SANGFOR
深信服科技

XXXX安全运营中心解决方案

面向未来　有效防护

深信服科技

SANGFOR
深信服科技

一．XXXX安全建设背景

二．XXXX安全建设思路

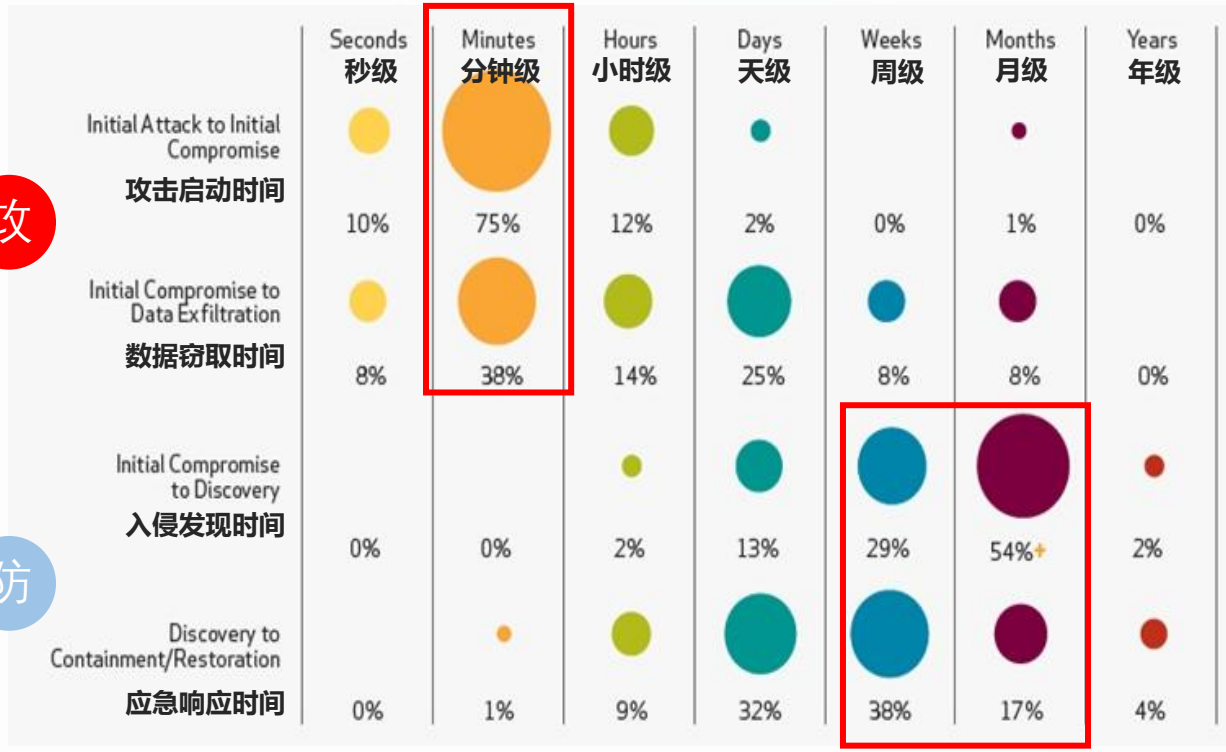
三．安全运营中心解决方案

四．项目团队及实施计划

没有一劳永逸的安全之法

SANGFOR 深信服科技

安全事件频发的本质是攻防不对等



数据来源：Verizon 2018 数据泄露调查报告

勒索攻击事件频发，变种数量不断攀升

14万

2018 年，CNCERT 捕获勒索软件近 14 万个，全年总体呈现增长趋势！

19

勒索软件 GandCrab 18年出现了约 19 个版本，一直快速更新迭代

勒索软件即服务

伴随“勒索软件即服务”产业的兴起，活跃勒索软件数量呈现快速增长势头，且**更新频率和威胁广度都大幅度增加**

外部威胁变化太快，大部分组织自身拥有的安全资源与安全能力难以有效应对！

安全运维压力大，事件处置不及时

SANGFOR 深信服科技

- 重复性工作如日志分析、事件处理
- 各类报表报告费时费力难处理
- 大量重要资产、核心系统日常巡检

安全运维工作量大

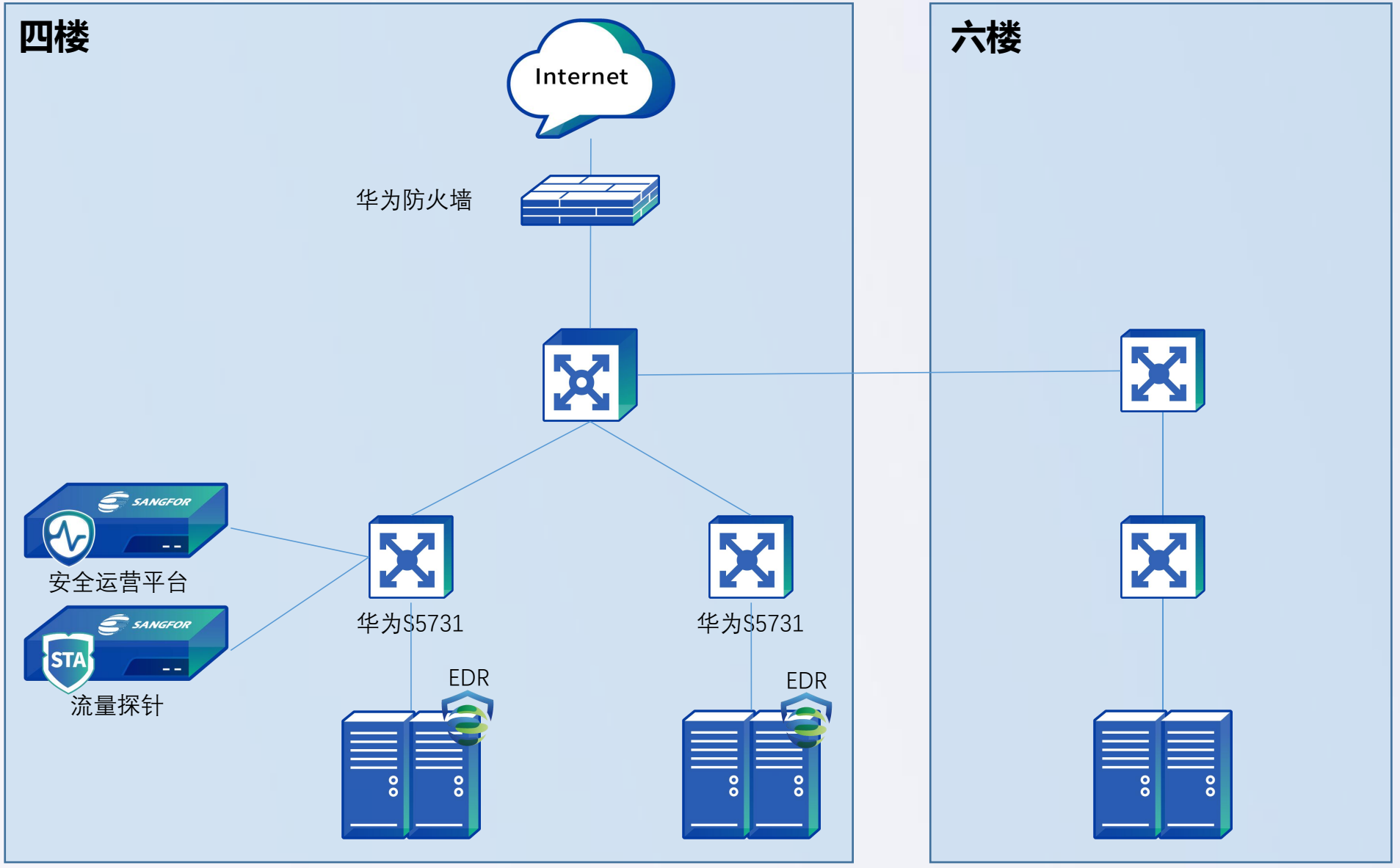
- 安全人员编制少，身兼多职难应对
- 对于复杂的问题安全分析能力不足
- 安全漏洞该不该处置、如何处置

人员不足，基础薄弱

- 自动化程度底，高度依赖人
- 无法辅助决策，问题难处置
- 处理进度难跟踪，处理结果无反馈

安全运维效率低

测试部署拓扑图


四楼
六楼
Internet
华为防火墙
SANGFOR
安全运营平台
SANGFOR
STA
流量探针
华为S5731
华为S5731
EDR
EDR

态势感知测试情况

SANGFOR 深信服科技

脆弱性态势

统计周期为最近7天 | 周三 2021-04-21 11:14:46

服务器总览

2 脆弱性服务器（个）

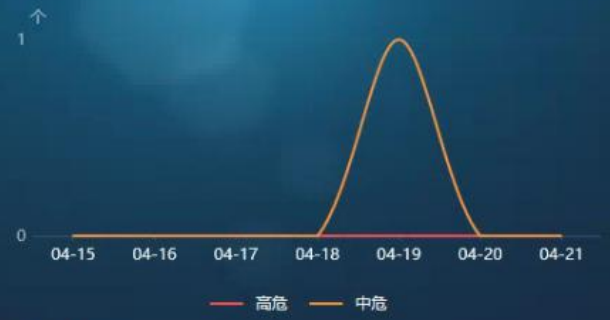
255 服务器总览（个）

脆弱性资产 TOP5

内网IP范围(10.3.70.3)	脆弱性风险2个	未处理
ceph-test(10.3.10.1)	脆弱性风险1个	未处理

脆弱性风险	风险标签
1	配置风险

漏洞风险态势



漏洞类型 TOP5

信息泄漏： 1个 | 100.00%

实时脆弱性监测

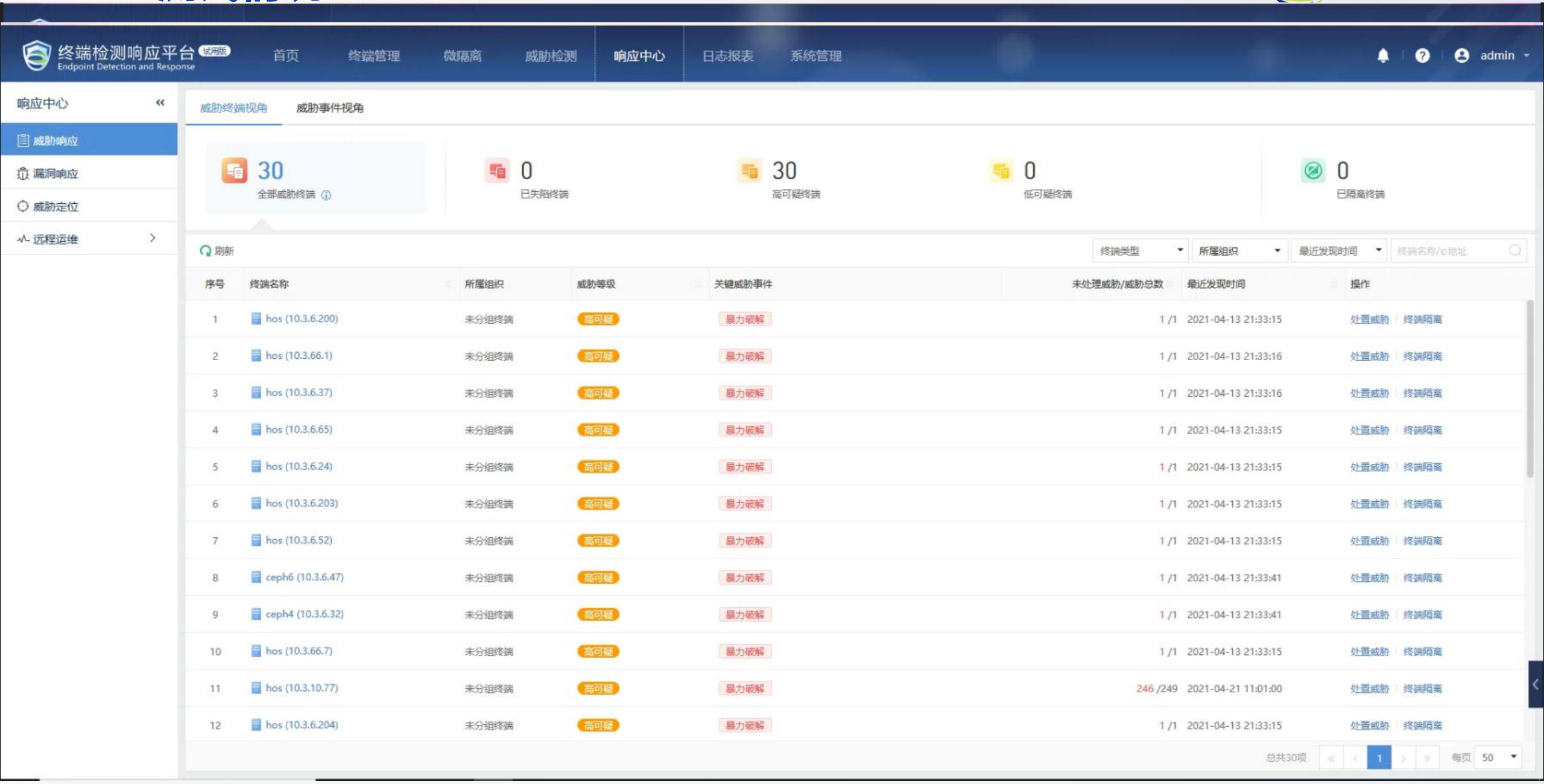
风险主机	所属资产组	脆弱性类型	严重等级	来源	详情	检测时间	处理状态
ceph-test(10.3.10.1)	内网IP范围	配置风险	中危	SANGFOR STA	主机：SSH远程登录	2021-04-21 06:08:37	未处理
内网IP范围(10.3.70.3)	内网IP范围	配置风险	中危	SANGFOR STA	主机：目标服务器存在目录浏览漏洞	2021-04-19 10:18:01	未处理
内网IP范围(10.3.70.3)	内网IP范围	信息泄漏	中危	SANGFOR STA	主机：服务器敏感文件访问检测	2021-04-19 09:52:47	未处理

高危漏洞 TOP5

暂未配置资产组， 立即配置

EDR测试情况

SANGFOR 深信服科技



测试总结说明

SANGFOR 深信服科技

态势感知测试总览

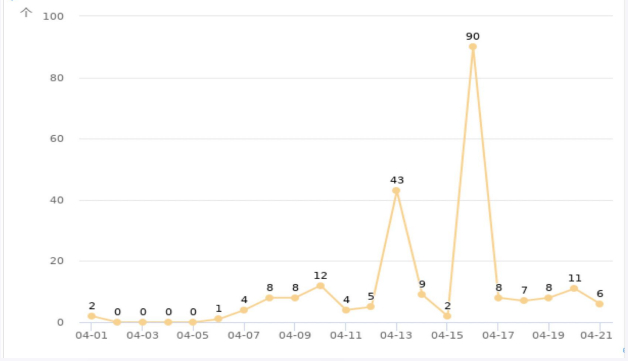
1.1 整体安全

在您的网络中，系统共识别了 255 个服务器，35 个终端。
主要安全威胁如下所示，风险主机共 81 个，其中高危主机 38 个、低危主机 43 个。共处理了 6 个主机，

当前的网络整体安全评级为差。

	已失陷	高危	中危	低危	处理状态
服务器	0	38	0	43	6 个已处理
终端	0	0	0	0	-

在报告期间，一共发生了 228 个安全事件，每天发生的事件个数如图所示，在 2021-04-16 达到最高峰：90 个。



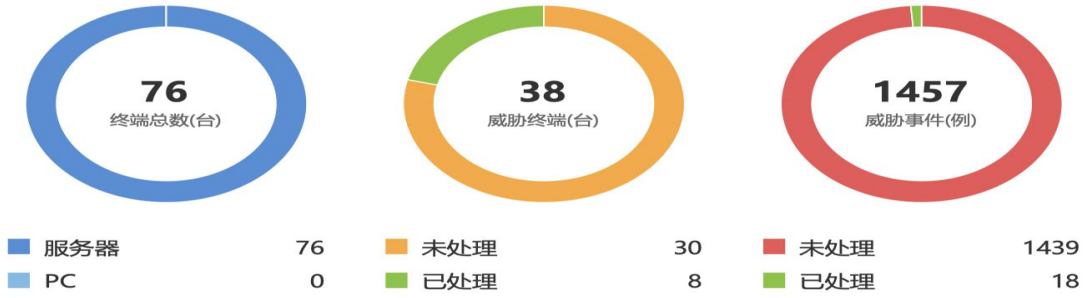
在报告期间，一共处理了 52 个安全事件，以下是已处理的安全事件 TOP10 概览，处理详情见安全事件分析章节。

序号	安全事件	处理个数	处理主机数	处理主机 TOP5
1	内网服务器收到来自新主机的远程控制连接	23	9	hos(10.3.15.36) hos(10.3.6.22) ceph-test(10.3.10.1) hos(10.3.1.1) hos(10.3.6.61)
2	主机遭受互联网远程风险访问	11	1	ceph-test(10.3.10.1)
3	主机遭受暴力破解	6	6	hos(10.3.8.88) hos(10.3.10.77) hos(10.3.6.25) hos(10.3.1.1) ceph-test(10.3.10.1)
4	主机感染了病毒	5	4	hos(10.3.6.61) hos(10.3.15.36) hos(10.3.6.31) hos(192.168.1.77)
5	主机感染了病毒	3	3	hos(10.3.15.36) hos(10.3.6.61) hos(10.3.6.31)
6	主机对内网主机的 tcp 端口发起扫描	2	1	内网 IP 范围(10.2.9.99)
7	主机对内网发起 tcp 端口扫描	1	1	hos(10.3.10.77)
8	主机对内网发起 arp 扫描攻击	1	1	hos(10.3.10.77)

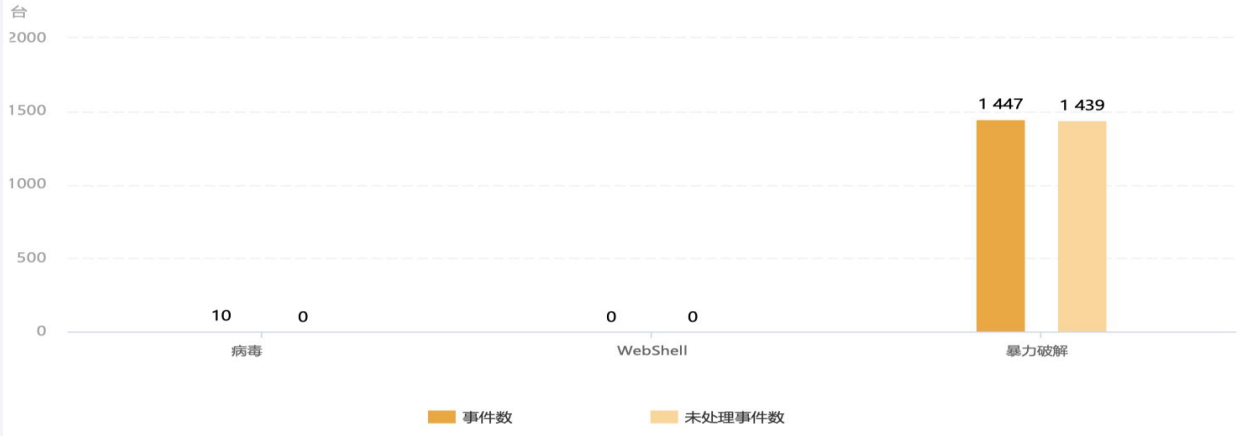
EDR测试总览

◆ 总览详情

威胁终端21.05%已被处理， 未处理威胁终端30台； 威胁事件1.24%已被处理， 未处理威胁事件1439例， 目前全网终端还存在安全风险，请在EDR平台的响应中心及时处理威胁终端以及威胁事件



统计周期内，共发现了1457例威胁事件， 其中暴力破解威胁事件发生了1447例， 占比99.31%，是发生次数最多的威胁事件类型， 未处理的威胁事件共有1439例， 建议尽快在EDR平台的"响应中心>终端风险视角"页面进行处理。以下是各类型威胁事件的发生及处理情况：



SANGFOR
深信服科技

一．XXXX安全建设背景

二．XXXX安全建设思路

三．安全运营中心解决方案

四．项目团队及实施计划

安全运营（管理）建设参考标准

SANGFOR 深信服科技

等级保护2.0

满足GB/T 22239-2019网络安全等级保护基本要求中关于安全运维管理方面的要求：

8.1.5 安全管理中心

- 应对分散在各个设备上的审计数据进行收集汇总和集中分析
- 应能对网络中发生的各类安全事件进行识别、报警和分析

8.1.10 安全运维管理

- 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等

NIST SP800-137

《 SP800-137 联邦信息系统和组织的信息安全连续性监控（ISCM） 》，ISCM的定义是**保持对信息安全、漏洞和威胁的持续了解，以支持组织风险管理决策。**推荐的策略包括:

- 梳理组织风险并确定优先级
- 提供有意义的安全状态指示的指标
- 确保所有安全控制措施的持续有效性
- 保持对资产安全性的可见性
- 了解和控制组织系统和运营环境的变更
- 保持对威胁和漏洞的意识

GB/T 36626-2018

《 GB/T 36626-2018信息系统安全运维管理指南》，用于**帮助和指导各组织建立和运行信息系统安全运维管理体系。**推荐的策略包括:

- 资产管理
- 信息系统安全分级
- 脆弱性管理
- 入侵管理
- 异常行为管理
- 通信安全
- 恶意软件防范等
- 信息传输

标准指引下的四大建设需求：风险管理、事件管理、资产运维、漏洞管理

主流技术趋势

SANGFOR 深信服科技

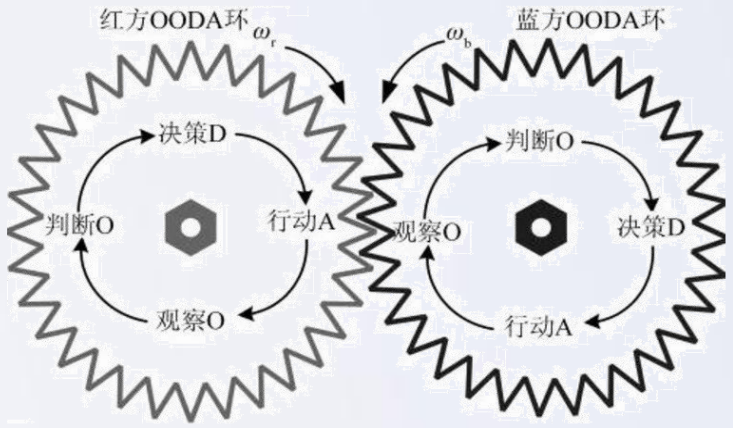
传统以静态检测和被动防御为中心的安全建设，正在向“智能化、自动化、动态化”的安全闭环转变

Gartner

- 《2019年七大安全和风险管理趋势》趋势二：到2022年有**50%的安全运营中心**将集成事件响应、威胁情报和威胁搜索能力。
- 《Gartner 2020数据和分析技术十大趋势》趋势八：到2022年，超过一半的主要新业务系统将采用**持续智能**，这些智能将使用实时上下文数据来改善决策。

IDC Analyze the Future

- 《全球安全产品和服务预测-中国启示》到2022年，50%的合理安全警报将进行**自动响应**，不受人类分析师的影响。
- 《2020年中国网络安全市场十大预测》预测1:到2022年，60%安全运营中心（SOC）的初级分析师将利用**人工智能**（AI）和机器学习（ML）**持续提高其工作效率并提升其运营的安全水平**。



包以德-OODA循环

OODA即observe（观察）、orient（判断）、decide（决策）和act（行动），由美国空军上校约翰.包以德（John Boyd）发明，并**广泛应用于网络战**、诉讼战和金融战。基本观点：**较量的本质可以看做是敌对双方对抗中，谁能更快更好地完成OODA循环，**然后迅速采取行动，干扰、延长、打断敌人的OODA循环。双方都从观察开始，根据持续感知到的外部威胁，及时调整系统，做出应对决策，并采取相应行动。

安全运营体系演进与选择

SANGFOR 深信服科技

- 主要以IT资产为管理和运营对象
- 只采集日志、告警、事件三类

以信息管理为核心

特点：只关注安全信息层面的采集，无法展示综合风险、无自动响应流程、事件处置无闭环等；

- 以IT资产、业务系统为对象
- 日志、告警、事件、威胁情报

以安全管理为核心

特点：能够进行整体安全态势可视但自动化处置流程不够完善，缺乏人机共智、智能决策等方面的能力；

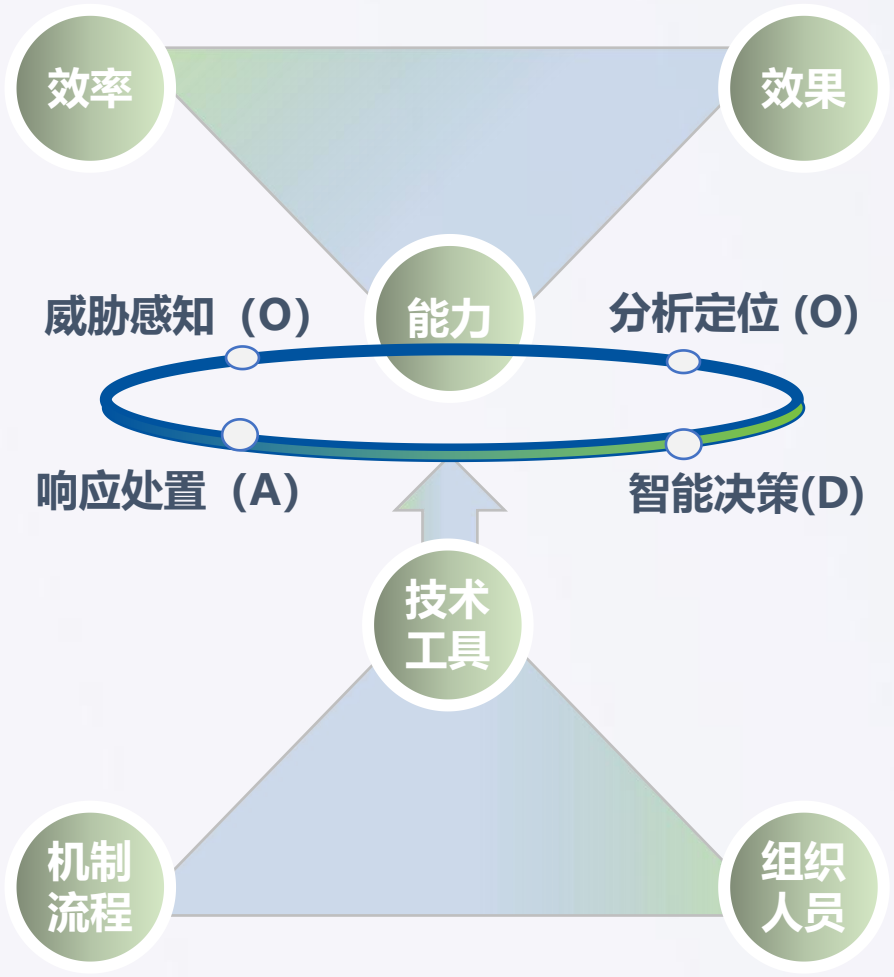
- IT资产、业务系统、数据等
- 安全事件、情报、流量、流程

未来安全运营中心

- 采用自动化、智能化的手段如基于SOAR的自动化流程支持自动闭环；
- 提供人机共智的智能化处置和应急；

站在理念制高位

作为耕耘20余年的前沿网络安全厂商，深信服认为未来安全运营中心的建设不仅应具备关联分析、安全可视等基本能力，还应能利用大数据、SOAR、UEBA、威胁情报等技术实现**“自动响应闭环，持续安全运营”**。



有效提升安全**能力**（提升安全建设效果）、运维**效率**（提升运维处置效率）、工作**效果**（体现安全工作价值）

我们将基于OODA的动态安全闭环理念
打造“自动安全闭环、持续安全运营”的新一代安全运营中心

建设“技术工具、组织人员、机制流程”有效协同，实现自动化联动处置，人机共智的持续运营及快速有效的应急响应能力

SANGFOR
深信服科技

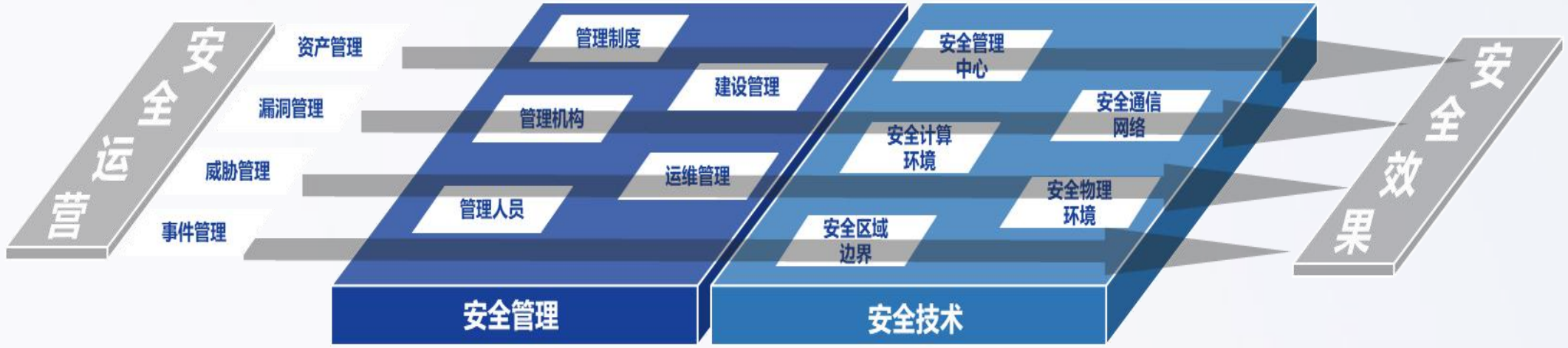
一．XXXX安全建设背景

二．XXXX安全建设思路

三．安全运营中心解决方案

四．项目团队及实施计划

【目标】构建以安全效果为目标的持续化安全运营体系



不为了安全而安全，为了服务而服务，一切以 **安全效果** 为目标

以 **资产、漏洞、威胁以及事件** 四个控制要素为抓手

通过“**人机共智**”模式开展持续化的网络安全保障工作

实现 **安全合规、风险可控、知识转移、价值呈现**

【方法】从业务风险出发设计整体安全

SANGFOR 深信服科技

S1:目标设定

- 组织战略
- 事件驱动
- 业务驱动

S2:安全评估与需求分析

政策法规
- 网络安全法
- 密码法
- CII保护条例
- 网络安全等级保护条例
- 行业法规

现状调研

风险评估

差距分析

安全标准
- GB/T20984 网络安全等级保护基本要求
- ISO27001
- 关键信息基础设施网络安全保护基本要求

安全需求
- 组织类
- 合规类
- 事件类
- 业务类
- 安全技术
- 安全管理
- 安全运营

安全需求汇总

安全需求确认

任务优先级排序/确认

S3:体系规划

实施 / 计划 / 检查 / 改进

- 安全技术
- 安全管理
- 安全运营

政策法规、标准与框架
- 网络安全法
- 密码法
- 等级保护
- 关基保护
- CARTA
- Kill Chain
- IPDRR
- ZTA
- APDRO
- IATF/ITIL/27001

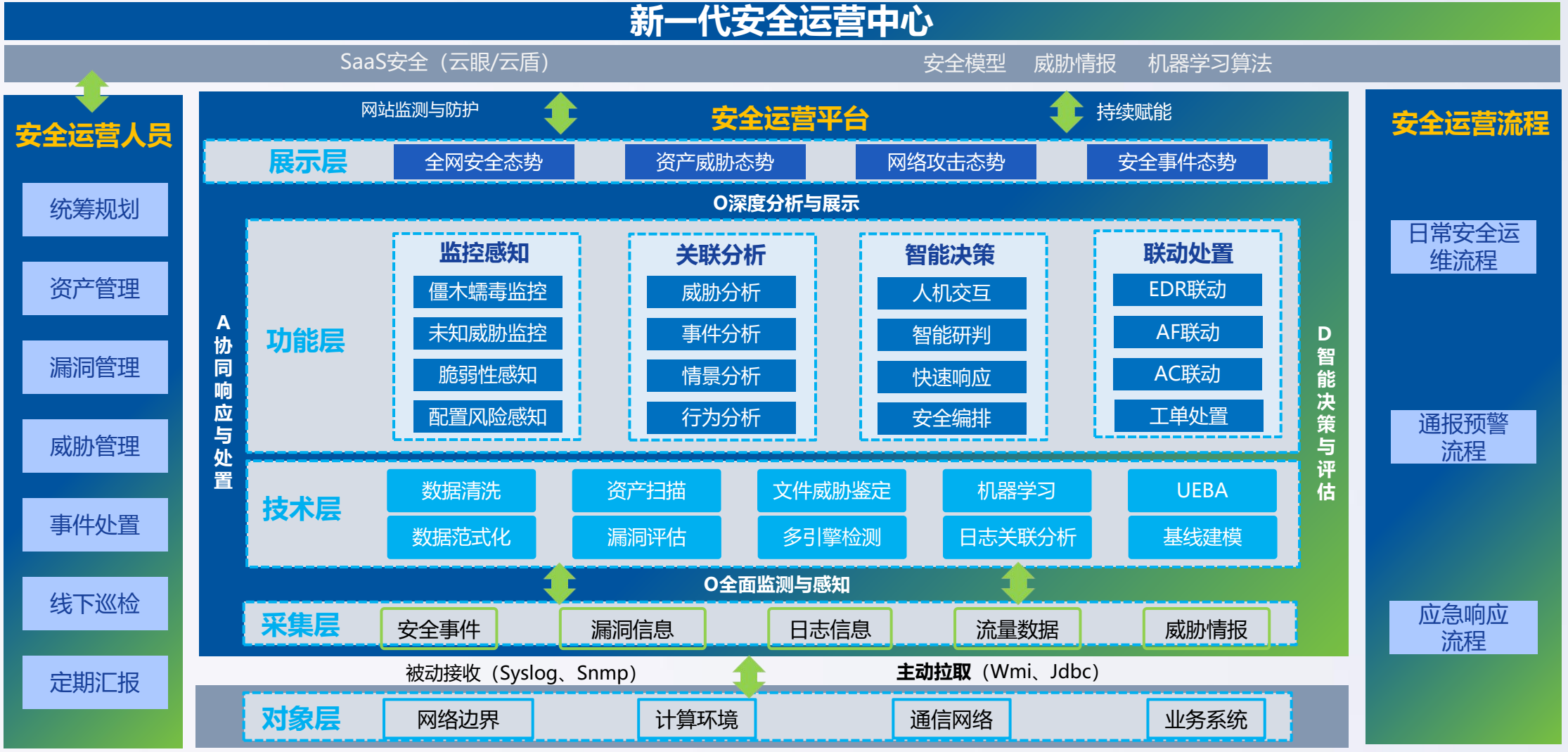
- 安全制度建设
- 安全开发
- 数据安全
- 网络建设
- 运维安全
- 出口安全
- 终端接入安全
- ……

网络安全规划方法论

【架构】安全运营中心方案架构

SANGFOR 深信服科技

安全运营中心方案整体架构包括**安全运营人员、安全运营平台、安全运营流程**三部分组成，帮助用户实现“**自动响应闭环，持续安全运营**”。其中安全运营平台通过UEBA、机器学习、联动分析等技术**为运营中心建设提供基础平台实现持续安全运营**，安全运营流程**制定各类场景下的流程机制**，安全运营人员通过**规范运营工作要求**利用平台及流程让安全运营中心发挥价值。



【拓扑】全国网络安全规划图

SANGFOR
深信服科技

深圳

Internet

流量探针

下一代防火墙*2

上网行为管理*2

VPN

终端检测与响应平台EDR

安全运营服务（安全运营中心专家团队）

安全运营平台

（防火墙做IPSEC VPN组网）

数据引流

数据引流

数据引流

数据引流

数据引流

IDC1

Internet

流量探针

下一代防火墙*2

终端检测与响应平台EDR

IDC1

Internet

流量探针

下一代防火墙*2

终端检测与响应平台EDR

IDC1

Internet

流量探针

下一代防火墙*2

终端检测与响应平台EDR

IDC1

Internet

流量探针

下一代防火墙*2

终端检测与响应平台EDR

...

IDC1

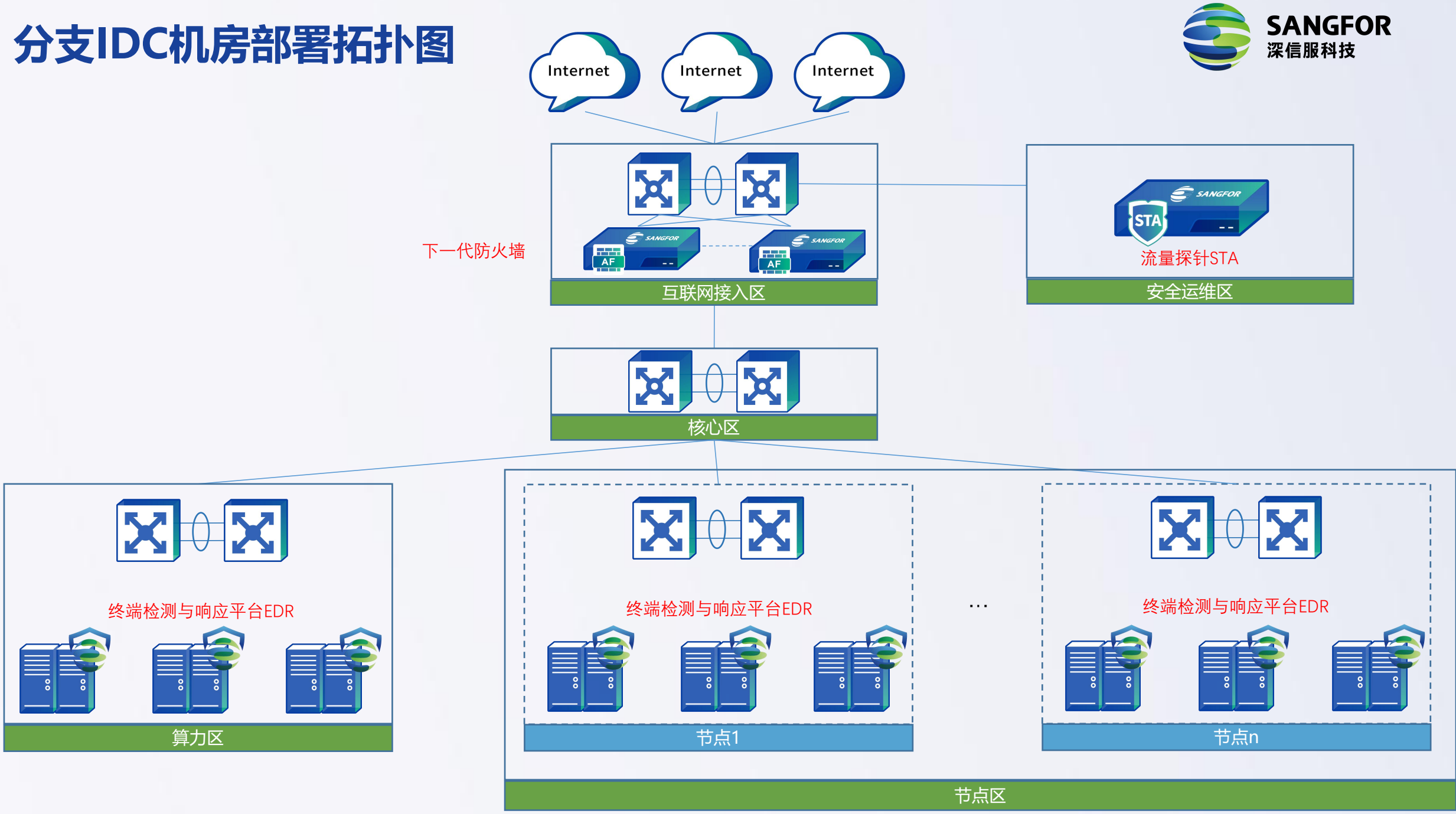
Internet

流量探针

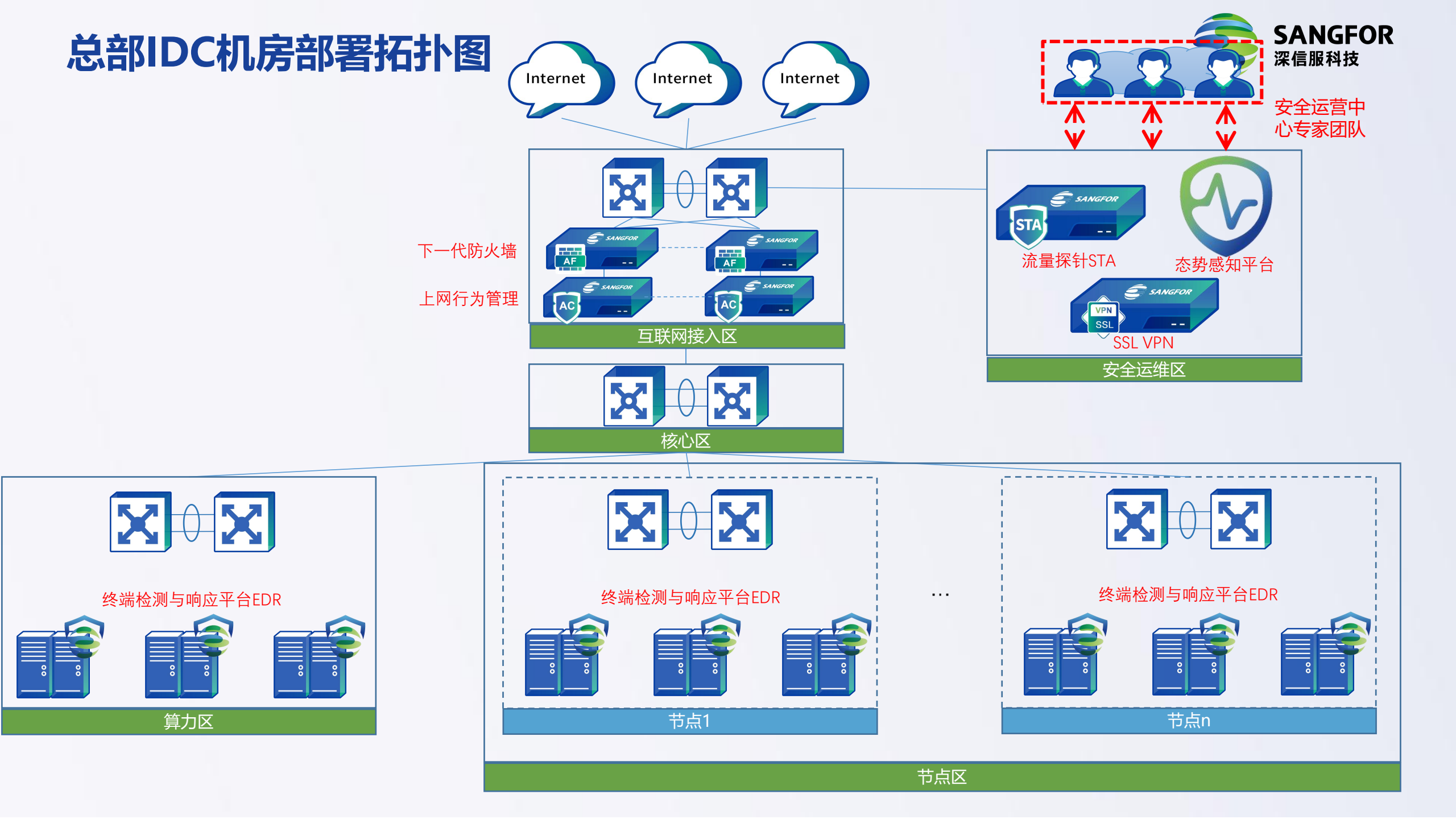
下一代防火墙*2

终端检测与响应平台EDR

分支IDC机房部署拓扑图



总部IDC机房部署拓扑图



SANGFOR
深信服科技

一、安全运营平台

安全运营平台基础功能

SANGFOR 深信服科技

通过运营平台为安全运营中心建设提供基础能力及实现环境，实现持续安全运营

(一)威胁感知

- 威胁感知-理资产
- 威胁感知-找威胁
- 威胁感知-摸风险

(二)分析定位

- 分析定位-关联分析
- 分析定位-智能推理
- 分析定位-风险可视

(四)响应处置

- 响应处置-设备联动
- 响应处置-电子工单
- 响应处置-自动编排

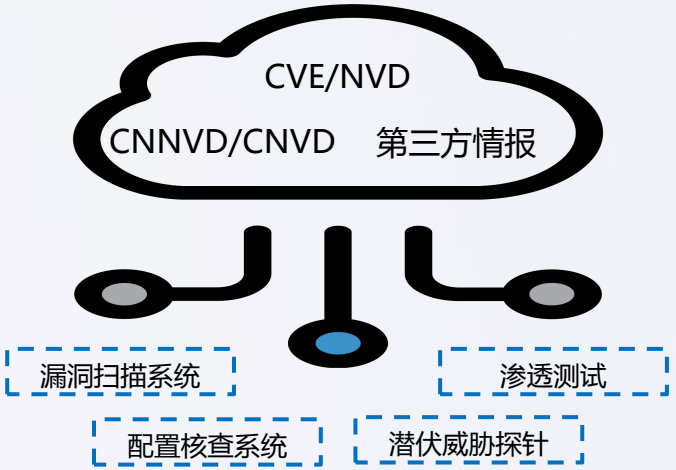
(三)智能决策

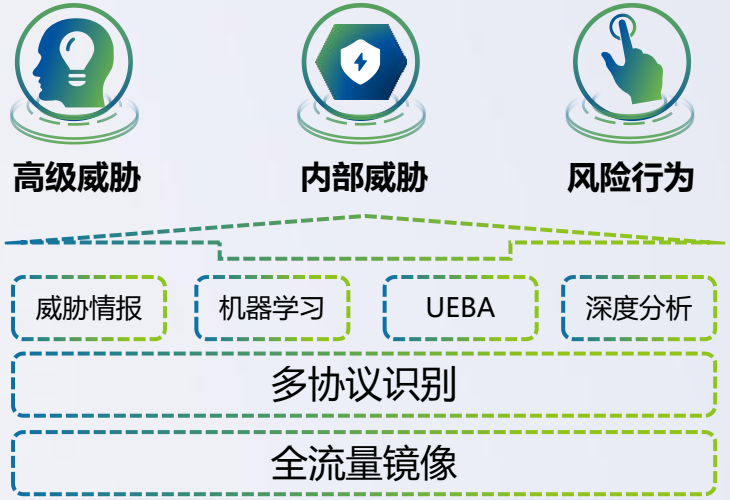
- 智能决策-事件影响呈现
- 智能决策-多视角评估
- 智能决策-攻击行为还原

（一）威胁感知三步走

SANGFOR 深信服科技

通过不断梳理资产与持续发现的风险、威胁相关联，洞察全网安全风险





理资产

通过主动扫描、流量发现、手动导入不断发现新生资产、影子资产、废弃资产通过审核入库、废弃退库持续维护资产台账。

摸风险

借助多方漏洞情报丰富情报库，通过多种漏洞发现方式全面摸清资产安全风险。

找威胁

采集全网关键业务流量并与资产及风险匹配，通过多种算法实现对已知/未知安全威胁的全面分析。

（二）智能分析定位，威胁快速发现

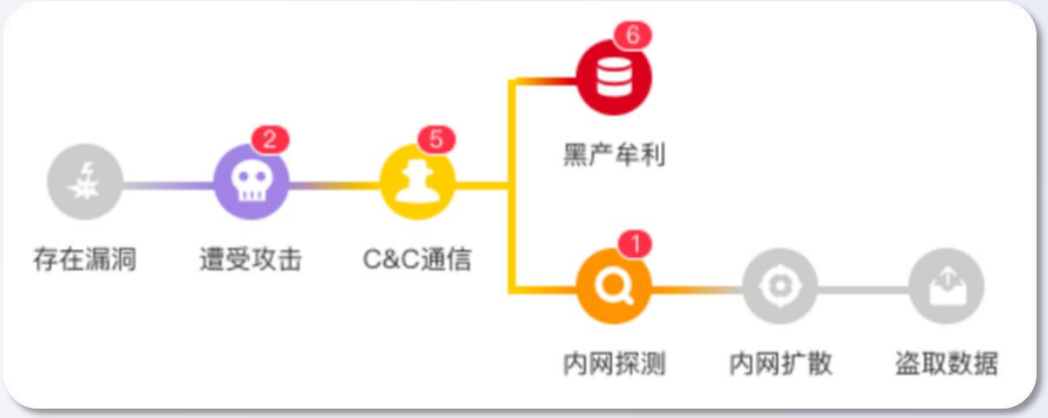
SANGFOR 深信服科技

基于智能关联、推理进行深度分析并进行可视化展示，实现威胁快速发现

智能关联分析引擎

- **事件分析**
  - 单事件关联分析
  - 多事件关联分析
- **行为分析**
  - 历史行为比对
  - 访问行为比对
- **情景分析**
  - 漏洞关联分析
  - 资产关联分析

关联分析：基于业务、设备、系统多途径采集的信息进行智能关联分析精准定位威胁，减少人工分析的低价值损耗



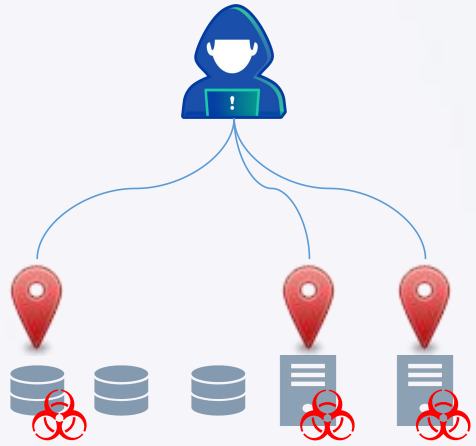
智能推理：通过攻击链关联等（聚类分析、威胁面分析）方式协助运维者进行攻击溯源，提高事件处置效率

（三）智能决策辅助，保障计划精准

SANGFOR 深信服科技

通过对安全事件的智能分析提炼其中关键信息进行可视化呈现，为日常决策提供重要依据

事件影响呈现



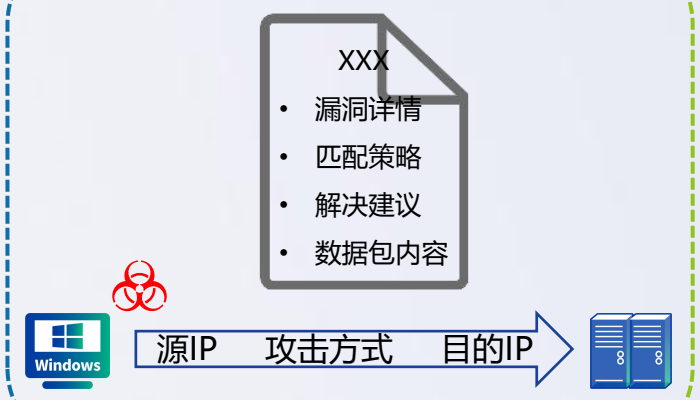
以攻击类型进行归类对资产影响范围及恶性结果进行分析展示，辅助运营规划

多视角分析

- 风险业务视角
- 风险终端视角
- 风险安全域视角
- 安全事件视角

通过对安全风险进行多视角的可视化展示，为事件分析提供依据

攻击行为还原



通过对攻击方式、漏洞情况、攻击分析、解决办法等信息的呈现，还原攻击流程，辅助问题处置

（四）响应处置之事件自动化闭环处置

SANGFOR 深信服科技

预设条件 → 响应策略 → 组件选择 → 策略生成 → 结果反馈

（四）响应处置之多视角闭环，提升运维效率

SANGFOR 深信服科技

通过多种响应处置方式实现事件处置闭环，依靠流程化&自动化提升安全运维效率

SOAR

以业务为中心的流程自动编排

SANGFOR
深信服科技

二、安全运营服务

安全运营人员工作重点

SANGFOR 深信服科技

安全运营工作不能仅依靠技术手段，规范运营人员工作才能让安全实现持续有效的运营

安全负责人

安全工作统筹规划 | 组织制定应急预案 | 跨部门、地区协调 | 监督考核 | 人员、物资保障

安全运维主管

资产管理	漏洞管理	威胁管理	事件处置	线下巡检	定期汇报
资产全面梳理录入	漏洞识别分析	持续检测	入侵影响抑制	设备运行状态	安全现状
明确核心资产	确定处置方案	分析研判	入侵威胁清除	授权情况	防护效果
探测资产变更	漏洞加固	问题处置	入侵原因分析	知识库升级	运营工作成果
维护资产台账	跟踪复测	审核归档	安全建设优化	策略有效性检查	遗留问题

可通过日常运维、应急响应流程完成相应工作

注：除线下巡检外，其他工作安全运维主管及运维人员工作均可依托运营平台完成，定期汇报工作可基于平台可视化报表完成

建立健全基于等级保护2.0的安全管理体系

SANGFOR 深信服科技

安全管理人员　安全管理机构　安全管理制度　安全建设管理　安全运维管理

控制类	安全控制点	文档名称
安全管理制度	安全策略	1、《网络安全工作的总体方针和安全策略》
	管理制度	2、《物理环境安全管理制度》 1、《网络安全管理制度》 2、《办公终端和主机设备安全管理制度》 2、《应用系统安全管理制度》 1、《数据安全管理制度》 1、《安全建设管理制度》 2、《安全运维管理制度》等
		2、《设备操作规程》等
	制定和发布	2、《制度制定、发布、评审和修订管理制度》
	评审和修订	
安全管理机构	岗位设置	1、《网络安全组织机构管理办法》
	人员配备	2、《网络安全组织机构管理办法》
	授权和审批	3、《授权和审批管理制度》
	沟通和合作	3、《沟通与合作管理制度》
	审核和检查	3、《安全审查和检查管理制度》
安全管理人员	人员录用	1、《人员安全管理制度》
	人员离岗	1、《人员安全管理制度》
	安全意识教育和培训	3、《网络安全培训管理制度》
	外部人员访问管理	2、《外部人员访问管理制度》

控制类	安全控制点	文档名称
安全建设管理	定级和备案	/
	安全方案设计	《网络与信息系统安全设计规范》
		/
	产品采购和使用	3、《IT产品采购管理制度》
	自行软件开发	3、《软件开发管理制度》
		3、《代码编写安全规范》
		3、《软件开发文档指南》
		3、《软件开发管理制度》
	外包软件开发	3、《外包软件开发管理规范》
	工程实施	2、《工程实施管理规范》
		2、《安全工程实施方案》
	测试验收	2、《工程测试验收方案》
		1、《系统交付管理》

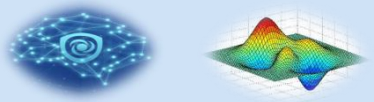
控制类	安全控制点	文档名称
安全运维管理	环境管理	2、《机房安全管理制度》
	资产管理	2、《信息管理制度》 2、《资产信息分类文档》 1、《信息资产管理办法》
	介质管理	3、《介质安全管理规定》
	设备维护管理	2、《设备维护管理制度》
	漏洞和风险管理	2、《风险评估管理制度》 2、《漏洞管理规定》
	网络和系统安全管理	1、《网络安全管理制度》 2、《系统安全管理制度》 1、《账户、密码及权限管理制度》
	恶意代码防范管理	1、《恶意代码管理制度》
	配置管理	2、《基本配置信息记录》
	密码管理	3、遵循相关的国家标准和行业标准要求
	变更管理	3、《变更管理制度》
	备份与恢复管理	1、《备份与恢复管理制度》
	安全事件处置	1、《网络安全事件与应急管理制度》
	应急预案管理	1、《网络安全应急预案》
	外包运维管理	2、《信息安全外包运维管理制度》

建立7*24小时的持续检测、主动闭环的运行机制

SANGFOR 深信服科技

威胁检测平台+安全专家+持续化威胁追踪流程

安全运营中心



安全能力中心

持续赋能

T1安全工程师　T2安全运营专家

攻防对抗专家　T3首席安全专家

安全大数据平台　云端运营团队

MSS分析服务

技术

紧急事警　重要事件

高危漏洞　中危漏洞

失陷事件　情报预警

待处置风险

流程

工单生成
误判确认
遏制影响
问题定位
溯源分析
加固建议

处置过程

系统可实现部分自动化

系统自动化
T1 安全工程师
T2 安全运营专家
升级处理
T3 首席安全专家

人

模式1：共享安全日志，由线上安全专家进行分析及安全事件处置

日志共享

联动处置

IPsec VPN隧道

模式2：本地工单发起，线上专家获取授权后接入本地进行分析研判，T1完成本地处置

本地安全专家

威胁检测平台

针对特殊场景、重大安全事件，需要到现场的，由高级安服人员，到现场进行分析研判、追踪溯源，提供安全加固建设方案；

流量采集探针
IT基础设施和应用系统日志
安全设备日志

威胁采集

资产识别

资产主动识别
资产被动识别

线上线下快速扩展高阶安全专家团队

服务组成员	
项目经理	1、开始启动项目 2、明确服务边界，服务规范、内容和需求 3、准备项目启动会相关材料 4、发起内部启动会并做人员安排 5、协调相关组件设备 6、沟通上架时间、协调首次上门时间 7、上线验收、服务讲解、工具介绍 8、服务交付物质量审核 9、服务汇报及项目验收等组织事宜
线上T1服务经理	1、 平台下发工单后作为第一接口人分析确认是否误报，分析确认后输出解决方案 2、威胁预警通告
线上T2安全专家	1、负责受理T1问题上升来的威胁处置问题，并输出相关处理报告 2、 问题无法处置、分析，上升至T3进行处置 3、安全日志综合分析，并输出威胁分析报告
线上T3安全专家	1、 负责受理T2无法解决的问题并输出相关解决方案
线下安服工程师	1、负责协助上门处置常见安全问题 2、配合云端远程处理安全问题 3、 定期上门汇报
信服小安	1、7*24小时值守将客户提出的问题进行解答。 2、对平台的安全事件进行分析预警并协助处置
服务质量管理（QA）	1、负责项目的进度及质量监管 2、负责组织审核确认各过程文档

Web管理端

微信服务群

邮 件

紧急电话

三级安全专家的配合示例

SANGFOR 深信服科技

S1： 运营中心监测到病毒

SOC发现病毒

S2： 中心发起处置工单

发起工单

S3： T2运营专家在线审核

T2专家在线审核

T1专家处理问题

S4：T1工程师和T3首席专家处理问题

用户发现病毒

T3专家处理问题

问题复核

S5：问题复核

处理完成

S6：处理完成归档

标准化的专家协同配合流程机制，线上跟踪安全事件的各个环节，确保专家之间的配合透明、可跟踪。

SANGFOR
深信服科技

三、方案特色与价值

方案特色：7*24小时持续有效

SANGFOR 深信服科技

多手段响应闭环，提升运维效率

安全成果可视，不断检视优化

多场景运营流程，有序消除隐患

威胁深度挖掘，持续策略调整

方案价值

SANGFOR 深信服科技

提升安全效果

- 持续威胁感知
- 智能分析定位
- 深度威胁挖掘
- 持续策略优化

提升运维效率

- 智能辅助决策
- 规范运营流程
- 建立处置机制
- 人机交互运维

安全效果可视化

- 漏洞修复比例
- 事件处置成果
- 安全整体评级
- 安全建设指标

有效解决安全运营工作的三大内部挑战：安全能力不足、运维工作压力大、安全效果不明显

SANGFOR
深信服科技

一．XXXX安全建设背景

二．XXXX安全建设思路

三．安全运营中心解决方案

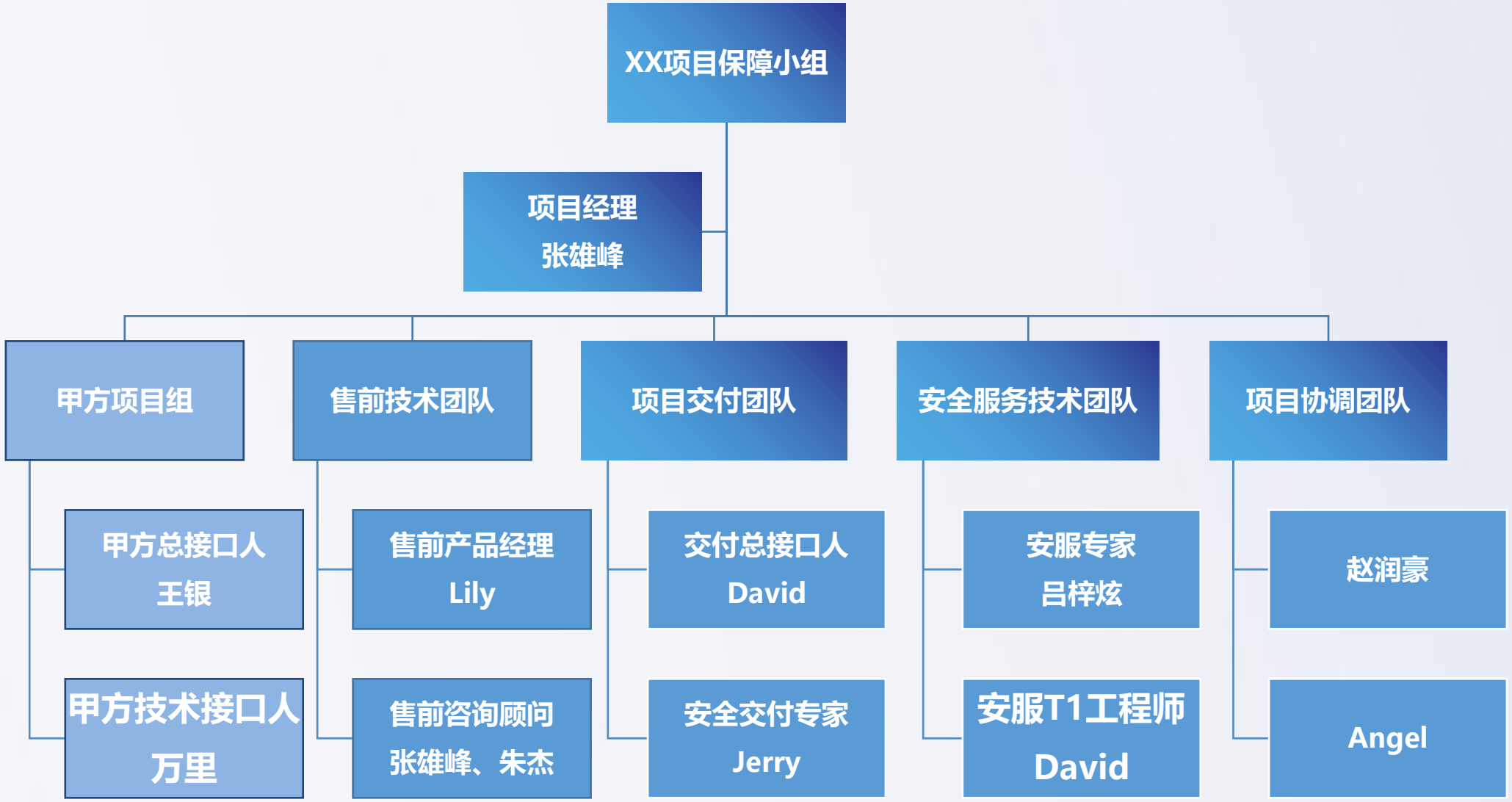
四．项目团队及实施计划

项目清单

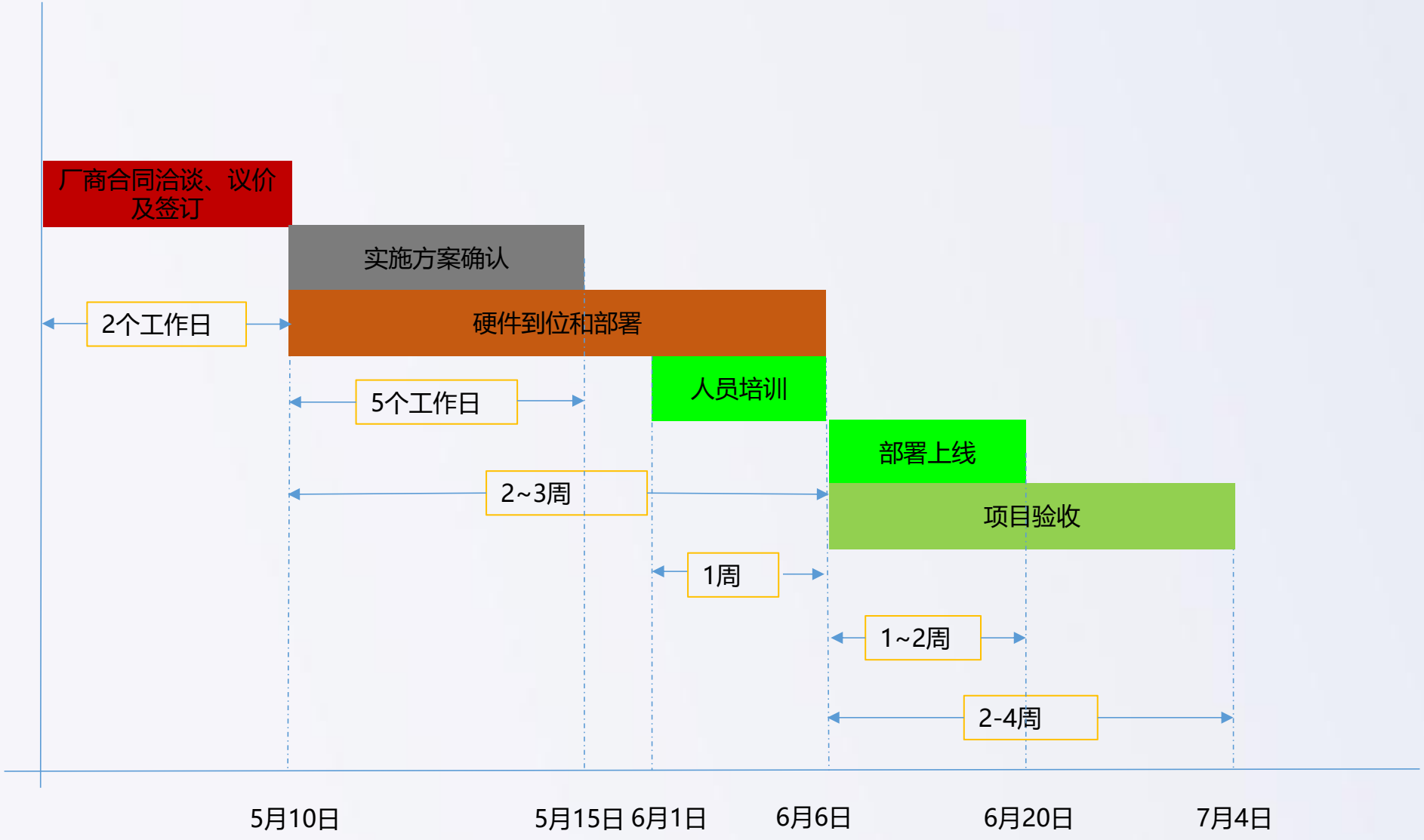
项目名称	产品名称	产品简介	数量
软硬件产品	终端检测与响应平台EDR	---轻量易用： 客户端轻量化业务无感知，自动构建防御，无需精力投入，半自动化安全运维 1、轻代理业务零侵害，客户端只保留核心功能，重载功能合入平台； 2、配置界面符合中国运维习惯，可视化操作最低学习成本； 3、一个管理平台，全面兼容，架构升级，安全始终适配； ---实时保护： 基于威胁攻击链多达30个功能构建多层次全生命周期立体防护 1、预防阶段核心优势：轻补丁漏洞免疫； 2、防护阶段核心优势：无文件攻击保护，勒索病毒专项防护 3、检测与响应阶段核心优势：基于AI的恶性病毒处置修复能力； ---东西向可视可控： 创新微隔离技术基于业务维度让终端间流量可视可控，同时做到简单落地，高效运维	每台服务器1个授权
	上网行为管理	本地办公人员的上网访问行为审计，上网日志全留存，做到事中审计，事后追溯	每个办公地点2台
	SSL VPN	通过SSL VPN加密隧道做到远程办公人员访问内网的安全接入	1台
	下一代防火墙	出口边界隔离，做到2-7层网络安全防护	每个IDC至少2台
	流量探针STA	探针STA采集全网流量进行预处理，将有效安全日志同步到态势感知SIP进行全网流量可视化分析和监测。	每个IDC机房至少一台
	态势感知平台SIP	深信服安全感知平台定位为本地的安全大脑，是一个集检测、可视、响应处置于一体的大数据安全分析平台，让安全可感知、易运营。产品以大数据分析为核心，结合了威胁情报、UEBA、机器学习、失陷主机检测、大数据关联分析、NTA流量分析、可视化等技术，对全网安全进行可视，帮助用户看清业务、看到威胁、看懂风险，并辅助用户决策。	至少1台

项目名称	交付内容		交付方式	交付频率	时间期限
安全运营服务	漏洞管理	漏洞分析与管理	安全专家+安全运营组件	7*24h	1年
		弱口令分析与管理	安全专家+安全运营组件	7*24h	
		最新漏洞预警与响应（可选）	安全专家+安全运营组件	7*24h	
		漏洞协助处置（可选）	安全专家+安全运营组件	7*24h	
	威胁管理	威胁分析与预警	安全专家+安全运营组件	7*24h	
		流行威胁通告与排查	安全专家+安全运营组件	7*24h	
		主动分析与响应	安全专家+安全运营组件	7*24h	
		策略管理	安全专家+安全运营组件	7*24h	
		持续攻击对抗	安全专家+安全运营组件	7*24h	
	事件管理	事件分析与处置	安全专家+安全运营组件	7*24h	
		应急响应	安全专家+安全运营组件	7*24h	
	运营可视	安全运营可视化	安全专家+安全运营组件	7*24h	
		定期安全运营汇报(事件分析与处置报告、漏洞协助处置报告、应急响应报告、综合分析报告、安全通告、季度汇报、年度汇报、漏洞举证报告、最新漏洞通告)	安全专家	每季度一次	

项目实施组织安排


XX项目保障小组
项目经理
张雄峰
甲方项目组
甲方总接口人
王银
甲方技术接口人
万里
售前技术团队
售前产品经理
Lily
售前咨询顾问
张雄峰、朱杰
项目交付团队
交付总接口人
David
安全交付专家
Jerry
安全服务技术团队
安服专家
吕梓炫
安服T1工程师
David
项目协调团队
赵润豪
Angel

项目实施周期安排


厂商合同洽谈、议价及签订
实施方案确认
2个工作日
硬件到位和部署
5个工作日
人员培训
部署上线
2~3周
项目验收
1周
1~2周
2-4周
5月10日
5月15日 6月1日
6月6日
6月20日
7月4日

SANGFOR
深信服科技

THANK YOU

深信服 张雄峰