工业互联网态势感知系统及应用

闫薛杰
南京宝玮科技有限公司　江苏　南京市　210012

【摘　要】随着当前社会的技术和经济的发展，工业企业正在经历着“信息化”、“数字化”、“智能化”的三化转型。工业企业的网络不再是一个封闭的网络，更多是一个大而互联的网络，这样才能发挥工业互联网产业的调控的效果，在管理和生产模式的变化的同时，也面引入了新的网络安全威胁。通过对工控网络的终端、网络、应用等不同层面装置网络探针，数据采集汇总来全面感知网络的安全状况。工业互联网态势感知系统由数据采集、数据存储、数据分析、数据呈现四大模块组成，其中数据采集是该系统的基础部分，为数据分析和数据呈现提供数据来源。本文根据《工业互联网安全框架》要求，结合当下的工业技术，对安全感知系统系统进行了设计。

【关键词】工业互联网；态势感知；数据采集；数据存储；数据分析；数据呈现

1 前言

1.1 背景

电力、能源、化工、交通、水利、冶金、航空等行业是国有经济命脉行业，这些行业中的工业控制系统更是保障着其行业的正常运转，是工业互联网的重要组成部分。工业中的各类控制设备及系统逐步从企业内网互联到互联网中，网络安全的攻击行为也逐渐威胁到了工业互联中的设备，国内外非法攻击者、黑客通过各种工具扫描系统和应用软件漏洞，并对重要工业设备和系统进行病毒和木马等攻击性工具的植入，来威胁攻击重要工控设备。一旦这类设备被攻击，会造成重大事故，对社会秩序造成严重影响，危及人民的生命安全，甚至给国家利益来重大伤害。

1.2 政策

2016 年 11 月，《网络安全法》已经发布，首次把网络安全提到国家法律层面，使得网络安全事件做到有法可依，有法必依。2019 年 5 月，由国家市场监督管理总局发布的《网络安全等级保护 2.0》标准体系已经发布，首次将云计算安全、移动互联安全、物联网安全、工业控制系统安全等要求列入标准管辖。2020 年 1 月，《密码法》已经正式实施，主要影响商密应用（电子签名等）和提升密码机制在网络安全中的渗透率两方面。2017 年 11 月，国务院印发了《关于深化“互联网 + 先进制造业”发展工业互联网的指导意见》，指导意见中从顶层对我国互联网安全进行规划，并出台相应规范，充分说明了国家对互联网安全的重视程度。工业互联网安全是工业生产正常进行的前提和保障，通过构建完整的工业网络安全态势感知技术体系和服务体系，来满足工业安全要求和安全管理应急机制，从而达到抵御外来攻击风险和消除内部安全隐患，进而确保工业互联网健康有序发展。

2 系统介绍

2.1 系统组成

工控网络安全态势感知能够对工业互联网的物理、传输、应用层面进行全面监控，及时发现网络攻击、系统 / 软件漏洞、木马和恶意代码的攻击等行为，对外来攻击进行防御，对内部隐患进行补漏加固，并通过现有安全事件对未来安全情况进行预警机，有效地帮助安全人员控制安全风险，提升整体工业互联网安全防护水平。本系统主要通过装置网络探针，对工业互联网中安全日事件、告警、日志进行采集，并把相关数据汇聚到感知平台，根据用户使用的业务模型对数据进行业务建模，及时发现网络异常和威胁事件，通过可视化平台将汇聚的威胁和异常展现给安全维护人员，通过对告警和事件响应的探测发现、记录跟踪、处置管理、实现安全风险的闭环管理。

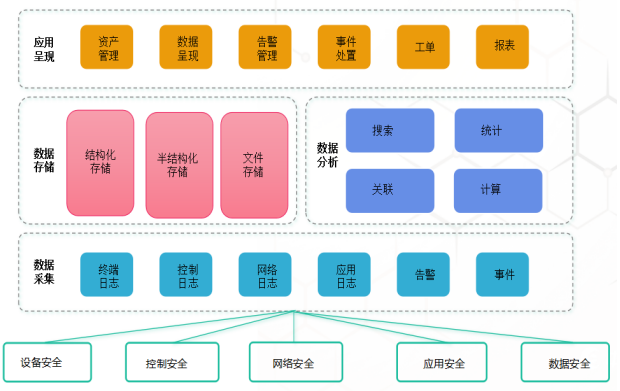

图 1　工业互联网安全态势感知平台

2.2 模块介绍

2.2.1 数据采集

对工业互联网，分别从设备、网络、控制、应用、数据安全等五个方面进行安全信息采集，安全信息包括告警通知、安全事件、系统日志内容。感知平台接收异构系统过来的系统日志，统一规划化处理后，进行存储分析。

2.2.2 数据存储

前端网络探针上传过来的告警通知、安全事件，系统内采用统一格式此类数据，进行结构化存储；对于网络安全中的大量网络审计数据流，进行半个结构化存储；对于涉及数据安全的原始文件系统，采用分布式文件存储系统。

2.2.3 数据分析

通过对存储的海量告警、事件数据，进行分类统计功能，并根据流数据进行实时统计计算，并根据告警和事件的相关性，计算安全危害的特征，并根据历史数据进行相应的安全事件预测。

2.2.4 应用呈现

应用呈现，提供可视化的界面，对网络安全的告警和事件信息提供安全不同维度的数据呈现，并且可以根据用户需求形成各种报表。并对严重告警进行工单流程处理。

3 系统设计

3.1 数据采集

3.1.1 设备安全

设备安全包括设备端点的物理安全和系统安全，对于接入工业互联网中的设备，均需进行安全漏洞扫描和加固，同时形成相应的安全日志，同时，根据设备硬件厂家提供的补丁，及时对设备端点进行系统升级，保证设备不因漏洞而受到安全性攻击。

3.1.2 控制安全

控制安全可以分为：控制协议安全、控制软件安全和控制业务安全三个方面。通过控制软件的接口，获得控制软件系统日志，通过扫描其漏洞，并形安全漏洞告警，并且感知平台提供相应的安全加固软件包。

3.1.3 网络安全

工业互联网是实现工控各个设备端点的互联互通，网络范围的扩大，使得安全范围的扩大，对网络的流程情况进行安全审计和网络设备的安全监视，形成安全告警、事件、日志等信息，为感知平台进行安全展示提供基础。

3.1.4 应用安全

工业互联网应用安全也应当从工业互联网平台安全与工业应用安全两个方面进行防护。对于平台安全，需从漏洞扫描、安全隔离、攻击防护、安全审计等方面进行安全防护，形成安全告警、事件和日志。对于应用安全，需要从应用的开发、测试、部署、运维等环节进行安全监测。

3.1.5 数据安全

对于数据安全，包括数据收集、传输、存储、处理环节，在这些环节中均要进行数据的安全保护，在这些环节中可以采用加密技术对数据进行安全保护。同时在存储和使用环节中，防止数据泄露、损坏、丢失等操作，并对该类事件形成日志或告警，在态势感知平台中进行统一呈现。

3.2 数据存储

对于系统采集层采集到的数据，主要有结构化数据（资产、告警、事件）、半结构化数据（各种流式的安全日志、网络安全审计报文），非结构化数据（网络协议传输文件系统），感知系统分别把三类数据进行统一个数据清洗、数据建模、数据存储。并对数据存储进行安全备份管理，防止被攻击和篡改。

3.3 数据分析

数据分析平台利用大数据技术，对海量告警进行分类统计和建模计算，可以采用分布式计算方式，对分析计算能力进行横向扩充。通过数据建模模型对海量的探针日志进行流式分析处理，同时通过关联模型，对告警进行关联，并进行海量告警的归一，实现告警合并功能，减少人工排查告警的工作量。并对告警信息进行实时统计和特征计算，为上层进行快速业务展示和处置分析提供基础。

3.4 数据呈现

上层业务应用提供应用交互界面，对资产、告警、事件根据不同的维度（业务、区域、责任人 / 单位）进行数据展示，可以在海量数据基础是实现关键字查询的秒级响应，用户可以自定义业务处置流程；根据告警的严重程度，对告警触发不同的派单流程，实现安全故障快速运维消除。并且根据客户的日常使用，可以定制各类的业务报表，减轻安全维护人员的工作量。

4 场景应用

本系统主要面工业互联网领域，对广大工业企业的工控网络安全具有监测、预警作用，利用平的安全监测能力，有效加强企业的现代化管理水平。电力是我国的重要基础行业，关系到国计民生，近些年国家电网向信息化、数字化、智能化的方向快速发展。为保证供电设备和供电系统本地 SCADA 系统的安全运行、预防系统发生重大网络安全事故，并在网络安全事故产生时，能够快速定位事故原因，并快速隔离故障，恢复生产。能够根据大量的安全事件特征预测安全事故，上报预警信号，从网络安全被动防护转变成主动感知防御阶段，极大提高了企业管理水平。

5 结束语

通过对设备、控制、网络、应用、数据等五方面数据采集，并基于大数据的存储技术实现高并发数据的无丢失存储，通过大量的业务模型对数据进行数据分布式计算分析，来满足多种上层应用业务数据展示和业务处置的需求，从宏观层面感知网络安全态势，从而让安全态势“可见、可管、可控、可防”，有效满足政府安全部门和行业管理部门的监管需求，极大地提升企业安全管理水平，同时大量网络安全数据的收集，为将来工业互联网安全大数据应用，人工智能技术（AI）的智能化预判奠定基础，进而为网络安全管理无人化值守打下了良好的数据根基。

【参考文献】

[1] 夏冰 . 网络安全法和网络等保 [M]. 北京：电子工业出版社，2017.
[2] 陆耿虹 , 冯冬芹 . 基于改进 C-SVC 的工控网络安全态势感知 [J]. 控制与决策 , 2017(7).
[3] 杜嘉薇等 . 网络安全态势感知：提取、理解和预测 [M]. 北京：机械工业出版社，2018.
[4] 姚羽等 . 工业控制网络安全技术与实践 [M]. 北京：机械工业出版社，2017.