威胁情报的业务安全应用价值

杨大路　　北京天际友盟信息技术有限公司 CEO

2018 ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
（原中国互联网安全大会）

天际友盟 TianJi Partners

目录

安全管理者每天面对的安全挑战

持续不断的网络攻击

员工和第三方敏感数据泄露

有限的资源和安全人才

低效的工具

海量内部告警缺乏有效的排序

外部威胁缺乏有效的收集手段

大量的解决方案都只能解决单点问题

越来越多的安全问题发生在企业边界以外

安全事件发生时我们想要什么？

- 你的数据在网上曝光
- 重要员工遭到钓鱼攻击或被假冒
- 攻击者将你列为计划的目标
- 犯罪分子在暗网上出售数据
- 员工或供应商引发的网络风险
- 基础设施存在未修补的漏洞

不会产生误报，并有应对措施。

目录

每天面对的安全威胁和挑战

威胁情报支撑数字风险防护

如何开展数字风险防护工作

业务安全面对的主要数字风险

数据泄露

品牌风险

网络威胁

资产暴露

第三方风险

对这些情报的全面掌握，是做好数字风险防护的基础

数据泄露举例

- 客户和员工信息泄露
  - 个人身份信息
  - 金融卡号信息
  - 网络账号密码
  - 网络行为数据
- 商业秘密泄露
  - 商业计划
  - 规划&方案
  - 客户资料
  - 会议纪要
- 知识产权泄露
  - 源代码
  - 产品设计
  - 专利

品牌风险举例

- 网络钓鱼
  - 仿冒网站
  - 仿冒APP
  - 仿冒社交媒体账号
  - 仿冒邮件
- 社交媒体言论
  - 言论的过度传播
  - 假冒的言论
- 品牌滥用
  - 山寨网站
  - 假冒社交媒体资料
  - 假冒伪劣商品和礼品卡

网络威胁举例

- 以客户为目标
  - 恶意软件
  - 仿冒品
  - 诈骗
- 破坏可用性
  - DDOS攻击
  - 勒索软件
- 政治动机
  - 网站篡改
- 新型动机
  - 挖矿

资产暴露举例

数字签名

漏洞

开放端口

子域名&URL

第三方风险举例

供应链软件漏洞

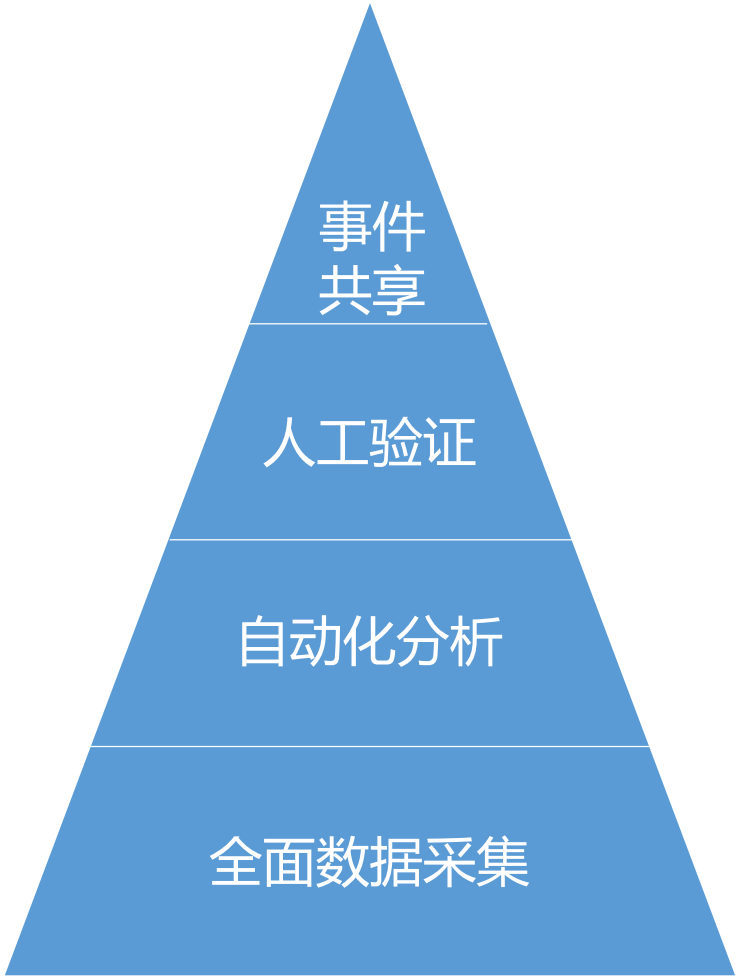
供应链诈骗

供应商数据泄露

供应商安全隐患

目录

我们的方法论及工作模型



主动出击、全面获取、快速共享

共享：通过系统、电子邮件提醒或API等方式，将相关的高优先级别的并具备可操作性的事件共享给相关部门。

人工分析：专家分析人员验证自动事件，排除误报，进行进一步研究，添加上下文，并指定严重级别。

自动化分析：利用数据科学、机器学习等手段，对数据进行去重、降噪、分类等工作

规划和收集：对互联网、深网及暗网上与公司资产相关的情报进行持续监控和自动化采集

数字风险防护的主要手段

数字资产管理

首要工作就是进行数字资产的识别和监控。结合企业实际业务，梳理当前阶段的数字资产清单，灵活运用各种技术手段（如爬虫等）对数字资产进行持续监控。

恶意对象处置

对恶意数字资产的发现和处置，比如钓鱼仿冒网站、仿冒APP、仿冒社交媒体账号、垃圾邮件账号等及时发现和快速关停。

负面信息监控

实施品牌负面信息监控，对主要媒体渠道的负面新闻、官方社交媒体评论中的用户投诉和有害信息（违法、暴力、政治评论等），企业的域名和IP被网络服务商或安全厂商列入黑名单，企业开发的软件、APP等被杀毒软件识别为病毒等情况进行全面监控。

负面信息解除

品牌负面影响消除能力，是数字风险防护的重要环节。

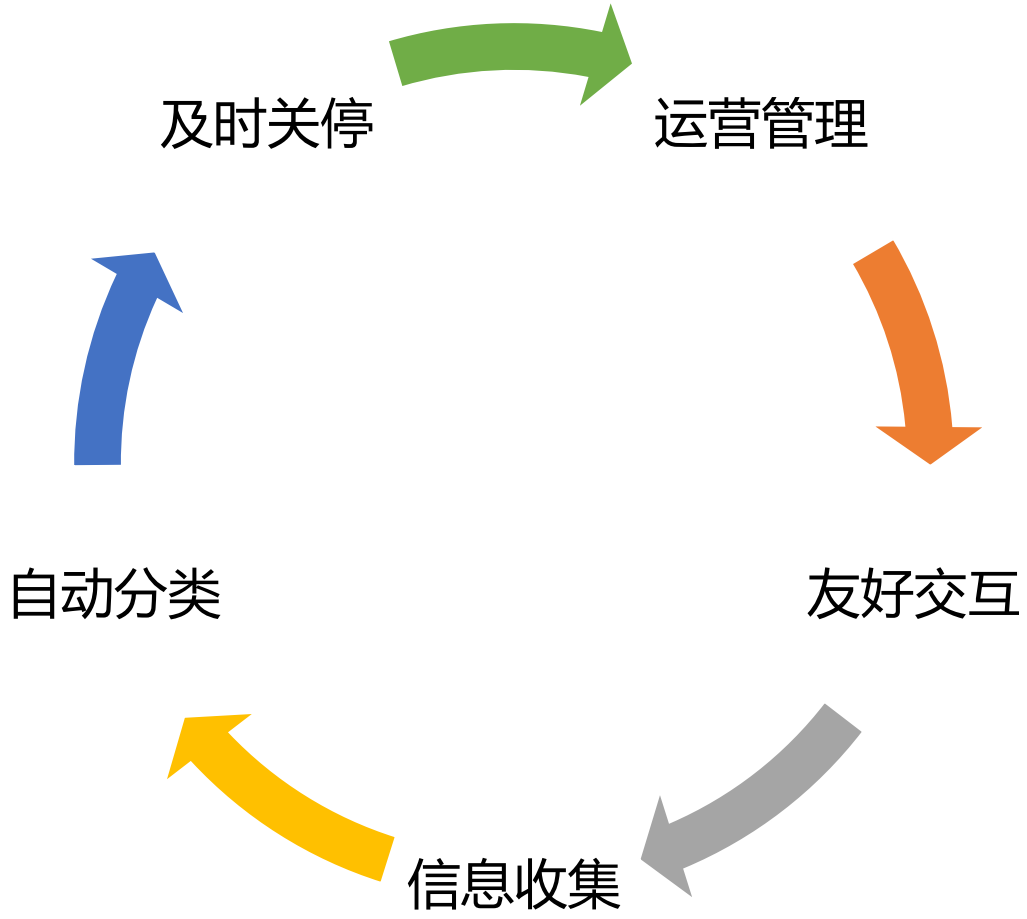
供应链安全管控

及时掌握供应链主要风险环节的情报，并能够结合自身业务快速评估风险，主动响应。

开展数字风险防护的能力要求

- 对仿冒网站、仿冒App、仿冒社交媒体账号、垃圾邮件账号等监测发现能力；
- 对上述监测到的事件进行快速关停的能力；
- 将企业拥有的IP和域名从黑名单剔除的能力；
- 企业软件或App被识别为病毒后，能够剔除误报的能力；
- 将公开渠道出现的敏感数据快速下线的能力；
- 对供应链全面安全监控的能力。

数字风险防护能力评价



天际友盟
TianJi Partners

ISC 2018
ISC互联网安全大会

360互联网安全中心

谢 谢！

2018 ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China
（原中国互联网安全大会）