 DOI: https://doi.org/10.12349/iser.v4i5.1731

Research on the Application of Network Security Situation Awareness Platform Based on Big Data

Wei Wang Shan Huang Yafeng Wang

College of Big Data and Artificial Intelligence, Shaanxi Technical College of Finance & Economics, Xianyang, Shaanxi, 712000, China

Abstract

In order to ensure the network information security monitoring and early warning capability, and realize the accurate identification of asset data, this paper applies big data technology, from the platform overall architecture design, platform construction process design two aspects, complete the design of network security situation awareness platform, and apply the platform to an enterprise. The results show that under the application background of big data technology, the network security situational awareness platform built in this paper effectively improves the overall network security guarantee capability of enterprises, ensures the efficiency and effect of security event processing, and fully meets the expected design standards and requirements. Hope that through this study, to provide an effective reference and reference for the relevant personnel.

Keywords

big data; network security; situational awareness; platform application

基于大数据的网络安全态势感知平台的应用研究

王伟 黄珊 王亚凤

陕西财经职业技术学院大数据与人工智能学院，中国 · 陕西 咸阳 712000

摘 要

为保证网络信息安全监测预警能力，实现对资产数据的精确化识别，论文应用大数据技术，从平台总体架构设计、平台建设过程设计两个方面入手，完成对网络安全态势感知平台设计，并将该平台应用于某企业中。结果表明：在大数据技术的应用背景下，论文所构建的网络安全态势感知平台有效地提高企业总体网络安全保障能力，保证安全事件处理效率和效果，完全符合预期设计标准和要求。希望通过这次研究，为相关人员提供有效的借鉴和参考。

关键词

大数据；网络安全；态势感知；平台应用

1 引言

在信息时代背景下，网络威胁变得越来越复杂化、多样化，其技术先进性不断提升，传统计算模式过于落后，无法满足抵御网络威胁需求 [1]。而网络安全态势感知平台的构建和应用，可以有效地解决以上问题，该平台运用大数据技术，有效地执行网络安全检查、资产数据梳理、风险识别等环节，保证网络信息安全监测预警能力。因此，在大数据技术的应用背景下，如何科学地设计和应用网络安全态势感知平台是技术人员必须思考和解决的问题。

2 平台设计

2.1 平台总体架构设计

首先，网络安全态势感知平台在具体设计时，要结合网络管理对象、运营支撑系统，对各种安全事件、漏洞、流量等信息进行实时采集，全面地了解和掌握互联网安全状态。其次，从关联分析安全告警信息、取证流量信息、对比威胁信息等方面入手，综合判断和分析所采集好的信息。同时，还要结合安全事件出现源头、涉及范围，提出具有建设性的建议 [2]。最后，将安全管理与最终分析结论进行结合，保证网络风险处理质量。系统功能设计示意图如图 1 所示。

2.2 平台建设过程设计

在大数据技术的应用背景下，为保证网络安全态势感知平台设计质量，技术人员要严格按照如图 2 所示的平台建设过程，对该平台进行科学化构建。

2.2.1 安全管理咨询阶段

对网络安全管理现状进行调研和收集，并分析网络安全管理存在的漏洞和不足。为保证网络安全管理现状调研和梳理的全面性，技术人员严格按照网络安全规范和要求，对安全管理工作存在的问题进行分析和评估，从而确定出需要

【作者简介】王伟（1979–），男，中国陕西西安人，博士，高级工程师，从事计算机、人工智能、大数据研究。

优化的事项，这为后期网络安全态势感知平台的构建提供重要的数据支撑 [3]。强化对网络安全管理体系的优化和完善，并形成一套健全网络管理制度。为了实现以上目标，需要根据所调研的数据，对网络安全管理制度进行优化和完善，并确定出网络管理重点和目标。

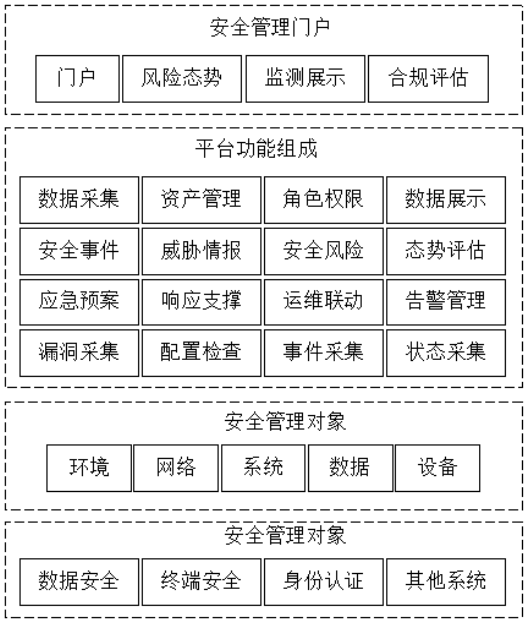

图 1 平台功能设计示意图

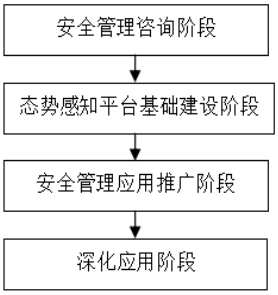

图 2 平台建设过程

2.2.2 态势感知平台基础建设阶段

①系统建设实施。

对该态势平台系统进行调试，确保该系统可以成功上线运行，借助网闸设备，运用访问控制方案，将互联网数据准确、高效地导入到该平台中，并将这些信息数据统一呈现在商网内。

②资产梳理与接入。

在采集和汇总互联网网络资产相关信息的基础上，确定出网络安全监测内容，获取各项安全设备数据，在格式化处理安全设备告警信息的基础上，对数据进行高质量化、高标准化管理，同时，还要智能化、全面化监测和分析网络安全数据 [4]。

③数据接入标准规范。

制定平台数据接入规范体系，确定接入数据的种类、属性和内容等参数，为后期平台数据准确化接入创造了良好的条件。

④定义安全场景、建立分析模型。

结合网络安全需求，确定出以下两大网络安全场景：

第一，网络安全合规性场景。该场景主要是指根据网络安全相关法律法规，构建工作时间访问互联网分析模型。

第二，网络安全攻防场景。该场景主要是指结合主流网络安全攻击内容，构建端口探测扫描分析模型。

当场景定义和分析模型构建结束后，运用该平台从海量安全数据中，对安全分析模型与相关规则进行有效地匹配，从而保证安全告警处置质量，避免因人工分析事件不精确而导致安全告警出现漏洞问题。

2.2.3 安全管理应用推广阶段

①安全管理功能开发。

严格按照网络安全通道管理相关标准和要求，对保护信息填报功能、网络安全通报管理功能进行有效开发和实现，并应用网络安全态势感知平台，对管理工作流程进行固化处理。

②单点登录技术实现。

在集成化开发和实现网络安全态势感知平台、统一用户管理平台、人力资源管理系统的基础上，将网络安全工作人员数据信息准确无误地导入和传输到该平台中，确保用户采用单点登录的方式，正常登录和访问该平台。

③应用推广。

明确用户在该平台中使用权限，并在汇总和整理网络安全等级保护信息的基础上，对网络安全通道工作进行全面落实。

2.2.4 深化应用阶段

①扩展技术功能。

为实现对该平台技术功能的优化和完善，技术人员要重视对网络安全流量回溯分析功能、配置检查功能的开发和实现，确保该平台具有安全事件追溯能力高、取证能力强等特点，便于用户借助该平台合理化配置网络资产信息。

②完善态势呈现功能。

为保证网络安全事件监测的全面性和实时性，技术人员要借助该平台直观形象地呈现网络安全宏观发展趋势，并开发和实现平台态势显示功能，并采用大屏展示的方式，将该平台态势信息呈现在用户面前。

③建立安全运营体系。

该平台在具体运行时，要结合网络安全事件监测情况、强化对安全事件处置体系的制定和优化，同时，还要构建和完善侵害安全运营制度，并从网络安全风险监测、日常通报检查、安全时间处置等多个方面入手，制定一体化安全运营体系，确保网络安全工作落实到位。

3 平台应用案例

某企业在参与网络安全攻防演习活动时，运用该平台依次落实互联网安全监测、安全事件分析、预警信息收集等工作，并制定相关监测体系，以达到实时化监测互联网运行状态、安全事件以及相关异常行为，取得显著应用效果，其

应用成效如下。

3.1 互联网侧

3.1.1 安全监测

在进行企业互联网监测时，要运用网络安全态势感知平台对数入侵防御系统、防火墙技术、威胁情报监测技术等先进技术，实现对相关告警信息的自动化采集，同时，运用网络流量监测系统,定位和识别网络攻击流量数据、告警事件等，并结合所确定的攻击源网络协议地址，分析网络攻击特发。

3.1.2 分析处置

互联网网络攻击事件分析处置内容如下：分析和判断攻击特征的识别，对目标系统所造成的影响，并借助攻击源 IP，对攻击源进行追溯。一旦发现互联网存在异常行为，需要借助网络流量分析系统，对原网络攻击流量数据进行还原处理，并根据防护设备相关告警信息，对攻击特征进行精确化识别，以实现对攻击源 IP 地址的追溯和确定，在此基础上还要采用操作系统日志审计的方式智能化检测系统账户登录信息、操作记录信息等重要信息的，分析和判断系统是否被恶意攻击和破坏。

3.2 商网侧

3.2.1 安全检测

在进行商网监测期间，要借助该平台，集中化采集和分析各个监测设备相关告警事件信息。同时，还要对网络安全攻击源头进行初步化定位，并运用网络流量监测手段，对降低安全误报出现概率，从而保证攻击特征识别结果的精确性和真实性，这样一来，不仅可以智能化监测和处置安全告警事件，还能有效地整改和处理网络异常行为，避免互联网出现一系列安全隐患问题。

3.2.2 分析处理

①网络安全攻击事件。

对于商网而言，在分析其网络攻击事件时，要综合运用流量回溯分析法、攻击数据模拟法，对攻击事件进行综合分析和判断。

在这个过程中：首先，要从威胁情报系统中，采集和对比病毒恶意域名、出错主机，并对疑似被网络病毒感染的主机进行精确化定位。其次，结合商网入侵检测系统的安全事件告警信息，应用网络流量分析系统，对其流量进行回溯分析，确保攻击代码还原初始状态。同时，还要在准确化识别攻击特征的基础上，筛选和删除部分误报告警信息。最后，在分析应用系统漏洞问题时，要采用流量分析法，收集所需要的攻击代码，并采用伪造信息的方式，完成对特定访问链接的构建，这为后期有效验证、修复系统漏洞问题提供重要的依据和参考。

②异常访问事件。

在分析商网异常访问行为时，要运用访问控制法，综合分析和判断异常行为特征。一方面，应用商网邮件系统，综合分析邮件账户异常访问事件，同时，采用回溯分析的方式，综合分析垃圾邮件网关日志信息，经过分析，如果没有发现恶意收发恶意邮件行为，说明邮件账户安全，不存在被恶意控制的问题。另一方面，对部分数据库异常访问行为、系统异常登录行为进行监测和分析，并与系统管理员进行配合，核实这些行为是否正常，经过核实，发现这些行为属于正常访问时，说明数据库和系统安全，不存在被恶意攻击和操控的风险。

4 平台应用效果

应用大数据技术所设计的网络安全态势感知平台应用效果如下。

4.1 积极防护，构建主动防御体系

企业借助该平台，可以构建网络安全防护、网络安全审计、安全事件响应等一体化安全防护体系，运用该体系，可以对安全源头进行审计和追溯，同时，采用安全加固法，对网络安全危害蔓延趋势进行实时监测和控制，将网络安全风险降到最低。

4.2 优化机制，形成协同保障能力

运用该平台，可以制定一套系统、完善的网络安全工作机制，借助该机制，可以更好地明确企业所有员工的职能，同时，还能对企业相关网络安全事件处理流程进行有效地优化和完善，提高企业发现和处置安全事件能力，将企业网络安全风险降到最低。

5 结语

综上所述，论文所设计的网络安全态势感知平台通过综合运用大数据技术、安全技术等先进技术，依次落实安全管理、安全运营等环节。在这个过程中，实现通过构建平台上下级联架构，实时上报、呈现安全时间、预警等相关信息。此外，严格按照网络安全标准和要求，评估和预测安全管理工作存在的漏洞和缺陷，同时，统一管控所采集好的应急响应相关数据，并形成集安全监测、安全检查、安全处置为一体化的安全运营体系。

总之，在大数据技术的应用背景下，论文所设计的网络安全态势感知平台具有较高的应用价值和应用前景，值得被进一步推广和应用。

参考文献

[1] 陈迎春.构建支撑网络安全态势感知的大数据平台[J].青海科技,2021,28(1):55-57.

[2] 胡志军.基于大数据的网络安全态势感知平台的应用思考[J].金融科技时代,2019(10):44-46.

[3] 包利军.基于大数据的网络安全态势感知平台在专网领域的应用[J].信息安全研究,2019,5(2):168-175.

[4] 和乾.大数据技术的网络安全态势感知平台分析[J].计算机产品与流通,2022(12):184-186.