2023年全国高校工业互联网安全前沿技术师资培训邀请函

近年来，随着信息技术的快速发展、工业互联网进程的快速推进，云计算、移动互联网、物联网等新兴技术在电力、电网等工业控制领域得到了广泛的应用，实现了企业数字化、网络化、智能化的发展。工业互联网在带给工业系统生命力的同时，也打破了传统网络安全界限，导致大量网络安全威胁向工业内网延伸渗透。一旦遭到破坏，极有可能造成工业生产停滞，发生生产事故，危及人身财产安全，甚至导致整个产业链瘫痪。国际上围绕网络空间安全的斗争愈演愈烈，发生的许多安全事件表明，我国能源、制造等多个行业的关键基础设施网络面临较大的网络安全风险与挑战，成为网络攻击的重灾区，网络安全形势不容乐观。

党的十八大以来，党中央、国务院高度重视网络安全工作，相继出台了《国家网络空间安全战略》、《网络安全法》、《关键信息基础设施安全保护条例》等一系列政策法规，为我国网络安全的发展提出战略指引，对落实企业网络安全主体责任，完善网络安全监督管理体制机制，加强全方位网络安全管理，强化关键信息基础设施安全保护，加强行业网络安全基础设施建设，加强网络安全人才师资队伍建设等方面作了统筹安排，推进网络安全工作。

从国家网络空间安全战略，到网络空间安全一级学科设立，再到 2017 年 6 月《网络安全法》正式施行，在信息技术飞速发展的时代，建立信息安全保障体系，人才是关键。2016 年 7 月中央网信办发文〔2016〕4 号文件关于加强网络安全学科建设和人才培养的意见中，第四条特别指出，要强化网络安全师资队伍建设，鼓励高等院校有计划地组织网络安全专业教师赴网信企业、科研机构和国家机关合作科研或挂职。打破体制界限，让网络安全人才在政府、企业、智库间实现有序顺畅流动。鼓励和支持符合条件的高等院校承担国家网络安全科研项目，吸引政治素质好、业务能力强的网络安全教师参与国家重大科研项目和工程。采取多种形式对高等院校网络安全专业教师开展在职培训。为提升高校教师对工业互联网前沿技术的理解和认知，促进各高校网络安全培养体系的更新升级，博智安全联合工业与信息化部电子第五研究所、暨南大学网络空间安全学院以及产业合作伙伴，将工业互联网技术以及工业互联网安全领域当前核心的前沿技术以及

教学资源赋能给高校教师，使高校教师在知识技能、教学模式等多方面得到扩展提升。

本期培训为期三天，结合教学实训平台以及面授方式，采取“核心理论+实操+案例应用”模式，将重点介绍工业互联网安全领域的前沿理论及课程设计思考。着重讲解工业互联网技术基础、工业控制协议分析、工业控制系统漏洞分析、工业企业综合渗透及工业控制系统攻防实训演示等领域。此外，我们还会围绕工业互联网安全新趋势，深入探讨行业领域行业相关威胁案例，如电力行业等。课程期间将穿插丰富的应用案例，使老师能够深入理解掌握前沿技术理论并在实际教学工作中有所应用。

现诚邀全国高校、职业院校计算机相关专业（信息安全、网络空间安全、计算机科学与技术、网络工程、软件工程、信息工程、自动化、工业互联网技术等）学科带头人、专业骨干教师参加。

主办单位：工业与信息化部电子第五研究所、暨南大学网络空间安全学院

承办单位：博智安全科技股份有限公司

一、培训时间：2023 年 11 月 24 日——2023 年 11 月 26 日

二、培训地址：工业与信息化部电子第五研究所 1 号楼 401（广州增城区朱村大道西 76-78 号）

三、报名安排：

培训人数：40 人（报满截止）

报名时间：即日起至 2023 年 11 月 20 日

报到时间：2023 年 11 月 23 日 15：00—18:00

餐饮住宿：餐饮及住宿费用自理

推荐住宿：赛宝双创人才基地（广州增城区朱村大道西 78 号）

四、培训费用：3200/人

五、培训准备：请老师自带手提电脑。

六、培训大纲：

日期	时间	培训主题	主要内容
11月24日（第一天）	9:00-10:30	工业互联网相关政策介绍和解读	主要讲解部、省、市相关工业互联网促进数字化转型政策宣贯与解读。
	10:30-12:00	工业互联网技术基础	工业互联网技术发展历史、技术体系架构介绍、典型案例分享。
	14:00-15:00	赛宝实验室参观、合影	参观、合影。
	15:00-17:00	工业控制系统现状分析	主要讲解关键基础设施中工业发展历程，工业网络组成，典型工业四成网络脆弱性风险分析，工业安全发展政策引导方向以及工控安全发展解决方案，最后针对典型协议进行分析，突出工业安全方向协议方面漏洞安全防护手段与XDR防护思路重要性。
11月25日（第二天）	9:00-10:30	威胁情报与应急响应	网络环境日益复杂，各类平台及应用的普遍利用使得界限变得模糊，导致安全事件频发，如何根据安全事件及相关威胁情报驱动应急响应工作、如何做好安全应急处理，提升应急响应能力成为一个企业安全运维的重要工作。
	10:30-12:00	网络流量分析	主要讲解流量抓取方式，讲解wireshark、tcpdump、科莱等常规网络流量分析方式，实际分析ftp、http、tcp、udp等协议内容与还原，以此了解ids、ips等工具的过滤原理，最后讲解网络故障、内网病毒、webshell等恶意流量分析溯源方法。
	14:00-17:00	攻防渗透行为分析	主要针对攻防渗透测试概述进行讲解，渗透测试典型流程及关键技术、渗透测试漏洞等级划分及常见漏洞所属级别说明、常见渗透测试信息收集方法、渗透测试典型案例分解，使得学员了解典型常规渗透测试方法与过程。
11月26日（第三天）	9:00-10:30	工业控制协议分析	主要讲解常用工业控制协议，包括Modbus、S7等；工业控制协议存在的安全缺陷；工业控制协议进行数据报文分析技术。
	10:30-12:00	工业控制系统漏洞分析	主要讲解下位机漏洞（如未授权访问、工控协议安全缺陷、Web用户接口漏洞和后门账号等）和工业控制网络设备漏洞（如Web服务漏洞等）；典型工业控制系统漏洞利用技术，包括PLC CPU

			拒绝服务攻击等。
	14:00-17:00	工业控制系统攻防实训演示与考核	主要通过模拟的攻防实训环境，演示攻防过程，包括病毒木马攻击、工控设备攻击、上位机软件攻击等。

七、培训证书：

本期培训结束后，由主办方、承办方联合颁发《工业互联网安全前沿技术培训结业证书》。如有需要工信部教考中心《工业互联网质量安全工程师证书》，考核通过后，自费 500 元可以颁发《工业互联网质量安全工程师证书》。

八、报名联系方式：

填写报名表并邮件至：zqliu@vip.qq.com

电话咨询：暨南大学刘志全 18578785978

电子五所张锐鼎 19584856378

博智安全刘立东 18820775445

九、报名付款信息：

1. 账户信息：单位名称：博智安全科技股份有限公司

开户行： 南京银行红山支行

银行账号：0170230000000961

2. 付款备注：院校名称+姓名

工业与信息化部电子第五研究所（盖章）

暨南大学网络空间安全学院（盖章）

博智安全科技股份有限公司（盖章）

日期：2023 年 10 月

附件：

报名回执

单位名称						
通信地址						
发票抬头						
纳税人识别号				开票项目	*技术服务*技术培训费	
序号	姓名	性别	部门及职位	手机号	邮箱	身份证号
1						
2						
...						
备注：如果有特殊要求的请填写此处。						