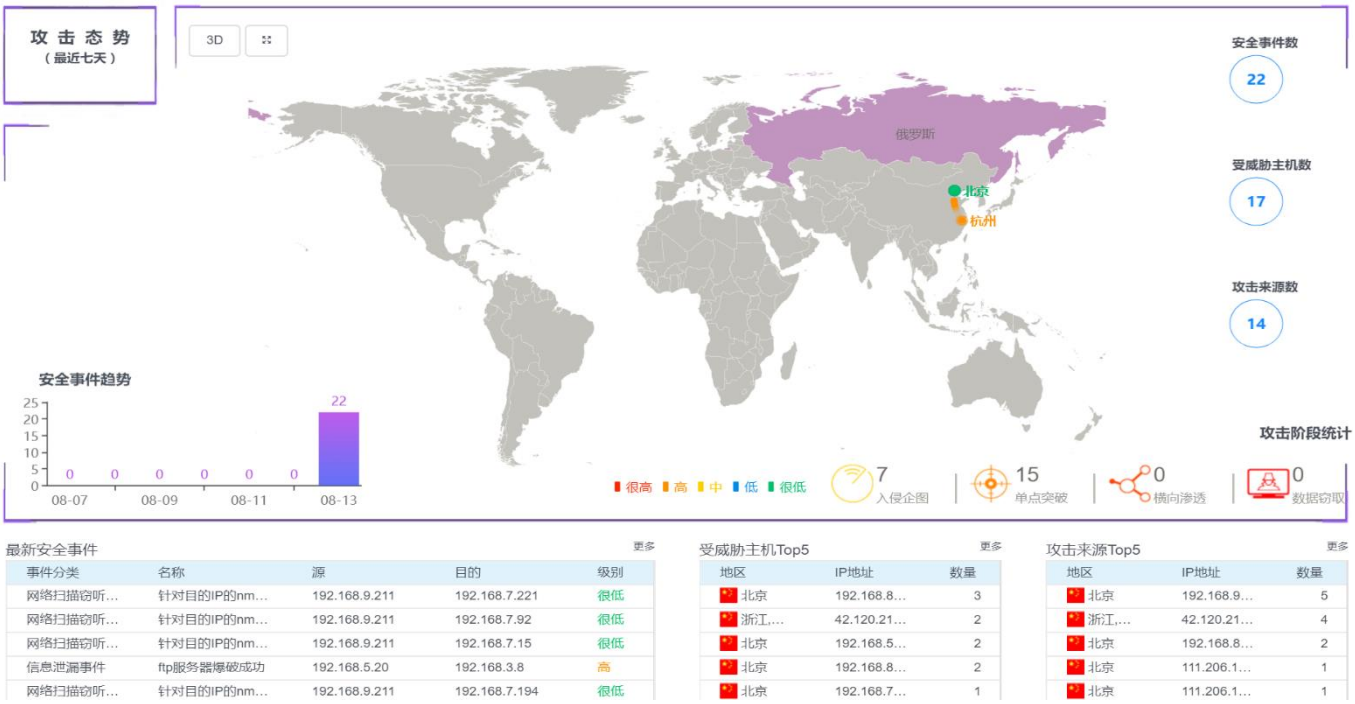
H3C SecCenter CSAP-ATD 高级威胁检测引擎

产品概述

随着计算机软硬件技术和网络通信技术的飞速发展，针对计算机和网络系统的攻击行为越来越高级、越来越频繁，并且随着新技术的出现而持续进化，攻击手段变得越发高明，攻击者也呈现出团队化、集团化的趋势。在所有的网络攻击之中，APT（Advanced Persistent Threat）攻击是最为人熟知的新型高级攻击，这种攻击是有别于传统威胁的新一代威胁，首先是因为此类攻击具有极强的隐蔽能力，通常是利用企业或机构网络中受信任的应用程序的零日漏洞（尚未被发现，没有对应的指纹或特征能够进行检测）来发起攻击，所用恶意软件会基于各种各样的隐蔽隧道来传输，或采用加密加壳等方式来逃避特征检测，因此能够轻易地贯通目标网络，直达受害主机；其次 APT 攻击具有很强的针对性，攻击触发之前通常需要收集大量关于用户业务流程和目标系统使用情况的精确信息，情报收集的过程更是社会工程艺术的完美展现。一次成功的 APT 攻击，轻则造成公司核心商业机密泄漏，给公司造成不可估计的损失；重则导致金融行业、能源行业、交通行业等涉及国计民生的行业陷入瘫痪，其效果不亚于一场战争。

面对 APT 攻击，传统的以特征检测、边界防护为主的安全防护手段几乎无能为力，当前广泛部署的防火墙、IPS、防病毒软件、终端安全软件等产品，主要采用特征匹配的检测模式，其自身的机理决定了无法应对未知威胁的挑战。所有的特征检测都属于静态检测，在安全厂商没有发现并提取到恶意代码的特征信息之前根本就无法检测，即使安全厂商识别并发布了该恶意代码的特征库之后，如果不及时更新，也还是无法检测。而不依赖于特征或指纹的动态行为检测则能有效避免这一缺陷，只要模拟运行环境能够有效触发恶意代码的各种行为，就能够及时检测并产生告警。

基于对高级恶意威胁的深刻理解，以及团队成员深厚的技术积累，新华三面向业界推出了一套针对 APT 攻击检测和防御的安全产品和解决方案——H3C SecCenter CSAP 高级威胁检测引擎。H3C 高级威胁检测引擎通过镜像现网流量来检测外部黑客发起的钓鱼邮件攻击，或在内部子网间传播的恶意软件，利用软件虚拟运行、沙箱逃逸对抗等技术对恶意软件的真实意图进行深度剖析，能够发现常规手段无法检测的 APT 攻击等高级恶意威胁，并能与防火墙等设备进行安全联动，阻断威胁的进一步蔓延，为企业或组织机构的网络安全保驾护航。



H3C SecCenter CSAP 高级威胁检测引擎

产品特点

全面的流量解析

产品提供独立的流量分析和文件还原能力，支持 IPv4 和 IPv6 双栈协议解析，支持 VxLAN 流量识别 ，可以深度解析 HTTP、SMTP、POP3、IMAP、FTP、SMB/CIFS 等应用层协议，并能够还原出协议载荷中承载的各种类型的应用文件。

全面的系统和应用覆盖

产品支持对主流操作系统进行模拟，包括 Windows、Linux 和 Android 等操作系统，支持对各种格式的应用文档进行威胁检测，包括 Word、Excel、PPT、PDF、HTML、JS、EXE、JPG、GIF、PNG 等几十种格式，支持对多级嵌套压缩文件进行深入检测，支持对 Windows7、Windows8、Windows10 等操作系统环境中文件的未知威胁检测

全面的威胁检测

产品内置高性能动态沙箱、AV 检测引擎、yara 检测引擎、入侵检测引擎、威胁情报检测引擎和机器学习检测引擎，既能对流量中的威胁进行检测，也能对文件中的威胁进行检测；既能检测已知威胁，也能检测未知威胁；既能对实时发生的网络威胁进行检测，也能基于通信特征对部署前已感染的网络威胁进行检测，覆盖威胁的全生命周期。

全面的网络仿真技术

为避免因产品部署环境缺少恶意文件运行所需的网络资源而导致不能完全诱发恶意文件运行的问题，系统实现了网络仿真技术，能够在不连接外部网络的情况下，仿真内部办公网环境、仿真 WEB 服务器、仿真 DNS 服务器、仿真文件服务器、仿真邮件服务器，

从多个维度保证恶意代码的网络行为都能展现出来。

强大的逃逸对抗能力

沙箱模拟真实物理机环境，利用各种防逃逸技术自动满足逃逸样本的环境检测要求（比如虚拟机特征检测、系统时间检测、用户交互检测等逃逸技术），欺骗具有逃逸能力的样本继续正常运行，进而捕获其行为并进行威胁检测。支持检测已公开和未公开的 40+种沙箱逃逸行为，能够全面对抗各种高级恶意软件，发现真正的 APT 攻击。

强大的关联分析能力

产品通过自研的行为模式分析引擎和基于复杂状态机的关联分析引擎，可以对产品输出的各类数据包括沙箱行为日志、各类网络日志、各类基础事件、威胁情报等进行多维度关联分析和相似事件归并，有效提高了安全事件告警的准确性，同时又大大减轻了安全管理员需要关注和处理的告警数量。系统内置数百种关联分析规则，并允许用户自定义关联分析规则。

高效的机器学习检测

利用卷积网络、深度神经网络等机器学习技术建立 webshell 检测模型、PE 检测模型和 DGA 检测模型，并应用于产品中实现对恶意文件和恶意域名的检测。可识别并检测 php、jsp 和 asp 等多种格式的 webshell、exe 和 dll 等多种类型的 PE 文件，可识别 gameover、locky、nymaim、symmi、bamital 等多个恶意家族 DGA 恶意域名。系统定时升级模型库，以保证对检测模型的及时更新。

优异的溯源取证能力

产品能够记录监控范围内的网络流量会话日志、HTTP 日志、DNS 日志、邮件日志，支持 http 代理追溯，支持全量记录并保存原始网络流量，也可以按需记录指定 IP 或威胁相关的网络流量，支持可视化分析和交互式分析，能够对所有基础安全事件和关联分析产生的安全事件以及流量审计日志提供多要素混合检索及字段级详细查询，能够有效地支撑威胁分析和溯源取证需求。

业内一流的检测性能

产品提供业内一流的沙箱检测性能，能够根据文件检测压力自适应调整沙箱数量，提高资源利用率的同时也极大提升了检测效率；Office 沙箱可并发执行多个样本，并隔离不同样本的行为日志；通过优化虚拟机调度机制，在同时运行数十个沙箱的情况下，通过底层优化、多级镜像和 IO 模式优化等机制能够实现沙箱秒级恢复。

灵活多变的部署方式

产品旁路部署，不影响现有业务运行，既可以部署在 Internet 出入口，也可以部署在广域网分支边界、数据中心边界或内网不同分区边界，还可以部署在隔离网络的文件摆渡机旁边，对进网文件进行深度未知威胁检测。产品可以独立部署，也可以与防火墙联动部署，还可以作为流量探针跟态势感知平台进行分布式部署。

多样化的生态对接

产品提供标准化接口，支持与防火墙第三方安全设备对接，联动阻断网络威胁；同时产品可以将自身检测发现的威胁事件发送至态势感知、日志审计或综合监管等外部平台，进行深层次关联分析或威胁处置。

产品规格

项目	功能
流量采集	支持采集 IPv4、IPv6 和 VxLAN 流量并进行协议解析。
文件还原	支持从 HTTP、FTP、POP3、SMTP、IMAP、SMB/CIFS 等协议中还原出承载文件。
检测文件格式	支持包括 Office（Word、Excel、PPT、RTF）、WPS、PDF、HTML、JS、PE（EXE、DLL 等）、swf、压缩包（ZIP、7Z、RAR 等）、脚本文件（BAT、VBS、CMD、Powershell）、APK 等默认文件格式。
入侵检测	包括网络恶意扫描行为检测、僵尸网络命令检测、应用服务安全检测、恶意软件及木马程序检测、网络渗透攻击行为检测、未知网络攻击检测等多种攻击行为检测。
弱口令检测	支持 Telnet、FTP、POP3、SMTP、IMAP 协议的弱口令检测。
病毒检测	系统内置病毒检测引擎和基于 yara 规则库的自研检测引擎，支持集成多个 AV 检测引擎。
威胁情报检测	支持对恶意 IP、恶意 URL、恶意域名和恶意 Email 的检测
机器学习检测	支持利用机器学习模型检测 webshell 文件、恶意 PE 文件和 DGA 域名。
动态沙箱检测	利用沙箱动态行为分析技术来检测已知威胁和未知威胁，沙箱类型包括 Windows XP 沙箱、Windows 7 32&64 沙箱、Office 沙箱、WEB 沙箱、Linux 沙箱和安卓沙箱。
网络行为仿真	支持多种常见网络协议仿真，包括 ICMP、DNS、HTTP、SMTP、POP3 等，模拟样本外联服务器进行应答，能够在不连接外网的情况下获取更多的恶意样本网络行为。
沙箱数量自适应	根据各类沙箱的文件检测队列长度，能够自动调整沙箱数量，动态适配变化的网络流量模型和不同的应用场景；
样本内嵌文件检测	能够打开并运行样本中内嵌的文件，根据行为进行威胁判定。
嵌套压缩文件检测	支持对多级（至少 3 级）嵌套压缩文件的子文件进行威胁检测。
数字签名检测	能够对样本的数字签名状态信息进行分析，包括证书验证结果、时间戳、序列号、使用者、有效期等，并能识别签名有效性，能够识别证书过期、伪造等信息。
多样本并行检测	Office 沙箱可并发执行多个样本，并隔离不同样本的行为日志，提高检测性能
自定义规则检测	支持自定义检测规则，包括电子邮件、WEB 访问、远程控制、文件传输、非标端口通信五类，通过邮件账号、网站地址、文件名称和非标端口等多种关键字进行自定义检测。
样本网络行为抓取	手动上传样本在沙箱内运行时能对其网络行为进行抓包，保存为 pcap 文件且可下载至本地分析。
文件伪装识别	能够根据文件内容而不是通过扩展名进行格式识别。
事件关联分析	支持通过关联分析规则实现多类型事件的关联分析，生成高级安全事件。
流量审计	能够审计并记录网络流量会话日志、邮件收发日志、网页访问日志、DNS 协议日志。
流量存储	支持全流量存储、异常流量存储（流量检测模块发现威胁的恶意流量）及自定义存储（通过 IP 地址范围来限定流量存储范围）等多种存储方式

项目	功能
安全分析	支持可视化分析和交互式分析，内置多种可视化分析面板，支持编码格式转换，支持本地威胁情报查询，支持本地可疑文件上传检测，支持自动下载指定 URL 的网络共享文件并进行检测。

订购信息

新华三高级威胁检测引擎可以根据实际需求按照主机、配件进行选购。

H3C SecCenterCSAP 高级威胁检测引擎配置

选择主机

模块	数量	备注
H3C SecCenter CSAP-ATD-A高级威胁检测引擎高级版Bundle,含CSAP-ATD-A主机,含系统软件及一年特征库升级授权	1	
H3C SecCenter CSAP-ATD-E高级威胁检测引擎专业版Bundle,含CSAP-ATD-E主机,含系统软件及一年特征库升级授权	1	
H3C SecCenter CSAP-ATD-P高级威胁检测引擎专业版Bundle,含CSAP-ATD-P主机,含系统软件及一年特征库升级授权	1	

根据实际需要选择配件

描述	备注
DDR4-32G-2Rx4-R 32G 内存模块	选配。
HDD-4T-SATA-6G-LFF 4T 硬盘模块	选配。
4 端口千兆以太网电接口模块	选配。
2 端口万兆以太网光接口模块	选配。

新华三技术有限公司
北京总部
北京市朝阳区广顺南大街 8 号院 利星行中心 1 号楼
邮编：100102

杭州总部
杭州市滨江区长河路 466 号
邮编：310052
电话：0571-86760000
传真：0571-86760001

http://www.h3c.com

客户服务热线
400-810-0504