智能化网络安全监测预警平台建设和运营思路探讨

Discussion on Construction and Operation of Intelligent Network Security Monitoring and Early Warning Platform

黄昌熙，朱　磊，余润泽，滕泽滨（华信咨询设计研究院有限公司，浙江 杭州 310052）
Huang Changxi，Zhu Lei，Yu Runze，Teng Zebin（Huaxin Consulting and Designing Institute Co.，Ltd.，Hangzhou 310052，China）

摘　要：
数字化转型背景下，信息网络面临的安全风险和威胁形势愈发严峻，传统的安全防护和监测预警技术已经无法应对高级可持续威胁（APT）攻击带来的挑战，网络安全开始向智能化方向发展。通过分析智能化监测预警平台的技术架构，提出基于海量多源数据采集和智能分析引擎的监测预警平台建设思路，结合全流程的安全运营服务支撑，变被动防御为主动，实现安全闭环管理。

关键词：
大数据；智能分析引擎；监测预警；安全运营
doi：10.12045/j.issn.1007-3043.2023.01.006
文章编号：1007-3043（2023）01-0027-05
中图分类号：TN915.5
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
In the context of digital transformation，the security risks and threats faced by information networks are becoming more and more serious. The traditional security protection，monitoring and early warning technology can no longer cope with the challenges brought by Advanced Persistent Threat （APT） attack，and network security begins to develop towards intelligence. By analyzing the technical architecture of intelligent monitoring and early warning platform，it puts forward the construction idea of monitoring and early warning platform based on massive multi-source data acquisition and intelligent analysis engine. Combined with the whole process of safe operation service support，the passive defense is changed to active，and the safety closed-loop management is realized.

Keywords：
Big data；Intelligent analysis engine；Monitoring and early warning；Safe operation

引用格式：黄昌熙，朱磊，余润泽，等. 智能化网络安全监测预警平台建设和运营思路探讨[J]. 邮电设计技术，2023（1）：27-31.

1 概述

随着数字改革不断深入，行业发展面临巨大机遇，“新基建”打破了传统的产业边界，加速了产业间的融合创新，网络信息量正呈现爆发性增长，新型的网络攻击威胁层出不穷，勒索病毒、APT攻击、数据泄露等安全事件频发，政府和企业网络的核心业务系统面临严重的安全隐患。根据国家互联网应急中心（CNCERT）数据统计，境外APT攻击组织以“新冠肺炎疫情”“基金项目申请”等相关社会热点投递钓鱼邮件，冒充我国卫生机构发起定向攻击，造成了较为严重的网络安全风险。

面对严峻的网络安全威胁，多国启动了应对措施。美国顺应网络威胁与技术的发展演变，多举措提升攻防能力；俄罗斯积极构建网络空间安全屏障，在加密货币、人工智能等领域加大投入；日本采取开发基于人工智能的系统抵御网络攻击；我国在“国民经济和社会发展第十四个五年规划”中明确提出提升网络安全威胁发现、监测预警、应急指挥、攻击溯源能力，加强网络安全关键技术研发，加快人工智能安全技术创新，提升网络安全产业综合竞争力。可以预见，智能化网络安全监测预警技术适应未来发展趋

收稿日期：2022-12-09

势。

2 网络安全监测预警技术分析

网络安全监测预警是通过对网络和安全设备日志，系统运行数据等信息进行实时采集，以关联分析等方式对监测对象进行风险识别、威胁发现、安全事件实时告警及可视化展示，对安全风险和威胁快速定位、预警和响应处置。

a）传统技术。传统网络安全监测预警是将各类安全设备日志、主机日志、网络日志、Web 日志等采集到统一的日志存储平台，实现日志集中存储分析，通过获取互联网已公开漏洞信息、恶意域名、代理攻击 IP 地址等信息与资产匹配，呈现网络安全风险状况。传统技术手段主要实现数据汇总和静态呈现，统计图形较为简单，输出的专业报表晦涩难懂，采用统计型、规则型和特征匹配型算法为主，关联分析和智能分析技术应用较少。

b）智能化技术。智能化网络安全监测预警是采用人工智能技术、大数据技术，加入协同联动接口，基于多源数据采集，结合流量分析、日志分析、用户和实体行为分析（UEBA）、大数据关联分析、机器学习等技术，在监测预警、响应处置、溯源取证和可视化展示等方面更加高效智能，可以应对复杂环境的网络攻击。网络安全监测预警技术对比如表 1 所示。

表 1　网络安全监测预警技术对比

技术类型	主要技术	达到效果
传统技术	日志采集存储分析，使用统计型、规则型和特征匹配型算法	汇总数据，静态呈现
智能化技术	多源数据采集，结合流量、日志、资产和脆弱性、威胁情报数据采集，使用机器学习、大数据关联分析、UEBA 等技术	智能监测预警和可视化展示，攻击溯源取证

3 网络安全监测预警平台建设思路

3.1 平台架构设计

传统的网络安全架构和安全模型不能满足新形势的网络安全需求，网络安全监测预警平台在架构上需要进行融合设计，通过采集网络流量、设备日志、资产和脆弱性数据、威胁情报等多源海量数据，运用机器学习、数据关联分析等智能分析引擎，将人工智能技术应用于网络安全领域，高效识别和预警安全威胁风险，实时精准可视化展示。智能化网络安全监测预警平台总体上分为数据采集层、安全大数据中台、安全服务层和展示层，具有第三方安全平台对接接口，实现更大范围网络监测预警、共享和协同处置。智能化网络安全监测预警平台架构如图 1 所示。

3.2 多源数据采集方案

3.2.1 网络流量采集

网络流量采集是在互联网出入口、云边界等重要

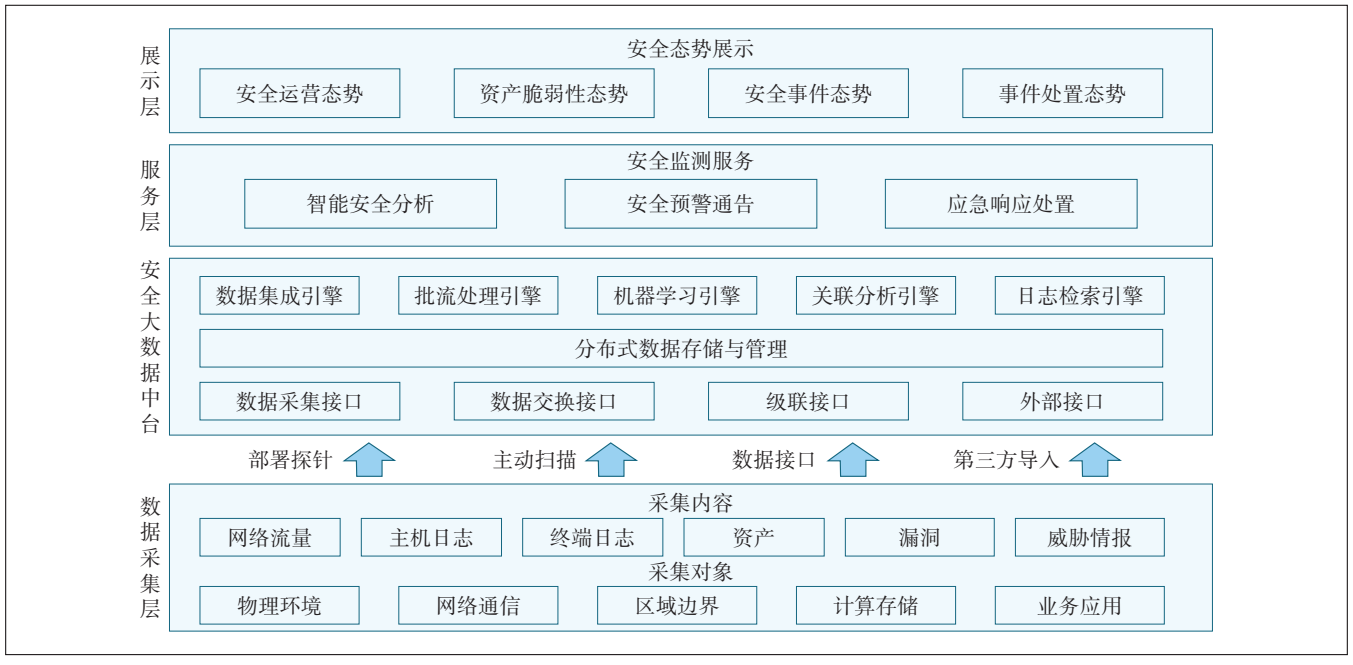

图 1　智能化网络安全监测预警平台架构

网络出入口采集原始流量数据，为智能化安全分析提供基础数据来源。网络流量采集使用探针旁路部署模式，与路由器、交换机或防火墙等网络安全设备镜像端口相连，不改变原有的网络结构，数据采集获得的是链路中流量数据的拷贝，主要用于监听和检测网络中的数据流及各类异常行为。

网络镜像流量首先需要进行数据预处理，检测识别所有接收到的流量，然后抓包把需要处理的应用数据报文抓取到应用层，经探针处理后形成流量元数据，包括由TCP、UDP等组成NetFlow以及由四层以上的重要的协议如HTTP、DNS组成的HTTPFlow、DNS-Flow等xFlow形式元数据，并检测输出异常行为数据、文件样本和检测日志，为智能分析提供数据来源。网络流量采集基本过程如图2所示。

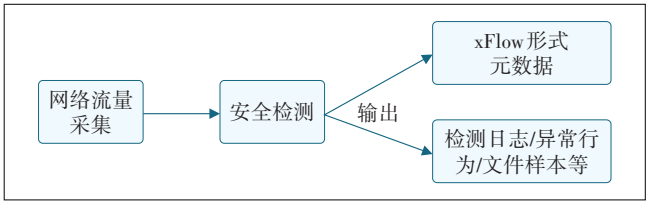

图2　网络流量采集基本过程

3.2.2 日志采集

系统日志是监测预警平台对接采集的各类安全设备、网络设备、主机的告警、操作等日志信息。Flume组件是一个高可靠和分布式的海量日志采集、聚合和传输组件，Flume组件采集网络中的文件、文件夹、syslog、socket数据包等各类型数据，通过定制各类数据发送方，将数据格式化封装到事件里，写入数据传输通道，实现日志采集、过滤、缓存、中转分发和调度。

3.2.3 资产和漏洞数据采集

网络资产包括终端、服务器、网络安全设备、物联网设备等，资产识别需要建立指纹特征库，指纹特征库包含设备基本信息、操作系统信息以及应用程序详情。完成建立相应指纹特征库后，使用正则表达式特征匹配识别出相应的网络资产情况。使用主动扫描、被动流量检测发现存活的IP/URL信息，识别内容关联、合并、去重和除错处理，形成网络的资产列表。

资产的漏洞识别分为主动扫描和被动扫描，主动扫描识别资产中的漏洞、配置、弱密码、Web明文传输等风险，被动扫描是在分析用户主机遭受攻击后，识别出用户主机的安全漏洞风险。按照漏洞扫描结果、资产重要性及漏洞的威胁情报，排序漏洞重要性，以确定修复的优先级。

3.2.4 威胁情报采集

威胁情报包括域名类、IP类、文件类等，利用大数据技术收集获取，平台接入第三方专业的威胁情报数据，利用外源威胁情报指导内源威胁信息，不断积累形成新的威胁情报。威胁情报关联网络中的安全日志、流量，精准检测网络和主机的威胁状况，及时感知新型威胁。

3.3 智能安全大数据中台构建

数据融合处理是智能化网络安全威胁感知的重点，具有支撑持续监控、威胁预警、多角度可视化数据呈现的能力。安全大数据中台包含数据集成、批流处理、机器学习、关联分析等智能分析引擎。

3.3.1 数据集成引擎

按照数据标准化治理过程，完成数据格式转换、数据解析、数据清洗、数据增强等数据泛化能力，可以对JSON、CSV、KV和正则等数据格式进行处理，涵盖各类数据分析场景，能够结合地理位置、资产信息、黑白名单和威胁情报信息添加标签。

3.3.2 批流处理引擎

批流处理引擎包括可视化建模和安全编排与自动化响应(SOAR)。可视化建模技术以拖拽控件的方式设计关联规则分析流程，将安全算法灵活编排组合，实现针对特定安全场景完成关联分析建模。SOAR具有自动编排执行能力，依据场景编排安全动作脚本，匹配不同安全需求，建立自动化风险处置流程。SOAR基本流程如图3所示。

3.3.3 机器学习引擎

基于机器学习框架的分类、聚类等算法，选择合适的算法进行模型训练，训练好的模型在真实环境探测网络异常行为，按照配置的规则生成安全事件或者威胁告警。根据流的统计特征分类，避免了流量加密

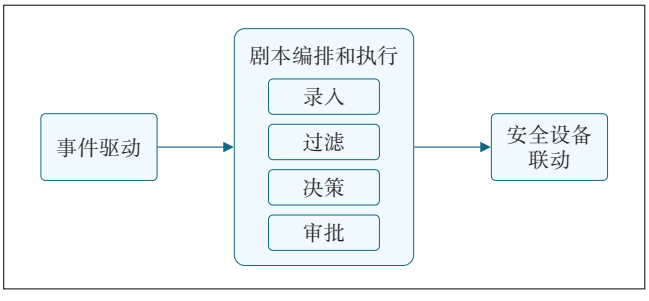

图3　SOAR基本流程

带来的影响。可以直接使用已经封装好的安全威胁检测算法或模型而不需要关心其内部逻辑实现。模型训练基本流程如图4所示。

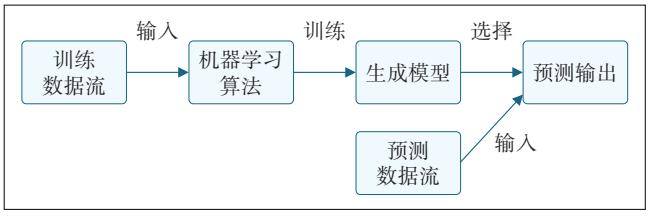

图4　模型训练基本流程

3.3.4 关联分析引擎

关联分析引擎具有违规行为、数据泄露、漏洞利用、关联告警等常用的关联分析规则，关联分析引擎使用多种模式的关联分析模板，如过滤分析模板、计数模板、求和模板和Follow by时序模板等，利用关联分析规则模板配置各类关联分析模型。

3.3.5 日志检索引擎

从结构化信息中定位出原始流量包数据，存储经过流计算关联规则之后的安全事件信息，供上层安全态势展示使用。日志检索引擎以SPL语句为查询语言，SPL是对全文检索引擎查询语句的封装，通过关键字完成过滤、聚合、排序和数据量裁剪，提交搜索引擎进行查询和统计分析。

3.4 综合安全分析和预警响应

利用智能分析引擎综合分析发现潜在的攻击威胁，按照预先设定的规则和流程发布预警和应急响应。

3.4.1 综合安全分析

a）异常流量分析。提取原始流量日志，基于机器学习、关联分析引擎对未知异常流量检测和未知攻击事件的分析发现。

b）异常行为分析。利用UEBA分析技术，结合威胁情报库和主机访问异常等各种异常行为事件，以聚类方式识别和划分具有相似行为、属性的群体，通过群体分析发现异常行为，预测未知风险。

c）恶意代码分析。监测捕获多种来源恶意代码，分析样本行为和同源性，获得恶意代码的演进过程、行为特征、事件关联等主要数据，建立入库恶意代码样本和数据的索引查询。

d）攻击威胁溯源。从网络流量、日志数据、威胁情报、恶意样本等多维度，关联分析攻击者的入侵方式，还原攻击事件的整个过程，实现安全溯源分析甚至是攻击者画像。

3.4.2 预警通告

通报预警消息输入来源于自动分析产生或手工输入的安全事件告警消息，在格式化安全事件告警消息后，评估关联需要发送的对象，通过短信、邮件等方式发送预警通告，持续提醒安全管理人员快速跟踪处置。

3.4.3 响应处置

响应处置模块下达网络安全事件处置指令，指令接收人员按照标准操作流程开展事件处置，进行现场勘察，固定证据，快速恢复，消除危害和影响。对事件处置情况、现场勘察情况以及证据建档、归档和入库。

3.5 多维度安全态势展示

提取系统安全特征和指标，发现网络安全风险，汇总成有价值的情报，将网络安全风险通过可视化技术直观地展示出来，综合呈现网络安全整体态势情况。具备多维度图表展示，如总体态势展示，资产概况展示、预警信息展示、安全事件展示等，可以获取详细信息轨迹，高效支撑决策指挥。

4 安全运营服务方案设计

信息保障技术框架（IATF）提出了安全保障依赖于人、技术和操作等3个要素，人是信息保障体系的核心。要以驻场安全人员和远程专家协同运营服务为基础，借助智能化监测预警平台，从安全风险资产、威胁和脆弱性出发，覆盖云、网、应用、数据和终端的安全，掌握网络空间安全防御技术，了解网络安全实战技能，周期性开展安全风险评估、渗透测试和应急演练，加强组织与能力保障，实现事前、事中、事后全生命周期安全运营。网络安全运营架构如图5所示。

安全运营可以分为3个阶段，第1阶段为初期运营，完成网络中各类融合数据的统一接入与管理，具备基础威胁检测、分析和响应能力；第2阶段为优化阶段，根据业务场景，建立安全分析模型，实现智能融合检测和关联分析，建立标准化安全运营体系；第3阶段为持续安全运营阶段，不断优化模型检测规则，优化运营流程，评估安全风险并持续改进。全流程的安全运营服务项目和内容如表2所示。

安全运营是不断优化检测规则和运营流程、评估安全风险并持续改进的过程。安全运营服务应当具备全过程安全保障、事件闭环处置能力，随着安全运营的深入和效能的提升，安全事件的数量将越来越

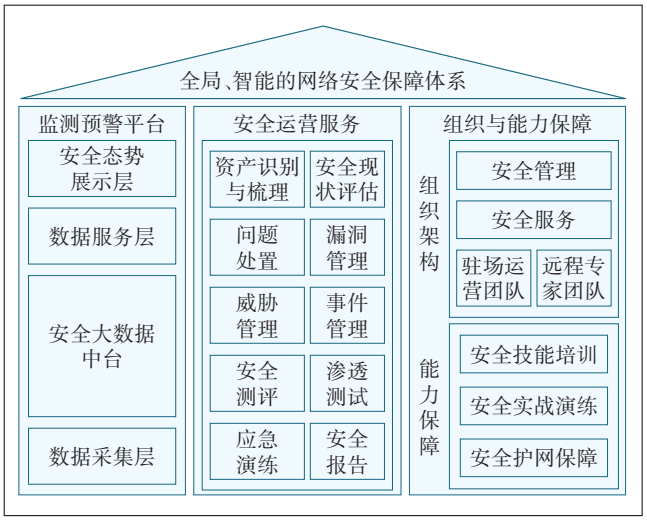

图5　网络安全运营架构

表2　安全运营服务项目和内容

序号	服务项目	内容
1	资产识别与梳理	资产发现与识别、资产信息梳理与管理
2	安全现状评估	脆弱性评估、病毒类事件评估、攻击行为评估、失陷类事件评估
3	问题处置	脆弱性问题处置、病毒类事件处置、入侵攻击行为处置、失陷类事件处置
4	漏洞管理	漏洞分析与管理、弱口令分析与管理、最新漏洞预警与响应、漏洞协助处置
5	威胁管理	威胁分析与通告、流行威胁通告与排查、主动分析与响应、策略管理、持续攻击对抗
6	事件管理	事件分析与处置、应急响应
7	安全测评	定期安全风险评估
8	渗透测试	Web应用系统渗透、主机操作系统渗透、数据库渗透
9	应急演练	定期应急演练
10	安全报告	资产清单、安全通告、安全监测运营分析报告、事件分析与处置报告、漏洞扫描报告、基线评估报告、渗透测试报告、应急演练报告

少，最后在可接受的范围内波动，安全运营成熟度不断提高。

5 结束语

信息爆炸时代对网络安全提出了新的要求，传统网络安全防护手段无法应对新型网络攻击威胁，智能化安全技术是当前安全研究的重点，以大数据和人工智能为代表的智能化网络安全监测预警技术在应对复杂的网络环境时安全防护效果显著。安全攻击威胁的技术在不断演变，智能安全算法和安全检测模型也需要持续优化，提升攻击检测效率和准确率。安全离不开人的因素，安全运营服务需要顺应新时期安全形势，加强网络安全风险评估和攻防对战演练是有效的主动防御措施。需要从组织和机制上做好网络安全保障，提升人员安全意识，健全安全管理制度，加强安全领域的合作，更好地支撑数字经济社会发展。

参考文献：

[1] 葛自发，孙立远，胡英．全球网络空间安全战略与政策研究(2020-2021)[M]．北京：人民邮电出版社，2021.
[2] 林宝晶，钱钱，翟少君．网络安全能力成熟度模型：原理与实践[M]．北京：机械工业出版社，2021.
[3] 张胜，赵珏．网络安全监测数据可视化分析关键技术与应用[M]．北京：电子工业出版社，2018.
[4] 陈铁明．网络空间安全实战基础[M]．北京：人民邮电出版社，2018.
[5] 国家互联网应急中心CNCERT. 国家互联网应急中心(CNCERT)发布《2020年中国互联网网络安全报告》[EB/OL]．[2022-09-25]. http://www.cac.gov.cn/2021-07/21/c_1628454189500041.htm.
[6] 全国信息安全标准化技术委员会．《网络安全态势感知技术标准化白皮书(2020版)》发布[EB/OL]．[2022-09-25]. https://www.tc260.org.cn/front/postDetail.html?id=20201109171657.
[7] 中国信息通信研究院安全研究所，腾讯安全．数字产业：2019年度网络安全威胁情报分析[EB/OL]．[2022-09-25]. http://www.caict.ac.cn/kxyj/qwfb/ztbg/202004/t20200430_280571.htm.
[8] 朱常波．中国联通网络安全战略的思考与实践[J]．邮电设计技术，2019(4)：1-5.
[9] 黎宇，杨世标．互联网业务端到端感知监测分析系统[J]．邮电设计技术，2021(8)：84-87.
[10] 黄韬，刘江，汪硕，等．未来网络技术与发展趋势综述[J]．通信学报，2021，42(1)：130-150.
[11] 张红斌，尹彦，赵冬梅，等．基于威胁情报的网络安全态势感知模型[J]．通信学报，2021，42(6)：182-194.
[12] 顾玥，李丹，高凯辉．基于机器学习和深度学习的网络流量分类研究[J]．电信科学，2021，37(3)：105-113.
[13] 张颖君，刘尚奇，杨牧，等．基于日志的异常检测技术综述[J]．网络与信息安全学报，2020，6(6)：1-12.
[14] 刘小虎，张恒巍，马军强，等．基于攻防博弈的网络防御决策方法研究综述[J]．网络与信息安全学报，2022，8(1)：1-14.
[15] 郑禄鑫，张健．云安全面临的威胁和未来发展趋势[J]．信息网络安全，2021，21(10)：17-24.
[16] 赵志岩，纪小默．智能化网络安全威胁感知融合模型研究[J]．信息网络安全，2020，20(4)：87-93.

作者简介：
黄昌熙，工程师，学士，主要从事网络安全和信息系统的咨询设计工作；朱磊，工程师，学士，主要从事网络安全和信息系统的咨询设计工作；余润泽，工程师，硕士，主要从事网络安全和信息系统的咨询设计工作；滕泽滨，工程师，硕士，主要从事网络安全和信息系统的咨询设计工作。