

2020北京网络安全大会

2020 BEIJING CYBER SECURITY CONFERENCE

」 一 天际友盟 TianJi Partners

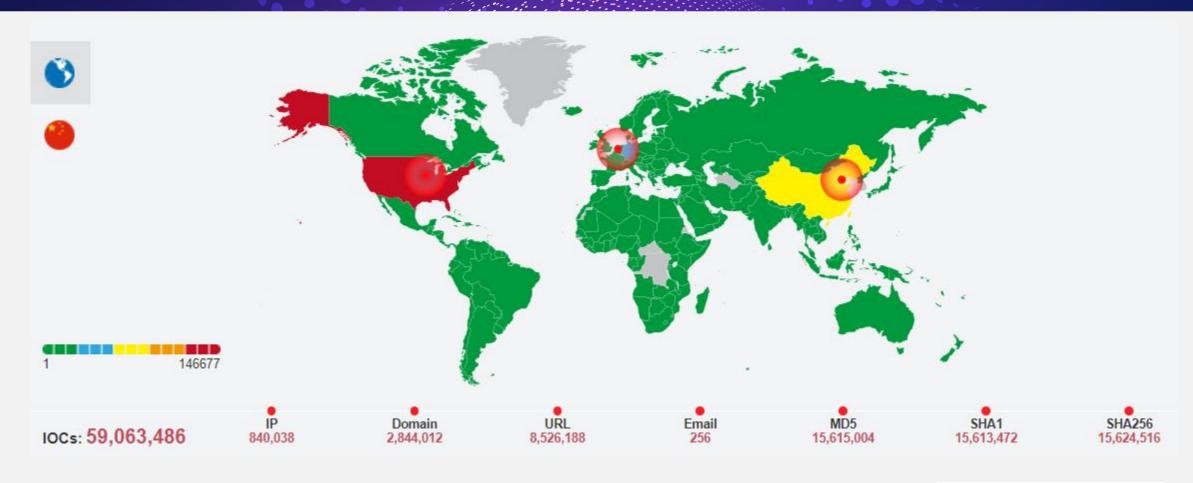
威胁情报与主动防御

---关于数字化安全呈现无边界趋势的思索

SECURITY DEFENSE ENDPOINT NETWORK HUNTINGS CRITICAL CLOUD INTERNET BEHAVIORAL ANALYTICS TO

分享人: 杨大路 (天际友盟 CEO)

全球安全现状



APT攻击常态化

专注、专业、持续

攻击门槛 日益降低

Wannacry/notpetya

5G带来的新风险

网络规模快速扩大

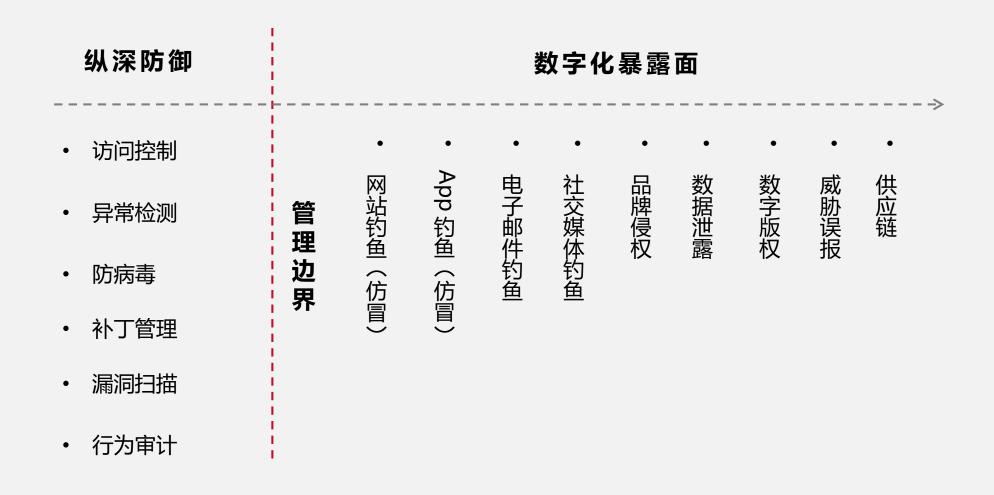
钓鱼欺诈攻击加剧

面向关键基础设施

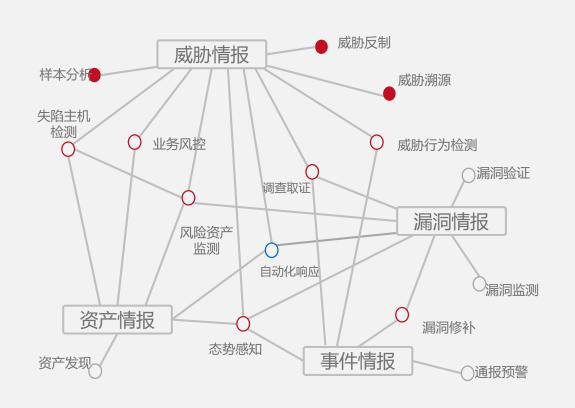
数字化进程带来的挑战



企业信息安全不仅仅是关注企业网络边界路由器内的安全,更多的分布在管理权限外的潜在威胁使得数字风险的边界越来越模糊,响应和处置越来越困难



威胁情报为何可以用于主动防御

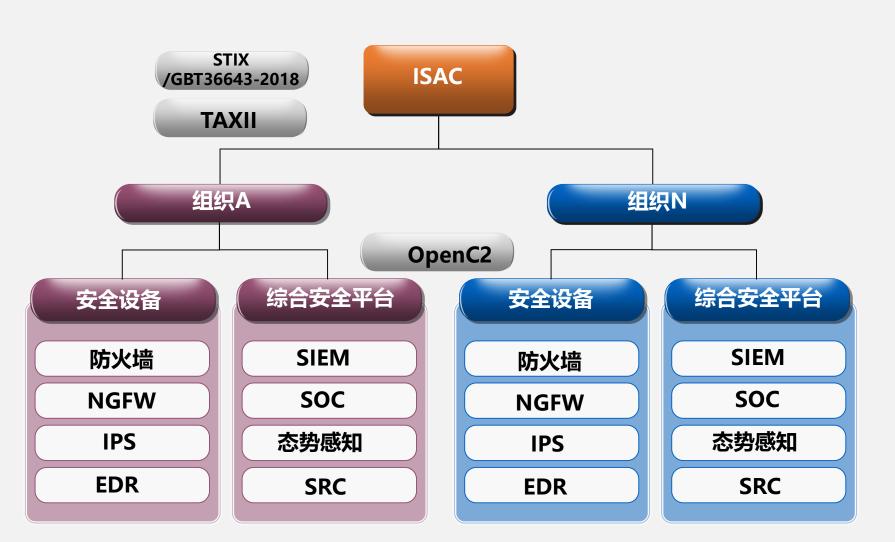


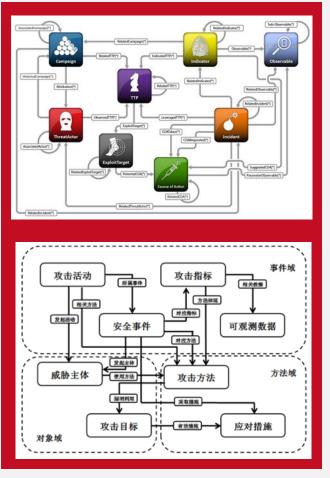


威胁情报应用的关键在于分享



基于"烽火"的思想,威胁情报才能够在主动防御中发挥更大价值





以情报应对安全运营的挑战





超负荷告警

通过环境内部的事件和相关指标来自动增加和 丰富外部数据,洞悉事件发生的细节,使用威 胁评分来进一步缩小数据集规模,例如:何人 于何时、何地、攻击了什么,为什么以及如何 进行的攻击等信息。

减少误报

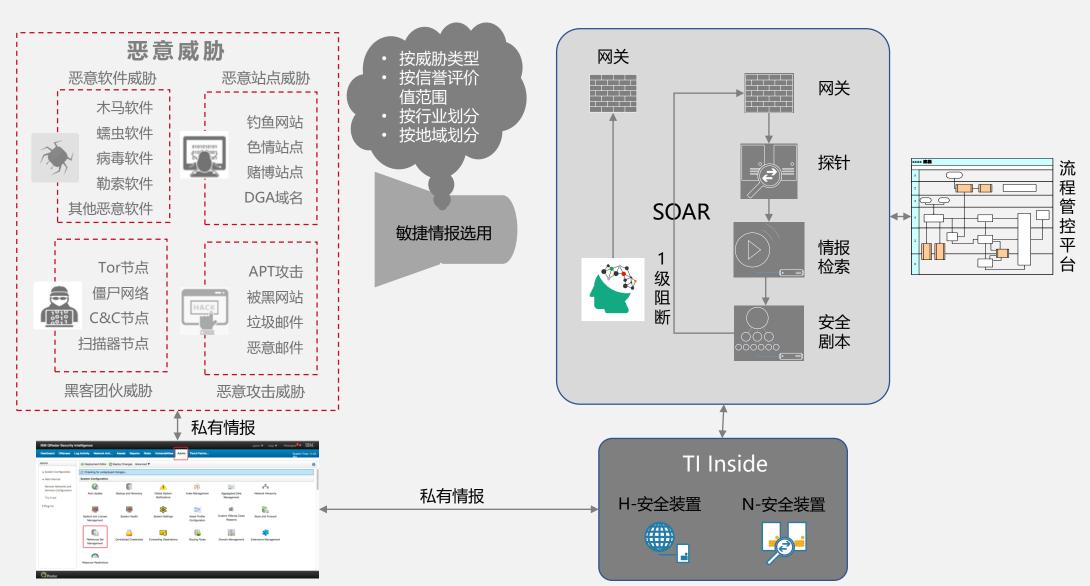
利用现有的案例管理工具或SIEM(安全信息和 事件管理)来自动共享相关的优先级威胁情报 这些系统可以更高效、更有效地执行优先级事 项,并减少误报。

主动防御

将整合的威胁情报直接导出到传感器网络(防火墙、防病毒软件、 IPS / IDS、网络和电子邮件安全、端点检测和响应以及NetFlow 等), 允许这些工具生成并应用更新的策略以降低风险。

威胁情报&主动防御-SOAR架构

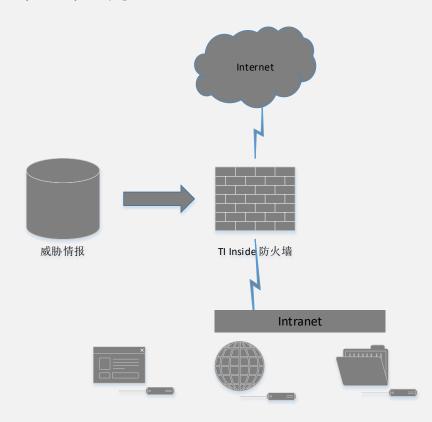




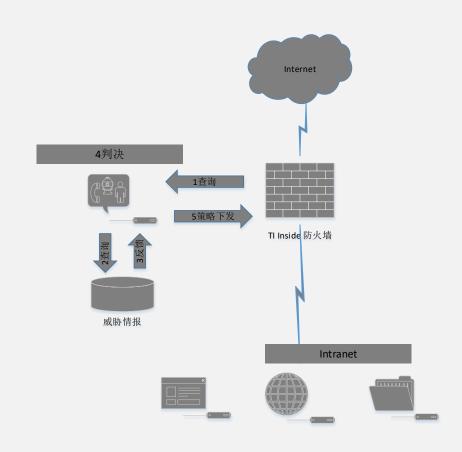
时间-主动防御的关键指标



"一步之差,天壤之别"

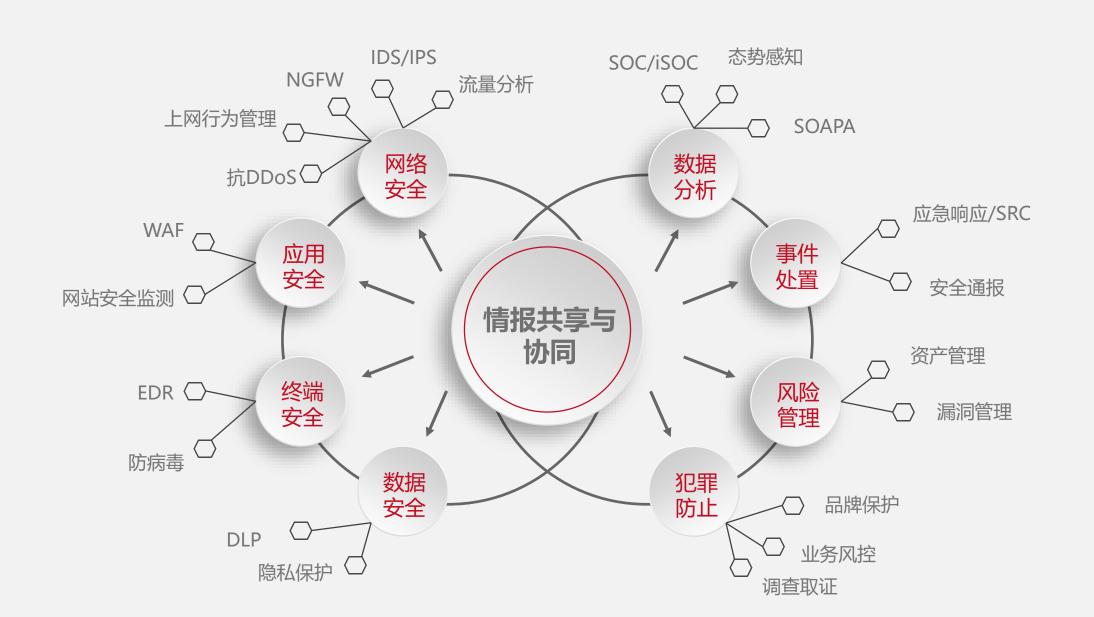


"情报嵌入"模式,威胁直接被阻断,避免了后续的潜在风险

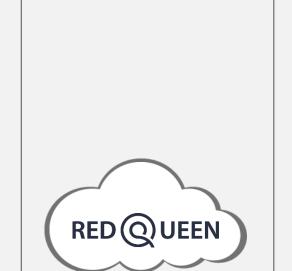


"查询-反馈"模式,时延是痛点,面临对手横向移动的风险

以情报共享促智能协同



检测/防护类安全设备







安全厂商更新源/ 用户情报平台



- …钓鱼、色情、赌博等站点的违规外联 与C&C、TOR、僵尸网络等相关的可疑外联

下行流量

- 过滤恶意、垃圾邮件
- 阻断外部扫描行为 切断恶意软件、勒索软件







- 实现外部情报与本地上/下行流量日志的命中匹配;
- 2、根据命中匹配结果,自动过滤恶意的访问和外联行为。



情报数据与安全管理平台的联动应用

情报输出



SIEM、态势感知等平台类产品



资产信誉 安全漏洞 病毒木马

上传溯源请求&返回溯源结果

定制化情报(国标格式)

数据泄露

资产发现

勒索软件

方式一:根据定制化情报直接形成事件告警,并依此为线索进行进一步的事件分析与处置。



C&C节点 垃圾邮件 木马软件

僵尸网络

可机读威胁情报 (MRTI)

方式二: 将可机读威胁情报 (MRTI) 入库, 完善事件检测与告警规则库, 并根据命中匹配结果进行基于情报的分类事件告警和分析。

方式三:通过溯源接口,借助云端的海量历史情报数据库进行威胁溯源和线索扩展。



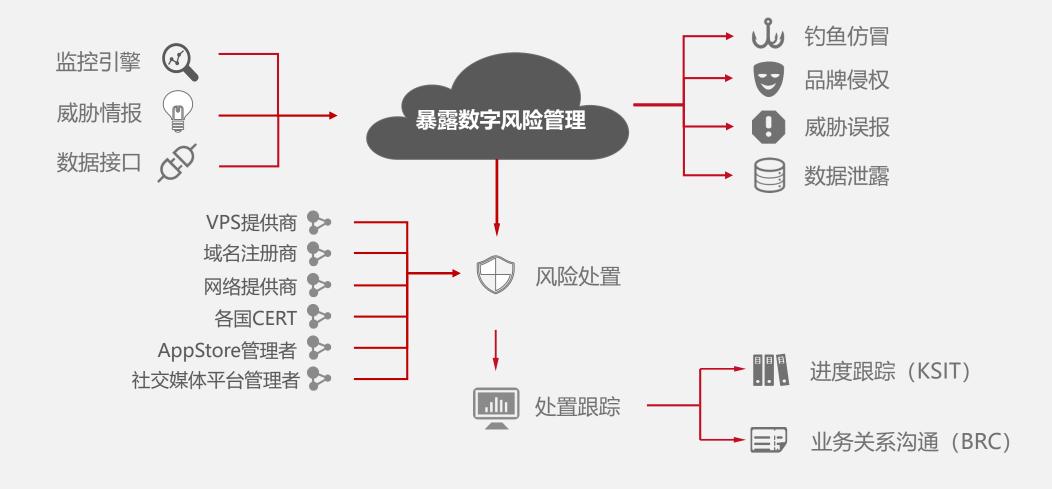


SOC/SIEM等平台类产品

威胁情报&主动防御-虽远必诛



面对外部风险, 主动防御是企业品牌维护的重要手段



可用于主动防御的指导框架



IPDRR (识别,保护,检测,响应,恢复)





迄今,天际友盟所处置的风险事件对象,遍布全球100多个国家和地区



风险事件处置对象所在的国家与地区排名

(截至2019年底的服务事件数量统计)

1	美国	16	罗马尼亚
2	中国香港	17	伊朗
3	南非	18	马来西亚
4	中国大陆	19	土耳其
5	新加坡	20	印度尼西亚
6	德国	21	西班牙
7	荷兰	22	中国台湾
8	英国	23	波兰
9	印度	24	越南
10	巴西	25	日本
11	加拿大	26	瑞士
12	澳大利亚	27	意大利
13	俄罗斯	28	乌克兰
14	法国	29	孟加拉
15	韩国	30	爱尔兰

安全情报驱动全面的数字风险防护



数字化转型, 使企业业务面临复杂多变的外部安全威胁



我们致力于协助企业解决在线业务的全方位数字风险



2020北京网络安全大会

2020 BEIJING CYBER SECURITY CONFERENCE

FELISE SERVICE BUSINESS WEAPONIZATE ALARM REPORT OF THE PROPERTY OF THE PROPER

全球网络安全 倾听北京声音







内生安全 从安全框架开始

ENDOGENOUS SECURITY: STARTING FROM A CYBERSECUR BY FRAMEWORK

威胁情报创新发展论坛 暨网络安全威胁情报生态联盟发布会

情报使能生态共赢

主办单位: 奇安信威胁情报中心、中国网络空间安全协会

协办单位:烽火台联盟、TIXA联盟

全球网络安全 倾听北京声音

圆桌研讨: TO B 企业安全市场

在各位专家领域里如何更好的消费威胁情报



嘉宾

汪列军

奇安信威胁情报中心负责人



嘉宾

权小文

远江盛邦CEO



嘉宾

马涛

网宿科技网络性能

主持人 李少鹏

数世咨询创始人



嘉宾

王雪松

志翔科技研发副总裁



嘉宾

周毅

派网软件产品总监



及安全事业部副总经理

嘉宾

张斌

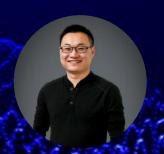
云溪智联创始人



嘉宾

林榆坚

安赛创想CEO



嘉宾

杨大路

天际友盟创始人



嘉宾

王伟

虎符网络CEO





内生安全 从安全框架开始

ENDOGENOUS SECURITY: STARTING FROM A CYBERSECUR BY FRAMEWORK

威胁情报创新发展论坛 暨网络安全威胁情报生态联盟发布会

情报使能生态共赢

主办单位: 奇安信威胁情报中心、中国网络空间安全协会

协办单位:烽火台联盟、TIXA联盟

全球网络安全 倾听北京声音