



**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



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

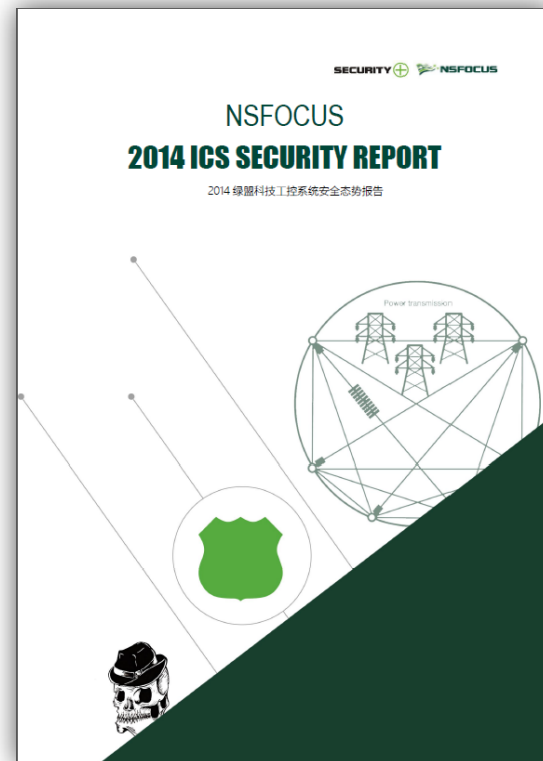
- 云安全联盟、虚拟化、SDN

- 工控安全研究

- 新威胁、新防护



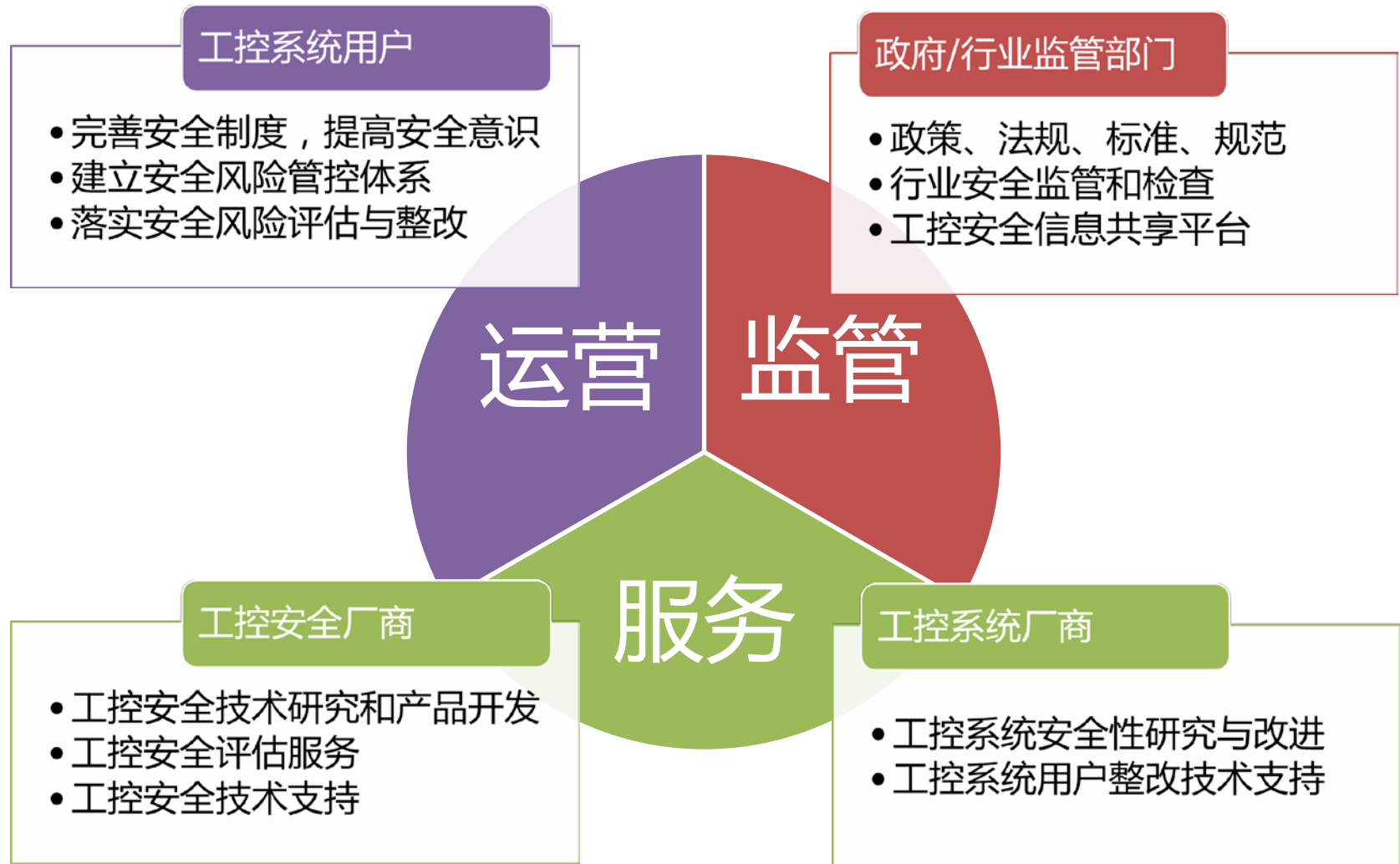
- 工业控制系统信息安全产业联盟发起人



绿盟工控安全治理思路

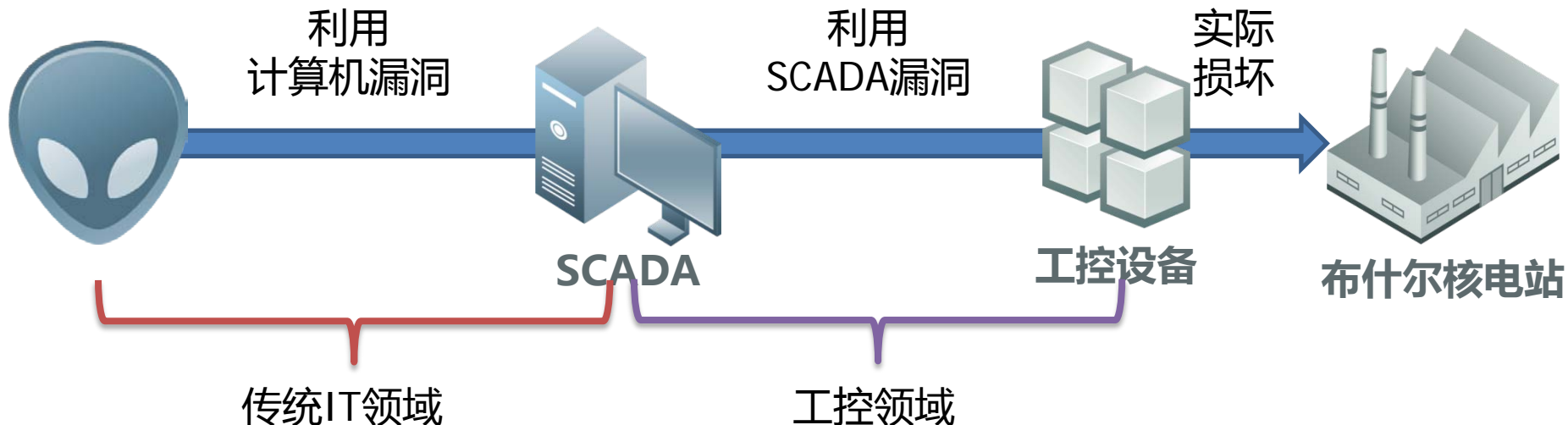
——治标更要治本

求同存异，共同开拓，推进工控安全发展



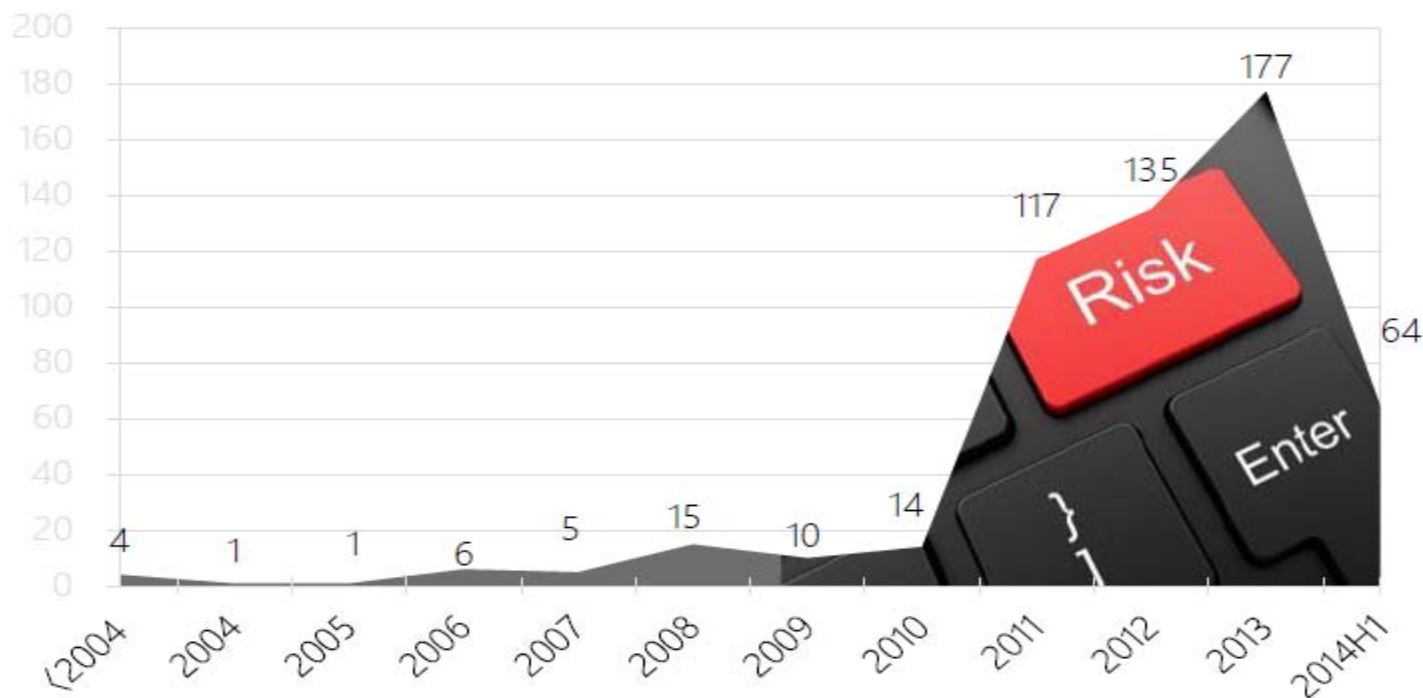
• 两化融合是机遇也是挑战

- 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。

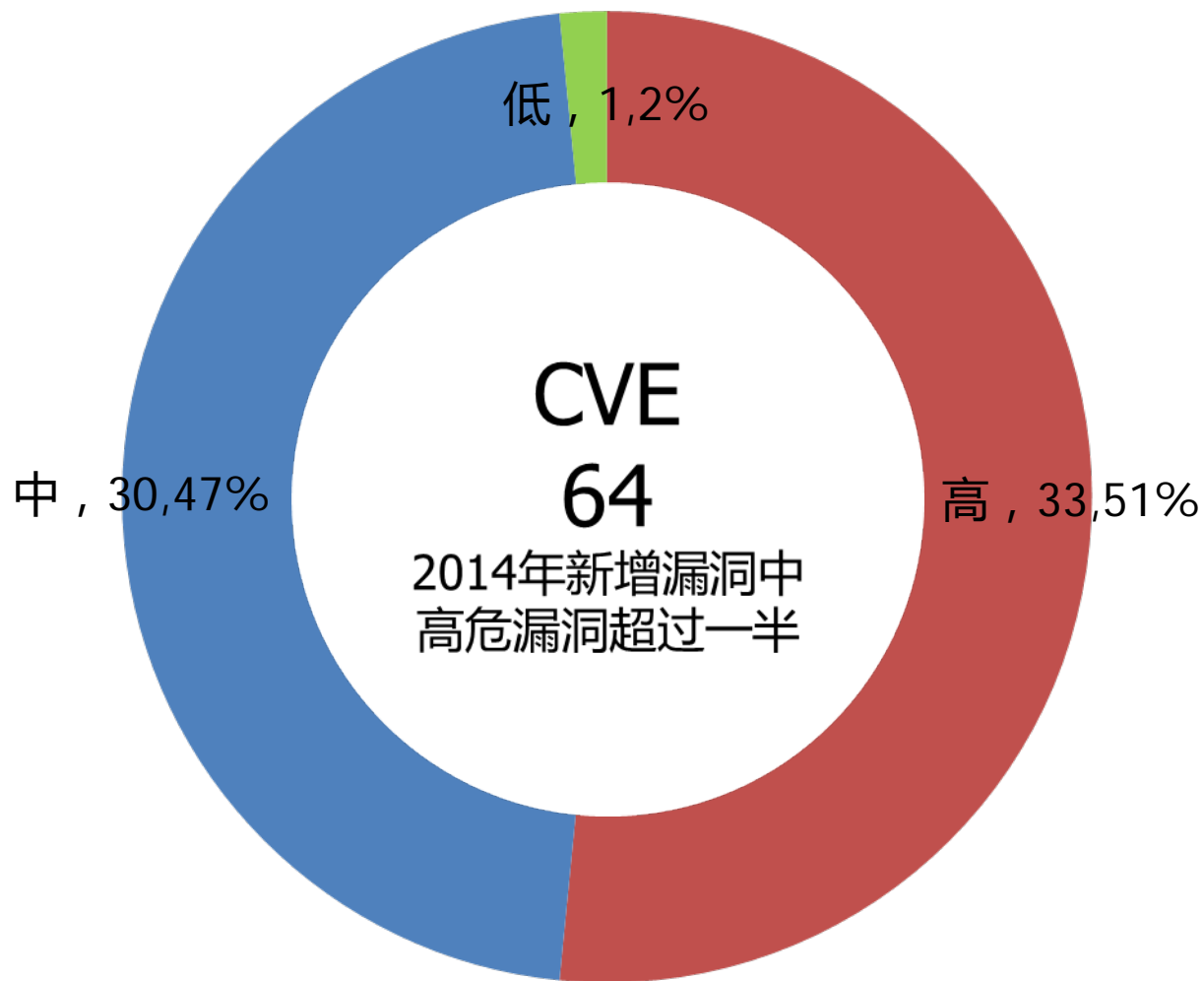


• 工控安全问题之本

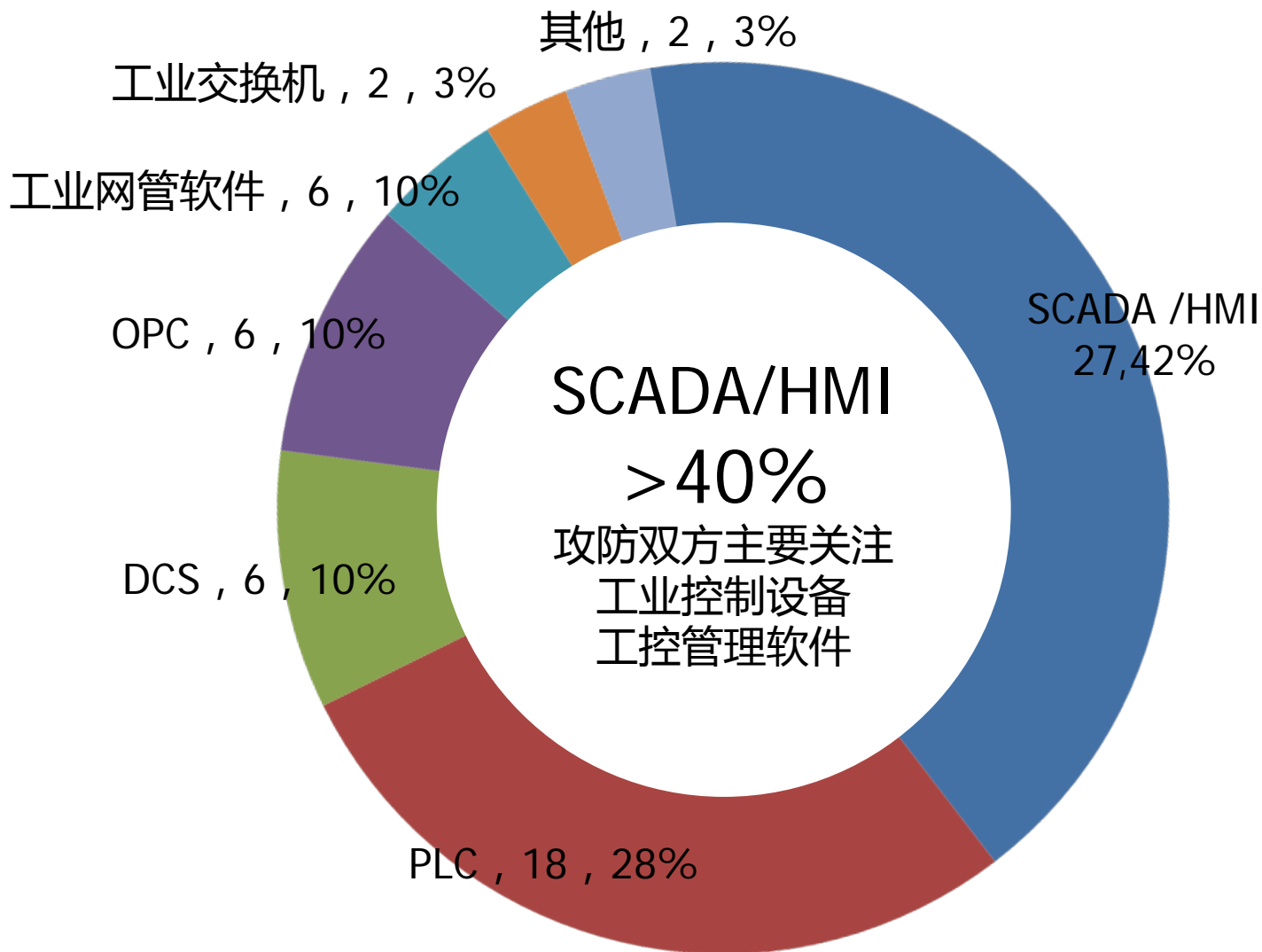
- 黑客组织是当前工控系统所面临的**最大安全威胁**
 - 信息泄露、设备控制、设备损毁、安全事故
- 无论哪种入侵方式，都要利用**系统安全漏洞**
 - 包括工控系统漏洞和IT系统漏洞



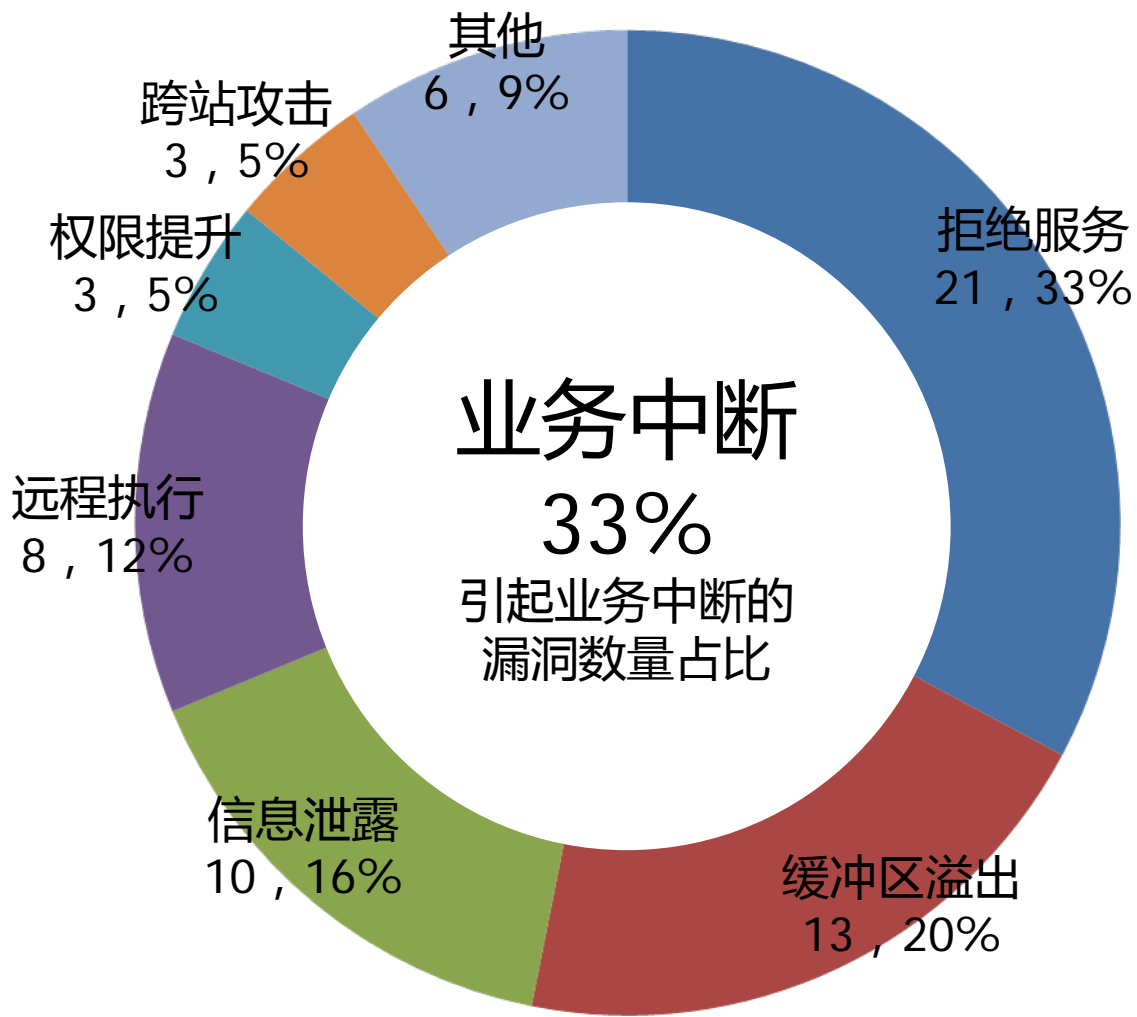
- 2014年上半年新增漏洞情况



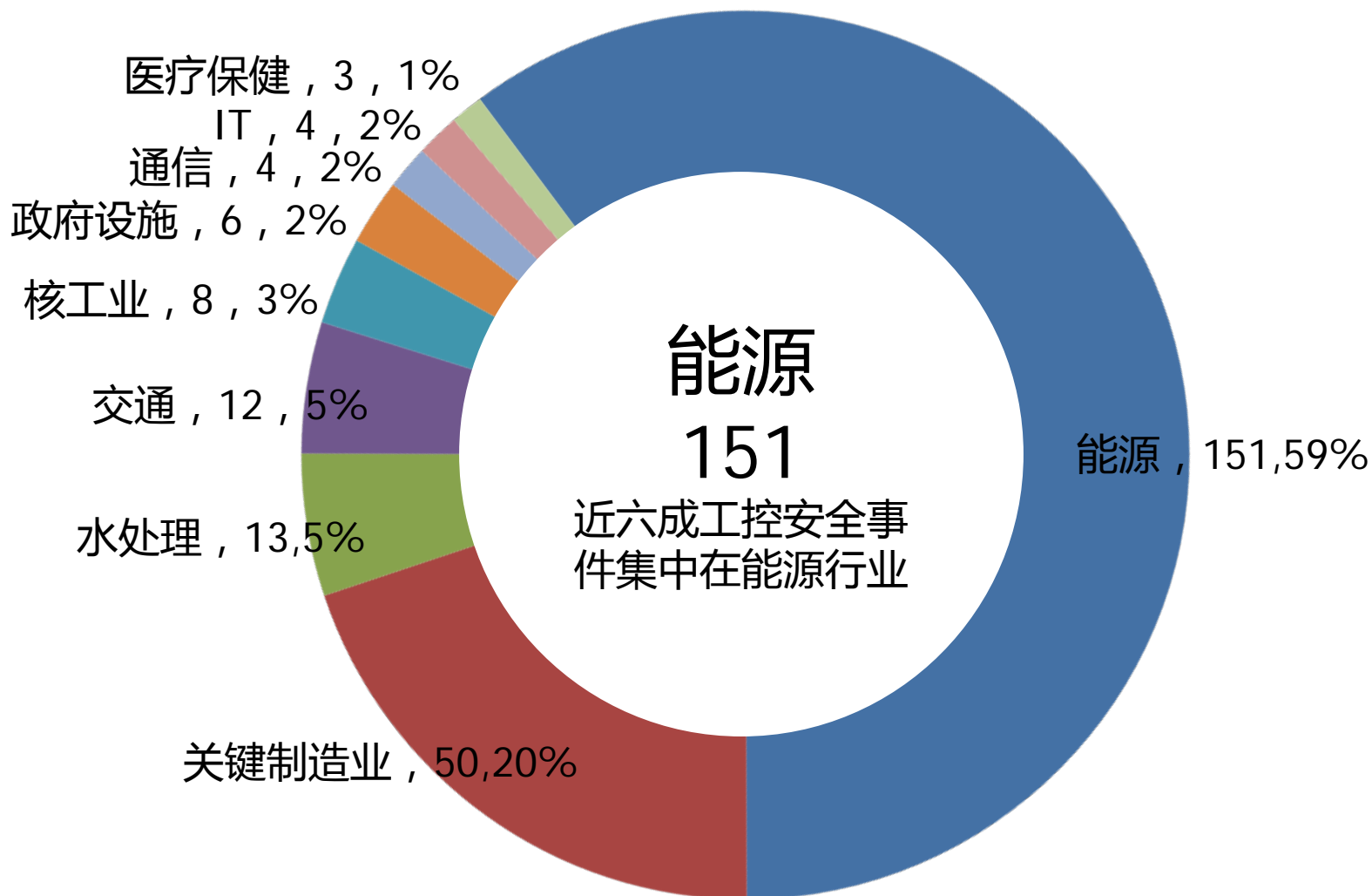
- 2014年新增漏洞影响的系统



- 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

- 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



- 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



- 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



- 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。



- 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

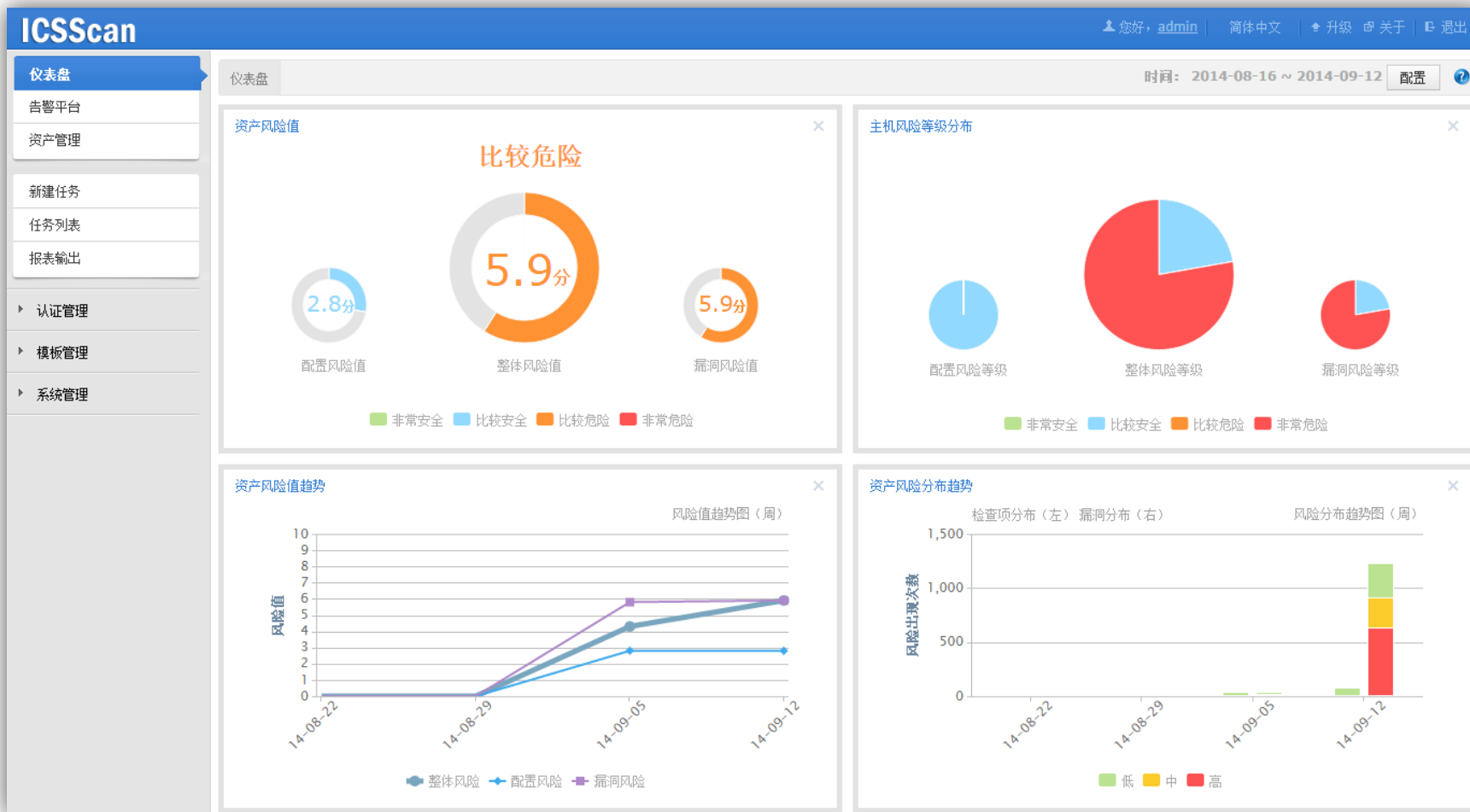
- 定时复查安全隐患修补情况

- 自动/手动重新扫描验证



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。



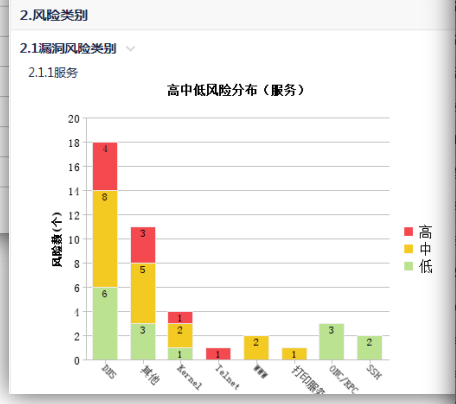
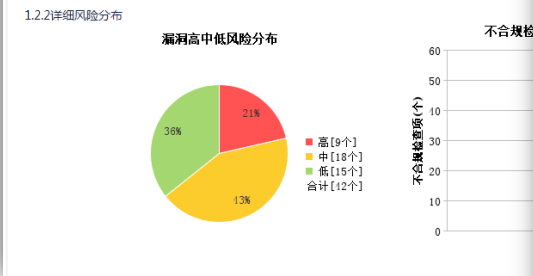
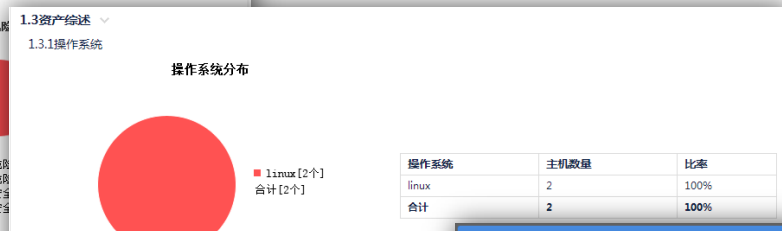
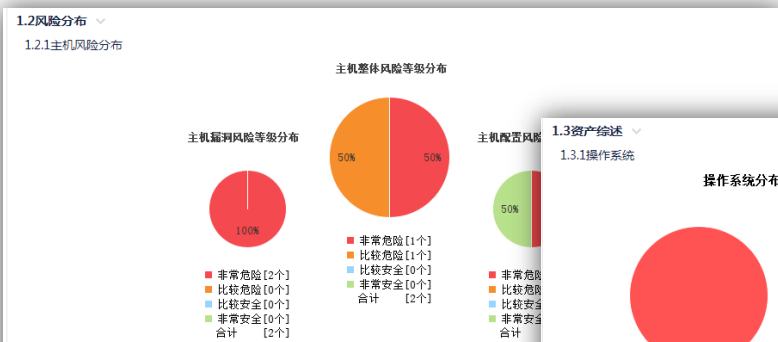
工控风险告警平台

— 工控安全风险**全面展现**在告警平台上

告警管理	风险类型	IP地址	时间	数量
<input type="checkbox"/> + SMB账号信息: HelpAssistant	弱口令风险	10.65.30.62	2014-05-07 17:58:54	1
<input type="checkbox"/> + SMB账号信息: ASPNET	弱口令风险	10.65.30.62	2014-05-07 17:58:54	1
<input type="checkbox"/> + SMB账号信息: Guest	弱口令风险	10.65.30.62	2014-05-07 17:58:54	1
<input type="checkbox"/> + SMB账号信息: SUPPORT_388945a0	弱口令风险	10.65.30.62	2014-05-07 17:58:54	1
<input type="checkbox"/> + KingView `HistoryServer.exe` 堆缓冲区溢出漏洞 (CVE-2011-0406)	漏洞风险	10.65.30.62	2014-05-07 16:15:16	1
<input type="checkbox"/> + KingView `HistoryServer.exe` 堆缓冲区溢出漏洞 (CVE-2011-4536)	漏洞风险	10.65.30.62	2014-05-07 16:15:16	1
<input type="checkbox"/> + SMB账号信息: SUPPORT_388945a0	弱口令风险	10.65.30.62	2014-05-07 16:15:14	1
<input type="checkbox"/> + SMB账号信息: HelpAssistant	弱口令风险	10.65.30.62	2014-05-07 16:15:14	1
<input type="checkbox"/> + SMB账号信息: Administrator	弱口令风险	10.65.30.62	2014-05-07 16:15:14	1
<input type="checkbox"/> + SMB账号信息: Guest	弱口令风险	10.65.30.62	2014-05-07 16:15:14	1
<input type="checkbox"/> + Wu-ftp目录限制访问绕过漏洞	漏洞风险	10.65.44.86	2014-05-06 15:55:07	1
<input type="checkbox"/> + Invision Power Board <= 3.3.4 unserialize() PHP代码执行漏洞【原理扫描】	漏洞风险	10.65.44.86	2014-05-06 15:55:07	1
<input type="checkbox"/> + wu-ftp fb_realpath()远程单字节缓冲区溢出漏洞	漏洞风险	10.65.44.86	2014-05-06 15:55:07	1
<input type="checkbox"/> + Wu-ftp S/key验证缓冲区溢出漏洞	漏洞风险	10.65.44.86	2014-05-06 15:55:07	1
<input type="checkbox"/> + X.Org libXfont LZW解压`BufCompressedFill()`本地权限提升漏洞	漏洞风险	10.65.44.86	2014-05-06 15:55:07	1
<input type="checkbox"/> + 应用程序账号信息: root	弱口令风险	10.65.44.86	2014-05-06 15:55:04	1

工控风险评估报告

—美观的综述分析，详细的解决方案



漏洞信息

漏洞名称 Schneider Electric Products FactoryCast服务安全漏洞(CVE-2013-0664)

漏洞描述 施耐德电气为100多个国家的能源及基础设施、工业、数据中心及网络、楼宇和住宅市场提供整体解决方案。其中多个产品使用的SESU工具用于更新windows PC系统上的软件。客户PC上的Schneider Electric软件使用SESU服务作为Schneider Electric中心更新服务器的通信机制，可用于定期接收软件更新。
Schneider Electric Quantum 140NOE77111 和140NWM10000, M340 BMXNOE0110x, 以及Premium TSXETY5103, TSXWVY100 PLC模块中的FactoryCast服务中存在漏洞。通过在SOAP HTTP POST请求中嵌入Modbus报文，远程认证攻击者可利用该漏洞发送Modbus报文，并因此执行任意代码。

解决方法 Schneider Electric
目前厂商已经发布了升级补丁以修复这个问题，请到厂商的网页下载：
http://download.schneider-electric.com/files?l=en&p=&p_docId=&p_docId=&p_Reference=SEVD201302-01&p_EnDocType=Technical20leaflet&p_File_Id=305141688&p_File_Name=SEVD-2013-023-01B.pdf

危险分值 8.5

危险插件 否

发布日期 2013-04-11

CVE编号 CVE-2013-0664

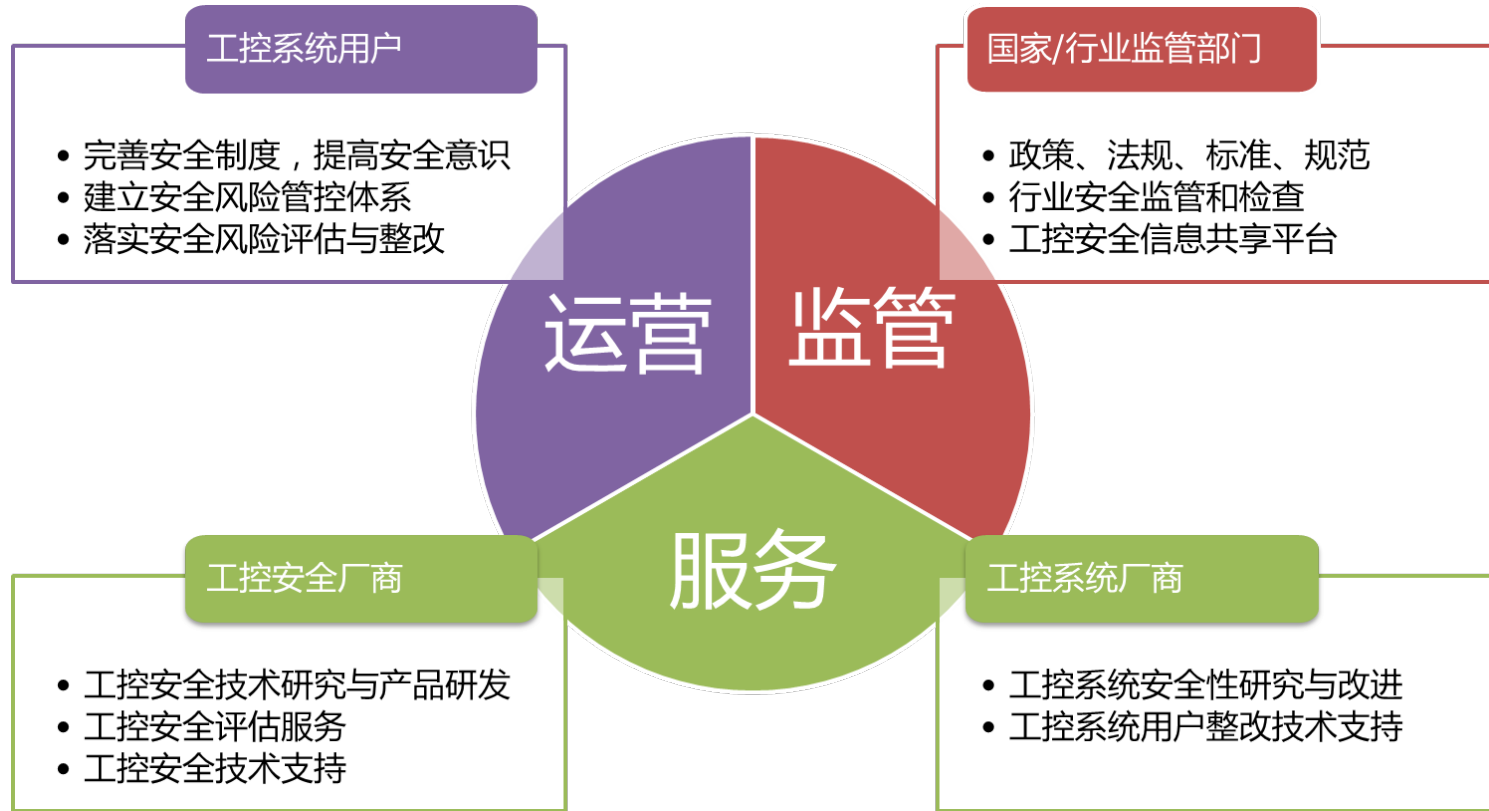
CNCVE编号 CNCVE-20130664

关闭

- 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





- 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



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