的API访问管控：能够有效防止未经授权或越权的API访问，并防范API的滥用行为。通过身份验证和授权机制，确保只有经过授权的用户可以访问API，保障API的安全性和合规性。
- 基于访问基线的管控：学习API访问频率基线，API关联访问基线等，基于学习基线，对API进行管控。
- API令牌管控：使用加密和重放保护技术，保证在API访问过程中的API认证令牌的安全性，防止对API令牌进行窃取或篡改，保障API访问过程的完整性和可信度。
- 实时权限状态管控：实时监控API用户的权限状态，及时感知API用户权限状态的异常变化，有效防范针对API的水平或垂直提权攻击。



基础防护

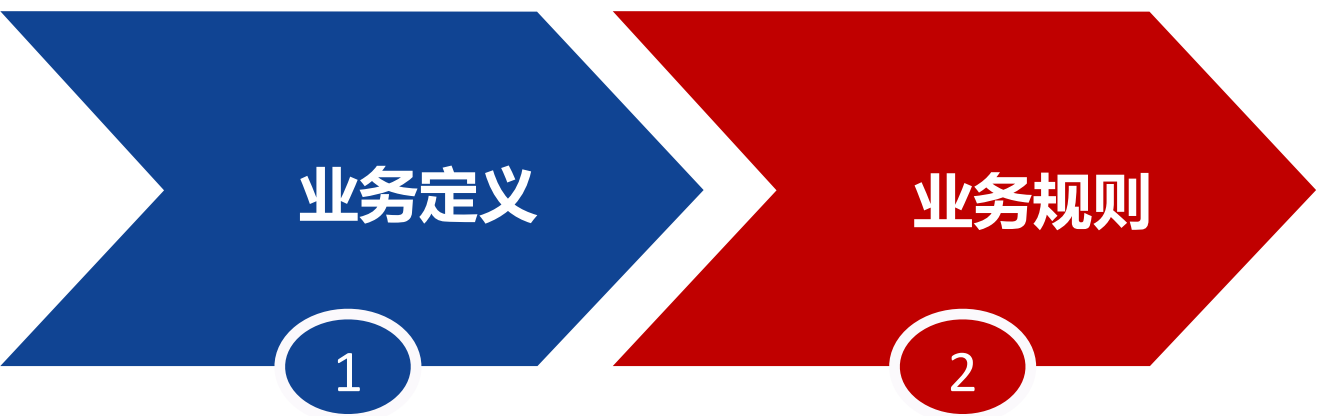


接口调用防护



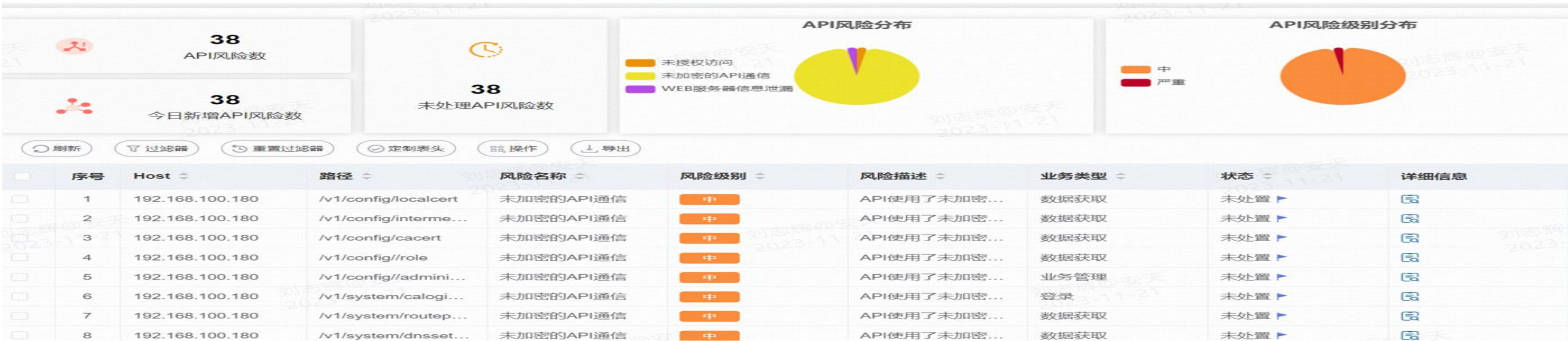
- DDoS防护、反自动化工具、JSON/XML数据规范、OpenAPI合规、API数据脱敏。
- API自发现和API风险评估组件紧密联动。

业务逻辑防护

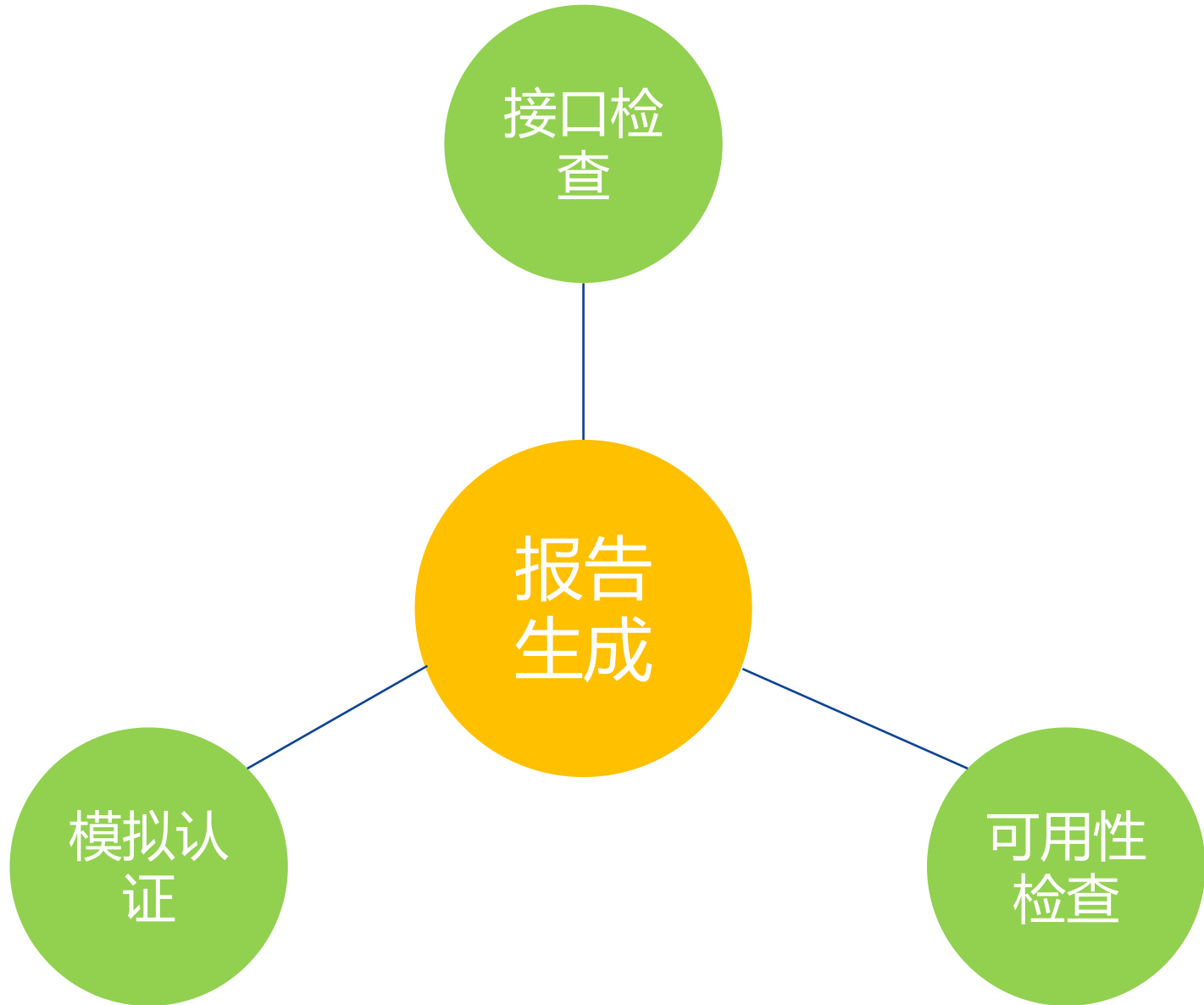


- 业务异常描述语言支持定义复杂的业务访问逻辑
- 基于IP和用户上下文安全的检测机制发现具有高隐蔽性的业务异常

- **API资产识别评估：** API类型、数据识别，API风险评估；
- **API资产关联：** 接口资产，站点资产与业务部门关联，落实资产到人；
- **业务访问威胁评估：** 内置威胁模型评估业务访问情况，标识异常访问行为；
- **建档分析：** 多维建档，分析业务，用户，来源交叉联系，追踪溯源，确认问题根源；



- API健康监测定期发送API请求来探测API的可用性，验证其连接和服务的可达性，确保API能够正常地接收和响应请求。当监测到API不可用时，监测系统会第一时间向管理员发出告警。
- 通过测量API请求的响应时间，评估API的性能和响应速度，分析统计API请求的平均延迟、最大延迟和最小延迟，生成相应的延时指标和报告。
- 通过跟踪每个API请求的状态码和错误信息，统计API调用的错误率，以评估API的稳定性和错误处理能力，及时发现异常错误率的API，并针对性地解决问题，以提高API的可靠性和稳定性。



第一章 摘要

最近一天分析结果中，共包含2个业务，其中认证失败的业务有1个,响应超时的业务有2个,异常响应的业务有0个。

业务总数	认证失败业务	响应超时业务	异常响应业务
2	1	2	0

表1 业务情况总览

1.1 认证失败业务统计

业务名称	URL	总数
monitor		7

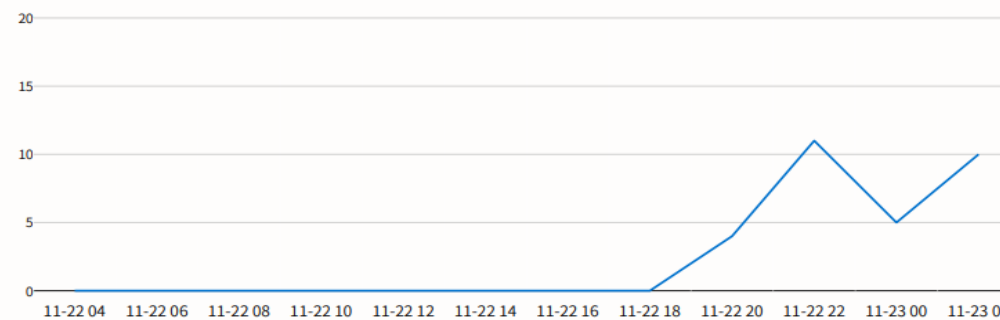
表2 认证失败业务统计

1.2 响应超时业务统计

业务名称	URL	总数
monitor		4
interface		24

表3 响应超时业务统计

2.1.1 响应时间趋势



2.2.2 响应结果占比

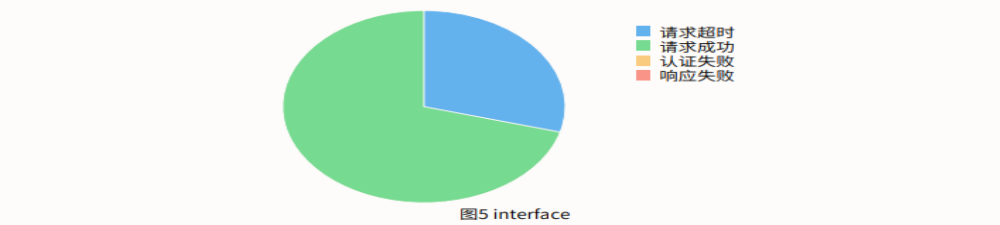
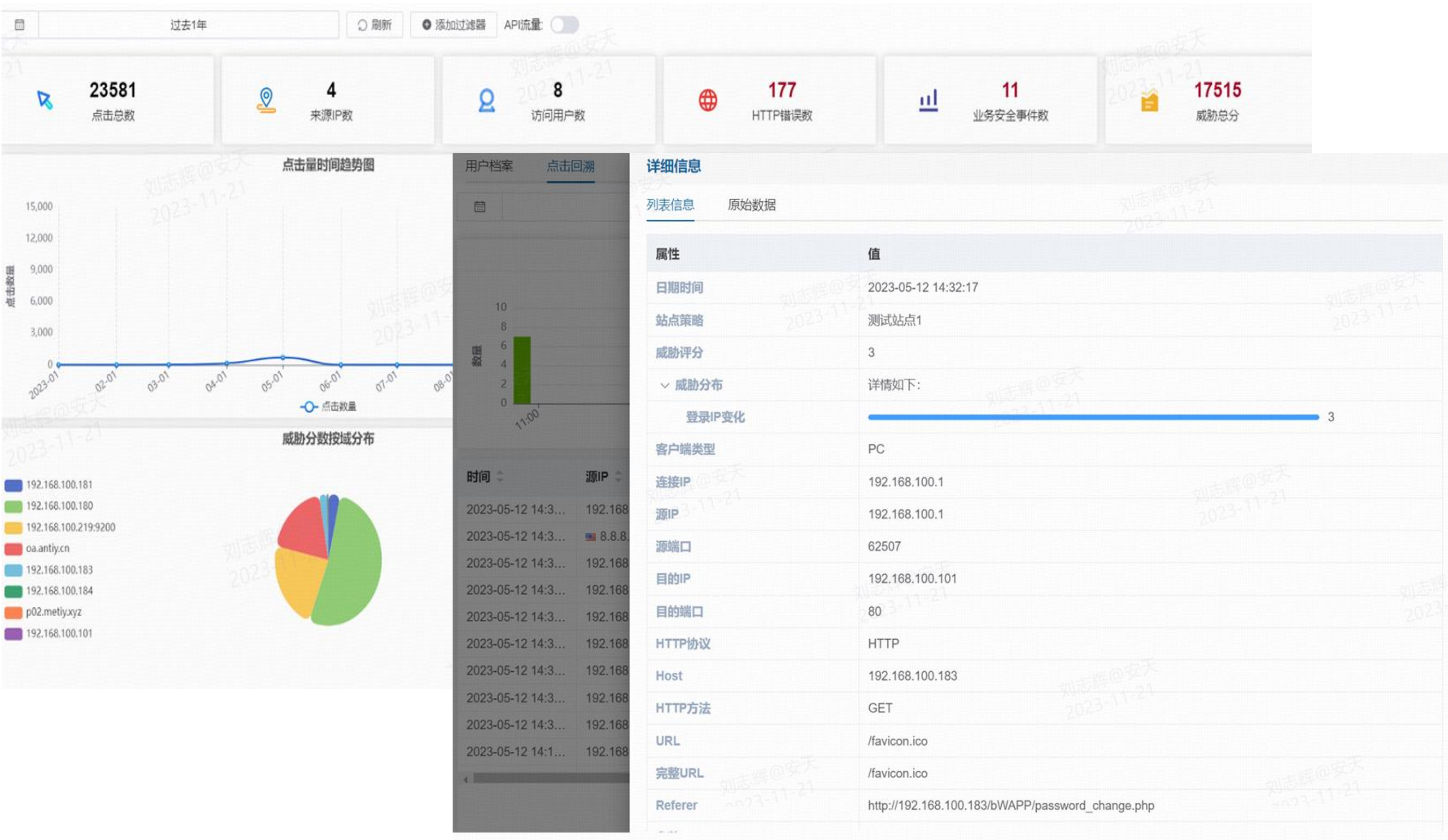


图5 interface

响应结果	总数
请求超时	24
请求成功	58
认证失败	0
响应失败	0

- 在API安全领域，API审计扮演着至关重要的角色。系统借助API识别技术，能够精确识别用户对API相关的操作，并结合API当前用户、威胁评分、客户端类型、API业务类别等API安全上下文信息，详细记录API的访问情况。
- 系统进行多维度建档，可以便捷地进行API安全事件的纵深调查和横向分析；从来源客户端、用户、API威胁等多个维度展开对API安全事件的调查，深入了解API安全事件起因和结果。





网络空间威胁对抗与防御技术研讨会
暨 第十一届安天网络安全冬训营

北向守望

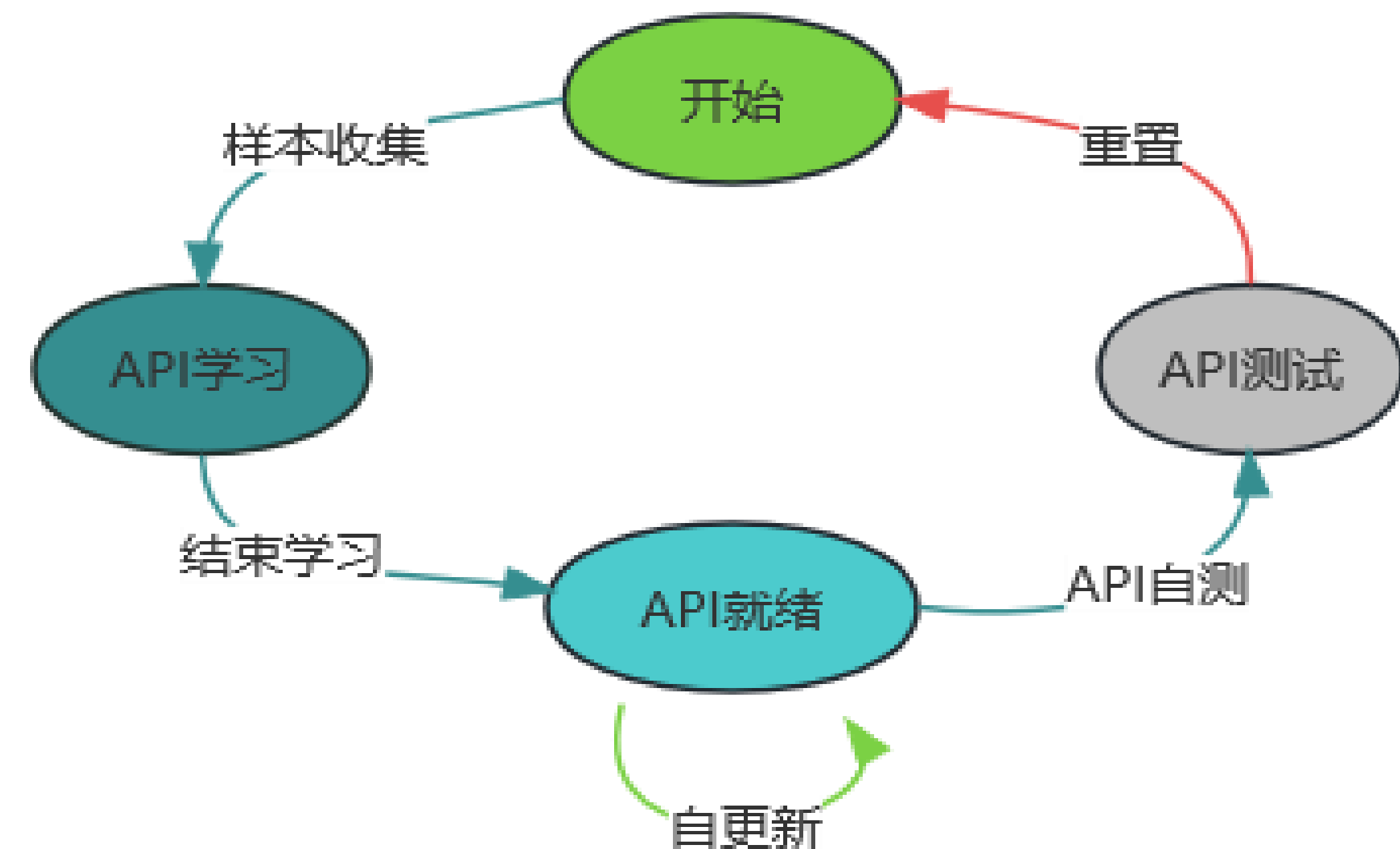
03

技术优势与用户价值

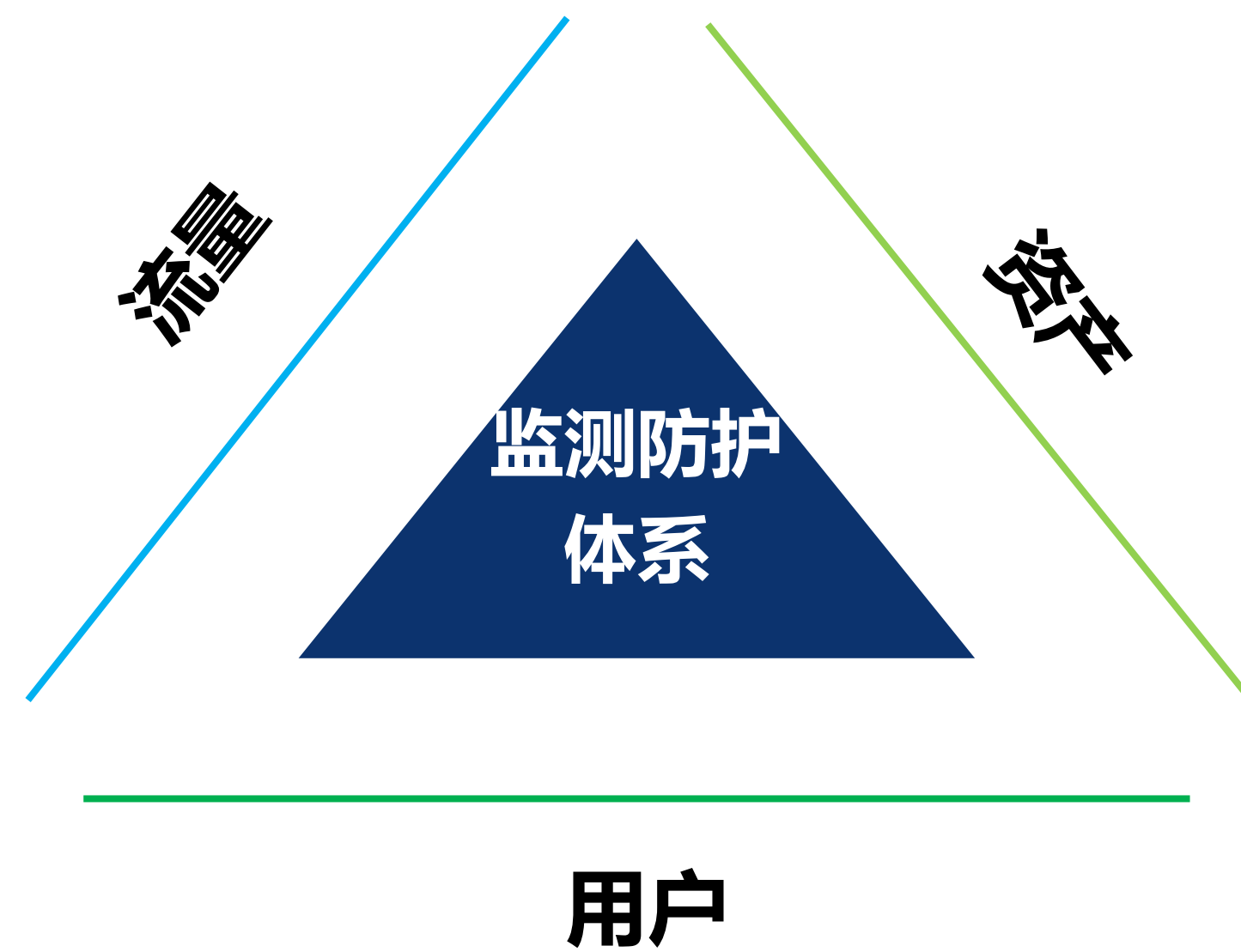
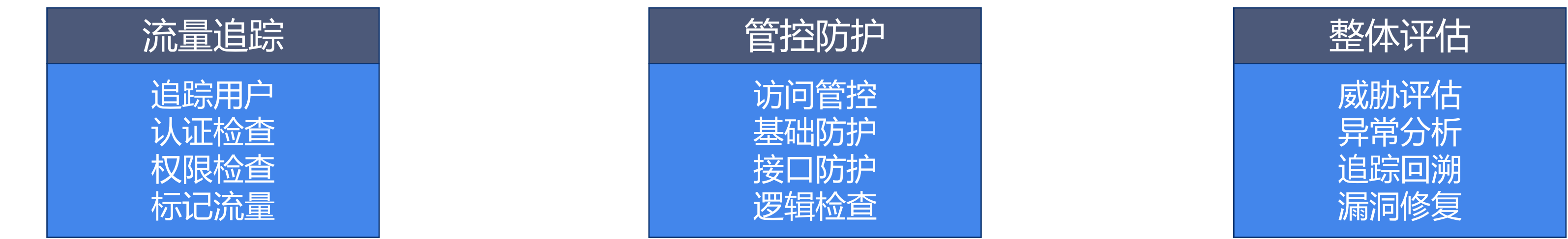
用户API并不是一成不变的，需要持续学习，感知API变化

动态评估API变化，决定是否需要进行合并更新

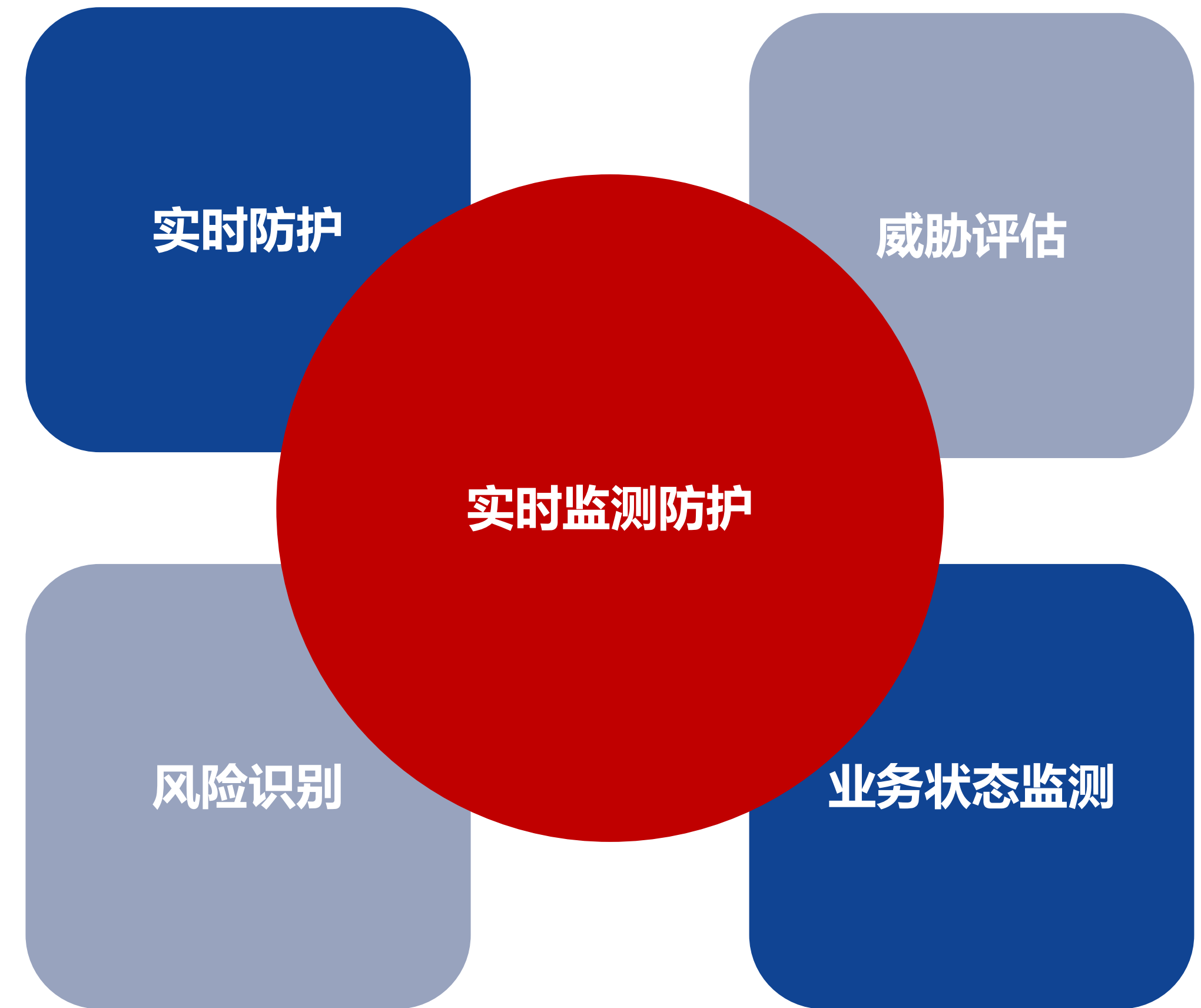
对API进行实时测试，当发现大量不同源的用户出现匹配异常时则重置API



- 数据接入，系统认证过程分析；分析接入流量，对用户进行追踪，监测提权，认证风险；
- 标记流量，为管控、防护、溯源提供基础支撑；
- WEB基础防护评估接口内部是否存在注入等常规风险；
- API接口防护，业务自定义监测业务逻辑漏洞，数据泄漏和业务滥用风险；
- 对整体业务使用情况进行威胁评估，发现异常行为，快速定位；
- 修复漏洞，减少业务损失；



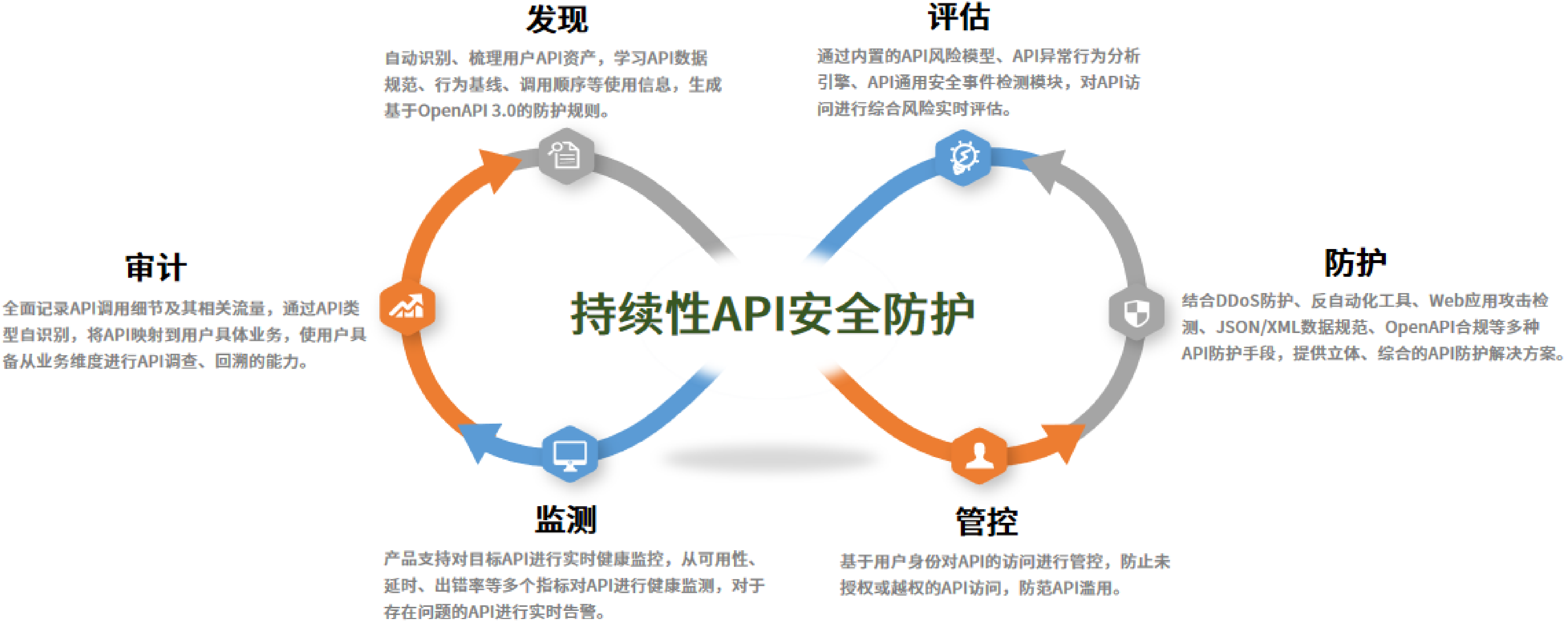
- 流量监测自动识别API资产，零配置方便部署；
- 在线部署，有效解决多云，微服务等加密流量的流量识别；
- 资产识别、评估与在线实时防护联动，发现问题及时拦截，保障资产安全访问；
- 在线防护结果辅助识别威胁评估过程，优化识别结果，提高评估准确率；
- 威胁评估结果反馈实时防护策略，提高防护效果；
- 在线服务检测，保证业务稳定运行；



随时了解业务访问情况；多维度展现业务威胁、还原事件过程



- ✓基于风险的展示方式使得用户专注关键业务事件。
- ✓用户，业务，访问来源三者关联分析，掌握业务运行状况，发现用户非法行为和业务隐藏问题。
- ✓回溯用户行为，还原整个攻击过程，发现攻击第一现场。





网络空间威胁对抗与防御技术研讨会
暨 第十一届安天网络安全冬训营

北向守望

04

安天零配置安全工具API Radar

- **资产不清**：对外和内部之间多种服务，彼此提供接口不清。
- **生命周期混乱**：服务接口版本更新不规范，新旧接口管理混乱，存在安全隐患。
- **接口不规范**：多种服务，由多个团队开发，接口规范不清晰，存在被攻击风险。
- **风险未知**：业务存在未知风险，没有有效监测评估。

数字资产

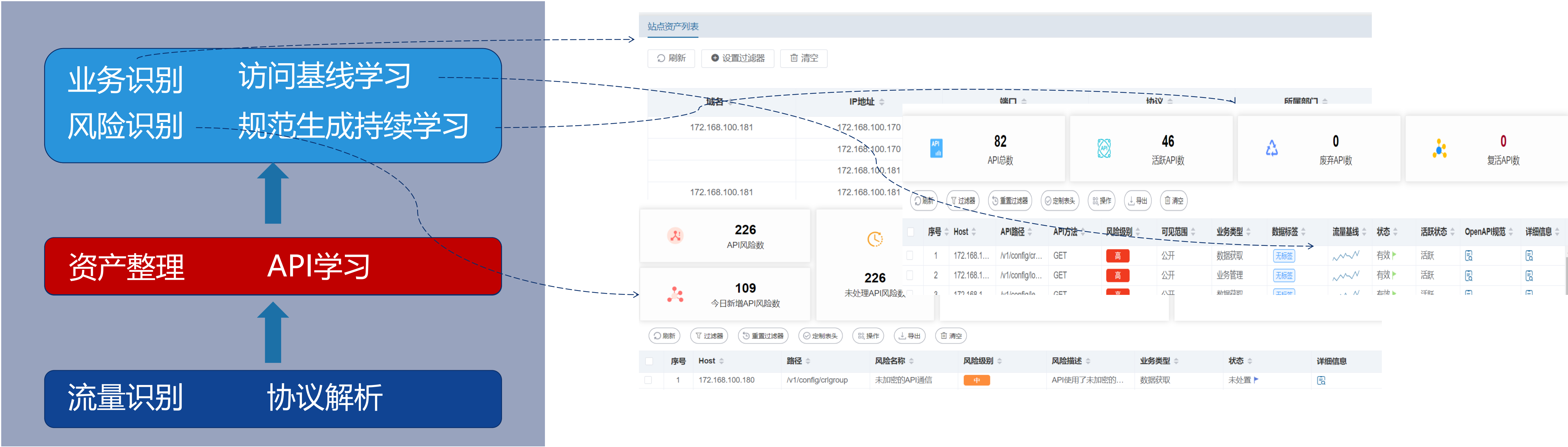
资产数字化：自动识别站点、API资产；帮助客户梳理业务资产，控制资产暴露面；学习资产使用情况，优化管理资产生命周期。

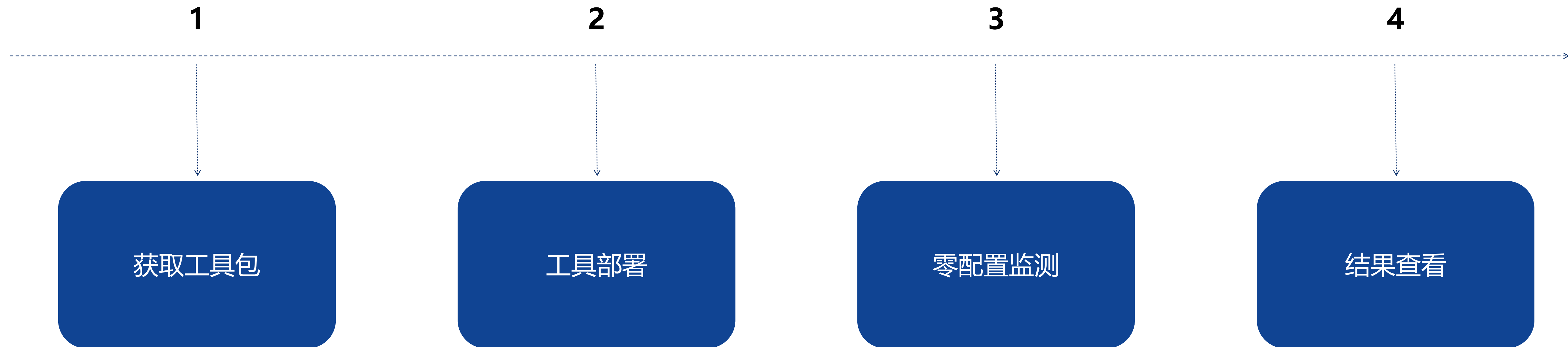
标准接口

资产标准化：API资产深度识别，帮助用户形成OpenAPI标准，防止接口滥用。

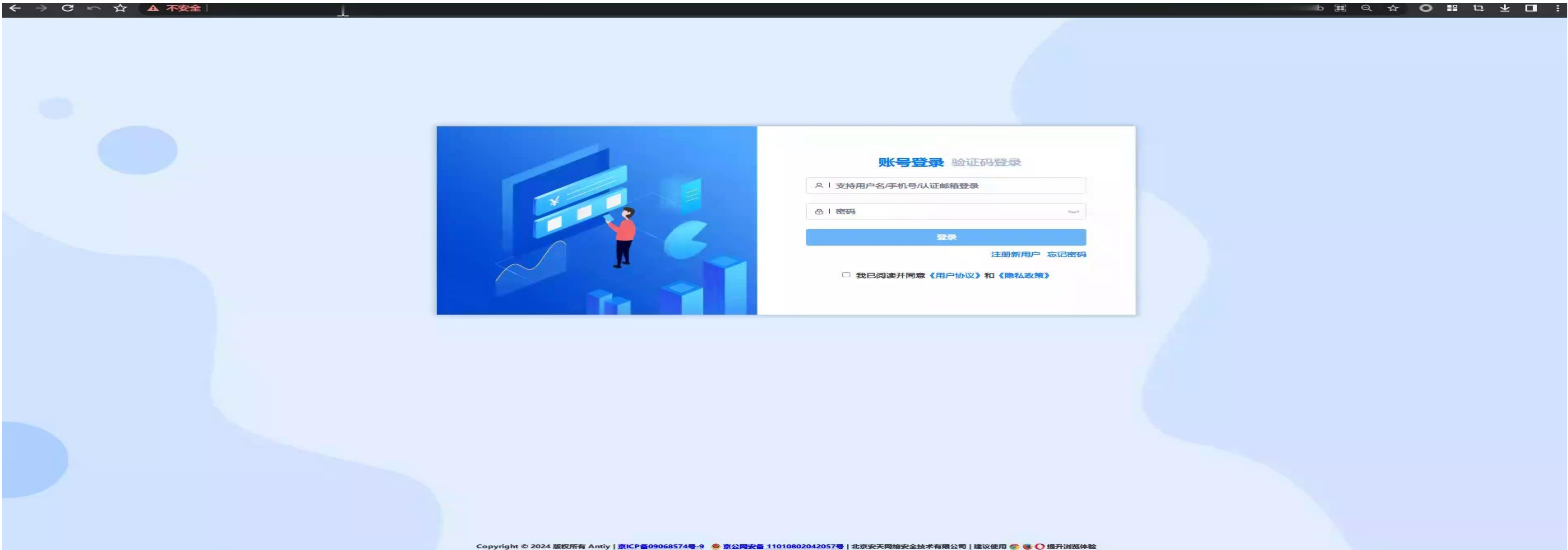
风险预知

风险可视化：内置几十种风险模型，自动识别API风险，帮助客户发现安全隐患，及时修复。





资源索取、技术支持请您联系：apisec@antiy.cn





网络空间威胁对抗与防御技术研讨会
暨 第十一届安天网络安全冬训营

欢迎联系使用API Radar



安天冬训营 wtc.antiy.cn

执行体治理赋能与大模型辅助

北向守望