永达电子

安全风险监测分析系统设备

产品概述

安全风险监测分析系统设备是基于业务系统面临的脆弱性关联人和组织、资产和业务系统、网络和安全域等，并融合了类量子存储与大数据分析技术、大数据建模技术、可视化技术、威胁情报于一体，辅以大数据 AI 算法并支持分析模型训练与分发检测功能。

通过采集多种数据，对全要素信息的数据进行融合、数据清洗、数据挖掘、特征提取、动态响应与预测、机器学习等，并从数据中自动学习、建模、分析形成规律，并利用规律对网络空间进行网络安全风险监测分析、网络威胁评估和网络态势预测，实现对网络空间安全状况的可视化、可预测、可管理、可控制、可追溯和可预警。并建立信息安全联动工作机制，提升安全决策的准确度和效率，从而构建了多层次、多角度、多粒度的安全风险监测分析平台。

产品功能

01 - 大数据安全分析

可视化态势分析

综合态势分析、资产态势分析、漏洞态势分析、威胁态势分析、网站态势分析、僵木蠕态势分析、文件态势分析、攻击态势分析、业务行为溯源分析、告警统计、风险主机统计、漏洞统计、流量统计及展示。

行为检测分析

会话还原、会话提取、关联分析、业务合规性检测。

威胁分析

资产监测分析、网站监测信息、漏洞风险监测、攻击行为监测分析、异常行为监测分析。

02 - 数据采集

数据采集包含实时采集数据包、定期采集全网日志、自定义数据采集、文件导入数据、扫描导入数据、代理导入数据、探针导入数据、网络设备接入采集、操作系统接入采集、数据库接入采集、设备接入采集。

03 - 数据处理

数据处理支持产品数据融合处理和数据关联分析。包含建立安全威胁元数据模型、建立漏洞风险元数据模型、安全威胁元数据模型评估、漏洞风险元数据模型评估、数据模型发布、数据预处理、数据挖掘、数据搜索、数据高级搜索管理、数据搜索配置管理、数据搜索接口等。

04 - 数据存储

数据存储包含分布式文件存储、分布式列式数据存储、分布式结构化数据存储、分布式图数据存储。

05 -安全基线管理及动态分发

包括对资产基线库和网络设备、安全设备、服务器、终端、虚拟化软件、操作系统、数据库、业务应用系统进行配置，建立并维护配置基线库。提供配置基线的版本管理与控制，对配置进行集中分发，并监控配置的变化，为资产的配置完整性提供监控与恢复的机制。

06 - 安全事件自动处理编排

支持安全策略编排。

07 - 预警决策处置中心

支持下发处置任务、响应预案。

08 - 威胁情报

威胁情报包含威胁情报类型、威胁情报管理、威胁情报集成、威胁情报共享、威胁情报生产。

09 -审计管理

审计管理包含审计内容、审计操作、审计记录、审计查询、审计存储、审计备份、审计安全。

10 - 拓扑图

包括拓扑图扫描和发现、拓扑图编辑、拓扑的映射。

11 - 可视化管理

可视化管理支持自定义仪表板、发布仪表板、菜单管理、面板表单管理、仪表板数据源绑定、新建面板、修改面板、删除面板等功能。

12 -系统管理

系统管理支持角色管理、用户管理、权限管理、指标管理、配置管理、运维管理、安全管理、登录、退出等功能。

产品参数

性能指标

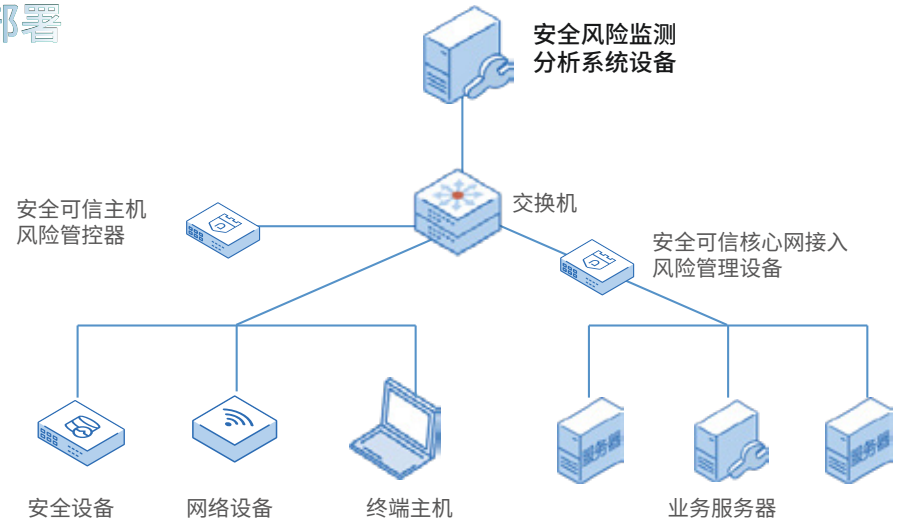
1. 设备应内置**不少于 8 种**机器学习分析场景模型
2. 设备应内置包括规则模型、关联模型、统计模型等在内的**6大类**安全分析模型
3. 数据采集和处理性能**>15000EPS**（每条数据大小>1KB）
4. 接入日志源**≧200个**
5. 10亿数据关键字查询结果响应时间**<2秒**
6. 流量吞吐量**≧8Gbps**
7. 新建会话**≧20W**
8. 并发连接数**≧2500W**
9. 采集响应时间**≤1ms**
10. 安全事件预警响应时间**≤5ms**
11. 检索速度支持**千亿级**资产信息的表征化处理与**毫米级**的快速资产检索定位能力

硬件参数

形态	2U机架安全设备	电源	2个热插拔800W交流电源模块，支持1+1冗余
管理接口	1 个10/100/1000BASE-T管理网口	温度	5°C to 45°C
业务接口	4个GE以太网接口，4个万兆光口(SFP+)	尺寸	650*440*89mm
供电	支持220~240V AC		

⋆ 规划中产品规格，具体当前可配置信息以详细产品手册为准。

设备部署



产品亮点

- 大数据基础架构
- 全面的数据采集与分析
- 高性能关联分析
- 多维度精准检测
- 丰富的威胁情报
- 安全风险监测分析可视化
- 自定义业务扩展

客户案例

国家部委

- 中共中央统一战线工作部
- 中华人民共和国工业和信息化部
- 中华人民共和国应急管理部
- 中华人民共和国科学技术部

地方政府

- 北京市东城区人民政府
- 成都市应急管理局
- 深圳市发展和改革委员会

国有企业单位

- 中国国家铁路集团有限公司
- 中国十八个铁路局集团有限公司
- 通号通信信息集团有限公司
- 北京经纬信息技术有限公司

本产品符合以下国家标准：

- GB 42250-2022《信息安全技术 网络安全专用产品安全技术要求》
- GA/T 911-2019《信息安全技术 日志分析产品安全技术要求》（基本级）
- GB/T 37722-2019《信息技术 大数据存储与处理系统功能要求》
- GB/T 38676-2020《信息技术 大数据存储与处理系统功能测试要求》
- YD/T 3734-2020《基础电信企业网络安全态势感知系统技术要求》
- YD/T 2388-2011《网络脆弱性指数评估方法》
- YD/T 2389-2011《网络威胁指数评估方法》
- GB/T 28517-2012《网络安全事件描述和交换格式》
- GB/T 36643-2018《信息安全技术 网络安全威胁信息格式规范》

深圳市永达电子信息股份有限公司
Shenzhen Y&D Electronics Information Co, Ltd.

★ 国家级高新技术企业　★ 国家信息安全服务二级资质企业
★ ITSS二级资质企业　★ 涉密信息系统集成甲级资质企业

地址：深圳市南山区科技北一路17号摩比天线大厦5楼
电话：0755-26727588　传真：0755-26727593
邮箱：sales@s-ec.com
官网：http://www.s-ec.com

售后热线 400-884-0006