企业网络信息安全自动化防护方案浅析

Analysis on Automatic Protection Technology of Enterprise Network Security

赵奕霖[1]，沈　涛[1]，宋齐军[1]，杜　锋[2]，马朝暾[1]（1. 中讯邮电咨询设计院有限公司郑州分公司，河南 郑州 450007；2. 中讯邮电咨询设计院有限公司，北京 100048）

Zhao Yilin[1], Shen Tao[1], Song Qijun[1], Du Feng[2], Ma Zhaotun[1] (1. China Information Technology Designing & Consulting Institute Co., Ltd. Zhengzhou Branch, Zhengzhou 450007, China; 2. China Information Technology Designing & Consulting Institute Co., Ltd., Beijing 100048, China)

摘　要：

随着数字经济的蓬勃发展，各行各业迎来数字化转型新机遇，这对企业安全防护提出了更高的要求。传统的基于安全管理人员手工接收情报指令、操作安全设备与系统进行安全防护的模式面临越来越多的挑战和困难，安全防护自动化、智能化势在必行。简要介绍和分析了企业网络安全管理各环节自动化防护场景，并探讨了运用软件开发技术实现网络自动化防护，以降低企业安全管理成本、提高安全管理可靠性的可行性方案。

关键词：

网络安全；自动化防护；自动化监测；自动化处置

doi：10.12045/j.issn.1007-3043.2022.09.015

文章编号：1007-3043(2022)09-0071-06

中图分类号：TN915.08

文献标识码：A

开放科学(资源服务)标识码(OSID)：

Abstract:

With the vigorous development of digital economy, all industries welcom new opportunities for digital transformation, which puts forward higher requirements for enterprise network security protection. The traditional security protection mode based on security managers manually receiving superior instructions, operating security equipment and system is facing more and more challenges and difficulties. Therefore, intelligent and automated network security protection is imperative. It briefly introduces and analyzes the automatic protection scenarios of each link of enterprise network security management. Meanwhile, it discusses the feasible scheme of using software development technology to realize network automatic protection, so as to reduce the cost of enterprise network security management and improve the reliability of network security management.

Keywords:

Network security; Automatic protection; Automatic monitor; Automatic handling

引用格式：赵奕霖，沈涛，宋齐军，等. 企业网络信息安全自动化防护方案浅析[J]. 邮电设计技术，2022(9)：71-76.

0 前言

“十四五”以来，数字经济蓬勃发展，各行各业迎来了数字化转型新机遇，越来越多的数字化生产类、管理类、创新类业务平台应运而生，随之而来的网络安全风险和问题逐渐成为企业发展的重大威胁[1,2]。作为建设网络强国、发展数字经济的基石，网络安全关乎着企业发展、国家安全、人民幸福。鉴于此，提升网络基础设施运行安全保障能力，构筑网络空间安全可信的第1道防线，成为企业网络安全防护工作的重中之重。随着来自网络空间的安全威胁与安全攻击日益剧增，传统企业网络信息安全防护模式面临着越来越多困难和挑战，探索一种能降低企业安全管理成本同时提高安全管理可靠性的网络信息安全自动化、智能化防护方案势在必行。

1 企业网络信息安全防护现状与不足

随着网络和信息技术的高速发展和普及，信息化

收稿日期：2022-07-01

已经成为现代企业生存和发展的必备条件。通过建立企业局域网[3]（内网），并在其基础上开发与应用各种基础专业软件，可有效地实现企业内部的资源共享、信息发布、技术交流、生产组织。此外，通过互联网出口与外网相连，企业可方便地实现内外部信息双向交互。然而，信息的双向交互在为企业信息化、数字化发展提供便利的同时，也给企业带来了来自外部网络世界的安全威胁和安全攻击。为有效应对威胁和攻击，企业通常会采购诸如边界防火墙、IDS、态势感知系统、防病毒网关等安全管理设备，并安排专职安全管理人员、安全技术人员运用这些设备或系统进行手工安全防护[4-6]。随着来自网络空间的安全威胁与安全攻击日益剧增，传统的手工安全防护模式面临越来越多的挑战和困难，主要包括以下方面。

a）安全防护任务繁重，安全管理人工成本高。企业网络安全管理及安全技术人员除要应对来自网络空间的日常安全攻击外，往往还要承担着特殊时期的安全重保工作，随着企业互联网暴露面系统不断增多，安全防护任务越发沉重，企业用于投入安全工作的人力成本直线上升，这给企业生产经营带来了一定负担。

b）安全防护系统与设备种类繁多，统一管理难度大。企业往往会根据自身安全防护需要采购多家安全公司的、不同种类不同功能的安全防护系统和设备。在未统一拉通管理的前提下，如此繁多的安全系统与设备给安全管理和技术人员带来了更高的学习成本，也给企业统一安全管理造成了很大的困难。

c）重复劳动量大，耗时耗力且易出错。在日常网络信息安全防护工作中，存在着大量人工重复劳动的工作场景。例如，日常办公网威胁告警监测、攻击IP封堵处置、业务系统安全漏扫等。这些重复工作占据了安全管理员大量时间，且易出错，这很大程度上制约了安全管理工作效率和质量的提升。

d）安全防护工作台账管理不善。目前大部分企业安全管理工作依靠线下方式（微信、钉钉、邮件、excel等）进行，安全防护工作信息留痕不充分、台账记录往往较为随意、不系统，这给后续安全事件复盘和总结带来了很大困难，从而一定程度上制约了企业网络信息安全防护工作的持续改进。

2 企业网络信息安全自动化防护解决方案

近年来，为解决传统手工安全防护工作存在的问题和不足，业内对网络安全自动化防护技术进行了研究，但大都停留在理论层面，且应用场景有限[7-9]。针对这些问题，本文提出了一种可落地应用的基于企业内部统一安全管控平台（以下简称平台）的自动化安全防护解决方案。平台主要包括数字化资产统一管理、数字化安全工作台账管理、自动化安全大脑情报与威胁告警信息统一收集、自动化安全研判分析与防御处置调度、自动化安全防御处置执行五大基础模块。其中，数字化资产统一管理模块负责对企业基础网络设备（防火墙、路由器、交换机等）、业务系统资产（IP资产、Web资产、中间件、数据库等）进行统一线上化管理以替代传统线下资产管理模式；数字化安全工作台账管理模块负责对各项安全管理或防护工作进行全生命周期自动化、系统化记录，并永久存储。以上2个模块是平台的基础服务提供模块。下边具体介绍平台的三大业务模块。

2.1 自动化安全大脑情报与威胁告警信息统一收集

该模块是平台的“哨兵”、“千里眼”。安全情报主要来自于外部收集（上级指挥调度平台或安全大脑情报中心）与内部监测（IDS、态势感知等）2种渠道。如图1所示，基于自动化技术的企业安全情报收集机器人（以下简称情报收集机器人）拉通了企业各级安全情报和威胁监测系统，实现全自动内外部情报、威胁收集功能，能有效解决传统情报收集方式成本高、效率低的问题。

该情报接收机器人包括定时任务管理、后台API调用、Web-driver、OCR文字识别、数据处理与存储模块。

定时任务管理模块负责统一调度管理各平台的情报收集任务。安全管理员可定制化调整各平台的任务执行策略。

情报机器人通过向各平台主动发送Web API请求（数据爬虫）收集各平台情报数据。基于API请求的情报收集速度通常较快（单次毫秒级）。然而部分网站出于安全考虑会通过技术手段限制后台API接口爬虫，基于Web-driver的数据抓取则不受此影响。其原理是通过程序自动操作浏览器，模拟人进行页面操作，达到信息收集的效果。其缺点则是操作速度慢[10]。表1为2种数据抓取模式的详细对比，通常建议优先使用API接口调用获取数据，当API调用受限时，使用Web-driver作为替代方案。

部分网站会使用验证码校验技术，这给信息自动

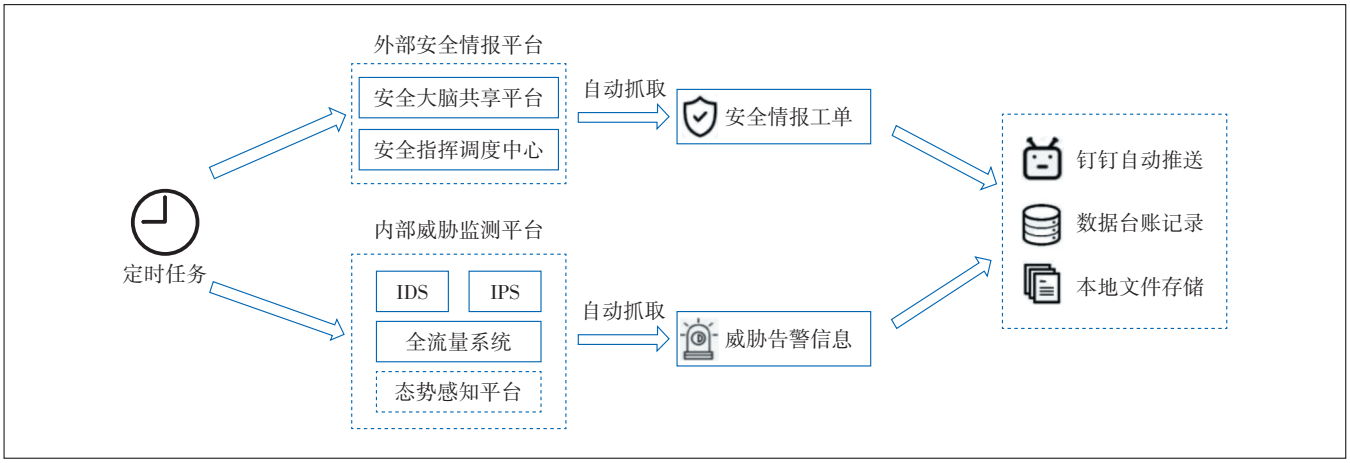

图1　基于自动化技术的企业安全情报收集机器人

表1　安全情报数据抓取方案对比

方案	原理	效率	抓取限制
API接口调用	程序后台调用API获取数据	抓取效率高（单次毫秒级）	易受网站技术手段限制，导致爬取失败
Web-driver访问	程序驱动浏览器，模拟人进行页面操作	抓取效率相对低	几乎不受任何技术限制

抓取带来了很大的困难。OCR文字识别模块负责情报抓取过程中验证码的智能识别。具体步骤为先保存验证码截图，再进行智能去噪点，最后完成OCR智能文字识别。对经常识别出错的字符，可以运用机器学习技术进行有针对性的样本训练[11]，在训练得当的情况下识别成功率可显著提升。

完成情报信息收集后，需要对威胁告警信息进行自动分析、整合、存储，为后续安全防护工作提供情报信息支持。

2.2 自动化安全研判分析与防御处置调度

在传统的安全防护体系中，接收到情报或威胁（以下间称安全事件）后，由安全专家进行研判分析，安全管理员负责处置调度。在处理过程中，大量的数据取证（日志、会话、告警记录）工作和处置调度均依靠纯手工操作，耗时耗力且效率低下。

自动化安全研判分析与防御处置调度机器人可有效实现关键信息提取、研判分析数据预收集以及防御处置自动调度。其主要有两大类应用场景。

2.2.1 常态化安全防护工作全自动化研判分析与防御处置（场景1）

诸如每日漏洞预警处置、IP封堵、终端扫描等此类常态化安全工作可实现全自动化研判分析与防御处置。以每日漏洞预警处置为例，传统的漏洞预警完全依靠人工管理，这种管理模式耗时耗力且无法实现漏洞影响面的精准管理。如图2所示，基于漏洞特征值-资产台账关联的漏洞精准化预警可有效解决上述

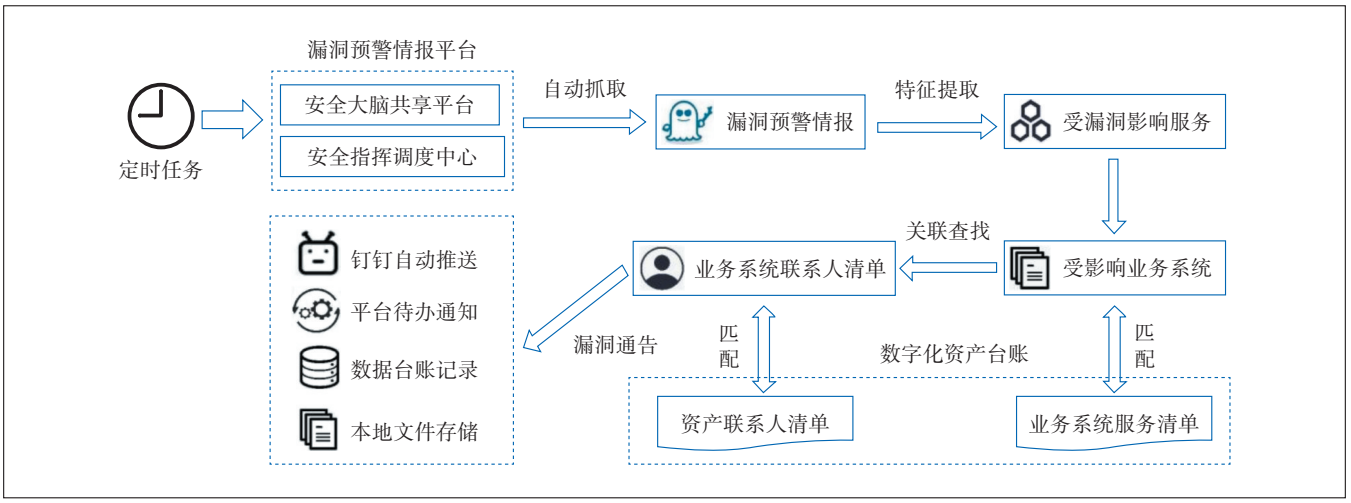

图2　每日漏洞预警自动分发处置机器人

问题，其实现步骤如下：

步骤1：开启定时任务，查询最新漏洞预警工单并进行关键信息提取，包括名称、级别、受影响的服务、防护或修复建议等。例如，接收到“Spring RCE漏洞”，级别为高危，JDK9及以上版本会受此漏洞影响，防护建议为接入WAF并启动*.class过滤。

步骤2：通过漏洞特征值匹配技术将漏洞影响面与业务系统资产台账进行关联，精准匹配出受漏洞影响的业务系统。例如，A业务系统采用JDK9，与该漏洞的特征信息匹配，故A系统会受此漏洞影响，需要进行重点预警通告。

步骤3：向受影响的业务系统负责人或安全管理员发送漏洞警报并记录系统台账便于后续管理。

2.2.2 突发安全事件关键信息智能提取与研判数据取证（场景2）

在安全日常管理工作中，例如某IP攻击内网、某终端染毒、某钓鱼邮件被转发等突发安全事件也时有发生。这类事件场景中，自动化安全研判分析与防御处置调度机器人可实现关键信息智能提取与研判数据取证，为专家研判提供依据。

以公网IP攻击行为排查（见图3）处置为例，假定企业接收到安全事件工单——“近日情报中心发现192.168.124.162曾出安全攻击事件，请核查近一个月内是否存在与该地址的交互记录，并研判影响。”（以下简称IP攻击排查工单），该方案的执行步骤如下：

步骤1：开启定时任务，查询到该IP攻击排查工单。

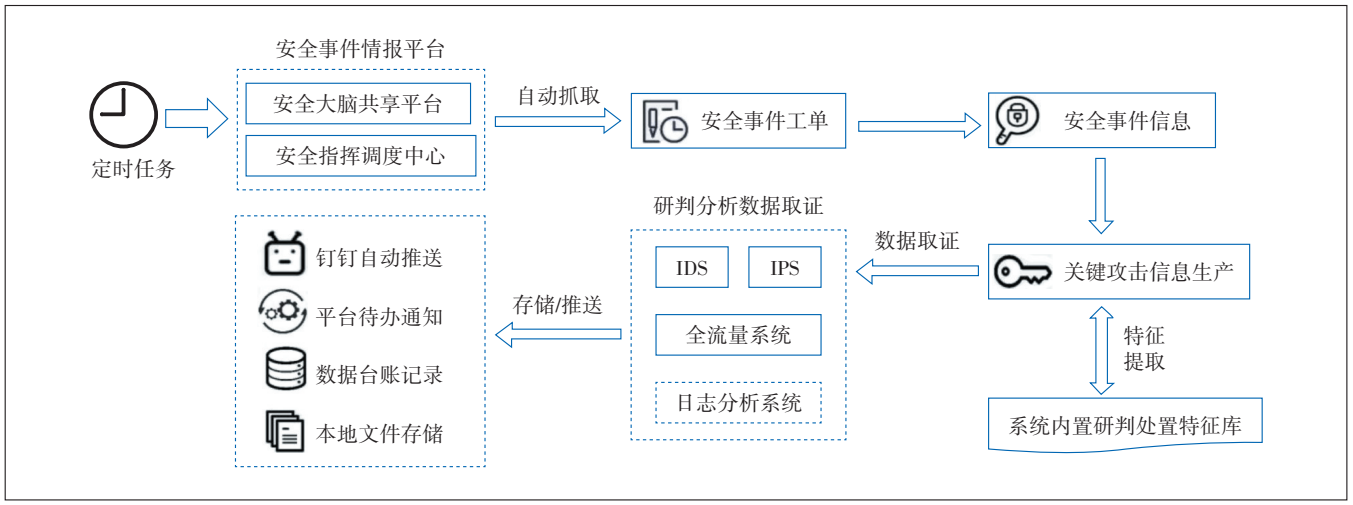

图3　IP攻击排查事件研判数据取证机器人

步骤2：对该工单进行包含“源—行为动作—目的—处置操作—时间窗口”的关键信息提取，对应上例，即源（192.168.124.162）—行为动作（安全攻击）—目的（公司内网）—时间窗口（1个月）—排查内容（访问记录）。

步骤3：根据关键信息，自动匹配防御处置调度策略，在本例中，机器人将自动查询最近1个月192.168.124.162的会话记录（全流程系统）、访问告警日志（IDS、态势感知），并将结果整合、导出为文件，为专家研判分析提供数据支持。

为提高安全事件关键信息提取成功率，可对同一类事件内置多个特征标签描述。除此之外，还可考虑使用自然语言处理技术（NLP）改进关键描述信息识别能力[12]，以实现更加智能的网络安全研判分析与防御处置调度。

2.3 自动化安全防御处置执行

安全防御处置大都遵循标准化模式，因此其适于软件工具自动化、批量化处理。相比传统人工方式，自动化技术的引入让处置效率显著提升，人为出错概率也大大降低。

下面就2个典型的自动化防御处置应用场景举例说明。

2.3.1 自动化威胁IP封堵机器人（场景1）

如图4所示，自动化威胁IP封堵机器人（以下简称封堵机器人）可用于攻击IP全自动收集、解析、封堵、通知。具体实现步骤如下：

步骤1：平台接收到IP封堵处置工单，将待封堵IP

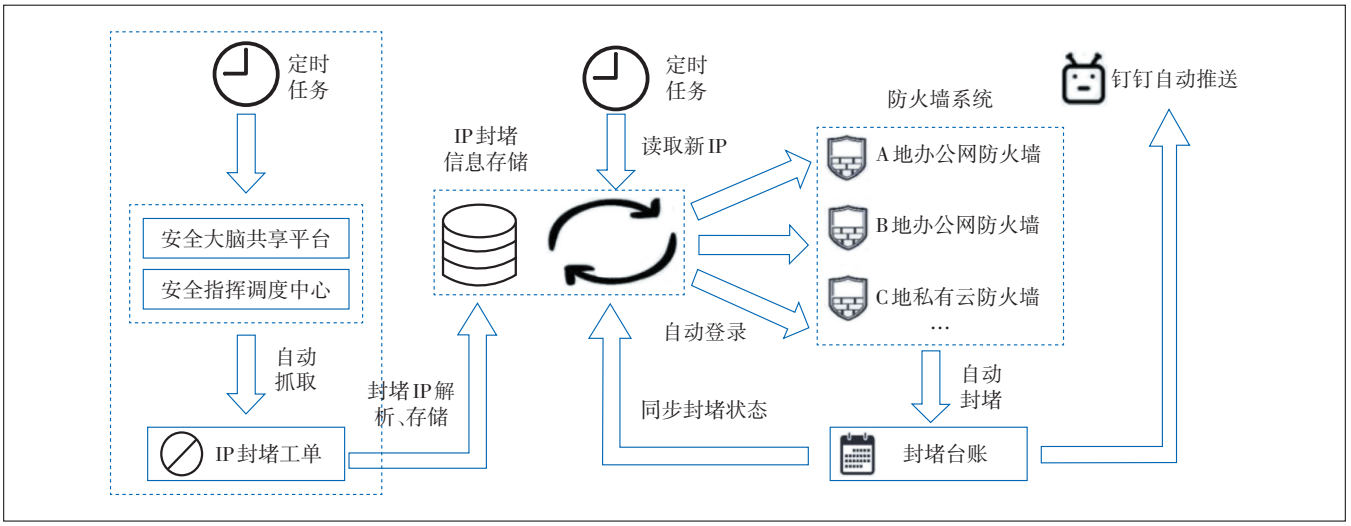

图4　自动化威胁IP封堵机器人

列表存入数据库中。

步骤2：封堵处置调度器定时启动，从数据库中加载待封堵IP列表。

步骤3：依次登录公司各地防火墙，执行IP封堵操作。需要注意的是，各安全厂商防火墙封堵处置操作步骤不同，需要定制化编写封堵脚本。

步骤4：封堵成功后，同步修改至数据库中，并自动将消息推送给安全管理人员。

步骤5：若封堵失败，记录异常日志信息，并推送给安全管理人员，人工介入排查，完成线下修复后，重新执行封堵，直至成功。

2.3.2　自动化安全漏扫调度执行机器人（场景2）

如图5所示，自动化安全漏扫调度执行机器人（以下简称漏扫机器人）可实现对指定业务系统的全自动安全漏扫检查。具体实现步骤如下：

步骤1：平台接收到关于某业务系统的攻击事件，安全团队决定对该系统进行安全漏扫检查，放入待执行队列中。

步骤2：漏扫机器人定时启动，依次调用各漏扫工具执行安全检查。需要注意的是，各漏扫工具操作步骤不同，需要定制化编写漏扫执行脚本。

步骤3：调度器定期监测漏扫任务的执行情况，并将漏扫结果整合成最终报告，发送至相关安全管理人员处。

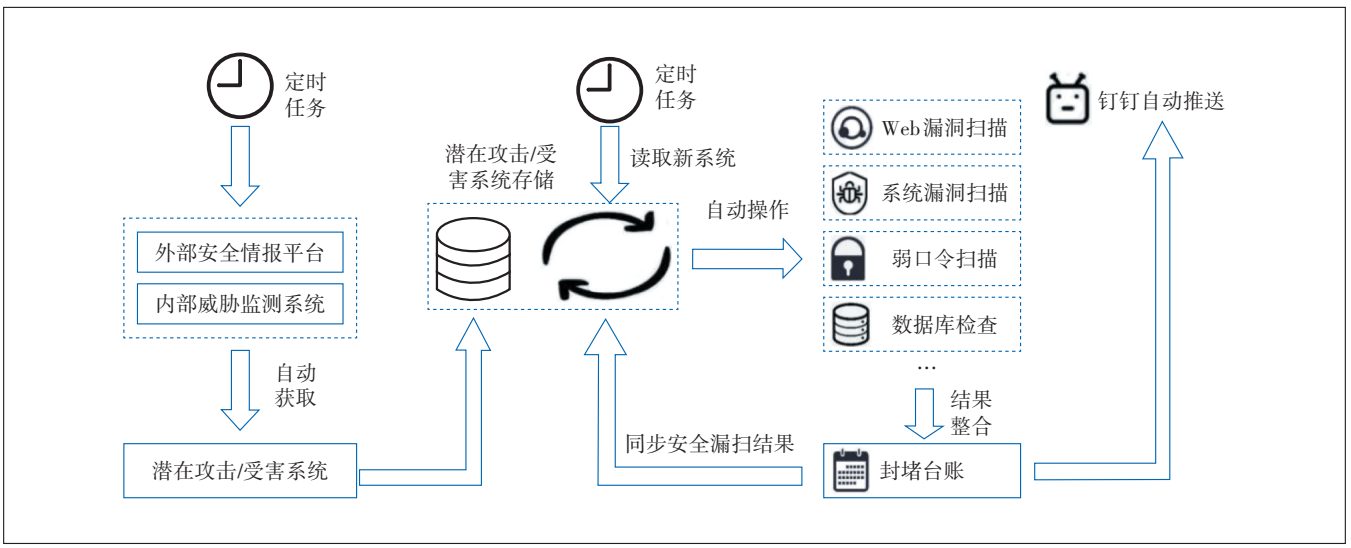

图5　自动化安全漏扫调度执行机器人

步骤4：若漏扫工作执行失败，记录异常日志信息，并推送给安全管理人员，人工介入排查、完成线下修复后，重新执行漏扫，直至成功。

3 应用效果

目前，本文提出的自动化防护解决方案已经在某企业安全防护中得到了实际部署与应用，经过了多轮安全专项检查的验证，取得了良好效果，相较于传统手工安全防护，其存在如下显著优势。

a）人员配置更加合理。以应用该方案的企业为例，在采用该方案前，该企业投入了多名技术人员参与日常安全防护工作，这些技术人员需要花费大量精力忙于日常安全情报收集、防御处置执行等重复性劳动，导致人手紧张；采用该方案后，安全情报收集与防御处置执行实现了全流程自动化，仅需安排1~2名专职人员值班即可，其余人员可专注于研判分析和安全方案研究等高精技术工作。相较于传统的手工安全防护，该方案缓解了技术人员紧张的问题，提升了防护效率。

b）安全事件响应、处置速度快。相较于人工处理，基于自动化程序的安全事件响应与处置速度大大提高。以该企业为例，在采用该方案前，单个安全情报、威胁告警的收集时间、单次IP封堵、安全策略配置、终端杀毒的执行时间平均为30 min；采用该方案后，平均响应与处置时间降到3 min以内（经过多轮安全专项检查验证），闭环时间提升一个数量级。

c）安全防护可靠性高。本文提出的安全防御处置是基于全自动化工具的，可有效避免人为误操作导致的安全事故发生。以该企业为例，在采用该方案前，诸如IP误封堵、漏封堵、安全策略误配置等安全事故时有发生，采用该方案后，此类安全防御处置都采用全自动化实现，通过应用程序内置的状态监测、异常处理与故障恢复机制，使安全防护可靠性得到了显著提高，至今未发生具有影响力的安全事故。

4 结束语

随着信息技术不断发展，企业面临越来越多来自网络空间的安全威胁与安全攻击。本文分析总结了当前企业网络信息安全防护模式所面临的困难和挑战，并根据网络信息安全管理要求，提出了一种基于内部统一安全管控平台的企业网络安全自动化防护解决方案。该方案可以实现企业安全防护主要流程、工作自动化，并为企业系统化、科学化、智能化安全防护提供实际的指导帮助。不仅可以有效降低企业安全管理成本，还能显著提高企业安全管理可靠性。目前，需要注意的是，网络安全防护不是一劳永逸的事情，本文提供的方案对未来可能面临的新的安全问题难免会有遗漏之处，安全防护人员需要根据新的问题不断改进防护策略和技术手段，筑牢企业网络安全防线。

参考文献：

[1] 国家计算机网络应急技术处理协调中心. 国家计算机网络应急技术处理协调中心[EB/OL]. [2022-05-21]. https://cit.buct.edu.cn/2021/0925/c7951a157921/page.htm.
[2] 奇安信行业安全研究中心，齐安信态势感知第1事业部，网络空间测绘系统（全球鹰），等. 2021中国网站安全报告[EB/OL]. [2022-06-01]. https://www.163.com/dy/article/H97JQSRD0531NODR.html.
[3] 张新月，曹嘉翼，江江，等. 企业局域网规划与设计[J]. 电脑知识与技术，2019，15(1)：63-64.
[4] 马利，姚永雷. 计算机网络安全[M]. 北京：清华大学出版社，2010.
[5] 王明胜. 企业局域网网络安全问题与应对策略分析[J]. 网络安全技术与应用，2021(10)：112-114.
[6] 韩冰. 网络安全实战攻防演练防守方初探[J]. 广播电视网络，2022，29(3)：44-46.
[7] 崔永波，潘东雷. 检察机关网络安全事件应急处置研究[J]. 网络安全技术与应用，2021(8)：123-124.
[8] 陈洁，严聪，冉豪，等. 网络安全智能化与自动化技术应用研究[J]. 信息系统工程，2022(4)：149-152.
[9] 李慧芹，汪亚娟，刘爽，等. 网络安全防护中的一种智能化解决方案[J]. 网络安全技术与应用，2022(2)：14-15.
[10] 李晨昊. 基于BeautifulSoup+requests和selenium爬虫网页自动化处理的实现和性能对比[J]. 现代信息科技，2021，5(16)：10-12，18.
[11] 潘浩，李兰. 基于Tesseract引擎样本训练的验证码识别[J]. 信息与电脑，2020，32(1)：138-139，142.
[12] 刘奇飞，沈炜域. 基于Word2Vec和TextRank的时政类新闻关键词抽取方法研究[J]. 情报搜索，2018(6)：22-27.

作者简介：
赵奕霖，工程师，硕士，主要从事软件开发和网络安全技术管理相关工作；沈涛，高级工程师，硕士，主要从事软件开发、网络安全技术管理相关工作；宋齐军，教授级高级工程师，硕士，主要从事软件开发和网络安全技术管理相关工作；杜锋，高级工程师，学士，主要从事网络安全、数据安全技术管理相关工作；马朝暾，工程师，主要从事网络安全、数据安全技术管理相关工作。