极元第二代蜜罐系统

传统技术的不足

可被绕过或攻破

防火墙

防毒软件

加密技术

补丁管理

生物识别技术

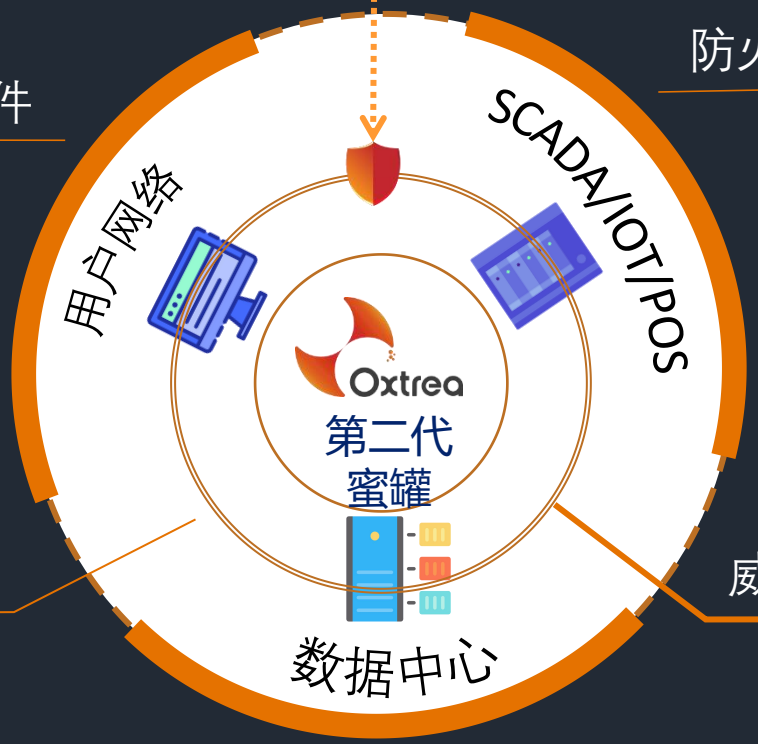
Web应用防护系统

威胁检测和防御

网络准入控制

网关过滤

访问控制



欺骗策略的形成

高仿真

虚假服务器和
交换机

虚假环境和
端口

虚假专用设备

虚假链接

虚假凭证

虚假数据库

虚假服务

SSM | SMB | STP

RDP

虚假账密

虚假数据

欺骗性文件

欺骗性社交
媒体信息

攻击链的欺骗防御

初始侦查

虚假设备

攻破网络

建立立足点

提权

保持控制

横向移动

内部侦查

虚假服务

内网渗透

虚假文件

设置诱饵

>>

捕捉隔离

>>

解决威胁

极元第二代蜜罐系统

Oxtrea Next Generation Honeypot System

极元第二代蜜罐系统是一款基于攻击混淆与欺骗技术的威胁情报产品。通过在黑客必经之路上构造陷阱，混淆其攻击目标，精确感知黑客攻击的行为，并溯源黑客身份及攻击意图，形成黑客攻击情报，发现利用病毒、木马以及0day漏洞的APT攻击行为，保护客户网络免遭0day等攻击造成的各种风险（如敏感信息泄露、关键基础设施破坏等）。该产品可用于保护易受黑客入侵攻击的业务系统，特别在政府、运营商、企业集团、医疗、公检法司、金融、交通、电力等包含大量用户数据、资金等敏感信息的业务环境中。通过构建用户威胁情报体系，实现从安全事件的被动响应到安全威胁的积极应对，帮助企业有效应对安全风险。。

功能架构

- SSH/TELNET蜜罐
- Webmail/phpmyadmin/Vcenter蜜罐
- Redis蜜罐
- MySQL蜜罐

- 单机海量部署，单机支持超过1万个节点
- 支持多个VLAN部署
- 自动跳过已经使用IP，蜜罐自动填补未使用IP
- 蜜罐按照时间和源IP自动变换

- 低交互端口蜜罐
- 端口自定义
- 外部扫描无漏洞
- 低资源消耗

- 攻击路径展示
- 攻击动画播放
- 攻击路径摘要
- 攻击报表导出

低交互蜜罐

- 根据需求虚拟出大量的IP地址，同时开启一系列常用端口，伪装成真实在线主机。
- 与真实主机混杂高密度海量部署，大大提高命中率。
- 陷阱主机可以自动占用网络中的空闲IP地址，并完成部署。
- 陷阱主机由系统本身生成，不需要消耗额外的计算资源。
- 四层蜜罐，无实际系统，因此本身无被攻破的风险。

ID	IP	子网掩码	网关	虚拟交换	数量	状态	操作
2	10.10.0.50-10.10.0....	255.255.255.0	10.10.0.254	vs10	5	开启	编辑 删除
3	172.16.20.50-172.1...	255.255.255.0	172.16.20.254	vs20	5	开启	编辑 删除
4	172.16.0.50-172.16....	255.255.255.0	172.16.0.254	vs100	5	开启	编辑 删除
5	192.168.3.50-192.1...	255.255.255.0	192.168.3.99	vs99	5	开启	编辑 删除

ID	主机IP	主机类型
5	10.10.0.51	虚拟主机
3	10.10.0.52	虚拟主机
4	10.10.0.53	虚拟主机
1	10.10.0.54	虚拟主机
2	10.10.0.57	虚拟主机
11	172.16.0.51	虚拟主机
12	172.16.0.53	虚拟主机
14	172.16.0.60	虚拟主机
15	172.16.0.64	虚拟主机
13	172.16.0.86	虚拟主机
6	172.16.20.51	虚拟主机
10	172.16.20.52	虚拟主机
7	172.16.20.53	虚拟主机
8	172.16.20.55	虚拟主机
9	172.16.20.56	虚拟主机
16	192.168.3.51	虚拟主机
20	192.168.3.52	虚拟主机
19	192.168.3.53	虚拟主机
17	192.168.3.54	虚拟主机
18	192.168.3.59	虚拟主机

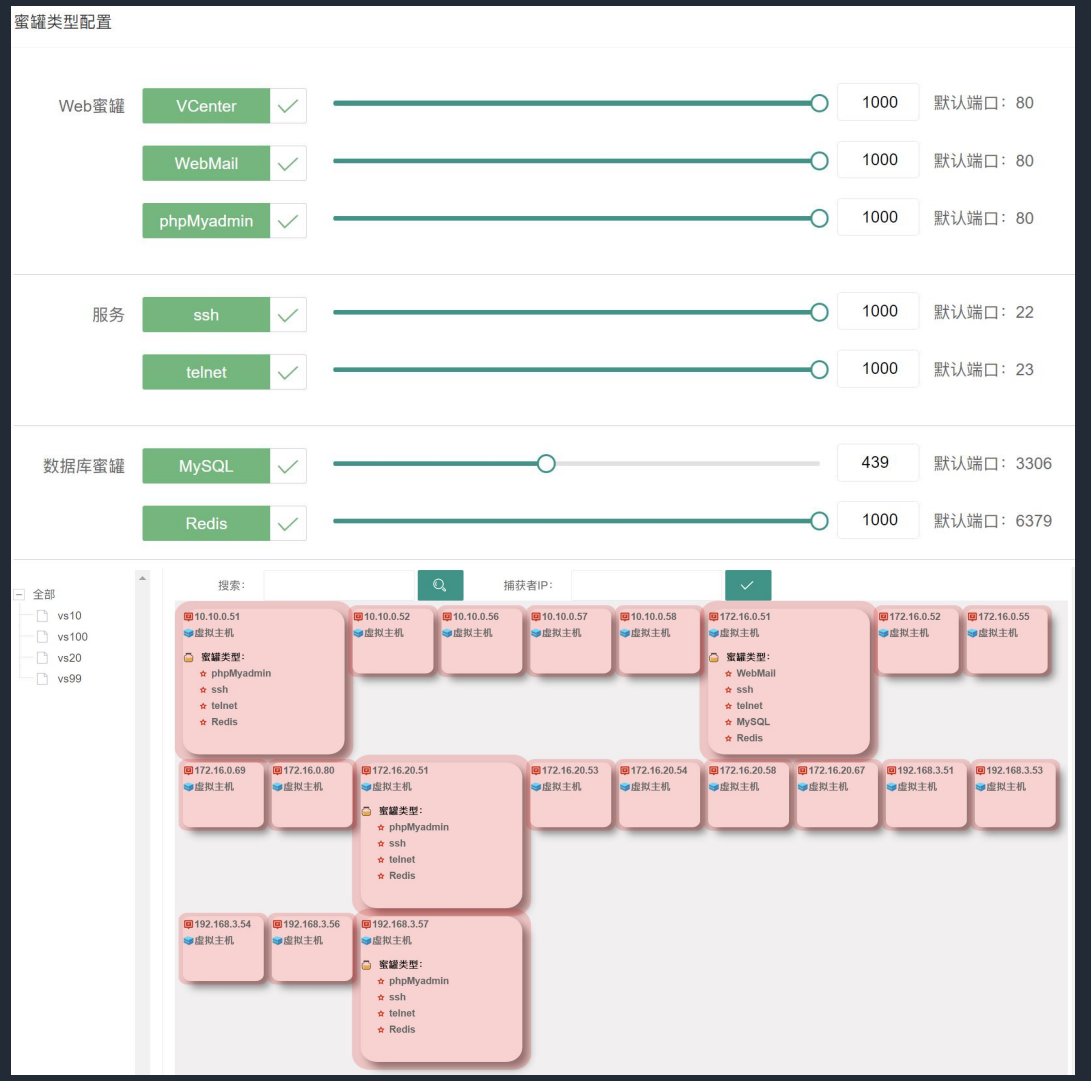
低交互蜜罐-捕获详情

源IP	位置	端口	开始时间	结束时间	攻击次数	操作
192.168.3.112	unknown	139,445	2021-09-10 09:45:56	2021-09-10 09:45:56	4	查看详情
192.168.3.114	unknown	3389	2021-09-10 10:55:11	2021-09-10 10:56:08	6	查看详情
192.168.3.81	unknown	139,1433,1521,445,9090	2021-09-10 10:40:52	2021-09-10 11:21:18	57	查看详情

源IP	目的IP	位置	端口	开始时间	结束时间	攻击次数
192.168.3.81	192.168.3.250	unknown	1521	2021-09-10 10:52:14	2021-09-10 11:21:18	4
192.168.3.81	192.168.3.250	unknown	1433	2021-09-10 10:52:23	2021-09-10 11:21:18	3
192.168.3.81	192.168.3.250	unknown	139	2021-09-10 10:52:28	2021-09-10 11:21:18	3
192.168.3.81	192.168.3.250	unknown	445	2021-09-10 10:52:36	2021-09-10 11:21:18	3
192.168.3.81	192.168.3.51	unknown	1521	2021-09-10 10:45:46	2021-09-10 11:20:02	4
192.168.3.81	192.168.3.51	unknown	1433	2021-09-10 10:45:57	2021-09-10 11:20:02	3
192.168.3.81	192.168.3.51	unknown	139	2021-09-10 10:45:59	2021-09-10 11:20:02	3
192.168.3.81	192.168.3.51	unknown	445	2021-09-10 10:46:00	2021-09-10 11:20:02	3
192.168.3.81	192.168.3.51	unknown	9090	2021-09-10 10:46:23	2021-09-10 11:20:05	4
192.168.3.81	192.168.3.52	unknown	139	2021-09-10 10:40:52	2021-09-10 11:18:35	3

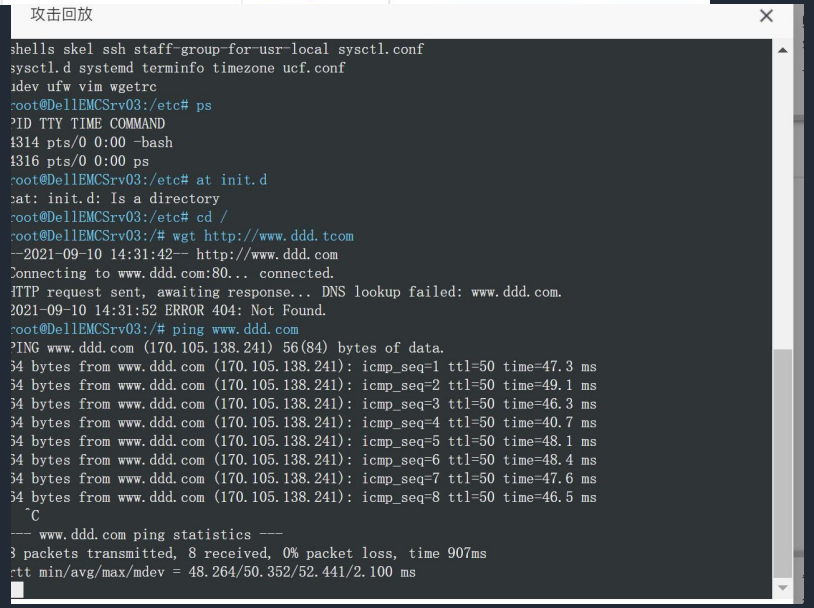
高交互蜜罐

- 生成大量高交互蜜罐，引诱攻击者进行更深入的攻击，进而达到捕获、取证、反制的防护目的。
- 非虚机、Docker形态，非真实的操作系统。
- 类系统模拟器，内置与伪装业务同样的命令库、界面等，并对交互做出相应的回显，以达到可交互性，从而迷惑攻击者。
- 无需耗费额外的计算资源（占用内存不超过200M），无被攻破的风险.



高交互蜜罐-捕获详情

源IP	位置	开始时间	结束时间	捕获陷阱	攻击次数	级别	操作
192.168.3.114	unknown	13:54:09	13:56:12	ssh	5	高	查看详情 下载
192.168.3.250	unknown	13:22:53	13:22:53	phpMyadmin	1	低	查看详情 下载
192.168.3.81	unknown	10:40:52	11:21:18	phpMyadmin …	317	低	查看详情 下载
192.168.3.112	unknown	09:45:46	09:45:46	webMail	1	低	查看详情 下载
192.168.3.120	unknown	09:15:14	13:22:52	phpMyadmin …	27	中	查看详情 下载



应用场景

高级威胁检测

行为入侵检测机制
感知多种攻击行为

黑客追踪溯源

记录观察高联动
形成精准威胁情报

勒索病毒监测

提前预知勒索病毒的爆发

HVV

对攻防进入反制和发现

应用场景-勒索软件检测

勒索软件

邮件安全网关

将勒索软件
注入端点

工作站VLAN

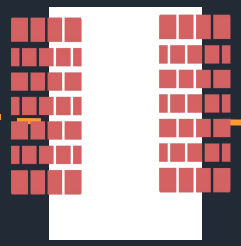
勒索软件开始加密
本地和网络驱动器

端点工作站

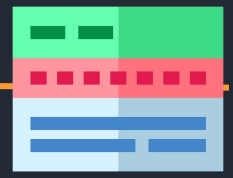
勒索软件开始加密虚
拟网络和仿真文件

仿真文件服务器

检测到活动
发出警报



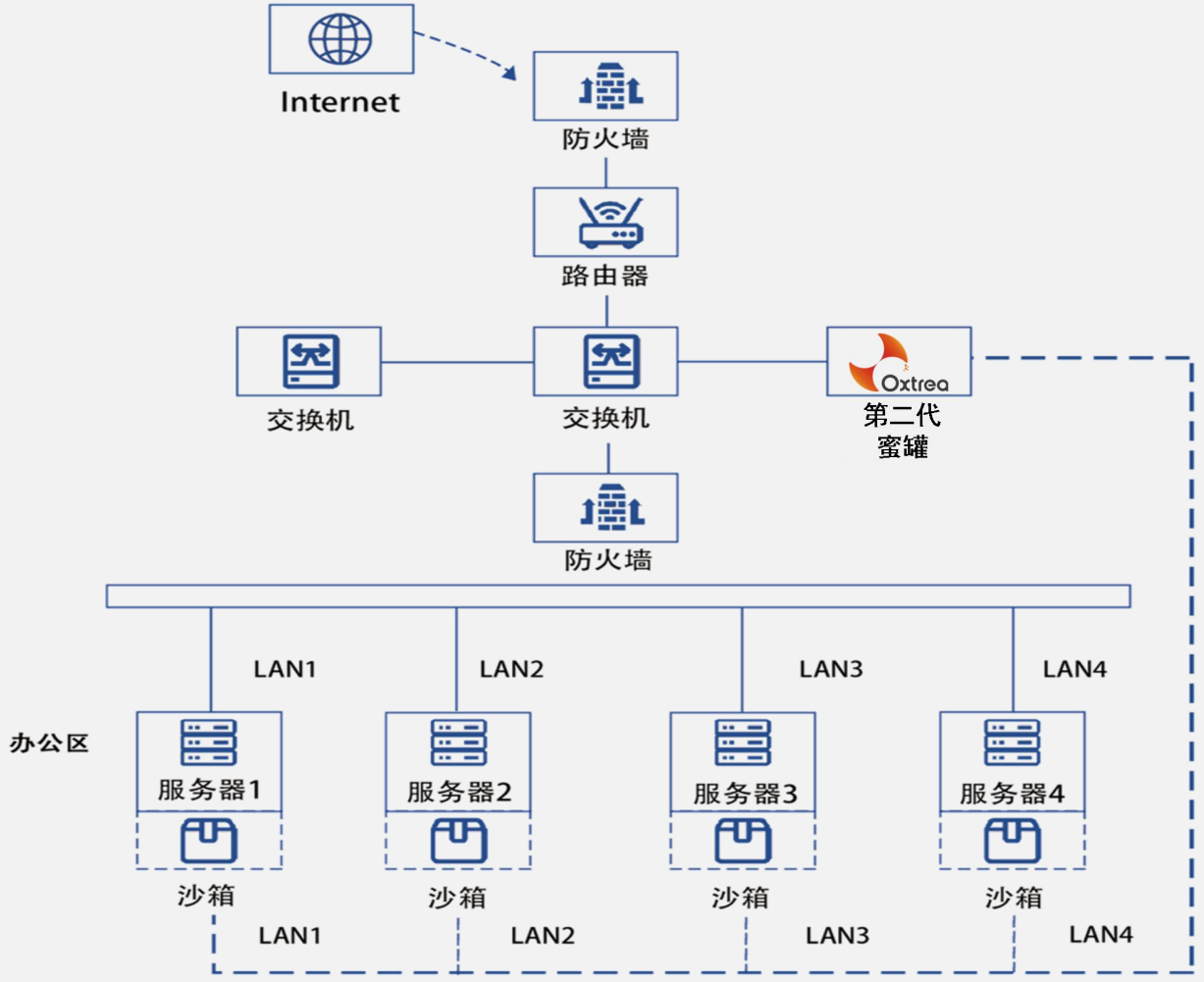
断开端点
网络连接



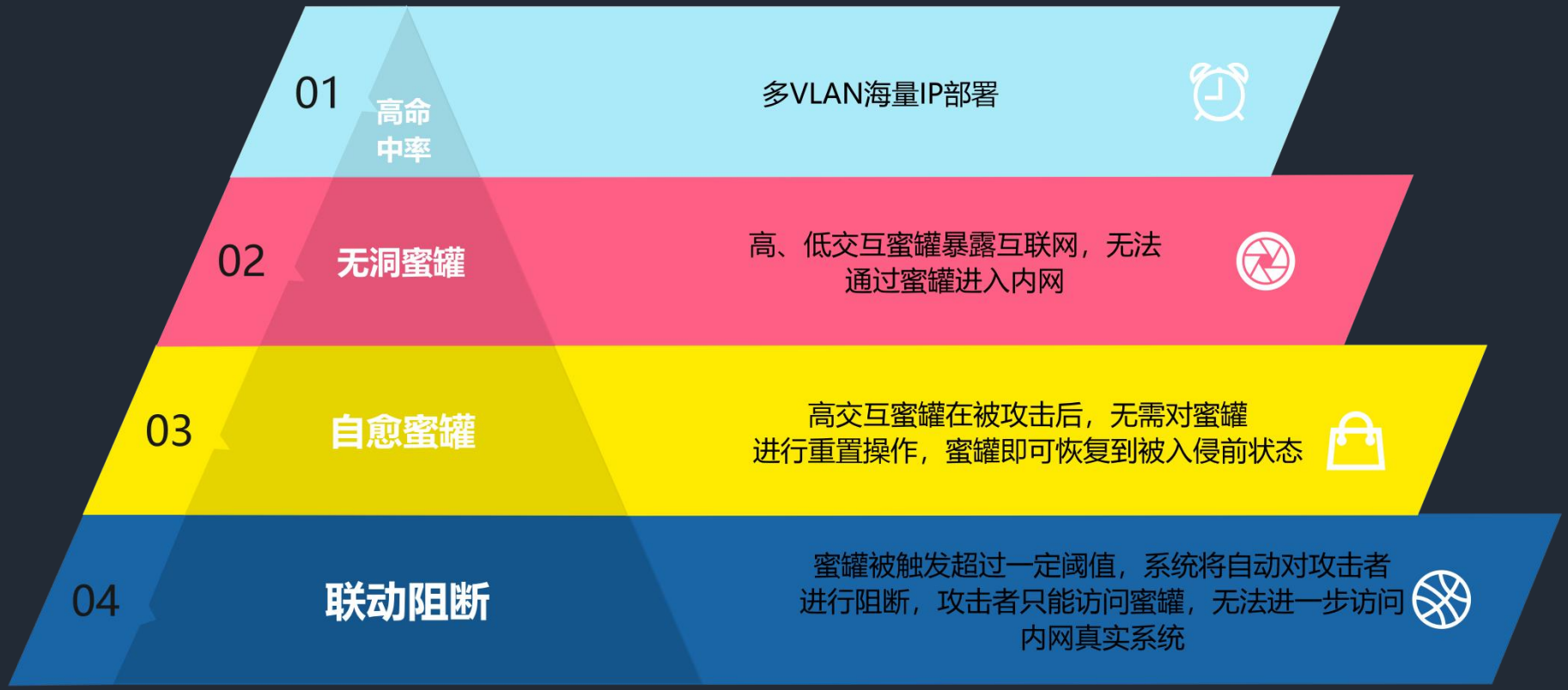
服务器VLAN

互联网

部署方式


Internet
防火墙
路由器
交换机
交换机
Oxtrea
第二代
蜜罐
防火墙
LAN1
LAN2
LAN3
LAN4
办公区
服务器1
服务器2
服务器3
服务器4
沙箱
沙箱
沙箱
沙箱
LAN1
LAN2
LAN3
LAN4

优势


01
高命中率
多VLAN海量IP部署
02
无洞蜜罐
高、低交互蜜罐暴露互联网，无法通过蜜罐进入内网
03
自愈蜜罐
高交互蜜罐在被攻击后，无需对蜜罐进行重置操作，蜜罐即可恢复到被入侵前状态
04
联动阻断
蜜罐被触发超过一定阈值，系统将自动对攻击者进行阻断，攻击者只能访问蜜罐，无法进一步访问内网真实系统

Thank You for Today

谢谢

www.oxtrea.com