工业控制系统
信息安全产业联盟
Industrial Control Systems Information Security Industry Alliance

治标更要治本

——工控安全治理新思路

张旭
绿盟科技

目录

关于绿盟科技

绿盟工控安全治理思路

绿盟工控漏洞扫描系统

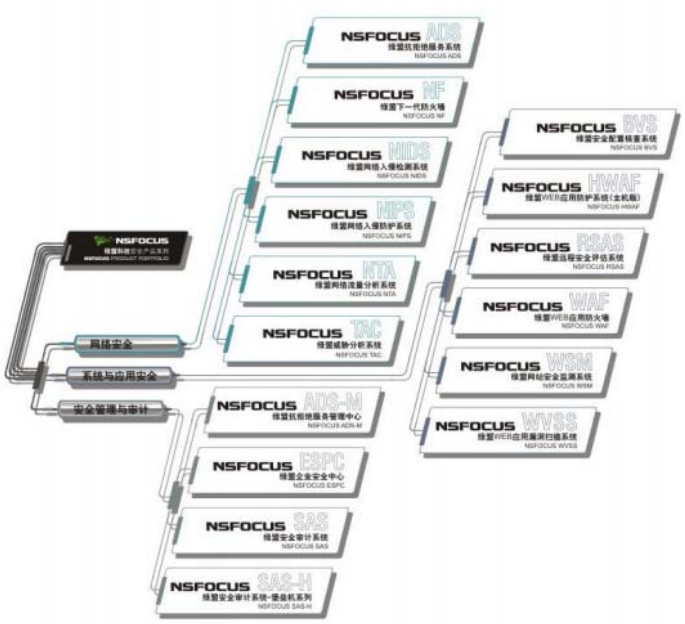
最后的总结

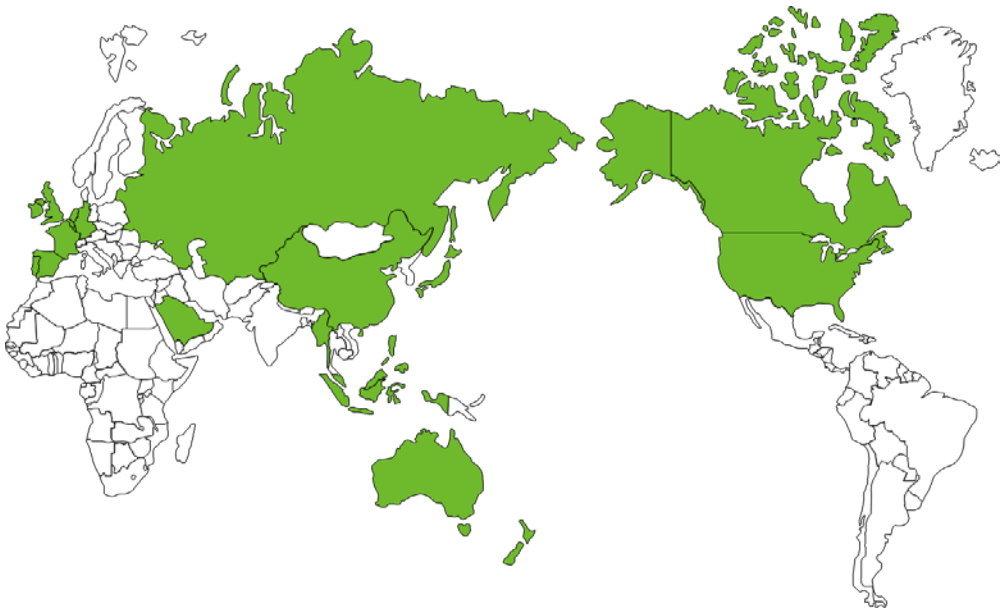
绿盟科技

——巨人背后的安全专家

- 北京神州绿盟信息安全科技股份有限公司
  - 2000年成立，2014年上市（股票代码：300369）
  - 在全球范围内，提供基于自身核心竞争力的企业级网络安全解决方案，成为最受客户信赖的网络安全公司。

- 绿盟科技
  - 1700员工
  - 3个子公司：中国、美国、日本
  - 40个国内分支机构，4个海外分支机构
  - 3大类近20种安全产品

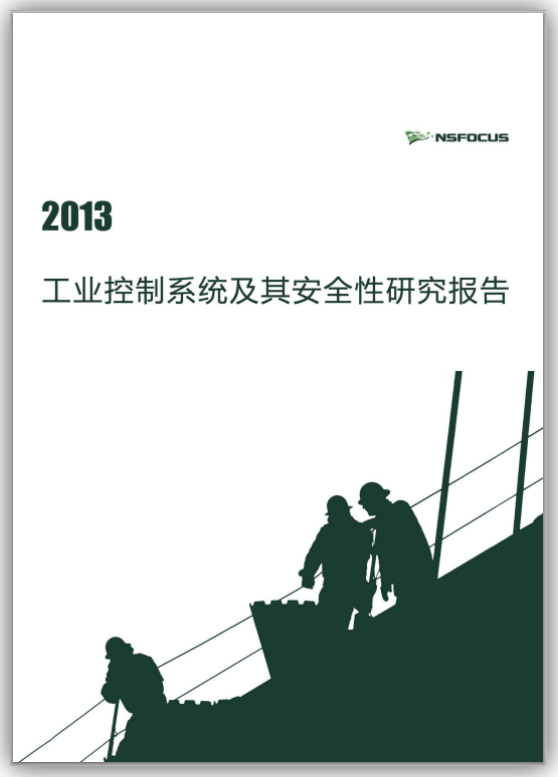


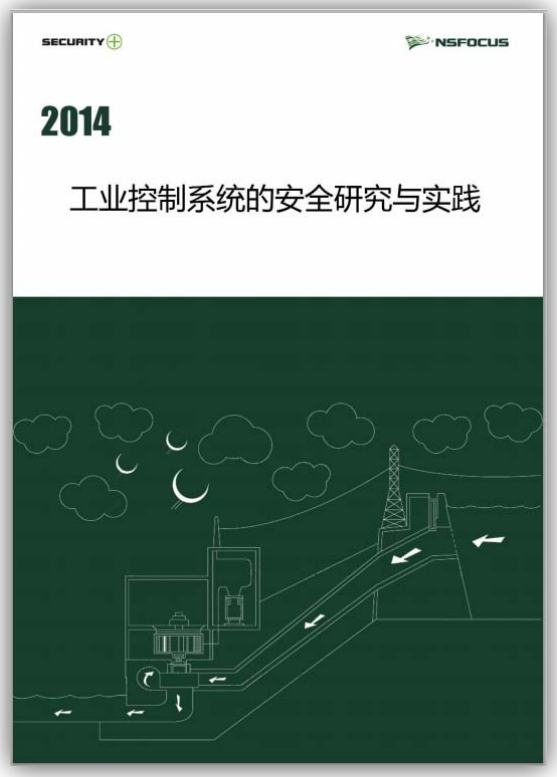


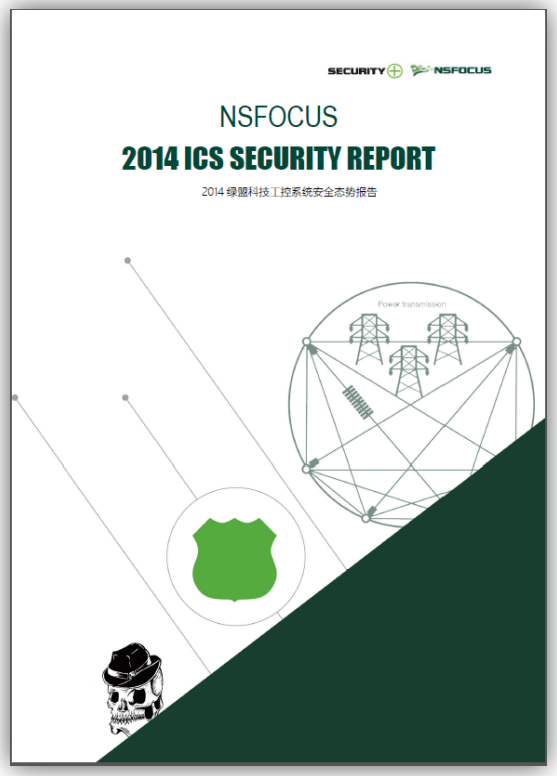
- 绿盟科技
  - 拥有国内顶级安全专家组成的绿盟科技研究院
  - 安全攻防研究
    - 漏洞、威胁、态势、智能、APT
  - 云安全研究
    - 云安全联盟、虚拟化、SDN
  - 工控安全研究
    - 新威胁、新防护

在工控领域持续跟踪研究

- 工业控制系统信息安全产业联盟发起人





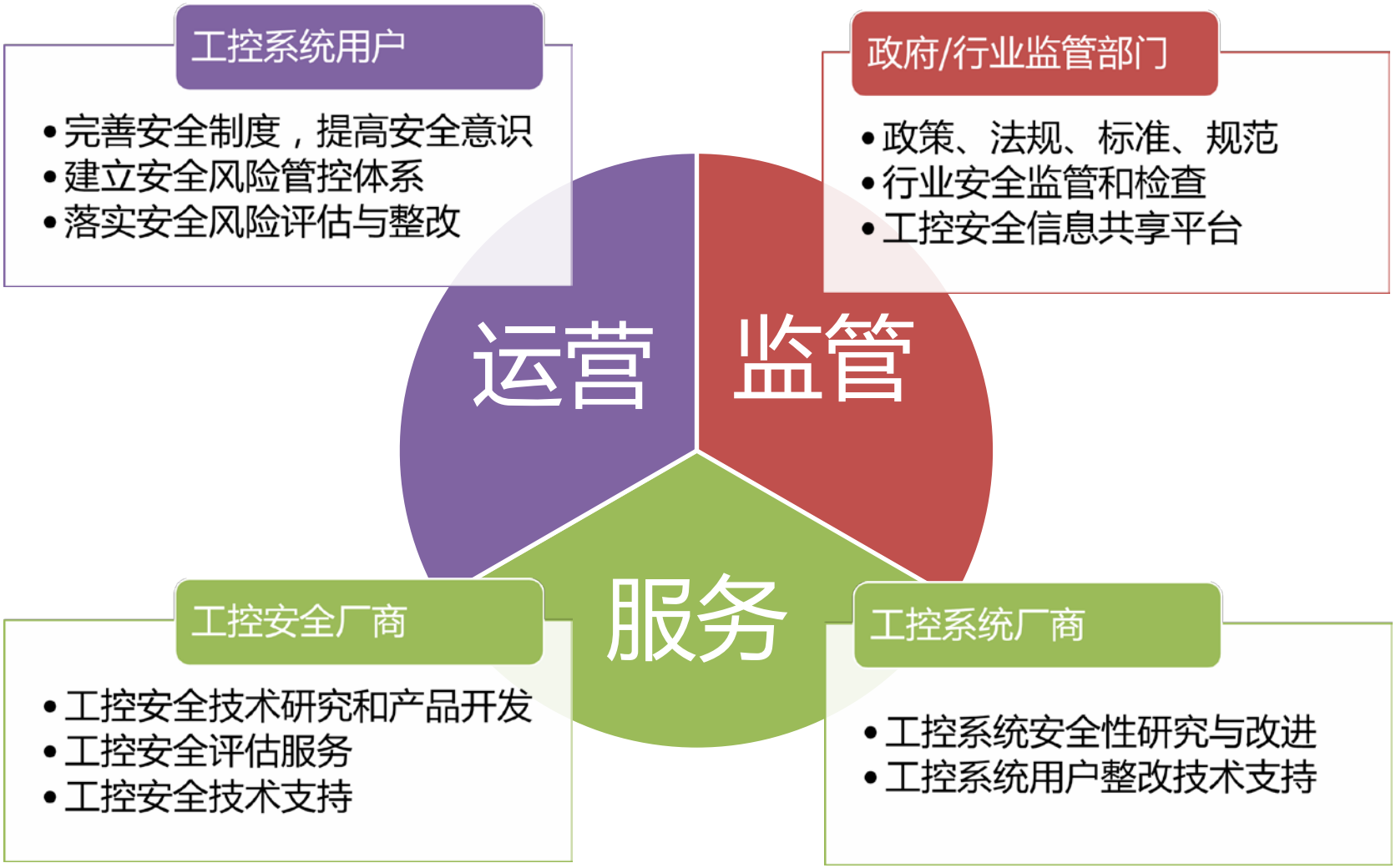


绿盟工控安全治理思路

——治标更要治本

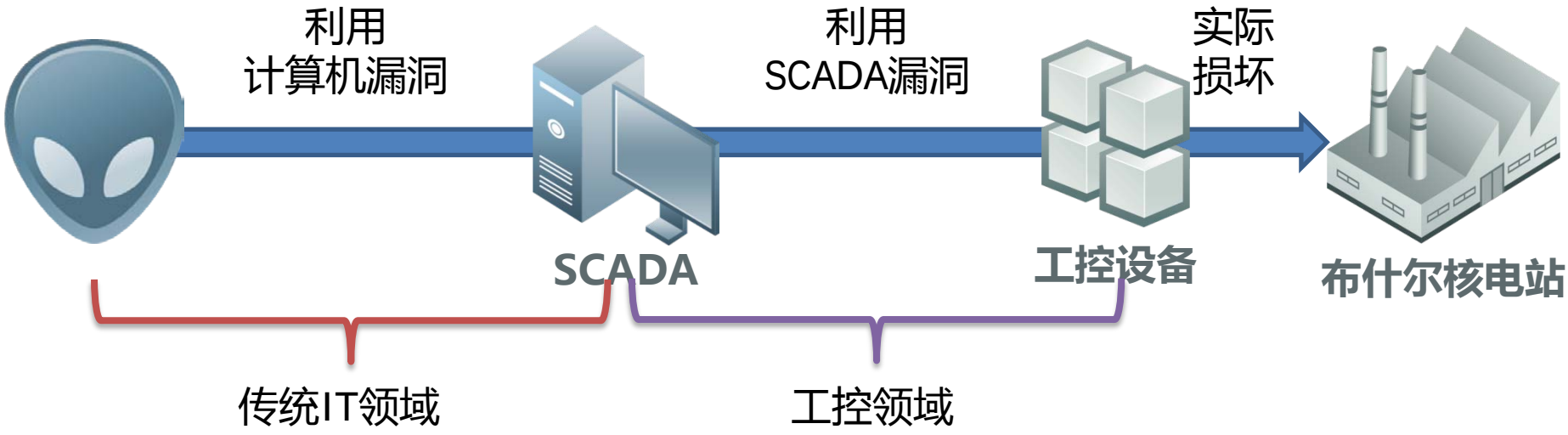
工控安全产业生态环境模型

- 求同存异，共同开拓，推进工控安全发展

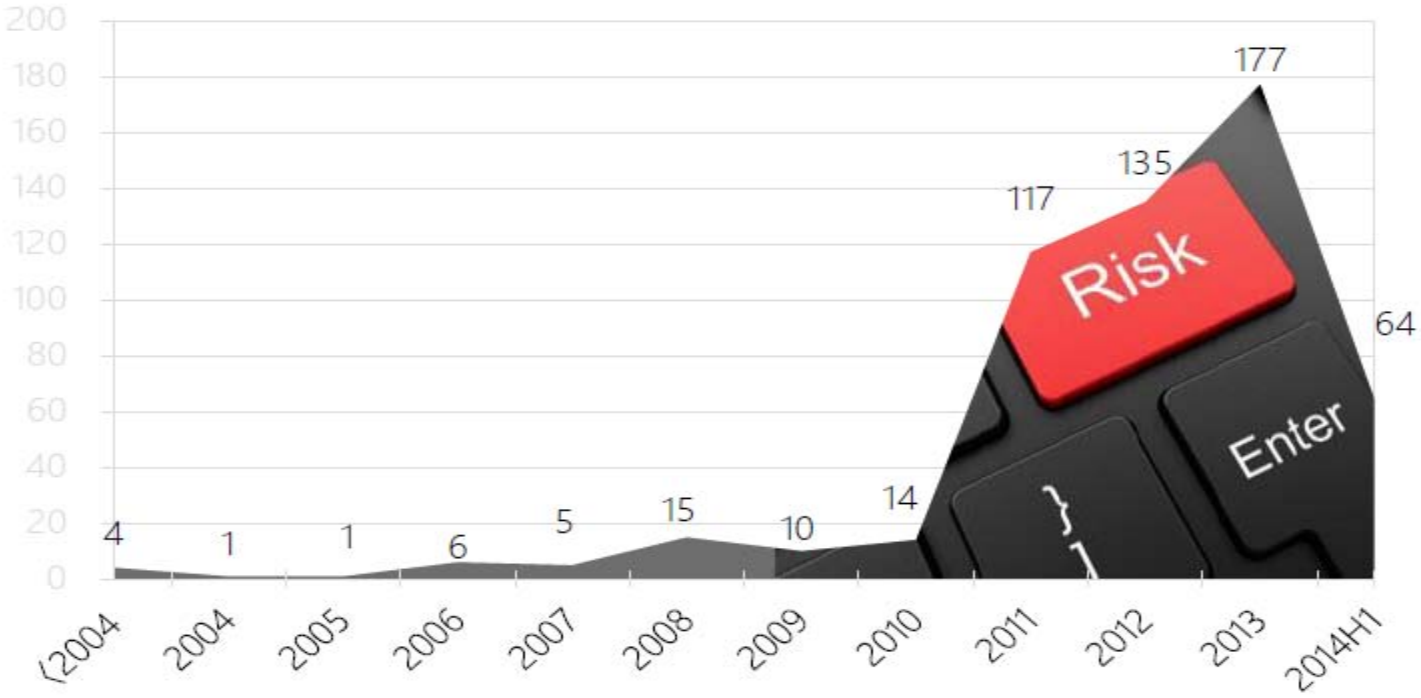


从工控安全厂商的视角看问题

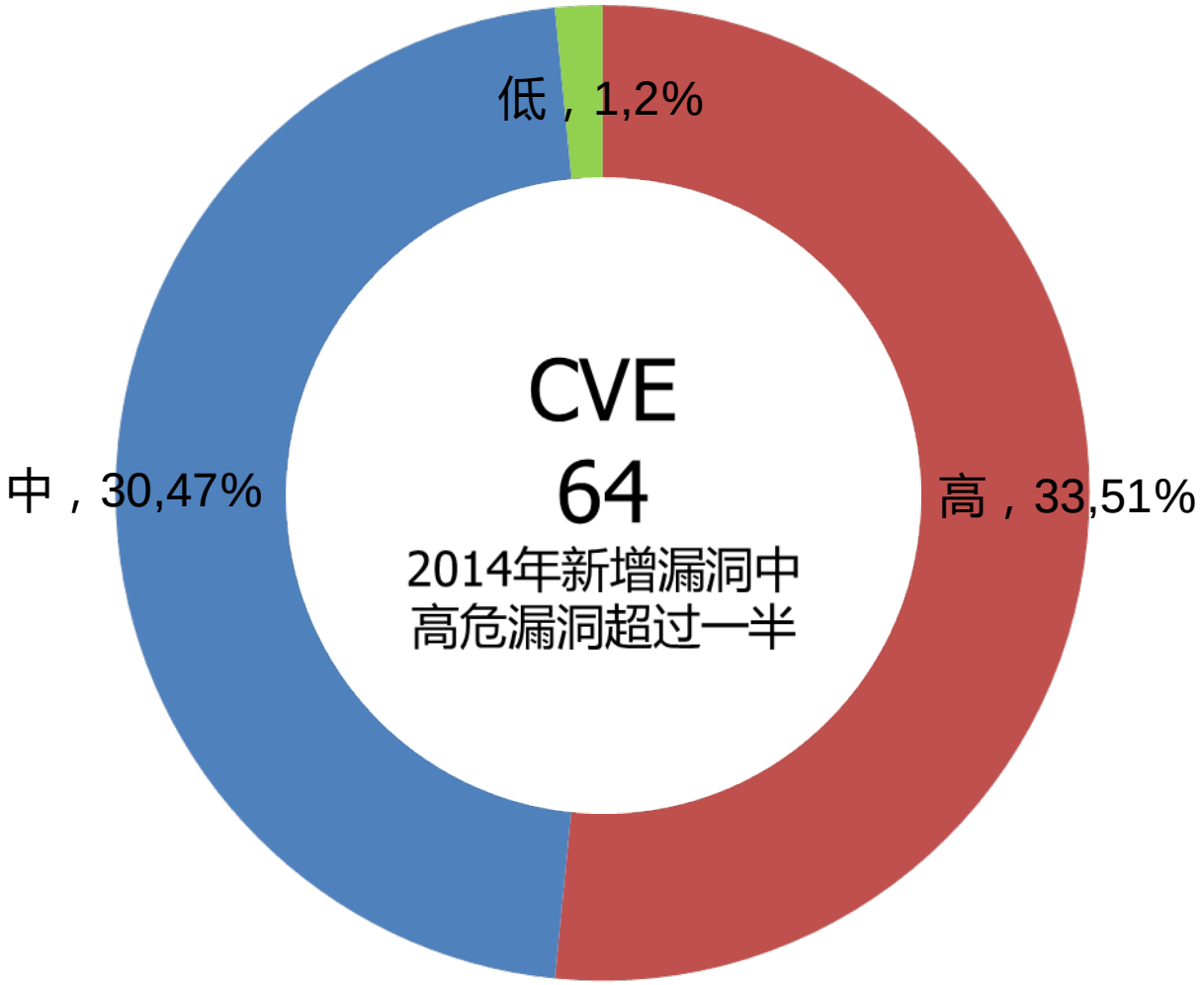
- 两化融合是机遇也是挑战
  - 现代工控系统已经是传统工控设备和IT设备的结合体。
  - 两化融合提高了工控管理水平也降低了黑客攻击难度。
  - 工控设备和IT设备的安全隐患都会造成安全问题。
  - 工控系统的安全风险管理要兼顾工控设备和IT设备。



- 工控安全问题之本
  - 黑客组织是当前工控系统所面临的最大安全威胁
    - 信息泄露、设备控制、设备损毁、安全事故
  - 无论哪种入侵方式，都要利用系统安全漏洞
    - 包括工控系统漏洞和IT系统漏洞

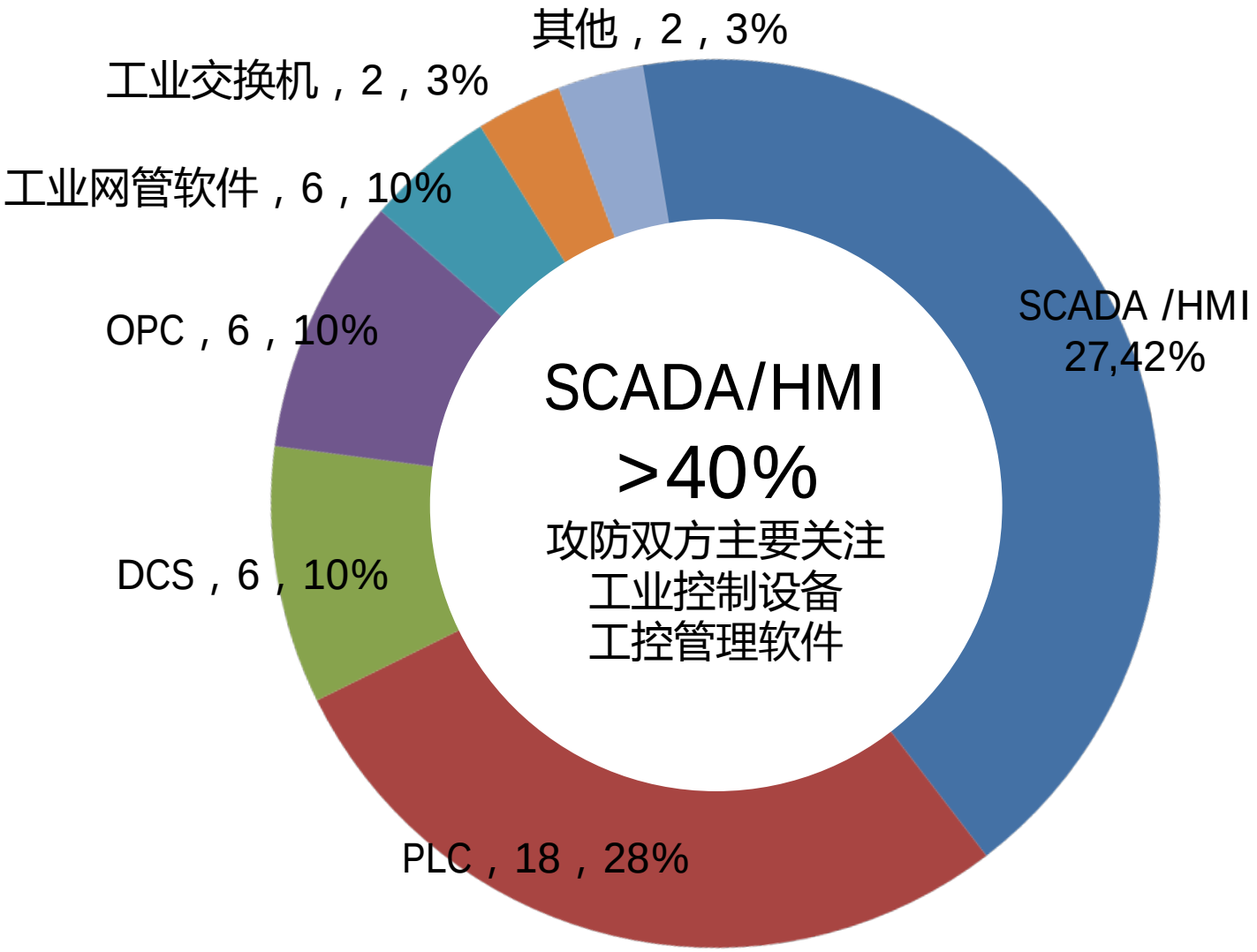


- 2014年上半年新增漏洞情况

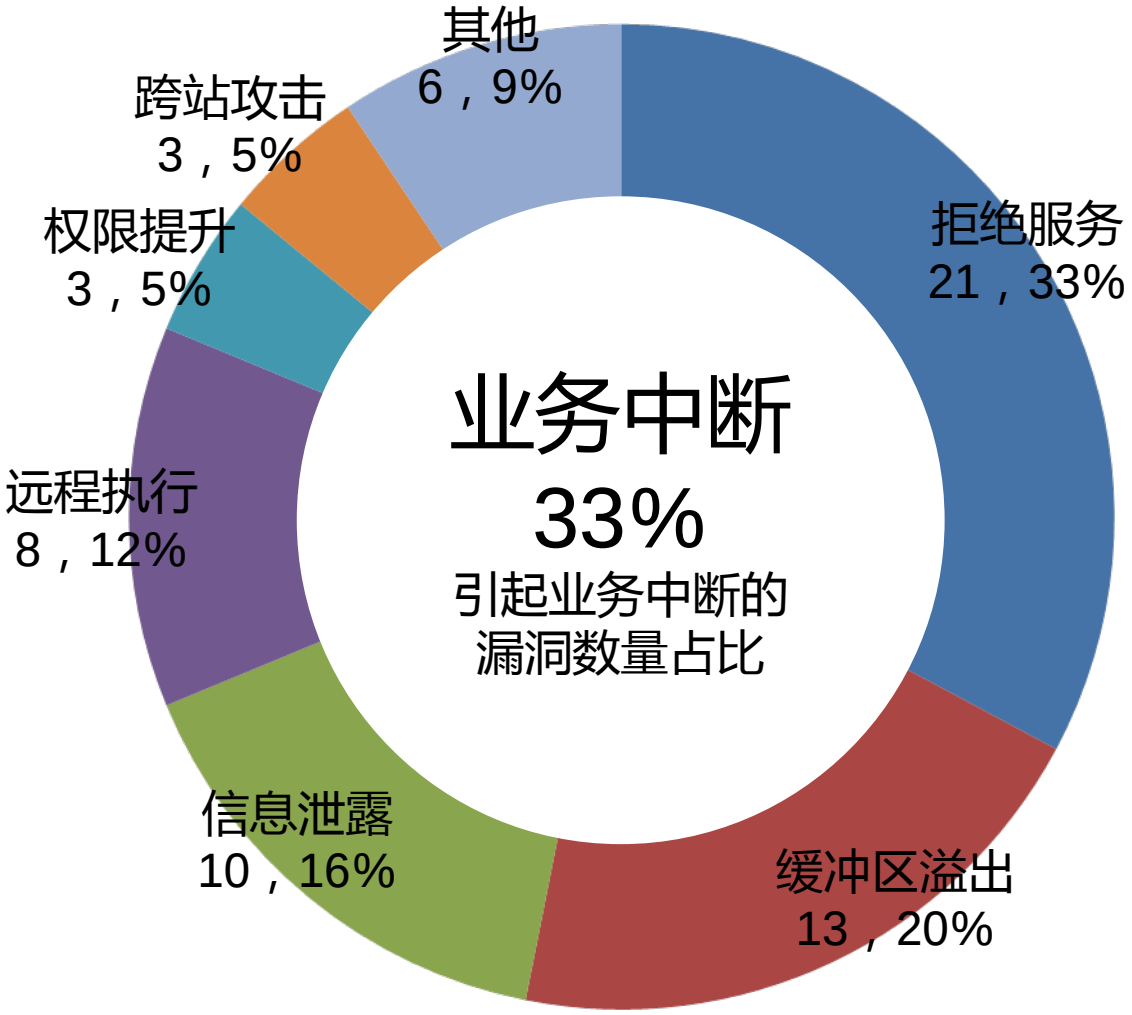


工控漏洞问题日益严重

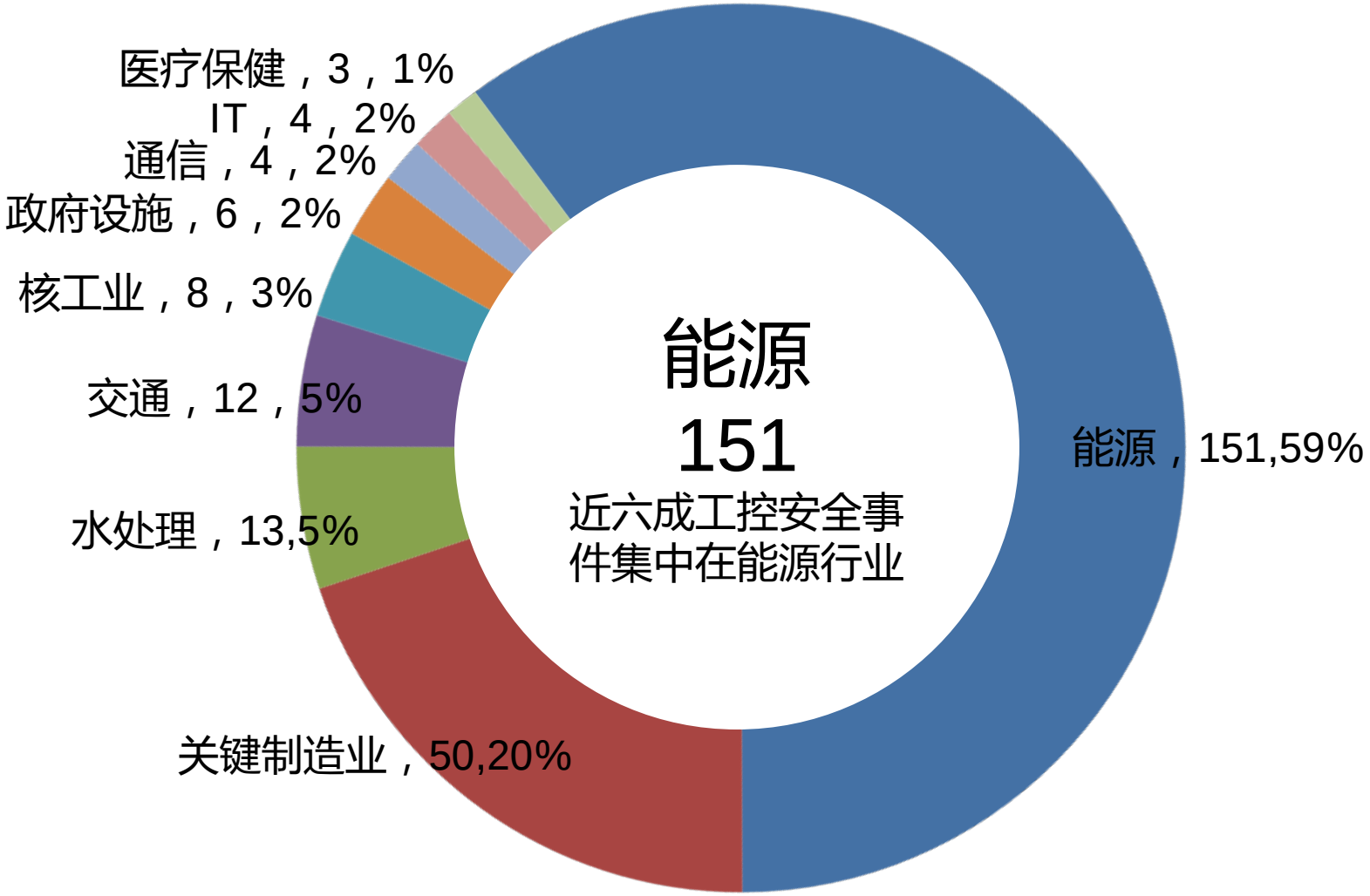
- 2014年新增漏洞影响的系统



- 2014年新增漏洞造成的影响



- 2013年工控漏洞引发的工控安全事件



- 面对严重的工控漏洞问题
  - 我们希望工控系统漏洞问题引起大家足够重视
  - 无论哪种入侵方式，都要利用系统安全漏洞
  - 修补工控系统漏洞是解决工控问题的根本途径
  - 在工控漏洞引发安全问题前进行漏洞管理和修补

亡羊补牢 不如 防微杜渐

- 将成熟的IT风险管理理论移植到工控系统之中
  - 梳理工控资产台账清单
  - 持续跟踪工控漏洞曝光情况
  - 新设备上线前风险评估
  - 老设备离线检修时安全检查
  - 及时联系维护人员修补漏洞
  - 上线前完成修补并进行验证
  - 建立管理制度保障落地执行

绿盟工控漏洞扫描系统（ICSScan）

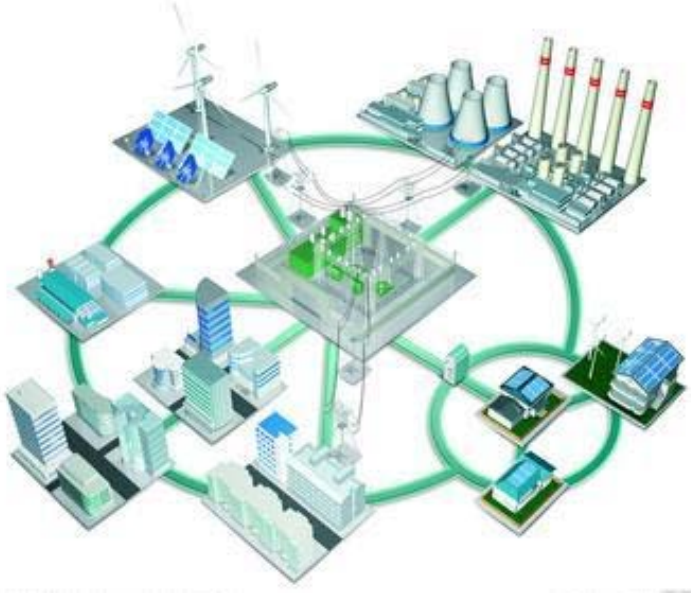
——全面发现工控安全风险

在擅长的领域提供优秀的产品

- 绿盟工控漏洞扫描系统——ICSScan
  - 全面发现工控系统安全漏洞
    - PLC、SCADA、HMI、组态系统……
    - IT系统、网络设备、数据库
  - 风险管理，简单实用
    - 工控风险闭环管理
    - 风险评估报告美观实用

强大的工控扫描能力

- 工控资产漏洞扫描能力
  - **20+**个品牌工控产品**150+**漏洞扫描
  - 支持Modbus TCP、西门子S7系列总线
  - 支持西门子S7、施耐德、ABB等PLC设备
  - 支持多个品牌的SCADA/HMI和组态应用
  - 支持Vxworks、基于Linux实现的嵌入式操作系统



强大的工控扫描能力

- IT资产漏洞扫描能力
  - **12000+**个IT系统漏洞扫描
  - 涵盖所有主流网络对象
    - 基础架构：操作系统、数据库、中间件、通信协议
    - 应用系统：常用软件、应用系统、虚拟化系统
    - 硬件设备：网络设备、安全设备、办公自动化产品

强大的工控扫描能力

- IT资产漏洞扫描能力
  - **600+**种B/S架构工控系统网页漏洞扫描
  - 很多工控系统软件是B/S架构系统
    - 工控系统操作页面是网页
    - 工程师在浏览器里打开网页操作
    - 网页漏洞可以直接影响后台系统正常运行。

强大的工控扫描能力

- IT资产安全配置核查
  - **2000+**个IT系统配置风险检查项目
  - 支持的三十余个品牌IT系统的配置检查
    - 操作系统：Windows、Linux……
    - 网络设备：CISCO、华为……
    - 防火墙：NetScreen、Fortigate……
    - 数据库：SQL Server、Oracle……
    - 应用系统：IIS、Apache……
    - 无线网络设备：华为、H3C……
    - 虚拟化产品：VMware、Xen……

- 围绕工控设备实现风险管理
  - 工控资产自动发现或手工导入

- 围绕工控设备实现风险管理
  - 全部工控风险管理工作围绕资产树
  - 实现真正工控设备风险管理

- ICSScan工控风险闭环管理
  - 建立资产列表
    - 包含工控设备归属部门，责任人，其他相关信息。
  - 对资产进行安全评估
    - 可自动评估（周期/定时）、手动评估
  - 评估结果自动发给资产责任人
    - 工控设备评估报告与解决方案
  - 定时复查安全隐患修补情况
    - 自动/手动重新扫描验证

直观的工控风险展现

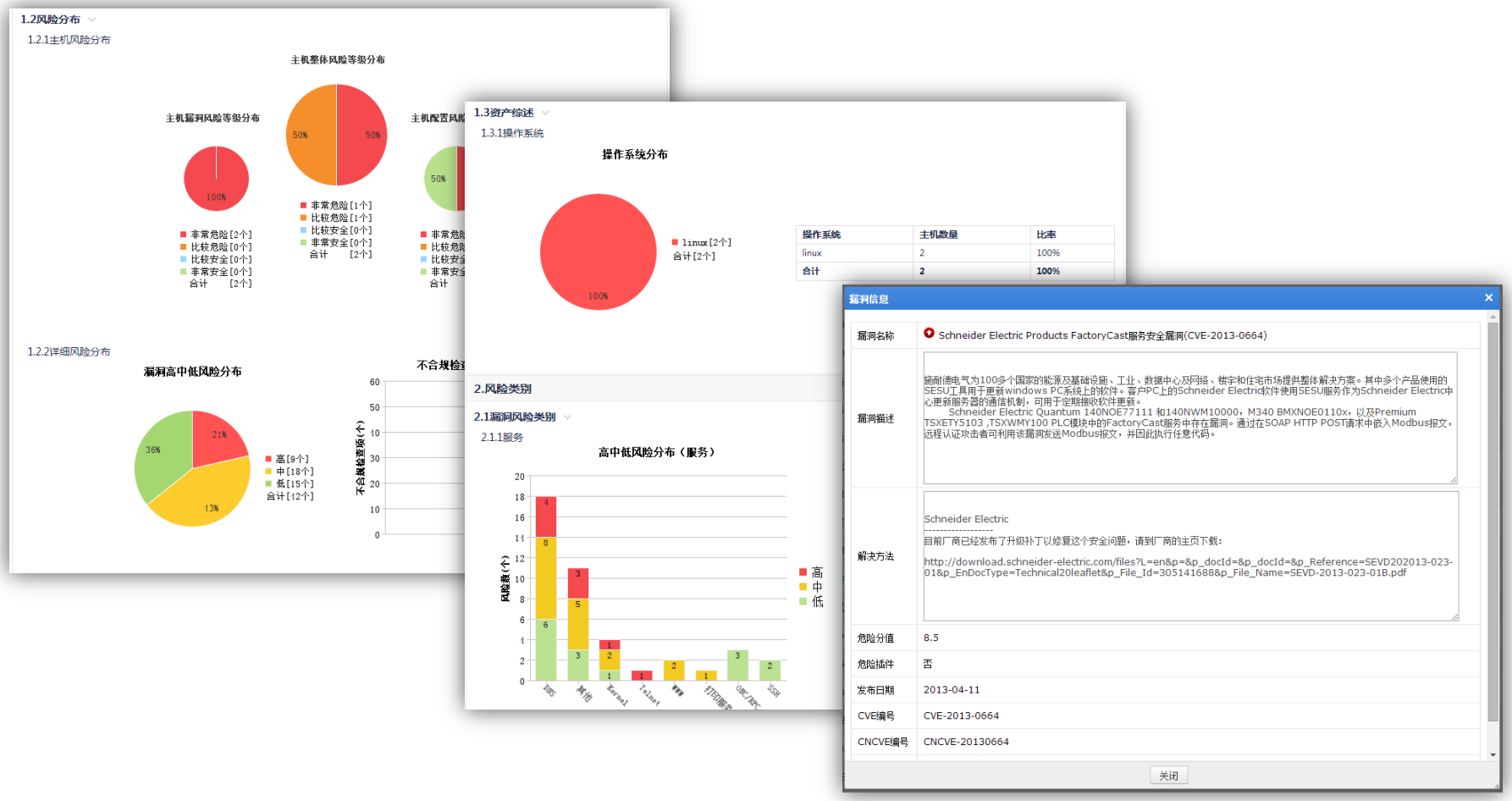
- 工控风险仪表盘
  - 进入系统，第一时间获得工控系统风险态势。

直观的工控风险展现

- 工控风险告警平台
  - 工控安全风险全面展现在告警平台上

直观的工控风险展现

- 工控风险评估报告
  - –美观的综述分析，详细的解决方案



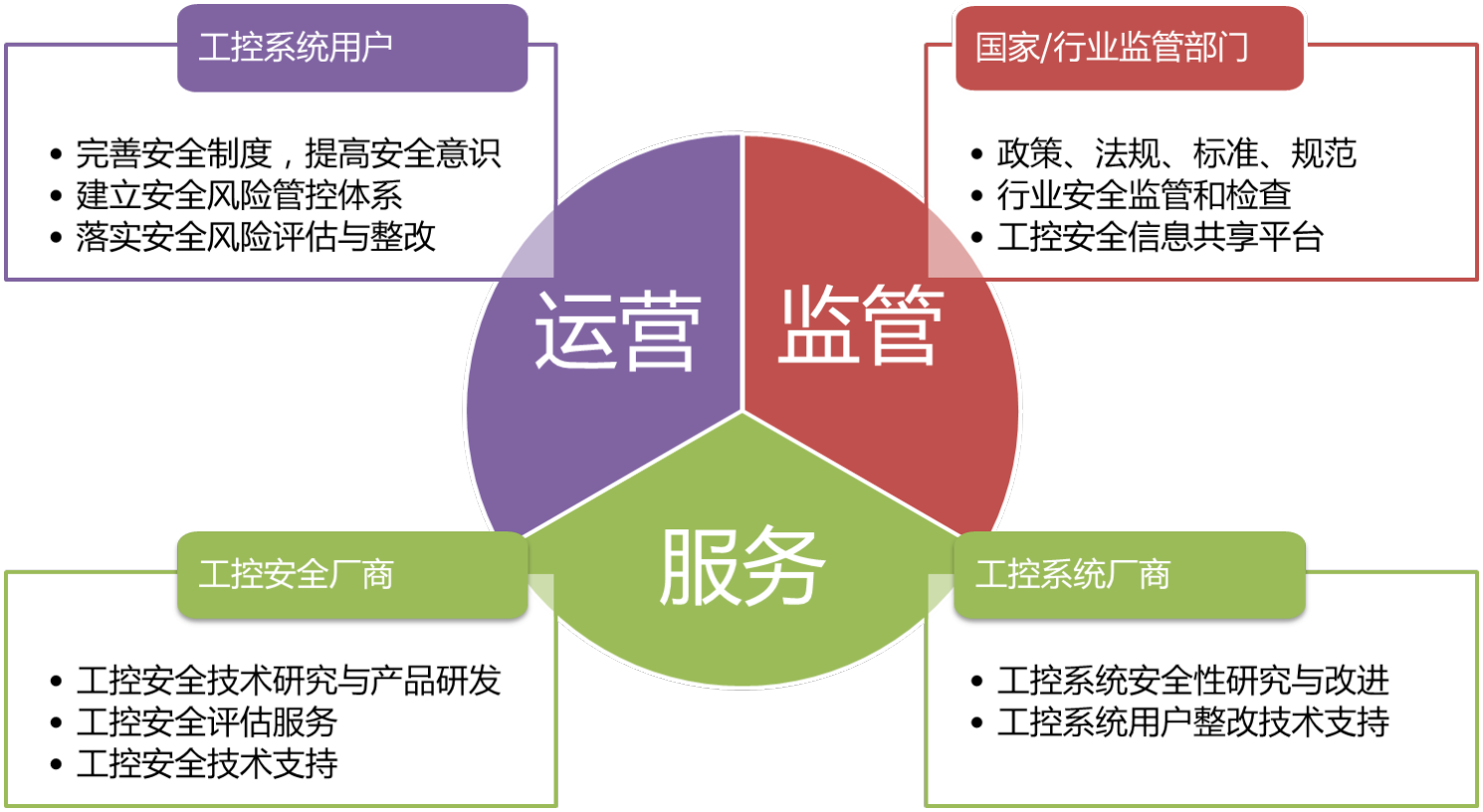
优秀的产品服务各类客户

- 绿盟工控漏洞扫描系统
  - 协助工控系统用户
    - 全面掌握工控系统资产风险
    - 顺利完成等保安全建设和日常安全检查
  - 协助国家/行业监管机构
    - 完善工控系统安全检查能力
    - 促进工控安全研究事业开展
  - 协助风险评估、测评机构
    - 强化对工控客户服务能力
    - 完善测评技术手段

总结一下

——专攻术业 成就所托

提出工控安全产业生态环境模型



引入成熟的IT风险管理理论

在擅长的领域提供优秀的产品

- 绿盟工控漏洞扫描系统
  - **20+**个品牌工控产品**150+**漏洞扫描
  - **12000+**个IT系统漏洞扫描
  - **2000+**个IT系统配置风险检查
  - **600+**种B/S应用web端漏洞扫描
  - **Modbus TCP、西门子S7协议**
  - 漏洞闭环管理和修补方案

感谢聆听

绿盟科技研究报告下载链接

2014 工业控制系统的安全研究与实践

2014 绿盟科技工控系统安全态势报告