粟毅，安小伟，李振，等 . 安全态势感知联动防护在地震网络安全保障的应用 [J]. 华南地震 , 2020, 40（4）：63-70. [SU Yi, AN Xiaowei, LI Zhen, et al. Application of Security Situation Awareness Linkage Protection in Seismic Network Security Assurance [J]. South China journal of seismology, 2020, 40（4）：63-70]

安全态势感知联动防护在地震网络安全保障的应用

粟 毅，安小伟，李 振，吕 帅，刘鹏飞
（云南省地震局，昆明 650224）

摘要：近年来，云南省地震局地震信息系统经过多次的攻防演练和信息安全监测，结果表明云南省地震系统正面临严峻的网络安全挑战。在传统的网络安全管理模式下虽投入大量人力和物力，但效果并不理想，很难满足当前的网络安全形式需求。因此，对全网网络安全的动态监测、联动防护、追踪溯源、分析取证是未来网络安全建设思路。通过对安全态势感知和联动防护在云南省地震系统中的应用进行探索和分析，并在实践中进行了验证，最后总结了网络安全防护体系建设经验。

关键词：信息安全；安全态势感知
中图分类号：P631.4 **文献标志码**：A **文章编号**：1001-8662（2020）04-0063-08
DOI：10.13512/j.hndz.2020.04.09

Application of Security Situation Awareness Linkage Protection in Seismic Network Security Assurance

SU Yi, AN Xiaowei, LI Zhen, LV Shuai, LIU Pengfei
(*Yunnan Earthquake Agency*, *Kunming* 650224, *China*)

Abstract： In recent years, the seismic information system of the Yunnan Earthquake Agency has undergone many offensive and defensive drills and information security monitoring, and the results show that the seismic system of Yunnan Earthquake Agency is facing severe network security challenges. Although a lot of manpower and material resources have been invested in the traditional network security management mode, the effect is not satisfactory, and it is difficult to meet the demand of the current network security requirements. Therefore, dynamic monitoring, linkage protection, traceability, analysis and evidence collection of the entire network security are the ideas for future network security construction. This paper explores and analyzes the application of security situation awareness and linkage protection in the earthquake system of Yunnan Province, verifies it in practice, and finally summarizes the experience in building network security protection system.

Keywords： Information security; Security situational awareness

0 引言

随着网络内部结构的不断复杂化，网络病毒对于互联网的威胁也越来越大，传统的网络安全维护技术的适应性进一步下降，进行全新技术的研究和推广显得很有必要，安全态势感

收稿日期： 2020-02-10
作者简介：粟毅（1981-），工程师，主要从事信息服务、网络安全建设等相关工作。
E-mail: suyiwy@163.com

知技术在这时应运而生。安全态势感知就是利用数据获取采集、数据挖掘、数据融合、智能分析、面向多类型的网络安全性相关的技术，能够主动并及时的进行网络状态的监控，对当前和未来一段时间内网络的安全状况进行全面分析评估，从而预测网络安全风险，实现动静相结合的安全防御方式。企业主要面临三类安全风险：一是企业存在风险对象公网违规暴露。二是内外网系统存在软硬件安全漏洞、弱口令等安全隐患。三是企业对安全事件监测防范能力较弱，后门、蠕虫等影响企业网络安全事件长期潜伏。行业整体安全形势严峻，安全监管需求日益迫切[1−3]。

1 云南省地震系统近年主要网络安全事件

2014 年 1 月云南省地震局门户网站出现访问异常，检查发现网站服务器受到攻击，经过数据分析，服务器被植入僵尸木马并对外部发起攻击。服务器以每 0.1 s 对外发送上万次频率的请求，导致服务器资源被大量占用以至网站瘫痪。

2018 年 4 月云南省地震局门户网站无法打开，网站服务器内存耗尽，查看安全日志显示某 IP 正在攻击网站服务器，持续约 1 h，经安全设备阻断后恢复正常。

2 网络安全现状及拓扑

2017 年 6 月 1 日《中华人民共和国网络安全法》正式实施，信息安全重要性进一步凸显，云南省地震局加强了网络安全能力建设，先后部署了防火墙、防病毒系统、全流量分析系统、行为管理系统以及安全网闸等设备（图 1）。由于安全设备种类较多，安全技术能力薄弱，无法准确、及时的发现网络安全威胁，为进一步提升网络安全防护能力、整合现有安全设备，达到统一管理、统一发现、统一处理的目的，2019 年云南省地震局新部署了一套态势感知系统，逐步实现云南省地震局网络安全体系建设。

3 网络安全感知建设方案

以全流量分析为基础，结合威胁情报、行为分析、UEBA、机器学习、大数据关联分析、可视化等技术对全网流量实现业务可视化、威胁可视化、攻击与异常流量可视化，从而全面发现各种安全威胁。

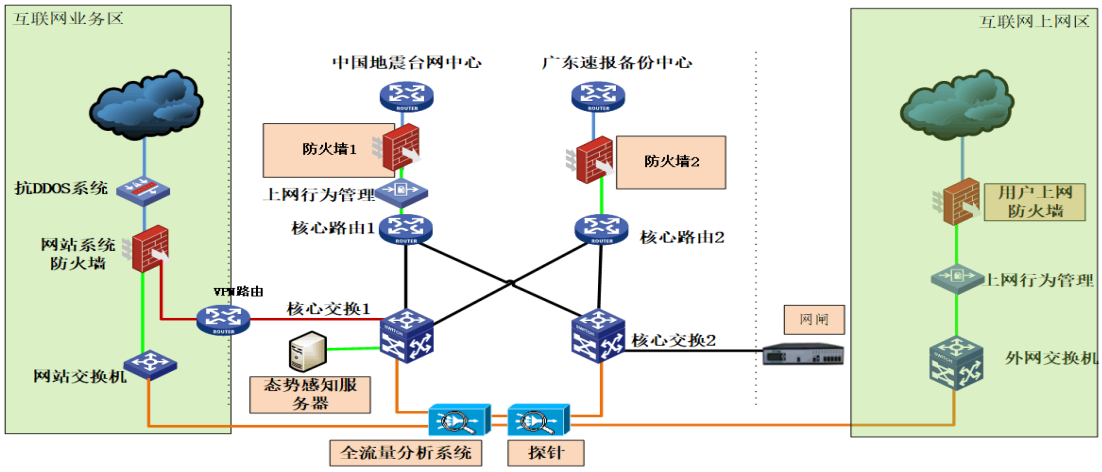

图 1 网络安全拓扑图

Fig.1 The topology diagram of network security

3.1 安全感知架构

通过流量镜像的方式采集终端数据、流量数据、第三方设备日志、中间件数据、威胁情报数据等，经过数据预处理后上传至安全感知平台进行 MapReduce 并行处理，最终实现安全日志可视、潜伏威胁可视、脆弱性可视、朔源分析等功能（图 2）。

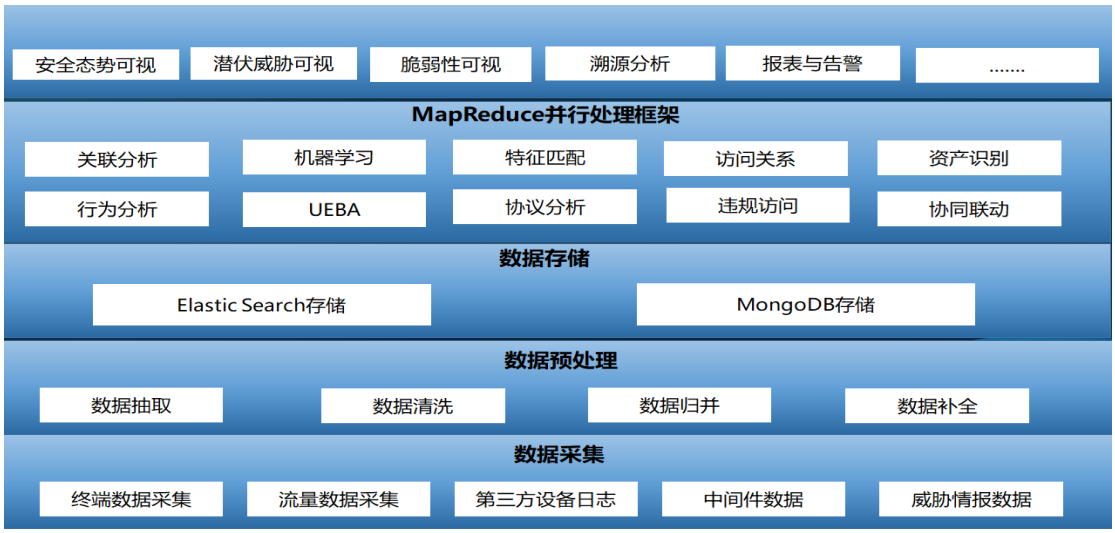

图 2　安全感知平台架构图

Fig.2　The architecture diagram of safety awareness platform

3.2　安全感知检测原理

将人工智能 SAVE 检测引擎与多种机器学习算法有机结合：LSA, AutoEncoder, LogicRegression, SVM, 随机森林, XGBoost 等。采用随机森林分类模型检测威胁，该模型充分考虑了 webShell 样本与正常的样本的特征差异性，例如网页的孤立性、被访问的时间和次数、被访问的参数特点、网页内容特点等等。针对标记的样本，进行词法 / 语法分析提取统计之后，利用特征随机化组合增强特征表达力，训练出随机森林分类模型（图 3）。

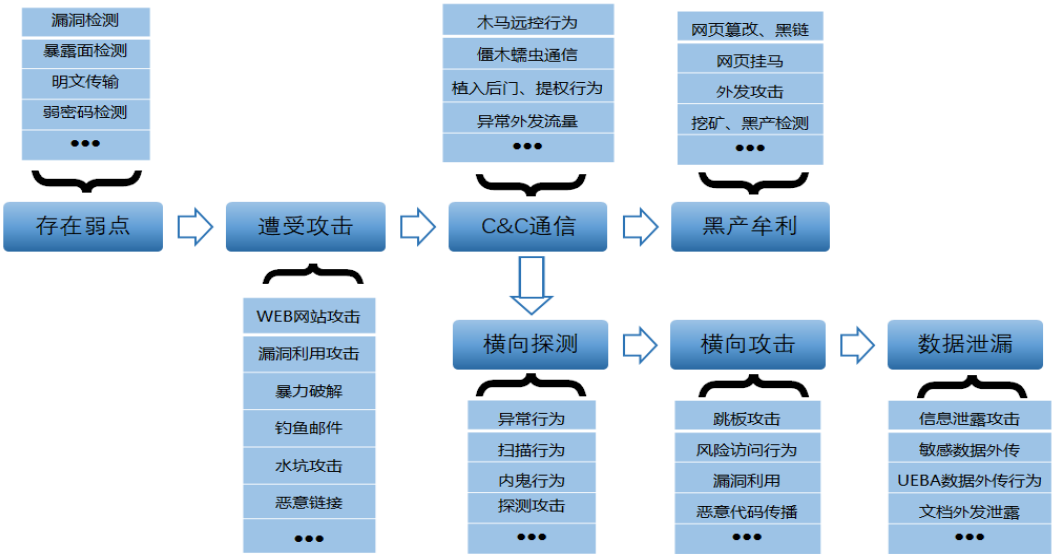

图 3　安全感知检测流程图

Fig.3　Safety perception test flow chart

3.3　恶意软件流量模型自动化生成与检测

恶意软件流量模型通过两个阶段进行检测（图 4），训练阶段：对大量的恶意软件流量样本进行建模，通过聚类分析发现恶意软件家族的共性和特性。对未知样本进行特征化，利用训练好的分类模型对样本进行检测；检测阶段：利用训练得到的模型，对实时网络流量进行智能分析，发现未知的恶意软件变种精确率和检出率都非常的高。

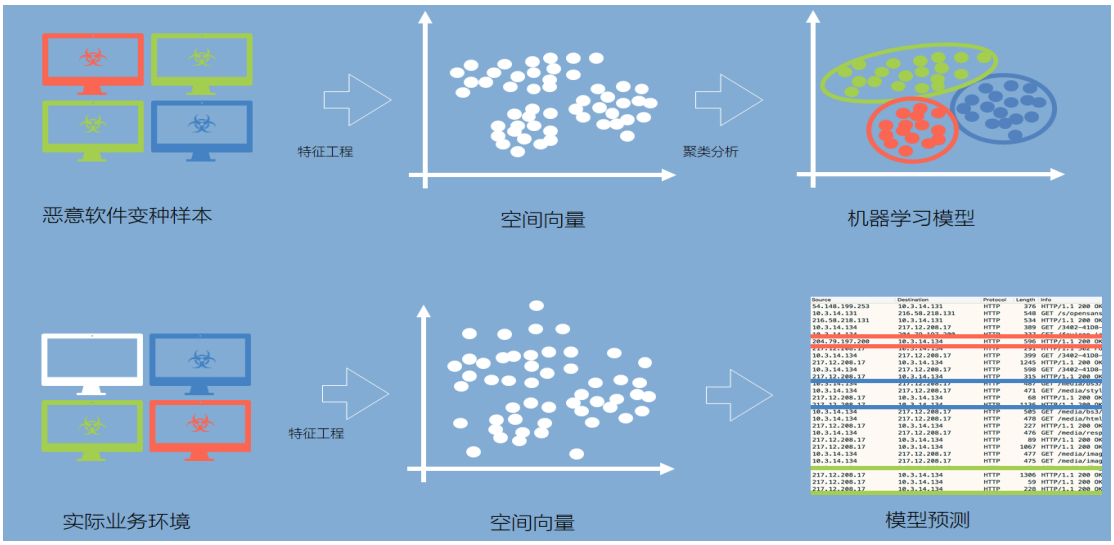

图 4 恶意软件流量检测模型

Fig.4 Malicious software flow detection model

3.4 LSTM 算法检测 DGA

LSTM（Long Short Term Memory Network）长短期记忆神经网络，通过对字符串提取特征，训练分类器分类域名，实现威胁检测。LSTM 较 N-gram 有显著提升，在“能否检测出僵尸网络”问题上达到 99.7% 的 F 值，在“检测出具体是哪一种僵尸网络”问题上达到了平均 90.3% 的 F 值。DGA（域名生成算法）是一种利用随机字符来生成 C&C 域名，经常被勒索病毒、蠕虫、僵尸网络用于逃避威胁情报、域名黑名单检测的技术手段 [4-5]。

安全感知采用 LSTM 在云端大数据中心训练恶意软件家族随机生成的域名（DGA）和白域名，并将训练结果下发到安全感知平台，结合 DNSFLOW 引擎实现 DGA 检测，从而有效追溯勒索病毒、蠕虫、僵尸网络的控制信息等。

3.5 DNS 隐蔽信道检测

正常域名是有含义的，例如，ww.baidu.com、facebook.com、bookstore.com，而编码后的 URL 多是随机生成的。信息熵匹配，载荷的信息量、离散程度不同，有含义的 URL 信息熵是低的（即数据是规律的）；而隐蔽信道传输的信息基本上是加密的，其 0、1 字符串规律性弱，信息熵较高。安全感知通过 iForest（孤立森林）算法对正常页面与异常页面在关键词、网页路径结构层次数、cookie 键值对数、返回网页结构相似度、访问行为、POST/GET 熵值、cookie 键值对熵值、跳转关系、访问频率等多个特征上的差异，生成机器学习模型，从而有效检测 0-day webshell、web 隐蔽通道外传，根据 DNS 隐蔽信道检测原理能成功区分出异常信息。

3.6 机器学习算法检测 webshell

webshell 可以在 web 服务器上执行的后台脚本或者命令执行环境，黑客通过入侵网站上传 webshell 后获得服务器的执行操作权限，比如执行系统命令、窃取用户数据、删除 web 页面、修改主页等。

3.7 用户与实体行为分析 UEBA

发现一些显著的小概率异常事件，这些事件可能是病毒攻击、黑客攻击，也可能是违规访问、内鬼作祟、数据泄露。通过结合访问对象 + 访问行为两层逻辑，根据服务器的历史“访客”首先发现可疑的访问对象，然后基于该“访客”的访问行为是否可疑来识别异常。这里的异常指的是有重要变化的小概率事件。

4 网络安全感知联动应急处置

4.1 高效协同响应

在全局性的分析发现威胁之后，通过安全感知平台与下一代防火墙或上网行为管理联动，一键阻断僵木蠕与外部的通信。如果是阻断的用户 PC，还需要进行阻断提醒。在终端服务器上，平台与 EDR 联动，对服务器进行僵木蠕查杀和隔离。

4.2 自动化联动机制

联动下一代防火墙（AF），当 AF 同步信息到安全感知平台后创建联动应用策略，用于主机发生严重风险（如中勒索、感染病毒等），发现主机有 C&C 通信行为时进行主机封锁，保障网络边界安全。

联动终端检测和响应（EDR），在安全感知平台接入 EDR 设备进行信息同步，读取 EDR 日志包括暴力破解、僵尸网络、杀毒、webshell 等，将日志归类到安全感知平台的检测日志中分析安全事件进行联动处置，联动 EDR 实现基于僵尸网络 C&C 域名的进程 / 文件调查取证，辅助威胁定位。作为终端检测端用户可实现防病毒、入侵防御、防火墙隔离、数据信息采集上报、安全事件的一键处置等功能。

联动上网行为管理（AC），在 AC 平台配置接入安全感知平台，将用户信息同步至安全感知平台获取到用户上网信息，在进行联动时可实现用户上网提醒，发现风险用户访问时冻结用户上网行为并发送风险处置意见。

联动 SSLVPN，将 SSLVPN 接入到安全感知平台，同步用户信息、管理员操作日志、系统日志，用户信息包括登入、登出、访问资源等，接入后在安全感知平台显示用户操作信息。

自动化联动机制用于自动联动接入到安全感知平台上的各种设备，实现自动化响应闭环。配置“安全事件智能联动”策略后开始监听全平台安全事件，在产生具体安全事件时检测引擎智能匹配相关策略自动进行处置，同时可接入第三方品牌安全设备读取日志进行辅助分析。如中了勒索，可自动获取处置手段为：禁止主机的方向为出站、端口为 445 的流量，确认后即可实现直接限制对应端口的访问。自动化联动机制解决了安全产品繁多无专业人员逐一进行维护，发现了问题不知道怎么处置，无法闭环，对安全事件的发生、中病毒或受到木马攻击时处理不及时等问题，解放了安全维护人员压力，提升了安全防护能力。

5　安全态势感知系统在云南省地震局测试效果

云南省地震局网络结构复杂，现存四张独立网络，区域中心服务器、终端、业务系统、办公电脑等种类繁多，信息安全监测和防范一直是个较为棘手的问题，在经过多方调研后上线了安全态势感知平台进行测试（图 5），测试内容主要为全网资产识别和管理，全流量监控和分析，安全事件检测和响应，安全设备联动和处置，全网业务可视化、安全风险可视化、安全事件可视化、网络攻击可视化等功能，测试时长约三个月，总体来看安全处置和防护效果较原来有较大的提升。

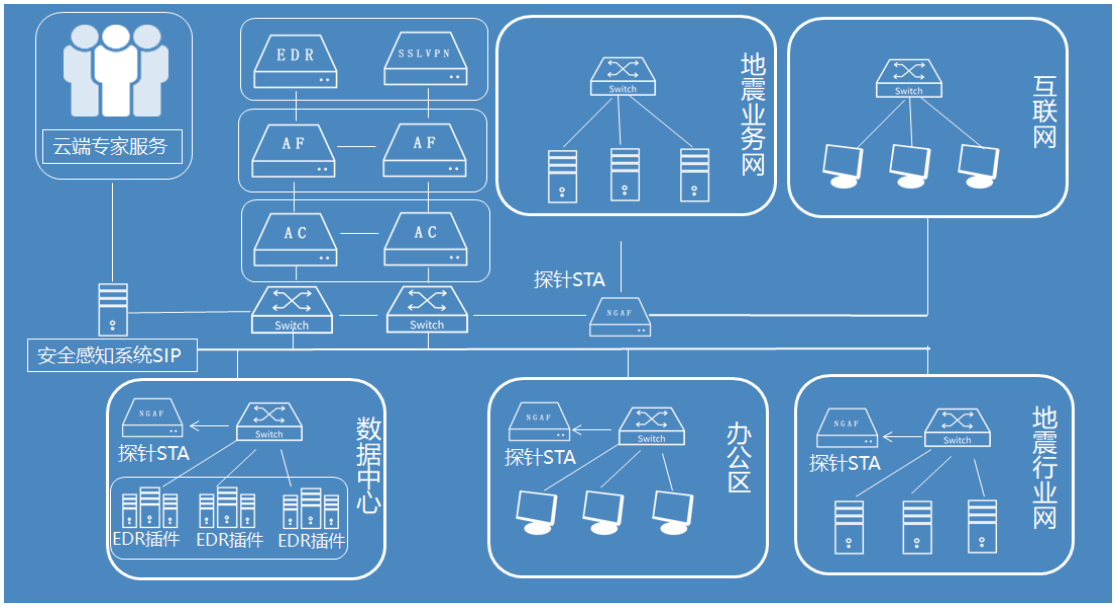

图 5　安全感知平台连接图

Fig.5　Connection diagram of safety awareness platform

5.1 风险安全检测

共检测出 139 台风险主机，其中已失陷主机 28 台，高危主机 6 台，主要安全风险发生在互联网区和州市地震行业网区，发生风险事件以病毒、木马、僵尸网络为主（图 6、7）。

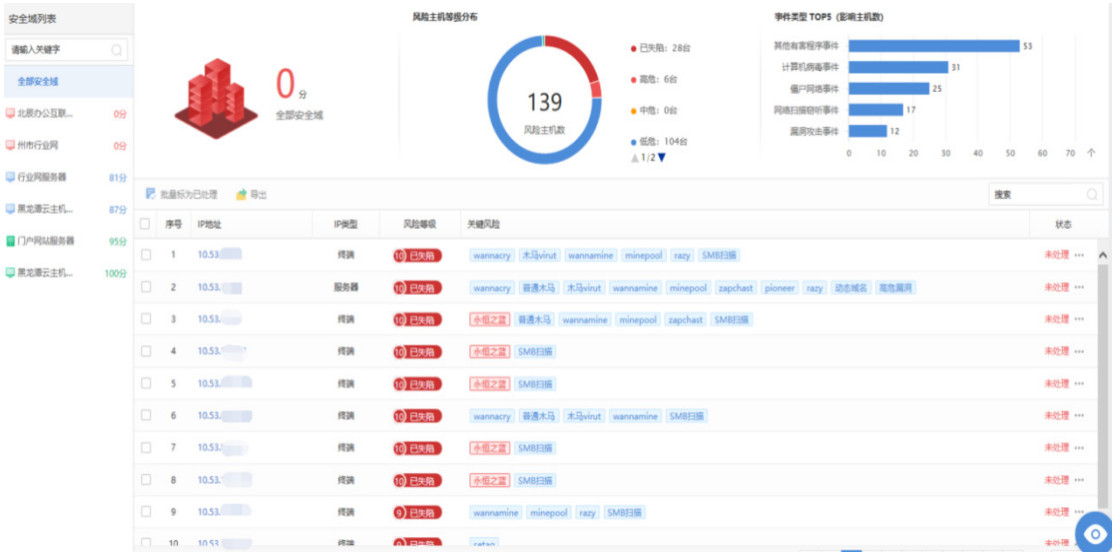

图 6 风险安全可视化

Fig.6 Risk security visualization

图 7 安全事件可视化

Fig.7 Security incident visualization

5.2 网络攻击检测

一周内共有 140 余次攻击行为，主要攻击目标为云南省地震局门户网站系统，主要攻击手段有系统漏洞攻击、信息泄露攻击、WEB 漏洞攻击等（图 8）。

序号	攻击者IP	攻击者所属地	受害者	受害者所属分支	受害者所属业务	攻击类型
1	39.130.152.40	云南	192.168.1.111	门户网站	-	system漏洞攻击(141), 信息泄漏攻击(55), 目录遍历攻击(13), web漏洞攻击(11), 系统命令注入(7), WEBSHELL上传(4), SQL 注入(1), 文件包含攻击(1)
2	39.130.152.40	云南	192.168.1.125	门户网站	-	system漏洞攻击(141), 信息泄漏攻击(54), web漏洞攻击(13), 目录遍历攻击(10), 系统命令注入(6), WEBSHELL上传(4), SQL 注入(1), 文件包含攻击(1)
3	49.79.193.54	江苏	192.168.1.111	门户网站	-	WEBSHELL上传(81), web漏洞攻击(27), WEB整站系统漏洞(9), 系统命令注入(9)
4	103.212.32.192	香港	192.168.1.111	门户网站	-	WEB整站系统漏洞(57), 系统命令注入(27), WEBSHELL上传(24), SQL 注入(12)
5	150.129.80.179	香港	192.168.1.111	门户网站	-	WEB整站系统漏洞(58), WEBSHELL上传(22), 系统命令注入(21), SQL 注入(11)
6	104.192.84.71	美国	192.168.1.111	门户网站	-	WEB整站系统漏洞(52), WEBSHELL上传(30), 系统命令注入(15), SQL 注入(10)
7	211.149.249.229	四川	192.168.1.111	门户网站	-	WEBSHELL上传(65), web漏洞攻击(18), WEB整站系统漏洞(6)
8	203.195.222.240	广东	192.168.1.111	门户网站	-	WEBSHELL上传(40), WEB整站系统漏洞(26), SQL 注入(8), 系统命令注入(8), 信息泄漏攻击(2)
9	222.186.30.21	江苏	192.168.1.111	门户网站	-	WEB整站系统漏洞(36), 系统命令注入(18), WEBSHELL上传(12), SQL 注入(6)
10	222.186.135.29	江苏	192.168.1.111	门户网站	-	WEBSHELL上传(45), web漏洞攻击(15), WEB整站系统漏洞(5), 系统命令注入(5)

图 8　网络攻击可视化

Fig.8　Network attack visualization

5.3　终端安全检测情况

在 EDR 服务端可一键发起终端检测工作，检测内容多达一百余项，主要检测项目为弱口令检测、账户安全检测、访问控制检测、安全审计检测、病毒木马检测、系统漏洞检测等（图 9）。

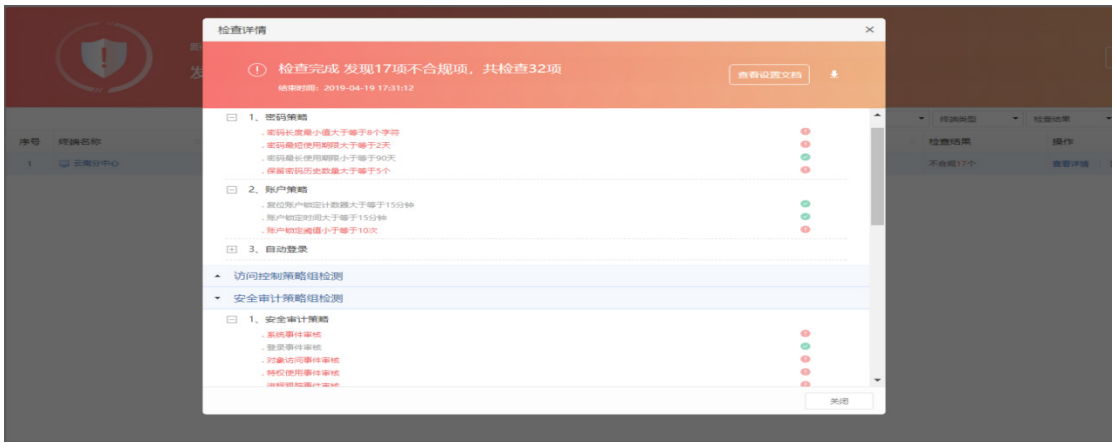

图 9　终端安全可视化

Fig.9　Terminal security visualization

5.4　全局业务系统检测

可实时查看业务系统操作系统、CUP、内存使用等信息，点击查看详情可获取更多业务系统信息（图 10）。

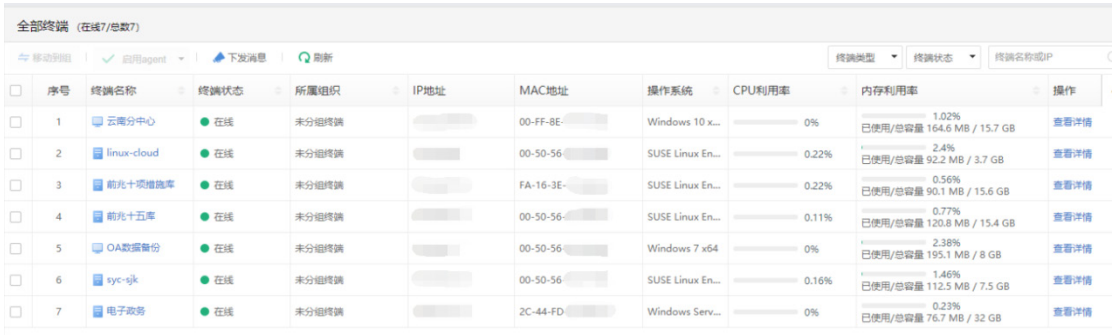

图 10　业务详情可视化

Fig.10　Business information visualization

5.5 安全事件联动处置

制定好联动处置策略后，发现安全威胁立即启动相关策略进行阻断、冻结、查杀等操作（图 11）。

图 11 安全事件联动处置

Fig.11 Security incident linkage disposal

6 结论

本文总结了安全态势感知检测能力、安全事件联动响应处置能力，应用在云南省地震局网络中检测情况，分析了针对云南省地震局信息安全的防护能力，结论如下：

（1）安全态势感知是建设体系化安全防护措施的有力技术支撑，能够实时、准确地掌握网络安全威胁状况，检测恶意攻击行为，让网络安全工作具有主动性和条理性，是监测和预防网络安全事件的有效途径。

（2）根据实际测试安全事件自动化响应处置能力发现，在自动处置时偶尔会发生识别错误和误判、误操作等。所以信息安全防护措施不能完全交由智能化处理，需要安全感知平台提出处置建议配合人工分析进行处理。

（3）安全态势感知系统在云南省地震局的应用总体表现不俗，信息安全防护体系建设需多维度统筹考虑，从网络安全法的解读、制定网络安全发展的规章制度，根据信息管理、用户需求分析、实现方式、平台建设、运维管理、相适应的管理制度等各方面，结合自身的实际情况、管理水平、功能需求分析，进行分阶段建设。

参考文献

[1] 汤永田 . 工业互联网安全态势感知技术及其应用研究 [J]. 自动化博览 , 2019, 36(S2):106-109.

[2] 李敏，郑川，李永强 . 云南省省、市、县级地震应急信息协同技术系统的设计与实现 [J]. 地震研究 , 2018, 41(1):139-147.

[3] 粟毅，安小伟，姚远 . 基于 Hyper-V 虚拟化技术采用 NAS 存储实现 4G 无线测震波形数据的汇集 [J]. 地震研究 , 2018, 41(4):646-649.

[4] 刘磊，许贺，朱宏，等 . 地震数据共享与网络安全机制 [J]. 网络安全技术与应用 , 2018(01):94-95.

[5] 孙路强，刘磊，李刚，等 . 天津数字地震观测网络平台与网络安全建设 [J]. 网络安全技术与应用 , 2017(12):129+131.