文档密级：公开

安全检测平台

Uxsino SecurityCenter

产品介绍

北京优炫软件股份有限公司

目　　录

1 产品概述

优炫安全检测平台（Uxsino SecurityCenter，简称 Uxsino SC）是一款将实时的网络数据包检测、日志分析与风险及漏洞管理相互结合，让企业可以实时并持续地监控威胁和违规行为的综合管理系统。优炫安全检测平台使用全球最为广为人知的风险及漏洞扫描系统，可对网络、WEB 应用服务器、智能移动终端、数据库及应用程序、工业设备、物联网设备、智能网设备等进行深入的扫描作业。

优炫安全检测平台、漏洞扫描系统，可以进行高速扫描、系统配置稽核、资产发现、恶意软件发现、敏感性资料探索、补丁程序管理整合和漏洞分析。优炫软件的漏洞研究团队准确的依据环境需求，提供不断更新的数据库（plugins），目前已支持超过 78,000 个漏洞和系统配置检查。优炫安全检测平台能扩展并适用于最大型的企业环境，而且部署十分容易。

2 优势特点

2.1 产品优势

1. 方便定制以达到企业不同的需求。
   - ✧ 弹性部署、扫描和报告；
   - ✧ Uxsino SC 可透过电子邮件通知扫描结果、漏洞修复建议；
   - ✧ 漏洞修改。
2. 迅速且全面的安全评估。
   - ✧ Uxsino SC 可整合修补程序管理系统（patch management systems），更清晰且有效的识别系统状态；
   - ✧ 提供尚未安装的修补程序列表。
3. 有效降低网络威胁、漏洞、合规和稽核风险。
   - ✧ 扫瞄后以附件方式自动寄出分析结果。
4. 低部署成本。
   - ✧ Uxsino SC 包括了软件更新、合规和稽核档案的在线下载并且享有原厂技术服务；
   - ✧ 自动的漏洞数据库更新。
5. 可利用浏览器随时随地连接到 Uxsino SC。
6. 高度精确的扫描和极低的误报率。
7. 最完整的扫描能力和功能。
8. 易于部属和维护。

2.2 产品价值

优炫安全检测平台可辨识企业内全部的混合式 IPv4/IPv6 的 IT 资产、实时检测系统风险及漏洞、持续监控影响企业安全的变更，让企业全盘了解存在的安全风险，持续监控系统的变化。它还整合了现有网络、安全性和修复系统，提供最新的漏洞分析和实时更新讯息，让企业信息与稽核人员能做出最快与正确的决定。Uxsino SC 具备可自定义的仪表板、报告、高级资产探索，以及支持企业上下各种角色的报告共享功能，方便您轻松监控、分析及交流资讯安全讯息。

使用 Uxsino SC 您可以：

- 消除风险，不仅在有线或无线网络环境，即使是在智能手机、虚拟平台或是云端架构中，仍能持续监控。
- 迅速对 APT、Botnet 攻击和违反企业信息安全规范的行为做出回应。
- 找出已被恶意软件入侵的系统。
- 简化安全事件识别程序。
- 识别信息安全风险。

3 主要功能

- 辨识全部 IT 资产，可侦测包含移动终端等等联机到网络的所有系统、寻找复杂网络区段内不可扫描的资产，并自动评估风险以判定对应的工作。
- 经由统计分析追踪殭尸网络、蠕虫、恶意软件和未经授权的系统变更，并从因特网身分识别、全球威胁数据库及被攻击指针等威胁清单中判断异常状况，达到实时异常活动侦测。
- 透过分析所有用户、系统配置、资产及认证数据,并以网络装置、系统及应用程序的稽核记录，侦测隐藏的攻击者、恶意软件及造成危害的系统，让企业可以加速事件响应。
- 提供高级分析以及数据相互关联技术，内置多种可订制化报告，协助您识别和响应安全与法规遵循的问题。
- 主动监控违反企业规范情事，可在遇到偏差状况时发出警示，并持续追踪是否符合法规要求，以供稽核。
- 执行稽核与法规遵循报告，依据业界标准及法规授权范围，例如 FISMA、PCI DSS、HIPAA/HITECH、DHS CDM 及 DISA STIG，落实以结果为导向并兼顾安全性与合规性的安全性措施。
- 依照不同角色层级制订报告、警示和动作，企业可依照自有组织架构制订和发布安全报告。
- 结合企业既有信息安全，网络设备和系统等信息，透过优炫软件强大的自动关联与分析技术，为企业提供实时的安全管理平台，找出企业内主要的安全风险，准确反应资安事件。
- 有效监控 APT（高级持续威胁）攻击，提供实时分析，协助企业阻绝攻击。

4 Uxsino SC 组件介绍

4.1 Nessus 主动式漏洞扫描引擎

Nessus 为业界部署最广泛的漏洞扫描、系统配置与合规性验证产品。全球已超过 2 万 4 千家企业使用，在信息安全和法规遵循产品中，获得众多专业人士认可。Nessus 可以进行高速扫描、系统配置稽核、资产发现、恶意软件发现、敏感性资料探索、补丁程序管理整合和漏洞分析。优炫软件的漏洞研究团队准确的依据环境需求，提供不断更新的数据库（plugins），目前已支持超过 78,000 个漏洞和系统配置检查。Nessus 能扩展并适用于最大型的企业环境，而且部署十分容易。

4.2 PVS 被动式流量安全扫描引擎

Passive Vulnerability Scanner（PVS）被动式流量安全扫描是一项已取得专利的网络监测及漏洞分析技术，可由非侵入性方式提供持续即时的网络状态剖析及监控。PVS 被动式安全扫描能在网络通讯中监控 IPv4 与 IPv6 网络，以判定拓朴结构、网络服务、网络流量和漏洞。而整合了 PVS 被动式安全扫描的 Uxsino SecurityCenter，还能集中分析日志、管理漏洞,让您全面检视企业的安全状况。

4.3 LCE 日志关联分析引擎

Log Correlation Engine（LCE）日志关联引擎，能针对网络和系统中的事件做日志分析，例如来自原始网络通讯、入侵检测及永久储存系统、防火墙、服务器、应用程序与用户活动……等等，进行汇总、正规化、相互关联和分析。通过整合、关联和分析从整个企业的网络设备（包括基础网络和安全设备）、主机和应用程序服务器收集的日志记录，执行可行性及安全分析。透过自身的动态负载平衡机制，能让多台 LCE 日志关联引擎一同运作，由 Uxsino SecurityCenter 平台进行事件与日志分析。