

动态安全 - 构建等保2.0时代的主动防御

马蔚彦 瑞数信息



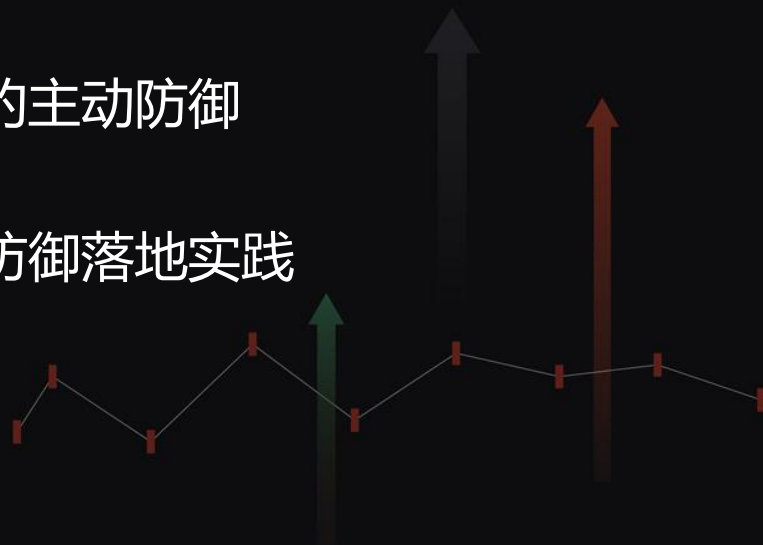
议程



对等保 2.0 主动防御的理解

动态安全所构建的主动防御

动态安全的主动防御落地实践

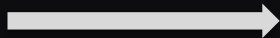


等保2.0的重要变化 – 企业安全建设视角



//// 主动防御的具体体现和诉求

被动防御

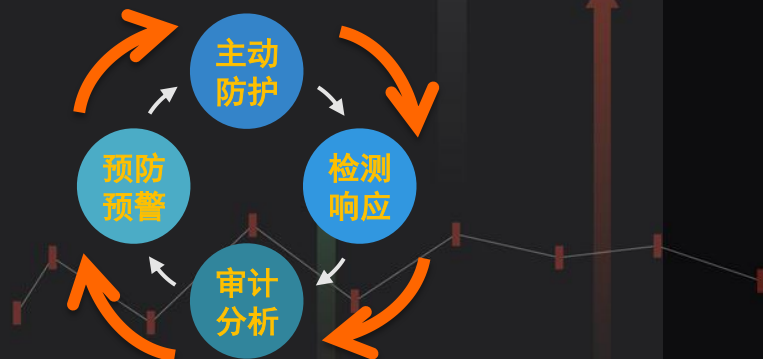


主动防御

- 目标：防护（单一）
- 技术：被动防护
- 体系：静态防御



- 目标：预警、检测、审计（多机制）
- 技术：可信计算、主动免疫
- 体系：动态防御



//// 主动防御的技术趋势 – IDC报告

移动目标式的动态防御 成为主动防御技术领域的技术方向

移动目标式的主动防御

- 迫使攻击者不断重新适应，并对动态转移的薄弱点作出反应，从而有效防止攻击者使用自动化僵尸程序

机器学习

- 利用大数据和机器学习解析法，熟悉和学习企业的正常流量，从而判定企业业务的异常访问

主动行为分析

- 主动行为分析和指纹识别来识别客户端的正常流量，用户使用模式和用量来检测和启发式推测可疑活动

安全情报及主动预测

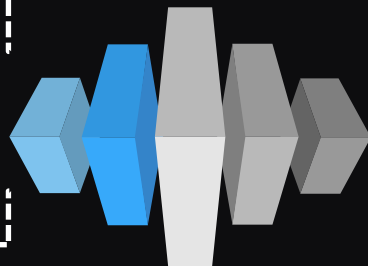
- 通过情报交流和第三方数据收集安全威胁情报，包括诈骗风险情报数据库让企业知悉最新的攻击信息



//// 主动防御的技术趋势 – Gartner WAF报告

易于使用，**减轻运维**和影响

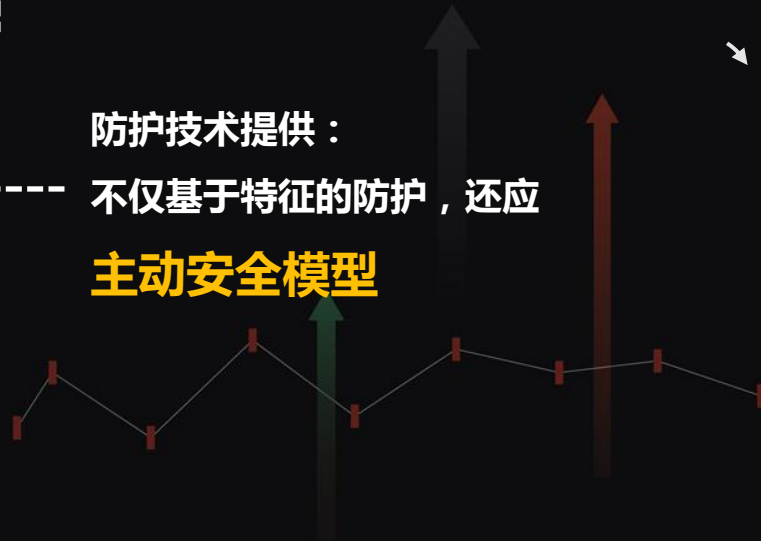
提高检测率：
不仅已知威胁，还要
未知威胁



Gartner®

区分**自动化流量**和人类用户流量

防护技术提供：
不仅基于特征的防护，还应
主动安全模型





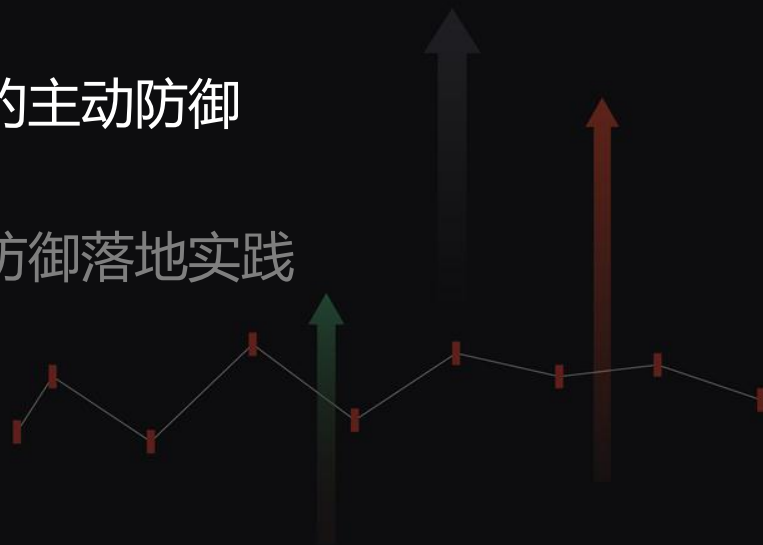
议程



对等保 2.0 主动防御的理解

动态安全所构建的主动防御

动态安全的主动防御落地实践




////// 动态安全技术的理念及特点

以“先发制人，掌握先机”
的防护哲学彻底颠覆攻防态势



 降低管理负担

 加快防护响应

 提升攻击难度

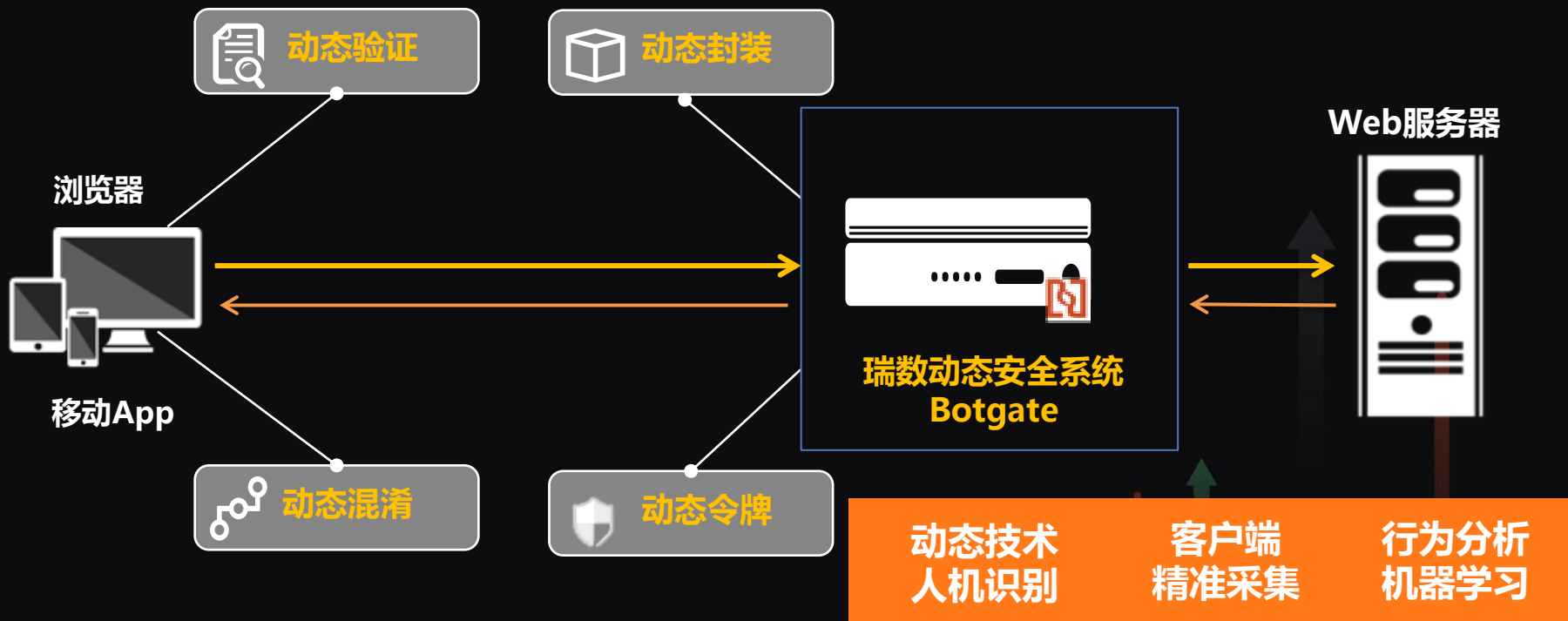
传统防护理念：

挖掘 漏洞
匹配 特征
设置 规则

主动式防护理念：

隐藏 漏洞
变换 自身
验证 真伪

////// 动态安全 – 四大核心技术保护业务及数据安全



////// 动态安全 – 应对数字经济带来的安全新挑战

- “工具”的规模化业务风险
- 业务逻辑安全问题
- 未知威胁问题



网站安全

- 防漏洞探测
- 防零日漏洞
- 防应用 DDoS
- 防代码分析



数据泄漏

- 防爬虫
- 防内鬼
- 防数据遍历
- 防拖库



账号安全

- 防撞库
- 防暴力破解
- 防批量注册
- 防短信轰炸



交易欺诈

- 防虚假交易
- 防交易篡改
- 防黄牛党
- 防薅羊毛



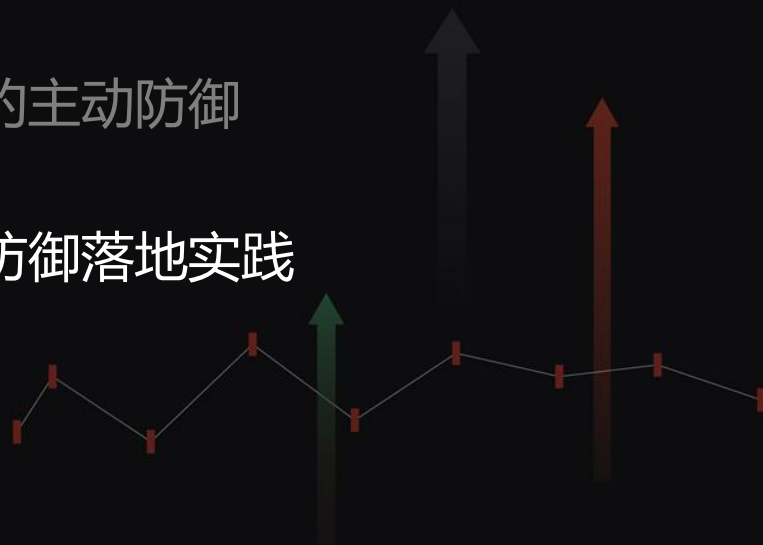
议程



对等保 2.0 主动防御的理解

动态安全所构建的主动防御

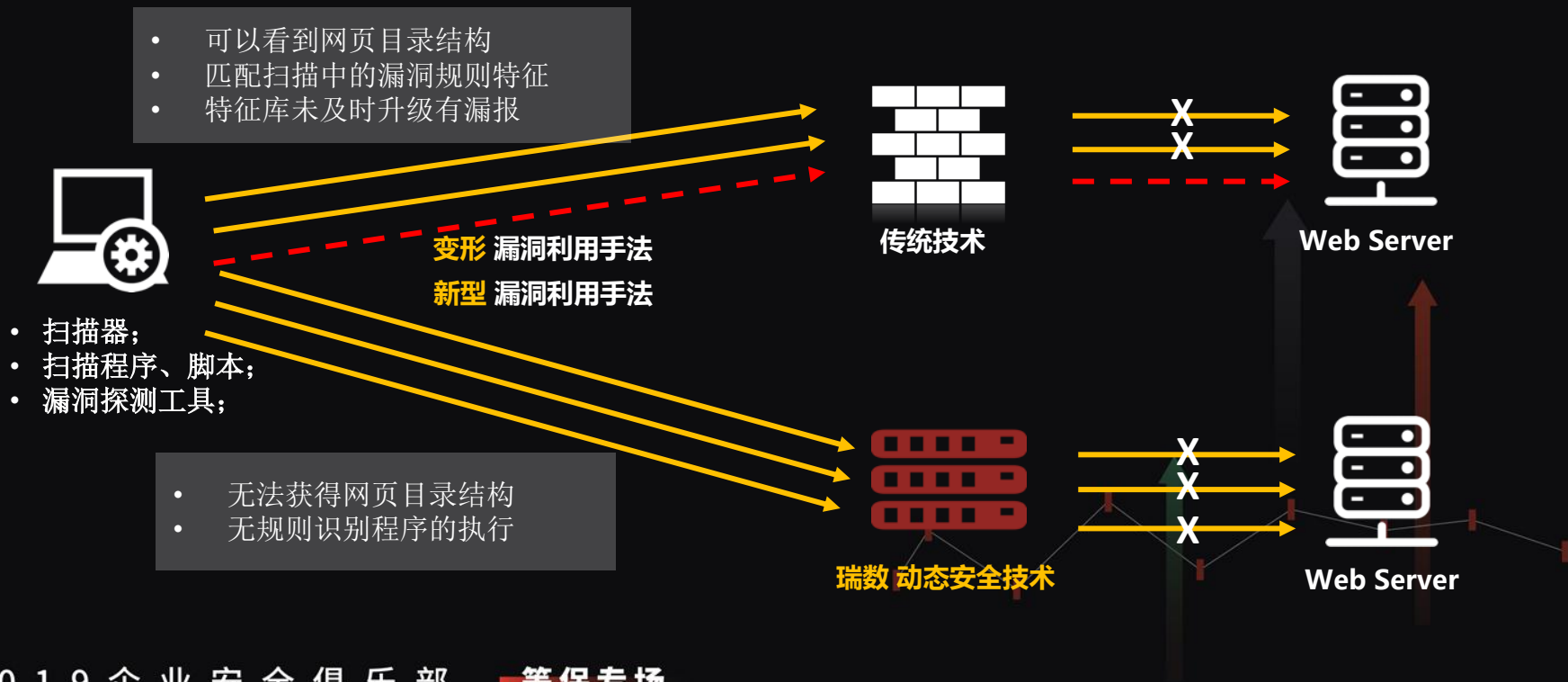
动态安全的主动防御落地实践



////// 动态安全 – 主动防御的特点体现

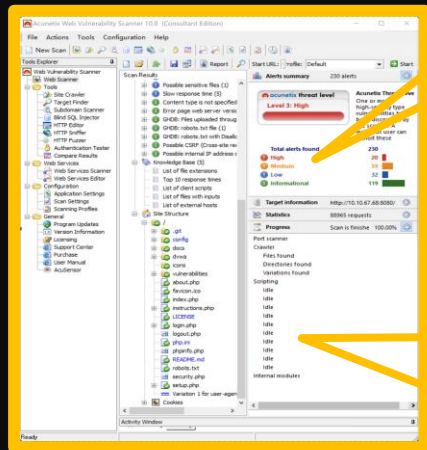


///// 隐藏漏洞防探测 – 将探测止于扫描程序的执行



///// 隐藏漏洞防探测 - 效果

防护前的扫描

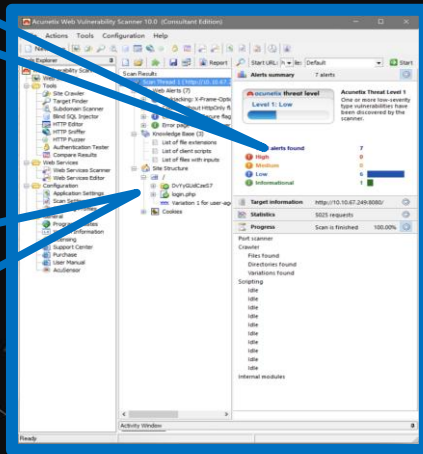


Total alerts found	230
High	20
Medium	59
Low	32
Informational	119

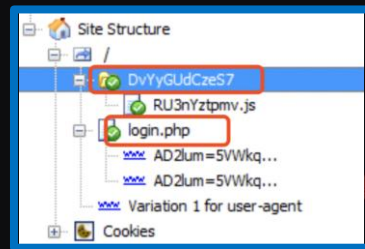


Total alerts found	7
High	0
Medium	0
Low	6
Informational	1

防护后的扫描

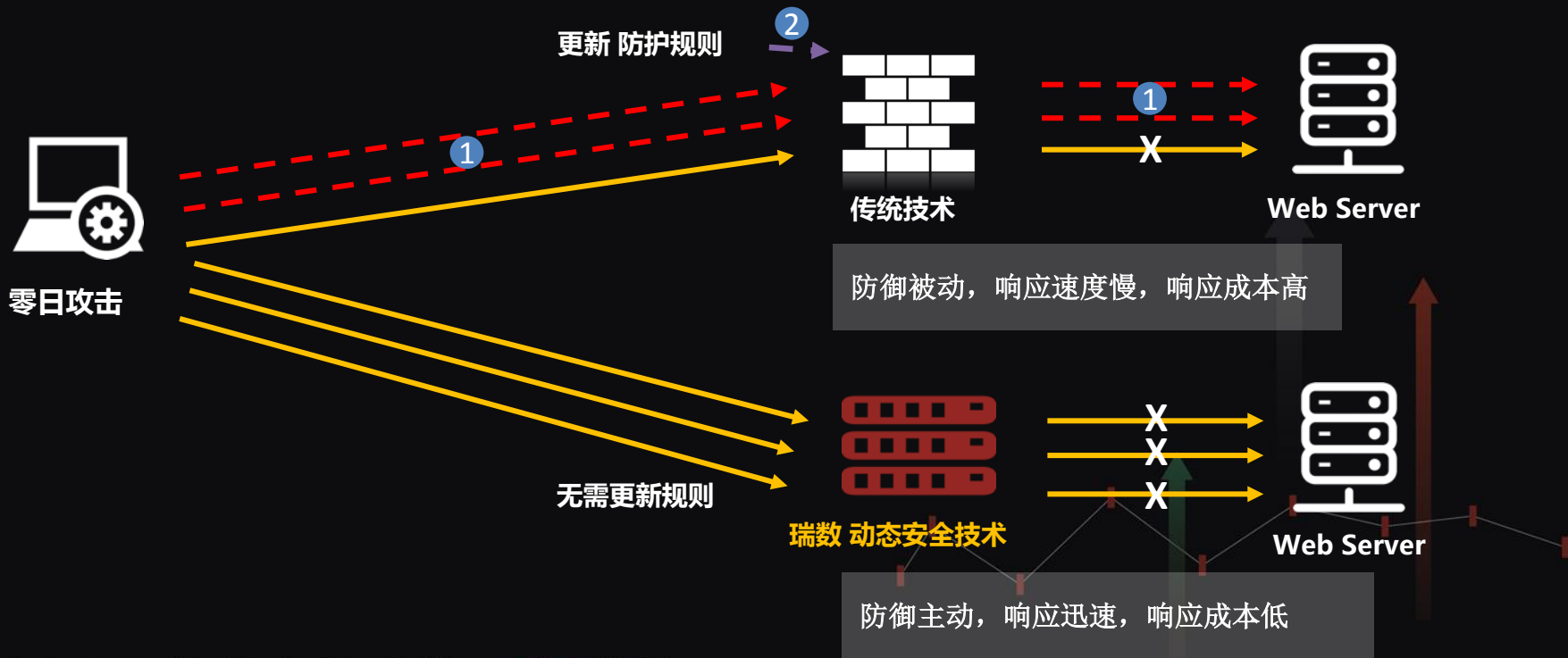


隐藏漏洞



隐藏网页目录结构

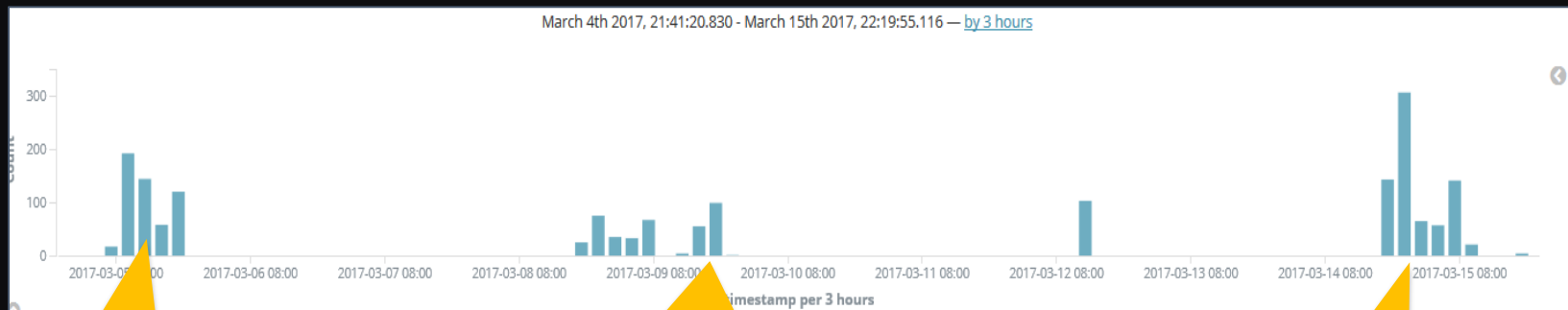
//// 无规则防零日 – 实现主动防御



///// 无规则防零日 – 效果

某网站 Struts2 漏洞防护实例

- 瑞数信息在漏洞公布前2天已经做了拦截
- 攻击中除当时报出的S2-045外，还有2016年披露的S2-032漏洞。
- 累计拦截了数千次各类 S2 攻击（绕过了部署在瑞数设备前端的WAF）



S2-45漏洞正式公布前2天，已经有黑客开始利用S2相关漏洞攻击

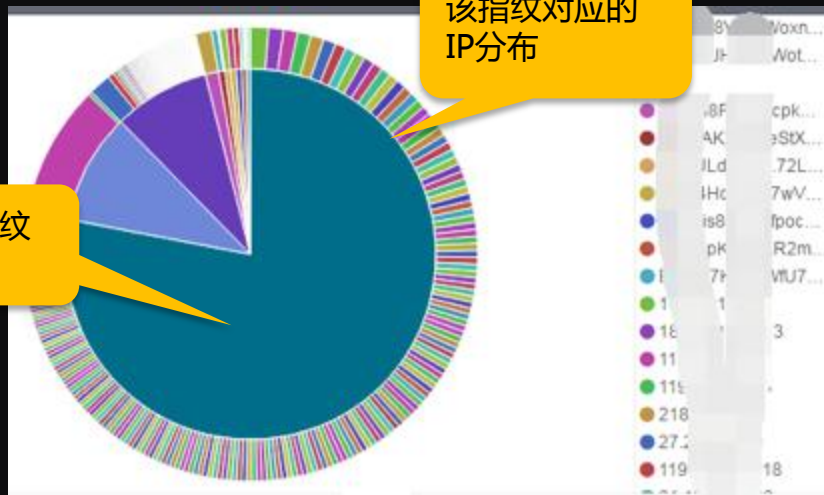
漏洞正式公布后2天，前端WAF 升级特征库防范S2-045，但黑客利用S2-032漏洞，穿透了WAF防护

两会闭幕时，黑客发起第三波攻击

///// 模拟合法操作逻辑 – 事中实时精准识别

多源低频 “撞库” - 不依赖事后分析

- 攻击者不停更换IP隐藏自己，瑞数动态技术准确识别。
- 日志中通过浏览器指纹进行IP关联分析，发现大量分布式IP是集成的浏览器指纹
- 封IP、限频率的传统手段完全失效



多IP源 低频率攻击

src_ip: Descending	
113.	15
182.	13
117.	12
11.	117
21.	115
27.	110
119.	94
61.16	92
183.1	91
182.1	89

////// 动态安全为基础的主动防御体系 – 落地实践等保2.0

动态防御

- 动态验证
- 动态封装
- 动态令牌
- 动态混淆

威胁预测

- 机器学习
- 威胁洞察
- 趋势预测
- 策略调整



态势感知

- 终端指纹采集
- 业务逻辑感知
- 操作行为感知
- 陷阱异常捕获

智能响应

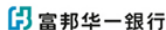
- 风险可视
- 智能拦截
- 威胁取证
- 协同响应

////// 动态安全为基础的主动防御体系 – 我们的客户

35+运营商



10+银行、基金等金融机构



15+国家政府机构



15+大型企业



15+教育、医疗、出版及互联网企业



THANKS