Enterprise Information Security Summit

2017企业信息安全峰会

暨安全+沙龙年会 上海站

2017年11月24日 | 上海

Nov.24,2017 | Shanghai

BC Consulting 彰熠咨询

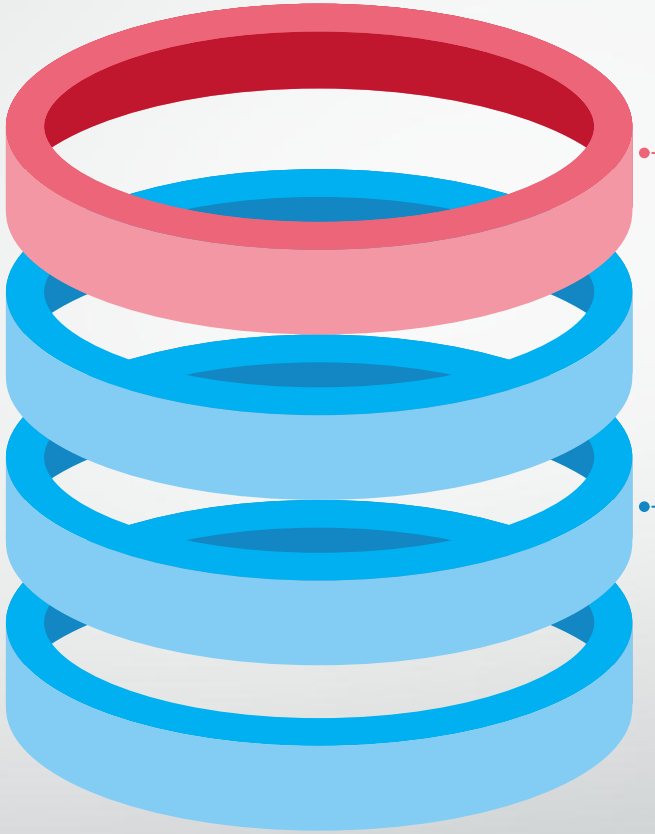
互联网运维安全建设与运营经验分享

- 携程高级信息安全工程师 江榕

1.目标及范围

运维安全=安全运维？

运维安全覆盖范围



人

安全规范
安全标准
安全意识

基础应用与服务

安全规范
安全标准
访问的认证授权
配置
漏洞

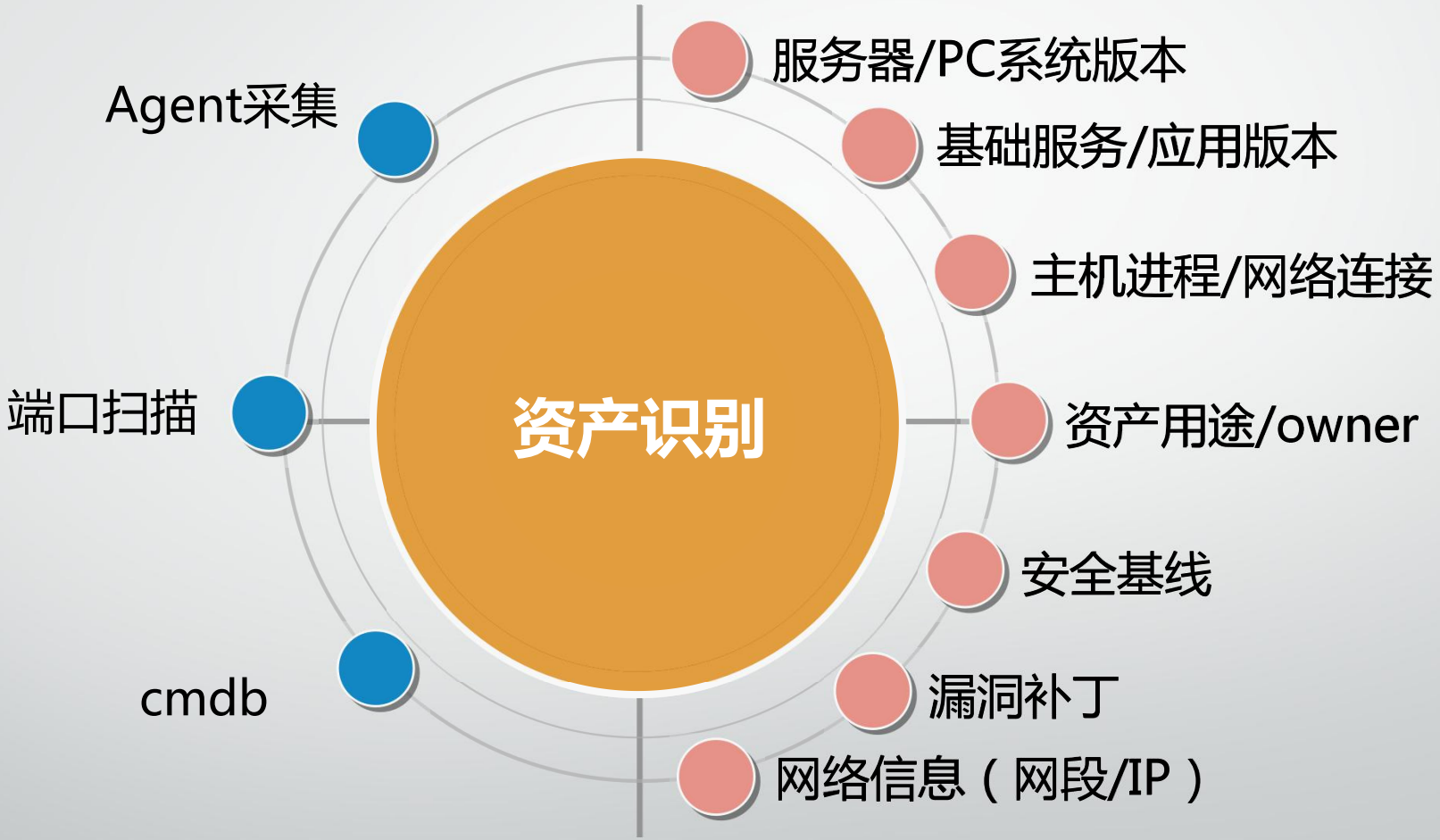
服务器/PC

安全规范
安全标准
访问的认证授权
系统漏洞
配置
补丁
弱口令
恶意程序
反弹shell

网络

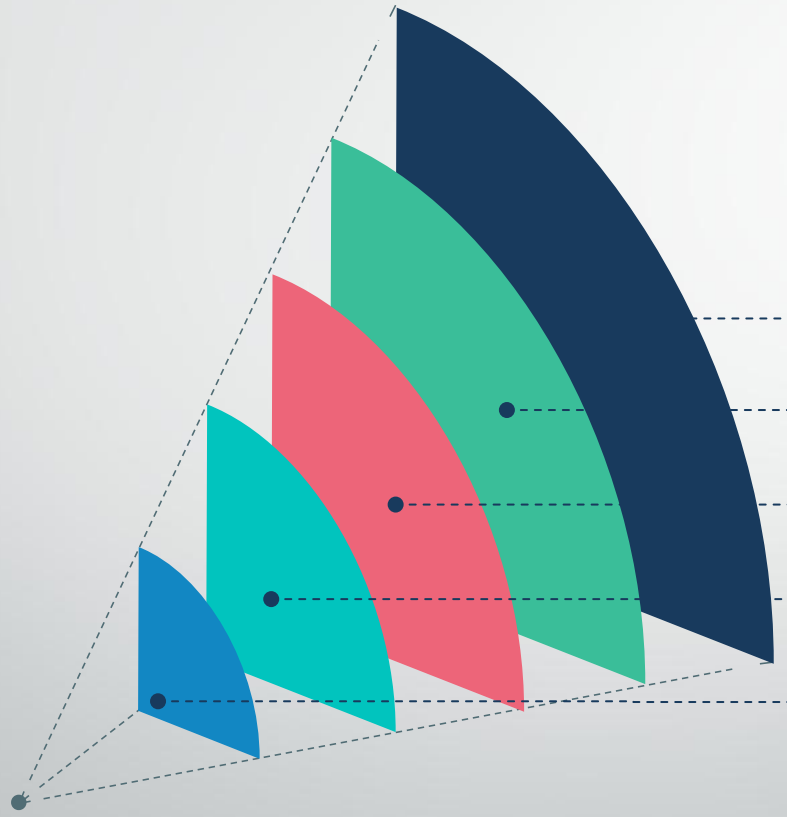
安全规范
安全标准
设备漏洞
配置
权限
弱口令
边界防火墙策略
网络域间互访标准

资产信息收集


资产识别
服务器/PC系统版本
基础服务/应用版本
主机进程/网络连接
资产用途/owner
安全基线
漏洞补丁
网络信息（网段/IP）
cmdb
端口扫描
Agent采集

2.体系与产品

纵深防御



外网边界

NIDS边界流量检测、心跳请求检测、外网蜜罐、外网端口扫描、防火墙策略评审

网络域边界

网络域分级、NIDS边界流量监测、时光机、边界防火墙日志、防火墙策略评审

内网横向流量

内网蜜罐（sensor）

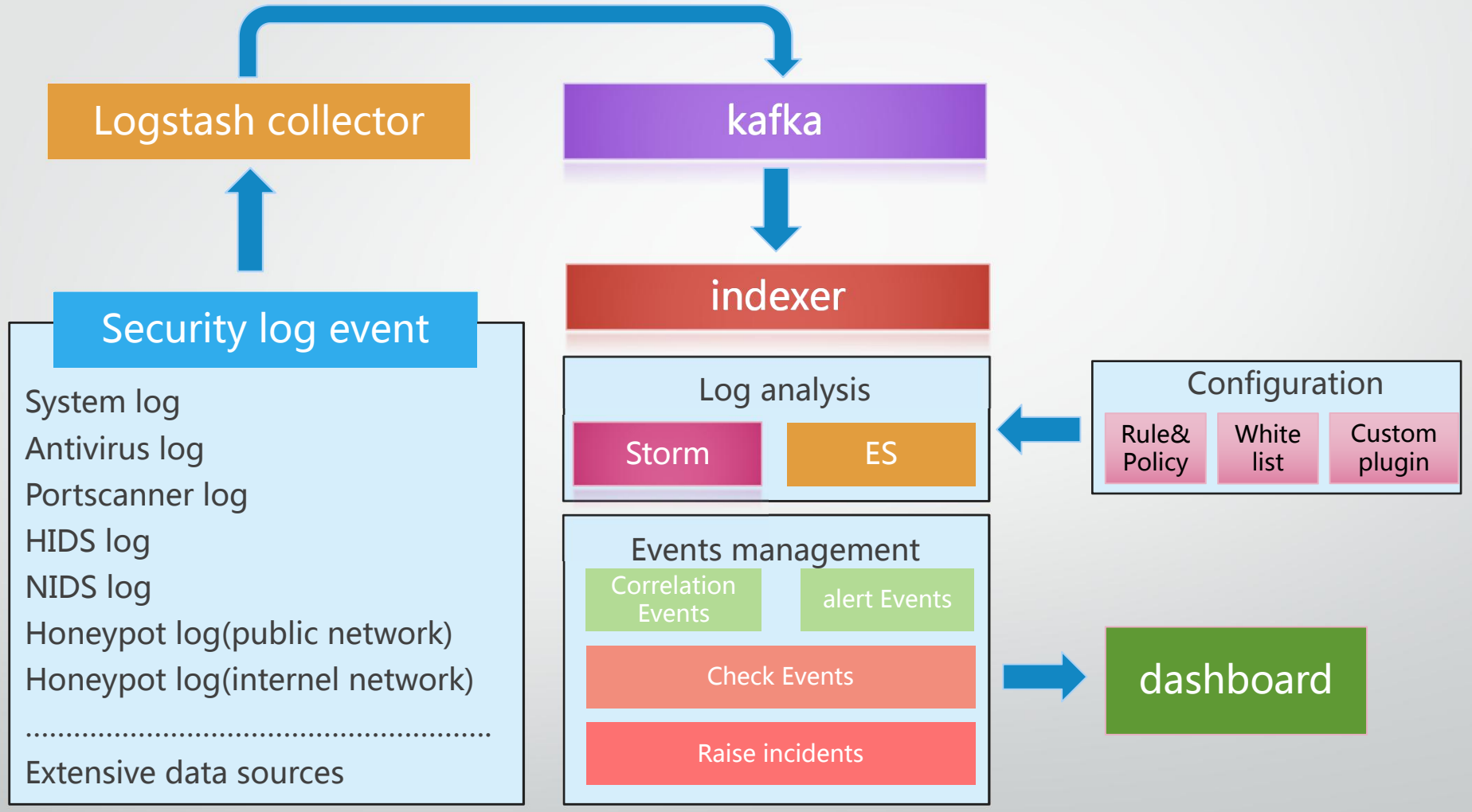
终端/应用日志审计

登录、访问、操作、堡垒机

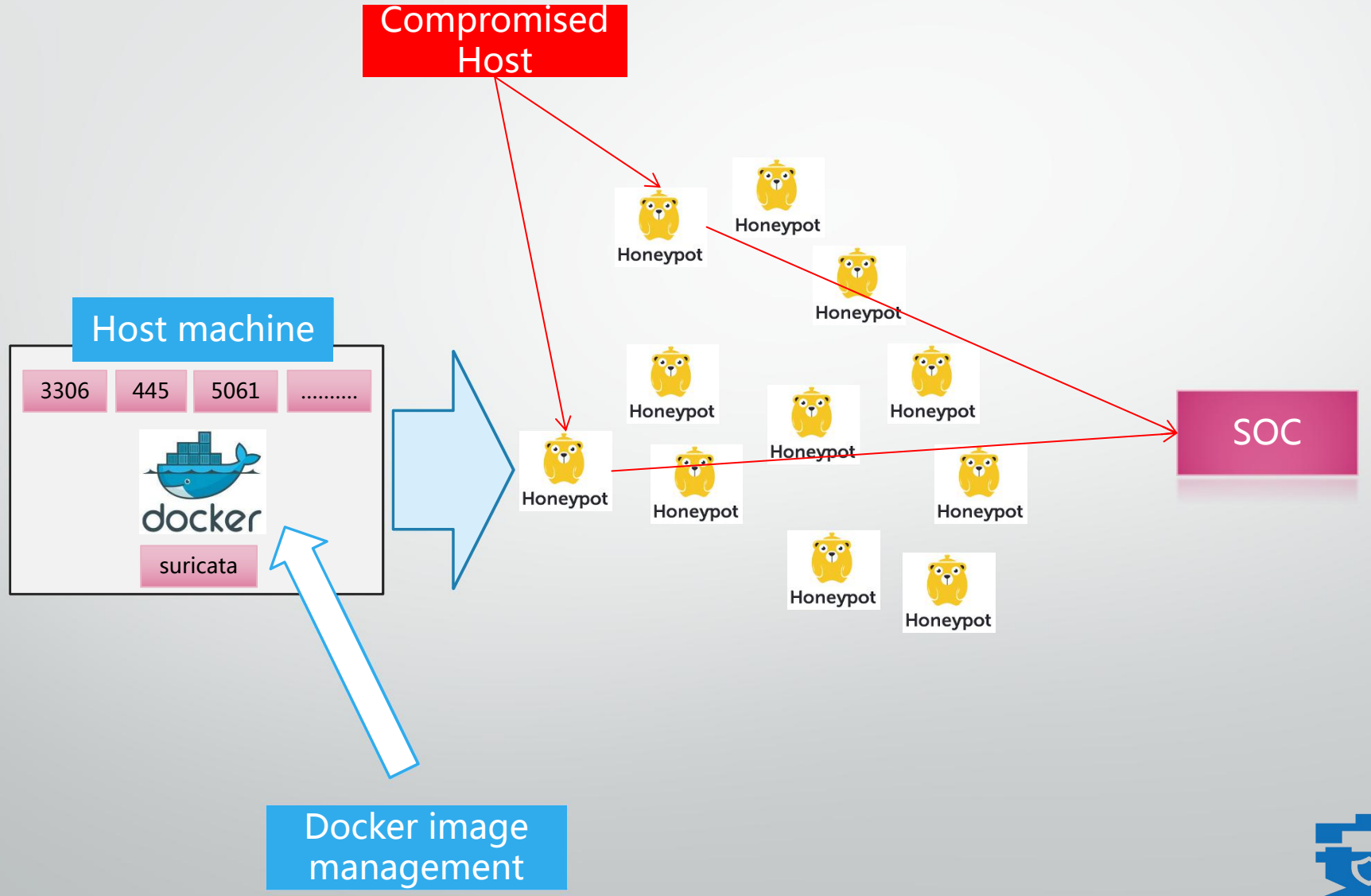
终端行为分析监控

HIDS（主机进程行为、网络连接行为、关键文件监控、安全基线、webshell检测）、防病毒

SOC


Logstash collector
kafka
indexer
Security log event
System log
Antivirus log
Portscanner log
HIDS log
NIDS log
Honeypot log(public network)
Honeypot log(internel network)
.....
Extensive data sources
Log analysis
Storm
ES
Configuration
Rule& Policy
White list
Custom plugin
Events management
Correlation Events
alert Events
Check Events
Raise incidents
dashboard

内网蜜罐系统

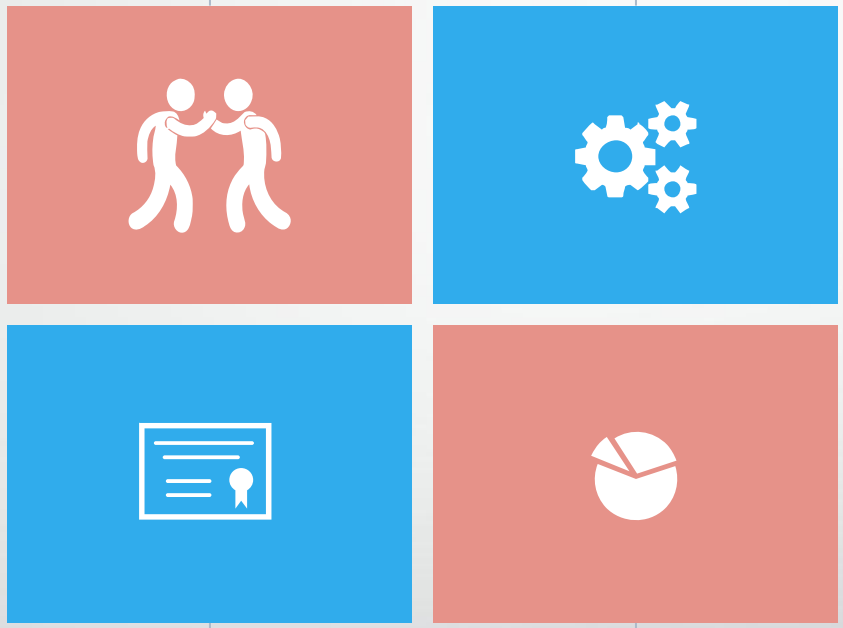

Compromised Host
Honeypot
Honeypot
Honeypot
Host machine
3306
445
5061
.....
docker
suricata
Honeypot
Honeypot
Honeypot
Honeypot
Honeypot
Honeypot
Honeypot
Honeypot
SOC
Docker image management

3.运营经验

检测效果有效性

红蓝对抗

形式包含且不局限于人工、扫描器。开展时间可为定期、随机时间、case by case



安全产品运行状态

应用层及系统层各指标监控

安全策略有效性

误报、漏报（红蓝对抗的输出）、搭建沙盒环境

安全agent状态

覆盖面、存活率、系统影响、策略下发生效

灰色地带

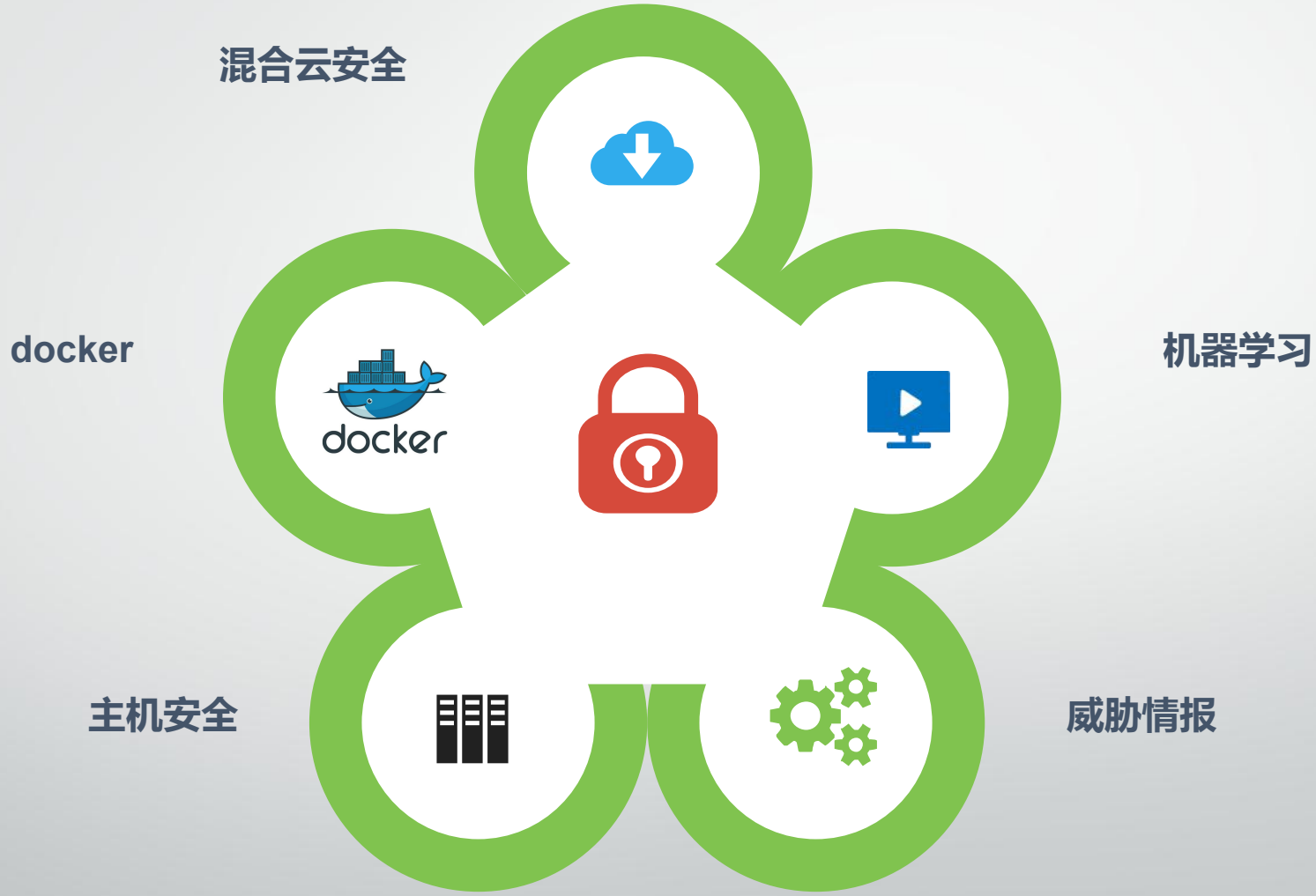
1. agent部署覆盖率
2. 无人关注的资产
3. 非标服务器及应用
4. 第三方厂商设备
5. 开放在互联网上的管理后台、高危端口、文件上传点
6. 已被爆漏洞的第三方应用
7. 自带入域设备

事件应急响应


生成event
确认影响面/确认严重性
受影响资产/严重级别、利用难度/已造成的危害、损失
定级
升级为incident
根据定级结果，评估事件响应范围（所需资源）
响应和处理
隔离/补救/发现新增受影响面重新评估定级
事后分析
原因/处理事件过程中的困难和阻碍/事件处理过程提升点/事前检测防御提升点/报告需提供至相关责任部门
措施执行
可立项对上一步总结项进行逐一整改，持续改进
报备归档

4.Any more ?

我们将来要做的



Thanks