新华三云智- SecCenter CSAP 网络安全态势感知平台

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，推出新华三云智（H3C SecCenter CSAP 网络安全态势感知）平台。

新华三云智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”。

新华三云智贯穿安全风险监控、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 云智效果图

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

多引擎协同感知

- 安全分析引擎完成威胁检测、异常发现、攻击溯源、态势呈现和联动响应等功能
- 智能学习引擎完成判别模型、预测模型、关联模型和学习进化模型的构建
- Web 安全引擎完成漏洞检测、木马检测、网页篡改检测和可用性检测等功能
- 云化运维引擎完成配置基线建立、等保合规检查、资产风险监控和运行状态监测等
- 云沙箱引擎完成样本的静态分析、动态分析及虚拟环境执行等

智能化威胁分析

- 通过多维度（资产、漏洞、统计、规则）进行数据关联分析，发现潜在的安全问题
- 利用内置的多种分析规则，对数据进行多维度关联分析，有效发现攻击行为和违规访问
- 基于机器学习和专家系统，对大范围样本数据进行安全分析，发现威胁并预判趋势
- 通过用户行为基线、异常流量基线、威胁攻击基线，建立基于行为模型的趋势预测模型
- 建立知识库，通过机器学习+专家系统不断优化模型，实现系统自愈免疫

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，包括 3D 图表、雷达图、拓扑图、热度图等样式
- 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

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，并提供全量原始日志的检索功能，对攻击事件的影响和系统防御效果态势进行自定义调查
- 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，为用户呈现一次攻击的完整过程，覆盖攻击的源头、手段、目标、范围等相关信息，并可对被发现的未知威胁进行快速溯源和定性

云网端协同联动

- 建立知识库进行策略管理，快速生成应急响应预案，实现安全事件的预警、响应和处置
- 云端检测，形成云网协同的主动防御体系，实现控制闭环反馈
- “云-网-端”协同联动，根据实时场景自适应决策响应，全网关键设备被推送安全策略

自动化运维响应

- 对关键对象的状态实时监控，对重要资产进行风险分析，将资产进行分级分类动态管理
- 当系统状态变化时，能够快速生成配置策略和任务工单，实现运维的响应和处置
- 支持工单的作业化管理，实现工单的自动触发、派发、跟踪、提醒和关闭
- 简单部署、快速开通，模块化设计，灵活扩展

标准化合规检查

- 充当安全合规自检平台，内置专业等保工作箱，为用户的安全合规检查提供参考
- 产品架构符合 ISO 27001 系列信息安全标准，满足国家等保分保法规和行业安全性要求
- 定期进行系统安全自我检测和评估，符合内控管理条例、等级保护、分级保护的要求
- 配备专业人员和评估系统在建设和改造前后进行安全规划评估和成效检验

产品功能

新华三云智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、流量、行为、运维和合规等六大态势进行感知，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	支持网络拓扑风险展示、业务拓扑风险展示、攻击态势态势展示、业务风险态势展示
关联规则	支持实时关联分析、历史关联分析
威胁预警	针对受到的威胁情况，向用户进行预警
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	支持对资产安全状况进行监控。资产包括主机设备（Windows、Linux、Solaris 服务器）、网络设备（交换机、路由器）、安全设备（防火墙、IPS）、中间件（Tomcat、webshpere）、数据库（oracle、SQL Server）、存储、虚拟化（EXSI）、应用系统（Mail、WEB）；
等保合规	支持等保合规性检查
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。支持通过声音、短信、微信、邮件等多种方式进行告警

订购信息

新华三云智是 H3C 公司自主开发的网络安全态势感知平台产品，可以根据实际需求按照主机、采集和探测引擎、软件授权、配件等几部分进行选购。

H3C 云智平台配置

选择主机

描述	备注
H3C SecCenter CSAP-Platform 网络安全态势感知基础平台	必配。自带 150 节点授权
H3C SecCenter CSAP-Cluster 网络安全态势感知平台-集群扩展单元	选配。

采集和探测引擎

描述	备注
H3C SecCenter CSAP-LogCollector 网络安全态势感知平台-分布式日志采集器	必配。
H3C SecCenter CSAP-VNScan 网络安全态势感知平台-漏洞扫描引擎	选配。
H3C SecCenter CSAP-NTA 网络安全态势感知平台-分布式流量采集器	选配。

描述	备注
H3C SecCenter CSAP-WMC-MGT 分布式调度引擎	选配。
H3C SecCenter CSAP-WMC-WebEngine WEB 检测引擎	选配。
H3C SecCenter CSAP-WMC-NDP 通报处置平台	选配。。
H3C SecCenter CSAP-WMC-BTWEngine 僵木蠕检测引擎	选配。

根据功能需求选择软件授权

描述	备注
H3C SecCenter CSAP 网络安全态势感知平台高级功能包-关联分析组件授权函	选配。
H3C SecCenter CSAP 网络安全态势感知平台高级功能包-威胁处置组件授权函	选配。
H3C SecCenter CSAP 网络安全态势感知平台高级功能包-安全策略合规分析组件授权函	选配。
H3C SecCenter CSAP 网络安全态势感知平台高级功能包-攻击路径分析组件授权函	选配。
H3C SecCenter CSAP 网络安全态势感知高级功能包-流量及行为分析组件授权函	选配。
H3C SecCenter CSAP 网络安全态势感知高级功能包-异常流量及行为分析组件授权函	选配。
H3C SecCenter CSAP 网络安全态势感知平台高级功能包-等保合规检查组件授权函	选配。
H3C SecCenter CSAP 网络安全态势感知平台高级功能包-分级管理组件授权函	选配。
H3C SecCenter CSAP 网络安全态势感知平台高级功能包-多厂商日志一年适配开发服务授权函	选配。
H3C SecCenter CSAP 网络安全态势感知平台高级功能包-研发定制化开发服务授权函	选配。
H3C SecCenter CSAP 网络安全态势感知平台高级功能包-威胁情报一年更新升级授权函	选配。
H3C SecCenter CSAP 网络安全态势感知平台高级功能包-威胁情报三年更新升级授权函	选配。
H3C SecCenter CSAP-WMC WEB 检测引擎特征库一年更新授权函	选配。
H3C SecCenter CSAP-WMC 僵木蠕检测引擎特征库一年更新授权函	选配。
H3C SecCenter CSAP-WMC Web 大屏展示引擎授权函	选配。

根据节点数量选择增量授权

描述	备注
H3C SecCenter CSAP 网络安全态势感知平台高级功能包-25 节点增量授权函	选配。
H3C SecCenter CSAP 网络安全态势感知平台高级功能包-50 节点增量授权函	选配。
H3C SecCenter CSAP 网络安全态势感知平台高级功能包-100 节点增量授权函	选配。
H3C SecCenter CSAP 网络安全态势感知平台高级功能包-200 节点增量授权函	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。
2TB 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