新华三安全威胁发现与运营管理平台标准版（H3C SecCenter CSAP-S）

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标准版（H3C SecCenter CSAP-S）。

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，通过威胁情报、机器学习等技术对海量日志等信息进行深度分析，同时关联网络攻击事件，多维度、可视化地呈现全网的安全风险状况，围绕资产和业务，融合安全和网络管理，实现风险告警到安全联动响应的完整安全闭环。系统极大程度降低了企业内部安全运维人员的时间成本，有效的提升了威胁事件发现和处理能力。

H3C 安全威胁发现与运营管理平台标准版效果图

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、互联网爬虫、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和全生命周期管理
- 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

多维度风险预警

- 通过可视化技术的利用，将原本碎片化的威胁告警、异常行为告警、资产管理等数据结构化，形成高维度的可视化视图
- 通过全网威胁情报和大数据分析对入侵事件进行实时检测，提供丰富多样的数据可视化效果，
- 以安全大数据为基础，从不同视角和维度进行风险呈现，实现安全事件实时监控与预警
- 漏扫设备配合进行全网脆弱性管理

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

产品功能

新华三安全威胁发现与运营管理平台标准版产品通过采集全网安全事件数据，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，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，形成闭环处理。

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	攻击阶段风险展示：展示各攻击阶段的风险主机数，可下钻
	攻击态势态势展示：从攻击维度展示攻击源、攻击目的、攻击类型等信息

项目	功能
	脆弱性态势展示：从漏洞角度展示资产漏洞分布情况
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，可以通过短信和邮件等形式向用户进行告警
日志审计	对收到的各类日志进行审计
资产管理	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
	支持系统日志、操作日志管理

订购信息

新华三安全威胁发现与运营管理平台标准版可以根据实际需求按照标准版平台、全流量威胁检测引擎、特性授权、配件等几部分进行选购。

H3C SecCenter CSAP-S 安全威胁发现与运营管理平台标准版配置

选择平台

描述	备注
H3C SecCenter CSAP-S 安全威胁发现与运营管理平台标准版	必配。

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-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标准版高级功能包-研发定制化开发服务授权函	选配。

描述	备注
H3C SecCenter CSAP 安全威胁发现与运营管理平台标准版高级功能包-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标准版高级功能包-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。
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