执行体全量识别与精细管控

混合云场景威胁猎杀

安天 | 安全服务中心

目 录

01 云上网络安全需求

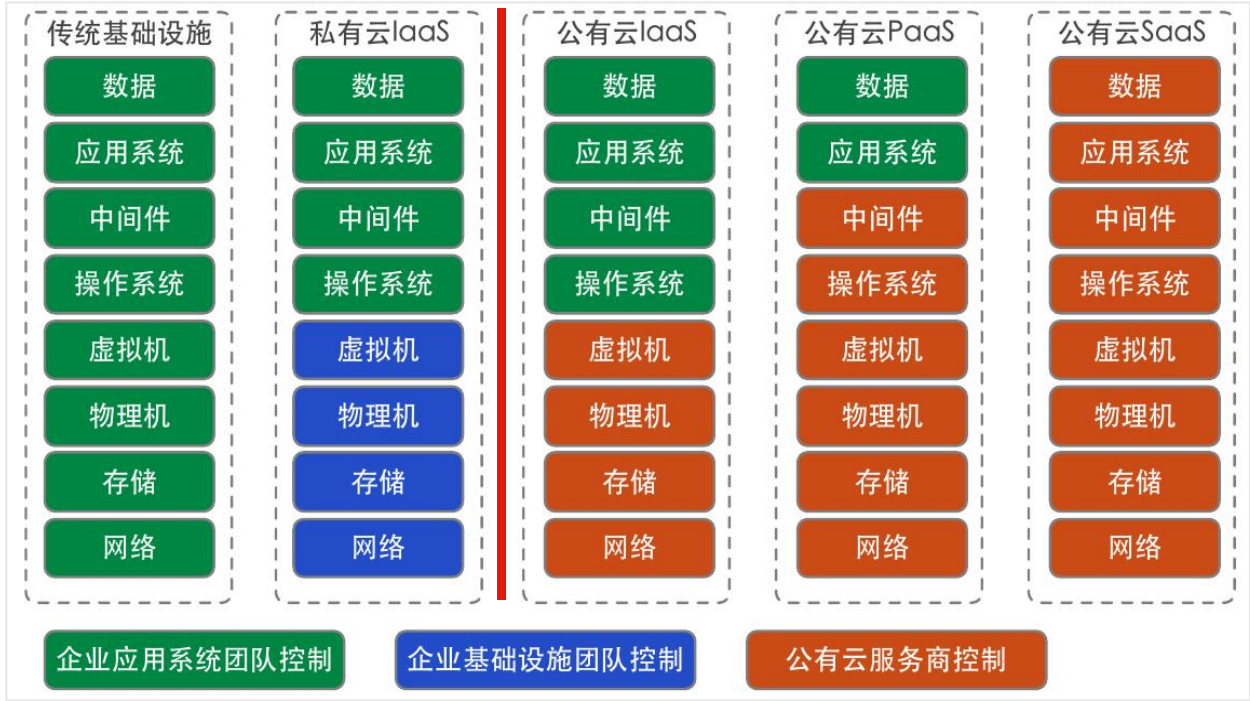
云供应商与云租户的责任边界

云服务商

- IaaS服务类别，负责底层的物理和虚拟资源；
- PaaS服务类别，负责底层的物理、虚拟资源和PaaS服务的软件平台；

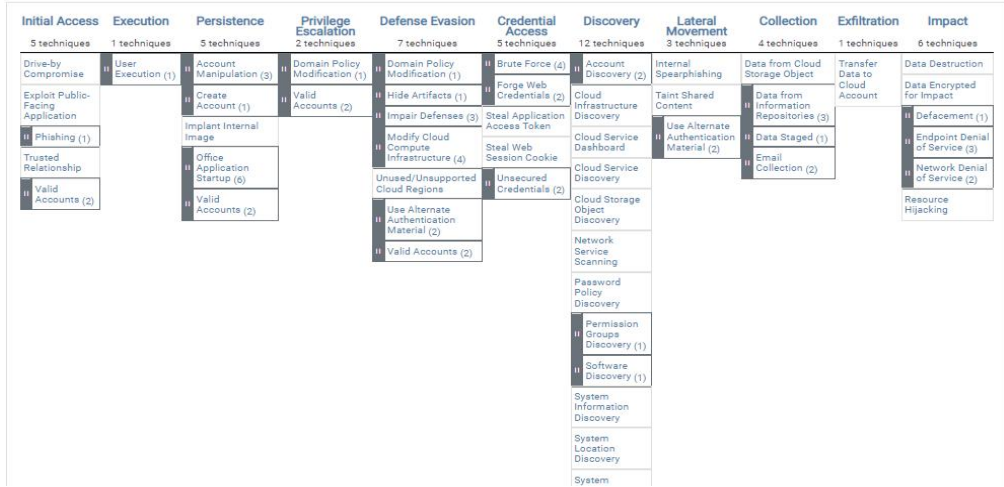
应用系统团队

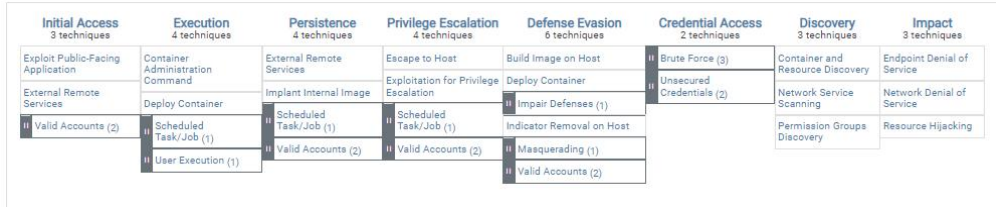
- IaaS服务类别，负责访问和使用IaaS服务的用户凭证、工具、应用系统、中间件、数据；
- PaaS服务类别，负责访问和使用PaaS服务的用户凭证、工具、系统、数据。



合规性需求与威胁对抗需求

云计算安全扩展要求	控制点
安全物理环境	基础设施位置
安全通信网络	网络架构
安全区域边界	访问控制、入侵防范、安全审计
安全计算环境	身份鉴别、访问控制、入侵防范、镜像和快照保护、数据完整性和保密性、数据备份与恢复、剩余信息保护
安全管理中心	集中管控
安全建设管理	云服务商选择、供应链管理
安全运维管理	云计算环境管理





ATT&CK

信息系统安全防护工作模式需要演进

满足一系列信息安全标准与法律法规的相关防护要求，“**被动合规**”工作模式	工作模式	应立足于更加积极的合规驱动工作模式，并针对重要领域实现**主动有效的全方位体系化防护**工作模式
信息安全**风险管理模式**，“突出重点、平衡风险、适度安全”	防御理念	根据网络与信息系统的国家安全、社会安全和业务安全属性，客观判断必须能够**有效对抗**哪些层级的网络空间威胁，并据此驱动网络空间安全防御需求
尝试罗列各种可能的网络威胁，并设计零散防御措施进行被动应对的传统式**“威胁导向建设模式”**	建设模式	全面建设必要的网络安全防御能力，并将其有机结合形成网络空间防御体系的“**能力导向建设模式**”

引自：黄晟《网络空间安全防御与态势感知》译者序

安全运营需求

资产与系统　应用与执行体　网络与拓扑　身份和账户　数据与业务

02 威胁猎杀实践案例

背景与需求

2022年8月，安天为某单位开展安全运营服务，通过部署安全运营中心与主机探针，安全运营工程师与威胁猎杀工程师持续开展实战化运营。

1.数据中心（物理服务器）

测试系统

部分存续系统

2.行业云

OA系统

上云系统

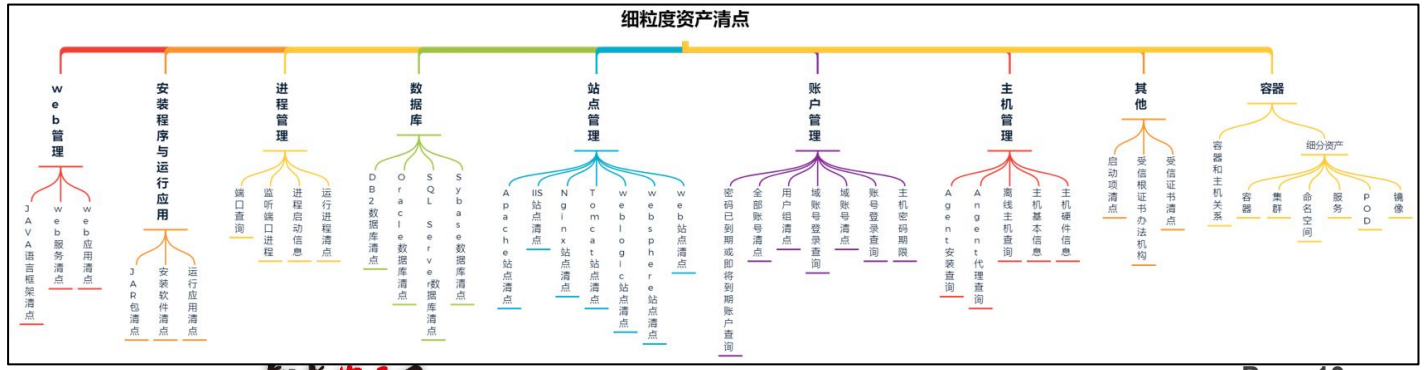
3.超融合

各部门生产系统

日常安全运营工作开展

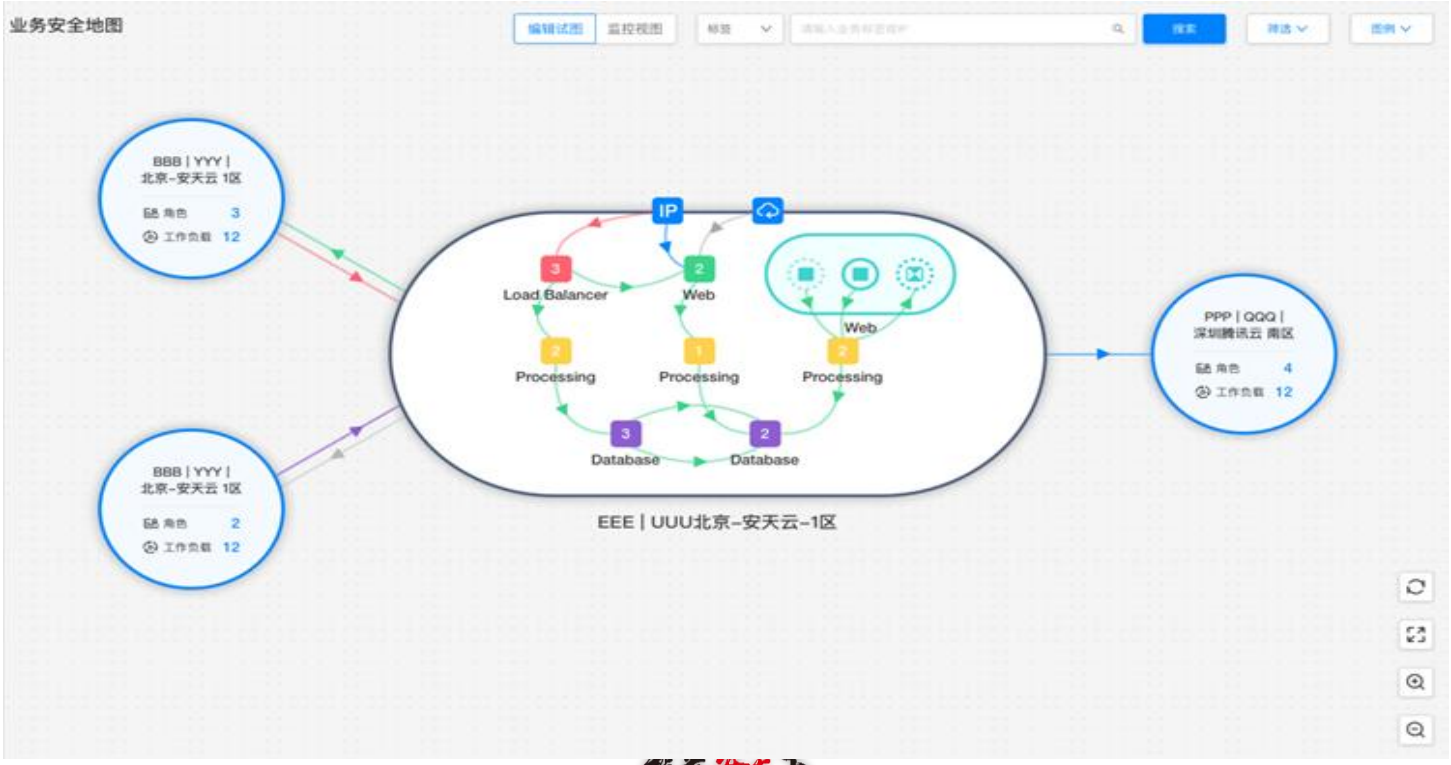
- 安全运营工程师通过安全运营中心向客户端下发指令，实现资产管理、配置核查、风险核查、漏洞管理；掌握全网业务资产安全状态
- **资产管理**可实现进程级资产梳理
- **配置核查**可按照csa、等级保护要求等标准开展核查工作
- **弱口令核查**可对主机与应用开展核查，告警弱口令

- 支持Windows、Linux操作系统各发行主流版本，自动化识别主机层面基础软、硬件环境信息。包括主机信息、硬件配置、系统账号、进程端口、软件应用、数据库、web应用、web服务、web站点、web应用框架、安装包类库、系统环境等。如：Nginx、Apache、JBoss、Mysql、Memcache、Redis、HBase等主流中间件、数据库、应用资产等。
- 支持容器资产包括容器集群、命名空间、服务、POD、节点、镜像、镜像仓库。自动获取与容器相关信息，如：容器的运行状态、连接情况、关联镜像等。



日常安全运营工作开展

- 安全运营工程师通过掌握资产清单，与运维人员调研，梳理资产访问清单列表，明确各业务安全组，参考应用部署位置、访问需求
- 通过主机探针的安全能力，划分安全组。如云上业务1安全组、IDC业务2安全组、安全管理安全组



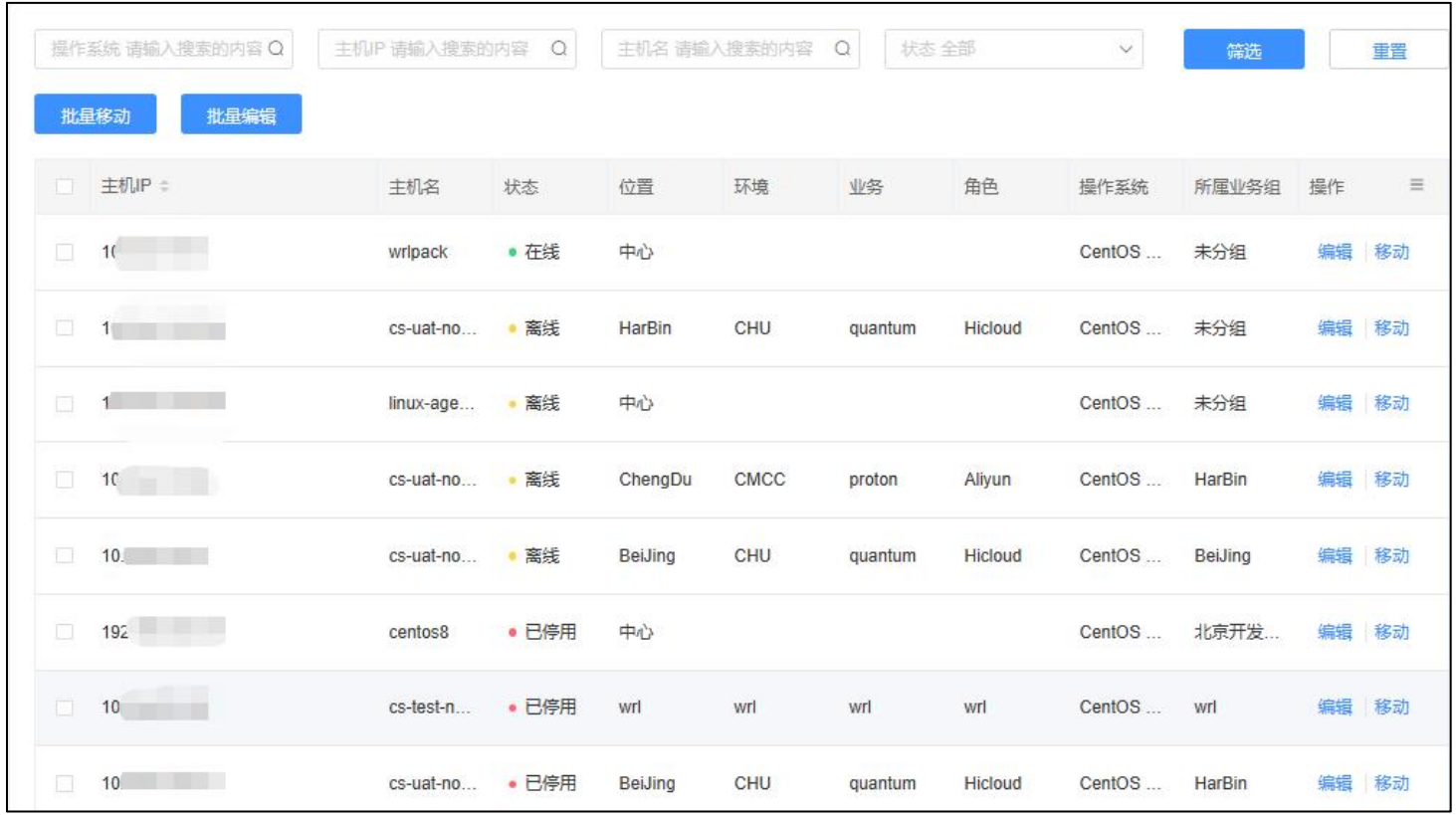
日常安全运营工作开展

安全运营工程师每天巡检安全运营中心的安全事件告警，响应处置包括：

- ✓ 行为基线
- ✓ 异常登录
- ✓ 暴力破解
- ✓ 勒索、挖矿
- ✓ 本地提权
- ✓ WebShell
- ✓ 反弹shell
- ✓ 防篡改

威胁猎杀——异常线索

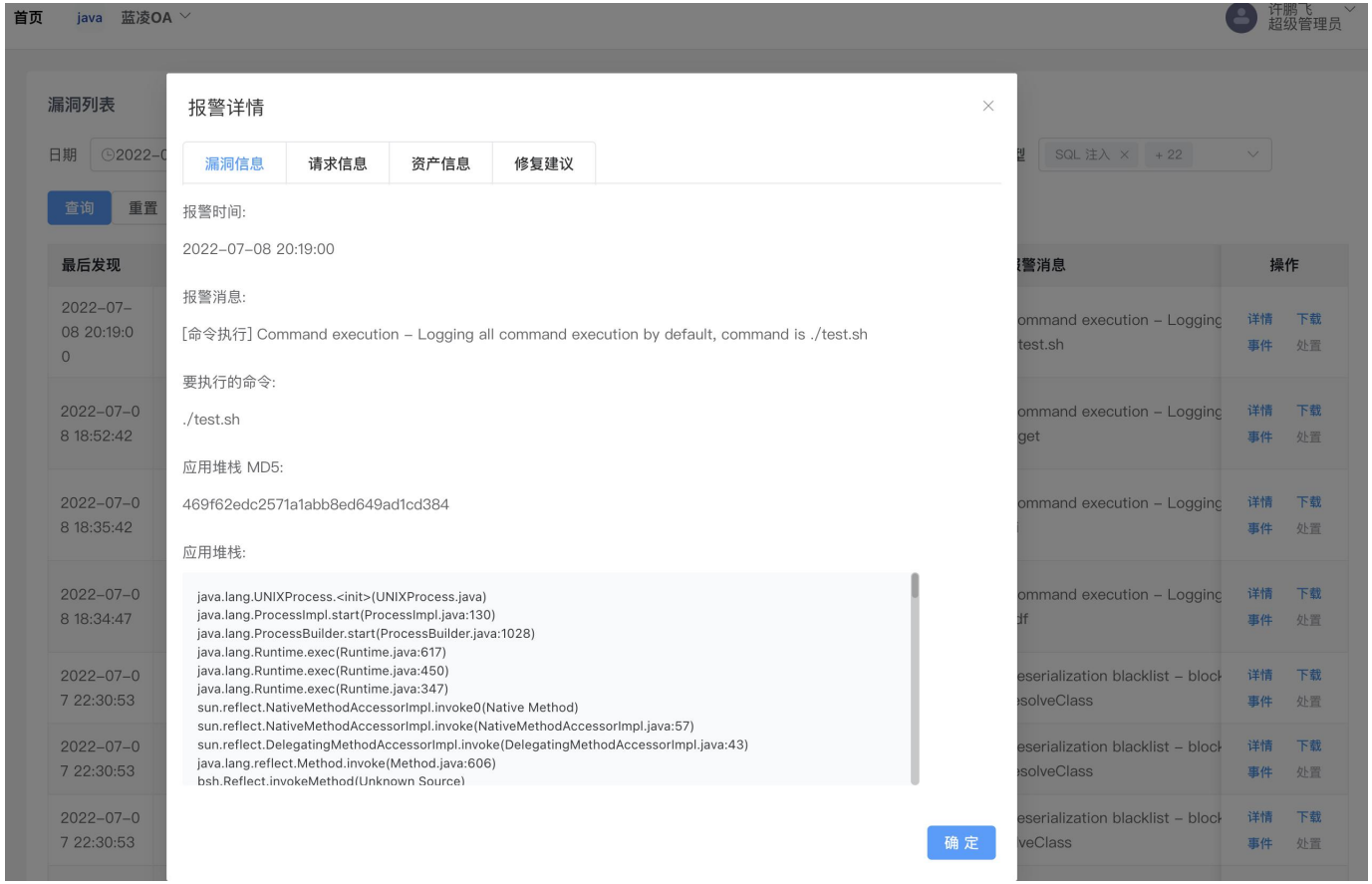
- 安全运营工程师于清晨8:00巡检，发现运行OA系统云主机，安全探针处于离线状态
- 查看安全运营中心，凌晨02:38安全探针下线
- 此事件开展排查，确认探针下线时间无运维人员操作，此前未出现自动下线事件
- 工程师登陆主机，排查网络连接，未发现异常连接



主机IP	主机名	状态	位置	环境	业务	角色	操作系统	所属业务组	操作
10	wrlpack	在线	中心				CentOS ...	未分组	编辑 | 移动
1	cs-uat-no...	离线	HarBin	CHU	quantum	Hicloud	CentOS ...	未分组	编辑 | 移动
1	linux-age...	离线	中心				CentOS ...	未分组	编辑 | 移动
10	cs-uat-no...	离线	ChengDu	CMCC	proton	Aliyun	CentOS ...	HarBin	编辑 | 移动
10.	cs-uat-no...	离线	BeiJing	CHU	quantum	Hicloud	CentOS ...	BeiJing	编辑 | 移动
192	centos8	已停用	中心				CentOS ...	北京开发...	编辑 | 移动
10	cs-test-n...	已停用	wrl	wrl	wrl	wrl	CentOS ...	wrl	编辑 | 移动
10	cs-uat-no...	已停用	BeiJing	CHU	quantum	Hicloud	CentOS ...	HarBin	编辑 | 移动

威胁猎杀——定位威胁入口

- 工程师查看安全运营中心的日志，发现人为卸载主机探针
- 工程师第一时间重启客户端
- 经确认，此OA系统为最新版本，无历史漏洞
- 由于安全探针未开启运行时保护能力（rasp），工程师临时向OA系统下发rasp能力，
- 通过蹲守，rasp能力发现攻击者使用OA软件N day漏洞利用，攻击OA系统
- 经了解，OA厂商升级时，由于升级包影响业务，故仅修复部分漏洞，同时将版本变更为最新
- 工程师将rasp监控策略，设置为阻断策略
- 在防火墙将攻击IP配置阻断策略



威胁猎杀——事件排查

- 安全运营工程师排查现场流量溯源设备，分析02:38 - 08:00流量
- 通过比对，发现此期间云主机与超融合主机间3000端口的通信次数频繁，较前一周有所提升
- 3000端口为免费运维软件A数据传输的通道，且是超融合主机仅对外开放的端口
- 工程师提取该运维软件，将运维软件交于恶意代码分析师研判

威胁猎杀——事件排查

- 工程师排查该免费运维软件，将软件交于恶意代码分析师分析研判

威胁猎杀——事件排查

- 工程师排查该免费运维软件，将软件交于恶意代码分析师分析研判

威胁猎杀——事件排查

- 工程师排查该免费运维软件，将软件交于恶意代码分析师分析研判

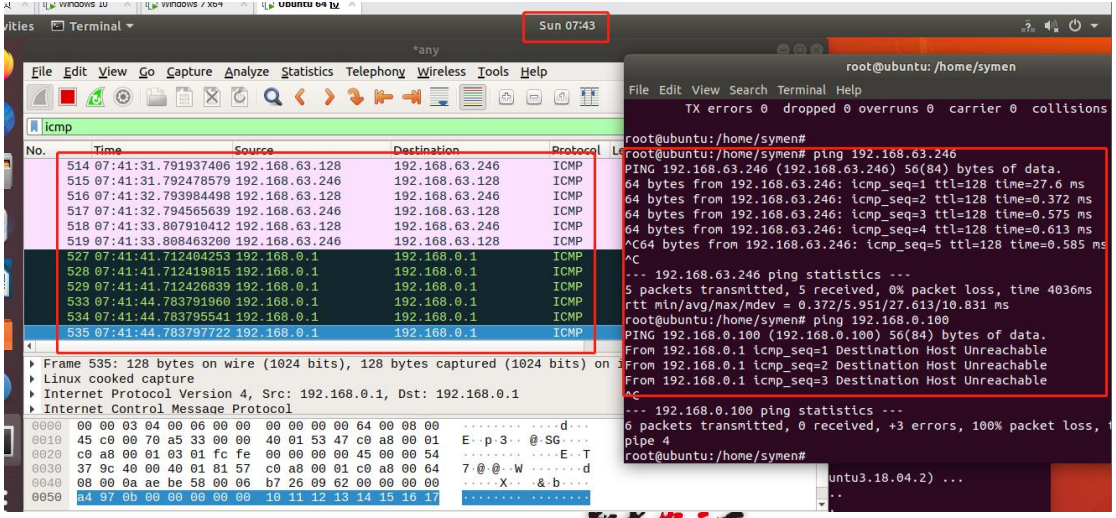
威胁猎杀——事件排查

- 恶意代码分析工程师动态调试

威胁猎杀——事件排查

- 工程师在涉事主机开展取证分析,查看安全运营中心日志记录，攻击者在主机创建一块虚拟网卡，实现模拟虚假IP；
- 增加路由访问特定网段。通过虚拟IP在内网开展资产探测，混淆自身实际入侵主机IP

```
93  ifconfig
94  ifconfig ens33:0 192.168.63.100 netmask 255.255.255.0 up
95  route add -net 192.168.63.0/24 dev ens33:0
96  ping 192.168.163.136
```



威胁猎杀——事件处置

- 处置工程师在安全运营中心下发策略，移除恶意运维软件，并重启服务器；
- 处置工程师沟通厂商修复OA系统漏洞，并全网探针增补rasp能力，防护业务应用
- 工程师评估网内安全损失
- 工程师协助用户对下级单位开展安全预警

威胁猎杀——总结

- 敌已在内、敌情不明”
- 传统安全设备
- 云基础设施基础防护
- 传统威胁对抗经验

用户能力

受害用户

安天赋能

- 高水平分析团队
- 高水平威胁对抗团队
- 威胁情报赋能
- 云主机安全产品赋能

- 团队化作业，分工明确
- 成熟商用军火平台
- 加密流量混淆
- 多重加密shellcode

行为能力

高能力网空威胁行为体

作战实力

- 对主流杀软免杀
- 无实体文件落地
- 关闭UAC、杀软
- 删除主机日志

03 云上安全运营方案

云上安全运营

安全运营团队使用云安全管理平台与客户端，开展资产管理、配置管理、漏洞与补丁管理、安全风险管理等，安全运营团队在网内持续开展安全猎杀，对网内异常实现闭环处置。

One团队

One中心

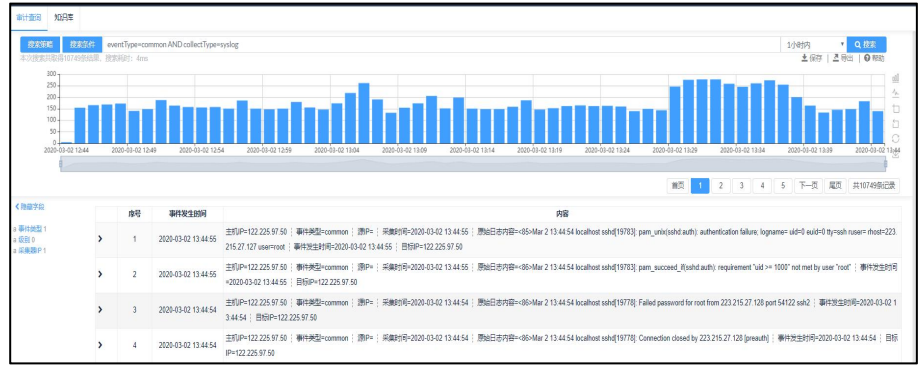
One Agent

团队支撑要素

	角色名称	角色职责	能力要求
	威胁猎杀分析师	负者对监控的到全流量和日志信息进行分析，找出异常和可疑信息，并进行分析，提出/更新假设，给出需要取证的清单列表；	网络协议分析技术、异常分析、日志分析、大数据分析、关联分析等等
	安全运营工程师	负者对取证清单列表进行取证； 负者对处置指南进行处置； 负者对来自外部情报和内部情报进行收集整，将情报中的IOC、TTP等	网络协议分析技术、全平台取证技术、数据库取证、数据恢复技术、对应工具使用等
	逆向分析工程师	负者对恶意样本的解剖分析，对样本的网络特征和文件特征进行提取，提取后的特征会分发给各产品下发规则进行排查，形成排查工具等，最后分析师通过关联分析和朔源分析形成分析报告。	高级威胁分析、二进制深度逆向分析、取证分析、工具开发等、
	指挥协调员	负者指挥排查处置工作和与客户侧人员协调等工作；	全局视野和全面的知识体系、沟通能力、表达能力等
	客户系统管理员	负责设备安装调试工作 ； 负责协助取证工作、部署/增补信息采集点； 负责协助现场工程师进行排查处置工作；	网络规划、日常运维、网络结构、网络设备安装调试、网络协议、故障检测等
	客户控制工程师	负责协助在工控系统中的取证工作、部署/增补信息采集点； 负责协助现场工程师进行排查处置工作；	掌握工控系统结构、工控协议、工控软件和仪表操作等
	客户安全管理员	负责协助取证工作、部署/增补信息采集点； 负责协助现场工程师进行排查处置工作；	网络安全设备使用、安全知识等
	厂商维护工程师	负责协助现场工程师进行排查处置工作；	对自身出品的各种软硬件系统进行安装、调试、维护的能力。

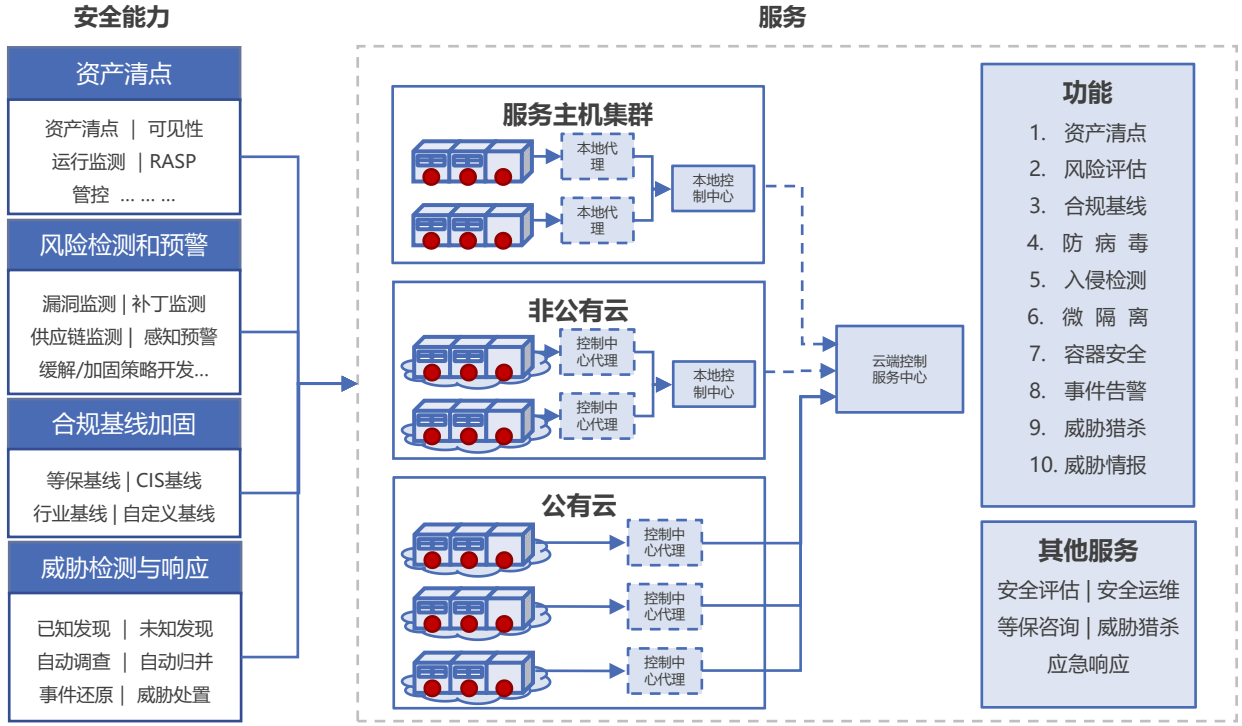
安全运营中心

安全运营中心以IT资产为基础，结合统一的主机探针，为安全工程师提供运营抓手，以业务信息系统为核心，从安全评估、安全监控、综合分析审计、安全运维等维度建立统一的业务支撑能力，通过面向业务的主动化、智能化安全管理，实现资产管理、配置管理、入侵检测、威胁猎杀等关键安全运营能力。



面向多云混合云的 统一云工作负载防护

- 支持物理机、虚拟机、容器等多种工作负载在多云、混合云场景下统一安全防护的需要
- 涵盖资产资产清点、风险评估、合规基线、入侵检测、容器安全、微隔离、容器安全等安全能力
- 支撑威胁猎杀，发现网络攻击线索
- 此外，提供安全评估、安全运维、等保咨询、应急响应等安全服务



系列化云安全产品能力框架图

感谢大家的关注

安天冬训营 wtc.antiy.cn