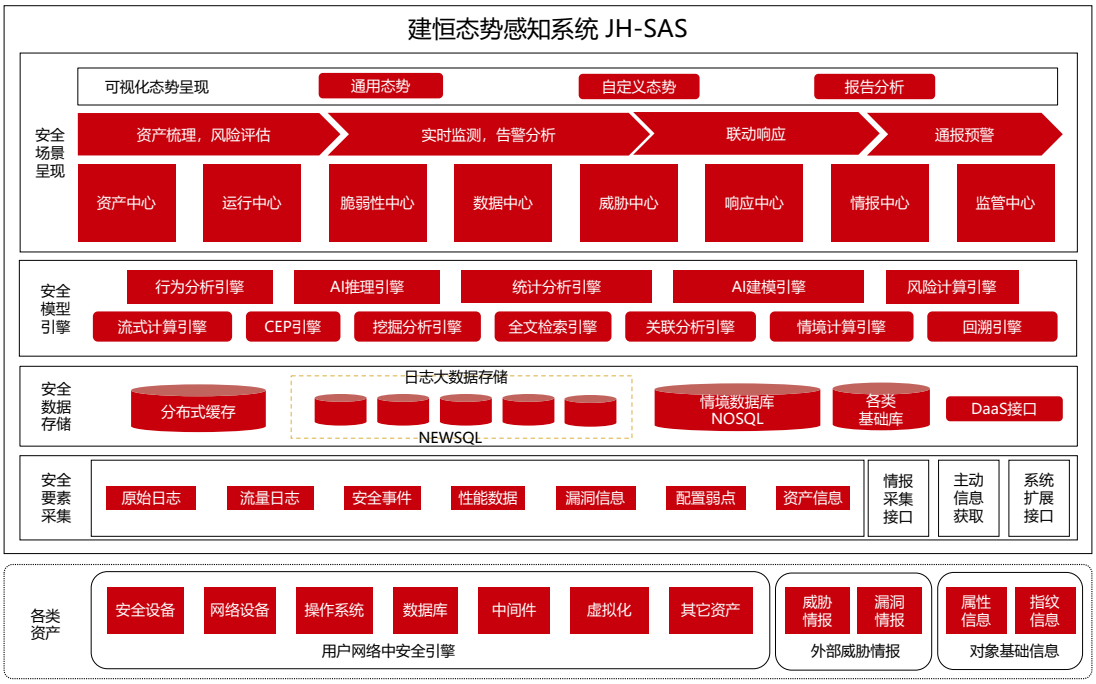
态势感知系统
JH-SAS

产品简介 | PRODUCT INTRODUCTION

建恒信安态势感知系统 JH-SAS 是依托大数据、人工智能等技术开发的全新网络安全态势感知与管理产品。系统通过接入日志审计探针、网络分析探针等多种方式获取数据源，对数据进行抽取、清洗、转换、聚合后形成网络安全行为记录，通过实体行为分析、行为关联分析，对攻击行为进行画像，对攻击链条进行还原，对资产面临风险进行评估，从而对网络整体安全态势进行预测。系统融合各种安全要素的基础上从宏观的角度实时评估网络安全态势，并可在发现威胁之后实现安全联动，进行及时阻断。系统以网络安全威胁识别分析、大数据可视化分析、安全决策基线建模等关键技术为基础，实现网络安全态势感知监测、预警、应急响应和处置工作。

系统主要面向大型行业用户，为信息化管理部门的决策分析提供依据，保护客户核心资产，为用户提供可落地的安全保障能力，构建动态的多层次、多维度、全天候、全方位的网络安全态势知防御体系。



产品优势 | PRODUCT ADVANTAGES

灵活的大数据技术架构

系统采用先进的技术架构，满足大数据海量异构数据的采集、存储和分析需求。支持在小规模数据情况下可采用轻量级的分布式非关系型数据库 ArkBase，也可以支持当项目规模扩大后移植到以 Hadoop/Spark 为代表的大数据平台上。

智能的资产发现技术和指纹库

系统提供智能的多种资产发现技术，结合丰富的指纹库精准识别资产，帮助安全管理人员摸清家底，全面了解网络资产态势。

智能易用的告警管理

系统提供智能化的告警管理能力，帮助安全管理人员实现告警分诊、告警总览、告警列表、告警调查、告警响应功能。告警管理的核心不仅是对告警安全事件的收集、展示和响应，更强调告警分诊和告警调查。只有通过告警分诊和告警调查才能提升告警的质量，减少告警的数量。同时系统提供了多种的告警响应手段，帮助管理员高效快捷的处理安全事件。

自有漏洞情报库

系统拥有完善的漏洞情报库，该漏洞情报库由建恒信安收集于国内外权威漏洞发布机构、漏扫系统厂商、安全漏洞社区等漏洞信息，经过综合分析，形成建恒信安漏洞标准描述格式。

基于机器学习的日志模式识别和可视化范化技术

系统采用了机器学习的技术对海量日志进行学习和识别，通过分析日志语法结构和聚类算法，自动化对日志进行聚类合并，形成一个个包含相似数据内容的日志集，并可以根据日志集内日志数量的大小进行排序。安全分析人员在查看数量繁多、种类复杂的搜索结果时，可以通过日志集模式进行查看和分析。这种技术可以帮助安全分析人员优先分析数量最少的日志集，从统计学的角度来说，这种小概率分布的数据往往是异常分析的入口线索。安全分析人员也可优先处理数据量最大的日志集，可对其进行范式化，方便后续分析和审计。

开放、可扩展的模块化应用开发平台

系统采用模块化技术开发，集成了安全事件和网络流量的采集、存储、告警、查询、分析和报表等全流程，内置大数据存储和智能分析引擎，提供功能界面定制和模块开发接口，用户可以快速部署、配置和开发一系列的安全管理相关应用。