工控安全服务

奇安信 新一代网络安全领军者

服务概述 ABOUT SECURITY SERVICES

近年来，国家对工业控制系统网络安全的重视程度不断加强，相关的政策、法规、标准接连出台，在风险评估、等级保护、分类分级等各个方面提出了越来越明确的要求，不断完善了工控网络安全防护标准体系。

奇安信工控系统网络安全服务，依据相关国家、行业标准规范，对企业工业控制系统进行全面摸底梳理、分析差距，通过安全服务各阶段工作，识别出工业控制系统存在的各种安全隐患以及风险发生的可能性，结合企业实际现状，输出安全整改方案，确保服务中发现的问题能够及时得到解决，结合试点单位建设经验，构筑强大的工业控制系统信息安全纵深防护体系，切实提高工控网络安全防护水平。

服务对象 CUSTOMERS

监管部门

工信、公安、网信、行业监管机构等

内容

1. 工控网络安全监督检查
2. 工控网络安全事件应急支撑
3. 工控网络安全攻防演习
4. 重大活动网络安全保障
5. 工控网络威胁情报支持

企业

联网工业企业、工业互联网平台企业、标识解析企业

内容

1. 工控网络安全评估
2. 工控网络安全咨询规划
3. 工控网络安全攻防演习
4. 工控网络安全检测
5. 工控网络安全事件应急保障
6. 工控网络安全建设
7. 工控网络安全培训

服务项目 SERVICES

工控安全评估与检查服务

评估与检查依据

法律法规：《中华人民共和国网络安全法》、《关键信息基础设施安全保护条例》
国家标准：《指南》、《等保2.0》、《分类分级》
行业标准

评估与检查流程

工作准备：现场调研、组建项目组、方案准备
现场实施：技术、管理、物理环境评估检查
安全分析：威胁分析、差距分析、风险识别
报告编写：文档编制、提出整改意见

评估与检查内容

合规性评估与检查：等保要求合规、防护指南要求合规、分类分级规范要求合规
威胁情报信息分析：异常行为和未知威胁检测、攻击快速发现和检测、非法内联设备检测
工控主机评估与检查：主机安全基线评估与检查、主机病毒检测、主机操作系统漏洞检测

工控安全体系规划服务

规划依据

法律法规：《中华人民共和国网络安全法》、《关键信息基础设施安全保护条例》
国家标准：《指南》、《等保2.0》、《分类分级》
行业标准：企业发展战略

规划流程

现状分析 → 安全需求分析 → 战略分析及架构设计 → 总体规划 → 实施规划

规划内容

管理体系规划：安全管理制度、安全管理机构、 安全管理人员
技术体系规划：网络安全、主机安全、业务安全、边界安全
运营体系规划：安全建设、安全运维、安全监管

工控安全攻防演习服务

1.演习组织

奇安信 组织单位

攻击方 → 攻防演戏平台 → 防守方

搭建仿真的离线攻防演习平台，进行可视化展示，
所有攻击行为安全可控，攻击录屏，视频监控

2.演习过程

调研阶段
演习目标系统选取
明确演习时间
攻防演习约束条件调研
攻防演习通报机制调研

准备阶段
攻防演习平台搭建
签署演习授权
签署保密协议

演习阶段
攻防演习攻击过程
攻防演习过程监控
攻防演习成果提交
演习过程应急处置

总结阶段
演习资源回收
攻击数据总结
对结果溯源审计
总结报告并汇报

定制化的工控安全检测服务

由奇安信专业渗透测试工程师，模拟黑客可能使用的攻击和漏洞发现技术，对目标工控网络、工业应用软件、工业主机、PLC、控制器等进行深度检测，发现其中存在的安全风险，并进行风险可利用性的验证。

准备阶段
明确检测范围　研讨测试方案　**获得测试授权**

检测阶段

信息采集	系统层　端口扫描　漏洞扫描	手工测试，验证风险，获取访问权
	网络层　网络信息　网络结构	提升权限，获取系统、主机权限
	应用层　应用扫描　代码分析	**编写测试报告及加固建议**

复测阶段
客户加固完成　手工验证风险是否加固　**提交风险验证结果**

工控系统应急演练服务

协助指导用户制定工控安全事件应急响应预案，并定期对工业控制系统的应急响应预案进行演练，必要时对应急响应预案进行修订

在工业企业遇到网络安全攻击时，第一时间予以响应，协助单位采取紧急措施、将业务恢复到正常服务状态，并调查、分析、研判安全事件发生的原因

初步处置：接到应急响应需求后，现场人员封存现场、保留证据、断绝扩散渠道的建议。

溯源分析：通过公司大数据资源，对攻击行为进行溯源分析、样本分析，挖掘攻击者行为特点，与本地分析相结合，判定事件类型与影响范围

现场检测：专家第一时间赶赴现场，进行日志分析、安全事件检测、网络行为分析、应用后门检测等现场检测与分析工作

现场检测：查明原因、结果、损失后，协助用户方对系统及网络进行安全回复，清除安全隐患，强化安全防护能力，恢复系统运行

服务案例 SUCCESSFUL CASE

- 湖北工信厅
- 三一重工
- 首都机场
- 南方电网
- 中车某研究所
- 武汉水务集团
- 水利部
- 天津港集团
- 京东方
- 京港地铁
- 甘肃烟草
- 中国石化

服务优势 ADVANTAGES

领先的安服团队：拥有专职、多梯队的数据分析、应急响应团队，包括省服务团队、大区及行业服务团队、总部二线支持团队。

国内领先的工控安全研究能力：首个落户民营企业的国家级工控安全实验室，由博士带队的工控系统安全研究团队专注工业互联网安全领域的研究

丰富的工控安全服务项目经验：奇安信已经成功在各个行业领域为企业提供安全服务，为企业网络安全提供有力保障。

强大的工控安全专家团队：团队成员来自于国内知名的安全公司、国家安全测评机构专家、公安网安部门、安全部门以及军队部门等领域的安全专家。