应急响应问题解答

（1）dns 报警就一定是感染了吗？怎么处理?

不一定。

引起dns报警的情况有：恶意软件感染，域名劫持，DNS欺骗，DDoS攻击等。

处理方法：

1、分析报警，查看报警类型、源IP地址、目标域名等，分析确定是否存在异常或潜在威胁。

2、流量分析

3、查看日志

4、利用威胁情报平台查看相关的IP地址、域名或URL是否被标记为恶意或可疑的。

5、响应和隔离

（2） 公网 ip 未流量交互，内网报警是什么情况？怎么处理

情况：

1、内部恶意活动引起的，如未经授权的访问、数据泄露等。

2、内部网络被入侵

3、内部配置问题，如防火墙设置，IDS配置错误等。

处理：

1、分析报警：报警类型、源IP地址、目标IP地址等。

2、流量分析：查看内部网络中的通信活动，包括源和目标IP地址、协议和端口等，以确定是否存在异常或恶意活动。

3、日志分析：检查内部设备的日志

4、内部调查：确定是否是内部用户活动引起的

5、隔离和响应

（4） 设备报警，显示 127.0.0.1 会有哪些原因？怎么处理?

问法 2：互联网 ip 攻击，但是流量中显示的是内网 ip，如何找到真实 ip

朋友 1：搭隧道被发现了

朋友 2：可能反向代理，探针

（5） 一台主机在内网进行横向攻击，怎么处理

问法 2：内网 ip 横向渗透怎么处理?

查看是否是误报，如果不是误报采取以下措施

1、隔离受感染的主机

2、收集证据：收集有关攻击的证据，包括日志、网络流量、被修改或受感染的文件等。

3、确定攻击的方式和方法，采取措施停止攻击行为。

4、清除恶意代码，更新和修补系统，密码和凭证重置，安全审查和加固。

（6） 态势感知中，实际的攻击的时候是公网 IP？为啥告警里写着是 内网 IP？如何去找真实 IP？以及会出现这样状况的原因有哪些

朋友 1：设备位置装错了

攻击流量可能经过了网络地址转换（NAT）或代理服务器等设备，导致告警显示为内网IP。

1、网络流量分析

2、日志分析

态势感知平台有一条告警，你会怎么去分析

查看告警详情，攻击类型，源IP分析，目的IP分析等，利用威胁情报平台分析

（7） 遇到一个挖矿病毒，你会怎么处理?

判断(第一步先判断)

1.查看cpu占用率(判断CPU占用率高不高)

2.查看天眼的流量分析，是否去别的有危险的网站下载东西，然后在本地执行了挖矿的一些命令:

(结合天眼设备分析，看是否去可疑网站下载过东西或在本地执行挖矿命令)

3.是否有外连，向远程ip的请求:(是否有外连或者远程ip请求 netstart –ano 查看所有端口)

事件分析(第二步分析)

(1)登录网站服务器，查看进程是否有异常;(查看网站服务器是否有异常进程 系统命令tasklist)

(2)进行查看异常进程的服务项是什么.选择可疑服务项，然后停止服务，其启动类型会变为静止。(并查看它的服务项，尤其是可疑服务项(系统命令services.msc查看服务项))

(3)进行查看一下计划任务有没有可疑的(查看一下有没有可疑的计划任务)

3、临时解决方案(最后解决并处置)

(1)停止并禁用可疑服务项，有时候服务项的名称会变，但描述不会变，根据描述快速找到可疑服务项，删除服务项;(然后根据描述寻找可疑服务项，停用可疑服务项)

(2)根据实际存在木马的路径，进行删除木马(如果知道木马路径的话，直接删马)

(3)重启计算机;

(4)使用杀软全盘查杀

（8） 知道一个恶意攻击我们的域名，反查域名后得到一个 IP，但是 此 IP 没有和我们交互流量，请问原因是什么

1、转发或代理服务器：攻击者可能使用转发或代理服务器作为中间节点来隐藏其真实IP地址。这样，攻击流量会经过转发或代理服务器，而不是直接与我们的系统交互。

2、假冒IP地址：攻击者可能使用了虚假的IP地址进行攻击，以隐藏其真实身份和来源。

3、攻击者未成功进入系统：尽管发现了恶意攻击的域名和相关IP地址，但攻击者可能尚未成功进入系统或发起有效的攻击。

判断误报

首先看ip是内网ip还是外网ip

1）如果是内网ip，并且有明显的恶意请求，比如ipconfig那么此内网服务器可能会失陷。还有可能就是内网

的系统有一些业务逻辑问题，因为内网在部署的时候很少会考虑一些安全问题。比如说内网的业务逻辑携带了

一些sql语句，这一类属于误报

2）如果是外网ip，根据请求报和响应包的内容进行对比判断。比如sql语句查询用户名密码，然后响应包返回

了相应的内容，这一类是属于恶意攻击。

（9） 文件上传数据包如何判断是不是攻击

1、查看响应体响应结果判断服务器是否接受了该上传请求，上传成功通常状态码为200，查看响应体中是否响应了上传路径，访问该上传路径查看文件是否被解析是否存在

2、通过查看日志判断文件是否落地

3、登陆受害者主机全局搜索上传文件

流量层面分析Apache Log4j2 远程代码执行漏洞是否攻击成功?

1、dnslog类:查看是否存在源ip与dnslog的外联日志记录

2、命令执行攻击

2.1 有回显:响应体中存在命令执行结果

2.2无回显 :存在源ip与ldap服务ip的外联日志记录

如何研判JBOSS 反序列化漏洞攻击成功?

1.在访问JBOSS漏洞页面/invoker/readonly后，返回值为500

2.请求体有collections.map.LazyMap、keyvalue.TiedMapEntry攻击链特征并且有明显的命令执行行为，比如whoami。

3.在返回500 堆栈报错页面内容中包含了系统返回内容 比如系统用户:root

如何研判Fastjson反序列化漏洞攻击成功?

1.请求头:method: POST content_type: application/json

2、请求体：data:com.sun.rowset.JdbcRowSetImpl,dataSourceName,@type

3.请求体: 包含攻击者C2服务器地址

4.状态码为:400 也可能是500

5.通过天眼分析平台进行回溯分析，在分析中心输入语法:(sip:(失陷服务器P)OR sip:(攻击者C2IP)AND(dip:(失陷服务器IP)OR dip:(攻击者C2IP)

如何在流量层面分析struts2命令执行是否成功

1.查看请求头或请求体中是否含有OGNL表达式，Struts2 命令执行的原理是通过Ognl表达式执行 java 代码

2.查看请求头或请求体中是否存在命令执行类代码

3.查看响应体是否返回上述命令执行的结果

要判断Log4j漏洞攻击是否成功，可以采取以下措施

监视受感染应用程序的日志，查看是否有异常或错误信息，或者是否包含与攻击相关的信息。
监视网络流量，查看是否有大量的请求被发送到攻击者的服务器。
检查系统中的异常或警告信息，例如系统崩溃、不正常的CPU使用率或内存使用率等。
在受感染的系统中进行代码审查，查看是否有与攻击相关的代码或配置文件。

负载均衡 XFF 头里有 IP0 IP1 IP2，请问哪个是真实 IP?

X-Forwarded-For头信息可以有多个，中间用逗号分隔，第一项为真实的客户端IP，剩下的就是曾经经过的代理或负载均衡的IP地址。

`X-Forwarded-For: client1, proxy1, proxy2`

因此为IP0

溯源思路

首先通过系统日志、安全设备截获攻击包等从中分析出攻击者的ip和攻击方式，通过webshell或者木马去微步分析，或者去安恒威胁情报中心进行ip检测分析，是不是云服务器，基站等，如果是云服务器的话可以直接反渗透，看看开放端口，域名，whois等进行判断，获取姓名电话等丢社工库看看能不能找到更多信息然后收工

设备

IPS

IPS代表入侵防御系统（Intrusion Prevention System），它不仅可以检测入侵行为，还可以主动采取措施进行防御。

IDS

IDS代表入侵检测系统（Intrusion Detection System），它通过监视网络流量、日志和系统事件来检测潜在的入侵行为。IDS基于预定义的规则或行为模式，分析网

络流量和事件，以发现可能的安全漏洞、异常行为或已知攻击的迹象。一旦检测到可疑活动，IDS会生成警报通知相关人员进行进一步的调查和响应。

蜜罐

部署一些作为诱饵的主机，诱使攻击方对蜜罐进行过攻击，对攻击方的攻击行为进行捕捉和分析，了解攻击方使用的工具和方法，从而增强增强真实系统的安全防护能力。

WAF

web应用防火墙，专门针对于HTTP和https请求，对客户端的请求内容进行检测，确保其合法性和安全性，还会对非法的请求进行及时的阻断。

天眼的使用

主要用天眼进行流量分析和流量监控，并且可以用他的日志检索模块进行溯源。

检索语法

dip ： 被攻击的 ip

dport： 被攻击的端口

sip：源ip

sport：源端口

uri ： 请求的 url 地址

data：请求包的正文内容

status：响应包的状态码

host：域名

client_os 系统 运算符 AND(AND或&&或+)OR(OR或||)ix.NOT(NOT或!或–)

天眼构成

①流量传感器(探针)②文件威胁鉴定器(沙箱)③分析平台④天擎(若有)

天眼菜单界面

流量传感器:状态监听，威胁告警，规则配置，策略配置，系统配置

分析平台:威胁感知–告警列表，分析中心–日志检索

告警类型

企图;成功;失陷;失败

天眼或者传感器上出现 命令执行告警，怎么应对?

1、验证此条告警是否真的成功?(成功的话，直接就可以出报告了)

2、失败的话，判断攻击者是手工还是扫描工具批量行为?

3、进入分析平台进一步分析，查看分析平台攻击IP除了文件上传以外是否存在其他攻击行为，攻击结果如何?

4、将发现时间及攻击行为反馈给护网客户

如果天眼设备上短时间内有大量告警，你会怎么进行分析?

根据轻重缓急进行筛选查看，从高危到低危，从命令执行到目录遍历这种等

天眼日志检索功能使用

1、在“分析中心”–“日志检索”模块，选择“高级模式”–“web访问”，再填写检索语句，再点击搜索

2、如果不知道具体的描述字段名?

在日志检索页面的左边，有一个展示字段，也就是说我们需要去记字段名，我们可以通过可视化界面把需要的字段进行选中，点点点就行了

天眼怎么判断受到了攻击?

规则库匹配，给出告警

天眼使用流程

1、天眼的作用

1.1、从部署角度来讲：首先是从核心交换机上镜像流量到探针，探针内部有规则库，会进行第一波分析，然后分析的结果会交给分析平台处理，然后分析进行整合

1.2、从使用者的角度：在“威胁感知–告警列表”里面进行筛选，进行有针对性的分析

2、攻击结果分为：失败(0)–企图(1)–成功(2)–失陷(3)

3、威胁级别分为：低危–中危–高危–危急

4、首先打开“威胁感知–告警列表”，然后筛选出成功和失陷的告警，然后筛选出威胁级别为高危和危急的告警

5、然后对每条告警进行分析：需要注意五元组信息：源IP、源端口、目的IP、目的端口、协议，然后就是对数据包进行分析

6、天眼的升级（包含探针/分析平台的规则库和系统升级）

6.1、天眼支持在线升级和手动导入升级包的方式进行升级，客户基本上都是手动升级，因为在线升级需要开策略，比较麻烦，一个是访问公网的行为比较危险

6.2、手动升级步骤：从天眼公有云系统（https://user.skyeye.qianxin.com/user/sign–in?next=https%3A//cloud.skyeye.qianxin.com/login）上下载最新的升级包，然后在天眼的系统设置里的升级栏里面导入升级包进行升级