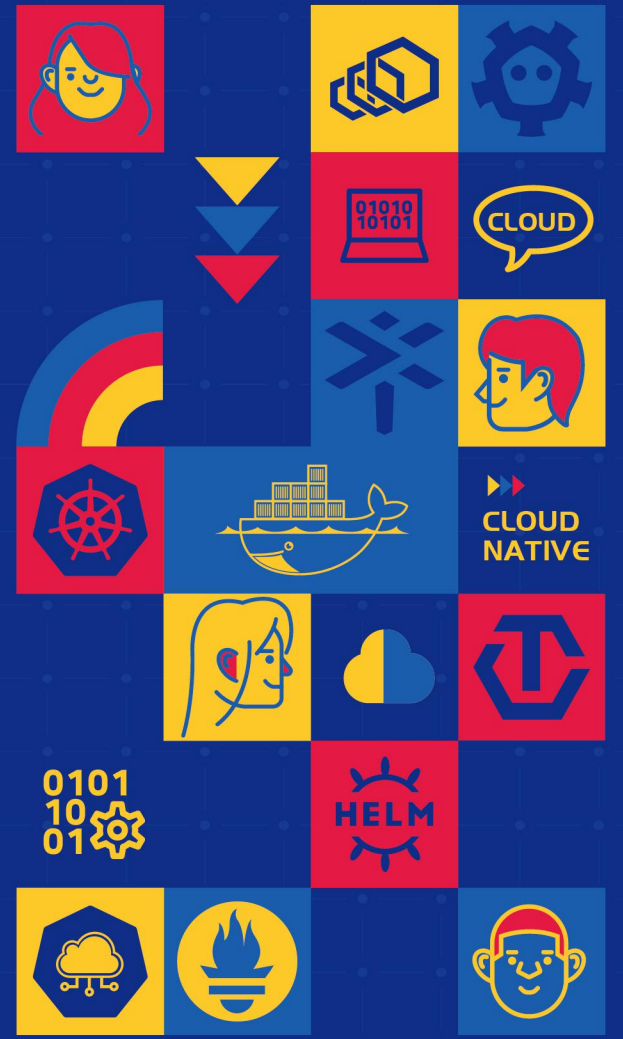
云原生产业大会
2021 CLOUD NATIVE INDUSTRY CONFERENCE
2021/05/26 × 中国 / 北京
原生蓄力 云领未来

浙江移动IT云安全防护实践

徐良

CAICT 中国信通院



安全工作思路

构筑多元立体、集中开放、智能随需的主动防御安全体系，推动网络安全赋能数智化发展。

关键举措

管理理念创新：从“合规管理”转向“网络对抗”。

运营机制创新：从“静态防护”转向“积极防御”。

技术手段创新：从单一孤立的手段建设转向多元化的、联动一体的技术研发。

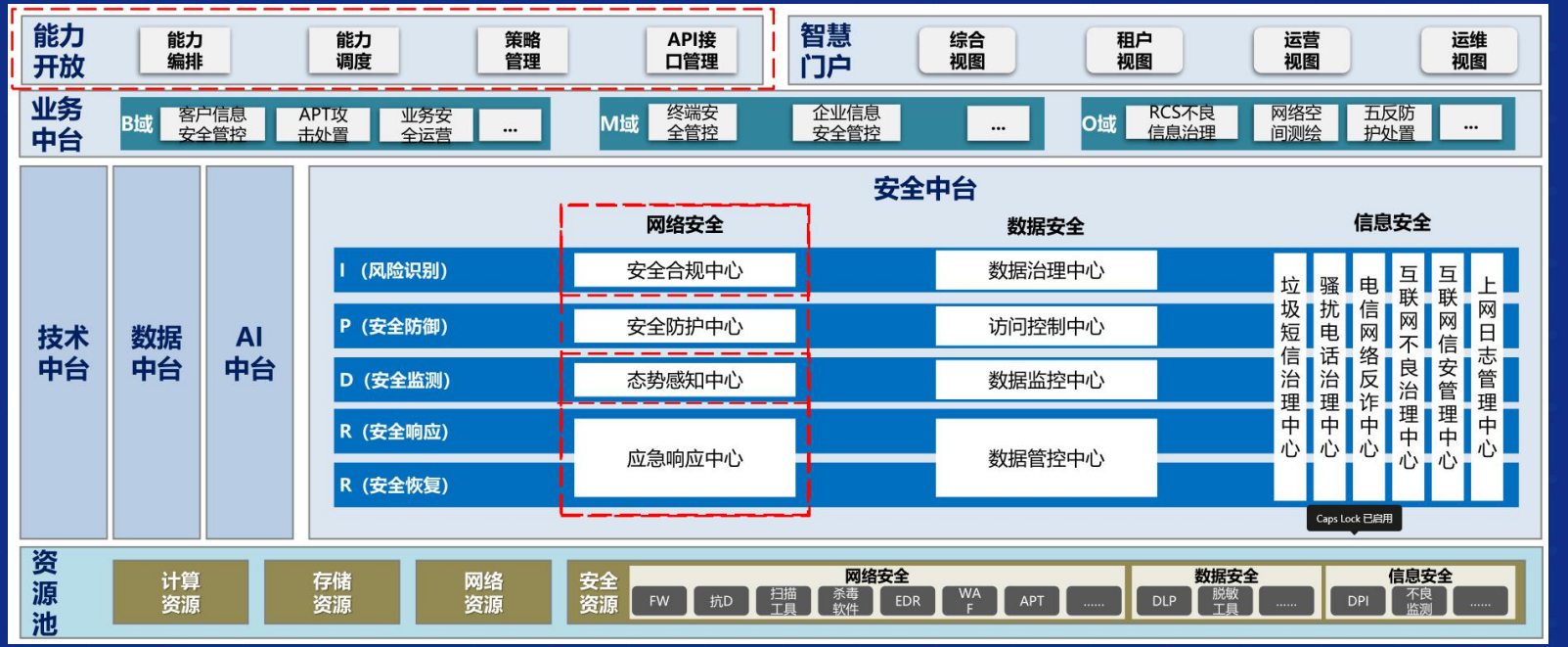
发展模式创新：从“业务安全”转向“安全业务”。

基于IPDRR模型建设安全智慧中台

从风险识别、安全防御、持续监测、安全响应和安全恢复5大方面全面构建**智能化的安全能力体系**，赋能各类安全业务，构建技术和运营协同的积极防御安全体系，助力实现网络安全的可管可控。

安全智慧中台规划蓝图

中台对已有安全能力基于“高内聚、标准化、可复用”的原则进行组件化，通过业务场景管理、跨中台业务编排能力，满足内外部用户各类业务场景对安全能力的需求，落实网络安全的风险识别、安全监测、安全响应、安全恢复能力。

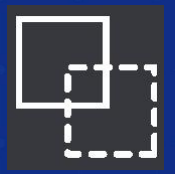


智慧中台支撑网络安全威胁监测及应急处置

以场景事件为牵引，构建安全能力图谱，快速精准的形成自动化响应处置能力，驱动的各设备协同工作，面向前台安全业务需求规模化开放复用，提升安全响应的速度和效率。

剧本

基于任务的图形工作流程，实现跨安全产品的流程可视化



知识库

安全问题知识图谱
安全能力图谱
安全处理流程图谱

日志统一收集&分析——智能研判

剧本 - 自动化工作流

IT云安全防护存在的难点

云上资产多、租户多，漏洞加固压力大，随着业务营销的互联网化，一线赋能、能力开放等新的场景增加了网络安全防控的难度，不少问题也随之显现。

01 云内部威胁监测及防护的问题

02 开源组件引入成为安全漏洞主要来源

03 暴露面应用安全评估加固的问题

04 定向安全应急处置能力提升的问题

IT云安全防护举措

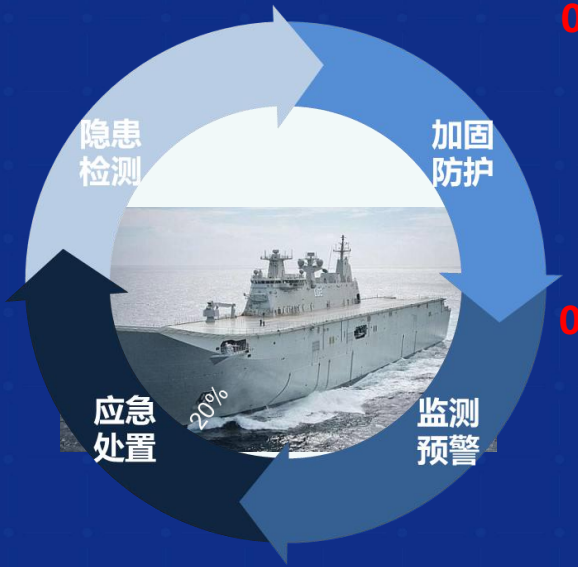
以“知彼知己，百战不殆”为作战指导思想，加强主动防御、纵深防护，提升0/1Day漏洞攻击、近源攻击和社会工程学攻击监测和防护能力。

01、评估加固

- **密闭性检修—访问控制策略审计加固**：防火墙策略/高危端口审计及策略优化
- **破损检修—漏洞评估加固**：系统及应用漏洞评估加固、组件镜像安全防护
- **后门检修—病毒木马清理**：主机病毒、木马、WEBSHELL检测与清理
- **军事化管理—账号访问管控**：VPN账号权限清理、应用访问强认证、 弱口令检测与加固

04、应急处置

- **战斗损管系统—应急处置**：网络应急处置、系统应急处置



02、攻击防护

- **舰体隐身—暴露面缩减**：临时关停网站
- **装甲—边界防护**：防火墙、WAF、防篡改
- **密封舱—纵深防护**：**租户微隔离**、容器应用微隔离

03、威胁监测

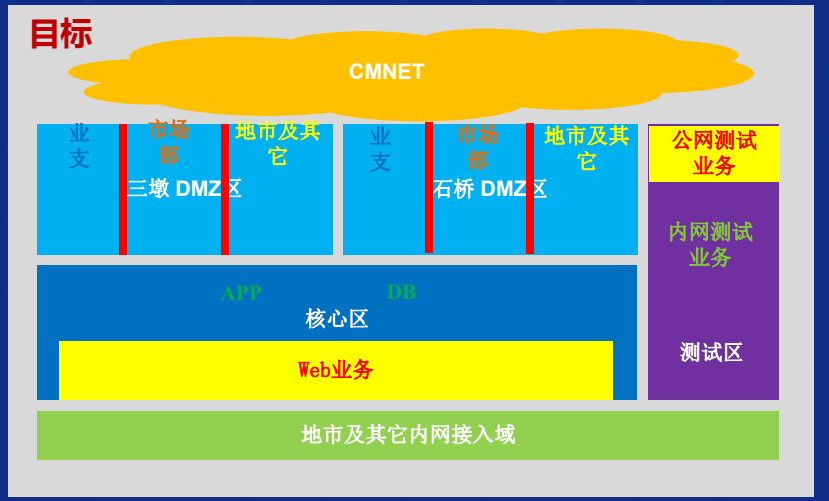
- **声纳、雷达—网络威胁监测**：互联网/IDC/外部接口/核心域边界WEB/APT威胁监测
- **舱体侵入报警—系统威胁监测**：主机威胁监测、横向威胁监测
- **防敌特—社工威胁监测**：社工钓鱼监测/恶意域名监测
- **电磁泄露监测—数据泄露监测**：GitHub、百度网盘等信息泄露排查

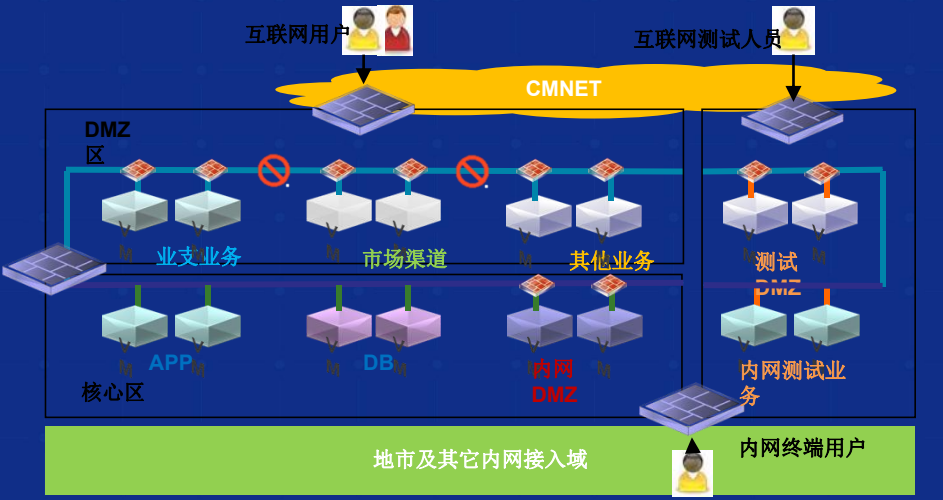
容器安全防护

云原生的快速推进，以容器为核心的生态迅速成长，通过开展容器安全防护试点，提升云资源池安全防护能力。

IT云租户及容器应用微隔离

- 进行主机虚拟化网络层改造，部署分布式防火墙， 实现每个虚拟机或容器都有自已的防火墙。
- 业务租户之间、外部业务与核心业务之间，通过虚机/容器的分布式防火墙基于主机属性、业务属性、IP网段进行隔离，满足租户业务区域安全隔离，同时实现租户内部不同应用的细粒度隔离。





开源组件安全防护

加强开源组件引入的安全管理，提升第三方开源组件资产识别和漏洞检测能力，做好组件引入的安全防护。

01 开源组件安全防护手段建设

- **开源组件识别：**提升资产自动化清点能力，实现各类主流中间件、WEB应用框架和组件的快速检测识别。
  - WEB框架组件：Apache（shiro、axis、dubbo、solr）...
  - WEB插件：fastjson、spring、Jenkins...
- **组件漏洞检测：**基于CVE、CNVD等漏洞披露信息，建立组件漏洞信息库，通过系统层文件信息、版本信息、配置信息、进程信息的综合分析比对，实现组件漏洞的快速检测，解决传统扫描器检测耗时长、覆盖不全的问题。

02 开源组件安全运营管理提升

- **安全基线管理：**针对引入的开源组件，编制组件安全基线规范
- **软件镜像安全：**开源组件发布上线前必须经过安全评估加固，加固后的组件由技术栈统一打包到基础镜像中，实现统一管理。

精准监测： 监测能力提升

主机监测能力

入侵检测 **欺骗防御** **威胁狩猎**

1、入侵检测：完善攻击监控能力，如无文件攻击、内网隧道攻击能力，提升后门提权、反弹shell监测能力。
2、欺骗防御：建设仿真环境，通过资产隐藏与威胁检测能力并用，实现对文件、进程、勒索攻击的威胁诱捕。
3、威胁狩猎：通过对操作、网络连接、进程启停、账号等行为进行监测，实现主机全行为周期的安全威胁研判。

终端监测能力

资产溯源 **终端威胁监测**

1、资产溯源：通过防病毒软件，有效掌握终端IP地址、主机名、MAC地址等信息，方便安全事件溯源。
2、威胁监测：部署终端防病毒高级威胁检测及响应子系统，实现终端异常文件操作、注册表操作、系统事件、网络事件的监测，提升终端攻击行为分析能力。

钓鱼监测能力

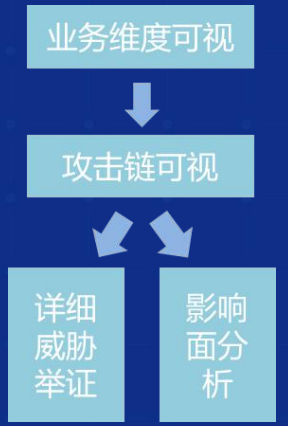
沙箱文件检测 **URL回连检测** **威胁情报关联**

1、沙箱文件检测：提升沙箱文件检测功能，除病毒木马检测外，新增文件执行动态检测分析能力。
2、URL回连检测：识别邮件中的URL，利用RPA工具对URL进行访问，识别是否下载执行恶意代码。
3、威胁情报关联：打通云端威胁情报网，判别回连IP、域名是否恶意。

精准监测：提升横向威胁分析能力

基于主机防火墙网络访问日志，利用大数据和AI手段，实现网络访问行为全链路追踪，拉通系统和网络威胁告警，提升横向威胁攻击分析能力。

□访问全链路拓扑构建及异常发现：基于资源与网络访问流量形成全链路拓扑，利用AI手段发现异常网络访问行为。



□横向威胁发现：对全网链路与各资源节点进行攻击监测，实时发现链路中横向移动，检测威胁情况。

安全事件自动化处置

依托中台SOAR能力，打造自动化安全运营处置体系，新增系统层威胁应急处置能力，实现问题资产网络或账号的快速隔离。

告警管理
告警信息补充，输出高质量、有价值的告警信息

案件管理
聚合告警信息、积累案件相关证据、丰富案件信息、判定威胁级别指派案件处理流程

剧本管理
规范化标准处理流程、积累安全知识库，积累安全处置能力

自动化编排
快速有效的制定安全处理流程，协调安全产品和工具，完成调查处置响应过程

自动化引擎
自动化执行剧本，加速响应并使分析师能够重新获取高优先级事件

开放式接入
开放性扩展接口，安全应用快速集成

SOAR

- 流程编排
- 安全剧本
- 自动调度
- 安全组件

剧本

- 钓鱼邮件处理
- 反弹行为处理
- 横向渗透处理
- 暴力破解处理
- 异常位置登录
- ……

脚本

- 路由器封堵IP
- 防病毒扫描
- 封禁用户
- 信誉查询
- ……

插件

- 防火墙
- 路由器
- DNS
- 防病毒
- 沙箱检测
- 威胁情报
- ……

接口

- 封堵IP
- 封堵域名
- **禁用用户**
- **查杀进程**
- **隔离网络**
- IP信誉查询
- 域名信誉查询
- 文件信誉查询
- ……

开展红蓝对抗演练

以建设纵深立体的防御体系为导向，开展红蓝对抗演练，检验现有安全防范水平，发现安全薄弱环节，为后续安全建设和运营提升明确方向，达到以攻促防的目的。

01 演练方案

- **演练规则：**
  - 制定红蓝双方得分规则，建立奖励机制。
  - 预防演练对业务系统造成破坏性影响。
  - 设置对抗演练关键指标，完善演练方案和演练场景。
- **演练频度：**定期开展大规模对抗演练，不定期开展预设场景演练。
- **演练复盘：**做好攻击过程所有关键行为与蓝方监测记录数据对账，检验监测能力和效果，能否还原整个过程监控，检查是否存在缺失，还需要在哪些方面进行改进和提升，是否存在安全盲区？

02 演练场景

- **定向信息收集：**
  - 收集暴露面资产域名、网站、IP、敏感目录和文件、开放端口和中间件信息，寻找渗透点
- **定向网络攻击测试：**
  - 纵向攻击测试（远程攻击、生产网内网攻击、办公网内网攻击）
  - 横向攻击测试（内网横向移动、关键数据/控制权限获取、痕迹隐藏）
- **社会工程学测试：**安全意识测试（邮件钓鱼）、人员权限攻击测试等
- **近源攻击测试：**办公场地入侵、办公网络入侵、办公电脑木马植入测试。

云原生 产业大会
2021 CLOUD NATIVE INDUSTRY CONFERENCE
2021/05/26 × 中国 / 北京
原生蓄力 云领未来

THANKS !

CAICT 中国信通院