1.1 案例十：智能油库工业控制系统网络安全建设——护航产业数字化变革，提升智能油库安全能力

1.1.1 方案概述

本方案的是结合智能油库的网络安全现状，确定油库企业的安全建设需求，按照《网络安全等级保护基本要求》（GB/T22239-2019）和中石化318号文等政策要求，加强“监测预警系统”、“终端安全查杀能力”、“应急响应手段”、“大数据安全平台”、“信息系统等级保护建设”的推进工作，全面提升油气集输行业的网络安全保护及整网安全能力，并建立一个完善的信息安全预防、监测、防御和响应的纵深防御的安全体系。

1.方案背景

工业控制系统是支撑国民经济的重要设施，是工业领域的神经中枢。目前工业控制系统已广泛应用于电力、轨道交通、石油化工、高新电子和航空航天等领域，这些领域中涉及国计民生的关键基础设施超过80%都需要依靠工业控制系统来实现自动化作业，由此可见工业控制系统已经成为国家关键基础设施的重要组成部分。

随着我国工业由传统产业向网络化、数字化和智能化的逐步转型升级以及工业互联网平台的建成，网络安全威胁日益向工业领域蔓延。与此同时，我国工业领域还存在信息安全防护水平偏低、管理力度稍显不足、防护措施不到位、从业人员安全意识不强和安全技术人才匮乏等问题。

为了保障网络安全，国家颁布了《中华人民共和国网络安全法》，将网络安全上升到了法律的层面。国标《网络安全等级保护基本要求》（GB/T22239-2019）暨等级保护2.0标准增加了工业控制系统扩展要

求。在等级保护的基础上又颁布了关键基础设施保护条例，对关键基础设施的保护力度大大加强。工信部发布了《工业控制系统信息安全防护指南》从管理、技术两方面明确了工业企业工控安全防护要求，《“工业互联网+安全生产”行动计划（2021-2023）年》提出坚持工业互联网与安全生产同规划、同部署、同发展，构建基于工业互联网的安全感知、监测、预警、处置及评估体系。我国针对工业控制系统信息安全颁布实施的一系列标准、政策、法规，表明了我国在保护工业控制系统安全方面的决心和力度。集团公司依据国家有关政策法规、工信部相关系列标准发布了《关于加强工业控制系统安全防护的指导意见》、《中国石化工业仪表控制系统安全防护实施规定》以及《关于推进工控系统安全防护治理工作的通知》，对企业提升工业控制系统的安全防护能力提供了指南和依据，通知要求工控系统管理部门和信息管理部门组建安全防护治理工作小组，对照实施规定及时整改网络架构，开展工控系统边界隔离防护和内外部安全加固，提高工控网络态势感知和事件追溯能力。

2.方案简介

成品油油库是销售公司石油供应链中至关重要的一个环节，而工控系统作为油库的核心系统，其安全与生产安全直接关联。随着油库的信息化建设和改造，工业化与信息化的结合日益紧密，油库工控系统安全环境也从单机走向互联，从封闭走向开放，从物理隔离的工业以太网走向开放的工业互联网。油库工控系统正面临着严峻的信息安全威胁，其尚未完善的网络安防体系给油库的工控系统运行环境带来了巨大的安全隐患，因此急需设计一套集安全防护、安全运营、安全集成与一体的综合性全生命周期的解决方案、加强油库工控系统安全建设，为油库的安全生产提供网络安全基础。

工控系统的安全方案设计应考虑物理安全、网络安全、应用安全和数据安全等多方面安全因素，任何一个方面的安全隐患都会给整个工业控制系统带来安全事故。目前国家网信办、工信部及公安部先后出台的网络安全和工控安全相关法律条例中对信息安全技术和工控系统信息安全等方面做出了指导与要求。2021 年，集团公司下发了工控系统安全防护治理工作的通知，要求开展工控系统边界隔离防护和内外部安全加固工作，提高工程网络态势感知和事件追溯能力，销售公司也对油库智能化建设标准提出了要求，对油库下一步信息化建设提出了指导意见和具体措施。在工业控制系统的安全防护建设中，需严格遵循国家和行业有关标准，并遵照中国石化相关安全管理规定，结合生产企业具体情况和需求进行规划与建设。

3.方案目标

目前销售企业油库整体智能化水平较低，大多数油库仅具备基本的信息安全防护条件，仍难以满足油库信息化建设对工控系统安全的要求，主要存在以下的问题：

（1）安全区域不清晰，缺少边界防护措施

油库缺失分区分域安全隔离，油库生产网与管理网混用，传统的 IT 网络威胁向生产网蔓延，工控网通讯协议较多，单一的隔离设备无法满足多样的网络通讯及安全隔离要求，难以保障油库工控网络隔离有效性，易感染病毒及恶意程序，同时也可能导致工业控制系统内不同安全域之间的边界防护机制失效。

因此，在油库工控系统中，存在缺少混合组网隔离、分区分域网络隔离、数据隔离防护措施及恶意代码防范措施等问题。

（2）缺少终端安全防护

油库工控网络中硬件设备或软件产品不足，部分设施和操作系统

老旧，漏洞补丁更新不及时，网络安全防护能力较低，缺少工控安全病毒防护，缺少网络准入等安全管理工具。同时工控安全领域中的终端防护软件种类多，难以形成统一的防护规范，亦存在重大安全隐患。

（3）缺少安全审计和分析

油库工控系统的数据本地存储、数据共享能力较差，应用深度不够，对数据库的访问人员缺乏统一账号管理，缺乏数据访问隔离措施及数据操作审计，缺乏对数据库信息的收集、审计和分析等能力。

（4）缺少统一的安全管理平台

油库缺乏对第三方运维机构的管控和统一安全运维管理，无法将各安全设备集中管控，缺乏对各运维人员身份的认证授权及操作行为的监管，造成日常运维操作繁琐、过程冗杂、效率低下等问题。油库部分系统孤立，集成度较差，不能实现数据共享，存在“信息孤岛”现象，导致油库工控网络全貌无法得到集中统一展现。同时，也给省级统一平台构建带来困难，不利于系统间集成、作业全流程跟踪、生产动态的实时掌控和预知预排，无法掌握整体信息安全态势。无法及时发现和追溯工控安全事件，缺乏对工控系统安全状态感知及可视化的展示方式。

本方案的建设目标是结合智能油库的网络安全现状，确定油库企业的安全建设需求，按照《网络安全等级保护基本要求》（GB/T22239-2019）和中石化318号文等政策要求，加强“监测预警系统”、“终端安全查杀能力”、“应急响应手段”、“大数据安全平台”、“信息系统等级保护建设”的推进工作，全面提升油气集输行业的网络安全保护及整网安全能力，并建立一个完善的信息安全预防、监测、防御和响应的纵深防御的安全体系。具体目标如下：

在技术方面，围绕“一个中心三重防护”策略构建基础防护：

➢ 通过安全计算环境防护，实现油库工控系统的工业主机、服务器、操作站、工业应用软件等计算环境安全防护；

➢ 通过安全区域边界防护，实现油库工控系统网络与非工控网络的安全隔离，保护工控系统网络安全；

➢ 通过安全通讯网络的搭建，保障油库工控系统的通信基础网络安全可靠；

➢ 通过安全管理中心实现对油库工控系统网络的全流量审计、分析，同时对油库工控系统威胁状态进行实时监控，对整个油库工业控制网络安全威胁集中管控和展示。

在管理方面，围绕安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理五个方面进行提升，以分区分域、可靠认证、综合防护、集中掌控为防护原则，实现技术和管理相结合的油库网络安全纵深防护体系，从而提升油库工控系统的主动防御、感知预警、事件追溯和集中安全运维的能力。

1.1.2 方案实施概况

1.方案总体规划

（1）方案设计原则

等级保护是国家信息安全建设的重要政策，其核心是对信息系统分等级、按标准进行建设、管理和监督。对于智慧油库信息安全建设，应当以适度安全为核心，以重点保护为原则，从业务的角度出发，重点保护重要的业务系统。对于工控安全建设，应当以适度安全为核心，以重点保护为原则，从业务的角度出发，重点保护重要的业务系统，在方案设计中应当遵循以下的原则：

适度安全原则

任何信息系统都不能做到绝对的安全，在进行工控安全等级保护

规划中，要在安全需求、安全风险和安全成本之间进行平衡和折中，过多的安全要求必将造成安全成本的迅速增加和运行的复杂性。

适度安全也是等级保护建设的初衷，因此在进行等级保护设计的过程中，一方面要严格遵循基本要求，从物理、网络、主机、应用、数据等层面加强防护措施，保障信息系统的机密性、完整性和可用性，另外也要综合成本的角度，针对系统的实际风险，提出对应的保护强度，并按照保护强度进行安全防护系统的设计和建设，从而有效控制成本。

技术管理并重原则

工控安全问题从来就不是单纯的技术问题，把防范黑客入侵和病毒感染理解为工控安全问题的全部是片面的，仅仅通过部署安全产品很难完全覆盖所有的工控安全问题，因此必须要把技术措施和管理措施结合起来，更有效的保障信息系统的整体安全性，形成技术和管理两个部分的建设方案。

分区分域建设原则

对信息系统进行安全保护的有效方法就是分区分域，由于信息系统中各个信息资产的重要性是不同的，并且访问特点也不尽相同，因此需要把具有相似特点的信息资产集合起来，进行总体防护，从而可更好地保障安全策略的有效性和一致性；另外分区分域还有助于对网络系统进行集中管理，一旦其中某些安全区域内发生安全事件，可通过严格的边界安全防护限制事件在整网蔓延；

标准性原则

安全保护体系应当同时考虑与其他标准的符合性，在方案中的技术部分将参考《GB/T 25070-2010 工控安全技术 信息系统等级保护安全设计技术要求》进行设计，在管理方面同时参考《GB/T

22239-2008 工控安全技术 信息系统安全等级保护基本要求》以及27001安全管理指南,使建成后的等级保护体系更具有广泛的实用性;

动态调整原则

工控安全问题不是静态的，它总是随着管理相关的组织策略、组织架构、信息系统和操作流程的改变而改变，因此必须要跟踪信息系统的变化情况，调整安全保护措施;

成熟性原则

本方案设计采取的安全措施和产品，在技术上是成熟的，是被检验确实能够解决安全问题并在很多方案中有成功应用的。

（2）总体安全防护设计

构建分域的控制体系：智能油库工业互联网安全解决方案，在总体架构上将按照区域边界保护思路进行,智能油库控制系统和外部系统从结构上划分为不同的安全区域,以安全区域为单位进行安全防御技术措施的建设，从而构成了分域的安全控制体系。

构建纵深的防御体系：智能油库工业互联网安全解决方案包括技术和管理两个部分，智能油库系统围绕着安全管理中心，从安全通信网络、安全区域边界、安全计算环境三个维度进行安全技术和措施的设计,保证业务应用的可用性、完整性和保密性保护;通过集中管理,可对安全设备进行联动,对确认的重大威胁或攻击可进行安全联动防护，充分考虑各种技术的组合和功能的互补性，提供多重安全措施的综合防护能力，从外到内形成一个纵深的安全防御体系，保障系统整体的安全保护能力。

保证一致的安全强度：智能油库等级保护设计方案将采用分级的办法，对于同一安全等级系统采取强度一致的安全措施，并采取统一的防护策略，使各安全措施在作用和功能上相互补充，形成动态的防

护体系。

（3）分域安全防护设计

安全域是根据等级保护要求、信息性质、使用主体、安全目标和策略等的不同来划分的，是具有相近的安全属性需求的网络实体的集合。一个安全域内可进一步被划分为安全子域，安全子域也可继续依次细化为次级安全域、三级安全域等等。同一级安全域之间的安全需求包括两个方面：隔离需求和连接需求。隔离需求对应着网络边界的身份认证、访问控制、不可抵赖、审计、监测等安全服务；连接需求对应着传输过程中保密性、完整性、可用性等安全服务。下级安全域继承上级安全域的隔离和连接需求。

智能油库安全区域的划分主要依监控系统的应用功能、资产价值、资产所面临的风险，划分原则如下：

系统功能和应用相似性原则：安全区域的划分要以服务智能油库业务系统应用为基本原则，根据应用的功能和应用内容划分不同的安全区域。

安全要求相似性原则：在信息安全的三个基本属性方面，同一安全区域内的信息资产应具有相似的机密性要求、完整性要求和可用性要求。

威胁相似性原则：同一安全区域内的信息资产应处在相似的风险环境中，面临相似的威胁。

安全域的原则：必须对高级别安全域进行保护，使之免受可能导致高级别数据被低级别安全域的用户泄漏、篡改、破坏的攻击，高级别安全域中的资源不能由非授权的低级别安全域用户使用、修改、破坏或禁用。

2.2 实施内容

（1）体系建设

本方案从安全管理、安全建设和安全运营三个方面对油库信息化安全方案进行设计与规划，通过制度建设、人员配置、技术建设、整体运维管控等措施，从制度上对油库工控安全进行管理与约束，从技术上提升油库工控安全防护水平，从而构建油库工控安全防护体系。总体安全方案设计架构如图所示：

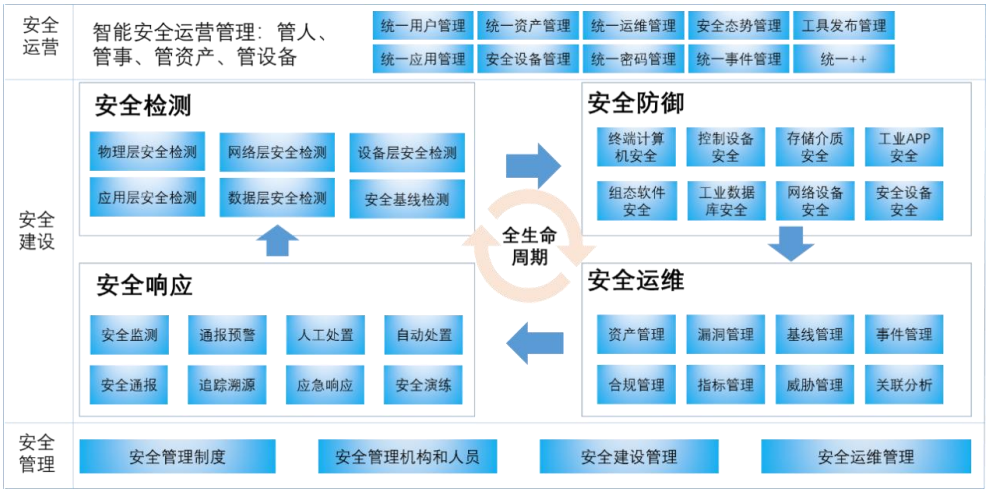

图 10-1　总体安全方案设计架构

● 安全管理

通过建立完善的油库信息化安全管理制度，组建人员成立安全管理机构，并对安全管理人员定期开展网络安全培训以提高油库工控安全整体管理水平，同时，在建设和运维方面也做出安全管理要求，制定油库工控系统安全建设和运维细则，加强在油库工控系统建设和运维环节的规范，实现油库工控安全管理的规范化、标准化与制度化。

● 安全建设

制定安全基线标准，定期开展安全监测工作，集中管控终端计算机、网络设备、安全设备，对油库工控网流量日志进行审计与分析，做到风险防控与阻拦；加强对安全事件、隐患漏洞、攻击行为的实时监测与智能分析，能够利用大数据分析、告警取证、流量画像等手段快速追踪溯源，采取自动处置与人工处置相结合的方式开展应急响应

工作，形成安全检测、安全防御、安全运维、安全响应的全生命周期管理。

● 安全运营

构建油库工控安全防护体系，搭建管理服务平台，通过统一身份认证、统一授权和统一监控等手段，加强对用户和运维角色的监管；通过对安全设备、资产及应用的集中管控，安全事件的自动监测，全天候全方位网络安全的态势感知，实现智能安全运营管理、增强网络安全防御能力。

（2）安全技术实施内容

首先对办公网和生产网进行纵向分层，划分横向安全区域，以工业防火墙、入侵检测和工业安全监测审计平台等工具构建安全区域边界，利用工业网闸实现油库生产网中的通信安全，保障重要业务系统间的数据传输安全；其次在油库终端设备上部署终端安全防护，并对数据库的操作进行审计，确保计算环境的安全性，并采用堡垒机，便携式安全移动运维平台等实现安全运维管理；最后通过工业安全管理平台、综合日志审计平台等搭建总体的安全管理中心，油库信息安全建设技术架构如图所示：

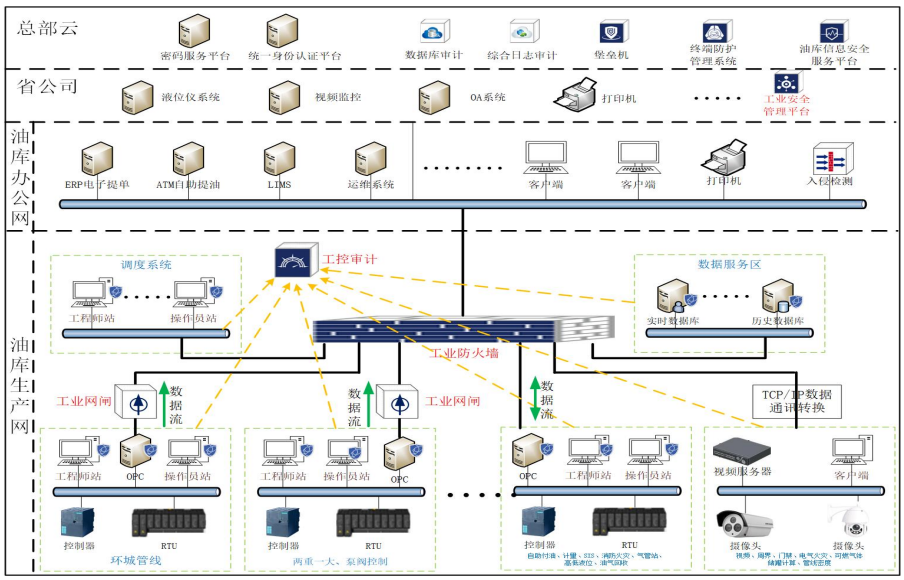

图 10-2　油库信息安全建设技术架构

● 网络安全

边界防护与区域隔离

根据油库的现状进行纵向分层、横向分区，通过相应的技术隔离手段，加强区域隔离、边界防护，细化访问控制策略，在办公网与生产网之间、生产网内部建立不同层级间安全防护，构建油库生产系统网络安全架构。如下图所示。

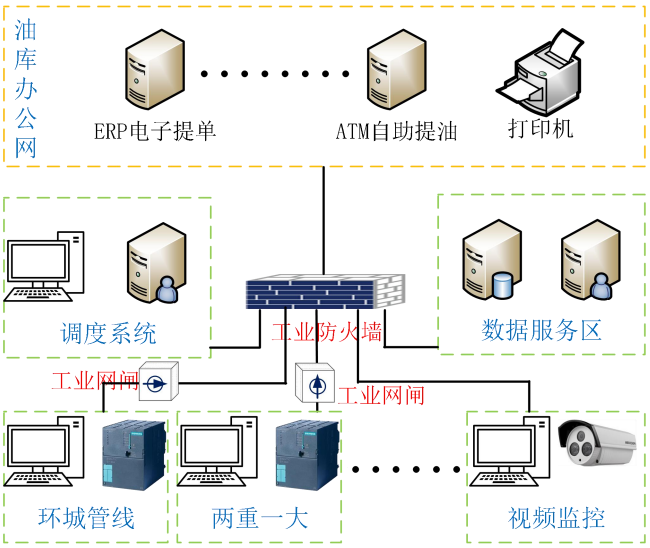

图 10-3　边界防护与区域隔离

纵向分层：按照网络划分为生产网和办公网，在生产网与办公网之间部署工业防火墙，通过白名单、访问控制等隔离技术手段，防止办公网的非法入侵和访问，保护生产系统的业务安全。

横向分区：按照现场的不同业务需求划分不同的安全域，将油库调度系统、视频监控、消防控制站以及安防系统等分别划分为不同的安全域，安全域之间通过工业防火墙的不同业务口实现安全域之间的隔离，利用设备本身的多个业务口，防止不同安全域之间安全威胁的蔓延以及对安全域之间的访问控制，阻挡来自其他安全域的病毒、蠕虫、木马、间谍软件、恶意软件等，有效地解决区域安全、流量控制等工控网络安全问题。

核心系统的安全防护：根据业务现状，对于重要的业务系统（例如：付油系统、阀门联动系统）设计单独的工业网闸，实现单向数据传输，确保业务系统的相对安全。

第三方信息交互：与第三方进行信息交互的场景，第三方网络通信链路连接到网闸外联口，通过网闸实现第三方网络与工控网络的安全隔离和信息的单向流动，可以在保障安全的情况下实现数据交换。

入侵检测与行为审计

在办公网和生产网中分别部署入侵检测和工控安全审计系统，实时发现针对重要工业控制系统的攻击和破坏行为，实时检测针对工业协议的网络攻击、用户误操作、用户违规操作、非法设备接入以及蠕虫、病毒等恶意软件的非法入侵和传播并实时报警，同时详实记录一切网络通信行为，包括指令级的工业控制协议通信记录，加强已知威胁、异常行为、异常流量等攻击行为的检测能力。如下图所示。

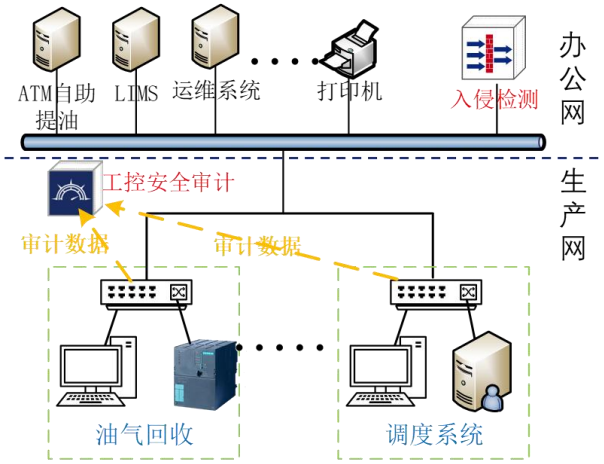

图 10-4　入侵检测与行为审计

在办公网的核心交换机上旁路部署，及时发现网络上的攻击和威胁。利用被动流量分析技术对僵尸网络、数据泄露等各类安全威胁进行深度检测、智能分析以及威胁感知，及时发现和定位网络中存在的安全威胁，在油库的网络、主机、应用等检测的基础上，实现业务零影响、持续跟踪的感知能力，提升攻击行为关联分析能力，为油库企

业等提供信息安全保障。

在生产网内部根据业务需求把相应业务系统的流量数据发送给工控安全审计，完成异常行为、异常流量的审计。通过对生产网中的工业协议进行深度解析，支持对 30 多种(OPC、SiemensS7、Modbus、IEC104、Profinet、DNP3 等）工控协议的深度解析和自定义扩展工控协议解析，还原工控指令，理解工控业务，提取关键信息，对当前的通信行为与已有的基线进行对比,实现异常指令操作、非法设备（IP 地址）等告警，工控审计对风险告警数据可进行细粒度的分类统计展示和联动操作，风险信息可一键关联至规则，对风险信息提供了可操作性强的处置措施建议。

对威胁与异常检测的审计主要分为以下五个方面：

一是异常报文检测：支持对 TCP/IP、工控协议畸形报文的攻击检测；

二是关键事件检测：支持对工程师站组态变更、操控指令变更、PLC 下装、零流量等工控关键事件的检测；

三是基线白名单检测：通过机器学习等自学方式生成工控环境资产基线、访问关系基线、流量基线、工控行为基线四种安全基线模型；

四是自定义规则检测：用户可自定义对多种工控协议进行细粒度的规则配置；

五是工控入侵规则检测：内置丰富的入侵检测规则库，支持利用已知工控设备漏洞的入侵攻击行为检测。

● 终端安全

在油库的终端设备上部署终端安全防护客户端，在省级安全管理中心上部署终端防护管理系统，解决终端设备的安全威胁，提高终端设备的安全防护能力。如下图所示。

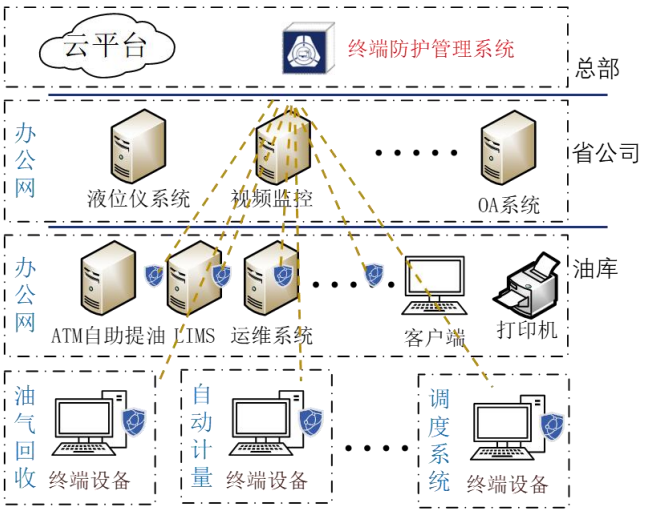

图 10-5　终端安全防护

对于可以安装终端安全防护客户端的终端设备，可以在终端防护管理平台上实时监控终端设备的性能、存在的漏洞、威胁事件等并进行统一管理。对于不能安装终端安全防护客户端的终端设备，利用总部的准入系统查看哪些终端设备没有安装。客户端可部署在 Windows 系列如 WinXP 、Win7 、Win10 、Win2003 、Win2008 、Win2012 、Win2016 等， inux 系统如 Centos5.0+ 、Redhat5.0+、Suse11+、Ubuntu14+等，国产系统如中标麒麟、银河麒麟、统信等终端系统上。

终端安全防护系统集白名单、黑名单和加固功能于一体，集成了丰富的系统加固与防护、网络加固与防护等功能的终端安全产品。包含专门应对攻防对抗场景的高级威胁模块和具有勒索专防专杀能力的文件诱饵引擎；通过内核级东西向流量隔离技术，实现网络隔离与防护；拥有补丁修复、外设管控、文件审计、违规外联检测与阻断、进程防护、端口防护和安全告警等终端安全防护能力。

● 应用及数据安全

在总部云平台上部署数据库审计与风险控制系统，提升对数据库的原始信息收集、审计和分析等能力，保障应用及数据安全，部署架构如下图所示。

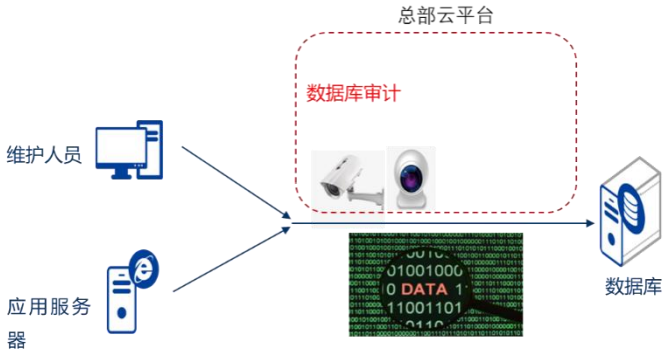

图 10-6　数据库审计与风险控制

数据库审计与风险控制系统实时记录运维人员及应用服务器对数据库的操作行为，并按照相关要求进行合规性管理，当系统检测到数据库面临风险行为时，会自动以邮件、短信、SYSLOG、SNMP 等形式进行实时告警。此外，数据库审计与风险控制系统还支持的功能如下所示：

加密协议审计及双向审计：系统不仅支持对数据请求的报文进行加密协议审计，同时也可以对请求的返回结果进行审计，如操作回应、作用数量、执行时长等内容，并能够根据返回结果进行审计策略定制。

建立安全访问基线：系统支持配置安全访问策略和设立安全访问基线，这样可以防范来自内外部的恶意攻击，保障油库工控系统数据的机密性和完整性，同时支持自行定义安全访问基线的检查项，因此可以根据油库实际业务需要定制检查阈值、自定义检查目录等以满足油库多样化的内部监管要求。

追踪用户访问行为：提供全方位的多层（应用层、中间层、数据库层）的访问审计，通过多层业务审计可实现对数据操作用户的精确追踪。并根据事件发生的时间、用户、访问方式（客户端、TELNET、FTP）、用户 IP、服务器等组合查询，对用户访问行为过程进行回放和追溯。

操作风险实时可知可查对数据库的操作行为进行实时检测，结合

预设置的风险控制策略和对数据库活动的实时监控信息进行特征检测，所有尝试攻击操作将被检测出来进而被阻断或告警。

● 安全运维与审计

在总部云平台上部署综合日志审计系统，对工业网络中的各种设备（网络设备、安全设备、工控主机设备、应用及数据库等）产生的日志进行采集、存储和分析，对危险的事件进行告警，同时将数据信息进行汇集然后集中展现，加强对异常事件的追溯及取证，便于管理人员集中查看所接入设备的运行状况并在第一时间获知当前发生的安全事件告警，使得等级保护满足合规检查。综合日志审计系统部署架构如下图所示。

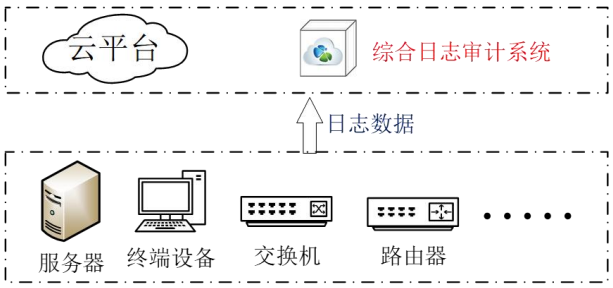

图 10-7　综合日志审计系统部署架构图

在总部部署运维审计与风险控制系统（简称堡垒机）是集用户管理、授权管理、认证管理和综合审计于一体的集中运维管理系统，在省级安全管理中心部署堡垒机可实现对企业运维人员在运维过程中进行统一身份认证、统一授权、统一审计、统一监控管理等一系列操作，使运维简单化，操作规范化，过程可视化，企业运维管控能力也得以提升，堡垒机部署架构如下图所示。

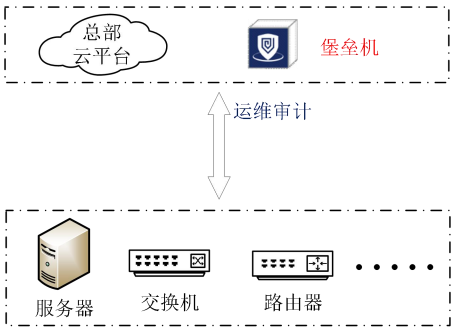

图 10-8　堡垒机部署图

● 安全集中管理

在总部云平台上部署工业安全管理平台，实现对工业防火墙、入侵检测、工控安全审计、堡垒机、数据库审计、工业网闸等安全设备的集中管控、状态监测、策略配置下发等，并支持通过标准接口（例如 syslog）与第三方设备通讯，从而实现资产安全状况的统一管理和安全风险的智能分析，工业安全管理平台以省公司为单位开通统一租户账号。如下图所示。

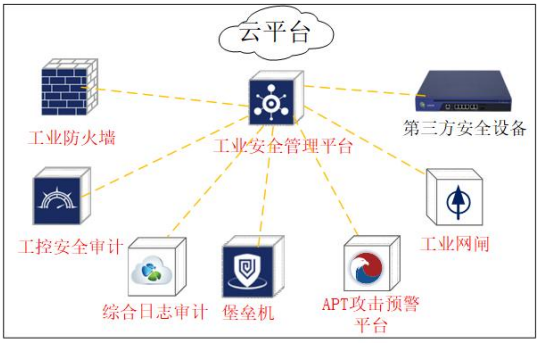

图 10-9　工业安全管理平台部署图

工业安全管理平台可及时发现、报告并处理工业控制系统中的网络攻击或异常行为，通过统一调度安全预警、安全监测、安全防护和应急处置，全方位保障工业控制系统信息安全。除此之外，平台可以对工业控制系统资产进行全局管理，帮助用户梳理工控资产，资产间的访问关系，网络中的工业行为等，尤其可对部署在系统中的安全防护类设备进行统一配置。

（3）安全管理方案

通过建立完善的油库信息化安全管理体系，组建人员成立安全管理机构，建立安全组织体系，制定油库工控系统安全运行细则，加强在油库工控系统建设和运维环节的规范，制定应急响应制度最大限度的减轻安全事件的危害和影响，并对安全管理人员定期开展网络安全培训以提高油库工控安全整体管理水平，实现油库工控安全管理的规

范化、标准化与制度化。

● **安全管理制度**

在信息安全中，最活跃的因素是人，对人的管理包括法律、法规与政策的约束、安全指南的帮助、安全意识的提高、安全技能的培训、人力资源管理措施，这些功能的实现都是以完备的安全管理政策和制度为前提。这里所说的安全管理制度包括信息安全工作的总体方针、策略、规范各种安全管理活动的管理制度以及管理人员或操作人员日常操作的操作规程。

安全管理制度主要包括：

管理制度：针对管理人员和操作人员的建立相关安全管理制度，形成由成安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。

制定和发布：安全管理制度的制定应由专业的人员负责制定，且要通过正式有效的方式发布并进行版本控制。

评审和修订：应定期对安全管理制度的合理性和适用性进行论证和审定并及时修订。

● **安全管理机构**

要建立一个健全、务实、有效、统一指挥、统一步调的完善的安全管理机构，明确机构成员的安全职责，这是信息安全管理得以实施、推广的基础。在单位的内部结构上必须建立一整套从单位最高管理层到执行管理层以及业务运营层的管理结构来约束和保证各项安全管理措施的执行。其主要工作内容包括对机构内重要的信息安全工作进行授权和审批、内部相关业务部门和安全管理部门之间的沟通协调以及与机构外部各类单位的合作、定期对系统的安全措施落实情况进行检查，以发现问题进行改进。

安全管理机构主要包括：

岗位设置：成立指导和管理网络安全工作的委员会或领导小组、设立安全管理工作职能部门、设立相关管理岗位并明确各岗位职责。

人员配备：配备专职安全管理员，根据情况配备一定数量的系统管理员、审计管理员和安全管理员。

授权和审批：明确各部门审批事项部门及批准人。对重要活动建立逐级审批制度，并定期审查审批事项，更新授权事项和审批方案。

沟通和合作：加强组织内部间沟通交流，定期召开协调会议，共同协作处理网络安全问题。

审核和检查：根据安全检查表格开展常规安全检查及全面安全检查，汇总安全检查数据，形成安全检查报告。

● 人员安全管理

很多重要的工控系统安全问题都涉及到用户、设计人员、实施人员以及管理人员。如果这些与人员有关的安全问题没有得到很好的解决，任何一个工控系统都不可能达到真正的安全。只有对人员进行了正确完善的管理，才有可能降低人为错误、盗窃、诈骗和误用设备的风险，从而减小了工控系统遭受人员错误造成损失的概率。

对人员安全的管理具体包括：

人员录用、离岗：录用时对拟录用人员进行专业技能考核并签订保密协议及责任协议。离职后严格办理调离手续。

安全意识教育和培训：根据岗位制定培训计划，并进行技能考核。

外部人员访问管理：外部人员应先提出书面申请，批准后有专人全程陪同监督。

● 系统建设管理

工控系统的安全管理贯穿系统的整个生命周期，系统建设管理主

要关注的是生命周期中的前三个阶段（即，初始、采购、实施）中各项安全管理活动。

系统建设管理分别从工程实施建设前、建设过程以及建设完毕交付等三方面考虑，具体包括：

产品采购和使用：拟选产品无比符合国家相关规定。对所选产品定期审定并更新候选产品名单。

自行软件开发：拟定详细的开发管理制度，说明开发过程的控制方法及人员行为。对软件设计的相关文档和使用指南进行控制。

外包软件开发：存储备份开发单位提供的软件源代码并审查软件中可能存在的各种问题。

还有工程实施、测试验收、系统交付、系统备案和安全服务商选择等。对建设过程的各项活动都要求进行制度化规范，按照制度要求进行活动的开展。对建设前的安全方案提出体系化要求，并加强了对其的论证工作。

● **系统运维管理**

根据基本要求进行信息系统日常运行维护管理，利用管理制度以及安全管理中心进行，主要包括：

环境管理：根据资产的重要程度采取对应的管理措施。

资产管理：编制保护对象资产清单，根据资产价值选择对应的管理措施。

介质管理、设备管理、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理等。使系统始终处于等保要求的安全状态中。

1.1.3 下一步实施计划

油库工控安全建设是一项涉及面广、影响大、安全运行要求高，

集数据处理、信息发布、资源整合于一体的信息化方案。为了更好的执行该方案，将采取统一指挥、并行实施、协调合作的实施办法，构建一套油库信息安全服务平台，逐级提升的油库工控安全防护体系。

油库信息安全服务平台是专注于工业环境的网络安全智能分析运营平台。平台全面采集各类工控流量及日志信息，通过内置的大数据安全分析模型整合零散的工业安全数据，深入挖掘安全风险与攻击事件，实现工业网络空间安全风险的预知。平台采用威胁发现、智能研判和自动化响应处置的闭环安全管理体系，有效提高安全运维工作效率，帮助油库实现智能安全运营，具体功能架构图如下：

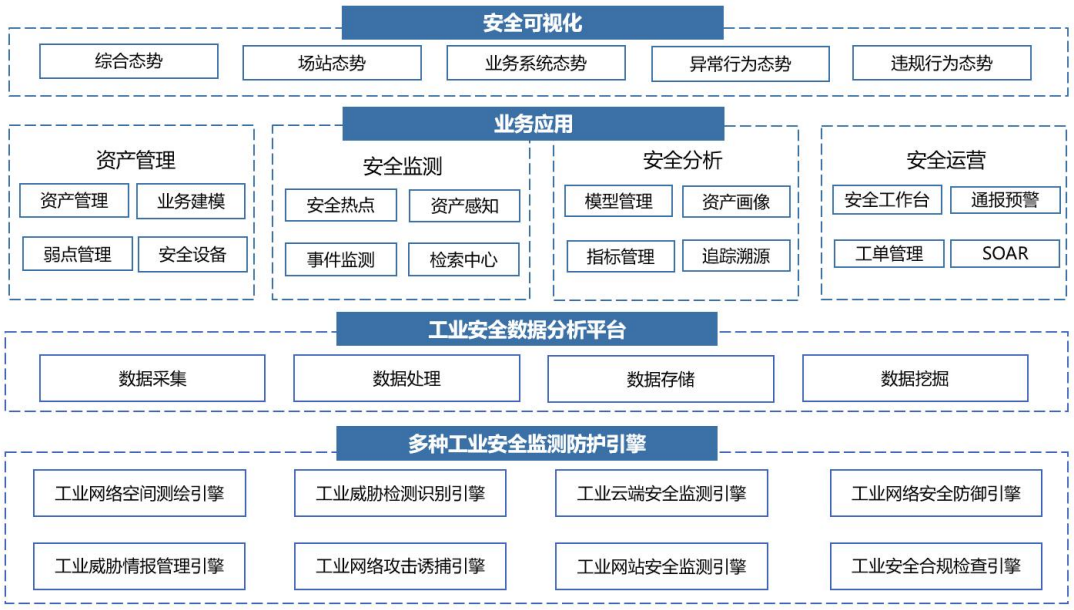

图 10-10 油库信息安全服务平台功能架构图

采用 8+1+4 的架构，即八大工业安全引擎、一个工业安全数据分析平台和四大业务应用模型。

■ 八大工业安全引擎

主要负责采集各类工控网环境的安全数据，包括工业网络空间测绘数据、工业威胁检测数据、工业云安全监测数据、工业网络安全防御、工业威胁情报数据、工业网络攻击诱捕数据、工业网站安全数据、工业线下安全检测数据，数据覆盖线上、线上采集。

■ 工业安全数据分析平台

提供数据采集治理、威胁情报碰撞、大数据智能分析、工业威胁建模。

■ 四大业务应用

在数据中台的服务能力基础上，以安全监测、安全分析、安全运营和资产管理四大业务应用为核心，为用户建立工业安全运营闭环管理体系。

1.数据采集方案设计

（1）多元异构日志采集

支持目前包括但不限于主流安全设备、网络设备、主机、数据库、中间件、应用系统和虚拟化系统等；

支持常见的虚拟机环境日志收集，包括 Xen、VMWare、Hyper-V 等

可以通过自定义配置将用户不关心的日志过滤掉；

支持对收集到的重复的日志进行自动的聚合归并，减少日志量；

支持将收集到的日志转发，当原始日志设备无法设置多个日志服务器时，可以通过本系统的日志转发功能将日志转发到其他日志存储设备。

为适配各种采集数据源，需要支持多种采集协议，以实现对各类数据的采集，包括不限于安全对象属性、运行状态、安全事件、评估与检测等数据。为实现对包括安全对象的属性、运行状态、安全事件、评估与检测等数据的采集，针对不同类型的数据以及对应的适配协议

每个数据采集引擎支持配置不同的采集策略，保证每个数据采集引擎有针对性的采集数据，如动态配置采集周期，清洗过滤策略等。需满足如下采集部署要求。

➢ 支持分布式多节点部署；

➢ 支持多采集节点存活、健康状态监控，发现节点异常后，及时告警；

➢ 支持对采集节点性能监控，保证采集性能与数据量匹配，防止数据丢失。

➢ 采集策略管理。支持对设备的采集策略的管理，包括采集频率、采集协议、采集目标、过滤策略等。

➢ 支持流量数据镜像采集的方式。支持在多个机房的交换机上复制镜像，分布式部署分光器和 DPI 的方式采集，并将多余的接口关闭；

➢ 支持主机终端的数据采集，支持数据库审计分析的数据采集；

➢ 支持数据汇聚。综合考虑专网传输性能的基础上，需满足将多个机房采集到的数据传输汇聚。

（2）全流量数据采集

面对全流量威胁进行识别，并通过双向流量检测对网络流量行为（例如数据报文恶意特征匹配、资源使用情况、使用者的访问行为等）判定，识别出病毒、木马、敏感信息等异常行为。

➢ 威胁行为分析

组件根据数据包特征和流量行为对流量进行深度解析，通过对数据流中威胁行为识别，达到恶意流量检测的目的。

通过流量深度解析，系统异常、网络木马、异常端口访问、网络扫描、DoS、通用协议命令解码、WEB 应用漏洞利用及程序攻击、恶意文件及病毒攻击、异常威胁、异常用户名登录请求、可疑执行代码等非正常和非 RFC 遵从的请求行为以风险级别实时呈现，为威胁风险分析和管理提供依据。

➢ 威胁行为识别

通过以下几个方面对威胁行为进行识别：

基于4000+条规则库进行特征匹配；

根据资源使用状况或者使用者访问行为进行识别；

基于异常检测技术识别威胁行为，例如病毒、木马、攻击等；

通过索引实时查询页面告警信息。

➢ 合规行为检测

通过以下多个角度对违规违法行为检测：

信息泄露：通过漏洞利用窃取用户信息。

不良信息内容：实现对不适宜信息内容检测审计。

敏感信息过滤：实现对身份信息、关键字、数据源等的自定义，实时

掌握流量中的敏感信息定位，实现对不合规行为有效监测。

隐私权侵害：通过策略获取信息系统内部系统访问权限，侵犯数据隐

私。

（3）资产信息探测采集

除了基于流量被动发现存货资产，工业安全数据分析平台可以与远程安全评估相结合，通过主动扫描的方式发现系统内存在的信息资产。

资产发现功能可对网络中所有在线设备进行自主网络扫描和深入识别，获取资产的网络地址、系统网络指纹、系统开放端口和服务指纹，并根据积累和运营的指纹库裁定每个资产的类型、操作系统、厂商信息等。其具体功能需要满足以下要求：

➢ 支持定时任务，用户可自定义任务开始的日期和时间

➢ 系统可采用主动探测的方式，对网络中在线设备的发现和识别，

能够识别到存活设备；

➢ 系统可实现资产详情信息的采集和定义，包括资产名称、所属系统、IP 地址、分组、厂家、型号、操作系统类型等；

➢ 系统需能够实现资产服务信息的采集，包括资产服务的 IP 地址、端口号、服务名、服务版本、协议等服务属性进行管理；

➢ 系统需要能够支持指纹库的管理，并能进行指纹的自定义；

➢ 可识别、定义网络中所有资产。

（4）漏洞信息探测采集

漏洞检测功能需要支持主动的系统、应用层、中间件、数据库漏洞检测，漏洞库具备实时更新和自定义功能；可检测主流 windows、Linux、国产操作系统漏洞；内置通用性弱口令字典，并可增加自定义字典。

本次系统的漏洞检测发现功能设计，基于安全自主研发的漏扫引擎，通过深度扫描、漏洞检测、木马检测、逻辑漏洞检测等方式对扫描对象进行全面的探测与检查，以脆弱性和漏洞为导向，以安全风险管理为基础，对资产进行深度遍历。支持主流的漏洞。

采用强大的过滤模块，过滤掉重复或者不必要的网页链接，提高运行效率。单引擎单位时间的发包速率的可控化，可以有效防止扫描数据量过大影响系统正常运行的问题。 扫描数据实时存储，扫描过程中实时存储扫描数据和结果，不管是由于程序自身引擎中断、进程人为关闭，还是机器断电引起扫描中断，扫描数据都不会丢失，可以进行断点续扫。系统具体功能模块实现页面如下所示。

系统内置可更新的漏洞知识库模块，对扫描出来的漏洞提供详细的解决方案参考。

提供接口可以导入第三方漏洞扫描结果。

2.详细功能设计

（1）工业数据采集处理

数据采集模块以协议/接口采集为主，Agent 收集为辅。针对不能通过协议采集或接口转发数据的必要采集对象，采用安装 Agent 的方式进行数据采集。

系统支持的数据采集方式如下：

➢ 协议/接口采集：支持采集节点通过 Syslog、Kafka、Ftp/Sftp、Webservice、SNMP、File、JDBC/ODBC 等方式；

➢ Agent 采集：Agent 支持 Windows、Linux、Unix 等系 统的数据收集。

系统支持采集的数据源类型如下：

➢ 网络系统全量数据：工业网络流量、工业日志数据、工业资产信息、组

织架构、安全域、人员、账号等以及第三方相关数据；

➢ 威胁情报：恶意 IP、恶意域名、邮箱和文件 Hash 值等；

工控网环境复杂，采集所得原始数据有一部分是非结构化数据，需要将这部分非结构化的原始日志处理转换为结构化数据。系统提供了一个链式可插拔的数据 ETL 模块，以插件的形式实现各种原始日志的格式化流程。

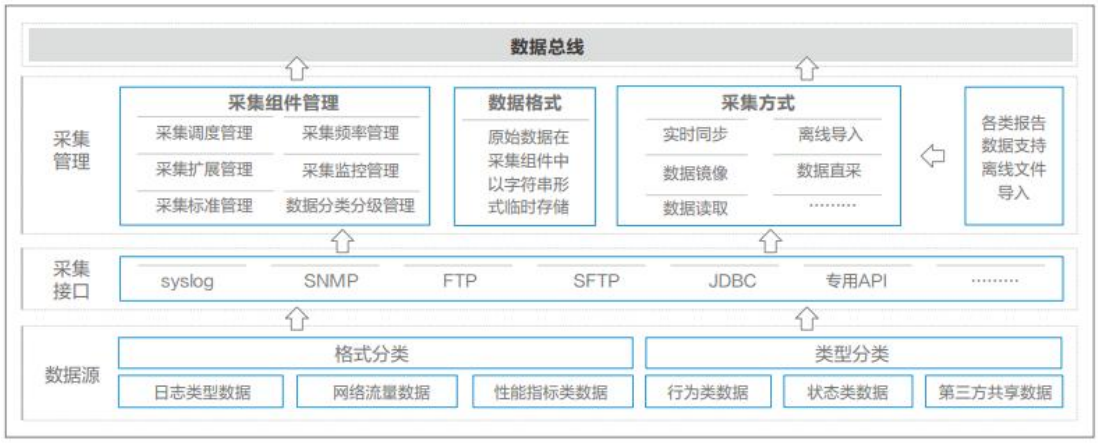

图 10-11　详细功能图

（2）分布式存储

分布式存储技术能够实现结构化及半结构化数据的统一存储，兼容传统的关系型数据库以及 SQL 访问模型，同时支持对海量数据的在线实时流式处理框架和离线分布式计算框架。分布式数据库面向时序数据和小文件数据存储进行深度优化，支持第三方存储引擎和传统关系型数据库的无缝接入；支持海量混合数据的统一存储管理和在线离线一体化查询；支持可插拔安全算法模块和主流分布式计算框架；支持跨库、跨源、异构数据库之间的跨库访问和关联查询，解决了多系统交互时对海量混合数据统一管控的问题；支持多源异构混搭数据间基于规则导向的高可靠近实时数据同步。主要功能包括：

➢ 大数据采集存储和分析处理

满足采集海量数据储存需要，如流量信息、设备状态、链路状态等，满足大规模结构化流式数据的并发能力、吞吐量、低时延的高要求。

➢ 分层架构、模块化设计、多场景支持

采用模块化的设计思路，在数据访问层、数据路由层和数据存储层都提供多种高内聚、低耦合的模块，通过这些模块的灵活搭配，分布式数据库表现出不同的技术特征，从而能够适应不同的业务场景。

➢ 在线检索和离线分析一体化

通过配置，分布式数据库可同时支持高速数据写入，在线交互访问、实时查询以及高并发大数据集查询在内的各种访问方式，适应在线检索和离线分析等不同业务场景。

➢ 混合数据支持

分布式数据库支持与传统关系型数据库 Oracle、MySQL 等联合访问。业务系统可以把部分表建在 Oracle 或 MySQL 上，把部分表建在

分布式数据库上，然后透明地访问这些表，包括在这些表之间进行join、union等操作。

➢ 跨域、多数据中心支持

分布式数据库在保证数据一致性的前提下支持多数据中心或多数据集群之间近实时的跨域数据同步复制，实现系统的跨域多中心部署模式。总体处理性能，数据读写、扫描等，随集群规模扩展线性增长。

➢ 分布式存储

分布式存储技术用于系统架构的大数据组件当中，使系统能够实现高效的数据采集和检索能力。

主要基于通用/定制化的服务器提供存储，可提供对象、文件和块存储，具备低成本、灵活扩容、高并发访问等优势，通过软件保障性能和可靠性。可作为资源池的分级存储手段，满足中低端存储、数据归档备份、大数据存储等需求。采用分布式块存储软件技术的Server-SAN在I/O能力、部署速度和扩展性方面已验证优于传统块存储技术。

（3）全文检索

全文检索技术是态势感知系统的核心基础功能，其基础要求是根据搜索条件快速、准确的匹配命中数据对象，为安全分析人员提供高效准确的分析工具，以便能更加快速的发现安全风险。因为大数据系统往往采用分布式存储技术，所以全文检索技术的选择必须能够支持主流的分布式存储系统。同时，分布式并行计算系统的支持也是在技术路线选择中必须考虑的因素，需能够做到对并行计算框架的无缝对接。由于需要具备对数据搜索准度、实时性与多样性的要求，这就要求检索技术需支持基于关键词，数值范围，日期范围等各种复杂的搜

索功能。

全文检索技术采用倒排索引的结构达到快速全文检索的目的，倒排检索是实现“单词”-“文档矩阵”的一种具体存储形式，通过倒排索引可以更加快速的获取包含这个单词的文档列表，倒排索引主要由两个部分组成“单词词典”和“倒排文件”，具体结构如下图：

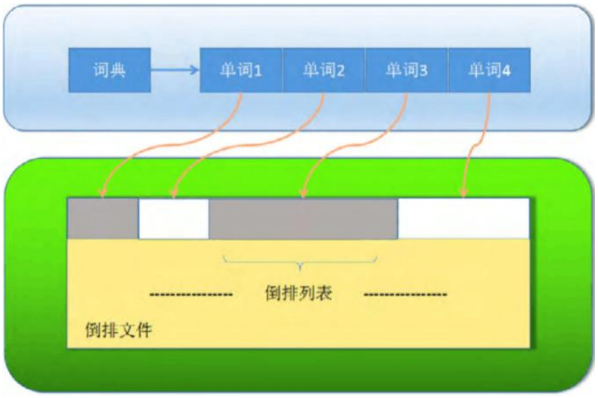

图 10-12　全文检索技术架构图

全文检索技术运用在安全监测中，主要用于对监测数据的检索查询，通过查询安全分析人员能够实现对安全事件的细致分析，并将有效数据运用于模型建立当中。

（4）威胁潜伏检测

平台利用认知攻击循环模型（侦查渗透、驻留控制、执行渗透或横向移动）和 ATT&CK 安全模型，通过对安全大数据中心（SDC）汇聚的网络数据包、文件元数据、终端日志、威胁情报、沙箱报告、漏洞知识库等进行智能分析，重建攻击全路径，洞悉发动攻击的人员、目标、时间、地点和手段，发现高级潜伏威胁。

（5）工业安全实时分析

在工业场景中，对数据的实时性要求很高，数据的价值随着时间的流逝而降低。工业安全监测分析能够对正在发生的事件进行实时分析，及时发现最可疑的安全威胁。

➢ 预置工业威胁模型

结合 IT 与 OT 应用场景，内置了 1300 多种安全分析模型，包括 180 多种扫描探查检测类模型、740 多种渗透攻击检测类模型、20 多种获取权限检测类模型、210 多种命令控制检测类模型和 30 多种资产破坏类检测模型，覆盖 Intrusion Kill Chain 的各个维度。

➢ 自定义工业安全分析模型

在工控网络中，用户对安全生产的要求是非常高的，要确保整个工控网络的稳定性和可靠性，利用自定义工业安全分析模型，可根据用户实际业务场景，将安全生产指标与网络安全指标进行融合分析，从中发现威胁与风险，并进行有效的处置。当前支持五大自定义安全分析模型，主要包括规则模型、统计模型、情报模型、关联模型和 AI 模型等。

➢ 威胁情报碰撞

平台集成海量的威胁情报数据。情报来源包括国内外 200 余家威胁情报交换数据。采用云沙箱、机器学习识别与专家分析等方式，提炼形成面向政企用户网络安全的高质量威胁情报中心。为用户提供如下核心情报功能：

情报收集（内部+外部各类情报源）

多源情报关联分析

情报检索验证与攻击溯源

情报更新维护

关联下游产品

（6）工业场景实体行为分析

在工业控制场景下，用户的操作可达到指令级，每个指令是否正常都意味着能否持续进行安全生产。通过对实识设备、用户、工业通信指令进行智能 AI 学习或进行基线设置，构建出用户在不同场景中

的基线状态。及时发现用户、系统和设备存在的可疑行为，解决海量日志里快速定位安全事件的难题。

该系统亮点如下：

➢ 快速发现异常用户行为

采用专用的用户行为分析算法，能够快速发现异常用户行为，包括历史未出现过的异常行为。

➢ 精准的用户异常行为监测

利用网络分析的方法，把看似不相关的用户和行为关联起来，从而提高异常行为监测的准确度和灵敏度，并通过多维态势可视化系统能够实时展现总体用户行为威胁状况。

➢ 定制化用户画像能力

由于用户行为随实际网络环境的不同存在较大差异性，平台支持根据用户实际业务场景定制行为分析画像，确保分析结果真实可靠。

图 10-13　定制行为分析

（7）资产管理

➢ 资产管理

资产管理作为态势感知的最基础功能，确定了安全管理的对象和目标，将所有业务系统的网络设备、工控设备、安全设备、服务器及其之上承载的操作系统、数据库、应用系统、接口方式、硬件属性、使用维护人员等信息均作为资产管理的内容，提供资产录入、管理、变更等管理功能。可通过流量监控开放端口、主动外连行为等。资产管理主要提供如下功能：

提供与第三方资源管理系统的接口以实现资源共享、同步更新、信息的查询和导入等功能。同时内置资产通用属性接口，用于实现与第三方资产管理系统的数据格式相互转换；

资产管理模块中各项资产的属性值将参与到安全事件管理、脆弱性管理、风险管理、拓扑视图、报表系统等其它安全管理模块；

提供资产的手动和自动发现，资产接入或者移除，能够自动更新，并作出提示，对新接入资产进行预管理，对移除资产进行记录管理；

将安全事件与资产进行绑定关联，实现以资产视角的安全事件管理，在资产拓扑视图上直接展现安全事件的信息，支持钻取溯源等安全处置功能；

提供根据客户组织架构或者网络架构进行资产域/安全域划分，方便运维。

资产管理的信息和维度包含如下：

基本信息：资产 IP、资产名称、资产重要性（普通、重要），资产标签、资产类型

更多信息：资产编号、资产状态、组织架构、使用人、C-机密性、I-完整性、A-可用性、是否等保资产、地理位置、描述等。

操作系统信息：操作系统、OS 版本、MAC 地址

设备管理：设备厂商、设备型号、设备版本、设备存放地址、管

理地址、日志量监控、在线状态检测。

➢ 安全设备管理

安全设备管理确定了本平台对接、联动和监控的安全设备目录，以及安全设备关联的防护资产信息，管理整个网络信息系统和业务资产的防护状态和安全建设系统。

安全设备编辑。提供安全设备的增加、编辑、删除功能。安全设备的管理信息包括设备名称、设备类型、设备厂商、关联资产等。

安全设备监控。提供包括安全设备拦截状态和安全设备运行状态监控，可跳转投屏。

➢ 区域管理

区域管理模块是根据企业网络环境、组织架构以及安全域分布实现资产/业务拓扑视图，并能够在资产视图上将弱点爆发的安全事件所属网络区域或业务系统分组予以展示。

安全域添加。根据企业的网络划分情报、组织架构等情况，进行安全域添加；

安全域修改。

安全域删除。

内部 IP 配置。对内部 IP 地址进行配置，解决企业网络内外网地址私用等情况。

➢ 业务建模

实现以业务资产视角，辅助客户以资产为核心的工作层面之上构建一个面向业务部门和管理层的业务资产模型。该功能主要管理用户的业务支撑系统，为用户提供业务的实时监控能力，保障用户业务的可持续平稳运行。为用户提供如下功能；

支持资产的自动发现和从客户现有的资产平台同步功能，支持资

产的修改、删除等管理功能，并根据客户资产的用途和网站结构进行划分，至少分为内部资产、互联网资产和重点安全资产；

提供安全资产拓扑视图，支持根据网络架构自定义资产拓扑，支持拓扑的模板导入和编辑好的资产拓扑文件导出；

用户可以根据具体的业务流程构建相应的业务模型，支持业务模型的管理功能。

图 10-14　业务建模

➢ 弱点管理

弱点管理是以资产和漏洞为视角，结合内部管理制度和流程，实现资产弱点的全生命周期管理的资产弱点综合性管理，通过标准化引擎，支持将扫描器扫描发现漏洞、安全服务人工渗透漏洞、内部运维人员运维发现漏洞、互联网公布漏洞等不同的漏洞进行自动化收集或人工录入、导入方式收集，将形式格式不一的漏洞进行标准化。同时，通过内部资产清单导入、扫描探测发现、人工录入、对接 CMDB 配置库等方式梳理企业资产。再通过自动化关联引擎，实现资产、弱点、业务系统、资产责任人的关联，形成资产维度的脆弱性视角。在此基础上，进一步结合企业的管理制度和流程，通过平台内置工单或对接企业内部工单系统，实现资产、漏洞的全生命周期管理，以辅助企业实现安全建设管理及决策。

图 10-15　弱点管理

（8）安全监测

➢ 态势感知

态势感知以单位数据、资产数据、网络安全事件与威胁风险监测为驱动，基于多维态势可视化技术，对网络空间安全相关信息进行汇聚融合，从不同视角出发感知网络安全态势。

综合态势：综合态势全面采集各类工控流量和日志信息，通过内置的大数据安全分析模型整合零散的工业安全数据，深入挖掘安全风险与攻击事件，可感可控工业系统安全，实现工控网安全态势的全面感知。

图 10-16　综合态势

场站态势：场站态势以各场站实际网络应用场景为底图，为用户建立可视的场站安全态势感知，通过绘制场站网络结构拓扑，标记关键资产和业务系统，及时发现场站发生的关键事件，达到快速处置目的。

图 10-17　场站态势

业务系统态势：业务系统态势以业务安全感知为唯度，监测各场站关键业务系统的在线运行状况，掌握各场站业务系统网络安全状态，如各业务系统流量，各业务系统威胁排行、发生安全事件排行、趋势等信息，及时发现关键业务系统的安全态势。

图 10-18　业务系统太少

异常行为态势：异常行为态势主要关注在场站内发现的异常流量行为，将不符合安全基线的行为记录并进行展现，主要包括工控异常行为、工控高危操作行为、无流量行为，不合规行为等。

图 10-19　异常行为态势

横向威胁态势：横向威胁感知主要关注企业内部资产之间的违规操作和病毒传播，实时监控跨安全域的访问行为和业务访问情况，通过自由布局和圆形布局观测资产之前的威胁关系，及时发现并处置违规资产对企业环境内部造成的破坏。

图 10-19　横向威胁态势

违规行为态势：违规行为态势主要关注来自各场站不同安全区是否存在跨区访问的情况，及时发现哪些资产主动外联，哪些资产经常被跨区访问，跨区外联的场站及所属安全区，以及这些违规外联访问是否发生安全事件。

图 10-20　违规行为态势

攻击者追踪溯源态势：攻击者追踪溯源可视化分析大屏，为安全运维人员提供包括攻击行为分析、团伙分析、攻击取证信息、攻击趋势、攻击手段，攻击影响范围等信息，支持任意攻击者信息查询，可生成详细的攻击者溯源报告，并能够一键导出报告。

图 10-21　攻击者追踪溯源态势

资产威胁溯源态势：资产威胁溯源可视化分析大屏，为安全运维人员提供包括被攻击行为分析、影响资产范围分析、攻击取证信息等，支持任意资产查询，可呈现被访问趋势、被攻击趋势、被攻击手段、资产状态，资产评分等信息。

➢ 资产感知

以资产为核心视角，直观了解自身网络环境中存在风险资产。资产感知通过攻击链形式展示，剖析从扫描探查阶段到资产破坏阶段资产失陷过程。感知失陷、异常资产，从海量的日志中提取有价值的资产溯源路线。平台简单易用，支持一键全方面钻取，降低运维成本，提高运维效率。

风险资产视图：以资产被攻击的维度展示网络内的安全风险，包括已失陷、高风险、低风险三种维度；

安全域风险视图：以资产安全域的维度展示网络内的安全风险，可根据安全域进行钻取处理事件；

风险资产列表：为用户列出正在遭受高级风险的资产列表，方便快速处置。

业务系统视图：以业务系统被攻击的维度展示网络内的安全风险，可根根业务系统进行钻取处理事件。

生产大区视图：以生产大区被攻击的维度展示网络内的安全风险，可根根业务系统进行钻取处理事件。

管理大区视图：以生产大区被攻击的维度展示网络内的安全风险，可根根业务系统进行钻取处理事件。

➢ 事件感知

事件感知可以通过搜索、聚合、关联等调查取证手段，提供攻击事件数据包、攻击者设备指纹等举证信息。平台支持基于源、目的、事件名、攻击意图等多种聚合调查方式，从不同维度聚合统计安全事件。可以关联资产信息、威胁情报、弱点详情、安全事件、处置方式等多维数据进行调查取证。同时提供场景化的事件感知能力，如安全基线事件分析、网络攻击分析等。

➢ 安全热点

安全热点是结合用户实际需求，将用户关心的安全热点问题进行自定义设置，用户可选择内置安全事件作为安全热点，也可以通过自定义威胁模型定义安全事件后再设置成安全热点。安全热点可帮助用户快速排查重点问题，发现最重要的事件，发起快速处置。

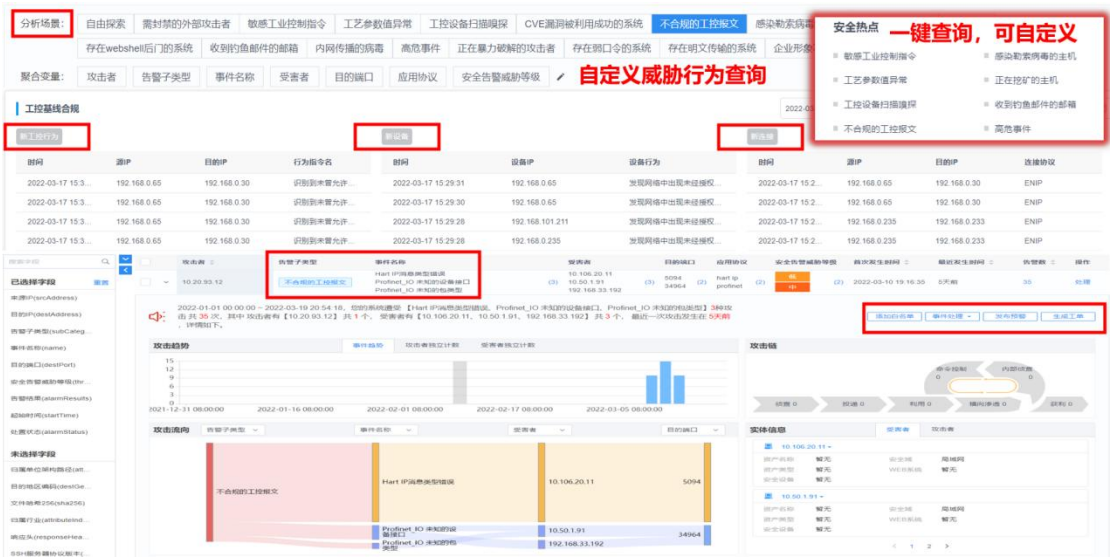

图 10-22　安全热点

（9）安全分析

➢ 威胁模型

提供集中的安全规则、模型以及策略的管理功能，制订统一的安全策略，并有效贯彻执行这些安全策略，不仅有助于提高安全水平，而且将这些安全策略进行上网发布也有助于知识的共享，让各级安全管理人员合理运用安全策略，有效地管理网络，保障网络的安全运行。因此，安全策略管理模块将负责全网的基本网络安全策略模板的制订，并将安全策略转换为可执行的脚本，便于安全策略的有效执行和快速部署。

图 10-23　威胁模型

应用层面设计策略管理模块，支持策略的维护、启停、编辑、新增等功能，并具备策略规则库字典的维护管理功能。具体如下：

提供对事件过滤规则进行编辑功能，可自定义过滤规则，归并事件告警，避免产生告警风暴；

关联规则匹配条件支持运算符、支持引用外部资源包括过滤器、资产属性、自定义资源、已有规则、黑白名单。触发条件支持对各不同字段的计数。支持预定义包括时间、地址、端口等在内的资源，可在规则定义中直接引用已定义的资源；

支持列表显示分析规则，显示内容包括规则名称、类型、类别、启用状态、规则创建时间、修改时间、规则触发后告警等。

模型构建和管理

设计便捷的拖拽式安全建模能力，可支持包括规则建模、安全事件关联、安全事件统计、威胁情报关联以及 AI 学习建模等安全威胁建模功能。

规则建模。为用户提供一个规则建模平台，可支持根据客户的网络安全状况、业务状况以及用户行为等构建分析规则能力；

关联建模。为用户提供一个关联建模平台，可将多个安全事件进行字段管理安、逻辑关联发现相关事件中隐藏的高级威胁及安全风险；

统计建模。支持用户对安全事件、安全行为以及安全威胁等特征进行统计分析，从网络信息中发现重要的安全威胁统计型特征；

情报关联。通过安全威胁分析与预警平台和威胁情报的集成，实现全网的基于威胁情报的协同联动，为用户发现精准的情报事件，做到防范于未然；

AI 学习建模。为用户提供一个内置大量集群学习算法，包含时序算法、分类算法、聚类算法等多种算法原型，为用户提供针对任意数据的学习分析能力，输出高级安全威胁和未知威胁等。

➢ 追踪溯源

平台能实现基于资产安全告警和攻击者的追踪溯源功能，结合先进的大数据关联技术能够实现对安全告警事件和攻击者的追踪与取证，并提供溯源报表的一键智能下载。

图 10-24　追踪溯源

告警溯源：能够对告警事件实现闭环式溯源，并提供对告警事件原始日志的查询服务。

攻击者追踪溯源：提供攻击者追踪溯源大屏，基于大数据关联分

析技术，聚合展现疑似黑客组织 IP 组、攻击引发告警类型以及类似攻击行为手段，可基于时间轴动态查看攻击行为取证列表，实现对攻击者的精准追踪溯源。

资产威胁溯源：提供资产威胁溯源可视化分析大屏，为安全运维人员聚合呈现资产被攻击行为、影响资产范围、告警取证信息等，支持针对网内任意资产查询并呈现被访问趋势、被攻击趋势、被攻击手段、资产健康状态，资产评分等信息。

➢ 资产画像

工业资产画像以采集到的各种数据为依据，通过安全建模分析，提供可视化工业资产画像，主要包括：资产基本信息、风险信息、访问关系、行为画像、服务端口、访问端口、脆弱性等。

工业资产画像可以快速分析重点资产的安全防护效果与威胁情况，为资产风险评估、安全加固和安全保护建设提供依据。

图 10-25　资产画像

➢ 日志检索

平台的日志搜索入口，提供关键字组合输入功能，实现日志快速检索，包含原始日志搜索、标准化日志搜索、自定义搜索模板和历史搜索快照。提供如下检索功能：

支持任意关键字、参数、和正则表达式进行过滤查询；并提供检索关键字排除功能；

支持可指定多个查询条件进行组合查询；可通过关键字、条件表达式、时间范围对事件及数据进行快速检索，快速定位到安全分析人员关注的威胁和上下文数据，并支持检索趋势统计；

支持以时间轴的方式展示检索结果，并支持时间轴钻取和追加搜索；

支持对检索结果追加检索，支持点击检索结果字段快速加入到检索条件；

支持对展示字段灵活定义，允许用户选择特定的字段显示；

支持将查询的条件存储为查询模版，方便再次使用；

支持检索结果导出（不少于 10000 条），至少支持 excel 或 CSV 格式。

具备如下日志分类检索功能，智能检索满足基本要求外，还提供以下特定功能：

原始日志检索：支持选择日志源进行检索；

安全告警检索：支持根据安全事件的处置状态、威胁等级、攻击意图、所处攻击链阶段等多个维度进行检索；支持检索结果进行处理，处理状态标签包括：未处理、处理中、处理完成、误报等；

安全事件检索：支持根据安全事件威胁等级、攻击意图、所处攻击链阶段等多个维度进行检索。

图 10-26　日志检索

（10）安全运营

➢ 通报预警

为用户提供预警和通报功能，用户对平台产生的安全告警进行新增预警，提示平台用户该告警可能存在一定风险隐患。

预警。提供用户/组织维度的安全风险预警，可选择特定的用户或组织进行下发 预警，可设置预警级别、标签等。针对未通报的事件，将根据事件信息，利用系统配置好的日常通报模板生成通报文件。

通报。提供全局维度的安全分析通报，按照预警名称的维度对公开预警进行查询的功能，并可根据指定的查询条件，快速定位需要重点关注的公开预警。

➢ 工单管理

提供工单管理视图，可以通过工单管理界面新增工单、通报详情页面新增工单、安全告警页面新增工单，并将工单指派给相应的处理人，经过各个环节的处理，工单记录状态未处理/处理中/已解决/已关闭，便于监督工单是否及时处理以及闭环。提供包括工单查询、工单新增、工单处置、工单删除、工单跟着以及工单批量操作等功能。

➢ 安全评价

安全评价实现对被考核对象的安全合规评价和工业网络安全状态的整体评价，支持按天、周、月、季度、半年、年度进行安全评定。安全评价有别于综治考核,综治考核为一年一次,有严格的计分标准。

➢ 订阅管理

提供安全事件、工单等消息的订阅功能，可将具备安全工单/消息推送给制定的人员。提供预警、工单、短信和邮件 4 种推送方式，当安全告警满足订阅规则时，平台对订阅规则通知人自动生成预警/工单、发送邮件/短信，让用户可以实时关注到平台告警情况。

➢ 安全工作台

为运维人员提供安全事件处置工作界面，包括工单管理、通报情况、最新安全动态等视图，并为用户提供代办工单状态工作台，方便用户快速进行需要处理的安全工单。

1.1.4 方案创新点和实施效果

1. 方案先进性及创新点

本方案在实施过程中,为了有效解决新场景新业务带来的新安全问题，创新的采用了一些新技术，主要体现在下面的几个方面：

（1）采用运行拓扑(topology)的 strom 架构

目前技术上一般提供 Hadoop 架构对大规模数据的计算进行分解，然后交由众多的计算节点分别完成，再统一汇总计算结果。Hadoop 架构通常的使用方式为批量收集输入数据,批量计算，然后批量吐出计算结果。然而在安全大数据分析的应用场景下,通常对告警的实时性要求较高，需要对海量的原始数据进行实时流式处理和持续处理，Hadoop 架构难以处理实时性要求较高的业务。针对这一难题，本方案采用运行拓扑(topology)的 strom 架构,极大的降低了安全事件的告警延迟。

Storm 集群提供控制节点(master node)和工作节点(worker node)。控制节点上面运行一个叫 Nimbus 后台程序，负责在集群里面分发代码，分配计算任务和监控状态。每一个工作节点上面运行一个 Supervisor 的进程，监听分配给它那台机器的工作，根据需要启动/关闭工作进程 worker，多个工作进程 worker 组成拓扑(topology)。

工作进程 worker 中每一个 spout/bolt（数据处理单元）的线程称为一个 task（任务），使用 Spout/Bolt 编程模型来对消息进行流式处理。Spout 组件是消息生产者，支持从多种异构数据源读取数据，并发射消息流，Bolt 组件负责接收 Spout 组件发射的信息流，并完成具体的处理逻辑。在复杂的业务逻辑中可以串联多个 Bolt 组件，在每个 Bolt 组件中编写各自不同的功能，从而实现整体的处理逻辑，只需将不同的实时分析数据处理任务按照一定的规则和接口纳入和封装到 Bolt 组件中，就可以动态的实现实时分析功能的模块扩展。

（2）基于机器学习算法的异常行为检测创新

本方案创新地将机器学习算法、分析方法应用到对系统日志、网络流量、告警日志等安全数据的分析中，实现了对异常行为、恶意流量的有效识别。首先，根据工业互联网系统中用户及网络设备之间访问行为的业务特征，确定行为指标。其次，提取行为指标作为多维变量数据，然后利用无监督算法对数据进行聚类分析并进行标记，标记后的数据再交给有监督算法进行分析并产生分类规则。第三，联合有监督和无监督算法对行为日志进行分析，经过反复迭代有监督算法分析，逐渐将专家经验积累到分析算法中。日志、流量等数据经过上述算法的分析，可以准确发现工业互联网中的异常行为、恶意流量。

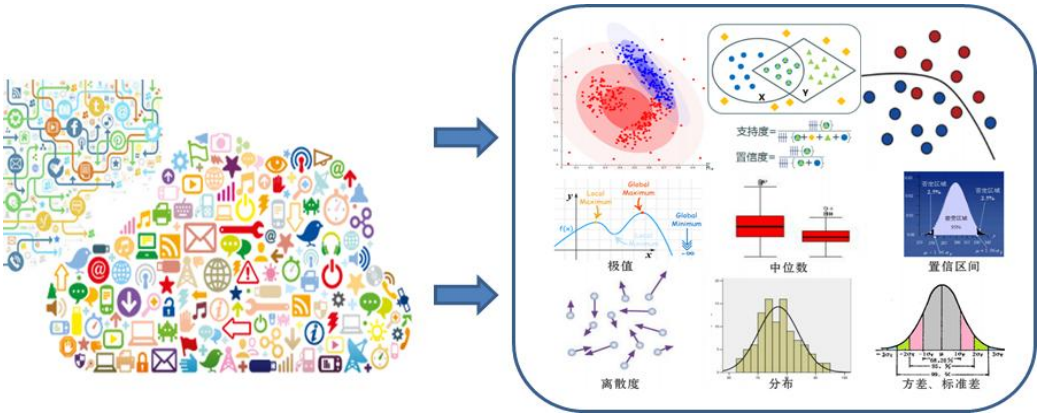

图 10-27　基于机器学习算法的异常行为检测原理图

（3）面向生产控制网络专有协议的深度数据包解析技术

解析工控网络专有协议的深度数据包，且能够对各类数据包进行快速有针对性的捕获与深度解析，同时满足生产系统在生产和制造过程中的通信效率保障和冗余机制等要求。

（4）基于智能机器学习的威胁感知技术

自动收集、分析和学习系统正常运行状态下的数据行为，智能提取用户节点的行为特征，并自动生成操作规则、白名单、配置规则等，实现自动化特征规则的提取和生成，对异常数据、操作行为、安全事件、安全隐患等进行告警及综合管理。

（5）基于 SOAR 的场景推理适度阻断技术

针对工业互联网安全领域安全事件频发，面对海量的工业互联网安全相关数据和告警，仅仅利用安全分析规则和粗放式的调用安全能力是远远不够的。在工业互联网网络攻击态势推理中，发现任何安全告警信号后，需要进行分拣、调查、核实、影响评估、取证、定级。利用多源异构数据进行自动化关联与推理，通过构建出网络安全知识图谱，提供跨越时间空间的强大有效的上下文环境，极大提升安全运维效率。

图 10-28　场景关联分析推理图

实现通过安全知识图谱驱动自动化响应。通过学习安全专家在安全事件响应中的处理，学习应对威胁的响应处置点、技术手段、流程，在安全知识库、漏洞库、处置案例库之间，构建这些知识间的联结，逐渐学习到如何设计纵深防御、组合防御等各种响应方案，学习阻断、隔离等不同策略，学习防火墙 ACL 列表、WAF 策略、SDN 流控制器等技术手段，学习扫描、POC 利用等检验评估过程和规则。

随着响应经验的持续积累，知识图谱会逐渐学习到安全事件、攻击、响应间的联结，自动化提出快速、有效的安全决策，自动化生成响应方案、推荐选择响应方案、最终实现自动化响应，实现网络威胁风险的智能推理可视化和适度阻断能力。

2. 实施效果

（1）划分安全域

横向安全域隔离，纵向边界防护，实现纵深防御工控网络与企业资源网的打通，导致网络安全风险增大，需要在两个网络间增加有效的安全隔离措施，保证两网融合后原有隔离网络的独立安全性，使其能应对各种未知信息安全风险，同时部署相应工控信息安全产品以实现横向安全区域间的隔离、生产数据单向采集及监控。

（2）部署工控信息安全产品

实现终端设备全天候防护油库生产运行中的终端设备应部署工控终端防护产品，及时更新版本，实现全天候病毒防护，产品可进行统一监控、策略下发、异常报警等，同时对移动存储介质使用进行管理，保障各工业现场主机能够有效抵御未知病毒、木马、恶意程序、非法入侵等对于终端的攻击。

（3）加强应用及数据的检测审计

实现异常告警两网融合后，数据横向和纵向交互增多，造成数据风险增大，需加强数据集成、数据上云和数据操作的机密性、完整性和可审计性，构建数据库审计系统，实现对数据实时、动态的监测审计，及时识别数据库的异常情况和风险行为并进行告警。

（4）建立主动防护机制

提升安全运营服务能力油库工控网络应具备主动防护功能，定期对业务系统进行漏洞扫描和安全检查，及时发现应用的安全漏洞及撞库攻击、暴力破解等恶意的攻击行为，提升漏洞发现、威胁感知、异常行为和异常流量的审计等安全运营服务能力。同时，需加强对油库资产、设备的集中管控和对运维人员身份认证、操作行为的统一管理，构建运维管理平台，提升油库运维管控能力。

（5）建立油库安全管理平台

实现统一安全运维管控，对分布在油库各网络中的安全防护设备进行有效的统一管理，实现各防护设备之间的互相支撑，密切协同，有机互动，从而充分发挥安全防护的作用。平台通过总体配置、调控，实现对油库各类安全设备的统一策略管理、监控、统一预警等；实现多种安全功能模块之间的互联互通，使得安全管理工作由繁变简，有效性得以提高，从而解决油库安全设备分散问题，实现统一安全管理。

（6）核心系统的安全防护

对于重要的业务系统（例如：付油系统、阀门联动系统）采用工业网闸专用的安全通道实现重要业务系统的信息交换，业务数据通过物理隔离、协议隔离、内容隔离等措施使其他业务系统的网络数据及有害数据信息无法进入该业务系统，保障了重要业务系统的相对安全。

（7）数据采集与共享

数据采集：油库工业控制系统环境复杂，由于一些系统比较落后，没有联网或者没有网络接口，通过工业网闸采集未联网设备（含串口总线设备），实现对未接入的数据采集，保证数据采集的全面性，为智能油库建设提供数据支撑。

数据共享：与第三方进行信息交互的场景，第三方网络通信链路连接到工业网闸外联口，通过工业网闸实现第三方网络与工控网络的安全隔离和信息的单向流动，可以在保障安全的情况下实现数据交换。

1.1.5 单位基本信息

杭州安恒信息技术股份有限公司（DBAPPSecurity），简称“安恒信息”，成立于2007年5月，是由“国家千人计划”获得者范渊先生创办的国家级高新技术企业，企业注册资金7407.4075万元。国内总部设在杭州高新区（滨江），并在北京、上海、广州、深圳、南京、成都、重庆、济南、西安、沈阳、武汉、福州、郑州、长春、内蒙等地设有分支机构。安恒信息主营业务涵盖云计算安全、大数据安全、应用安全、数据库安全、移动互联网安全、智慧城市安全等，包括安全态势感知、威胁情报分析、攻防实战培训、顶层设计、标准制定、课题和安全技术研究、产品研发、产品及服务综合解决方案提供等。安恒信息多次入选由美国著名网络安全风险投资公司（Cybersecurity Ventures）推出的 “全球网络安全企业500强”

榜单。

目前，企业正式员工4125名，其中研发团队人员1459名。公司设立有安全研究院和产品研发中心两大研发机构。安全研究院致力于前沿技术预研、创新业务探索和核心能力积累。研发中心主要由云事业群、AiLPHA大数据智能安全事业群、物联网+事业群、智慧城市事业群、基础安全事业群等多个子部门组成，除负责公司现有产品的迭代升级研发外，还覆盖云安全、移动安全，智能设备安全、大数据安全、工控安全等多个新兴领域产品的开发。

杭州安恒信息技术股份有限公司成立以来发展迅速，经营业绩快速攀升，各项业务指标持续快速增长。2020年，公司总资产达到260133.57万元，净资产达171463.85万元，营业收入129159.33万元，净利润12115.22万元。

作为国内网络信息安全领域的领导者之一，公司积极承担我国网络信息安全产业发展的社会责任。根据国家发改委正式发布的“2018年度国家地方联合工程研究中心”名单，安恒信息成为“大数据网络安全态势感知及智能防控技术国家地方联合工程研究中心”的依托单位，先后承担“国家发改委信息安全专项”、“工信部电子发展基金方案”、“科技部火炬计划方案”等国家级、省市级科技计划方案50余项。针对关键技术申请1490项专利（获得授权发明专利266项），拥有计算机软件著作权272项。参与制订信息安全类国家标准10余项，入选2020《中国网络安全能力100强》安恒信息荣获“领军者”称号。

2020年11月23日，安恒信息正式签约2022年杭州第19届亚运会，成为其网络安全类官方合作伙伴，这也是国际大型综合性赛事网络信息安全类最高层级合作，作为国家级重保核心单位，安恒信息先后参

与：2008 年北京奥运会、上海世博会、广州亚运会、历届世界互联网大会、G20 杭州峰会、厦门金砖、世界游泳锦标赛、武汉军运会等世界级重大活动的网络安全保障工作，并先后签约 2020 第六届亚沙滩运动会、2021 年成都大运会，以先进的理念和专业的服务获得各盛事主办方和监管机构的一致好评。