网络空间威胁对抗防御技术研讨会
暨 第十届安天网络安全冬训营

执行体全量识别与精细管控

基于HTTP元素和访问上下文的WEB应用管控

安天下一代WAF应用管控实践

安天 | 青竹智语实验室

目 录

01 WEB应用访问特点

WEB应用访问特点

WEB应用的整体性

- 访问来源
- 访问资源
- 访问协议
- 访问方式
- 传输内容

WEB应用业务逻辑性

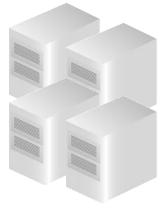
- 访问用户
- 访问路径
- 访问过程
- 权限管理

整体结构性管控

基于HTTP元素的管控

来源管控

方式和内容管控



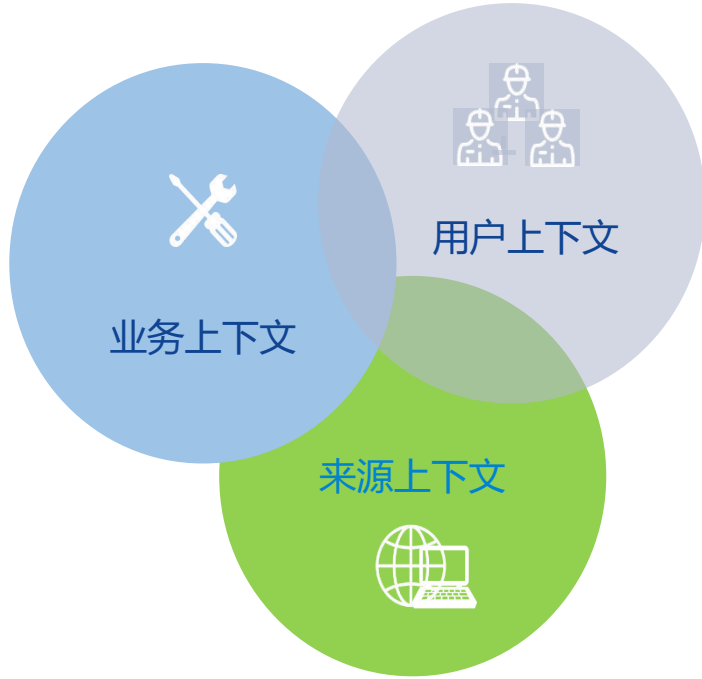
访问对象管控

- 对攻击者进行识别，拦截。
- 对访问资源服务进行防护。
- 对访问方式方法进行识别管控，访问的内容负载进行检测，攻击拦截。

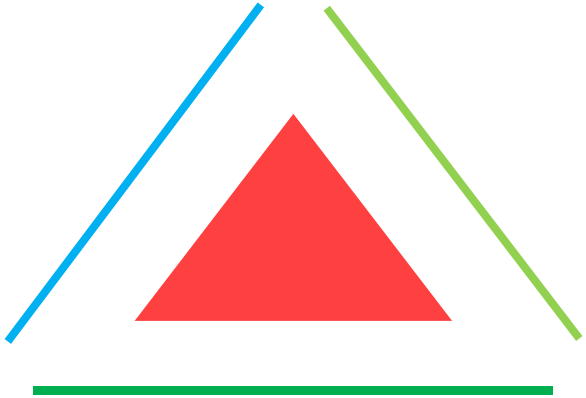
业务逻辑性管控

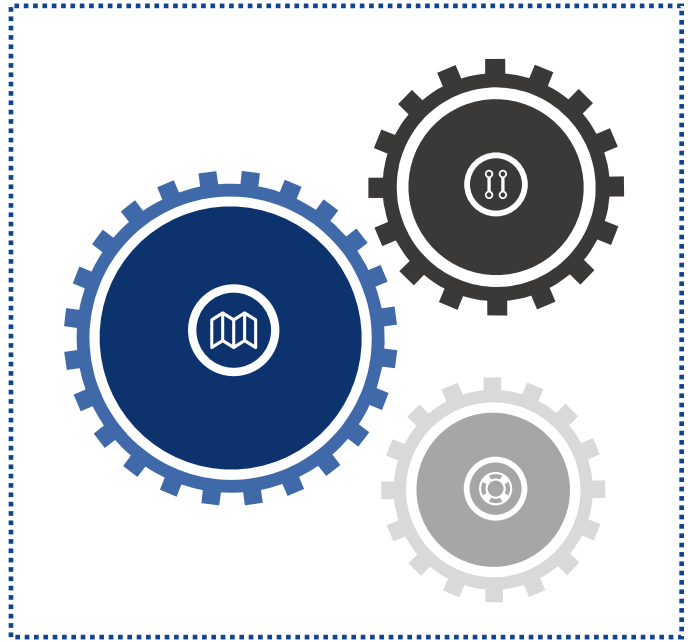
基于访问上下文的管控

- 从业务，用户，来源多个角度进行上下文分析。
- 不同角度间关联分析，发现深层次的异常行为和业务逻辑漏洞。



安天下一代WAF管控体系





基于HTTP元素的整体管控

基于访问上下文的逻辑管控

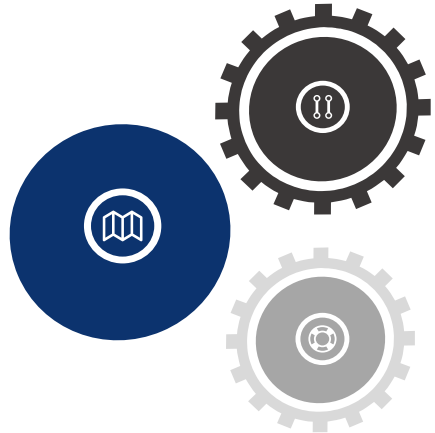
02 基于HTTP元素的管控

来源管控

访问控制和机器人检测相结合

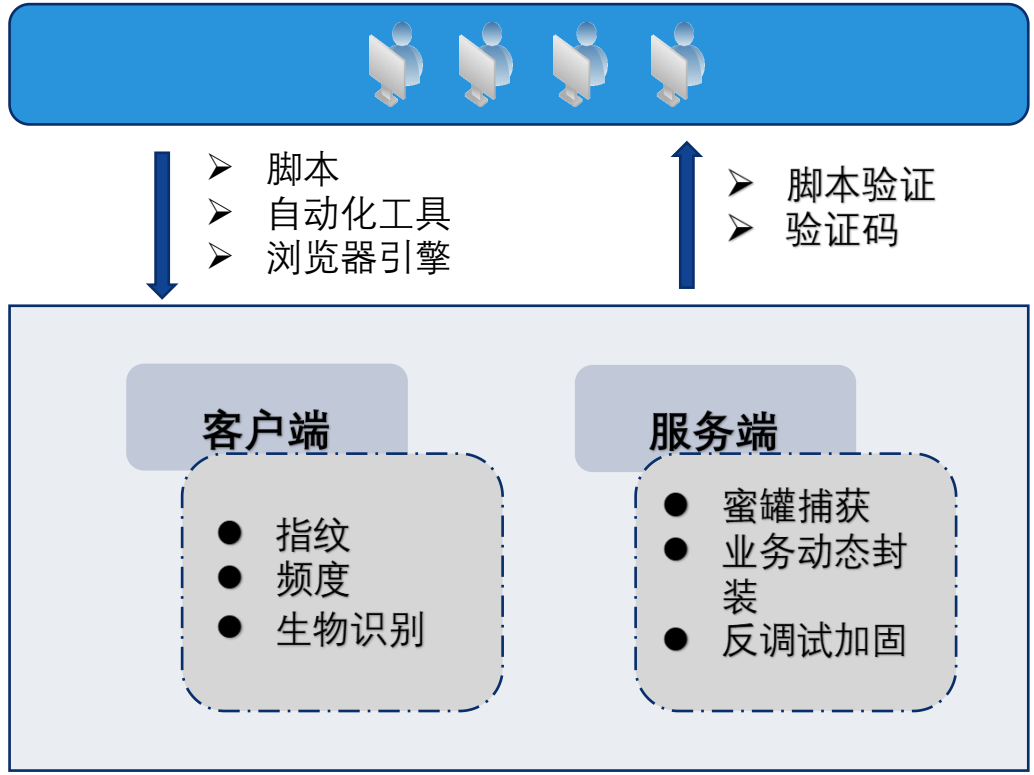
访问控制 → 机器人识别

- IP访问控制
- GEO访问控制
- 访问速率控制
- 访问连接数目控制



机器人防御

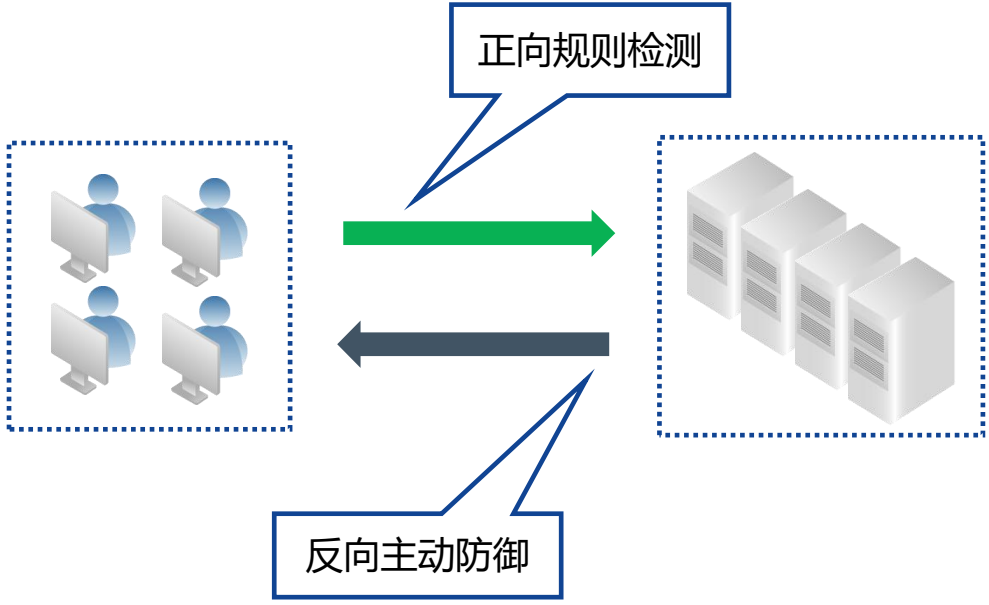
- 对机器人访问进行识别。
  - 在客户端通过指纹，生物识别对客户端进行人机识别。
  - 在服务端，加入诱饵，进行蜜罐捕获，通过业务动态封装和反调试加固阻止自动化工具的自动分析。
- 对检测结果，通过二次验证手段解决消除误报带来的影响。



资产管控

- 域名访问控制
- URL访问控制
- 参数控制
- 协议控制
- 非法内容过滤
- 网页防篡改

- 资产混淆加密：通过混淆加密，隐藏业务关键信息，防止攻击的重放行为。
- 安全加固：通过开启安全相关属性，对客户端安全进行加固，加强用户安全设置。



资产管控场景

/ticket?from=<city-name>&to=<city-name>

- 重复查询票务信息，获取票价变化
- 订单抢占，造成资源浪费。

/ enterprise-credit?name=<object-name>

- 遍历企业名称重复获取信用信息
- 信息倒卖，谋取利益

- 关键业务混淆
- 资产重放防护

nsmd="/@$@$YhwBEwGwewEanwlsn_WTSxPAPzeTrwRKA2aZd07LDkEwHdUxRj11BPL9SwNe0ZxpcwX-UDWgYclAoWBVA7Qb4kHEVdAi5KChFoVrY_I0bBa9VXU88erGiI"

/@$@$Yw0QExChagErUNNtOH1FJLZJdmDd_jJQQewh1IjNBNzFQstuswL3IM49W2hfWmLQ_44o3StgJSC-1IhXHPmVbxCmCzf93w0-xXgfxBTCHFvMrL1Ih3U4mo?xdxEdAe=<object-name>

/document?id=1526820085226

- 对id参数进行猜测，重复获取信息

- 隐藏资产信息
- 保护数据安全

@$@$YxwAExChexEqfpvykREtsT-zWQGS9w0yfXffbn6r49TOViBV-8q00cJj_Of8G4AGDQvYTX4DcWIAINc9kTiR3nqb75g__cVEa-k6nWgxxExyWlBgDdjE94

访问内容与方法管控

规则识别与词法语法分析结合

- 攻击特征识别
- CSRF防护
- 盗链防护
- 文件上传检测

- 攻击特征检测多个级别，多种响应方式，适应各种应用环境。

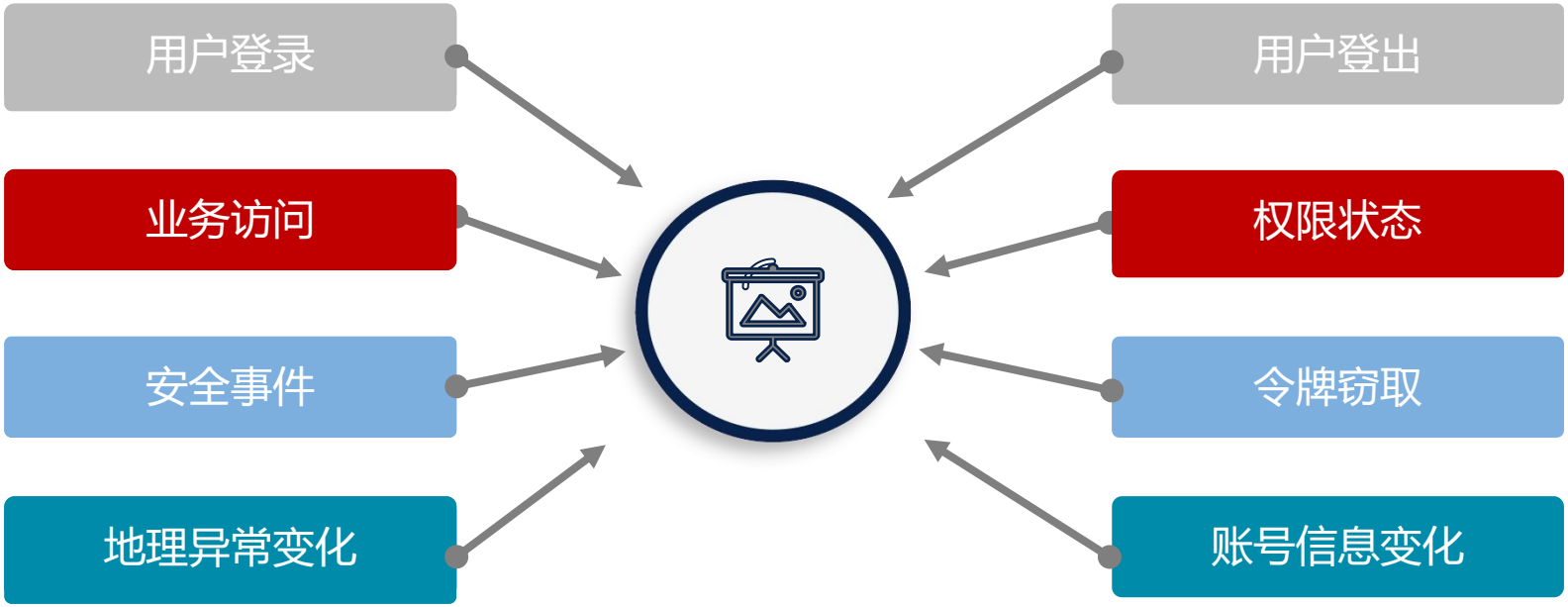
攻击类型	告警动作	阻断时间
SQL注入防护	阻断	
XSS 防护	告警	
已知漏洞防护	静默阻断	
应用注入防护	重定向	
WEB后门防护	长期阻断	— 180 + 秒

- 词法语法分析：语义分析通过对用户的输入进行词法分析和语法分析，构建语法树，有效的检测出真实有效的恶意攻击。提升检测准确率，缓解大量误报造成的影响。从而对危害行为进行快速有效响应。

- 词法语法分析减少误报，增强告警有效性。

03 基于应用上下文的管控

基于用户上下文的管控



- 跟踪用户访问的整个过程
- 监控账号安全相关状态

- 将业务访问与用户身份相互映射
- 快速定位安全事件关联的业务用户

基于业务上下文的管控

业务梳理

- 通过自学习，点击流记录，识别系统提供的业务服务。
- 统计业务使用情况，发现业务访问异常。
- 发现僵尸业务，后门服务。

业务定义

- 对关键业务进行定义。
- 提供通用模板和脚本，提高初始配置简便性，同时满足高级用户操作灵活性。

访问逻辑规则

- 根据业务定义，指定业务访问逻辑规则，进行访问逻辑管控。
- 对关键业务和推广业务进行严格检查，防止业务漏洞被利用。

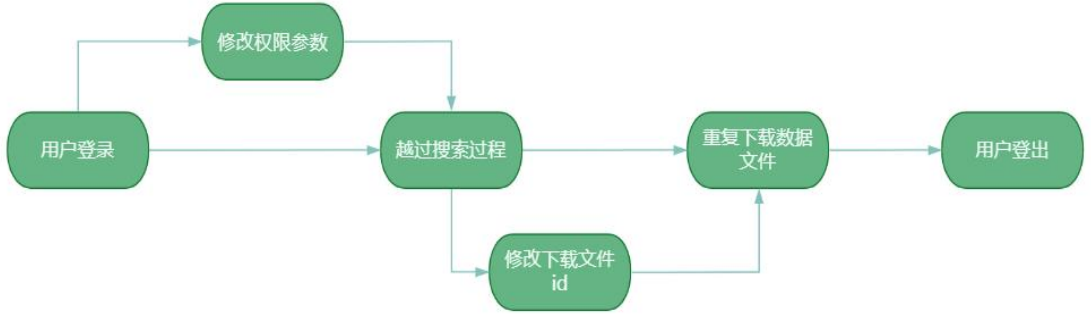
基于来源上下文的管控

- 单IP多次账号尝试登录检测暴力破解。
- IP多账号访问发现撞库行为。
- 账号多IP登录发现账号违规共享行为。
- 账号源IP变化，地理位置变化检测账号盗取行为。

上下文分析应用场景

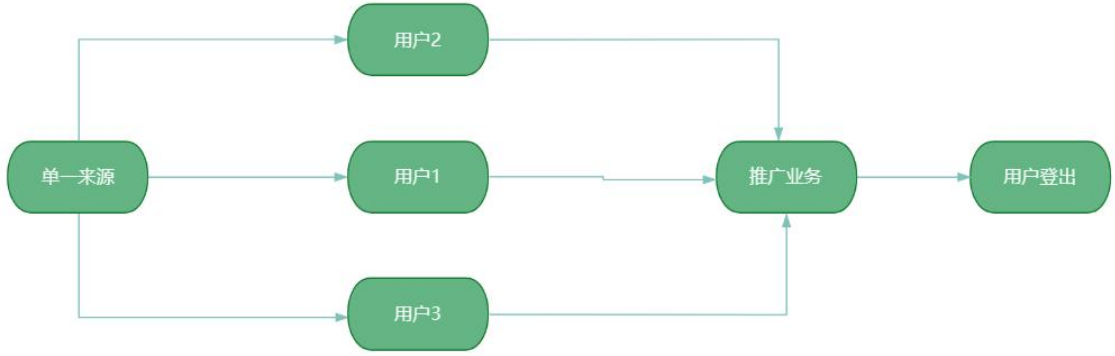
数据泄漏场景

- 通过业务逻辑上下文发现业务访问异常。
- 通过用户跟踪，发现数据重复下载。
- 通过权限id变化发现权限异常。



虚假账号资源抢占场景

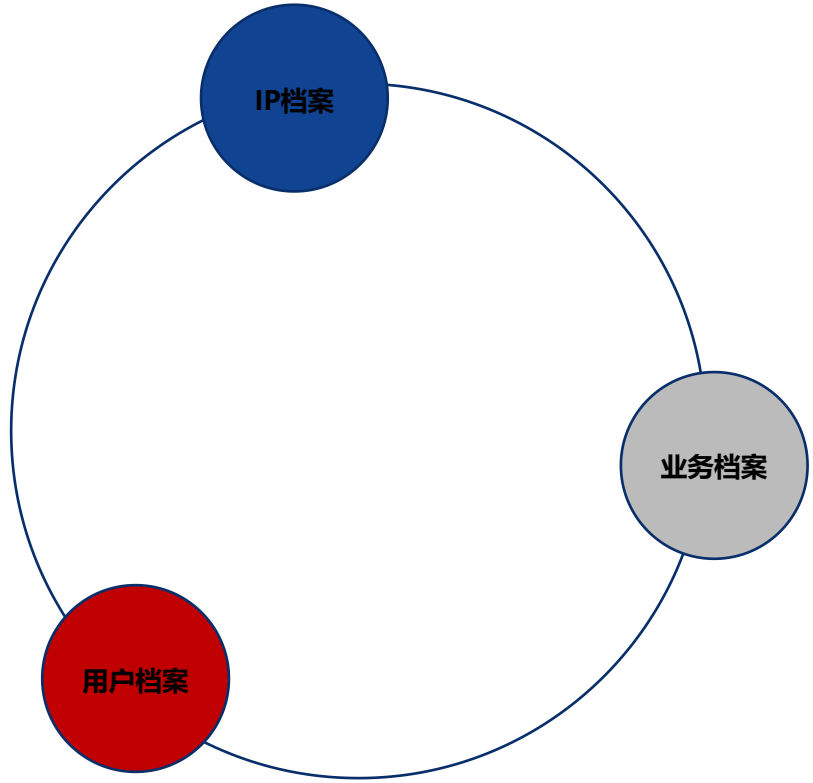
- 通过来源上下文发现账号异常。
- 通过业务，用户和来源上下文发现资源抢占。



单一过程没有明显攻击特征

用户来源业务关联分析

- 对用户，IP和业务三者进行上下文分析建档。
- 三者档案间进行关联分析，多个角度结合，检测访问中的异常行为。
- 基于上下文分析，对基于要素的管控进行有效补充，发现没有明显攻击特征的高级威胁行为。



04 API访问控制

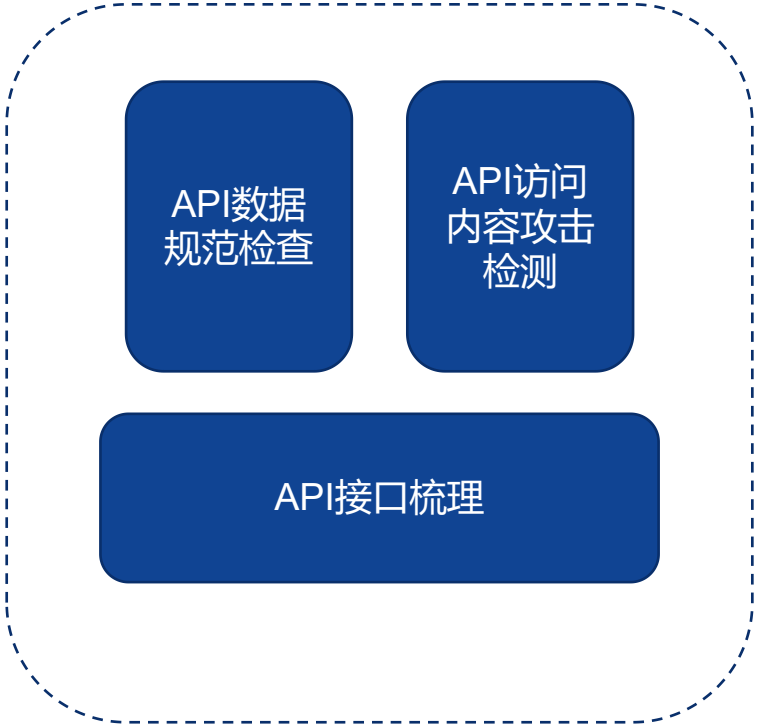
基于用户的API访问控制

API服务可知

●通过自学习对API服务接口进行梳理。统计接口访问情况。通过对API接口参数等学习，自动生成策略，防止0day攻击。

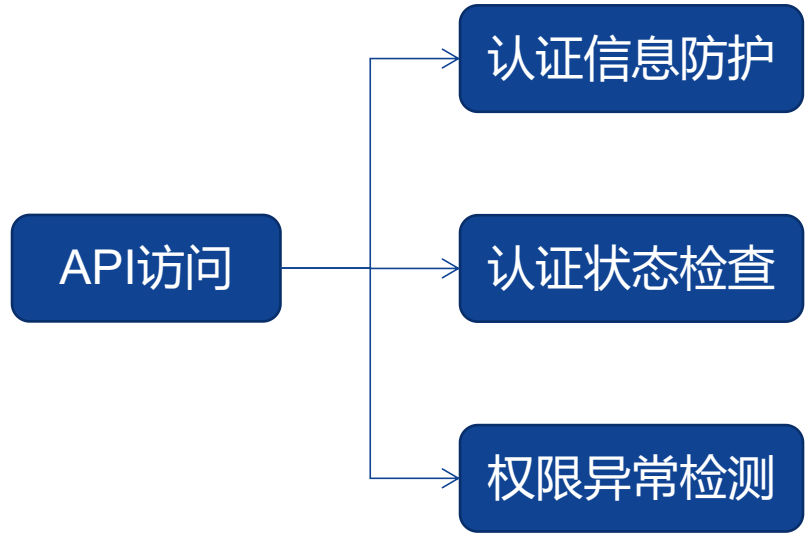
●识别常用XML，JSON等数据格式，对API访问进行规范检查。

●识别API访问的内容，对API访问的内容进行攻击检测。



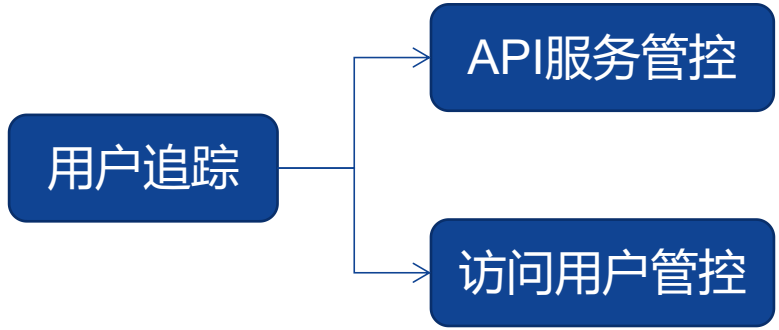
API访问者可信

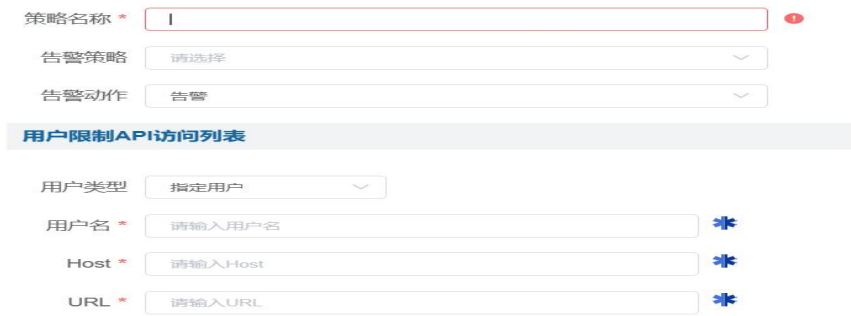
- 通过用户追踪，检查API访问用户的状态，防止非授权API访问。
- 产品通过对用户认证相关信息进行加密与重放保护，防止黑客对用户认证相关信息进行篡改、窃取与重放，保证用户认证信息的安全存储与使用。
- 越权访问是Web应用程序中一种常见的漏洞，由于其存在范围广、危害大，位居OWASP Web应用十大安全隐患的第二位。系统检查用户权限状态，通过用户识别绑定功能可以检测攻击者试图通过修改用户身份相关的标识ID来提升权限、越权访问非法资源的攻击。确保访问者权限可信。



API访问可控

- 通过用户识别，进行基于用户访问控制。
- 通过API访问情况检查，控制API的访问速度和方式。
- 限制API访问的参数规范。
- 发现异常API服务，对僵尸API进行访问禁止。



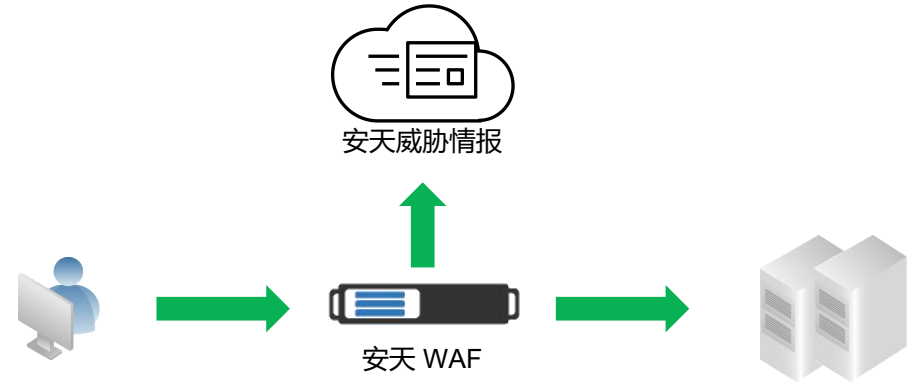


05 情报和AV引擎赋能管控

基于情报的来源检测

集成安天威胁情报，对访问来源精确识别

- 集成安天云端威胁情报服务。安天威胁情报根据多种威胁事件生成威胁情报。
- 攻击情报查询支持异步和实时多种方式，适应多种客户应用类型。
- 威胁级别精细控制，适应各种实施场景。



病毒检测引擎深度检测

集成安天自研病毒引擎，对上传内容进行深度检测

- 多种文件格式识别，包括但不限于二进制可执行文件、文档、包裹文件、脚本文件等。
- 支持对木马、蠕虫、黑客工具、广告软件、勒索软件、挖矿软件以及APT攻击载荷等进行精准检测。
- 多种文件解壳方式。
- 支持多种文件压缩格式解压检测。

感谢大家的关注

安天冬训营 wtc.antiy.cn