360政企学院

专业版

360高级持续性威胁预警系统

目录

01

标题

需求背景与产品定位

政策和法规要求

网络安全从“被动防御”向“主动检测与响应”转变！

网络安全法

“第三十一条、第五十一条、第五十三条”要求：
构建网络安全监测分析平台，并具备威胁检测、应急响应、事件处理等安全控制能力。

等保2.0

等保基本要求8.1.3.3章节：应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。
等保测评要求：测评对象需具有抗APT攻击系统、网络回溯系统等相关组件。

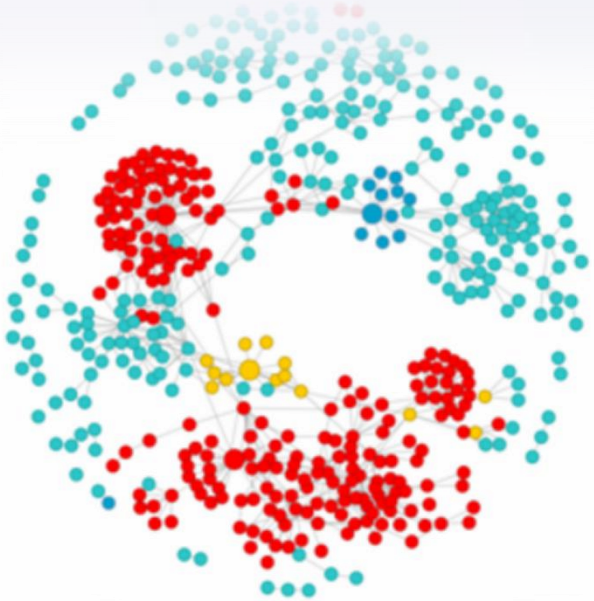
护网行动/深网行动

针对国家基础设施、重保单位的专项行动成为网络监管工作的又一重要抓手。

安可联盟

安全可靠技术与产业联盟在国产化安全方面已成为重要推手。

网络安全影响国家安全



被攻击范围广

涉及党政机关、科研院所、军队/军工、金融、运营商、能源等单位

危害严重

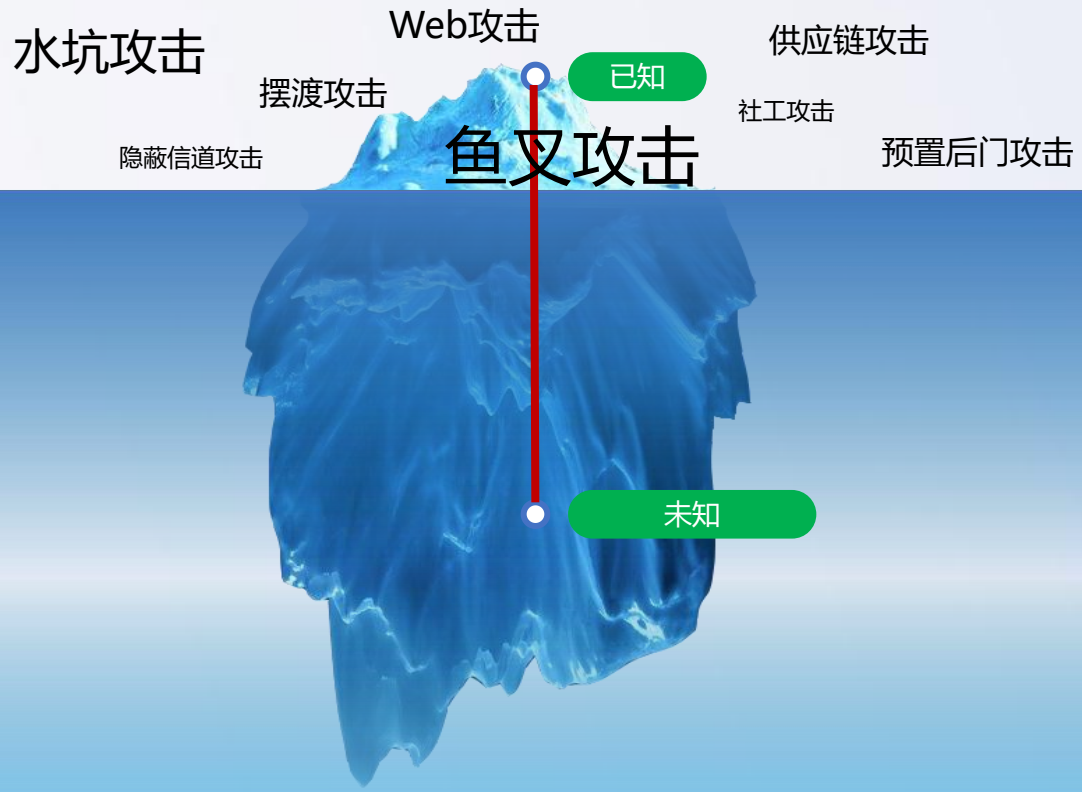
攻击者对我方网络长期进行数据窃取、远程控制、网络制毁等恶意行为

危及国家安全

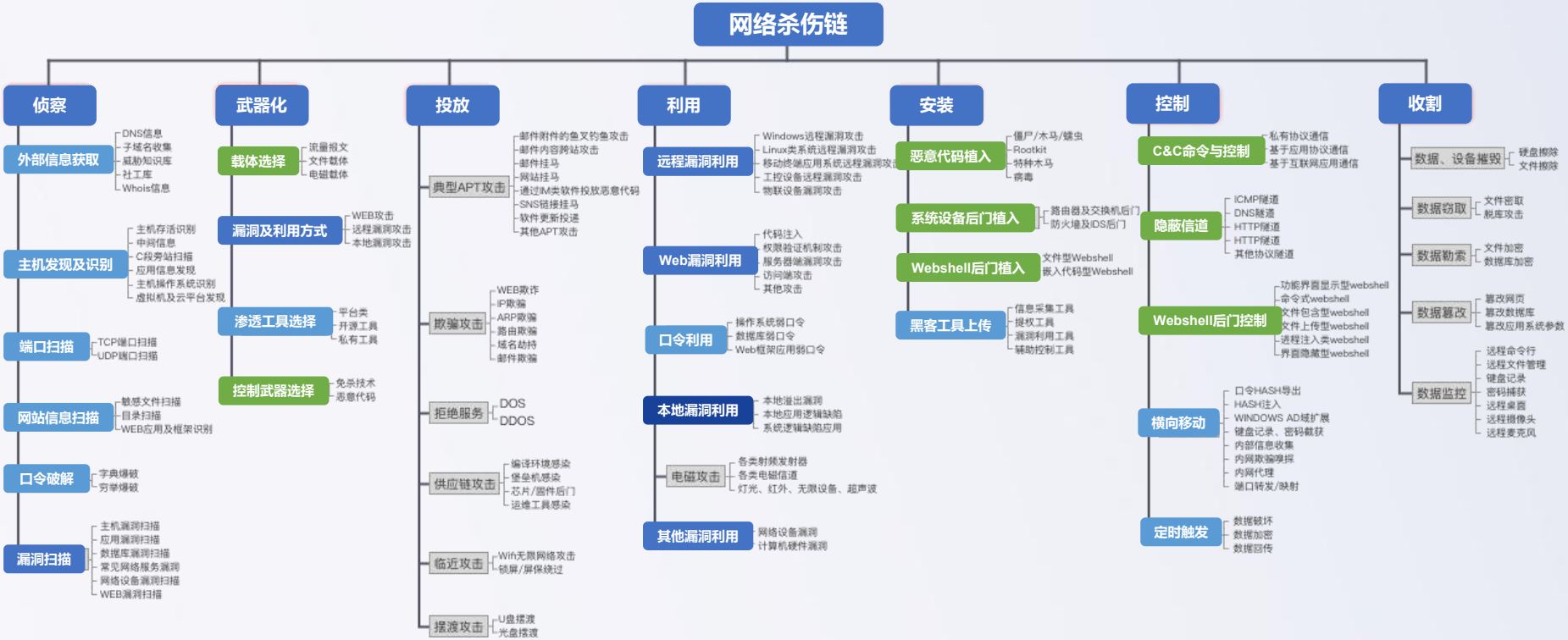
多数被监测单位的网络存在被控制或曾经被控制行为

没有网络安全就没有国家安全，提升网络安全防御能力是中国走向网络强国的必经之路

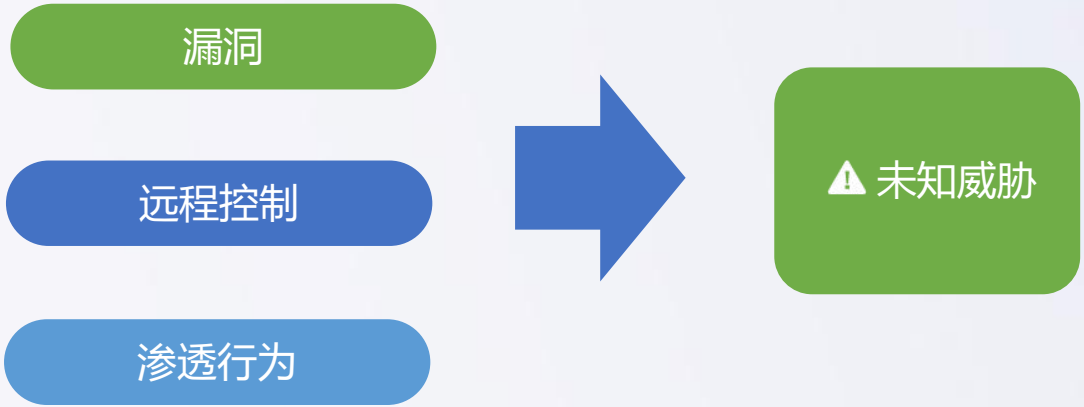
网络安全防护工作是持久战



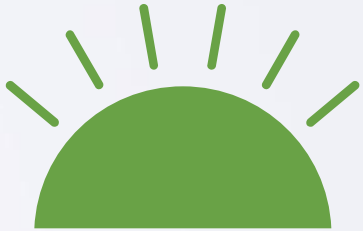
网络攻击杀伤链


网络杀伤链
侦察
外部信息获取
DNS信息
子域名收集
威胁知识库
社工库
Whois信息
主机发现及识别
主机存活识别
中间信息
C段旁站扫描
应用信息发现
主机操作系统识别
虚拟机及云平台发现
端口扫描
TCP端口扫描
UDP端口扫描
网站信息扫描
敏感文件扫描
目录扫描
WEB应用及框架识别
口令破解
字典爆破
穷举爆破
漏洞扫描
主机漏洞扫描
应用漏洞扫描
数据库漏洞扫描
常见网络服务漏洞
网络设备漏洞扫描
WEB漏洞扫描
武器化
载体选择
流量报文
文件载体
电磁载体
漏洞及利用方式
WEB攻击
远程漏洞攻击
本地漏洞攻击
渗透工具选择
平台类
开源工具
私有工具
控制武器选择
免杀技术
恶意代码
投放
典型APT攻击
邮件附件的鱼叉钓鱼攻击
邮件内容跨站攻击
邮件挂马
网站挂马
通过IM类软件投放恶意代码
SNS链接挂马
软件更新投递
其他APT攻击
欺骗攻击
WEB欺诈
IP欺骗
ARP欺骗
路由欺骗
域名劫持
邮件欺骗
拒绝服务
DOS
DDOS
供应链攻击
编译环境感染
堡垒机感染
芯片/固件后门
运维工具感染
临近攻击
Wifi无限网络攻击
锁屏/屏保绕过
摆渡攻击
U盘摆渡
光盘摆渡
利用
远程漏洞利用
Windows远程漏洞攻击
Linux类系统远程漏洞攻击
移动终端应用系统远程漏洞攻击
工控设备远程漏洞攻击
物联设备漏洞攻击
Web漏洞利用
代码注入
权限验证机制攻击
服务器端漏洞攻击
访问端攻击
其他攻击
口令利用
操作系统弱口令
数据库弱口令
Web框架应用弱口令
本地漏洞利用
本地溢出漏洞
本地应用逻辑缺陷
系统逻辑缺陷应用
电磁攻击
各类射频发射器
各类电磁信道
灯光、红外、无限设备、超声波
其他漏洞利用
网络设备漏洞
计算机硬件漏洞
安装
恶意代码植入
僵尸/木马/蠕虫
Rootkit
特种木马
病毒
系统设备后门植入
路由器及交换机后门
防火墙及IDS后门
Webshell后门植入
文件型Webshell
嵌入代码型Webshell
黑客工具上传
信息采集工具
提权工具
漏洞利用工具
辅助控制工具
控制
C&C命令与控制
私有协议通信
基于应用协议通信
基于互联网应用通信
隐蔽信道
ICMP隧道
DNS隧道
HTTP隧道
HTTPS隧道
其他协议隧道
Webshell后门控制
功能界面显示型webshell
命令式webshell
文件包含型webshell
文件上传型webshell
进程注入类webshell
界面隐藏型webshell
横向移动
口令HASH导出
HASH注入
WINDOWS AD域扩展
键盘记录、密码截获
内部信息收集
内网取验弹探
内网代理
端口转发/映射
定时触发
数据破坏
数据加密
数据回传
收割
数据、设备摧毁
硬盘擦除
文件擦除
数据窃取
文件密取
脱库攻击
数据勒索
文件加密
数据库加密
数据篡改
篡改网页
篡改数据库
篡改应用系统参数
数据监控
远程命令行
远程文件管理
键盘记录
密码捕获
远程桌面
远程摄像头
远程麦克风

网络攻击核心三要素



产品定位



面对层出不穷、复杂多样的未知攻击技术，传统防御手段已经无能为力

基于 **大数据、人工智能和网络攻防对抗** 思想的主动检测与响应体系应运而生

产品定位 - 网络攻击检测与响应(NDR)

360高级持续性威胁预警系统（360NDR）

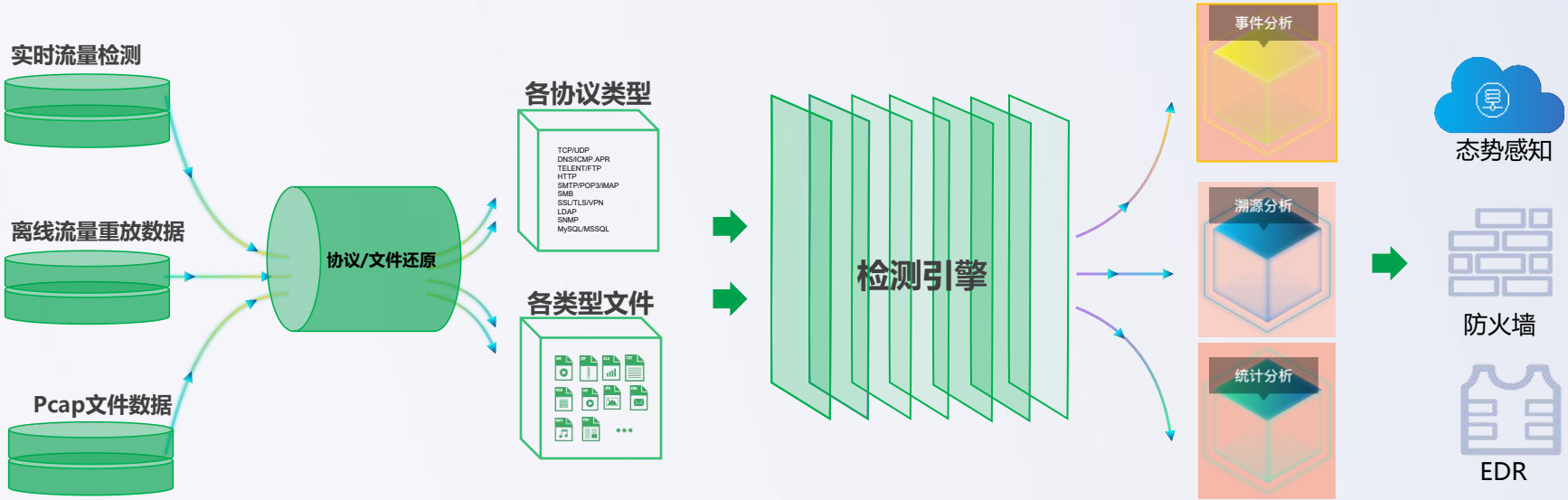
一款专门应对**高级网络威胁**的新一代智能安全产品。产品**旁路部署**在网络出口处，通过对网络进出流量进行监测和深度分析，检测**网络攻击、病毒木马**及**渗透行为等**攻击行为，帮助用户及时发现攻击行为和失陷主机情况，并深入分析攻击者的攻击途径、关联关系等，帮助用户进行快速响应、攻击溯源。

02

标题

主要功能与产品优势

工作原理



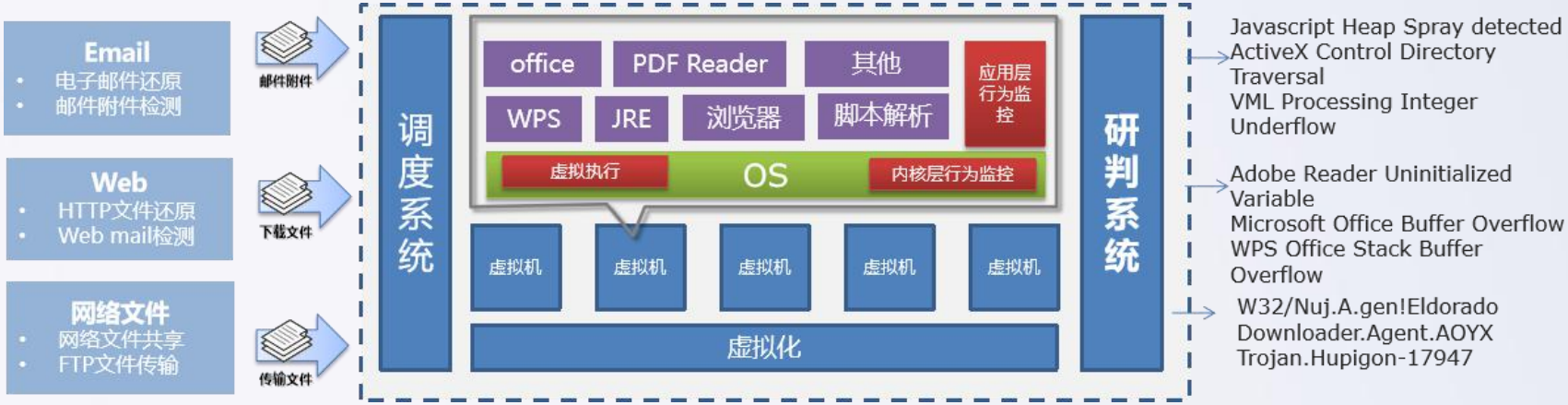
流量采集 → 数据还原 → 威胁检测 → 分析溯源 → 响应

检测功能

分类	特征检测	行为检测	威胁情报	AI/机器学习
流量	• 恶意代码通信 • 漏攻攻击 • web攻击 • **webshell通信**	• **DNS隐蔽信道**	• 黑白IP • 黑白域名 • 黑URL	**NA**
文件	• 杀软 • **webshell检测**	• **沙箱检测**	• 黑白HASH • C2地址	• **PE文件** • **PDF文件** • office文件 • PE恶意文件分类

沙箱检测

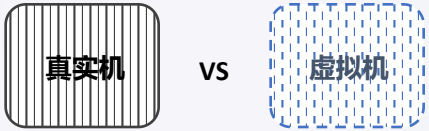
沙箱综合了多种恶意文件检测技术，其根据文件的**静态信息、可疑行为综合**判定，用于识别网络攻击中的已知木马和免杀木马、特种木马。



- 支持PE、脚本、网页文件、PDF、office文档、wps文档、JAVA、APK、压缩包等**近70种文件格式**检测
- 不用频繁更新规则库，**隔离网络**同样适用
- 提供恶意文件的**详细行为**，分析师可以**复核**，也便于提取**威胁情报**内容

沙箱逃逸

“差异性”是逃逸的关键



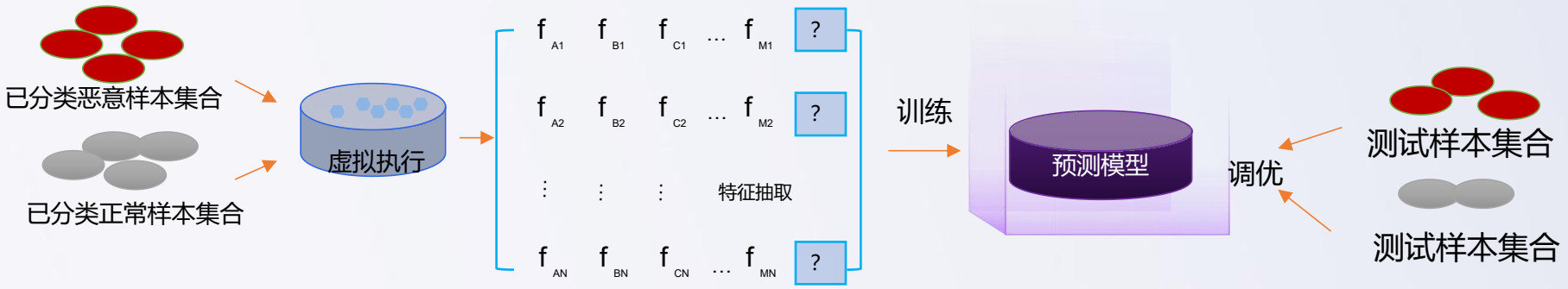
逃逸技术的核心原理：

寻找虚拟机和真实环境的差异性，发现是在虚拟机中就直接退出或执行正常代码。

能够检测三类共200+种逃逸手段

用户交互差异性	--执行路径 --输入操作 --使用痕迹	✓ 优化样本在虚机内的存放路径，调整样本执行的父进程 ✓ 模拟随机键盘、鼠标移动操作，以及有针对性的鼠标点击操作 ✓ 模拟用户对系统的使用痕迹，包括文档打开、浏览器记录等 ✓ ……
运行环境差异性	--虚拟机指纹 --特殊指令 --系统运行特征	✓ 检测在注册表中搜索VMware等字符串的行为 ✓ 修订硬件资源标识（内存大小、MAC地址、驱动信息等） ✓ 检测虚拟机特权指令调用行为、检测SIDT指令探测IDT基址 ✓ 检测对LDT和GDT的探测、检测STR指令探测TSS ✓ 修订系统软件标识（ComputerName、运行时长等） ✓ ……
业务逻辑差异性	--各种超时机制 --各种Hook探针	✓ 检测RDTSC指令探测CPU运行周期数 ✓ 压缩样本“睡眠”时间，优化对重启生效的样本检测能力 ✓ 使用更隐蔽的Hook方式隐藏探针的存在 ✓ ……

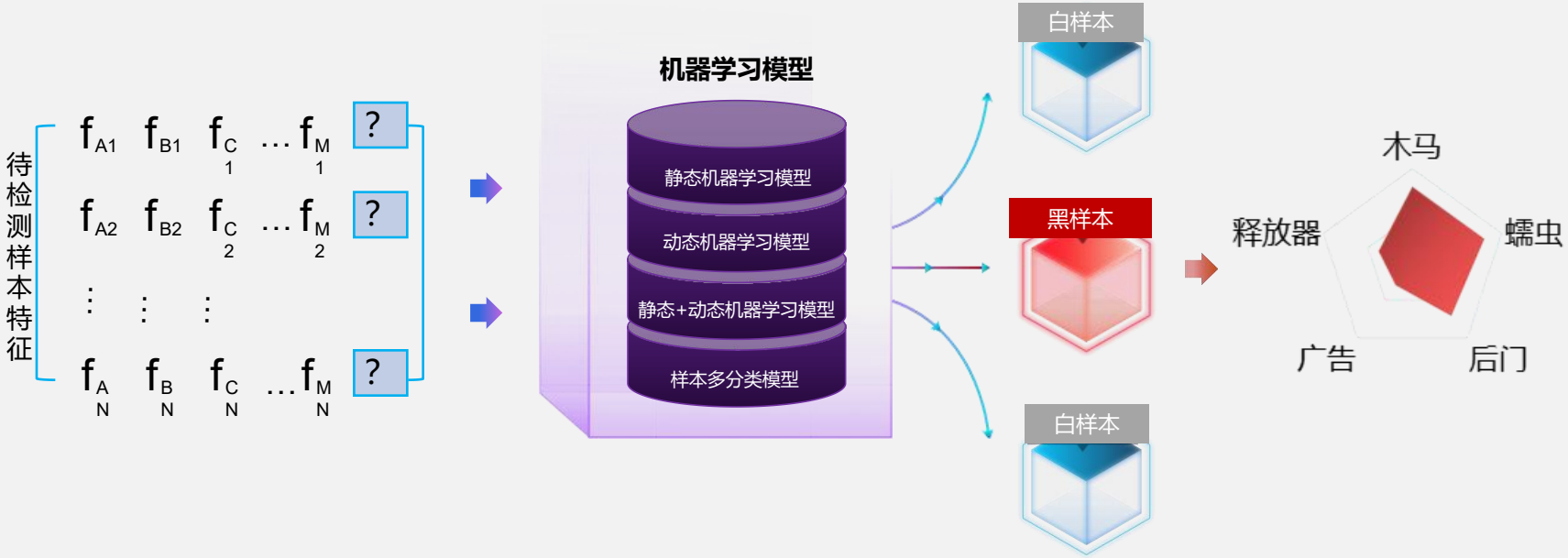
机器学习（学习过程）



场景	算法	输入	向量特征	预测模型	模型准确率
PE文件检测	随机森林	若干恶意PE样本	• 样本静态信息 • 样本动态行为信息	• 静态特征训练的模型 • 动态行为特征训练的模型 • 静态+动态特征一起训练的模型	96%+
PDF文件检测	随机森林	若干恶意PDF文件	• 关键字段信息 • JavaScript代码特殊函数或特殊字符串	pdf文档 静态特征训练的模型	99.77%
OFFICE文件检测	xgboost+逻辑回归	若干恶意OFFICE文件	• 样本触发的各种规则信息 • 样本包含的宏信息	office文档动态特征训练的模型	98.81%
PE恶意文件文件分类	softmax算法	Adware, Backdoors, Dropper, Trojan, Worm共计5类恶意代码	• 文件大小，节信息，签名信息，证书信息 • 调用的API	5类PE文件分类模型	96%+

机器学习（检测过程）

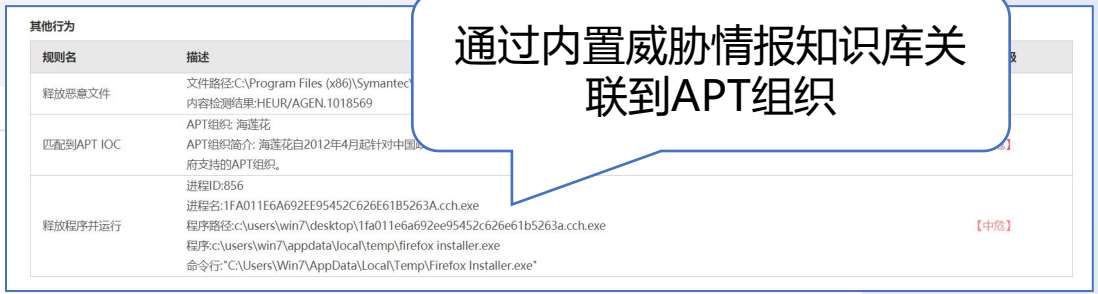
利用预置高检出率的**机器学习算法模型**，预测文件的**恶意程度**和**恶意文件所属分类**，可检测**未知恶意代码。**



- PE、office和PDF三类格式分开做模型，检测结果更准确
- 无须频繁更新规则库，可检测未知恶意文件，适用**隔离网络**

恶意文件检测 - 案例

APT组织（海莲花）攻击样本



通过内置威胁情报知识库关联到APT组织

检测总结 静态信息 动态信息 分析信息

检测信息: 1FA011E6A692EE95452C626E61B5263A.cch

威胁等级: 【高危】

HASH检测结果: 未检测到

行为分析结果: 【高危】

内容分析结果: HEUR/AGEN.1009557【威胁情报分析】

YARA检测结果: 无

机器学习检测结果:
模型【rf_pe_static_001】检测出威胁概率为98%
模型【rf_pe_dynamic_001】检测出威胁概率为34%
模型【rf_pe_sdynamic_001】检测出威胁概率为44%

机器学习研判模型

CVE检测结果: null

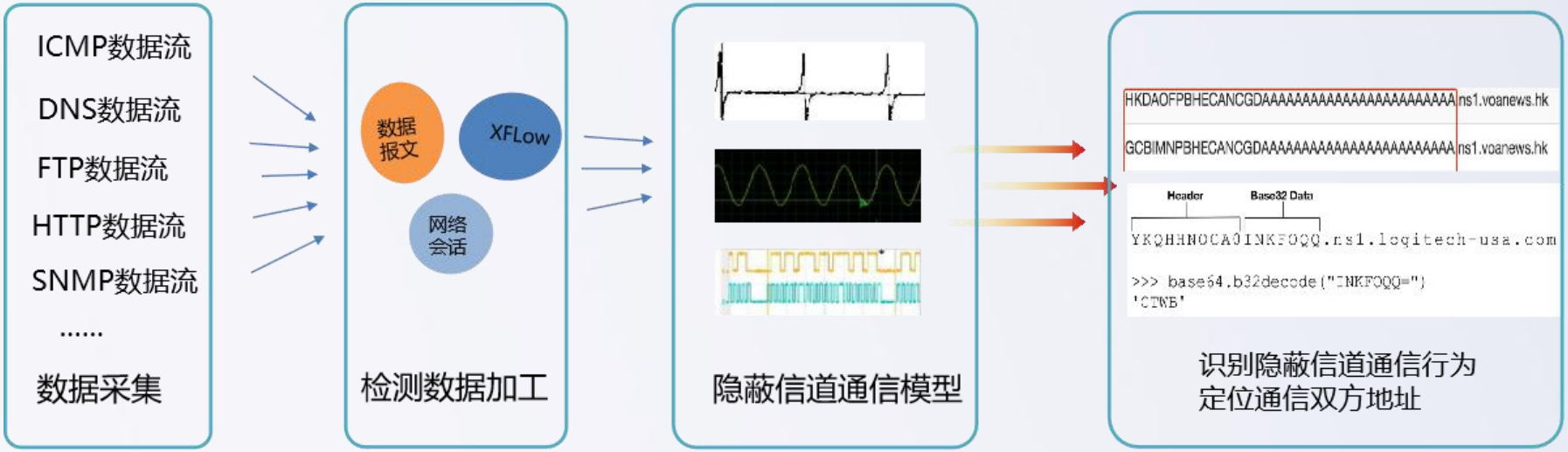
检测描述:
释放恶意文件 | 匹配到APT IOC | 释放PE文件到temp目录 | 修改IE浏览器代理设置 | 通过com服务添加任务计划程序 | 疑似尝试获取硬盘空间大小来探测虚拟机
分配可读可写可执行的内存块 | 调用ShellExecute创建进程 | 调用CreateProcess创建进程 | 获取用户名 | 疑似尝试获取内存大小来探测虚拟机 | 尝试连接网络主机
释放程序并运行

隐蔽的自启动行为

沙箱逃逸行为

隐蔽信道检测

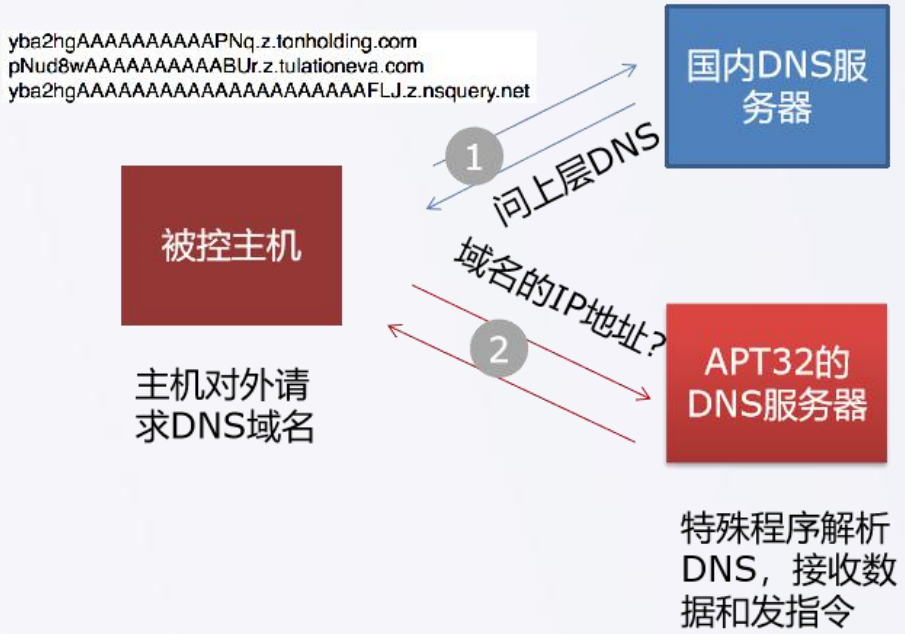
木马等利用正常访问协议进行隐蔽通讯、数据传输来躲避传统安全产品检测。隐蔽信道检测通过对协议中特殊字段、访问频率、访问内容进行分析和，形成不同分析模型，用于识别未知恶意代码通信。

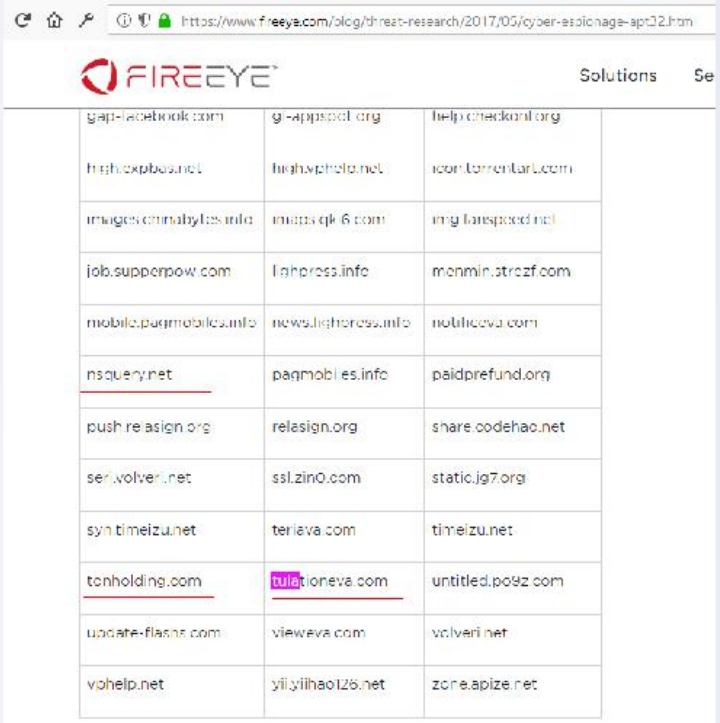


- 产品支持DNS隐蔽信道检测，支持检测Lable传输、TXT字段传输和NULL传输。
- 基于行为和模式匹配，无须频繁更新特征，隔离网络也适用。

隐蔽信道检测

2017年4月， 利用DNS隐蔽信道检测技术捕获到APT32组织（由国家赞助的黑客组织）8个活跃域名。



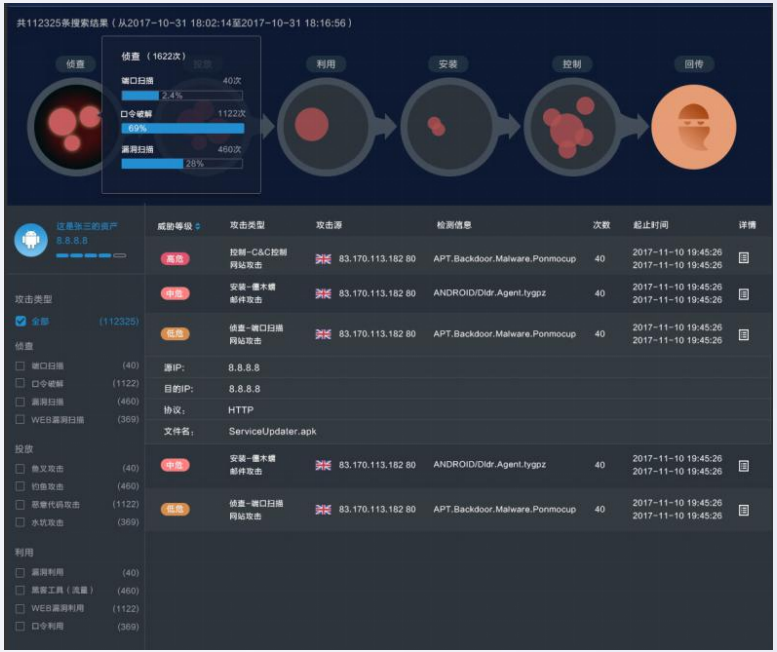


可视化分析

时间序列分析

还原攻击的先后**过程和步骤**

了解攻击发生的**时间段、集中点、时间频率**

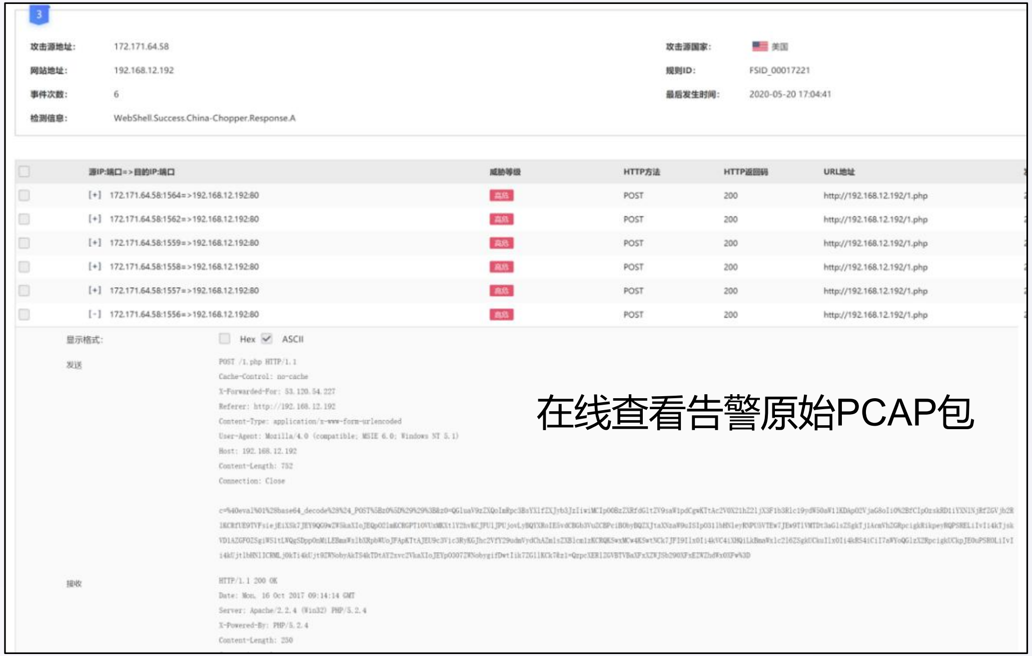


KillChain攻杀链分析

判断攻击是否**成功**

判断攻击是否为有**预谋的攻击**

溯源取证



在线查看告警原始PCAP包

文件运行原始行为

通过原始报文，快速求证攻击细节，排查误报和固定攻击证据

联动响应

设备协同联动响应，提升响应效率，缩短响应时间

03

标题

产品型号与竞争分析

产品型号和部署方式

型号	NT-AISA0106-C-HS-FX
性能	网络吞吐1Gbps
机型	2U
CPU	8核心8线程
内存	32G
硬盘	250G + 2T
管理口	2千兆电口
镜像口（可扩展）	4千兆电口

- 镜像流量，旁路部署
- 不改变网络结构
- 不影响网络性能

与现有安全产品区别

攻击阶段	监测能力	是否新型攻击	现有安全产品（防火墙/IDS/IPS/抗D/防毒墙）	360高级持续性威胁预警系统（360NDR）
扫描阶段	端口探测检测		支持，IDS/IPS支持	流量特征检测
	口令爆破检测		支持，IDS/IPS支持	流量特征检测
	漏洞扫描检测		支持，IDS/IPS支持	流量特征检测
入侵植入阶段	钓鱼/水坑攻击检测	是	部分支持，IPS支持部分监测	沙箱、机器学习、杀软、威胁情报
	web攻击检测		支持，WAF检测web攻击	web攻击特征
	0Day/nDay攻击检测	是	部分支持，支持Nday漏洞的检测	沙箱、机器学习
	DDOS攻击检测		部分支持，抗D设备支持检测与阻断	-
	已知木马检测		支持，防毒墙	杀软、威胁情报
	免杀、特种木马检测	是	不支持	文件沙箱
	webshell检测		支持，防毒墙，IDS/IPS支持部分	杀软、机器学习
控制回传阶段	命令与控制	是	部分支持，IDS/IPS支持部分特征检测	木马流量行为检测
	隐蔽信道通信监测	是	不支持	隐蔽信道检测技术

现有IDS/IPS等安全产品侧重于已知威胁，360APT涵盖已知威胁，更侧重于新型攻击的检测

与同类产品比较优势

对抗能力强，检测更精准

- 国内支持最多隐蔽信道检测，检测攻击方的高级木马通信
- 业界领先沙箱能力，更容易检出免杀邮件攻击、伪装木马
- 变种webshell和黑客工具检测，精准发现冰蝎、蚁剑等黑客工具

2018年CNCERT国内引擎测试大赛，综合第二名

样本总数量	威胁类型级别	检测数量	检出率占比
1726	恶意样本	1455	84.30%
	正常	271	15.70%

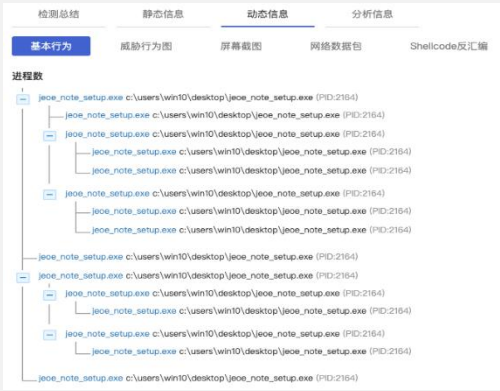
对比项目（功能测试）	检测结果
抽取具有危险的样本的IOC（Taged分析结果汇总）	共抽取了1457个具有威胁的样本的IOC
恶意代码命名（静态鉴定测试）	30测试样本，标出了30个测试样本结果
标签标记功测试（标记APT组织）	30测试样本，标出了30个测试样本结果

监测攻击面全，覆盖攻击类型多

- 覆盖攻击方95%+的攻击，扫描、web入侵、邮件入侵、控制、横向移动....
- 覆盖reGeorg、meterpreter等黑客工具
- 覆盖最新OWASP TOP10 和 最新主流CVE漏洞

一体化设备，易部署性能高

- 检测、分析、溯源、响应一体
- 同等配置，沙箱检测文件更多
- 自动生成样本行为、在线全流量pcap取证



04

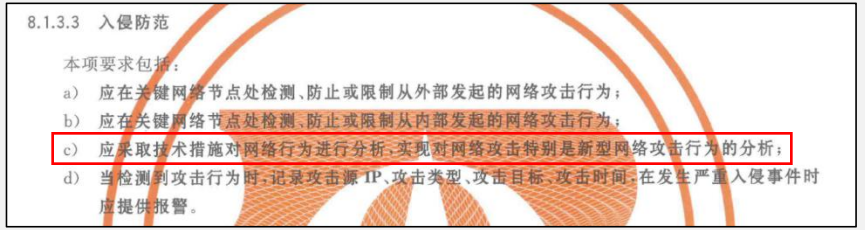
标题

应用场景与典型案例

场景-等保2.0：满足新型网络攻击行为的检测要求

场景需求：

- 等级保护基本要求：三级/四级系统应采取技术措施实现新型网络攻击行为的分析；
- 等级保护测评要求：需部署**抗APT攻击系统**应对新型网络攻击。



8.1.3.3 入侵防范

本项要求包括：

a) 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；

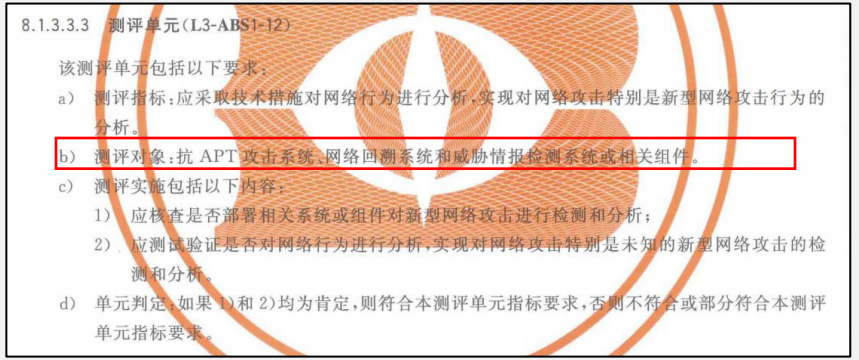
b) 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；

c) 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；

d) 当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。

解决思路：

- 在企业的**出口**部署360NDR设备
- 360NDR的威胁情报、行为分析、机器学习、隐蔽信道等新一代检测技术可满足等保要求
- 360NDR在日**常运维**、HW、重保中，还可帮助用户发现网络攻击和木马病毒



8.1.3.3.3 测评单元(L3-ABS1-12)

该测评单元包括以下要求：

a) 测评指标：应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。

b) 测评对象：抗APT攻击系统、网络回溯系统和威胁情报检测系统或相关组件。

c) 测评实施包括以下内容：

1) 应核查是否部署相关系统或组件对新型网络攻击进行检测和分析；

2) 应测试验证是否对网络行为进行分析，实现对网络攻击特别是未知的新型网络攻击的检测和分析。

d) 单元判定：如果1)和2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

客户收益：

- 提升三级/四级系统的**合规分数**
- 合规和安全同步实现，**一笔投入两笔收益**

涉及行业：

- **政府、金融、能源、运营商、教育、医疗、企业**等有等保建设和整改需求的客户

场景-勒索/失陷主机检测：发现勒索和失陷，联动处置

场景需求：

- 勒索病毒的勒索方式和技术手段不断升级，勒索软件种类众多
- **勒索软件更新迭代快**，杀软无法检测

解决思路：

- 360NDR**尽早发现，及时联动**终端杀软/EDR和防火墙隔离阻断
- 360NDR会利用威胁情报、行为检测、机器学习、勒索诱捕等**多种技术识别**勒索软件和已失陷的主机
- 360NDR**联动终端杀软/EDR/FW等进行隔离/查杀**，通知运维人员进行处置

客户收益：

- 采用多种技术结合，**检测**独立的、捆绑在正常程序中、利用office/PDF漏洞的多种类型的**勒索病毒**
- **及时联动隔离/阻断**勒索软件扩散，降低损失

涉及行业：

- **GA、能源、金融、运营商、医疗、制造、教育、央企**等

Malwarebytesd报告

2. 勒索病毒的勒索方式和技术手段不断升级。

勒索病毒持续活跃，全年捕获勒索病毒软件78.1万余个，较2019年同比增长6.8%。近年来，勒索病毒逐渐从“广撒网”转向定向攻击，表现出更强的针对性，攻击目标主要是大型高价值机构。同时，勒索病毒的技术手段不断升级，利用漏洞入侵过程以及随后的内网横向移动过程的自动化、集成化、模块化、组织化特点愈发明显，攻击技术呈现快速升级趋势。勒索方式也持续升级，勒索团伙将被加密文件窃取回传，在网站或暗网数据泄露站点上公布部分或全部文件，以威胁受害者缴纳赎金，例如我国某互联网公司就曾遭受来自勒索团伙Maze实施的此类攻击。

CNCERT 2020我国互联网网络安全态势综述

案例-某热力集团勒索软件检测

案例背景：

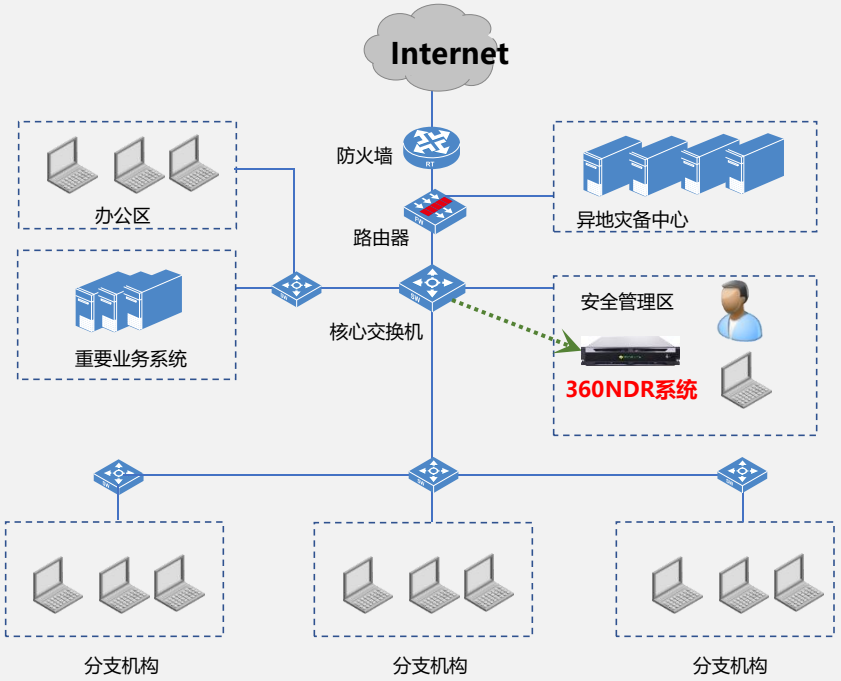
- 热力集团网络和下属分支机构网络连通，某次缴费/计费系统服务器遭受勒索病毒袭击，同时用户感觉网络中**仍存在一些中毒主机**，但不清楚总体网络安全现状

核心需求：

- 快速评估现有网络安全现状，包括集团总部、下属机构、备份中心
- 在现有资源下**控制病毒态势**，保证核心资产安全
- 对进入网络的文件进行深度检测，**防止再次遭受勒索**病毒袭击

部署情况：

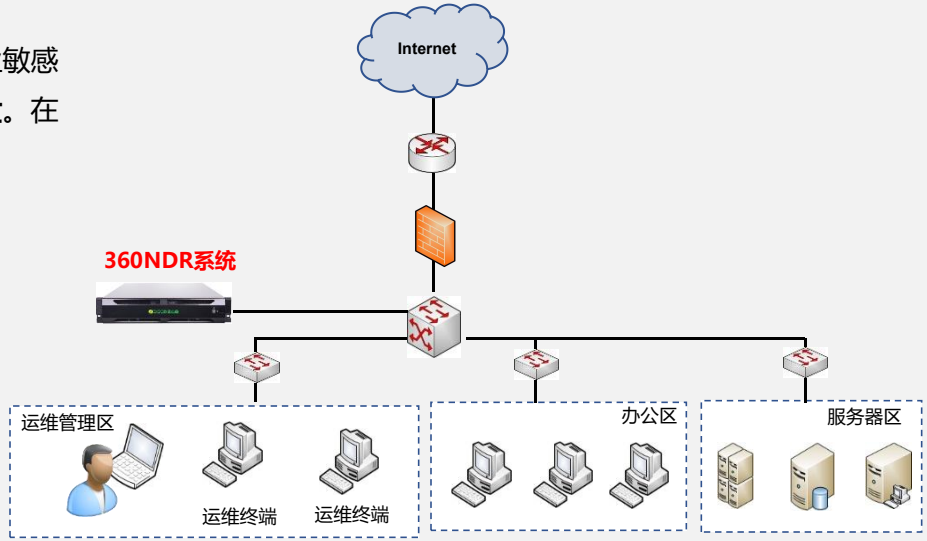
- 上线仅几小时，**发现定位**出网络中存在的大量挖矿和中毒主机，数量达100多台，包括总部其他业务系统服务器、办公主机、下属机构终端主机等，病毒在网络中利用系统漏洞在疯狂传播；
- **沙箱检测**到网络中某主机主动外连ftp服务器下载**木马文件**；
- **发现**内网中针对某些**服务器存在漏洞**，进行针对性加固措施。



案例-某央企失陷主机检测

案例背景：

- 由于业务需要，某央企每天会有大量的文件流转，其中包含商业敏感信息，为防止信息外泄事件的发生，**及早发现威胁遏制信息外泄**。在现有的安全防御产品基础上，部署APT检测类产品。



核心需求：

- 对进出网络的流量进行检测，**发现入侵**威胁和**失陷**主机
- 当出现威胁事件后，能快速**检测定位**出失陷主机和溯源攻击过程

部署情况：

- 在公司外网**出口处**部署了360NDR系统
- 360NDR系统部署后不到2小时，检测发现1台服务器被植入Gh0st**木马变种**程序。该木马变种程序，服务器上部署的**杀毒软件无法检测**出威胁，360NDR系统检测出威胁后，经人工上机操作，彻底清除掉木马程序。

场景-APT/态势监测：发现APT攻击，缩短响应时间

场景需求：

- CNCERT报告APT攻击呈上升趋势，涉及行业更加广泛
- APT攻击几乎都会**采用免杀或未知木马、漏洞攻击**等复杂手段，但现有的IDS/IPS/防火墙/WAF等产品应对困难
- **银行、运营商、电子政务**等中明确**发文要防范APT攻击**

解决思路：

- 在业务、办公网和分支机构的**出入口**部署360NDR，**配合态势感知平台**
- 360NDR利用**威胁情报、行为分析、机器学习、隐蔽信道检测等**技术监测网络中的APT攻击行为，尤其是漏洞攻击、免杀和未知木马，及时通知态势感知

客户收益：

- **有效检测**僵木蠕毒，尤其免杀、未知木马
- **符合行业规范**，如运营商的僵木蠕毒检测规范、银行也APT防护要求、电子政务外网建设规范等

涉及行业：

- **监管机构（WXB、GA）、政府、运营商、金融、能源、军工、医疗等**

2.攻击领域逐渐由党政机关、科研院所向各重要行业领域渗透。

2019 年，我国持续遭受来自“方程式组织”、“APT28”、“蔓灵花”、“海莲花”、“黑店”、“白金”等 30 余个 APT 组织的网络窃密攻击，国家网络空间安全受到严重威胁。境外 APT 组织不仅攻击我国党政机关、国防军工和科研院所，还进一步向军民融合、“一带一路”、基础行业、物联网和供应链等领域扩展延伸，通信、外交、能源、商务、金融、军工、海洋等领域成为境外 APT 组织重点攻击对象。

三、2021 年网络安全关注方向预测

（一）与社会热点相关联的 APT 攻击活动仍将持续。

2020 年，全球范围内多个 APT 组织都发起以新冠疫情主题为诱饵的 APT 攻击。攻击者通过“鱼叉”钓鱼邮件等方式对分布在全球的攻击目标实施窃密和控制。2021 年，在新冠肺炎疫情持续扩散、各国规模化开展疫苗采购和接种工作的背景下，这类攻击方式仍将流行，以窃取新冠肺炎疫苗相关信息为目标的 APT 攻击活动将持续，政府机构、关键信息基础设施运营者、疫苗生产厂商、卫生组织、医疗机构等将成为重点攻击目标。

CNCERT 2019/2020我国互联网网络安全态势综述

案例-某股份制银行全行APT监测

案例背景：

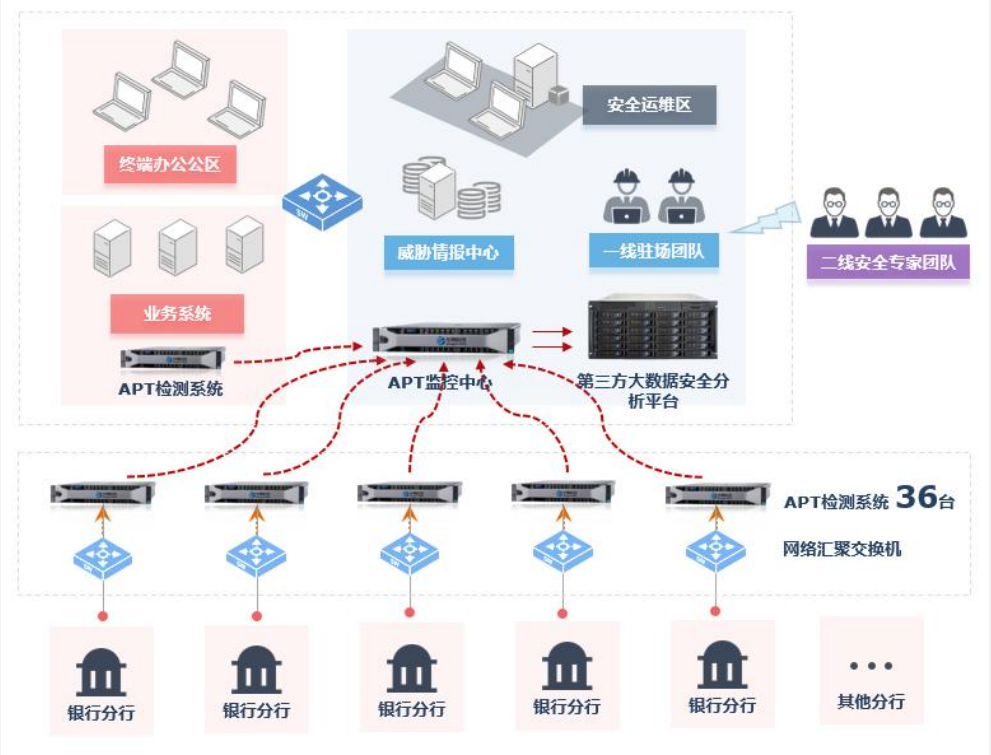
- 银行监管要求股份制银行**需具备APT防护能力**
- 银行业安全事件频发，为了应对高级持续性威胁，某股份制银行2017年建设全行APT监测平台。

核心需求：

- 对来自互联网上的**邮件附件**进行深度检测，识别高级威胁。
- **办公内网、生产网流量进行监测**，监测各类威胁，特别是APT类威胁。
- 将监测**结果上传到大数据威胁分析平台**，实现底层流量威胁数据的检测分析。

部署情况：

- 系统上线1年时间，累计发现**3500**余起高危攻击事件，并溯源出**1例APT黑产**组织。
- 为大数据威胁分析平台提供了流量威胁监测告警日志及原始数据流量，完善了整个安全威胁检测体系。



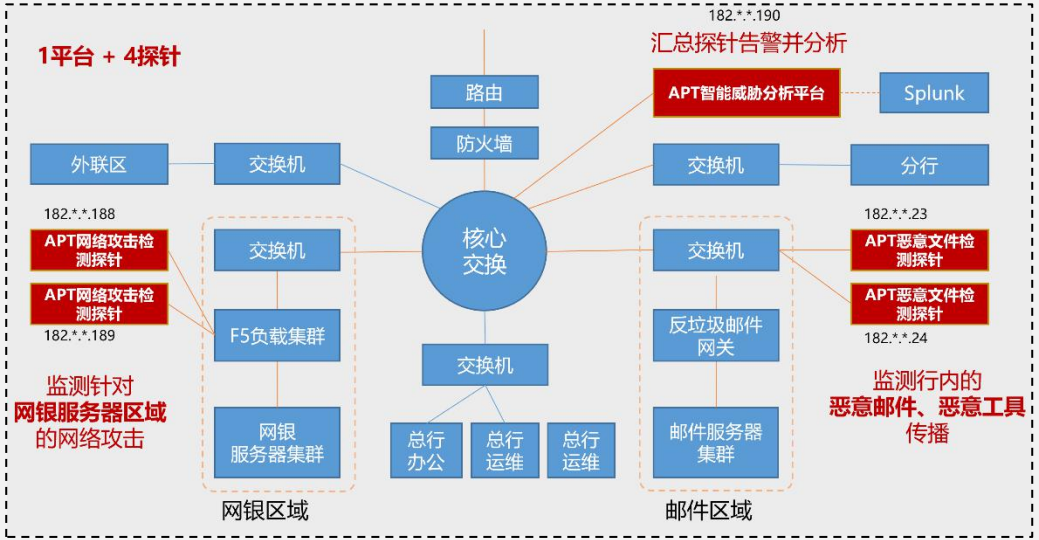
案例-某国有银行网银区域APT监测

案例背景：

- 已经部署了防火墙、全流量安全分析系统、漏洞扫描系统、防病毒系统、终端管理系统，数据防泄漏产品等，需要补充APT攻击检测与防护措施。

核心需求：

- 对**网银区的服务器**进行监测，检测**Webshell及各类攻击行为**；
- 对**邮件服务器**流量进行监测，检测**恶意邮件、恶意工具**的传播



部署情况：

- 2台NDR网络攻击检测探针部署在网银区域，2台NDR恶意文件检测探针部署在邮件区域；
- 1台NDR智能威胁分析平台，汇聚4台检测探针的数据，并提供分析；
- 文件检测探针检测发现多封邮件威胁；
- 网络攻击检测探针发现多次针对网银服务器系统的攻击，为处置工作提供依据。

案例-某运营商省公司APT安全监测

案例背景：

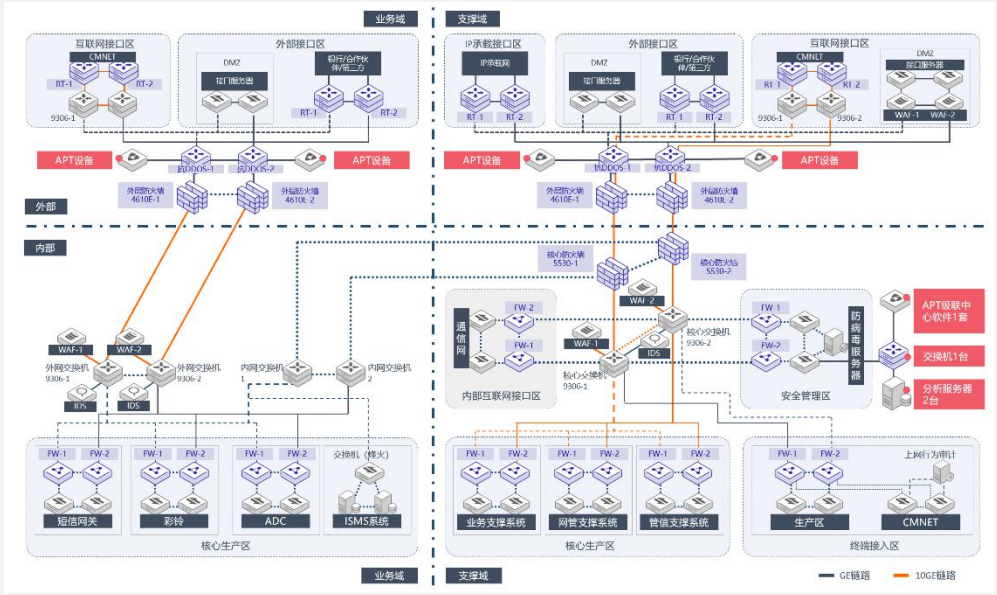
- 对全网（包括：**业务域、支撑域**）安全防护体系进行改造升级，**增加了APT威胁检测防护能力。**

核心需求：

- 对**绕过现有防护系统**直达核心生产系统的攻击行为进行实时检测发现。
- 及时**发现潜藏**在其网络中的安全威胁，对**入侵途径及攻击者背景的研判与溯源**，从源头上解决网络中的安全问题。

部署情况：

- **业务域**和**支撑域**各部署了2台NDR设备，覆盖攻击路径；
- 在支撑域的安全管理区部署NDR监控中心，对各NDR设备集中管控。



场景-HW/重保攻防监测：发现攻击，溯源过程

场景需求：

- HW攻防演练**已成常态化**，政府、能源、金融、医疗等多个行业的会被选中参与或者报名参加
- HW活动中，防守方需要**及时发现攻击方的攻击行为**并进行**响应处置**，否则会失分，越早发现越能减少失分的概率
- HW活动中，如果能**溯源攻击方**的过程和攻击方，可加分

解决思路：

- 在**业务、办公内网、第三方接入的位置**，部署NDR类产品，如360APT系统
- 360NDR**实时监测**攻击方惯用的**网站攻击、钓鱼邮件、木马控制、Webshell**和进入内网后的**横向移动**攻击，及时告警
- 360NDR会**存储攻击的原始流量**，方便进行**溯源取证**

客户收益：

- 帮助HW人员**及时发现**攻击团队的攻击行为，**尽早处置，避免丢分**
- 提供告警和**pcap包溯源取证**，提升溯源取证的效率
- 相比EDR终端产品，部署一台即可监测整个网络，**节约部署成本**

涉及行业：

- **政府、能源、金融、运营商、医疗、制造、教育、央企等**

“护网2020”网络攻防演习评分规则（防守方）

一、**加分规则：**防守方提交防守方报告上限为50个（不含总结报告）。对于加分规则第1、2、5、6、7条：攻防双方都没有提交该类型报告，可说明攻击方未攻击成功，防守方可得该类型的满分；其他情况按照提交的报告给分。

序号	类型	赋值规则	备注
（一）发现类（基础条件是发现的攻击IP来自演习平台，扫描类攻击行为不给分）			
1	发现webshell木马、主机木马	20-100分/个主机，根据木马发现的网络重要性给分	提供包含确凿证据的详细分析报告，得分累计不超过1000分
2	发现账号异常，并采取处置措施	普通用户：应用层5分，系统层10分，数据库10分，网络设备25分 管理员用户：得分*2	提供包含确凿证据的详细分析报告，得分不超过500分
3	发现恶意邮件（包含恶意链接、病毒邮件）	发现恶意邮件，对邮件进行分析，根据报告质量，得0-50分/个	提供包含确凿证据的详细分析报告，得分不超过250分
（二）消陷类（基础条件是发现的攻击IP来自演习平台，其他情况由指挥部研判给分）			
4	处置现场篡触式攻击	20分/次	提供包含确凿证据的详细分析报告，得分不超过100分
5	处置攻击者进入互联网区事件	25分/次	提供包含确凿证据的详细分析报告，得分不超过250分
6	处置攻击者进入逻辑隔离业务内网区事件	100分/次	提供包含确凿证据的详细分析报告，得分不超过1000分
7	处置攻击者进入生产网区事件	500分/次	提供包含确凿证据的详细分析报告，得分不超过2500分
（三）应急处置			
8	积极配合应急组工作，根据线索能快速准确定位受害系统，能提供充分的日志记录，配合执法机关有效固定证据完成勘验	能高效配合完成应急工作的，得分300；配合一般的，得分200；差的-100	得分累计不超过300分
（四）追踪溯源			
9	完整还原攻击链条，溯源到黑客的虚拟身份、真实身份，溯源到攻击队员，反控攻击方主机，根据程度给分	描述详细/思路清晰，提交确凿证据报告，根据溯源攻击者虚拟身份、真实身份的程度，500-3000分， 反控攻击方主机，再增加500分/次	不认可单一证据，需要提交可互相关联的证据。得分累计不超过9000分
（五）演习总结			
10	按指挥部要求，撰写并提交各类报告，包括：演习总结报告，防护技战法报告等	优秀：得1000分；不提交：减1000分	根据报告质量核定给分
二、减分规则			
（一）非正常防守			
1	发现防守方非正常防守，包括封C段、网站不可用、网站首页被改为图片等行为，被发现并提交确切证据的	/	从通知防守方开始，防守方有2个小时应急处置时间，2个小时后开始扣分，每30分钟减10分，7小时后，每30分钟减20分
（二）系统或网站被控：攻击方获得系统或网络权限，防守方相应扣分			
1、权限被控			
2	被获取域名控制权限	一级域名-100分，二级域名-50分	
3	被获取终端计算机权限	管理员权限-20分/个，普通权限不扣分	
4	被获取邮箱账号权限	-20分/个	
5	被获取Web应用系统、FTP等应用的用户权限	普通用户权限-20分，后台管理员权限-100分。同一系统的同等权限（包括管理员）只扣一次分	
6	被获取单点登录认证系统（SSO）权限	系统管理员权限-300分，能登入的系统-100分/个	
7	被获取服务器主机权限（含webshell权限）	普通用户权限-20分（同等权限按一个账户计），管理员权限-50分。通过多网卡进入新网络区域的，按照进入的网络类型扣分	
8	被获取域控系统权限	域控服务器管理员权限-500分，域内可控服务器按照服务器主机权限扣分	
9	被获取堡垒机、运维机权限	管理员权限-200至-500分，托管的服务器按照服务器主机权限扣分	
10	被获取云管理平台控制权、大数据系统控制权等	-1000至-2000分	
11	被获取数据库操账号密码（含sql注入）	普通用户权限-50分，管理员权限-100分，同一系统的同等权限（包括管理员）只扣一次分	
12	被获取防火墙、路由器、交换机、网闸、光闸、摆渡机、VPN等网络设备权限	依据最终成果附加减分，如对核心目标同网段，300分，以路由器为例，小型50分，中型150分，大型300分	
13	被获取物联网设备管控平台权限	按照平台上连接点数计算，-10分/台	
14	被获取IDS、审计设备等监测设备权限	管理员-200分/个，其他用户-50分/个	
15	被获取其他系统、服务器、设备等权限	/	由指挥部核定评分
2、边界被突破			
16	被攻击者进入逻辑隔离业务内网	-1000分	
17	被攻击者进入逻辑隔离业务内网	-2000分	
18	被攻击者进入核心生产网	-5000分	
19	其他情况	/	根据各单位内部网络实际情况，由指挥部核定扣分
3、目标系统被控			
20	位于互联网区的目标	-5000分	重要性等同于目标系统的系统被控，按照目标系统分值降低1000分进行扣分
21	位于业务内网的目标	-7000分	
22	位于核心生产网的目标	-10000分	
23	其他情况	/	由指挥部核定扣分

案例-某行2020和2021年HW

案例背景：

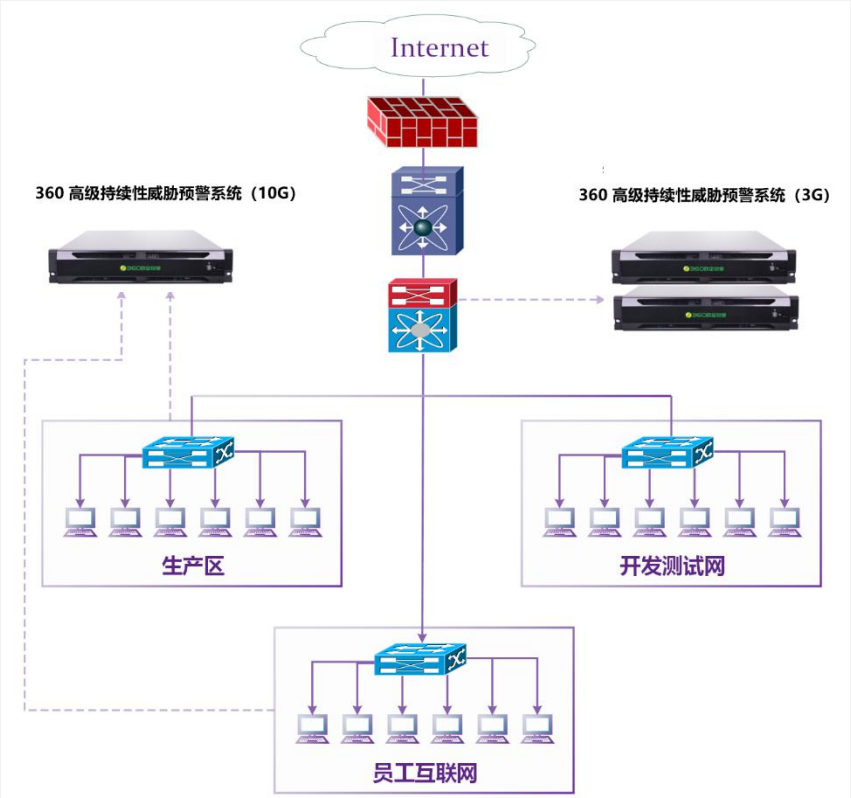
- 2020年和2021年全国HW攻防演练，金融行业属于重要基础设施相关行业是HW攻防演练重点攻防领域，某行高度重视，在原有较为完备的安全防护体系基础上，增加360NDR系统进行监测。

核心需求：

- 对**关键攻击路径上的流量**进行检测，发现威胁及时告警
- 重点防范攻击者通过**钓鱼邮件**或其它方式投递木马和远程控制软件

部署情况：

- 进出**邮件服务器流量、生产区、开发测试网、办公网、互联网业务等区域流量**全部接入360NDR系统进行监测；
- 2020年，共发现攻击IP地址**992个**，占封禁总IP数**30%**；
- 联动防火墙**封禁IP 45个，无一误报**；
- 重点事件72起；
- 准确识别了红队发送的CobaltStrike**木马邮件**；
- 2021年，监控并上报攻击源IP地址共计813个；
- 重点事件13起。



总结

产品定位	网络威胁检测与响应（NDR）
产品功能	• 检测：文件+流量，涵盖 特征检测、行为检测、威胁情报、AI/机器学习 • 分析：时间序列分析、KillChain分析 • 溯源：原始PCAP包、文件详细行为 • 响应：联动态势感知、防火墙、EDR..
3大优势	• 对抗能力强，检测更精准 • 监测攻击面全，覆盖攻击类型多 • 一体化设备，易部署
主要场景	• 等保2.0：满足新型网络攻击行为的检测要求 • 勒索/失陷主机检测：发现勒索和失陷，联动处置 • APT/态势监测：发现APT攻击，缩短响应时间 • HW/重保攻防监测：发现攻击，溯源过程