案例 1

公司名称：奇安信科技集团股份有限公司

主标题：基于数控机床场景的工控网络安全靶场建设

副标题：保障国家关键基础设施安全

引言：

奇安信科技集团股份有限公司（以下简称奇安信，股票代码 688561）成立于 2014 年，专注于网络空间安全市场，向政府、企业用户提供新一代企业级网络安全产品和服务，在人员规模、收入规模和产品覆盖度上均位居行业第一。2022 年 3 月 13 日，奇安信圆满完成了北京冬奥会和冬残奥会网络安全保障工作，兑现了北京冬奥网络安全“零事故”的承诺，为我国关键信息基础设施和重大活动的网络安全保障提供示范样本和有益经验。

随着数控系统在工控领域的广泛应用，逐渐成为国家关键基础设施和各类工业生产的核心组件。奇安信通过本项目的实施，构建工控安全攻防和工控安全渗透靶场环境，研究漏洞利用、恶意代码利用等技术，提高数控机床信息安全检测能力，助力数控机床的安全运行。

一、项目概况

1. 项目背景

随着信息和通信技术的高速发展，作为国家关键基础设施和各类工业生产核

心组件的数控系统面临越来越严重的安全威胁。当前国内外主流的安全防御思想已经逐渐由安全设备驱动、边界被动防御、已知威胁检测转变为海量数据驱动、多层纵深防护、未知威胁发现。大数据驱动下的异常发现、主动预警的安全监测响应体系正成为当前在隔离、加密等传统防护措施上的重要补充手段。APT 攻击、0day 漏洞等新型安全威胁会有针对性地绕开以预防为主的传统安全防御体系，在很长的时间内不易被发现，而内部人员出于各种目的的违规行为也是一个重要的安全事件根源。在新的形势下，被动防御体系面临越来越多的针对性问题，不同程度上限制了当前“互联网+”和中国智能制造战略、工业互联网等的技术发展和业务开展的灵活性。

由于数控系统在平台、系统和协议等方面的特殊性，现有的信息系统安全防护方法和工具很大程度上不能满足要求，亟需针对数控系统开展网络安全攻防能力建设，提高数控系统网络安全防护水平，满足工控侧对安全性、可靠性和稳定性的高要求。

2. 项目简介

基于数控机床场景的工控网络安全靶场具有攻防演练、渗透测试、漏洞挖掘、风险评估和检测预警等能力，实现基于数控系统场景的工控安全攻防靶场、工控安全渗透靶场的建设，主要包括：

（1）建设工控安全攻防靶场,采用工业漏洞扫描系统、工业漏洞挖掘系统等对数控系统进行全面的安全检测，探测发现数控系统中存在的安全漏洞，对漏洞进行危险性评估；此外，与安全建设相结合，部署工业防火墙、工业安全监测系统、工业主机安全防护系统等产品，验证防护方案有效性。

（2）建设工控安全渗透靶场，通过模拟恶意人员、黑客组织、敌对势力等不同强度的渗透活动，测试数控系统在渗透环境下的防护水平和安全短板；同时能够对渗透途径、漏洞利用、痕迹清除等渗透过程进行验证，从而提升数控系统的安全运行能力。

3. 项目目标

通过该靶场的落实实施，将虚拟化 IT/OT 网络与工业流程仿真模型相结合，建立工控系统网络安全攻防基础靶场环境，提供基于数控系统场景的安全可靠的演练、渗透和对抗等功能和服务，实现数控系统脆弱性检测，及时发现数控系统

网络威胁，实现工业企业网络安全攻防能力的整体提升。

二、项目实施概况

1. 项目总体架构和主要内容

基于数控系统场景的工控网络安全靶场以虚拟化、大规模网络仿真、渗透测试、漏洞扫描、数据采集分析、工业仿真等技术对数控系统中的网络架构、系统设备、业务流程、工艺状态、运行环境进行模拟仿真和复现，提供攻防演练、漏洞挖掘、风险评估、渗透测试、技术验证等服务的一体化靶场平台。

图 1：工控网络安全靶场平台

技术支撑层具备接入各类软硬件资源、网络仿真、可视化组网引擎等能力，为平台提供基础技术支撑；平台管理层通过对镜像、组件的接入，构建核心资源，提供对平台本身的运营管理支撑，包括用户管理、角色与权限管理等，同时提供应用层通用的资源库，如各类安全工具、知识库、数据采集工具等；平台应用层是根据工业企业典型使用场景和业务流程，支撑攻防演练、渗透测试、漏洞挖掘、风险评估和检测预警。

2. 具体应用场景和应用模式

(1)工控安全攻防靶场建设

依托工控网络安全靶场平台，构建工控安全攻防靶场环境。攻防演练是一项检验信息安全防护能力以及应急响应速度的信息安全服务。在靶场提供的可控演练环境内，集成网络安全攻防领域内漏洞扫描探针，使用专业的攻防手段，在完全可控的环境中构造网络攻防的真实场景并对其进行解析和分析呈现。工控安全攻防靶场支持两种演练类型：网络攻击和网络防御。

网络攻击场景架构如下：

图：工控安全攻防靶场——漏洞扫描架构

工控安全攻防靶场——漏洞扫描组件针对工控仿真环境中的控制器、伺服器和计算机集成制造网络中存在的常见漏洞、典型漏洞、0day 漏洞等进行扫描和检查，并利用大数据的分析技术对当前已发现的漏洞进行关联性分析，生产关联分析报告。

网络防御：工控安全靶场平台防御是通过接入该场景实施网络防御体系，包括但不限于边界防护类（工业网闸、工业防火墙）、检测与审计类（工业安全监测系统）、主机防护类（工业主机安全防护系统）、安全管理类（工业安全管理与运营分析平台）等产品，通过该体系，实时发现攻击行为并对仿真工控系统进行防护，验证安全产品和防护方案的有效性。

(2)工控安全渗透靶场建设

依托工控网络安全靶场平台，构建工控安全渗透靶场环境。该系统渗透测试功能模块主要实现利用主动渗透方式对当前的机床、工控系统、工业互联网网络及设备进行信息安全扫描，尝试以各种方式查看是否对当前系统造成威胁。渗透测试模块架构如下：

图：工控安全渗透靶场——渗透测试模块架构

渗透功能模块采用了载荷变形、编码和 HTTP 分片传输等技术，自动化绕过防护设备，防止被防护设备拦截而检测不出漏洞；支持通过高质量插件提供的漏洞利用接口，可以直接让使用人员通过接口利用漏洞，从而进行更深一步的测试；可以在对漏洞详情不太了解的情况下，对检测出的漏洞进行真正的漏洞利用，发挥漏洞真正的威力；考虑到漏洞发现、漏洞利用和后渗透的自动化衔接，渗透功能模块使用自动化渗透流程管控技术，实现了漏洞发现、利用到权限获取与维持的整个过程。

恶意代码渗透是一个无监管的、自动的从模型建立到模型检测的全方位功能模块。全模块分为工控系统恶意代码武器库、工控系统恶意代码渗透投放、工控系统恶意代码渗透状态评估三大功能，分为三大核心技术：恶意代码聚类技术、恶意代码检测规则自学习技术、恶意代码检测判定技术。

网络渗透可对控制器、伺服器和计算机集成制造网络等进行渗透，支持刺探、扫描、泛洪渗透、鉴别渗透、迂回渗透、伪装、读取、复制、窃取、篡改、删除等渗透动作。

3. 其他亮点

(1)解决工控系统缺乏网络安全攻防基础平台的问题

在工控系统网络安全研究中，攻击手段和防护方法的研究都是不可或缺的。在工业领域，工控系统一旦遭受攻击将带来较为严重的经济损失、人员伤亡，基于此特点，建设工控系统网络安全攻防能力平台，在工控系统未遭受真实攻击的情况下，对工控系统进行攻击模拟，直观反映攻击后果引起重视，同时也能综合

评价被测工控系统抵御网络攻击的能力，从而提出安全改进方案，提升工控系统安全防护能力。

(2)解决工控系统脆弱性检测能力不足的问题

国外在漏洞扫描技术方面的研究相对起步较早，并且也取得了一定的成果。基于漏洞扫描与挖掘的成果构建完备的漏洞库，是安全研究领域的一项重要课题。目前国内在这方面的能力相对较弱，基于该靶场可以利用工控漏洞扫描工具和工控漏挖工具对工控系统进行脆弱性探测，助力工业漏洞基础研究。

(3)解决工控系统网络威胁难发现的问题

传统的网络安全事件分析思路是遍历各个安全设备的告警日志，尝试找出其中的关联关系。但在工控实战过程中，针对工控生产装备的攻击，尤其是攻击者采用某些手段进行证据销毁工作后，依靠传统的分析方式、传统安全设备通常都无法对 APT 攻击的各个阶段进行有效的检测。基于数控系统场景的工控网络安全靶场建设，助力安全人员实现格式化检测，从海量的数据中找到有价值的信息。

三、下一步实施计划

1. 推广应用

基于数控机床场景的工控网络安全靶场培养客户操作员以及工控系统人员的安全意识和安全能力。靶场在检验企业数控系统整体安全能力的同时，可对数控系统进行定制化靶场环境复现，利用工业控制系统存在的漏洞进行专业演练，用可控的方式对其进行安全攻击，加强客户操作员和工控系统人员对漏洞本质的理解，客户根据靶场的漏洞特征分析报告有针对性的消除漏洞。本靶场将满足我国相关行业的需求，具备巨大的市场前景，同时也将大大提升我国关键基础设施的网络安全防护能力。

四、项目创新点和实施效果

1. 项目先进性及创新点

(1)漏洞发现和关联分析技术

基于大数据处理的漏洞发现和关联分析技术成为对工控系统安全漏洞、威胁、脆弱性、异常行为分析的有力武器。利用大数据分析对全网资产面临的安全漏洞影响面快速定位，应用资产价值、业务价值和业务连续性影响等数据，综合漏洞风险等级、漏洞类型、漏洞危害性等数据进行数据关联分析，给出漏洞处置优先级及处置建议。

(2)高度自动化的渗透测试技术

基于数控系统场景的工控网络安全靶场采用高度自动化的渗透测试技术，包括自动探测技术（端口扫描、指纹识别、子域名识别、漏洞探测等）、自动障碍绕过技术（机器学习验证码识别技术、Bypass WAF 技术）、自动利用技术（针对无法完全自动化利用的漏洞，“一键式”手动调用漏洞插件）和自动权限获取技术（利用漏洞、口令爆破等方法自动获取用户权限）。

(3)设备建模和数据对接技术

将大数据和网络安全分析技术相结合，实现对数据的采集分析，功能维度进行汇总、查看、统计及处置。设备仿真和数据采集技术成为对工控系统安全威胁和系统状态异常分析的有力武器。利用采集的数据进行分析能够对设备安全态势、运行状态和工控资产进行可视化展示，并通过可视化界面进行数据关联查询，及时对工控环境中未来风险进行预测、预防。

2. 实施效果

基于数控系统场景的工控网络安全靶场可以全方位模拟工控场景，将虚拟工控节点和实体工控节点相结合部署在同一业务场景之中，通过虚实结合的技术手段模拟真实工控业务场景。由于提供虚拟与实体结合的部署方式，可以提供灵活的、真实的生产场景，支持从管理、监控、操作、执行、现场的多层级模拟能力，最大限度的复原全部生产流程及供需。基于该靶场可以实现覆盖全行业场景，全产业要素，全领域空间的安全攻防演练和渗透测试，保障工业控制系统安全稳定运行，大大提升我国重要关键基础设施的网络安全防护能力。