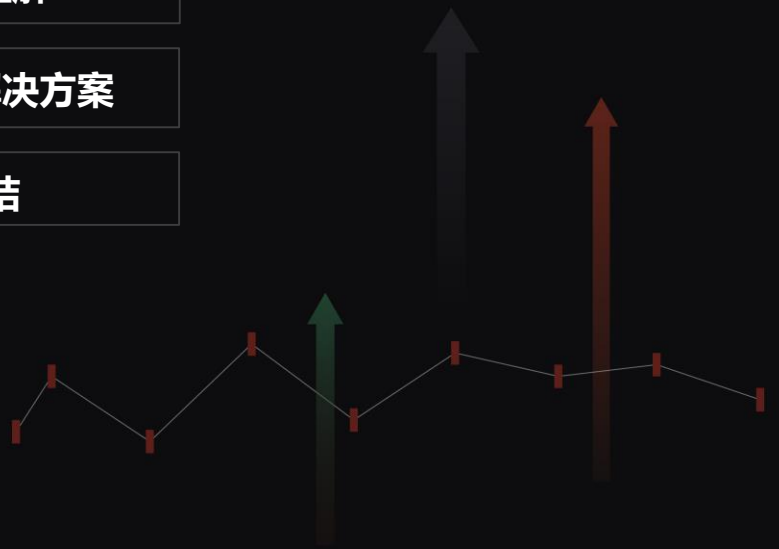
FREEBUF | 企业安全 俱乐部

人工与智能 助力新等保

张志鹏 高级安全顾问

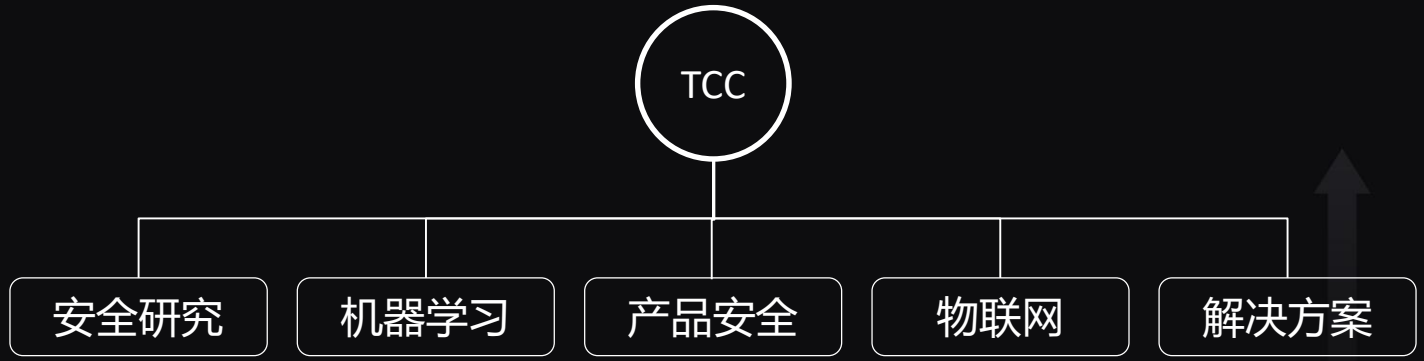
2019企业安全俱乐部 等保专场

目录



关于TCC

斗象能力中心（Tophant Comprehensive Center）是斗象科技的作战尖兵与能力保障，负责重点项目与高新技术的研究与落地。



发现问题，思考根源，改进解决。让生活与工作有意义。

等保的发展史

- 《计算机信息系统安全保护**等级划分准则**》
- 《信息系统安全等级保护**实施指南**》
- 《信息系统安全保护等级**定级指南**》
- 《信息系统安全等级保护**基本要求**》
- 《信息系统安全等级保护**测评要求**》...

- 2019.05.13 公安部发布了网络安全等级保护技术2.0版本

法规政策 → 等保体系 → 建设&推动 → 寻求变革

1994年 2005年 2008年 2017年 2019年

等保1.0 等保2.0

- 《中华人民共和国计算机信息系统安全保护条例》国务院147号条令
- 《国家信息化领导小组关于加强信息安全保障工作的意见》（中发办[2003]27号）

- 2014.2 中央网络安全与信息化领导小组第一次会议
- 习总书记 4.19讲话
- 2017.6.1**《网络安全法》**

新时代，新视角，新等保

求同存异

与时俱进

精益求精

《网安法》->等保2.0

Keywords: 关键信息基础设施 持续的风险评估 风险监控与响应 事件溯源 安全态势

网络与关键信息基础设施的运行安全

第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。

明确了等保重点工作内容

关键信息基础设施的定义；

关键信息基础设施的安全保护义务（第三十四条 运营者设置专门机构和负责人、网络安全教育培训、容灾备份、应急预案和演练等）；

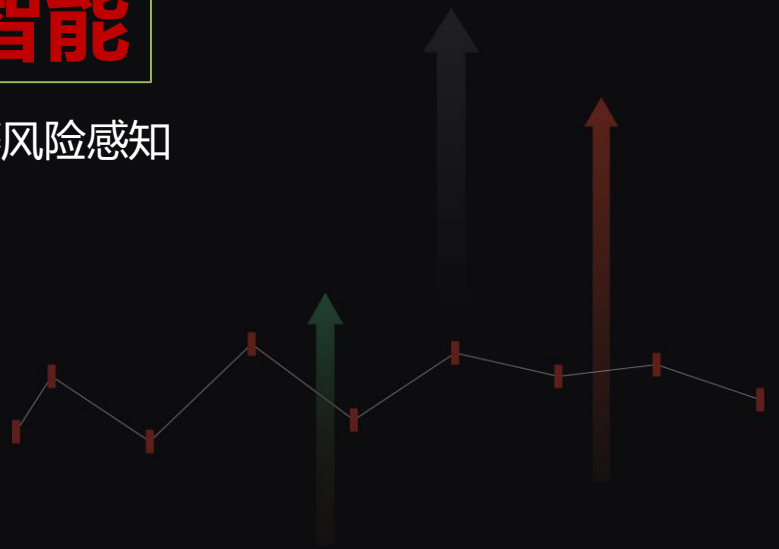
敏感信息保护（第三十七条 境内收集产生的个人信息和重要数据应当在境内存储。确需向境外提供的，应进行安全评估）；

风险评估（第三十八条 运营者每年至少组织一次安全风险检测评估，并评估情况和改进措施报相关部门）。

斗象等保服务解决方案

人工 & **智能**

升级版的安全服务　　网藤风险感知



我们需要怎样的服务

渗透测试

安全合规

对抗式安全服务
（攻防演练）

对抗式演练框架


运维主体
开发人员
业务人员
运维人员
渗透
管理
攻击工具&方法
信息收集类 如OSINT
漏洞扫描类 如wvs
pay load生成类 如Metasploit
密码破解类 如HashCat
命令控制类 如Cobaltstrike
ATT&CK攻击矩阵
执行
攻击流程
范围&信息收集
纵向渗透
应用渗透
漏洞利用
横向渗透
内网横向移动
关键目标 数据获取
达成目标
攻击
业务资产
主机系统
网络设备
应用系统
信息数据
防护
安全设施
防火墙
入侵防御系统
防病毒系统
安全审计
流量监控
防DDOS
支撑
防守活动
安全策略
应急响应
阻断攻击
分析溯源
漏洞修复
影响评估
优化改善
使用
保护
攻击方
漏洞盒子自有专家
白帽子资源
签约安全团队
攻防
防守方
领导层
执行层
事件检测组
事件处置组
威胁分析组
应急恢复组
制定
防守过程
事前 安全策略
事中 应急实施
事后 总结培训
实现

传统服务与攻防演练的差异

	攻防演练	安全/渗透测试
目的	目的不在发现漏洞多少； 检验防御有效性； 检验应急处置能力； 检验人员安全意识；	尽可能多发现安全漏洞，测试面全覆盖。
实施方式	攻击方需要隐藏自身，绕开防御设备，深入横向渗透； 攻击方式除了系统漏洞本身，还有社工、钓鱼等； 漏洞需要评估对业务实际影响；	攻击方无需隐藏自身。漏洞点到为止。
参与对象	过程需双方参与，防守方需要积极防御，并做相应应急响应 。	过程中主要乙方参与，完成渗透并输出报告 。

网藤与合规

《网络安全法》

强调了安全监测与关键信息基础设施的保护

- 建立统一的监测预警和应急处置制度和体系
- 信息基础设施重点保护
- 网安法二十一条，关键数据存储不少于6个月

《网信办》

“没有网络安全，就没有国家安全”

重点强调了网络安全攻防、态势感知能力、人工智能应用等工作方向

《网络空间安全战略》

公安与等保

- 等保2.0发布与推广，要求漏洞检测、入侵识别、风险管理
- 强调对网络空间的整体监控
- 监管部门对关键基础设施的监测与防护体系的建立

行业标准

- 全国信息安全标准化技术委员会
- 金融综合监管机构
- 发改委/工信部/保密局/行业协会

PRS-Enterprise
海量数据存储与索引

PRS-Enterprise
回溯分析 取证调查

CRS-云端检测中心
网站内容安全监测

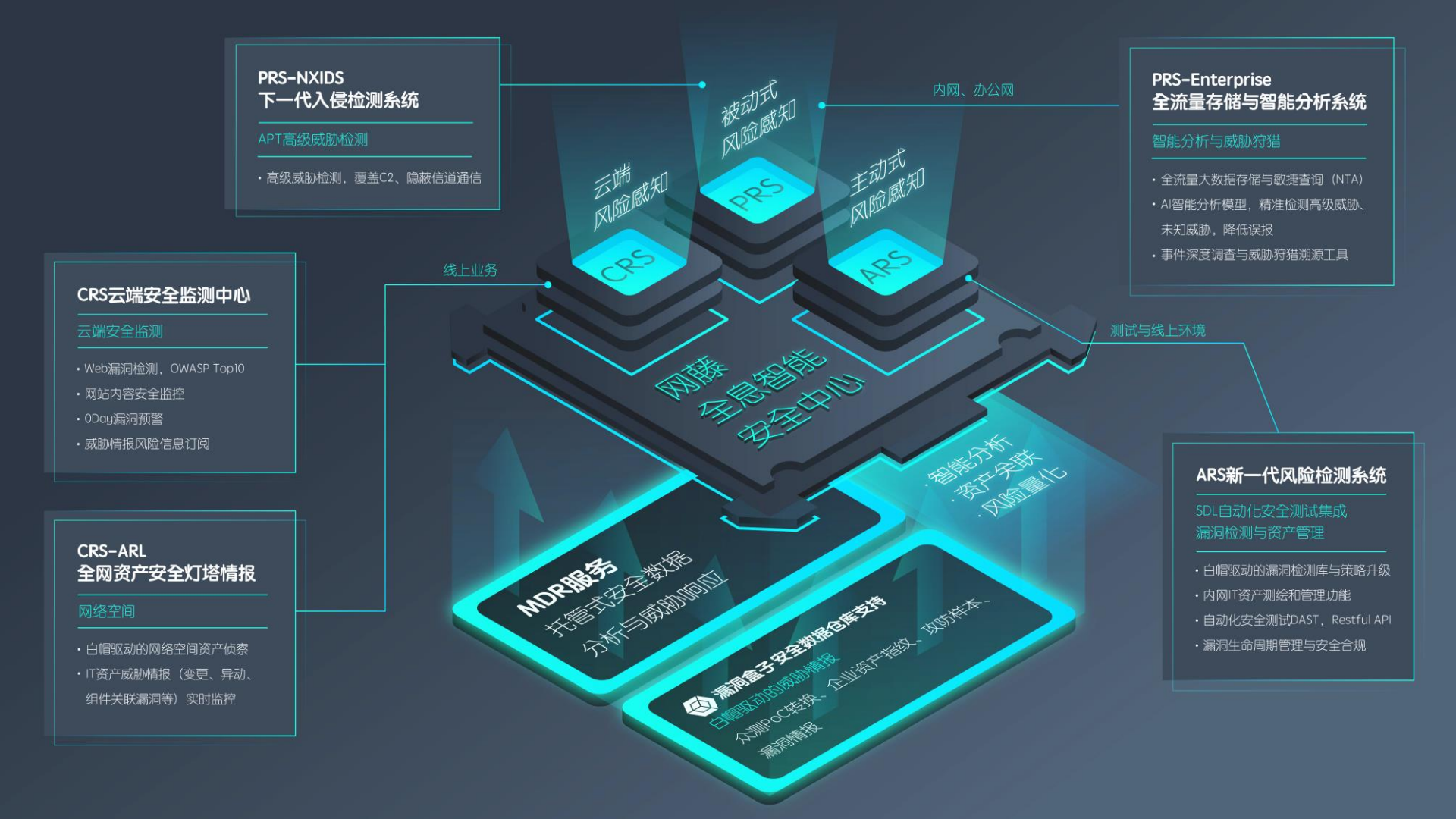
PRS-NXIDS
基于AI的高级威胁检测与响应

CRS-全网资产安全灯塔情报
全网资产智能侦察

ARS-资产安全风险检测
Web&主机安全漏洞检测

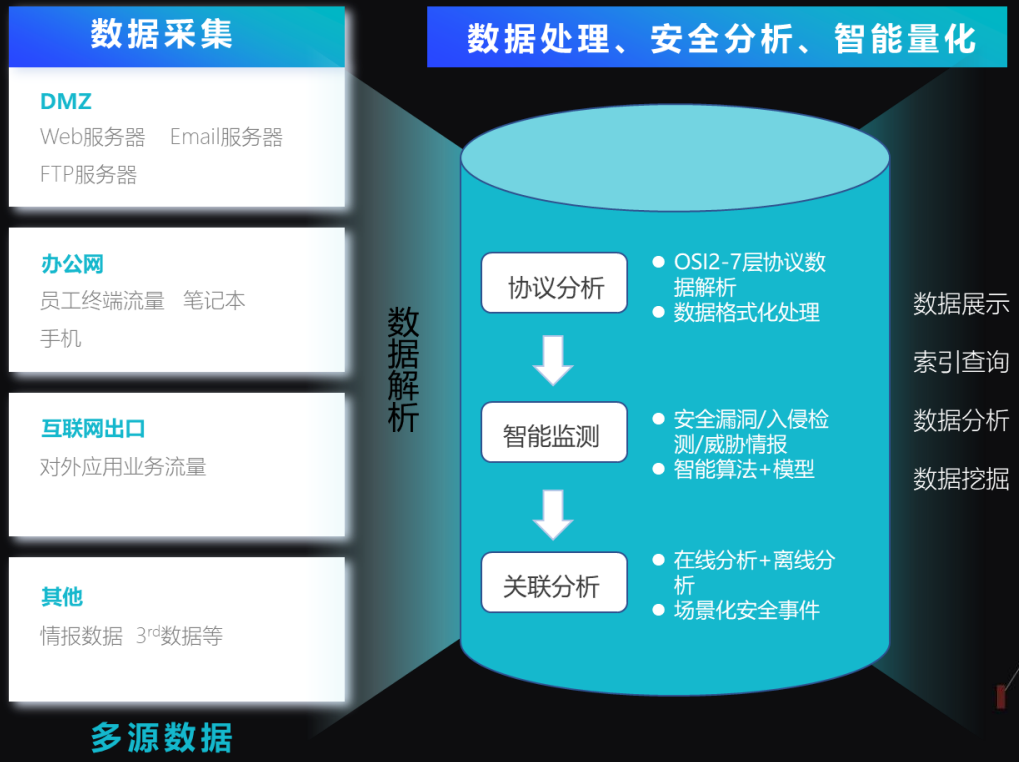
动态爬虫支持前端框架解析，
分线检测智能升级

自主可控
满足关键基础设施安全


PRS-NXIDS
下一代入侵检测系统
APT高级威胁检测
• 高级威胁检测，覆盖C2、隐蔽信道通信
CRS云端安全监测中心
云端安全监测
• Web漏洞检测，OWASP Top10
• 网站内容安全监控
• 0Day漏洞预警
• 威胁情报风险信息订阅
CRS-ARL
全网资产安全灯塔情报
网络空间
• 白帽驱动的网络空间资产侦察
• IT资产威胁情报（变更、异动、组件关联漏洞等）实时监控
线上业务
被动式
风险感知
云端
风险感知
主动式
风险感知
PRS
CRS
ARS
内网、办公网
测试与线上环境
网藤
全息智能
安全中心
·智能分析
·资产关联
·风险量化
MDR服务
托管式安全数据
分析与威胁响应
漏洞盒子安全数据仓库支持
白帽驱动的威胁情报
众测PoC转换、企业资产指纹、攻防样本、
漏洞情报
PRS-Enterprise
全流量存储与智能分析系统
智能分析与威胁狩猎
• 全流量大数据存储与敏捷查询（NTA）
• AI智能分析模型，精准检测高级威胁、未知威胁。降低误报
• 事件深度调查与威胁狩猎溯源工具
ARS新一代风险检测系统
SDL自动化安全测试集成
漏洞检测与资产管理
• 白帽驱动的漏洞检测库与策略升级
• 内网IT资产测绘和管理功能
• 自动化安全测试DAST，Restful API
• 漏洞生命周期管理与安全合规

网藤大数据存储与索引

网藤PRS通过旁路监听，高速、可靠分解全网络流量，所有网络信息全息可视可回溯



- 数据实时分析，大数据架构秒级处理万兆流量
- 高精准，高性能，高可用，可扩展
- 智能流量全解析，海量数据快速索引
- 快速侦测恶意攻击与安全风险
- 事件溯源，快速定位，提升效率，节约成本
- 标准协议协议50+，私有协议定制化

PRS-IOC调查画布

- IoC （Indicator of Compromise）信标：应用于计算机取证，指在网络或系统中可观察到的且高可信度的表明计算机入侵的工件。

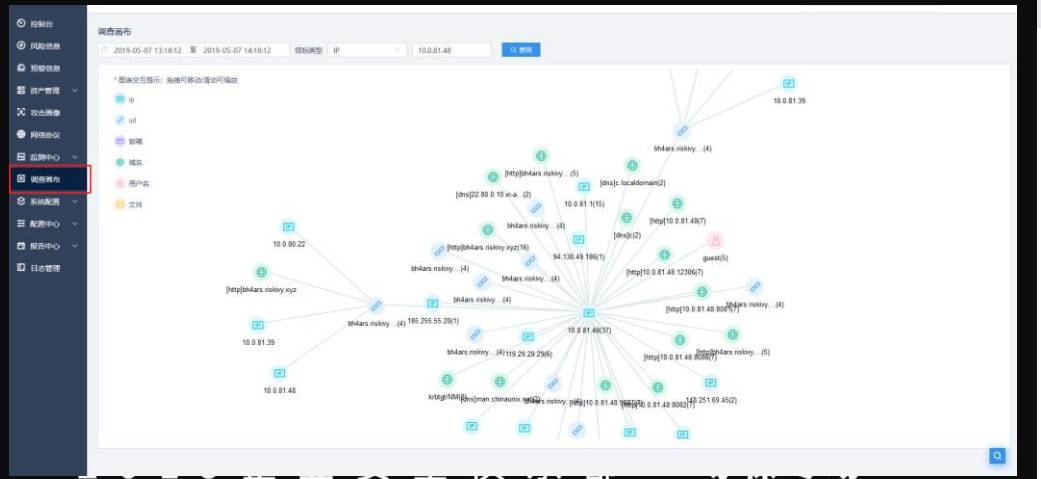
Eg. IP地址、域名、hash恶意文件、病毒签名...

Indicator of compromise

From Wikipedia, the free encyclopedia

Indicator of compromise (IoC) — in computer forensics is an artifact observed on a network or in an operating system that with high confidence indicates a computer intrusion.[1]

- IoC调查画布,是威胁狩猎的典型应用，将多组有关联的信标用可视化手段进行展示，可以更高效、清晰的展示攻击行为



PRS-智能驱动

对于多源杂乱数据进行有效梳理，提供有价值的规范化数据，主要应用方向：

- **数据内容的解析：**如协议内容、文件/图片内容的语义解析等
- **事件的关联分析**
- **行为分析**
- **风险预测**

风险检测引擎应用大量基于机器学习的安全模型，增加检出率，降低误报率，主要应用方向包括：

- **提升传统漏洞检出的安全模型：**如webshell、恶意文件等
- **威胁情报数据挖掘的安全模型：**DGA检测、恶意IP地址等
- **新型隐蔽通信的安全模型：**DNS tunnel、ICMP tunnel等

以科学的视角对安全监测及响应提供标准化数据，主要应用方向：

- **风险评估：**科学模型公式计算风险实际危害
- **多源数据融合处理：**对不同数据进行格式化处理，统一标准，提升数据处理效率。

ARS-资产采集与安全检测

漏洞检测

范围全覆盖：Web漏洞 | 主机漏洞 | API

通用漏洞规则

- Web类：注入 | 跨站 | CSRF | SSRF | CRLF | 目录穿越 | 文件包含 | 登录表单猜解 | 越权行为 | SSTI | 通用应用漏洞(eg.Weblogic/docker/Jboss/Oracle/...)
- 主机类：操作系统 | 数据库 | 网络设备 | 技术基础组件

漏洞库规则：外部：CVE/CNVD/OWASP | *内部：漏洞盒子

*最新0day：漏洞盒子&业界最新漏洞转换 + TCC最新研究成果

运维风险 / 人为弱点

- 配置文件核查
- 权限过大
- 控制宽松
- 内部端口对外
- 弱口令
- 敏感数据外泄

*威胁情报

- 互联网漏洞平台
- 全网数据侦查
- 最新安全动态
- 智能引擎驱动
- 数据联动分析

*资产全面识别

主被结合 | 前端框架支持 | 应用指纹识别 | C段资产

*被动式漏洞检测

基于网络流量，解析业务HTTP请求，提升测试覆盖度，解决传统所扫描器不能覆盖的业务死角和漏洞

*白帽定向插件

漏洞盒子

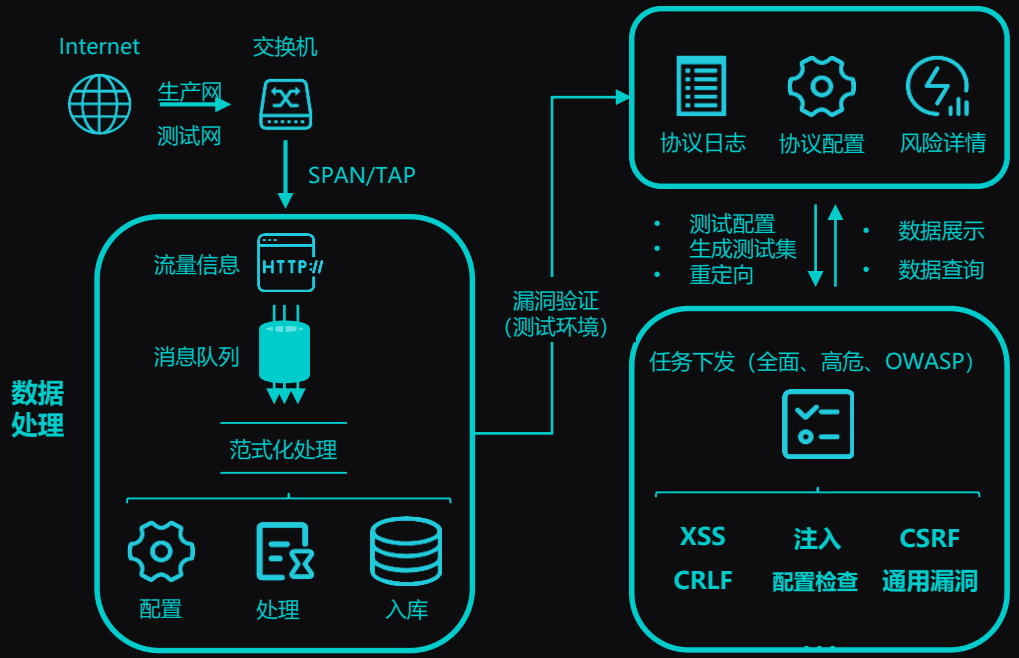
弱点资产 | 组件漏洞 | 专用框架 | 资产指纹

产品研发 → 产品测试 → 产品发布 → 产品运营与响应

网藤ARS具备全面的安全检测/监测能力，可有效融入企业安全开发流程，提升企业产品整体安全质量，实现安全漏洞全覆盖

ARS-流量式扫描

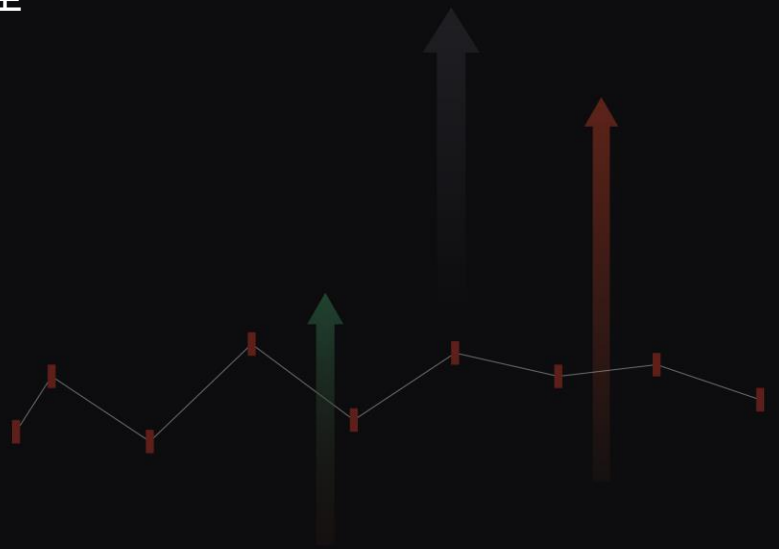
被动式流量扫描采用旁路镜像方式，深入分析流量中资源信息，提升扫描覆盖率。被动式扫描可以很好的解决主动扫描无法获取独立页面、业务逻辑触发的页面等问题，在提升扫描速度与扫描精准度方面同样效果显著。



- 被动式流量解析，request/response全信息存储，漏洞信息提供全面详细
- 提升检测覆盖率，挖掘深层隐蔽资源
- 减少爬虫时间，提升扫描效率
- 主被结合，提升扫描精度
- 分布式架构，部署方便，操作简易

总结

- 等保不是应付检查
- 安全不能事后处理
- 技术才是硬道理



FREEBUF | 企业安全 俱乐部

2019企业安全俱乐部 等保专场