中国电信
CHINA TELECOM

工业行业安全认证培训

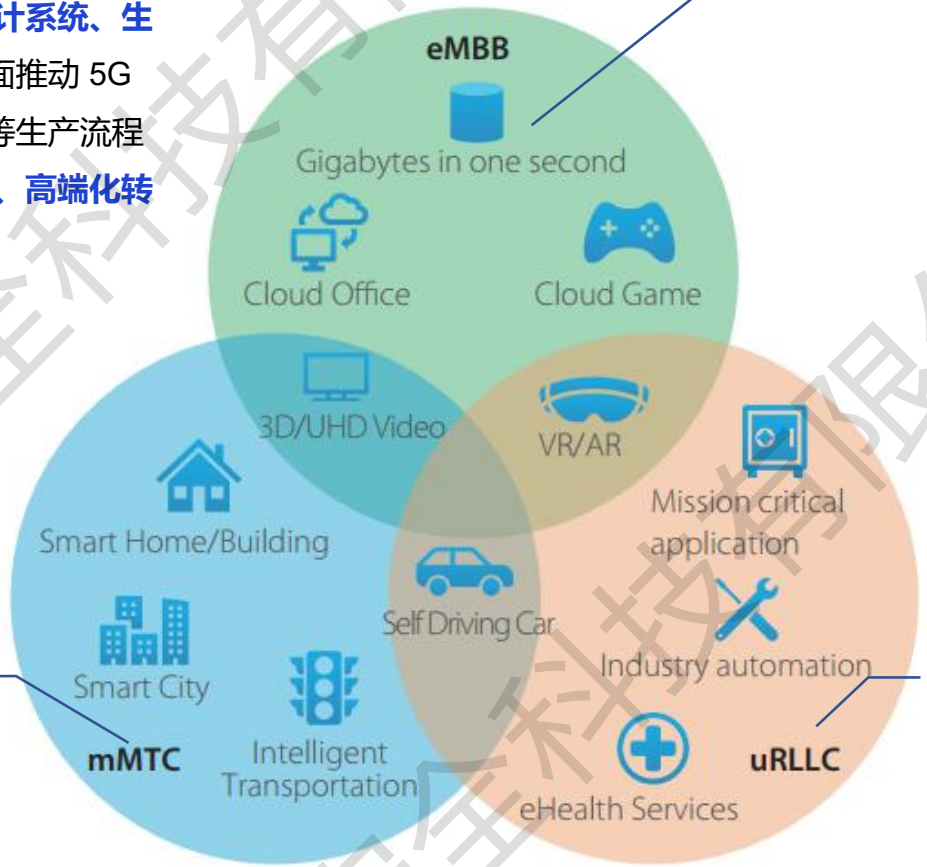
电信安全
China Telecom
Cybersecurity Tech

www.ctct.cn

01 工业安全介绍

5G+工业互联网的应用前景

5G 网络提供的 **灵活定制、弹性部署、多层次隔离、高可靠低延时** 等智能网络能力与工业生产中**研发设计系统、生产控制系统及服务管理系统等相结合**，可以全面推动 5G 工业互联网的研发设计、生产制造、管理服务等生产流程的深刻变革，实现 **工业网络向智能化、服务化、高端化转型**。



eMBB在工业互联网中的应用场景

增强型移动宽带，大带宽，峰值带宽超10Gbps

- 5G+机器视觉质检
- 5G+ 智能制造中的工业巡检无人机
- 5G+ 智能电网中的高空巡检机器人

mMTC在工业互联网中的应用场景

大规模机器通信业务，>1M连接/km2

- 5G+ 工业制造中的工业可穿戴
- 5G+ 制造环境中有害气体及温度检测

uRLLC在工业互联网中的应用场景

超高可靠低时延通信业务，时延<5ms，可靠性>99.999%

- 5G+ 港口中的远程操控桥吊作业
- 5G+ 矿山中的远程操控挖掘机、无人矿卡

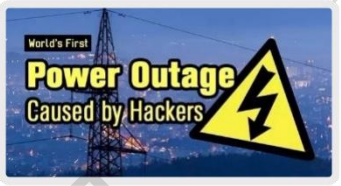
工控领域网络安全威胁事件

两化深度融合，推进了工业行业智能化升级转型建设，同时加速了传统信息安全问题在工控领域的延伸。

另一方面，针对工业控制系统的网络入侵破坏活动频现，造成重大生产事故，甚至危害人身财产安全。

针对工控系统恶意软件 BlackEnergy

2015 年 12 月 23 日乌克兰电力系统遭受攻击，黑客将 BlackEnergy 恶意软件植入乌克兰电力部门，造成电网故障并导致伊万诺 - 弗兰科夫斯克地区大约一半的家庭停电 6 小时。



2015年12月

针对工控系统恶意软件 Triton/Trisis

2017年下半年，恶意软件 Trisis（又称为 TRITON）利用了施耐德 Triconex 安全仪表控制系统（SIS，Safety Instrumented System）零日漏洞对中东一家石油天然气工厂发起网络攻击，导致工厂停运。

2016年12月

勒索病毒+管理失职

2018 年 8 月 3 日晚，台积电在台湾的三处生产基地，遭到 WannaCry勒索病毒入侵，生产线全数停摆。各厂区直到8月 6 日才陆续全部恢复正常生产。这一事件直接影响台积电三季度 3% 的营业收入，公司的毛利润率下降一个百分点。

2018年8月

勒索病毒+数据泄露

特斯拉、波音、洛克希德·马丁公司和 SpaceX 等行业巨头的精密零件供应商，遭受勒索软件 DoppelPaymer 攻击，泄漏与特斯拉和 SpaceX 签署的保密协议。

2020年3月

ICS漏洞难题

工业控制系统的漏洞频发，而且呈现出愈演愈烈的趋势。

2022年上半年，爆出了637个漏洞，涉及73个工业控制系统供应商。

其中有13%的漏洞是“永久漏洞”，没有补丁，且可能永远无法修复。

截至目前（2023年初），工控系统漏洞已达3100+。

截至目前

相关安全法规和政策

顶层法律

《中华人民共和国网络安全法》2017年6月1日开始实施

第三章 网络运行安全 —— 第二节 关键信息基础设施的运行安全

第三十一条 国家对关键信息基础设施，**在网络安全等级保护制度的基础上，实行重点保护。**

《中华人民共和国密码法》2020年1月1日开始实施

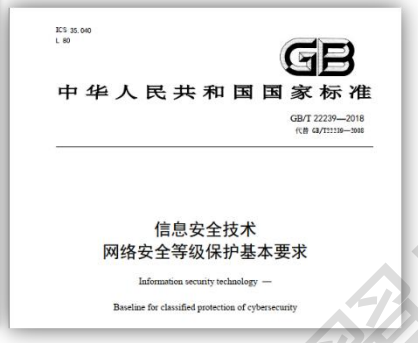
第三章 商用密码安全

第二十七条 要求使用商用密码进行保护的关键信息基础设施，应当**使用商用密码进行保护**，自行或者委托商用密码检测机构**开展商用密码应用安全性评估。**

国家安全标准

《GB/T 22239 网络安全等级保护基本要求》

2019年12月1日开始实施



8.1章节，规范了定级为第三级的信息系统的共性安全要求，即：**安全通用要求。**

8.5章节：规范了定级为第三级的工业控制系统的扩展安全要求，即：**工业控制系统安全扩展要求。**

附录G，**工业控制系统应用场景说明**，参考标准IEC 62264-1的层次结构模型划分，给出了ICS系统**5级划分模型**。

《GB/T 39204 关键信息基础设施安全保护要求》

2023年5月1日开始实施

第8章节，要求关键信息基础设施需要：

- 自行或委托网络安全服务机构，每年至少一次检测评估。
- 内部不限于国家、行业网络安全制度落实情况，等级保护落实情况，商用密码安全性评估情况，数据安全防护情况，供应链安全保护情况，风险评估情况，应急演练情况，攻防演练情况……
- 尤其关注跨系统、跨区域间的信息流动，以及资产的安全防护情况。

行业政策要求

国务院印发

《关于深化“互联网+先进制造业”发展工业互联网的指导意见》

2017年11月27日

工信部与国资委等十部门联合印发

《加强工业互联网安全工作指导意见》

2019年8月28日

工信部印发

《工业互联网创新发展行动计划（2021-2023年）》

2020年12月22日

工信部印发

《开展工业互联网企业网络安全分类分级管理试点工作的通知》

2021年1月13日

工信部印发

《关于开展工业互联网安全深度行活动的通知》

2022年5月13日

关于工业互联网企业的网络安全分级分类管理

等级	计分	推进工作	
三级	评分大于等于80分	企业清单定期报工业和信息化部； 建设企业级工业互联网安全监测平台，并接入属地省级工业互联网安全监测平台；每年一次符合性评测和风险评估；每年至少开展一次应急演练。	对标等级保护标准第三级要求
二级	评分大于等于60分，小于80分	鼓励建设安全监测平台，接入属地省级监测平台。每两年开展一次符合性评测和风险评估。每两年至少开展一次应急演练。	对标等级保护标准第二级要求
一级	评分小于60分	参照二级企业相关要求落实安全防护措施。	

1. **建立健全网络安全责任制**
   工业互联网企业主要负责人为网络安全第一负责人，开展网络安全责任制、网络安全管理制度、应急处置机制等安全工作的推进、落实及完善
2. **落实网络安全总体规划**
   企业应当根据自身信息化实际发展情况，结合网络安全总体规划制定合理、稳定、持续、可行的安全建设方案
3. **建设网络安全监测预警平台**
   企业应建立网络安全监测预警平台，与省级平台对接，完善工作机制，建立持续、有效协同工作，加强安全监测技术能力。
4. **开展符合性评测与风险评估**
   建立/接入网络安全监测预警平台之后，仍需对企业的风险实现闭环管理工作，以管理风险为核心，不断完善企业安全防护能力。
5. **完善网络安全事件应急方法**
   当发现重大网络安全风险和事件时，应具备安全应急处理能力，能够快速、及时、有效处理相关安全问题，及时向主管部门、通信管理局报告。

5G+工业互联网的新型安全风险和威胁

5G引入的安全风险

边缘计算风险

MEC部署下沉到了网络边缘，会导致包括终端、应用和平台等元溯暴露在不安全的环境中，带来新的威胁。

- MEC能力开放服务的越权访问
- 源自MEC接口的DDoS攻击，APP对UPF的恶意攻击
- 来自恶意软件注入MEC平台，导致的信息泄露
- 内部合法用户的恶意操作、日志篡改、数据删除等

5G网络切片，虚拟专网弱化边界

传统物理边界和传统安全防护手段不能适用虚拟专网边界。

- 切片间资源竞争，造成网络时延、干扰和攻击
- 切片非授权访问，造成信息拦截、窃听
- 切片的通信接口被攻击，可能造成数据机密性和完整性破坏
- 网络切片在与第三方交互时，可能遭遇API攻击

两化融合引入风险

以前相对隔离的生产设备、各种新增的传感器和其他控制器，现在成为了5G+工业互联网融合网络中的新端点，极大的增加了系统的暴露面，面临更多的安全风险。

工业互联网的安全威胁

漏洞威胁

- 专用终端的操作系统漏洞（工控专用终端强调可用性，所以普遍使用较低版本终端）
- ICS专用设备漏洞（ICS系统漏洞发现的数量越来越多，涉及的专业制造商越来越多，且因为存在互联网接入，使得威胁放大）

针对ICS系统的定制恶意软件

自2012年，Stuxnet横空出世，十年以来针对ICS系统的新型恶意软件不断涌现，并且呈现出针对工控系统中特定细分领域的态势。

- BlackEnergy / CrashOverride / Industroyer，针对电网系统，可造成供电中断，变电站故障，导致断电。
- Havex，针对工业设备制造商，置入RAT后门，有间谍软件特点
- Triton / Trisis，针对SCADA系统，可控制涡轮等器件的转速，引发恶性的生产事故。

工业通信协议缺陷

工业通信协议缺乏身份认证、授权和加密等安全机制，易被利用。工业互联网会将这个威胁放大。

另一方面，为了规避这个缺陷，意味着停产并全面更新系统和设备，往往难以承受。

工控系统的业务特点

高可用性特点

网络性能

- 实时通信
- 响应时间非常关键
- 吞吐量要求不高
- 不允许延迟和抖动

业务连续性

- 不允许重启系统
- 部署新系统/设备不能造成中断，需要详尽测试
- 中断需要计划任务

风险管理

- 风险发生，必须要有容错机制，任何计划外停机不可接受
- 人身安全最重要，其次是控制过程的高可用性

高专用性特点

系统和设备生态

- ICS系统和设备以特定工业过程为目标进行设计，没有足够的资源来扩展支持安全功能
- 使用无内置安全功能的专有操作系统
- 系统/设备上线之前需要严格线下测试

基础设施生态

- 主流的设备供应商，通常也会有专有的通信协议，如Modbus（施耐德电子）、S7（西门子）
- 因响应时间敏感性，工控通信协议还需进行升级优化，以叠加安全需求（如加密、认证等）

持久性特点

- ICS系统和设备所要求的售后服务支持通常长达15~20年
- 设备一经采购更换，需要运转很长时间，在此期间发现的漏洞问题，很多无法通过软件升级形式解决，只能考虑其他规避措施。

供应链特点

- 无论是专有设备还是软件系统，通常仅有单一供应商（专业性和历史惯性使然）
- 需要严格的供应链管控制度和流程，严控供应链安全风险

5G+工业互联网，网络安全实现架构图

安全基座
等保2.0合规（通用+工控+云计算），智能安全运营

安全管理和运营
安全团队、制度、流程的建设

关基合规+提质增效
关保合规，主动防御

关基合规+提质增效

安全技术

- 内外网攻击面管理
- 访问控制策略可视化与管理
- 数据安全全周期管控
- 干扰/溯源能力

安全管理和运营

- 检测评估
- 监测预警
- 供应链安全管理
- 数据安全治理

安全管理

- 管理人员
- 管理制度
- 管理机构
- 建设管理
- 运维管理

安全基座

企业资源层安全技术体系

安全管理中心	安全态势感知系统		
	统一威胁检测	SIEM	SOAR
安全计算环境	安全区域边界	安全通信网络	
WAF/云堤·网站安全专家	网络准入		
漏洞和基线管理系统	网络审计/NDR	云堤·域名无忧	
堡垒主机	IPS/防病毒墙	云堤·抗D	
EPP/EDR/防病毒	NGFW/微隔离	VPN/SDP	
安全池			
身份安全	密码安全	信创安全	

工控系统安全技术体系

安全管理中心	工控安全态势感知系统	
	日志审计与分析	工控安全管理系统
安全计算环境	工控主机身份认证	工控主机基线管理
	工控主机防病毒	工控内外联检测
安全区域边界	工控安全监测与审计系统	
	工控入侵检测	
安全通信网络	工控防火墙	
	工控网闸	
身份安全	密码安全	信创安全

安全运营

- 安全培训
- 安全演练
- 信息共享
- 风评+加固
- 应急+重保

02 工业安全基座

一、安全基座 —— 总图

安全基座
等保2.0合规（通用+工控+云计算），智能安全运营

安全管理和运营
安全团队、制度、流程的建设

关基合规+提质增效
关保合规，主动防御

关基合规+提质增效

安全技术				安全管理和运营			
内外网攻击面管理	访问控制策略可视化与管理	数据安全全周期管控	干扰/溯源能力	检测评估	监测预警	供应链安全管理	数据安全治理

安全管理

- 管理人员
- 管理制度
- 管理机构
- 建设管理
- 运维管理

安全基座

企业资源层安全技术体系

安全管理中心	安全态势感知系统		
	统一威胁检测	SIEM	SOAR
安全计算环境	安全区域边界	安全通信网络	
WAF/云堤·网站安全专家	网络准入		
漏洞和基线管理系统	网络审计/NDR	云堤·域名无忧	
堡垒主机	IPS/防病毒墙	云堤·抗D	
EPP/EDR/防病毒	NGFW/微隔离	VPN/SDP	
安全池			
身份安全	密码安全	信创安全	

工控系统安全技术体系

安全管理中心	工控安全态势感知系统	
	日志审计与分析	工控安全管理系统
安全计算环境	工控主机身份认证	工控主机基线管理
	工控主机防病毒	工控内外联检测
安全区域边界	工控安全监测与审计系统	
	工控入侵检测	
安全通信网络	工控防火墙	
	工控网闸	
身份安全	密码安全	信创安全

安全运营

- 安全培训
- 安全演练
- 信息共享
- 风评+加固
- 应急+重保

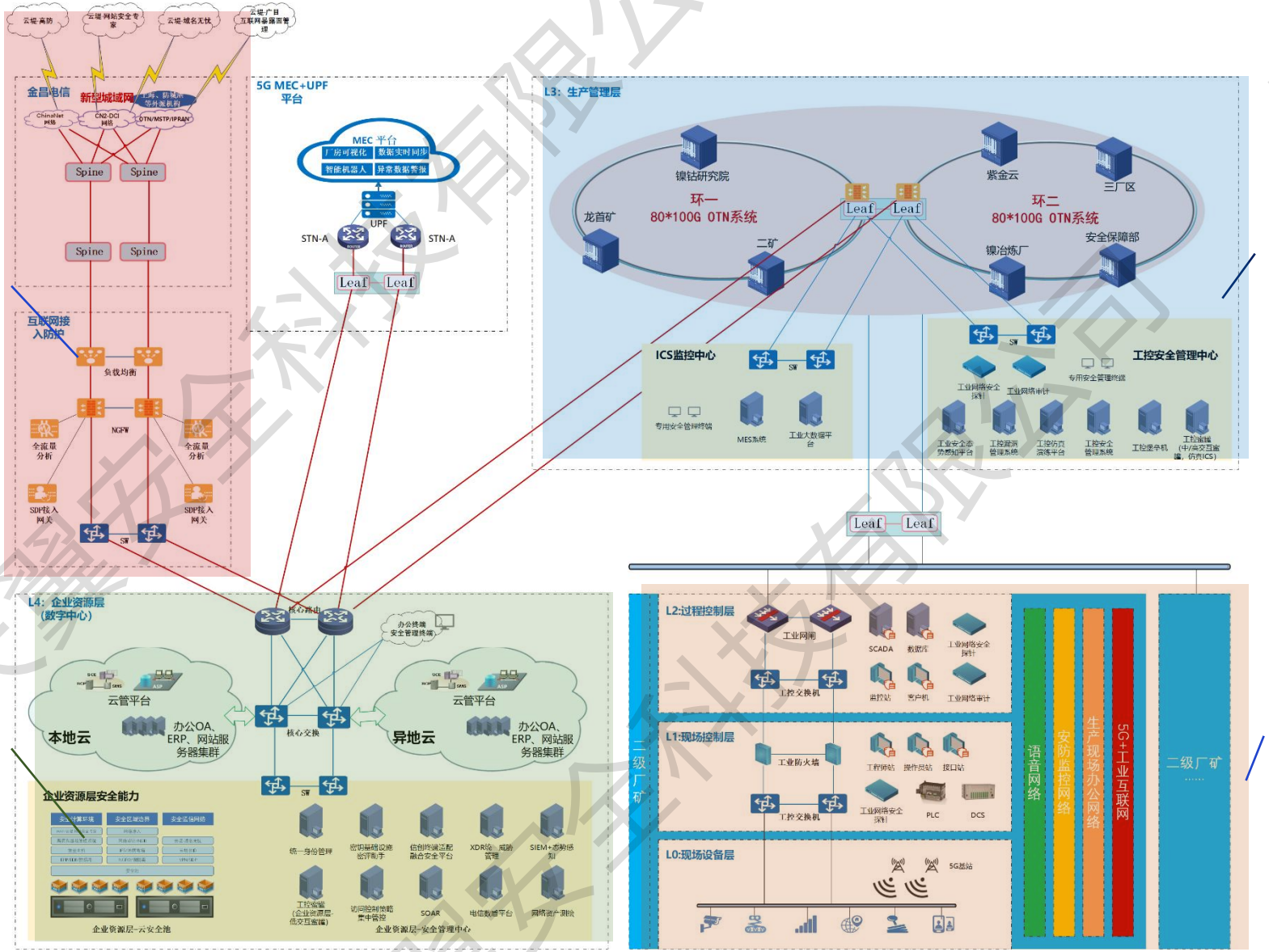
一、安全基座 —— 安全拓扑示意

互联网接入安全

- 双链路接入线路，结构安全
- 互联网威胁防范
- 电信云堤大网安全能力（DDoS高防、域名无忧、网站安全专家、广目）
- 远程办公接入安全
- 流量侧安全分析

L4：企业资源层安全管理

- 云安全池（提供云内各项安全能力）
- 身份安全基础设施
- 密码安全基础设施
- 信创安全基础设施
- 统一威胁和响应管理
- 数盾
- 攻击面管理
- 工控蜜罐



L3：生产管理层安全管理

- 工业安全态势感知
- 工控漏洞管理系统
- 工控仿真演练平台
- 工控安全管理系统
- 工控堡垒机
- 工控蜜罐

L0-L2：安全管理

- 层级间隔离（工控网闸、防火墙）
- 工控主机安全
- 工控安全探针
- 工控安全审计

一、安全基座 —— 工控安全等保合规 – 安全隔离

划清安全域、做好隔离

工业防火墙

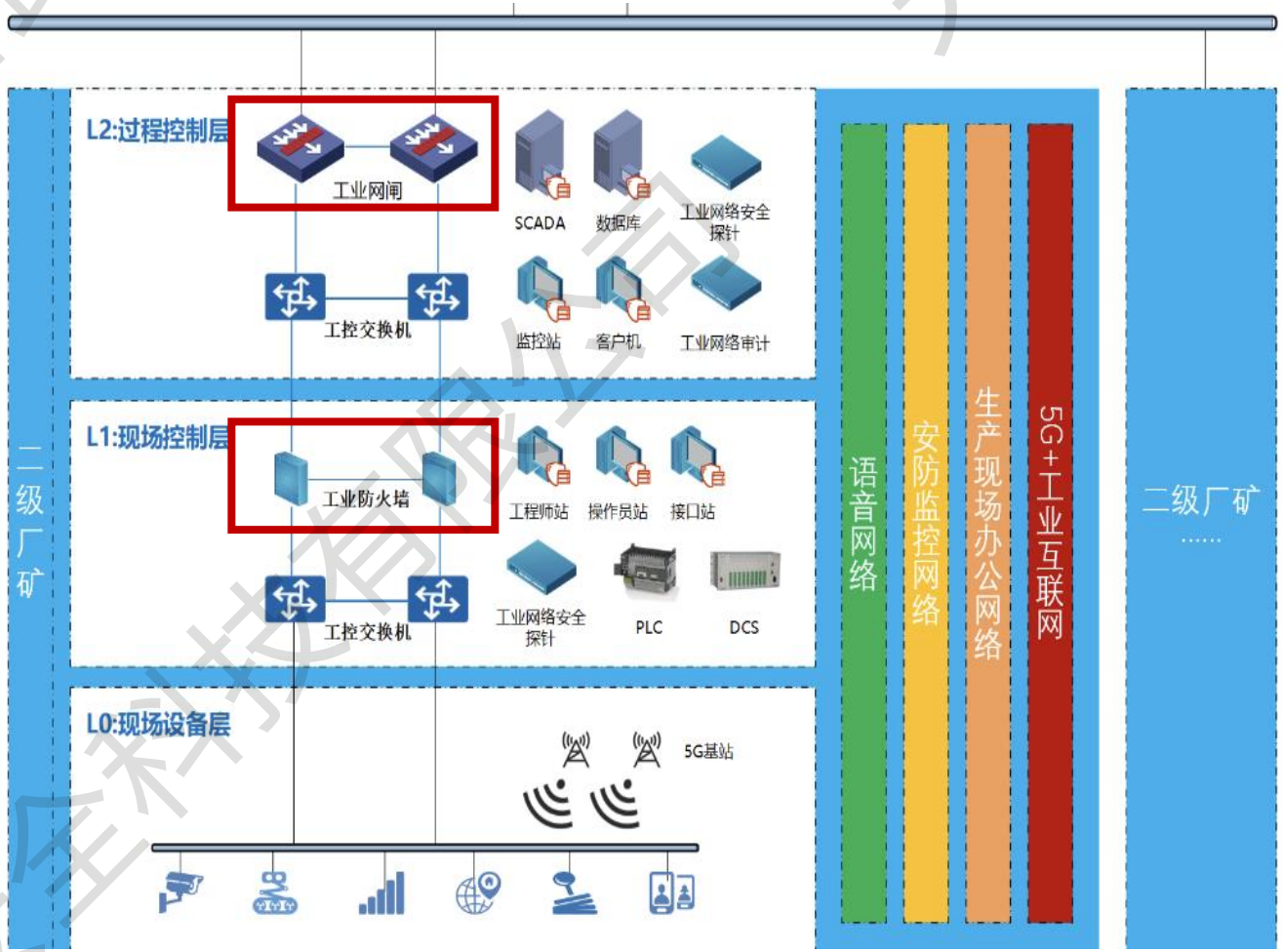
- 工业网络环境，宽温，无风扇，导轨/机架
- 工业控制协议解析控制，防病毒，应用识别
- 硬件Bypass（电口/光口）

工业网闸

- 不同安全域间的访问控制、协议转换、内容过滤和信息交换等
- 全封闭、无风扇、多电源冗余

隔离位置

- 各个作业区之间的隔离



一、安全基座 —— 工控安全等保合规 – 审计和检测

提高网络内、外入侵和恶意代码防御能力

工业控制系统指令级网络审计

及时发现高风险的潜在威胁

数据服务层对攻击的实时检测

已知/未知威胁深度包检测

网络流量采集分析 → 网络通信行为建模 → 网络异常行为监测 → 记录审计事件回溯

广泛采集分析，为后续模型的建立打下基础

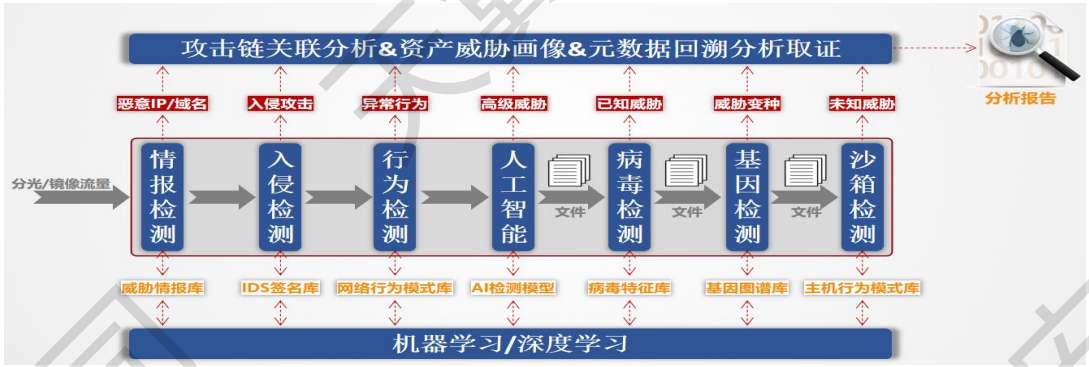
建立工控通信模型基线，为异常行为判定提供依据

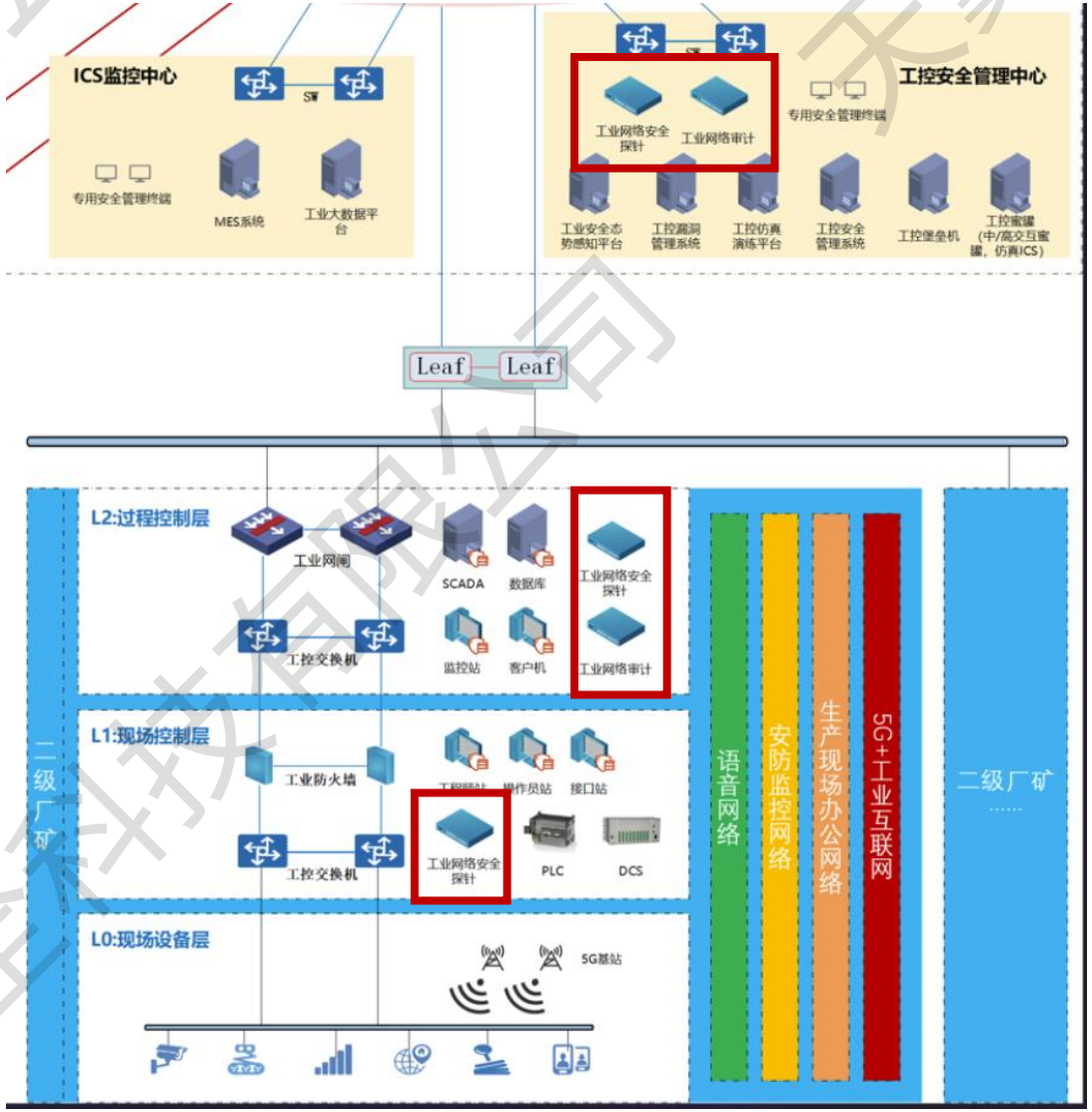
实时监测异常行为，持续识别现网威胁

为工业控制系统的安全事故调查提供详实的依据

事前 | 事中 | 事后

- 流量采集与协议深度解析，全量收集客户现场中使用的各类指令与功能码
- 通过智能自学习建立网络通信行为基线，包括连接基线与流量基线，构建判定异常行为的依据
- 将现网流量与建立的通信模型进行比对，对偏离白名单的行为、超出基线的波动进行告警
- 支持对流量的实时、历史的图形化统计
- 支持多维度的告警事件统计和回溯

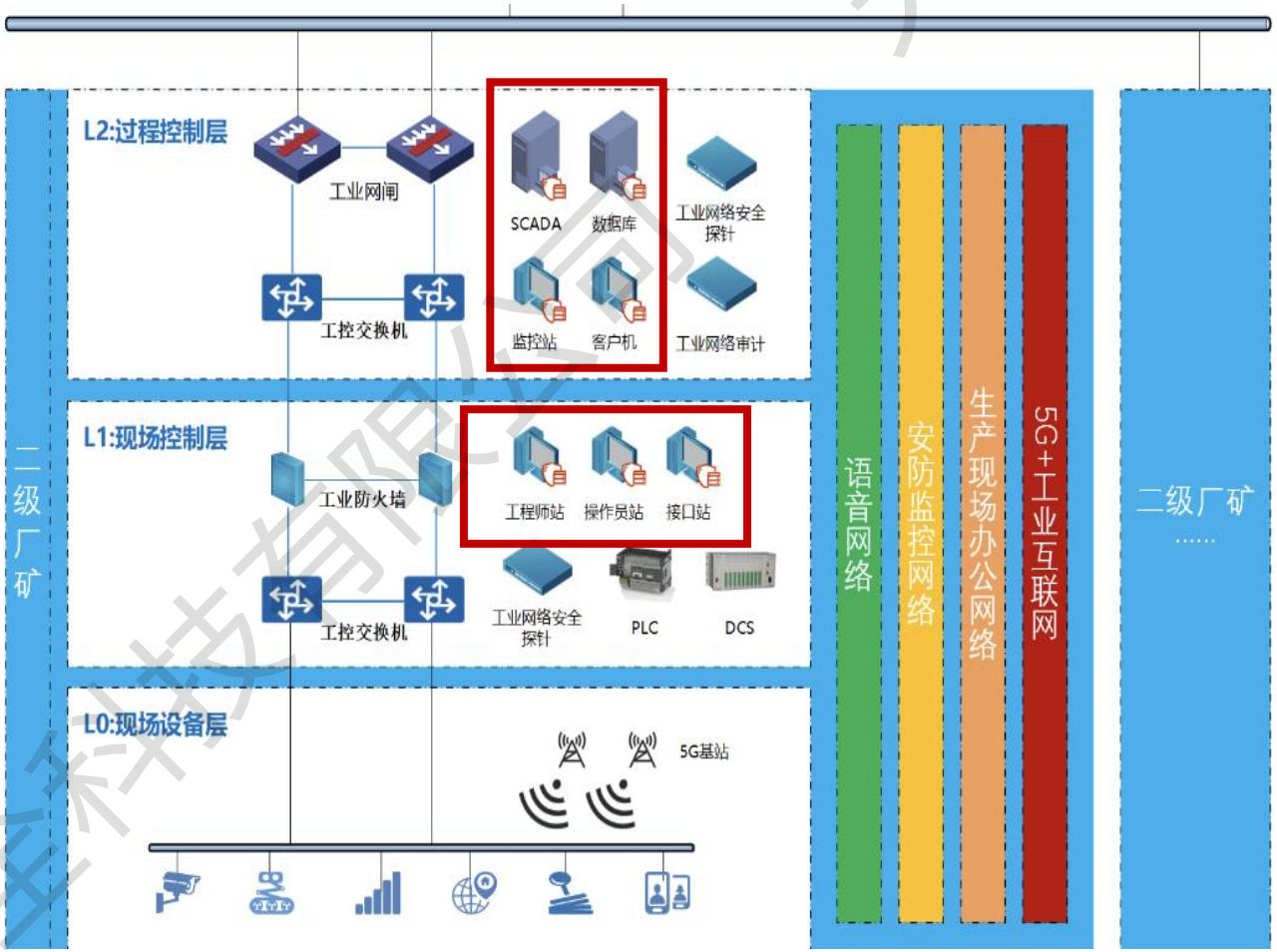




一、安全基座 —— 工控安全等保合规 – 主机安全

打造主机运行白环境

基于智能匹配的白名单管控技术、基于ID的USB移动存储外设管控技术、以及入口拦截、运行拦截、扩散拦截关卡式病毒拦截技术，防范恶意程序的运行、非法外设接入，从而进行全面的工业资产、安全风险集中管理，实现对工业主机的安全防护。



一、安全基座 —— 工控安全等保合规 – 平台管控

工控安全管理系统

- 统一收集各类工控安全能力日志，以及工控系统日志
- 进行日志关联分析，发现违规、恶意行为，并上交态势感知系统进行呈现

工控仿真演练平台

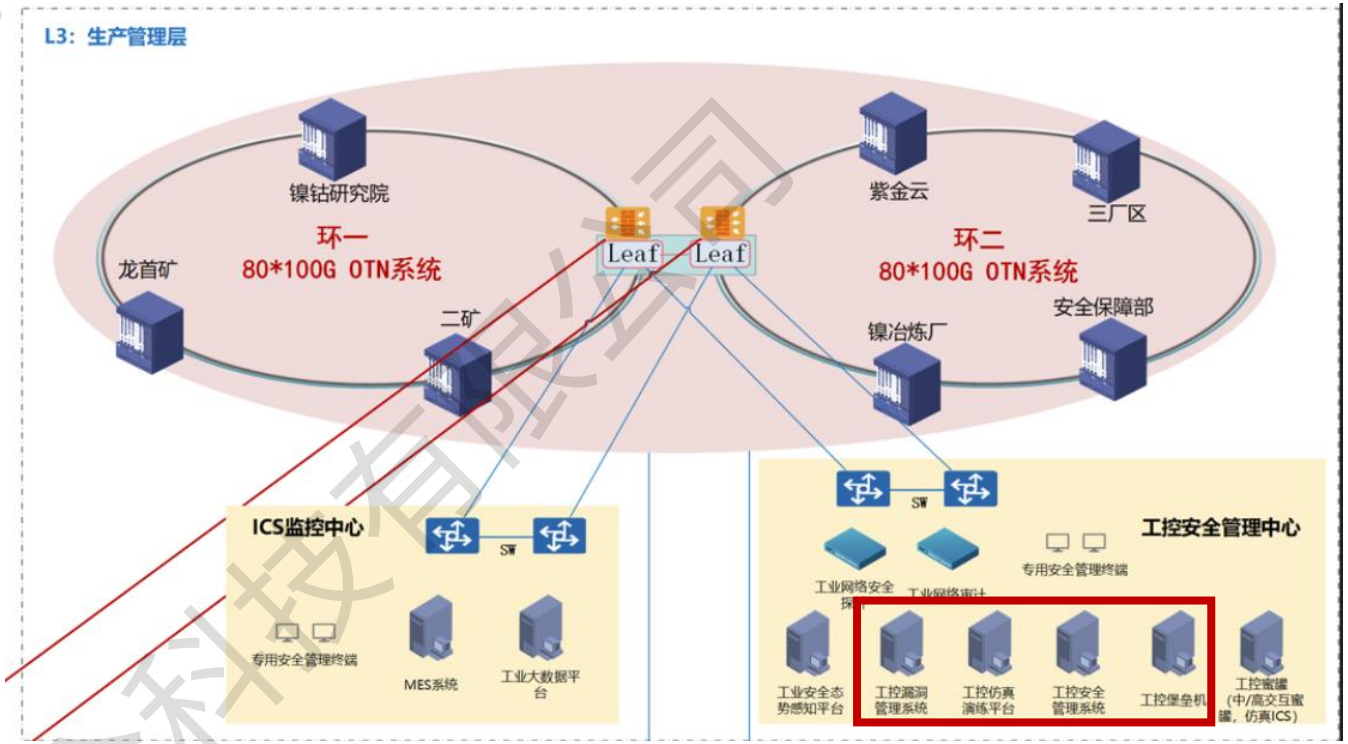
- 通过模拟针对工控系统发起的攻击渗透行为,直观展现攻击行为导致生产中止的影响和危害,验证阻断攻击的安全防护措施的有效性

工控漏洞管理系统

- 针对工业现场的控制设备、数字化设计制造软件以及控制系统的已知漏洞进行扫描、识别和检测,生成脆弱性评估报告,清晰定位系统脆弱性风险,给出漏洞修复建议和预防措施

工控堡垒机系统

- 基于认证、授权、访问、审计的管理流程设计理念，实现对网络设备、数据库、安全设备、主机系统、中间件等资源统一运维管理和审计；通过集中化运维管控、运维过程实时监管、运维访问合规性控制、运维过程图形化审计等功能，构建一套事前预防、事中监控、事后审计完善的安全管理体系。



一、安全基座 —— 工控安全等保合规 – 工控网络安全态势感知

工业态势感知打造工业安全“中控室”

“组态化”工业态势

“运营化”工业安全分析中心

- 工业资产管理
- 工业风险管理
- 工业漏洞管理
- 通信视图管理
- 工业知识图谱

预测管理 ③

协同防护 ④

- 工业主机防护
- 工业边界防护
- 工业数据防护
- ……

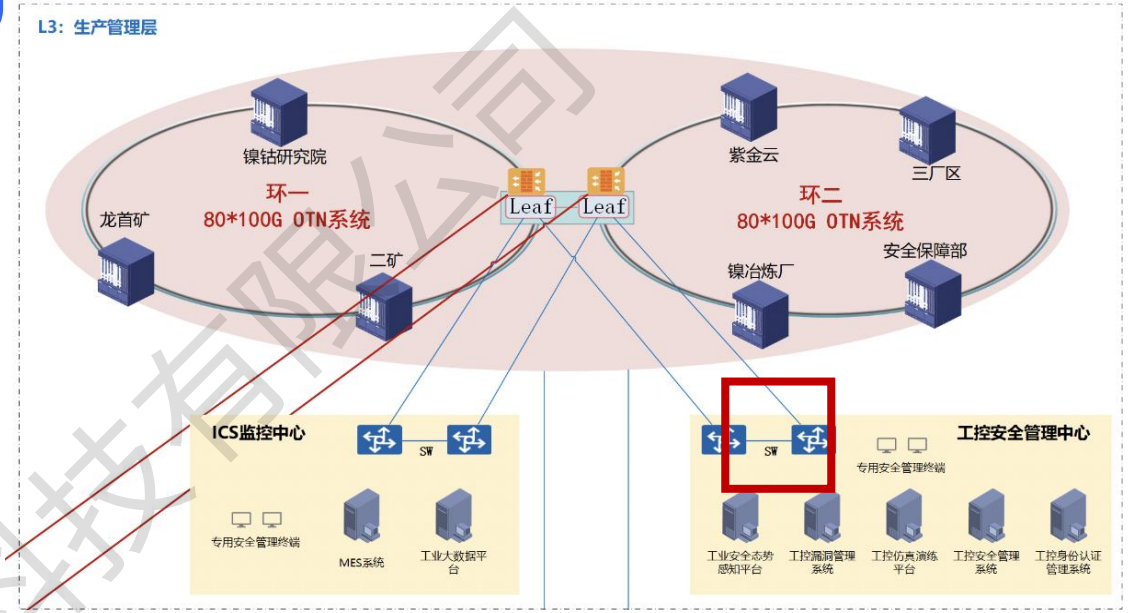
② 积极响应

- 调查分析
- 溯源取证

① 持续检测

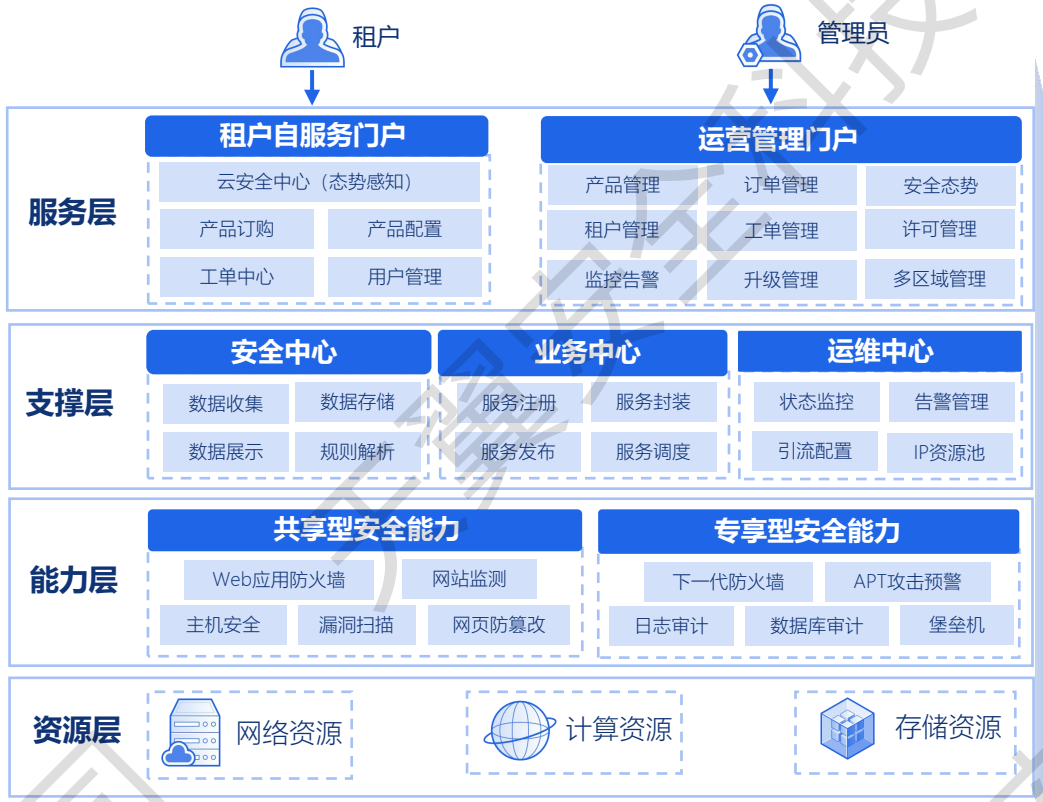
流量检测
- 工业资产发现
- 工业漏洞识别
- 工业威胁检测

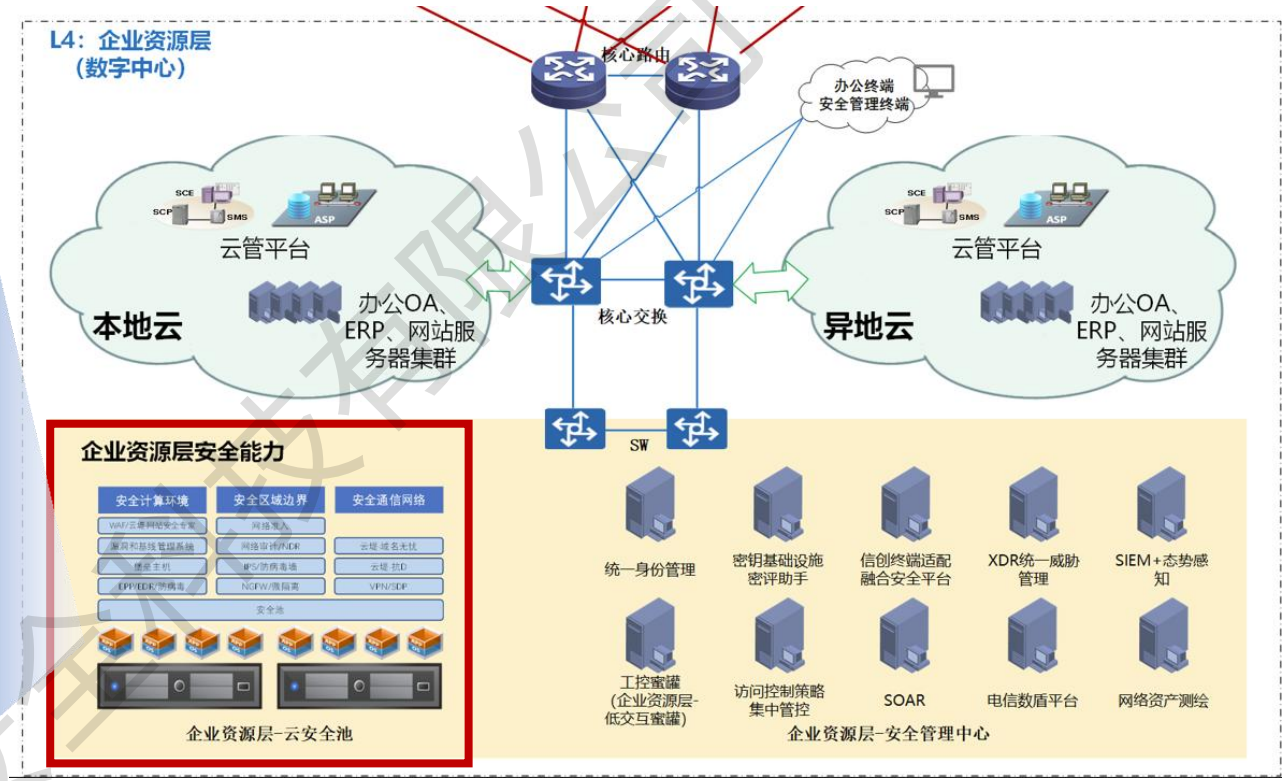
安全分析
- 工业威胁情报
- 威胁关联分析
- 工艺异常行为分析
- 资产非法接入/外联



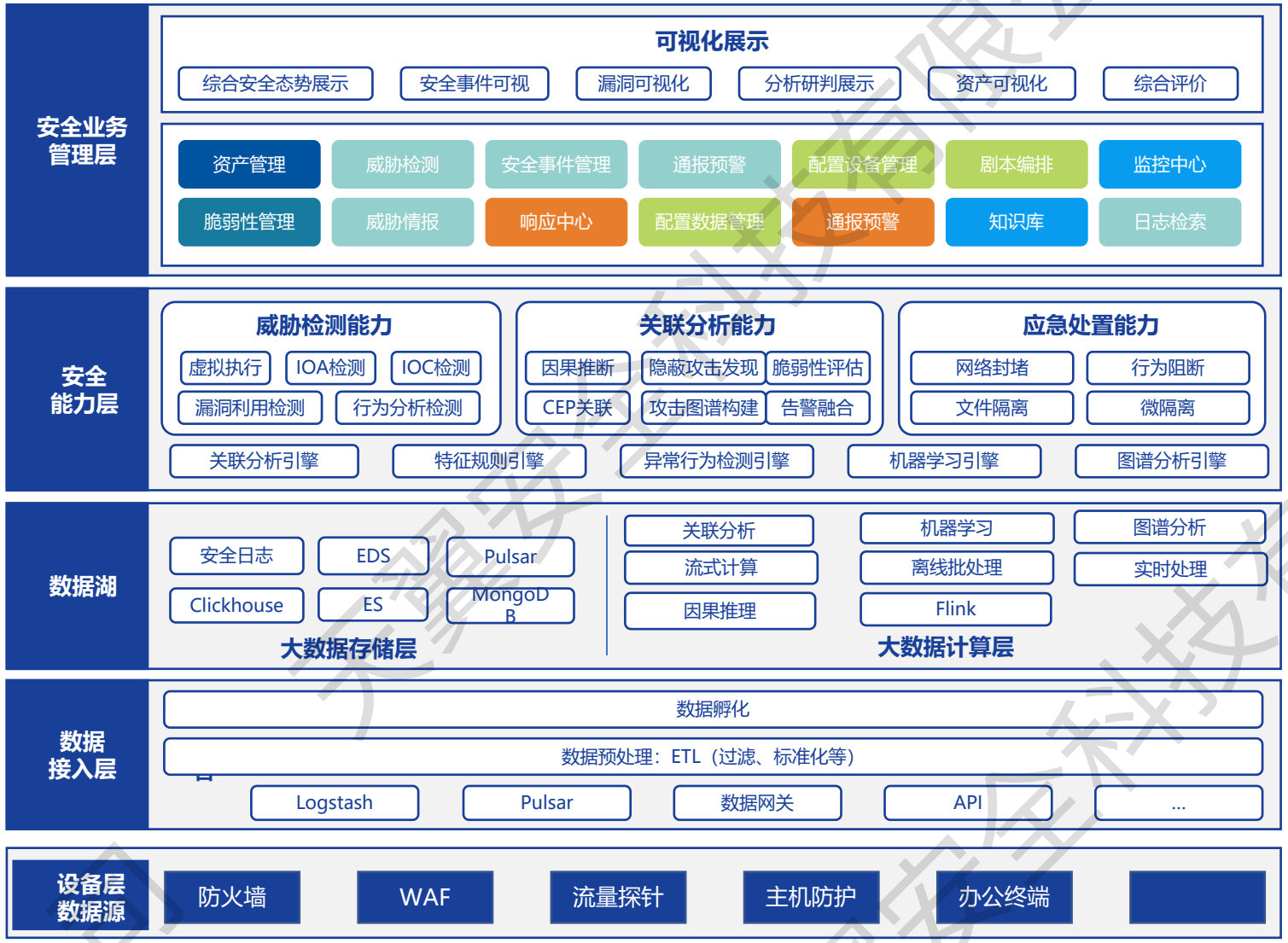
一、安全基座 —— 企业资源层安全合规，安全云原生化赋能

面向多云、混合云场景，利用虚拟化技术，集成检测类、防护类、审计类十余种安全能力，为用户提供一站式云安全综合解决方案。通过自身先进的技术架构、完善的安全能力、丰富的管理功能、灵活的部署方式，帮助用户轻松实现云上等保合规，并构建智能化的云安全防护体系。





一、安全基座 —— 统一威胁和响应管理-XDR



要求

安全防护-入侵防范：

- 应采取技术手段，提高对高级持续威胁（APT）等网络攻击行为的入侵防范能力
- 应采取技术手段，实现系统主动防护，及时识别并阻断入侵和病毒行为

关键价值

- **集中的威胁判断和分析能力：**统一采集各类具备安全检测、威胁监测设备/软件的安全数据，通过一手数据聚合、上下文情景关联、快速精准溯源能力，可提升调查速度，缩短处置时长
- **自动智能+人工专家分析：**采集网端一手数据上下文关联分析，云端专家持续进行威胁狩猎和检测确认，平台持续进行检测回扫，不漏过任何一起可疑攻击。响应处置闭环更快速

一、安全基座 —— 统一威胁和响应管理-态势感知

要求

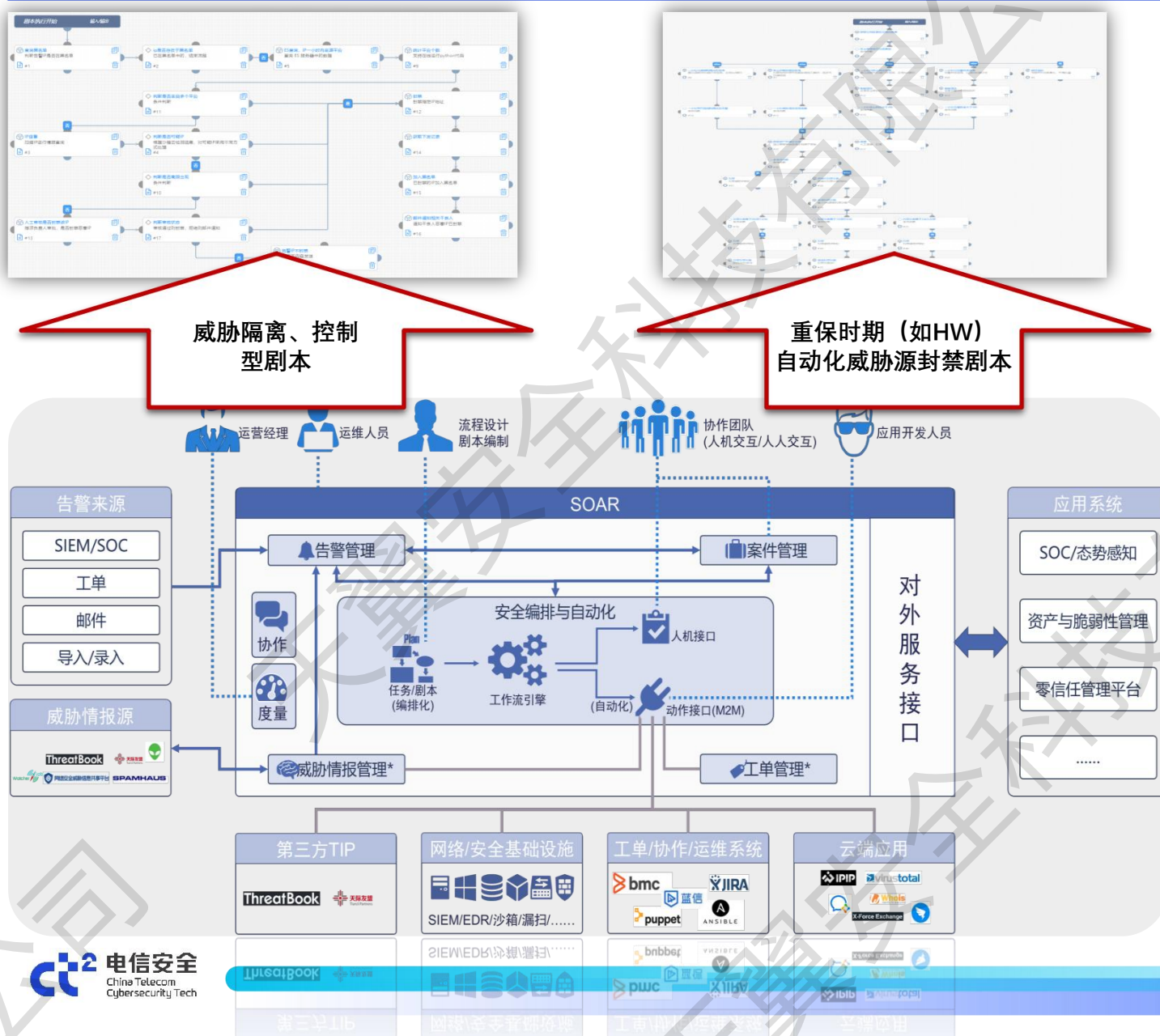
事件处置：

- 应采用自动化机制，对关键业务所涉及的系统的所有监测信息进行整合分析，以便及时关联资产、脆弱性、威胁等，分析关键信息基础设施的网络安全态势。
- 应全面收集网络安全日志，构建违规操作模型、攻击入侵模型、异常行为模型，强化监测预警能力
- 应将关键业务运行所涉及的各类信息进行关联，并分析整体安全态势

关键价值

- **安全数据集中存储：**实现海量多源安全数据的集中采集和存储，能够对安全数据进行查询、统计、关联分析，满足合规要求的同时，最大化利用安全数据的价值。
- **提升分析研判效率：**通过场景分析、实体分析、事件调查等威胁分析工具，结合安全运营工作实际场景，帮助提升安全事件研判和溯源的效率，及时进行响应处置。
- **精准检测高级威胁：**通过威胁情报、机器学习、关联分析和基线分析等多个维度进行威胁的检测，提升威胁检测准确度，快速定位真正的威胁。

一、安全基座 —— 统一威胁和响应管理-SOAR



要求

安全运营：

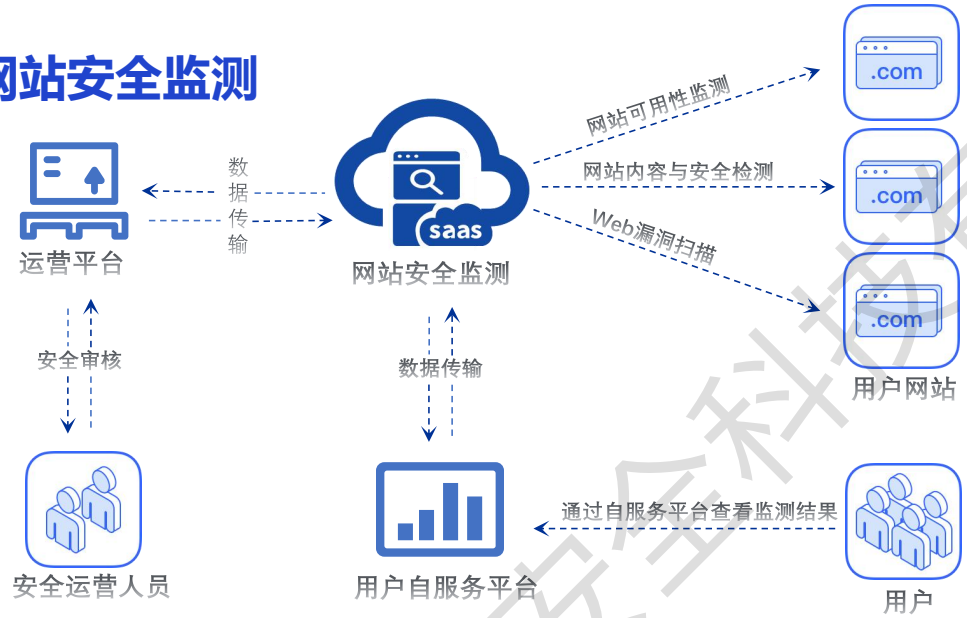
- 当发现可能危害关键业务的迹象时,能自动报警,并自动采取相应措施,降低关键业务被影响的可能性。
- 应按照事件处置流程、应急预案进行事件处理,恢复关键业务和信息系统到已知的状态;

关键价值

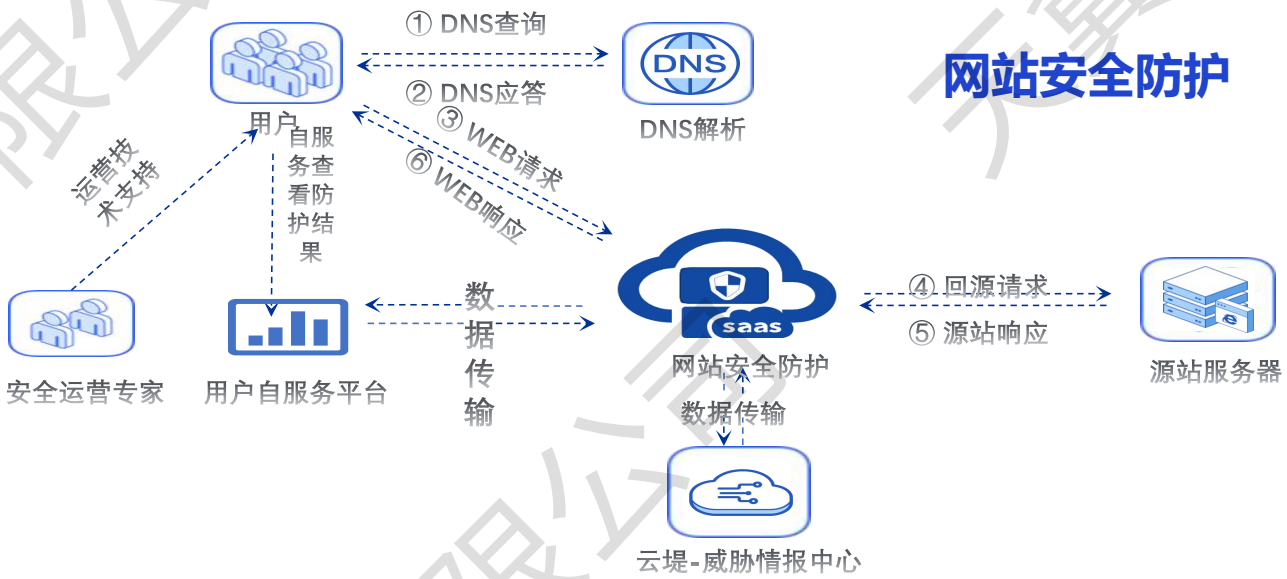
- **整合资源、协同连接：**将分散的工具、人员和流程有机地整合到一起，整合安全运营所需的各种资源，实现人与工具、工具与工具的连接与协作。
- **自动运营、减负增效：**将安全操作流程或其片段转变成编排化的安全剧本，并尽可能自动化的执行，从而大幅降低安全运营人员的工作负担，提升工作效率。
- **快速响应、及时补救：**借助编排与自动化，安全运营人员能够快速进行响应处置，降低平均响应时长。

一、安全基座 —— SAAS化安全能力

网站安全监测



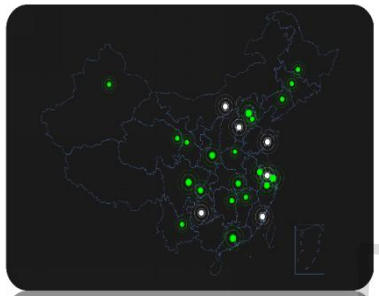
网站安全防护



抗DDOS防护

海外11个防护节点

国内26个省会节点



国内7大云化防护节点

全球部署的分布式近源防护，TB级网络攻击防护

覆盖中国电信全网DNS节点

域名无忧

实时流量监控，秒级全量刷新

域名监控

实时监控全网流量
及时发现域名的恶意篡改

域名修正

电信全网DNS与源站权威DNS的数据同步秒级修正

一、安全基座 —— 身份安全基础设施

企业资源层办公用户

- 双因素身份鉴别
- 最小权限原则
- 办公终端准入
- 杜绝弱口令问题

企业资源层运维人员

- 零信任动态验证，确保风险最低
- 结合堡垒机、特权账号管理，做全程的运维审计，账号权限管控
- 杜绝弱口令问题，缓解账号和权限蔓延问题

工控系统现场工作人员

- 双因素身份鉴别
- 杜绝弱口令问题
- 最小权限原则

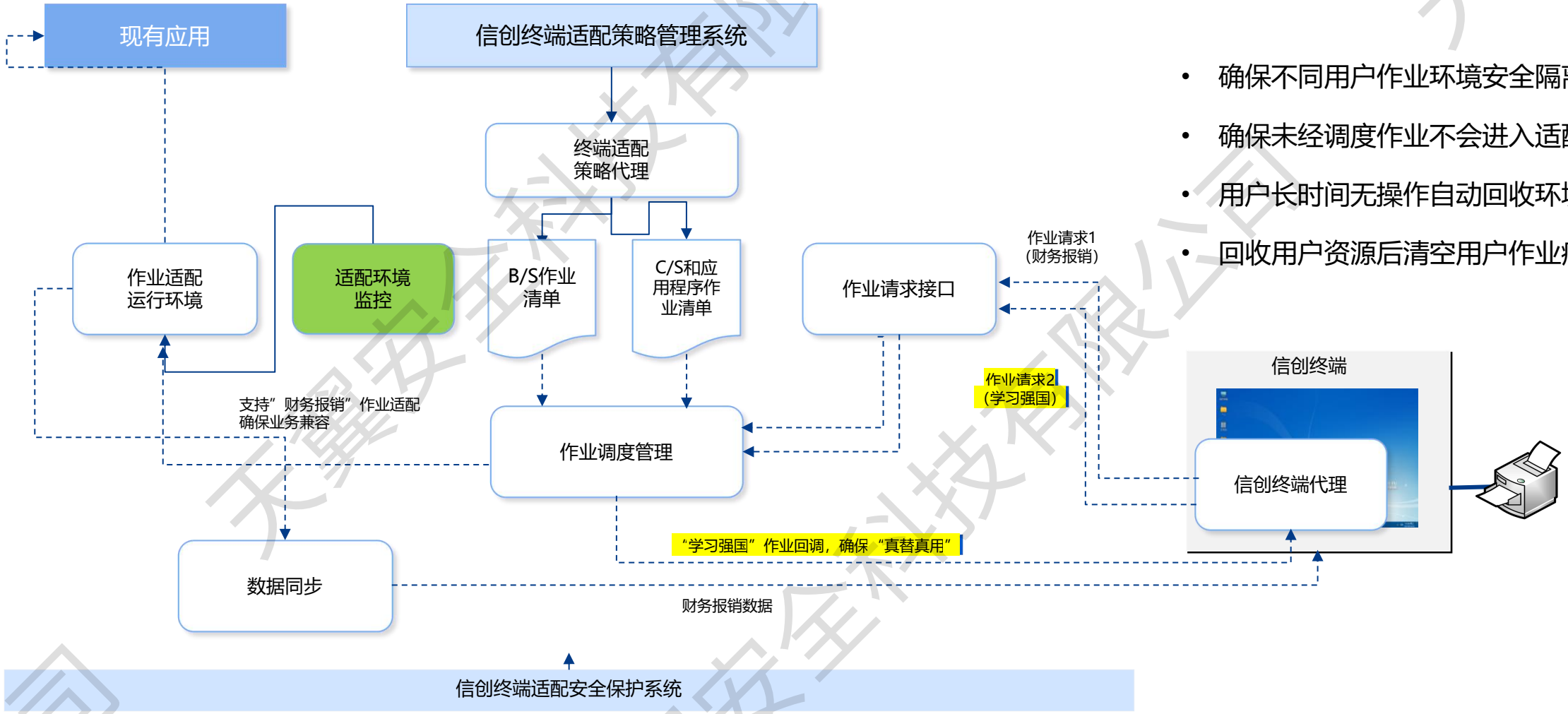
工控系统现场运维人员

- 零信任动态验证，确保风险最低
- 结合堡垒机，特权账号管理，做全程的运维审计，账号权限管控
- 杜绝弱口令问题，缓解账号和权限蔓延问题

一、安全基座 —— 密码安全基础设施

为满足客户在密码应用安全性评估过程中的密码应用合规性需求，中国电信安全公司依托于自有的国产商用密码服务中台，基于《网络安全法》《密码法》《国家政务信息化项目建设管理办法》等政策法规背景，提供“密评助手”服务，涵盖全面、专业的商用密码业务服务，包括密码设计咨询服务、密码原子能力租赁服务、密码应用改造服务、密码测评支撑服务等一揽子密码应用安全服务包。

一、安全基座 —— 信创安全终端



- 确保不同用户作业环境安全隔离
- 确保未经调度作业不会进入适配环境
- 用户长时间无操作自动回收环境资源
- 回收用户资源后清空用户作业痕迹

一、安全基座 —— 提供的价值

体系化设计

以政策为指导，以法律法规为标尺，以相关标准和指南为依据，从等保密评等合规建设、身份安全、统一威胁和响应几个方面提供**一站式安全方案**建设能力，形成**体系化**保障。

综合防护能力

形成网络+工控安全综合防护能力，全天候全方位监控关键生产设备及重要业务系统安全状况，及时**发现、处置、阻断**各类网络安全隐患风险，支撑溯源取证

统一运营

通过长期**整体运营**发现安全管理的薄弱环节，予以强化管理，发现安全体系的短板，予以补足，引入SOAR技术缓解**运营压力，降低成**本，提升运营效率

03 工业安全运营

二、安全运营 —— 总图

安全基座
等保2.0合规（通用+工控+云计算），智能安全运营

安全管理和运营
安全团队、制度、流程的建设

关基合规+提质增效
关保合规，主动防御

关基合规+提质增效

安全技术

- 内外网攻击面管理
- 访问控制策略可视化与管理
- 数据安全全周期管控
- 干扰/溯源能力

安全管理和运营

- 检测评估
- 监测预警
- 供应链安全管理
- 数据安全治理

安全管理

- 管理人员
- 管理制度
- 管理机构
- 建设管理
- 运维管理

安全基座

企业资源层安全技术体系

- 安全管理中心
  - 安全态势感知系统
  - 统一威胁检测
  - SIEM
  - SOAR
- 安全计算环境
  - WAF/云堤·网站安全专家
  - 漏洞和基线管理系统
  - 堡垒主机
  - EPP/EDR/防病毒
- 安全区域边界
  - 网络准入
  - 网络审计/NDR
  - IPS/防病毒墙
  - NGFW/微隔离
- 安全通信网络
  - 云堤·域名无忧
  - 云堤·抗D
  - VPN/SDP
- 安全池
- 身份安全
- 密码安全
- 信创安全

工控系统安全技术体系

- 安全管理中心
  - 工控安全态势感知系统
  - 日志审计与分析
  - 工控安全管理系统
- 安全计算环境
  - 工控主机身份认证
  - 工控主机基线管理
  - 工控主机防病毒
  - 工控内外联检测
- 安全区域边界
  - 工控安全监测与审计系统
  - 工控入侵检测
- 安全通信网络
  - 工控防火墙
  - 工控网闸
- 身份安全
- 密码安全
- 信创安全

安全运营

- 安全培训
- 安全演练
- 信息共享
- 风评+加固
- 应急+重保

二、安全运营 —— 等级保护安全管理体系建设

结合等级保护基本要求—安全管理要求，以及ISO27001标准，在安全管理体系建设的实务中，可将安全管理体系的建设分为现状调研、架构设计和体系建设三个步骤。

一、安全现状调研	二、安全架构设计	三、安全体系建设
1、现场访谈 2、问卷调查 3、技术调查 4、差距分析 5、安全现状现场调研报告	1、网络安全需求分析 2、网络安全战略目标 3、网络安全架构设计 4、网络安全管理总纲 5、安全架构设计报告	1、网络安全策略体系 2、网络安全绩效体系 3、网络安全培训体系 4、管理体系运行计划 5、体系检查评审整改

中国电信本身作为公安部推荐的等级保护测评机构，以等级测评、安全整改、安全服务作为主要服务手段，为客户构建覆盖全面、突出重点、符合实际的安全管理体系。

二、安全运营 —— 人员培训

方法	对象	产品	功能	
全面能力建设	训	人员	实训靶场	理论学习	课后练习
				组网实操	在线考试
	赛	团队	竞赛靶场	理论赛	攻防赛
				解题赛	运维赛
	测	系统	网络靶场	装备效能测试	工业控制仿真
				系统安全测试	超逼真网络环境

目标：工业安全人才培养、工业安全赛事保障、工控系统安全测试、攻防实战仿真对抗

要求

等级保护：

- 应对人员进行**安全意识教育和岗位技能培训**，对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训，并进行定期的**技能考核**。

关基保护：

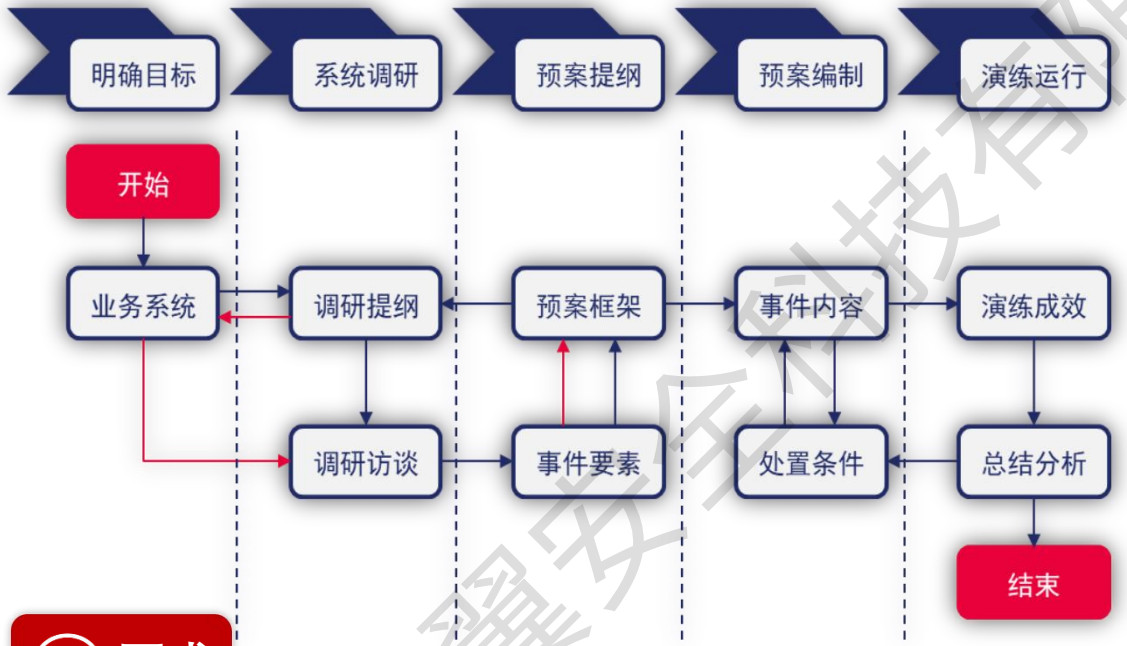
- 建立**网络安全教育培训制度**，定期开展网络安全教育培训和技能考核，关键信息基础设施从业人员每人每年教育培训市场不得少于**30个学时**。教育培训内容应包括网络安全相关**法律法规、政策标准，以及网络安全保护技术、网络安全管理**等。

关键价值

- **人员安全能力提升制度落地**，将企业的网络安全人员能力提升/培训制度进行落地，映射为课程、靶场训练、考试等形式，在满足合规要求基础之上，不断提升各岗位人员网络安全意识和专业技能。
- **贴近自身实际环境的仿真环境**，采用贴近自身信息系统的高仿真环境，评判防护措施、管理流程的有效性，帮助人员快速学以致用。
- **支持演练活动**，工业控制系统仿真，云计算环境仿真，办公环境仿真，为各类型的演练活动提供环境支撑。

二、安全运营 —— 安全演练

应急演练服务



攻防演练服务

红队：攻击小组

- 进行真实攻击
  - 多种协议约束不得私藏和获取客户数据
  - 多种身份认证机制保证身份不可抵赖
  - 全程VPN接入保证过程安全可控

蓝队：客户安全运营团队

- 配合督导方面完成演练方案设计/安全设备的上线部署
- 基于现有防御体系开展红蓝演练的防护工作：
  - 安全设备防御策略优化
  - 安全事件监控/分析/处置
- 安全加固
- 事件追踪溯源

紫军：负责演练导演、协同防守、监控进程、全程指导、应急处置、演练总结、技术措施与策略优化建议等技术咨询工作

要求

关基保护-应急演练：

- 在国家网络安全事件应急预案框架下，根据行业和地方特殊要求，制定网络安全事件应急预案；**每年至少组织一次本组织的应急演练**。

关基保护-攻防演练：

- 围绕关键业务的可持续运行设定演练场景，**定期组织开展攻防演练**。
- 应针对攻防演练中发现的**安全问题和风险进行及时整改**，消除结构性、全局性风险。

关键价值

- **主动防御合规满足：**帮助客户满足关于应急演练和攻防演练活动的合规性要求。
- **检验并促进安全运营活动有效性：**应急演练和攻防演练，均是维护业务连续性的必要的主动性措施，通过演练锻炼安全运营队伍技能，发现问题，完善流程，确保面临真实安全事故发生时的应对有度。

二、安全运营 —— 外部安全信息共享

网络安全咨询和威胁情报通告服务

业界动态

- 安全界的新闻大事，新技术发展动态

国家安全政策及法律法规

- 安全不仅表现在技术层面，还必须符合国家政策、法律、行业规范等。将收集整理这方面的信息，从更广泛的领域帮助客户提升安全水平

热点威胁情报

- 热点恶意软件、安全事故、攻击团伙，及其相关IOC

漏洞预警信息

- 将各种主机、应用、设备等的最新安全漏洞进行通告，包括漏洞的威胁、影响的平台及修补步骤

要求

关基保护-主动防御：

- 应建立**外部协同网络威胁情报共享机制**，与权威网络威胁情报机构开展协同联动，实现**联防联控**。

关键价值

- **保持对威胁信息的与时俱进：**威胁情报共享是通向主动防御的基础措施之一。组织内的网络安全专家和运维人员应时刻保持对可能威胁本组织的威胁信息保持关注。

二、安全运营 —— 风险评估+安全加固

风险评估服务

安全加固服务

要求

关基保护-检测评估：

- 应自行或委托网络安全服务机构，对关键信息基础设施安全性和可能存在的风险，**每年进行一次检测评估**，并及时整改发现的问题。。

关键价值

- **以风险管理为导向的动态防护：**安全风险会随内部业务变化和外部威胁变化而动态变化，因此也需要专业的风险评估和安全加固来动态的处置风险。

二、安全运营 —— 应急响应+重保服务

应急响应服务

应急响应安全服务范围

计算机病毒事件、
蠕虫病毒事件、
特洛伊木马事件、
网页内嵌恶意代码事件、
拒绝服务攻击事件、
后门攻击事件、
漏洞攻击事件、
网络扫描窃听事件、
信息篡改事件、
信息假冒事件、
信息窃取事件。

关键价值

采用高效的信息安全事件响应处置机制对客户网络或业务系统遭到的安全事件快速作出响应，根据安全事件等级，可在第一时间采用现场或远程的方式对安全事件进行应急处置，最大限度地降低安全事故带来的危害，抑制事件影响扩散，帮助客户将损失降至最低程度。

重要活动保障服务

活动保障前

第一阶段：评估加固

- 团队组建（角色/职责/流程）
- 隐患自查
  - 资产梳理，暴露面检查
  - 网络拓扑结构梳理
  - 账户与弱口令检查
  - 漏洞与基线检查
  - 泄漏信息与入侵痕迹排查
  - 渗透测试
- 防护措施落地（评估与加固）
  - 安全运维策略优化
  - 安全检测与防护设备部署
- （FW、DDOS、IPS、WAF、慧眼安全扫描工具、应急处置装置、威胁感知、风险管控平台）
- 应急演练（应急预案）

活动保障中

第二阶段：值守应急

- 安全态势监控分析
- 入侵事件行为分析
  - 扫描、破解行为
  - 漏洞利用行为
  - 木马上传与利用行为
  - 横向肉鸡利用行为
- 多产品联合策略优化分析
- 安全应急响应处置

活动保障后

第三阶段：总结汇报

- 活动总结汇报
  - 时间维度攻击趋势分析
  - 事件维度攻击手段分析
- 防护整改优化建议
- 防护策略优化建议
- 网络安全域改进建议
- 防护设备缺失补充建议
- 安全服务能力增强建议

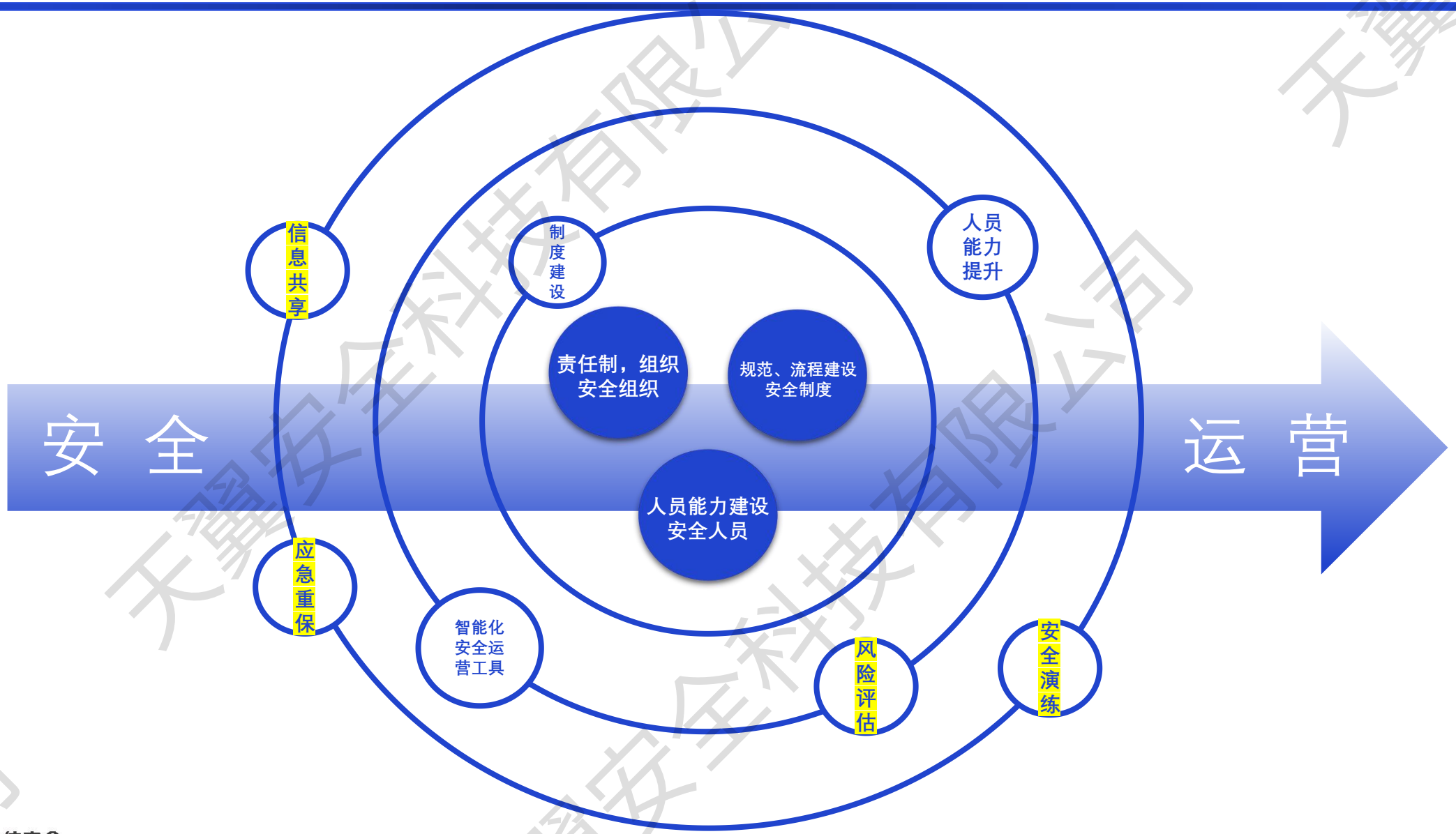
风险识别能力、安全防护能力、检测发现能力

响应处理能力、应急恢复能力

关键价值

在国家重要会议或重大活动期间协助客户保障网络基础设施、重点网站和业务系统的安全，通过明确的职责分工与协作，能快速应对各种网络安全事件，使重要会议或重大活动期间的客户业务系统安全平稳运行。

二、安全运营 —— 提供的价值



04 关基合规 提质增效

三、关基合规+提质增效 —— 总图

安全基座
等保2.0合规（通用+工控+云计算），智能安全运营

安全管理和运营
安全团队、制度、流程的建设

关基合规+提质增效
关保合规，主动防御

关基合规+提质增效

安全技术

- 内外网攻击面管理
- 访问控制策略可视化与管理
- 数据安全全周期管控
- 干扰/溯源能力

安全管理和运营

- 检测评估
- 监测预警
- 供应链安全管理
- 数据安全治理

安全管理

- 管理人员
- 管理制度
- 管理机构
- 建设管理
- 运维管理

安全基座

企业资源层安全技术体系

- 安全管理中心
  - 安全态势感知系统
  - 统一威胁检测
  - SIEM
  - SOAR
- 安全计算环境
  - WAF/云堤·网站安全专家
  - 漏洞和基线管理系统
  - 堡垒主机
  - EPP/EDR/防病毒
- 安全区域边界
  - 网络准入
  - 网络审计/NDR
  - IPS/防病毒墙
  - NGFW/微隔离
- 安全通信网络
  - 云堤·域名无忧
  - 云堤·抗D
  - VPN/SDP
- 安全池
- 身份安全
- 密码安全
- 信创安全

工控系统安全技术体系

- 安全管理中心
  - 工控安全态势感知系统
  - 日志审计与分析
  - 工控安全管理系统
- 安全计算环境
  - 工控主机身份认证
  - 工控主机基线管理
  - 工控主机防病毒
  - 工控内外联检测
- 安全区域边界
  - 工控安全监测与审计系统
  - 工控入侵检测
- 安全通信网络
  - 工控防火墙
  - 工控网闸
- 身份安全
- 密码安全
- 信创安全

安全运营

- 安全培训
- 安全演练
- 信息共享
- 风评+加固
- 应急+重保

三、关基合规+提质增效 —— 关基的认定/界定（1）

① 确定关键业务（参考下表）

行业		关键业务
能源	电力	电力生产（含火电、水电、核电等） 电力传输 电力配送
	石油石化	油气开采 炼化加工 油气输送 油气储存
	煤炭	煤炭开采 煤化工
金融		银行运营 证券期货交易 清算支付 保险运营
交通	铁路	客运服务 货运服务 运输生产 车站运行
	民航	空运交通管控 机场运行 订票、离港及飞行调试检查安排 航空公司运营
	公路	公路交通管控 智能交通系统（一卡通、ETC收费等）
	水运	水运公司运营（含客运、货运） 港口管理运营 航运交通管控

② 确定关键业务相关的信息系统或工业控制系统

行业	关键业务
水利	水利枢纽运行及管控 长距离输水管控 城市水源地管控
医疗卫生	医院等卫生机构运行 疾病控制 急救中心运行
环境保护	环境监测及预警（水、空气、土壤、 核辐射等）
工业制造 （原材料、装备、消费品、电子制造）	企业运营管理 智能制造系统（工业互联网、物联网、智能装备等） 危化品生产加工和存储管控（化学、核等） 高风险工业设施运行管控
市政	水、暖、气供应管理 城市轨道交通 污水处理 智慧城市运行及管控
电信与互联网	语音、数据、互联网基础网络及枢纽 域名解析服务和国家顶级域注册管理 数据中心 / 云服务
广播电视	电视播出管控 广播播出管控
政府部门	信息公开 面向公众服务 办公业务系统

三、关基合规+提质增效 —— 关基的认定/界定（2）

3 根据关键业务对信息系统或工业控制系统的依赖程度，以及发生网络安全事件后可能造成的损失，确定关键信息基础设施。

A. 网站类

（1）县级（含）以上党政机关网站

（2）重点新闻网站

（3）日均访问量超过100万人次的网站

（4）一旦发生网络安全事故，可能造成以下影响之一的：

（1）影响超过100万人工作、生活；
（2）影响单个地市级行政区30%以上人口的工作、生活；
（3）造成超过100万人个人信息泄露；
（4）造成大量机构、企业敏感信息泄露；
（5）造成大量地理、人口、资源等国家基础数据泄露；
（6）严重损害政府形象、社会秩序，或危害国家安全。

（5）其他应该认定为关键信息基础设施

B.平台类

（1）注册用户数超过1000万，或活跃用户（每日至少登陆一次）数超过100万

（2）日均成交订单额或交易额超过1000万元

（3）一旦发生网络安全事故，可能造成以下影响之一的：

（1）造成1000万元以上的直接经济损失；
（2）直接影响超过1000万人工作、生活；
（3）造成超过100万人个人信息泄露；
（4）造成大量机构、企业敏感信息泄露；
（5）造成大量地理、人口、资源等国家基础数据泄露；
（6）严重损害社会和经济秩序，或危害国家安全。

（4）其他应该认定为关键信息基础设施

C.生产业务类

（1）地市级以上政府机关面向公众服务的业务系统，或与医疗、安防、消防、应急指挥、生产调度、交通指挥等相关的城市管理系统。

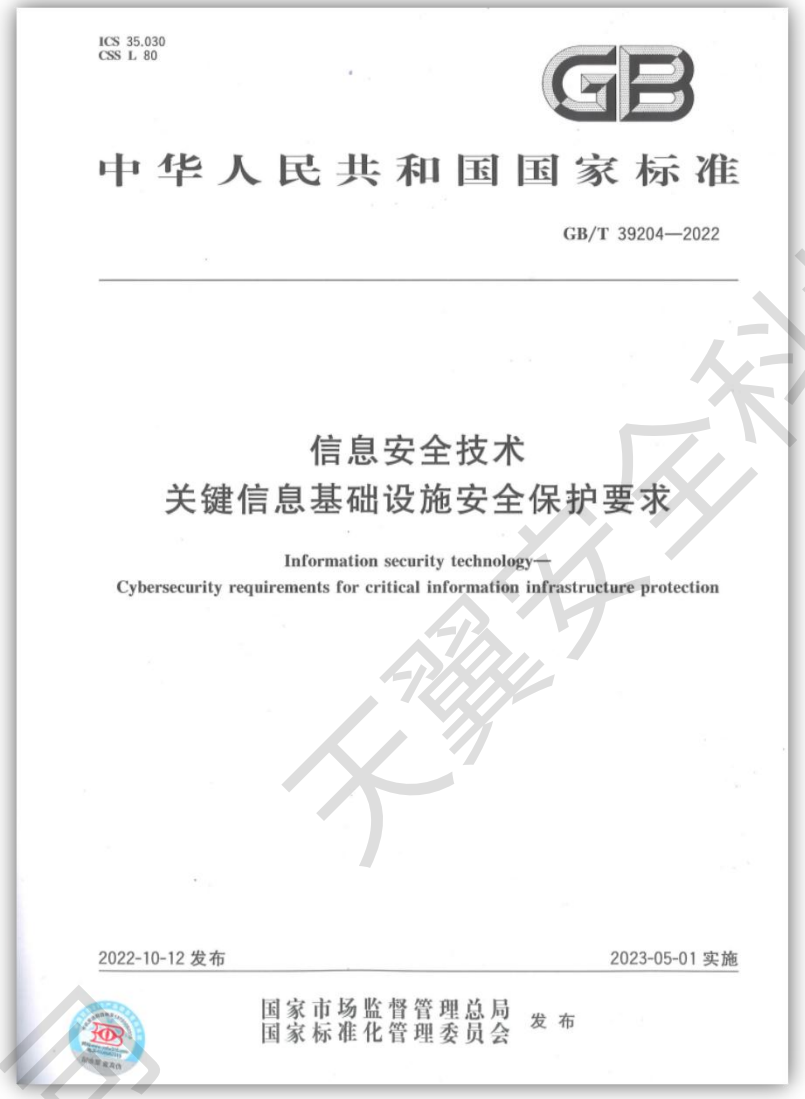
（2）规模超过1500个标准机架的数据中心。

（3）一旦发生网络安全事故，可能造成以下影响之一的：

（1）影响单个地市级行政区30%以上人口的工作、生活；
（2）影响10万人用水、用电、用气、用油、取暖或交通出行等；
（3）导致5人以上死亡或50人以上重伤；
（4）直接造成5000万元以上经济损失；
（5）造成超过100万人个人信息泄露；
（6）造成大量机构、企业敏感信息泄露；
（7）造成大量地理、人口、资源等国家基础数据泄露；
（8）严重损害社会和经济秩序，或危害国家安全。

（4）其他应该认定为关键信息基础设施

三、关基合规+提质增效 —— 关基保护要求的关注点


ICS 35.030
CSS L 80

GB

中华人民共和国国家标准

GB/T 39204—2022

信息安全技术
关键信息基础设施安全保护要求

Information security technology—
Cybersecurity requirements for critical information infrastructure protection

2022-10-12 发布　　2023-05-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

定位

关键信息基础设施安全保护应在网络安全**等级保护制度基础上**,实行**重点保护**。

三原则

（1）**以关键业务为核心的整体防控**。关键信息基础设施安全保护以保护关键业务为目标，对业务所涉及的一个或多个网络和信息系统进行体系化安全设计，构建整体安全防控体系。

（2）**以风险管理为导向的动态防护。**根据关键信息基础设施所面临的安全威胁态势进行持续监测和安全控制措施的动态调整,形成动态的安全防护机制,及时有效地防范应对安全风险。

（3）**以信息共享为基础的协同联防。**积极构建相关方广泛参与的信息共享、协同联动的共同防护机制,提升关键信息基础设施应对大规模网络攻击能力。

六活动

（1）**分析识别**。关键业务的依赖性识别，关键资产识别，风险识别。

（2）**安全防护**。针对识别到的业务、资产和风险，实施安全管理和安全技术保护措施，确保运行安全。

（3）**检测评估**。为检验安全措施的有效性，识别额外风险因素，需定期开展安全检测和风险评估活动。

（4）**监测预警**。建立并实施网络安全监测预警和信息通报制度；建立威胁情报和信息共享机制。

（5）**主动防御**。主动采取收敛攻击面、捕获、溯源、干扰和阻断措施；开展攻防演练和威胁情报工作。

（6）**事件处置**。对网络安全事件进行报告和处置，并采取适当应对措施，恢复因事件受损的功能或服务。

三、关基合规+提质增效 —— 互联网暴露面管理，外网攻击面收敛和监测预警

输入线索

- xxx.xxx.xxx.0/16
- xxx.xxx.xxx.1-253
- abc.com/cn
- IT资产批量导入模板

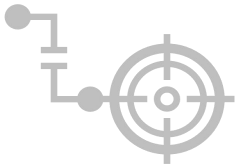
发现手段

- 主动探测
- 域名备案数据
- PDNS数据
- 情报数据
- 网站爬虫
- ……

数据清洗→资产列表

- 网站资产清单
- IP资产清单
- 端口指纹资产清单
- IP/网站组件清单
- 域名资产清单
- 疑似未知资产清单
- ……

风险识别



- 系统漏洞检测
- 应用漏洞检测
- 高危端口识别
- 弱口令识别
- 管理后台识别
- ……

输出监测报告

- 互联网资产发现及风险监测报告
  - 资产清单、资产分析
  - 风险清单、风险分析
  - ……
- 总结建议

要求

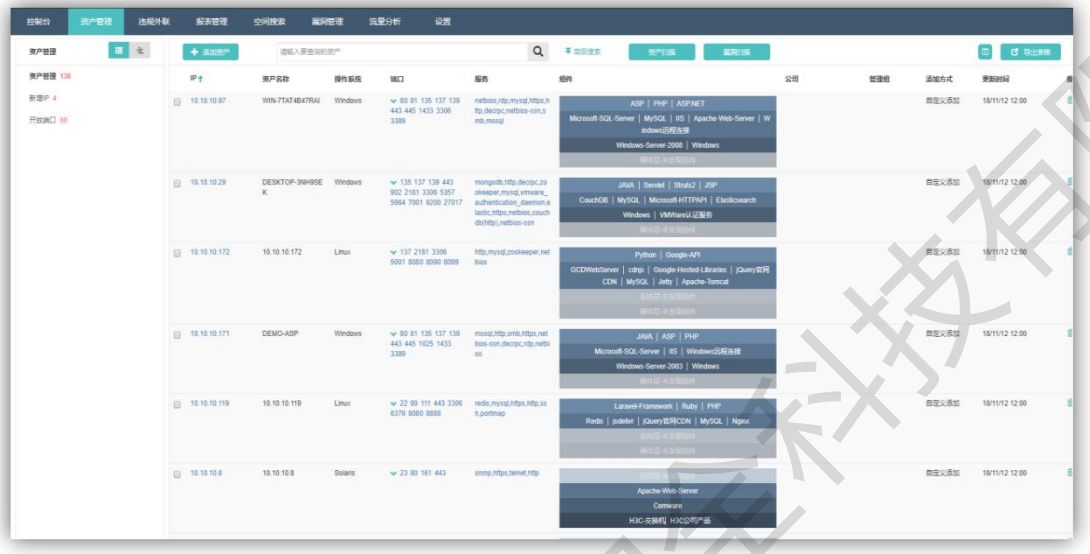
主动防御—收敛暴露面：

- **识别和减少互联网**和内网资产的互联网协议地址、端口、应用服务等**暴露面，压缩互联网出口数量**。
- **减少对外暴露**组织架构、邮箱账号、组织通信录等**内部信息，防范社工攻击**。
- **不应在公共存储空间**（如：代码托管平台、网盘、文库等）存储可能被攻击者利用的**技术文档**（如：网络拓扑图、源代码、互联网协议地址规划等）。

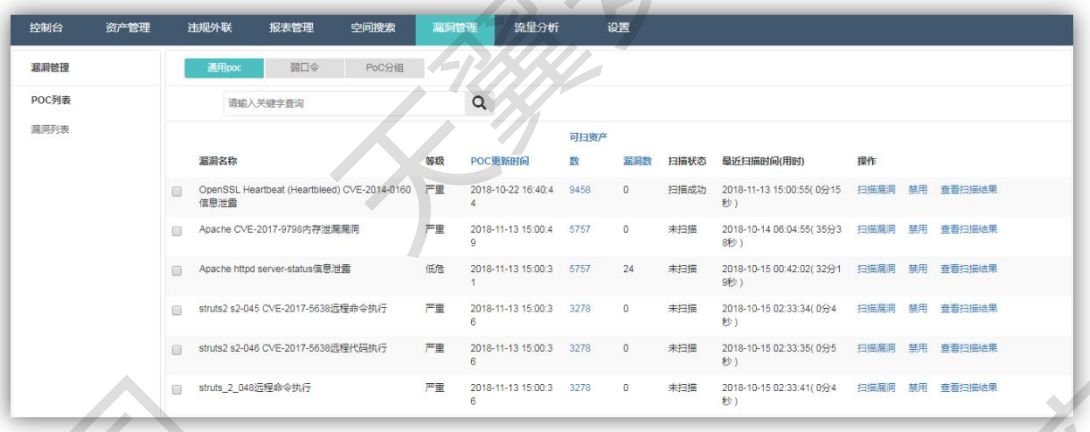
关键价值

- **互联网暴露面收敛**，清查未知暴露资产、业务，对暴露面进行有效监管和保护，避免潜在的安全隐患。
- **安全预警：快速排查新兴威胁影响的暴露资产范围**，以信息共享方式，在突发的安全漏洞和安全攻击事件中，快速定位受影响的资产范围，提高漏洞应急响应能力，抢占时间优势。

三、关基合规+提质增效 —— 网络资产测绘，内网攻击面收敛



内网资产彻查，并将资产和关键业务进行匹配，形成业务链



结合漏洞管理，可按照漏洞索引至资产和业务，梳理内部攻击面

要求

分析识别动作—业务识别、资产识别：

- 识别并梳理**关键业务链**，进而明确相关关键信息基础设施的分布和运营情况。
- 应采用**资产探测技术**识别资产，并依据关键业务链所依赖资产的实际情况**动态更新**。

关键价值

- **摸清家底**，通过网络探测技术清理内网资产和业务，建立**关键业务链**信息。
- **清查影子IT**（因管理人员变更，管理混乱，导致的连网但是未知的资产），避免内网未知攻击面的出现。
- **资产与漏洞信息匹配**，将攻击面与资产和业务相结合，获得清晰的攻击面信息，为风险处置动作提供基础信息。
- 以**搜索引擎**的使用方法和习惯，检索资产信息，可为各类网络安全评估工作提供必要支撑。

三、关基合规+提质增效 —— 访问控制策略的可视化和统一管理

防火墙访问控制策略集中管理，清理隐藏策略、冗余策略等无效策略

访问控制策略基线核查，确保访问控制策略与企业合规要求一致性

要求

安全防护动作—安全通信网络：

- 建立并完善业务系统之间、不同区域之间的**安全互联策略**。
- 应保持访问**控制策略**在不同业务系统、区域中的**一致性**。
- 对不同**业务系统和区域之间**的互操作、数据交互和信息流进行**严格控制**。

关键价值

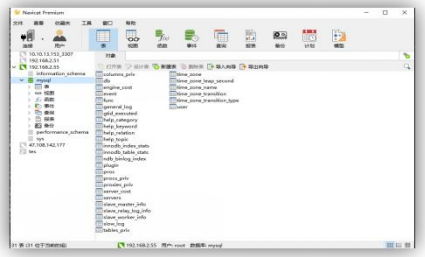
- **全网防火墙策略集中统一管理**，避免人工流程因信息不完备，操作异步，历史遗留问题导致的策略错误或漏洞。
- **策略自动优化**，快速优化清理，清理隐藏策略、冗余策略、空策略、过期策略等，归并相似策略。
- **策略生命周期管理**，事前仿真开通（模拟开通后的网络情况），事中API策略下发（降低设备使用门槛，避免误操作），事后策略合规基线检查。
- **应急响应**，与SIEM、态势感知等平台联动，可对高危威胁源进行自动化处置（阻断或隔离），避免威胁迅速蔓延。

三、关基合规+提质增效 —— 网络攻击干扰/溯源能力建设

① 攻击面动态化/欺骗化 → ② 主动干扰/误导攻击者 → ③ 溯源攻击者

高交互蜜罐
数控设备/PLC仿真

中交互蜜罐
SCADA/工控终端/办公业务仿真



低交互蜜罐
工业通信协议仿真
互联网通信协议仿真

摄像头蜜罐
摄像头视频流仿真
摄像头系统业务仿真

要求

主动防御—攻击发现和阻断：

- 应针对监测发现的攻击活动，分析攻击路线、攻击目标，设置多道防线，采取**捕获、干扰、阻断、封控**、加固等多种技术手段，切段攻击路径，快速处置网络攻击。
- 应及时对网络攻击活动开展溯源，对攻击者进行画像，为案件侦查、事件调查、完善防护策略和措施提供支持。

关键价值

- **攻击面动态化/欺骗化**，在企业管理层部署虚假的诱捕蜜罐系统，暴露虚假动态的攻击面，保护真实攻击面。
- **主动干扰/误导攻击者**，通过对办公系统、ICS系统的高仿真，干扰/误导攻击者，诱使其暴露自身信息。
- **溯源攻击者**，通过对攻击者在蜜罐中行为信息的提取，对攻击者进行画像，结合威胁情报，研判威胁源头，反向溯源。

三、关基合规+提质增效 —— 数据安全治理

要求

安全防护动作—数据安全防护：

- 建立基于**数据分类分级**的数据安全保护策略，明确**重要数据的保护措施**。
- 严格控制重要数据的**使用、加工、传输、提供和公开**等关键环节，采用**加密、脱敏、去标识化**等技术手段保护敏感数据安全。
- 建立数据处理活动**全流程安全能力**。

关键价值

- **数据安全风险可视**，针对数据生命周期中可能涉及到数据泄露、数据损毁的风险，通过对数据所处环境风险，结合应用、流量、威胁情报等外部信息，分析风险，看清问题。
- **数据全流程安全管控**，自数据产生（采集）开始，后续全流程闭环管理，实现企业数据安全管理制度到技术控制措施的全面映射。
- **数据流转可视化**，关键的重要数据都在哪里？流转情况如何？通过可视化来分辨数据使用是否合规。

三、关基合规+提质增效 —— 供应链安全管理

建立供应链安全管理策略

- 供应链风险管理策略
- 供应方选择和管理策略
- 产品开发采购策略
- 安全维护策略

对**供应链全流程**（商流、物流、信息流，运输，储存，装卸，搬运，包装，流通加工，配送，信息处理等环节）进行风险**识别、分析、处置、持续监测**的策略指南。

多供应商 | 供应商协调沟通 | 库存安全 | 供应链韧性 | 合同管理 | ……

建立并维护**合格的供应商目录**，选择有保障的供应方，防范出现因政治、外交、贸易等非技术因素导致产品和服务供应中断的风险。

供应商生命周期管理 | 供应商成熟度评估模型

采购网络关键设备和网络安全专用产品目录中的设备产品时，应采购通过**国家检测认证**的设备和产品。形成**年度采购网络产品和服务清单**；采购、使用的网络产品和服务应符合相关国家标准的要求。可能影响国家安全的，应通过**国家网络安全审查**。

- 要求供应商对网络产品和服务的**设计、研发、生产、交付**等关键环节**加强安全管理**。
- 要求供应商**声明**不非法获取用户数据、控制和操纵用户系统和设备，或利用用户对产品的依赖性谋取不正当利益或者迫使用户更新换代。
- 要求供应商签订**安全保密协议**，内容包括安全职责、保密内容、奖惩机制、有效期等。
- 要求供应商对网络产品和服务研发、制造过程中涉及的实体拥有或控制的已知技术专利等**知识产权获得10年以上授权**，或在**网络产品和服务使用期内获得持续授权**。
- 要求供应商提供**中文版运行维护、二次开发**等技术资料。
- 自行或委托第三方网络安全服务机构对定制开发软件进行**源代码安全检测**，或由供应方提供第三方网络安全服务机构出具的**代码安全检测报告**。
- 使用的网络产品和服务存在安全缺陷、漏洞等风险时，应**及时采取措施消除风险隐患**，涉及**重大风险的应按规定向相关部门报告**。

三、关基合规、提质增效 —— 提供的价值

① 分析识别

识别关键业务链（识别业务、资产、风险）

风险识别　风险分析　威胁情报共享

② 安全防护

安全技术措施，安全管理措施

风险处置　云堤云端安全服务协同联防

③ 检测评估

检验措施有效性，识别风险隐患残留，定期评估

风险持续监测　专业安全评估服务协同

④ 监测预警

监测预警和信息通报制度，威胁情报和信息共享机制

风险识别　风险分析　威胁情报共享

⑤ 主动防御

收敛内外部攻击面，主动捕获、溯源、干扰和阻断，开展攻防演练和威胁情报工作

风险处置　产品和服务协同

⑥ 事件处置

网络安全事件要进行报告和处置，及时恢复因事件受损的功能或服务

风险处置　产品和服务协同

关键业务为核心
整体防控

风险管理为导向
动态防护

信息共享为基础
协同联防

中国电信安全公众号

中国电信SRC公众号

中国电信安全微博

中国电信 CHINA TELECOM

电信安全 China Telecom Cybersecurity Tech

天翼安全科技有限公司
China Telecom Cybersecurity Technology Co.,Ltd
北京市东城区朝阳门北大街19号 100010
No.19, ChaoYangMen North Street, Dongcheng District, Beijing, China, 100010
www.ctct.cn