JSRC

2017 JSRC安全乌托邦 大数据与威胁情报

北京·奥林匹克公园·水立方3号门2层

2017年7月29日

用安全情报实现威胁检测和响应的闭环

杨大路
天际友盟 CEO

安全情报的范畴

安全情报

- 资产情报
- 威胁情报
- 安全措施情报
- 安全需求情报
- 漏洞情报
- 事件情报
- 业务战略情报

安全情报的作用

I（Intelligence）

安全情报的生产、应用、消费

E（Ecosystem）

厂商间的行业生态联动

D&A（Data&Ability）

产品间的数据与能力联动

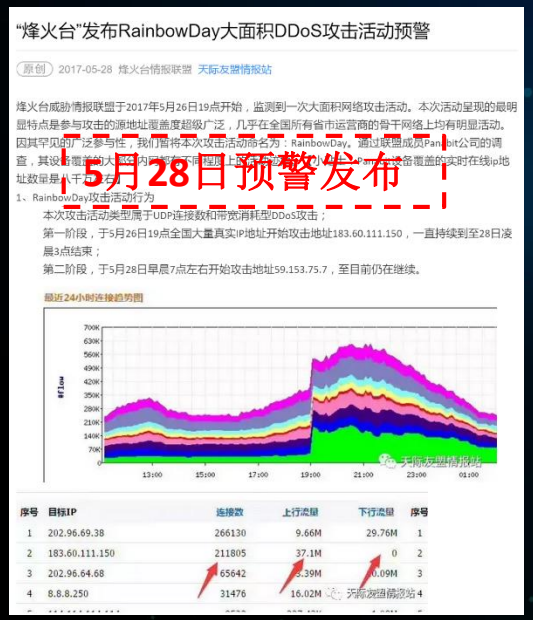
K（Knowledge）

人机间的知识联动

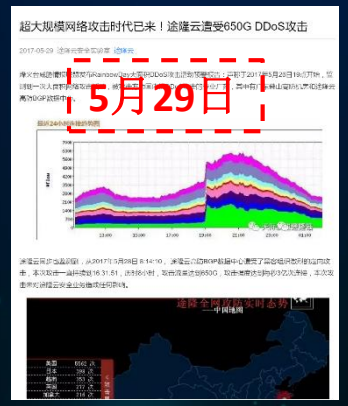
一个DDoS攻击、检测、响应的例子

发现接入网有大面积异常活动

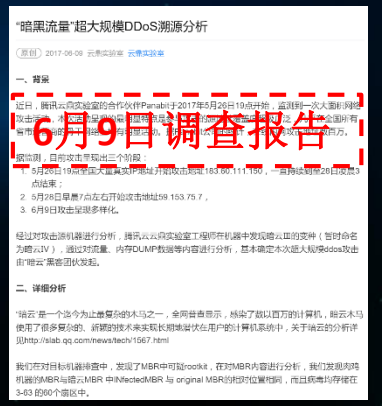
分析预警



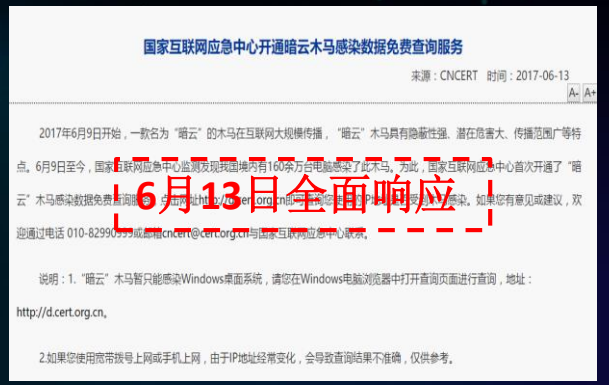
受害证实



调查取证



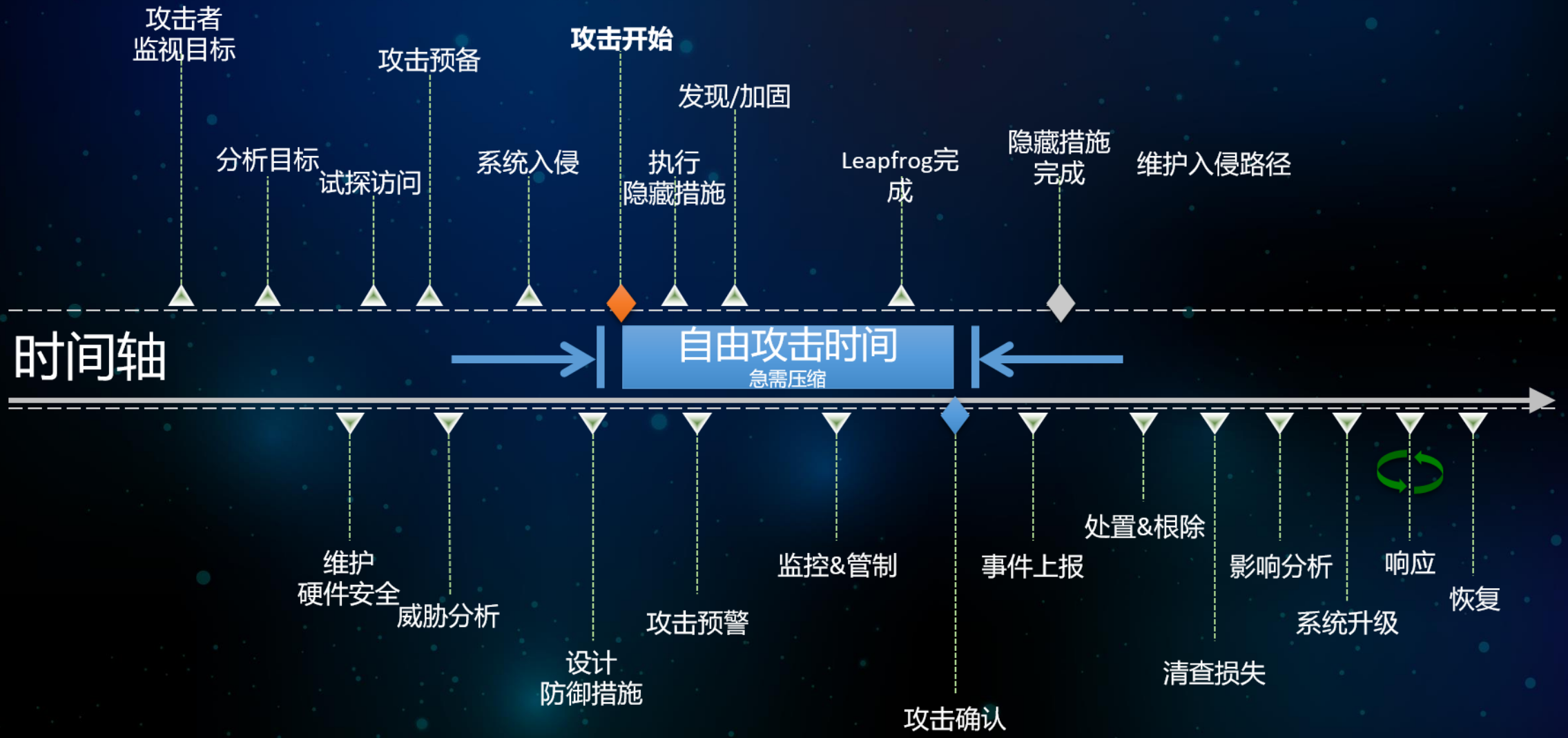
应急响应



攻击、检测&响应的现状

攻击技术飞跃，传统检测&响应手段低效

以缩短“自由攻击时间”为目标

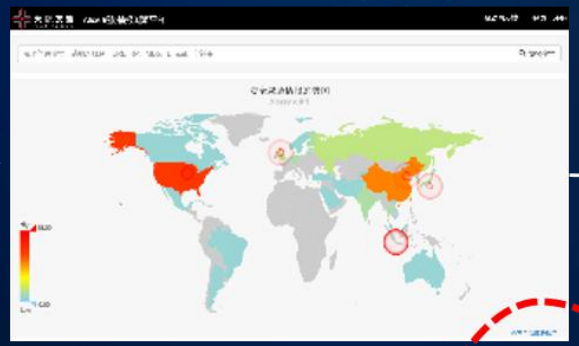


安全情报在检测&响应环节的价值

安全情报辅助网络异常检测

自己的情报
开源的情报
商业的情报

多源整合



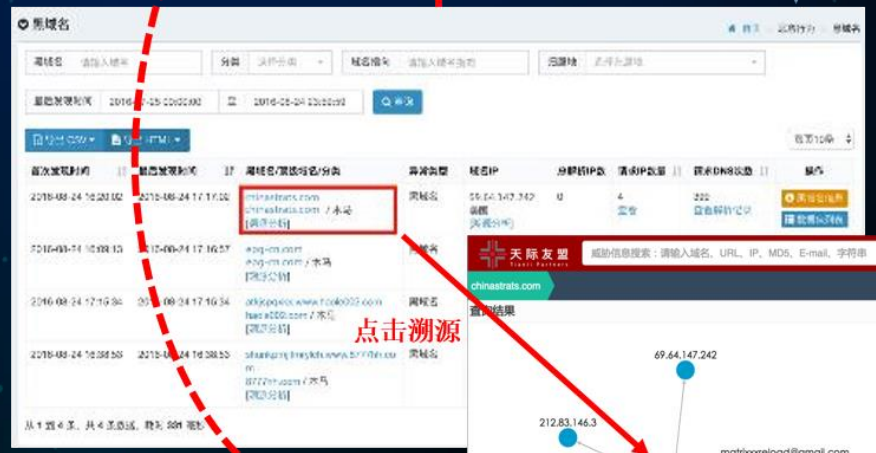
威胁情报
信誉Feed
检测规则

API自动获取

用户网络镜像流量

单点登录查询

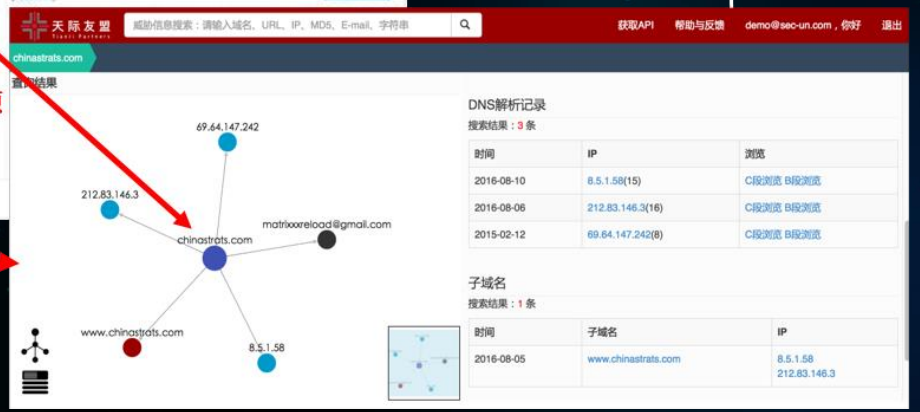
发现异常



结果返回

关联情报
关联IOCs

API自动获取



安全情报驱动资产漏洞管理闭环

外部漏洞情报
分发至本地

“Claire”安全情报中心（SIC）

安全态势 | 资产管理 | 情报管理 | 告警管理 | 扩展功能

情报输出接口

可视化

智能检索 | 报表生成

数据存储 | 数据匹配

资产情报 | 事件情报 | 威胁情报 | 漏洞情报 | 告警信息

情报输出

安全漏洞

模块联动

“Helena”资产与漏洞管理模块

外网资产监控

- 外网漏洞扫描
- 用户域名监控
- 社交媒体监控

内网资产发现

- 操作系统
- 应用软件
- 通用组件
- 网络设备

漏洞扫描&验证

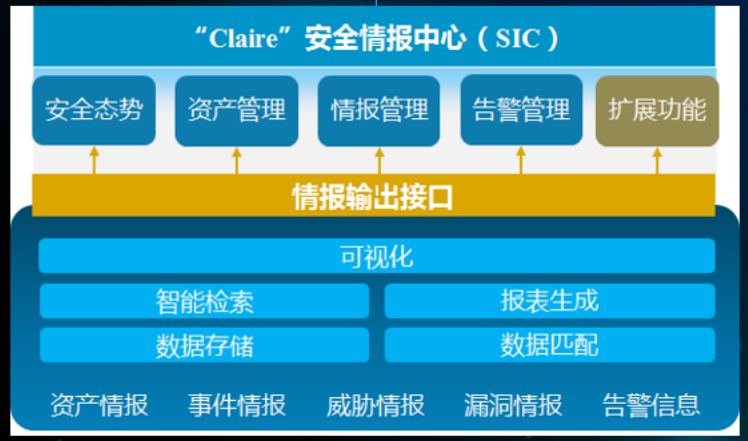
- 漏洞扫描
- POC/EXP智能调用
- 自动化漏洞验证

漏洞扫描&验证

- 资产漏洞情报推送
- 漏洞修复建议
- 辅助安全决策

安全情报驱动检测&响应闭环

外部情报
分发至本地



Step2：情报预警平台对转发的数据进行比对、展现

- 远控域名、ip
- APT
- 僵尸、钓鱼、勒索软件

Step3：

- 检测结果进行呈现——失陷主机、严重级别、攻击类型
- 下发策略进行流量过滤

过滤后流量

情报预警网关

原始流量

Step1：预警网关将被动监听数据传送给SIC

- IP通信日志
- URL访问记录
- DNS请求日志
- Mail邮件访问

通过数据管理提升安全情报质量

同源去重：将同一来源不同事件的情报数据进行去重汇总，合并威胁分类与影响范围标签。

去伪降噪：对数据进行验证，去除错误、失效、无效的数据信息。

老化处理：持续监控情报数据，去除信誉值低于输出阈值的数据条目。

多源去重：根据用户订阅需求，按标签筛选对应的情报数据，对结果进行多源聚合，合并情报来源、威胁分类与影响范围标签。

情报封装：基于STIX国际标准进行情报的封装打包。

安全情报提升主动防御能力

安全情报驱动产业生态协作案例

烽火台安全威胁情报联盟
FengHuoTai CTI Alliance

- 天际友盟 TianJi Partners
- 神州网云 SZWY
- 观星 Data Star Observatory
- Panabit®
- 山海相诚 日月互信
- 互信互通 HU XIN HU TONG
- cirrus gate 思睿嘉得
- WebRAY
- 云盾科技 CLOUDYSECURITY
- ipip.net
- SPINFO 世平信息
- Watcher LAB

➢ 联盟情况

国内首个威胁情报联盟，2015年10月成立，12家成员企业。

➢ 联盟宗旨

以安全威胁情报为核心，打造平等互惠的新生态圈模式，共谋共策，推进威胁情报的标准制定及应用推广。

➢ 合作理念

“联合”、“共享”与“共赢”。

➢ 合作模式

技术合作：关键基础设施共建，对内情报信息共享，对外产品联动协同。

服务合作：服务支持体系共建，服务人员集中培训，服务内容统一管理。

市场合作：解决方案整体打包，市场推广互通协作，客户资源信息共享。

THANK YOU !