1.1 案例一：装备制造行业一体化安全运营建设案例——构建 OT、IT 安全能力全面融合的工业互联网安全运营体系

1.1.1 方案概述

本方案通过建设一套自研可控可扩展的安全运营平台，实现在线化全生命周期的安全管理，助力用户全面安全能力的价值交付。结合方案案例用户前期安全设备及安全系统建设成果，以“安全三同步”原则帮助用户逐步补齐基础安全工具能力的不足、完善安全系统交融互通，打破信息系统及安全设备的数据屏障，汇总全面安全数据，将安全运营能力覆盖 OT、IT 存量操作系统、中间件、数据库、网络设备、安全系统及控制设备等，同时支持未来增量系统的全面运营。构建四大类信息安全运营工作，实现漏洞、基线、事件及风险业务的运营管理闭环。

1.方案背景

装备制造企业发展普遍具有分散性及阶跃性，依据业务经营的市场需求及业务战略的规划方向，企业会分时期在不同地理区域独立建设生产不同产品类别的生产园区，企业充分考虑原材料、运输能力、技术人才的平衡，用以服务不同下游行业的业务需求。不同园区的信息化建设工作普遍独立进行，同时方案建设应用的技术体系也存在一定区别，从而形成各具特色的信息化网络架构与 IT、OT 技术环境。伴随着装备制造企业下属生产园区数量的增多，企业业务数字化运营也遇到了前所未有的难题，“数据分散、架构差异、资源浪费、人低效下、决策困难”等用户痛点不仅仅存在于业务层面，也同样阻碍在企业信息安全层面层面。装备制造企业通过工业互联网平台、数据中台、技术中台统一构建一套服务于生产的业务运营体系，一定程度上

解决了上述难题。企业应吸取业务运营体系成熟经验，在信息安全方面构建一套 OT、IT 安全能力全面融合的工业互联网安全运营体系，助力装备制造企业信息业务与信息安全能力同步提升。

本方案用户为应对不同时期安全风险及迫切程度不同的安全防护需求，遵循“同步规划、同步建设、同步运营、适度安全”的原则，已分批完成了包含 IT 防火墙、OT 防火墙、IT 态势感知、漏洞扫描系统、终端准入、Web 应用防火墙等安全系统的建设工作，但对于 OT 侧态势感知能力、工业主机安全，IT 侧服务器主机安全等基础安全设备仍存在建设空白，亟需补齐对应安全防护能力；用户构建网络安全态势感知能力局限于公有云下信息系统流量分析，对于公有云上业务流量的安全事件无法一体化分析，存在业务流量分析不完整的风险，亟需实现对公有云流量也能做到全面的安全态势分析能力；用户当前安全能力建设被动，在多次攻防演练活动中被动防御，需要补充必要的安全诱捕反制能力助力安全运营的高效联动；用户各独立安全系统目前数据割裂情况严重，安全防护能力没有形成合力，不能汇聚海量安全数据挖掘其真正价值，针对安全整改工作流程无法数字化管控，迫切需要建设一套安全运营平台，构建 OT、IT 安全能力全面融合的工业互联网安全运营体系，实现安全分类分级运营，建立自动化安全管理流程，全面提升安全处置能力。

2.方案简介

公司结合自身工业 Know-How 的积累，真正理解工业企业安全需求，整合最优安全能力，全面提高工业用户安全防护和管理水平，进一步优化安全资源利用率，发挥安全资源应用价值，降低用户安全投入总成本，推动构建 OT、IT 安全能力全面融合的工业互联网安全运营体系建设进程。本方案建设贯穿用户“工具层”、“系统层”、“平台

层”、“运营层”以及“能力层”全面安全能力的融合管理。主要内容如下：

➢ **工具层：**利旧用户已建设的“IT 防火墙、OT 防火墙、IT 态势感知、WEB 应用防护、漏洞扫描”等安全技术成果，为用户补齐包括“IT 服务器安全、OT 态势感知、OT 主机安全、蜜罐”等安全技术能力短板;;

➢ **系统层：**实现用户多个公有云上业务系统与云下业务系统安全管理的全面融合,构建风险感知能力,实现安全感知能力全域无死角,并将安全数据汇总至安全运营平台安全大数据分析系统模块;

➢ **平台层：**构建 OT、IT 安全能力全面融合的工业互联网安全运营平台,包括用于安全大数据分析的安全中台以及用于支撑安全运营管理的安全前台,完成与安全系统及工具的解耦,模块化接入各系统、各设备安全运营所需数据;

➢ **运营层：**建设包含漏洞管理、基线管理、事件管理、风险管理在内的安全运营管理能力，同时打通 OA、飞书、等集团信息系统流程，实现安全系统与业务系统全面融合;

➢ **能力层：**完成系统化纵深安全防御与数字化高效安全运营的融合，由被动防御应对向主动运营反制转变，全面提升企业安全能力。

3.方案目标

方案建设总体目标包括完善基础安全防护能力、覆盖集团全面业务资产、实现安全分类分级运营、建立自动化安全工单管理流程、全面提升安全处置效率等内容，拆解实现运营管理效率提升目标如下：

➢ **漏洞管理目标：**实现集团 OT、IT 高危漏洞收集、通知、整改、完成、复检全流程管理，漏洞整改闭环率 100%，紧急漏洞 48 小时内完成响应与整改;

➢ **基线管理目标：**实现集团 OT、IT 相关系统、中间件、数据库、设备的安全配置基线检查结果收集、通知整改、整改完成、复检管理，基线覆盖率达到 95%；

➢ **事件管理目标：**实现集团 OT、IT 信息安全攻击事件工单处罚、通知整改、整改完成、工单关闭管理，事件响应时间不超过 8 小时；

➢ **风险管理目标：**实现集团 OT、IT 日常信息安全风险的发现记录、跟踪处置过程，风险覆盖率 100%跟踪。

1.1.2 方案实施概况

本方案建设实施主要包括一套一体化安全运营平台，以其为核心进行工具建设、系统建设、运营建设，打破信息设备及安全设备的数据屏障，汇总全面安全数据，实现 OT 侧与 IT 侧、云上与云下全面融合的安全运营管理。

1.方案总体架构和主要内容

（1）顶层设计架构

以构建 OT、IT 安全能力全面融合的工业互联网安全运营体系的目标为指导，顶层设计架构涵盖设备层、工具层、平台层、运营层等多个业务层级，其中平台层根据灵活性、松耦合的实际需求，拆解为平台中台与平台前台两部分，从而起到安全运营体系的承上启下作用，如图 1-1 所示。

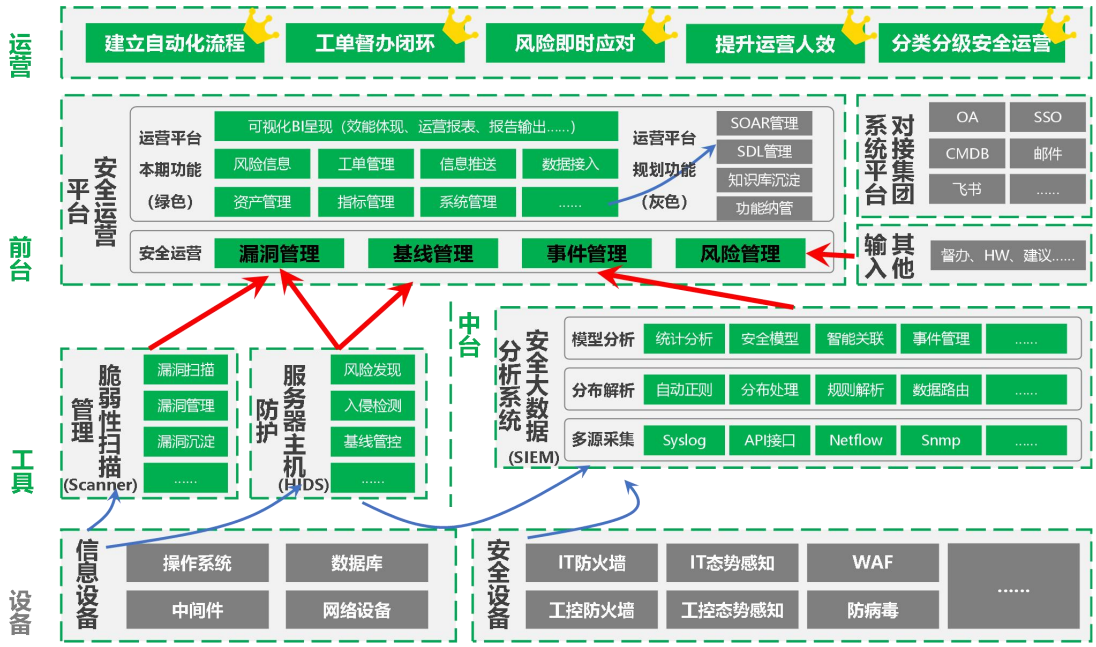

图 1-1　一体化安全运营总体功能架构

设备层包含 OT、IT 信息设备与 OT、IT 安全防护设备两大类，作为基础设施建设，既起到最直接的业务运行及安全防护支撑作用，又向上提供安全及业务分析所需海量数据；工具层利旧用户已建设的 OT、IT 系统脆弱性管理能力，同时建设服务器主机防护能力，实现主机及应用层漏洞及基线工具建设；平台中台层构建安全大数据分析系统，对下连接汇聚 OT、IT 设备安全数据及安全工具系统日志数据，对上支撑前台系统数据高价值应用调度；平台前台层构建涵盖漏洞管理、基线管理、事件管理、风险管理在内的运营交付能力，建立支撑全面安全运营的系统功能组件，对接集团三方业务系统；安全运营层依托上述业务层级能力实现分类分级的自动化安全运营，支撑风险及时应对，全面提高安全运营效率。

（2）公有云上与云下安全态势统一管理

为构建全面覆盖用户业务的安全风险识别能力，解决“信息安全木桶效应”的短板问题，充分考虑集团当前多公有云业务账号各成体系、云安全产品与云下安全体系适配困难、自动处理能力欠缺、生产

特征环境差异大”等业务现状，在不改变用户现有网络和业务架构的基础上，实现用户多个公有云上业务系统与云下业务系统安全管理的全面融合，构建风险感知能力，实现安全感知能力全域无死角，并将安全数据汇总至安全运营平台安全大数据分析系统模块，如图 1-2 所示。

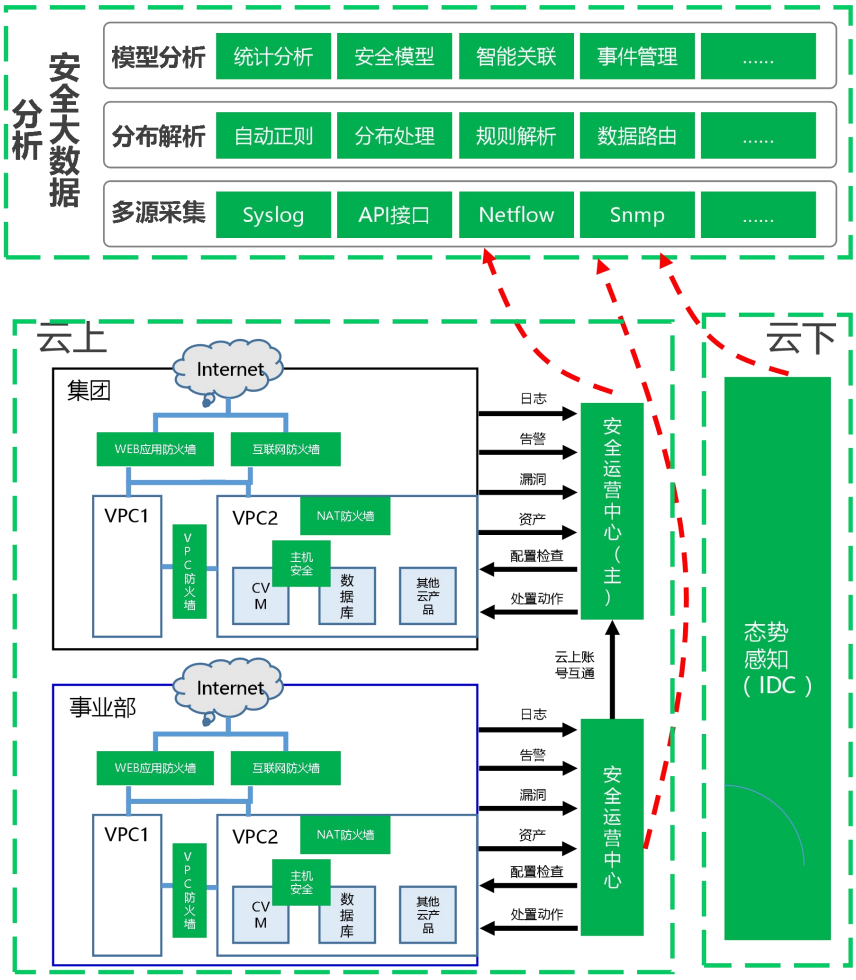

图 1-2　多公有云与云下安全态势统一管理架构

安全运营平台构建安全大数据分析系统，通过丰富的多源采集接口接入来自多公有云账号的安全数据以及云下 OT、IT 态势感知安全数据，并依托安全模型进行安全数据的价值提升与智能关联，将云上与云下、OT 与 IT 链接为一体，见微知著全面洞悉用户安全风险；云下部分利旧用户已建设的 IT 态势感知系统，同时建设针对于工业生产的 OT 态势感知能力，通过数据接口与安全运营平台进行数据交互，

实现动态闭环；云上部分依托公有云原生安全能力，通过云厂商支撑网络及数据接口平台研发打通各账号信息安全壁垒，实现与安全运营平台的数据交互，从而实现云上云下的一体化安全分析。

2.网络、平台或安全互联架构

（1）基础网络安全互联架构

公司致力于用户数据及信息内容的保护，严格遵循《网络安全法》、《数据安全法》、《个人信息保护法》等法律法规要求，为保障用户信息安全，针对网络、平台及安全互联架构进行脱敏抽象处理，用户网络安全架构仅做示意展示，如图 1-3 所示。

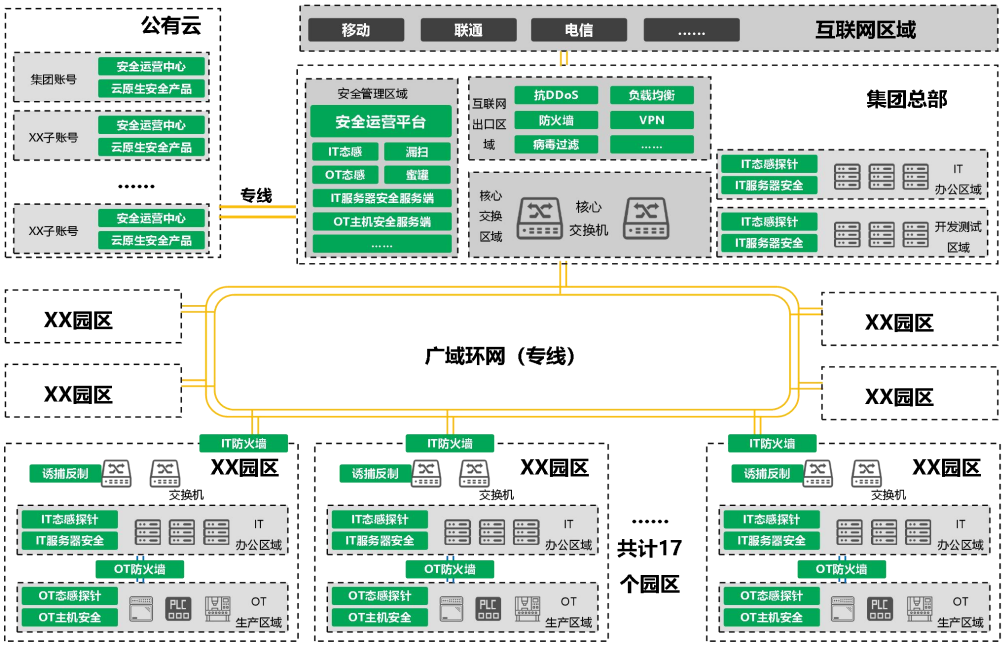

图 1-3　基础网络安全互联架构示意图

用户在全国范围建设涉及包括混凝土机械、挖掘机械、起重机械、筑路机械、桩工机械、风电设备、港口机械、石油装备、煤炭装备、装配式建筑 PC 机械等全系列产品的生产园区，并建设覆盖产品研发、设计、生产、销售、售后活动的业务系统。用户利用运营商专线建设骨干广域环网用于构建集团业务网络；各生产园区根据自身业务需要独立构建园区网络，并根据业务特点为工业生产业务独立构建 OT 生

产网络保证网络的分区分域隔离管理；用户公有云上存在大量业务系统，为保障业务的安全稳定性，集团与公有云运营商通过专线进行安全的互联互通。

本方案在用户集团安全管理区域部署一体化安全运营平台、攻击诱捕反制蜜罐系统、服务器主机安全防护系统、OT 态势感知系统、OT 工控主机安全系统，同时利旧用户原有 IT 防火墙、OT 防火墙、IT 态势感知、漏洞扫描、云原生安全等能力，共同构建 OT、IT 安全能力全面融合的工业互联网安全运营体系，各园区网络实现覆盖 OT 生产环境、IT 办公环境的边界防护能力、计算环境防护能力，通过态势感知探针实时洞悉网络安全风险，并在部分园区尝试性部署攻击诱捕反制系统用于变被动防御为主动反制。安全运营平台汇聚包含各园区 OT 生产区域、IT 办公区域、集团办公区域、研发测试区域、公有云业务区域在内的安全信息，形成海量的安全分析数据源，支撑 OT 侧与 IT 侧、云上与云下全面融合的安全运营管理。

（2）诱捕反制安全能力架构

本方案选取具有代表性的生产园区、集团部分业务网段、公有云部分业务网段作为攻击诱捕反制安全能力建设试点，希望实现将系统化纵深安全防御与数字化高效安全运营相融合，由被动防御应对向主动运营反制转变，全面提升企业安全能力。架构示意如图 1-4 所示。

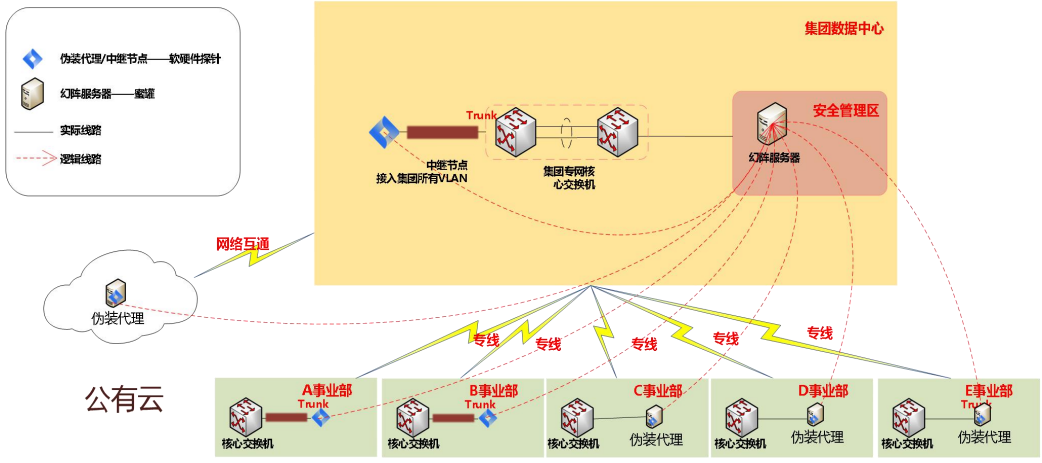

图 1-4　诱捕反制安全能力架构示意图

在集团安全管理区域部署诱捕反制系统模拟出多套仿真沙箱，实现对门户网站、协同办公系统、VPN 系统等面向互联网的业务系统进行模拟，将欺骗防御资产融入到用户集团的真实资产中，吸引攻击者的注意力，保护真实资产；在部分重要园区部署中继节点，在公有云环境中部署伪装代理，模拟和监听非业务端口，实现端口混淆，利用网络中空闲 IP 与真实流量构建具有迷惑性的资产暴露，实现分布式蜜网感知，将内网横向移动、僵木蠕毒行为诱导至沙箱；在互联网、内网等各个区域及各个园区密布诱饵，从而有助于发现、延迟或阻断攻击者的活动，达到增加信息系统安全性的目的。

3.具体应用场景和安全应用模式

（1）漏洞管理运营

漏洞管理运营功能依托安全运营平台对接用户 OA、SSO、CMDB 等三方系统获得统一的流程资产数据输入及权限管理，借助方案建设服务器主机防护及脆弱性扫描管理系统等工具，服务于包括整改责任人、安全管理员、事业部安全专员、事业部业务领导、集团领导在内的相关角色，完成贯穿漏洞管理信息获取、工单生成、漏洞整改、结果验证、工单关闭在内的全流程闭环管理。实现涵盖 OT、IT 系统在内的高效漏洞管理运营。应用示意图如图 1-5 所示。

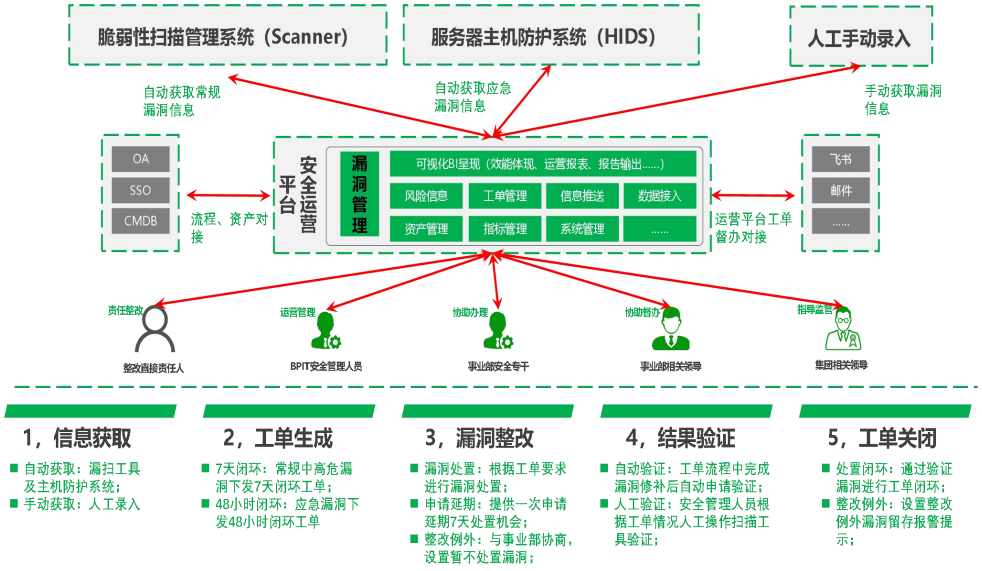

图 1-5　漏洞管理运营应用场景示意图

（2）安全工具自服务模式

本方案以安全能力自服务理念，全面提升安全资源效率，各事业部责任整改人收到安全整改流程督办信息后，根据安全运营平台知识库辅助完成安全整改工作，其后通过安全运营平台可实现针对安全问题复测提交，不借助安全运维人员，以自服务的形式进行安全工具使用申请，平台通过优先级业务逻辑选择，依照相关顺序完成复测检验，进一步优化安全资源利用率，发挥安全资源应用价值。应用示意图如图 1-6 所示。

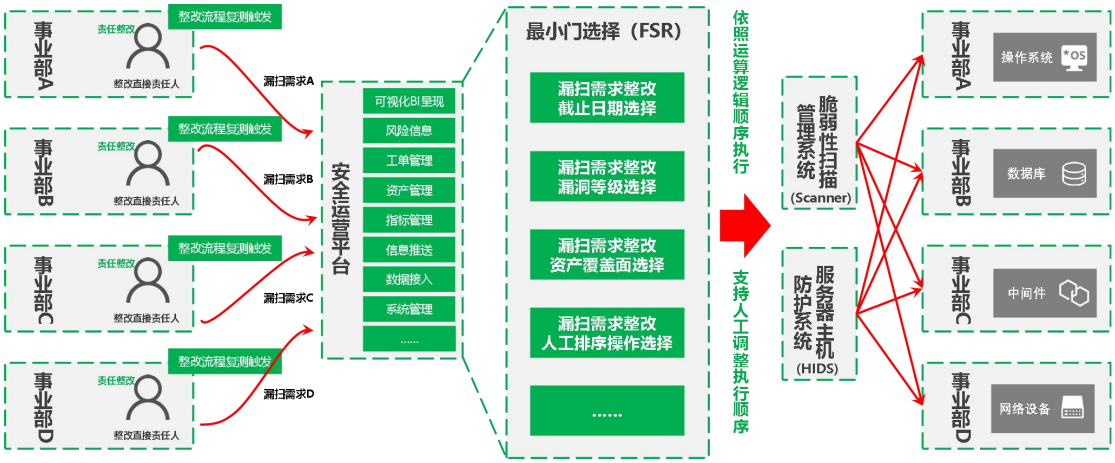

图 1-6　安全工具自服务应用场景示意图

（3）安全信息统一追溯管理

一体化安全运营管理平台汇聚安全数据涉及多系统、多区域、多层级、多主体，在安全信息的传递汇聚过程中不可避免的造成数据的可用性降低，信息缺失。为提升安全运营精准性，安全运营平台多维度构建信息来源追溯功能，通过包含设备 IP、时间印记、业务 ID 等信息在内的数据来源识别能力，帮助安全分析层层下钻。应用示意图如图 1-7 所示。

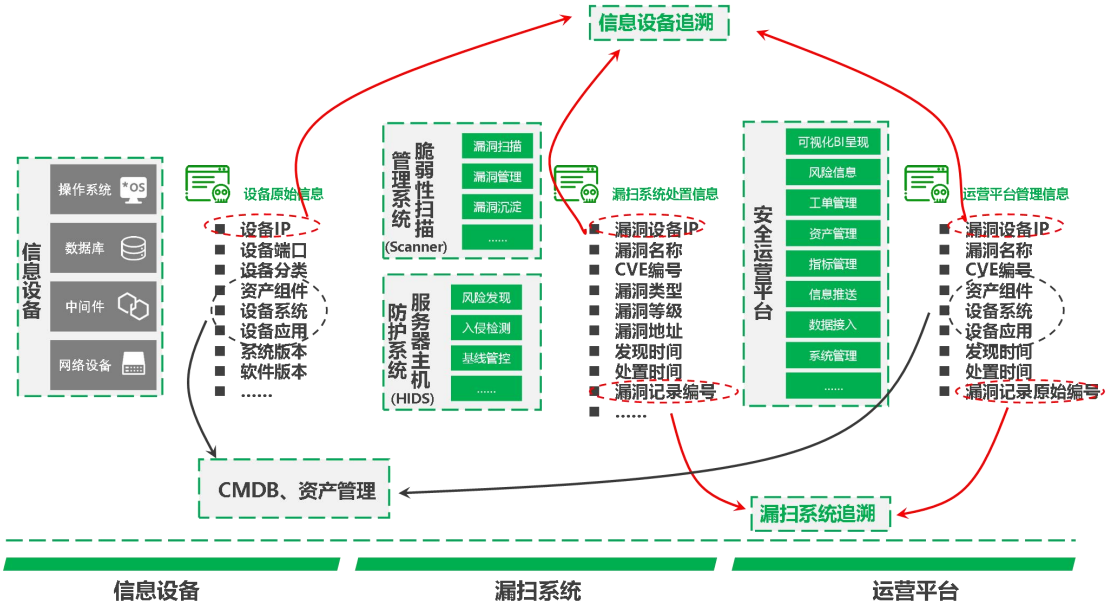

图 1-7　安全信息统一追溯管理应用场景示意图

4. 安全及可靠性

（1）完善的基础防护能力

本方案为构建 OT、IT 安全能力全面融合的工业互联网安全运营体系，对用户网络、业务、安全现状进行充分调研分析，帮助用户形成涵盖“网络、边界、主机、设备、应用”的基础防护能力及风险识别能力。网络方面通过 OT、IT 态势感知系统充分识别风险流量，边界方面通过 OT、IT 防火墙进行有效的访问控制管理，主机方面通过 IT 服务器主机防护系统及 OT 工控主机防护系统提供差异化的计算环境保护，设备及应用方面通过脆弱性管理系统保障 OT、IT 设备及系统漏洞可知、可管、可控，并通过安全运营平台构建覆盖用户集团整

体的安全运营管理能力。

（2）可靠的安全运营能力

方案通过安全运营平台打通用户安全流程协同管理，借助OA、BPM流程引擎，将安全与业务紧密融合；构建丰富的安全运营指标展示与考核功能，以数字化技术手段将安全数据价值全面提升展示；建立全自动工单闭环管理功能，保障安全运营督办的执行落地，多状态、多分支、多角色共同参与，保障业务安全有效平稳运行。

5. 其他亮点

（1）龙头企业示范效应

本案例用户作为我国工程机械装备行业龙头企业，其安全防护能力及安全运营能力建设成果对行业具有高度示范作用；同时，用户上下游产业链机构丰富，以点及面，行业影响效果显著。方案用户充分落实企业网络安全主体责任，为产业行业先进引领，完成了高质量的试点示范。

（2）重点活动成效显著

用户作为大型工业生产企业存在资产暴露面大、OT生产环境复杂、安全运营应急响应难度大等问题，在历年各级主管单位重点活动中演练成绩不佳。用户依托本方案安全运营体系建设，形成了OT、IT安全能力全面融合的工业互联网安全运营体系，于2022年度在其所在省份网络攻防演习获得第二名的优异成绩。

1.1.3 下一步实施计划

1. 运营平台能力提升

遵循安全能力“同步规划、同步建设、同步使用”的原则，本期方案功能规划预留了充分的能力提升空间。下一步计划将安全运营平台进行持续能力提升，当前安全处置仍需人工审核，在进一步积累安

全场景、安全处置剧本、安全响应标准动作的帮助下，逐步完善运营平台 SOAR 的能力，充分结合业务分类分级管理运营，将可控低影响的安全事件，逐步依托安全剧本自动化处置，进一步提升安全处置效率，将安全运营人力进一步释放。

2. 保护范围持续完善

根据用户业务的不断发展，以及业务系统应用技术的不断演进，用户容器部署的业务系统日渐增多，业务功能微服务化趋势明显。下一步计划在安全功能持续完善方面帮助用户将容器内的风险识别、安全保护、安全检测、安全响应融入整体安全运营平台体系，保障安全防护与业务系统同步发展、敏捷支撑。

3. 解决方案行业推广

伴随着本方案标杆案例的持续运营完善，业务安全处置模型的不断积累，安全运营功能的实用落地，安全指标维度的丰富积累。下一步计划发挥龙头企业标杆案例示范影响效力，在装备制造行业及上下游产业行业中进行构建 OT、IT 安全能力全面融合的工业互联网安全运营体系解决方案的持续推广，助力工业互联网安全产业不断发展。

1.1.4 方案创新点和实施效果

1. 方案先进性及创新点

本方案打破当前普遍存在的用户适应安全厂商固定安全运营产品的现状，高度重视用户业务需求，以自研可控、代码级交付的理念为用户按需交付安全运营能力，方案统筹考虑 OT 生产环境及 IT 办公环境的安全运营覆盖建设，创新性实践公有云安全风险与云下传统安全态势感知的统一运营管理，方案完成系统化纵深安全防御与数字化高效安全运营融合，由被动防御应对向主动运营反制转变，全面提升企业安全能力。部分先进创新内容如下：

（1）覆盖全、体量大

本方案覆盖生产园区 OT、IT 系统涉及全国十余个省市，涉及工业生产品类达数十种、服务器主机安全运营体量达万级、OT 工业主机安全防护近千套、OT 态势感知探针建设近百……

（2）品类多、全融合

本方案涉及安全信息来源广泛，存在大量 IT 系统及 OT 系统，包含多个公有云环境、集团 IDC 机房、集团研发测试区域、多省事生产办公区域……

2. 实施效果

通过本方案的实施，为用户实现了集团-园区、云上-云下的全面安全运营及安全防护能力提升，具体表现在运营效果、防护效果以及反制效果三个方面：

（1）运营效果

本方案通过一体化安全运营体系的构建，帮助用户打破安全数据交互壁垒，统筹安全能力，从而形成安全防护合力。建设以漏洞管理、基线管理、事件管理、风险管理为功能模块的安全运营前台，通过安全运营中台汇聚海量安全数据，挖掘数据真正价值，全面提高安全处置效率，提升安全岗位人效，赋能集团人员安全意识提升。促使用户集团信息安全处置效率提升 87%、安全数据可视化利用率达到 90%、安全资产管理率达到 99%。

（2）防护效果

本方案为支撑能够建设 OT、IT 安全能力全面融合的工业互联网安全运营体系，利旧用户原有 IT 防火墙、OT 防火墙、IT 态势感知、漏洞扫描、云原生安全等能力的同时，新增建设 IT 服务器主机安全防护系统、OT 态势感知系统、OT 工控主机安全系统，攻击诱捕反制

蜜罐系统。全面提升用户涉及“网络、边界、主机、设备、应用”的基础防护能力及风险识别能力。

（3）反制效果

本方案选取具有代表性的生产园区、集团部分业务网段、公有云部分业务网段作为攻击诱捕反制安全能力建设试点，实现系统化纵深安全防御与数字化高效安全运营融合，由被动防御应对向主动运营反制转变，全面提升企业安全能力。2022 年度用户在其所在省份网络攻防演习中，借助诱捕反制得分获得优异成绩。

1.1.5 单位基本信息

树根互联股份有限公司将新一代信息技术与制造业深度融合，开发了以自主可控的工业互联网操作系统为核心的工业互联网平台——根云平台。公司提供的工业互联网解决方案主要包括智能制造 IIoT 解决方案、产品智能化 IIoT 解决方案、产业链 IIoT 解决方案，赋能工业企业的智能生产管理、产品与服务的创新以及产业链协同，提供低成本、低门槛、高效率、高可靠的工业互联网数字化转型服务。公司是工信部遴选的第一批国家级跨行业跨领域工业互联网平台企业，并连续四年入选；2019 年根云平台成为了公安部信息系统安全等级保护（2.0）发布后首批通过三级测评的工业互联网平台；2021 年，公司收到国务院发展研究中心的致谢信：公司提供的“工程机械大数据——挖掘机指数”为国务院发展研究中心相关工作提供了数据支撑，并对有关政策制定和实际工作发挥了积极作用。根云平台于 2019 年、2020 年、2021 年连续三年入选权威机构 Gartner 全球工业互联网魔力象限，系唯一入选的中国工业互联网平台；在 IDC 发布的《2021

年中国工业互联网平台市场厂商评估》结果中，公司位于领导者象限，技术力位居中国第一；在福布斯中国《2021 年度中国十大工业互联网企业》排名中，公司位列第一；公司于 2021 年取得 CMMI 最高等级 5 级认证。