借助威胁情报和自动化手段，提升防护处置能力

中国xxx集团有限公司 张三 182xxxxxxxx

一、利用情报收缩攻击面

1、背景与目的：

攻击队主要采用两种方式获取内网权限：一种是利用企业暴露在外的服务器端口和业务系统本身的0day或Nday，这些都是通过正常手段入侵内网，并通过横向移动获取整个内网。另一种是通过敏感信息收集，主要通过爬虫、暗网、GitHub、码云、文库等方式收集企业人员信息、业务系统代码、域名、用户名、证书等信息，进而配合钓鱼邮件或代码审计等计数手段，入侵内网。该技战法的主要目的是利用外部威胁情报监控能力和威胁情报关联，发现企业暴露在互联网上的服务端口以及企业泄露在公网的敏感信息如（邮箱、账户、密码、代码）等，指导安全运维人员收缩资产暴露面，并对泄露的账号密码进行提前加固整改。

2、防守思路：

企业相关的IP、域名资产与威胁情报基础信息pDNS关联，可以通过信息资产扩展发现企业未记录的资产。进而通过情报查询获取企业IP、域名资产开放的端口、关联的证书信息，因此安全运维人员可以通过此类方法收敛外网攻击面，同时安全运营人员可以通过关键字（例如：企业名称、简称、域名等敏感信息）在搜索引擎、fofa.so、zoomeye.org等检索与企业相关的敏感词，识别企业泄露在外的邮箱、账号、密码等信息。另外，还可以通过漏洞收集网站对业务系统进行检索如乌云、CVE漏洞库等获取当前版本业务系统存在的漏洞信息。企业安全运维人员可以根据收集的情报对业务系统、账号进行重点监控和加固。此技战法主要以攻击者的视角在演习前对企业暴露资产、泄露信息、存在的历史漏洞进行识别监控。

3、攻防对抗过程：

在网络安全防护演习正式开始前，一般要提前至少一到两周，根据企业现有IP、资产，利用市面上威胁情报查询服务平台或企业内部自由威胁情报平台，关联企业资产开放服务端口，并利用市场上外部威胁情报监控平台对企业相关的敏感信息进行识别。发现开放在互联网上且非必要服务端口、管理后台，进行及时关闭，并对无法关闭的端口和管理后台进行加固和重点监控。演习期间，由于大量的敏感数据和暴露端口已经进行清除或加固，绝大多数极易被利用的攻击面无法被红队利用，大大降低被攻破的几率。攻击队队如果利用尚未关闭的端口或管理后台或泄露邮箱进行攻击，安全运维人员可以对早已进行重点监控的脆弱点进行监控，及时触发告警，进行封禁和溯源。

4、应用效果：

经过本次演习，大多数攻击队都是利用暴露的端口、后台或敏感数据进行攻击，毕竟拥有0Day的攻击队并不多。该技战法可以在演习前全面收缩攻击面，最大程度避免演习中被攻破的几率。

二、通过自动化分析脚本对海量共享情报IP进行封禁

1、背景与目的：

经过综合研究分析，演习中情报共享是蓝队防守人员对抗红队攻击者的一个有效的防护手段，蓝队普遍的防御手段也是通过封禁IP来达到安全的目的，但是共享情报的来源并不是准确的，存在大量的误封现象，导致访问异常，而海量IP封禁也对防护设备是一个考验。面对共享情报中的海量攻击IP，如何有效区分存在威胁的Ip是企业遇到的难题。该技战法是利用某些威胁情报网站对HVV演习IP验证与溯源研判，快速筛选准确演习IP和值得溯源的IP，帮助企业进行有效封禁和针对性溯源。

2、思路：

结合情报白名单、IP关联签名及相关属性，并通过调用情报网站API接口进行自动化查询，自动匹配出存在威胁的IP或者剔除白名单IP、网关IP等，生成一份高可信的演习攻击IP，企业可以直接将经过自动化处理的IP进行封禁。针对IP是否关联域名、域名是否具备手机号或邮箱等注册信息，进一步对IP进行溯源价值研判分析。

3、攻防对抗过程：

利用情报共享交换群组或者第三方威胁情报厂商快速获取共享情报IP，并导入自动化分析工具。自动化分析工具根据威胁情报网站获取IP相应标签，去除带有CDN、移动基站、网关等IP。并结合IP关联签名信息，生成筛选后的共享情报IP，进而联动防火墙进行封禁，避免大量误拦或者拦截策略条目过多，导致防火墙过载。针对筛选出的共享情报IP，在进一步关联情报信息，例如IP是否关联域名、域名是否具备注册信息，并结合外部溯源价值验证接口，综合判定溯源价值。企业根据高价值IP进一步获取溯源加分。

4、应用效果：

避免面对海量IP盲目封禁，导致误拦或防火墙过载的风险。演习中，人员有限，面对海量的共享情报IP无法进行一一识别，使用自动化脚本可以初步筛选后再导入，大大减少了IP误封数量，另外分析处置人员资源有限，面对每天上千僵尸网络的攻击，无法进行实时封禁，可通过态势感知或威胁感知设备API接口信息采集，实现自动化封禁，减少安全运维人员的工作压力，可以让更多的人力资源加入到分析溯源工作中去，从而实现溯源得分。