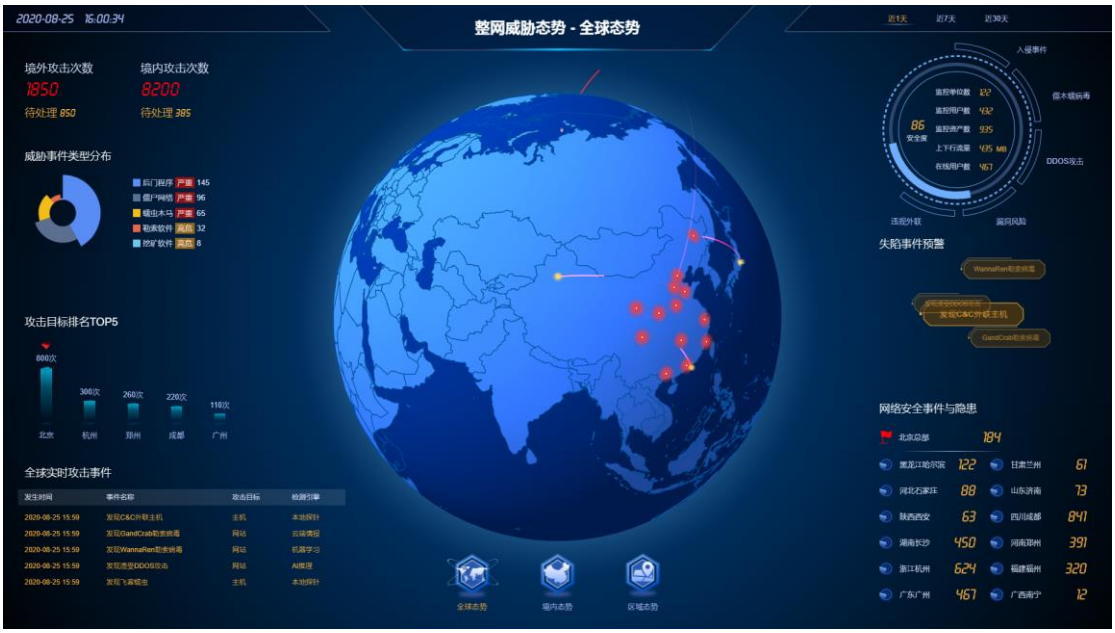
新华三安全威胁发现与运营管理平台（H3C SecCenter CSAP）

产品概述

近年来，国内外相继发生的“棱镜门”、域名系统遭攻击、国外情报机构网络攻击工具曝光、勒索病毒爆发、大规模用户信息泄漏等问题，以及信息通信诈骗等问题不断给我们敲响警钟。面对日益严峻的安全形势，新华三顺势而为，推出新华三安全威胁发现与运营管理平台（H3C SecCenter CSAP）。

新华三安全威胁发现与运营管理平台是以安全大数据为基础，对能够引起网络态势发生变化的要素进行获取、理解、评估、呈现以及对未来发展趋势预测的一个过程；是从全局视角提升对安全威胁的发现识别、理解分析、响应处置的一种能力；是通过智能分析和联动响应，结合机器学习和人工智能，实现“安全大脑”的闭环决策，实现安全能力的落地实践，真正做到对安全风险威胁的“主动发现、预知未来、协同防御、智能进化”。

新华三安全威胁发现与运营管理平台贯穿安全风险监控、分析、响应和预测的全过程，以威胁、风险、资产、业务、用户等为对象，基于安全日志、网络流量、用户行为、终端日志、业务数据、资产状态等多源数据，结合外部情报，通对全局状态评价、外部攻击评级、系统合规自检等手段，实现“事态可评估”；通过对攻击趋势分析、异常流量判断和终端行为检测，实现“趋势可预测”；通过对未知威胁的智能检测识别、流量/行为/资产的状态监控和多维度风险分析，实现“风险可感知”；通过对攻击溯源取证、云网端协同联动、工单流程闭环处理和设备策略自适应调整，实现“知行可管控”。



H3C 安全威胁发现与运营管理平台增强版效果图

产品特点

多样化数据采集

- 支持各种网络设备、安全设备、漏扫设备、主机及应用日志采集，可接入外部威胁情报
- 采用主动、被动技术实时采集网络中的异构海量日志；支持 SYSLOG 协议、HTTP/HTTPS 被动采集，FTP、数据库主动采集，部署代理等多样化日志接入
- 支持海量日志集中存储或分布式存储，满足快速查询的海量日志的要求
- 通过日志范式化和日志分类支持不同厂家日志与系统的快速适配

基于 AI 的智能化威胁分析

- 根据使用场景的不同，主动调整模型算法参数，使安全分析结果更加贴合网络实际情况
- 基于现有安全事件，依托攻防专家经验，关联资产、情报等多维信息，提供“专家级”推理分析
- 引入监督学习、强化学习等 AI 人工智能算法，利用“知识大脑”推理检测已知及未知类型的复杂攻击，全面掌握规模群体性事件的感染路径
- 建立行为基线，通过资产/用户的流量、动作等行为的偏离情况，判断各类异常行为

全过程溯源取证

- 针对攻击全过程对攻击者留下的任意线索进行多维拓展，可视化绘制出完整的攻击链条
- 对安全事件进行回溯和调查，主动对攻击过程进行抓包取证，提供完整攻击证据
- 针对 NAT 应用场景，基于 IP 和时间段信息，追溯地址转换关系，并呈现对应的安全事件
- 利用云端丰富的实时威胁情报和本地的网络行为、终端行为、文件信息，覆盖攻击的源头、手段、目标、范围等相关信息，对发现的未知威胁进行快速溯源和定性

自动化编排与响应

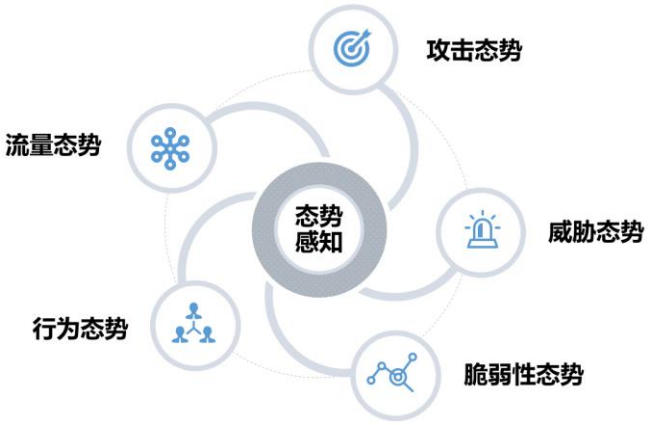
- 根据发现的安全事件，自定义安全响应剧本，根据防护需要调整处置步骤
- 响应处置动作类型多样，包括黑名单阻断、访问控制、告警、工单处置、用户下线、主机病毒查杀及隔离等操作
- 不仅可以针对 FW、IPS、WAF、ACG 等常见安全设备进行调度，更可以对交换机、路由、无线 AP 等网络设备进行调度
- 规范处置流程，提升安全管理水平

漏洞全生命周期管理

- 主动扫描网络安全漏洞，支持第三方漏扫结果导入
- 通过工单任务实现了漏洞加固任务的下发、审核、复验等功能
- 支持漏洞加固任务处置状态跟踪，对超期未处理任务可进行短信提醒
- 支持人工或工具的方式对漏洞进行复验。并根据验证结果自动同步漏洞当前状态

产品功能

新华三安全威胁发现与运营管理平台通过采集全网原始流量数据，结合云端的威胁情报，对海量安全数据进行挖掘和关联分析，对攻击、威胁、脆弱性、流量和行为等五大态势进行感知，生成全方位的安全全景视图，使用户能够快速准确地掌握网络当前的安全态势，并以此为依据进行联动响应。



项目	功能
环境温度	工作：5～35℃ 非工作：-40～65℃
环境湿度	工作时：10%~80% 非工作：5～95%，无冷凝
安全态势展示	支持网络攻击态势展示、威胁态势展示、脆弱性态势展示
关联规则	实时关联分析：在一定时间窗口内对日志进行关联，实时的给出相关告警
	历史关联分析：在长周期历史时间内，进行多事件关联挖掘分析
	支持自定义关联规则
威胁告警	受到网络攻击后，可以通过短信、邮件等形式向用户进行告警
威胁分析	针对受到的威胁事件，还原攻击过程
日志审计	对收到的日志进行进行审计
行为画像	支持用户行为画像，显示用户一段时间内的行为轨迹
流量统计	支持互联网应用流量分析、内网资产流量分析、用户流量分析
运维监控	支持资产、资产组：资产包括主机设备、网络设备、安全设备、中间件、数据库、应用系统
	资产管理：支持手工添加、导入，支持资产自动发现
安全编排及响应	支持安全处置编排，可自动下发并执行响应动作
报表	内置预定义报表，支持自定义报表，报表可导出为 PDF\HTML\DOCX\XLS 等不同格式
权限管理	支持三权分立，用户登录时可以对用户进行本地和外部认证。
系统管理	支持系统状态监控，包括服务节点监控和服务进程状态监控。支持通过短信、微信、邮件等多种方式进行告警

订购信息

新华三安全威胁发现与运营管理平台增强版产品，可以根据实际需求按照基础集群、日志采集器、全流量威胁检测引擎、软件授权、配件等几部分进行选购。

新华三安全威胁发现与运营管理平台增强版配置

选择平台

描述	备注
H3C SecCenter CSAP 安全威胁发现与运营管理平台-基础集群	必配。
H3C SecCenter CSAP 安全威胁发现与运营管理平台-集群扩展单元	选配。

日志采集器和全流量威胁检测引擎

描述	备注
H3C SecCenter CSAP 安全威胁发现与运营管理平台-分布式日志采集器	必配。
H3C SecCenter CSAP 安全威胁发现与运营管理平台-基础版分布式流量采集器	流量检测引擎三选一，必配
H3C SecCenter CSAP 安全威胁发现与运营管理平台-标准版分布式流量采集器	
H3C SecCenter CSAP 安全威胁发现与运营管理平台-高级版分布式流量采集器	

根据功能需求选择软件授权

描述	备注
H3C SecCenter CSAP 安全威胁发现与运营管理平台-关联分析组件授权函	选配。
H3C SecCenter CSAP 安全威胁发现与运营管理平台-流量及行为分析组件授权函	选配。
H3C SecCenter CSAP 安全威胁发现与运营管理平台-研发定制化开发服务授权函	选配。
H3C SecCenter CSAP 安全威胁发现与运营管理平台-威胁情报一年更新升级授权函	选配。
H3C SecCenter CSAP 安全威胁发现与运营管理平台-威胁情报三年更新升级授权函	选配。

根据实际需要选择配件

描述	备注
DDR4-16G-1Rx4-R 16G 内存模块	选配。
DDR4-32G-2Rx4-R 32G 内存模块	选配。
1TB 6G SATA 7.2K 3.5in HDD 通用硬盘模块	选配。
4TB 6G SATA 7.2K 3.5in HDD 通用硬盘模块	选配。

描述	备注
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。
800W 交流电源模块	选配。
550W 交流电源模块	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