

# 奇安信网神工业互联网安全公共服务平台ISPP

## 一站式工业互联网安全服务

奇安信网神工业互联网安全公共服务平台(简称 ISPP)是基于大数据架构自主构建的一套面向中小企业和政府的工业互联网安全的公共服务平台。该系统利用大数据等创新技术手段,结合奇安信的安全能力和安全技术积累聚焦工业网络安全数据分析处理,通过运营人员监测、分析和研判准确发现工业互联网安全事件;及时通报和预警重大工业互联网安全威胁,为中小企业提供集约化的安全监测,包括资产管理、威胁管理、脆弱性分析等,并能提供对威胁的事前预警、事中发现、事后回溯服务,为企业和政府监管部门提供分析结果、处置办法和运营报告,提升工业互联网安全防护水平。

## 用户价值 CUSTOMER VALUE



### 全面提升工业安全监督管理能力

可对工业企业的工业系统进行不间断监测、对系统风险隐患进行实时感知、精准研判,从全局视角获得当前辖区内工业互联网的整体安全威胁,全面提升辖区工业安全监管能力。



### 提高辖区内整体工业安全防护水平

在互联网层面上为企业构建一张巨大的安全监测和防护“大网”,弥补工业企业在工业互联网上防护能力不足、探测能力不够、安全技能薄弱的情况,为工业企业保驾护航。



### 一站式工业互联网安全服务

通过公共服务平台采集各类威胁数据和安全事件,进行分析及研判、处置反馈;依据国家政策法规及企业实践经验,提供在线咨询服务;提供从安全咨询规划、安全评估、威胁共享、安全运营、应急处置等线下企业服务;

## 产品功能 PRODUCT FUNCTIONS

<b>事件分析</b> 经过运营人员对告警日志以及威胁情报的分析,以威胁为中心的角度生成事件,系统自动从攻击者、受害者以及横向多个视角进行分析,同时根据分析结果形成处置办法协同企业处置,生成事件分析报告。	<b>告警分析</b> 对工业企业内的威胁进行告警生成、告警分析和告警处置的闭环管理。利用关联分析引擎对告警日志数据进行过滤、关联、统计、结算、对比、归并等操作,有效识别工业网络和资产的威胁。	<b>资产管理</b> 实现对各企业工业生产环境下资产的统一管理,并实时与资产漏洞知识库进行匹配,获取对应资产的漏洞信息,利用风险计算模型,实现资产风险评估量化,反应企业安全状态。
<b>互联网侧资产监测</b> 依托工业互联网资产探测引擎,利用互联网存活性探测技术和工控设备指纹识别技术,对暴露在工业互联网资产进行存活性扫描、深度分析和指纹匹配,全面发现工业互联网资产、漏洞和威胁情况。	<b>态势感知</b> 通过数据采集、归集和处理等,完成数据监测分析的统计汇总,从多维度对数据监测结果进行汇总分析与统计,宏观展示企业及城市的安全情况,便于趋势预测和研判响应。	<b>运营管理</b> 平台提供多层次的运营管理功能,分为企业管理、服务管理和探针管理。为运营人员提供方便的功能和分析途径,从而可以高效的为政府和企业提供分析结果、处置办法和运营报告。

## 产品优势 PRODUCT ADVANTAGES



## 产品优势 PRODUCT ADVANTAGES



## 部署场景 DEPLOYMENT SCENARIO

奇安信网神工业互联网安全公共服务平台部署方式如图,主要组件有:公共服务平台(软件)、日志采集探针(硬件);日志采集探针通常旁路部署在工业生产网的汇聚交换机和接入交换机位置,不会影响用户业务网络;公共服务平台采取云端对接探针日志数据,支持分布式或者集群的扩容方式,满足不同规模用户的高性能分析需求。

