

马士兵教育

定制未来，成就更好的你

花名：万里

曾就职于奇安信集团，担任高级渗透测试工程师，从事网络安全工作7年，参与四届全国HW行动、北京冬奥重保等活动，担任CISP-PTE、CISP-IRE出题及监考，为CNCERT、SRC平台等提交数百漏洞。专注研究前沿网络安全技术，具有丰富的实战经验。擅长技术：Web渗透、内网渗透、代码审计、Kali、安全工具开发等。



中华人民共和国网络安全法

第二十七条

任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

课程内容仅用于以防御为目的的教学演示
请勿用于其他用途，否则后果自负

1、《中华人民共和国刑法》的相关规定：

第二百八十五条规定，非法侵入计算机信息系统罪;非法获取计算机信息系统数据、非法控制计算机信息系统罪;提供侵入、非法控制计算机信息系统程序、工具罪是指，违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金;情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。

单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。

第一条

非法获取计算机信息系统数据或者非法控制计算机信息系统，具有下列情形之一的，应当认定为刑法第二百八十五条第二款规定的“情节严重”：

- （一）获取支付结算、证券交易、期货交易等网络金融服务的身份认证信息十组以上的；
- （二）获取第（一）项以外的身份认证信息五百组以上的；
- （三）非法控制计算机信息系统二十台以上的；
- （四）违法所得五千元以上或者造成经济损失一万元以上的；
- （五）其他情节严重的情形。

实施前款规定行为，具有下列情形之一的，应当认定为刑法第二百八十五条第二款规定的“情节特别严重”：

- （一）数量或者数额达到前款第（一）项至第（四）项规定标准五倍以上的；
- （二）其他情节特别严重的情形。

明知是他人非法控制的计算机信息系统，而对该计算机信息系统的控制权加以利用的，依照前两款的规定定罪处罚。

目录

1. 常见的安全公司
2. 态势感知
3. 终端防护
4. 蜜罐设备
5. 沙箱平台
6. 威胁情报
7. EDR 设备

课程安排

常见的安全公司

网络安全企业

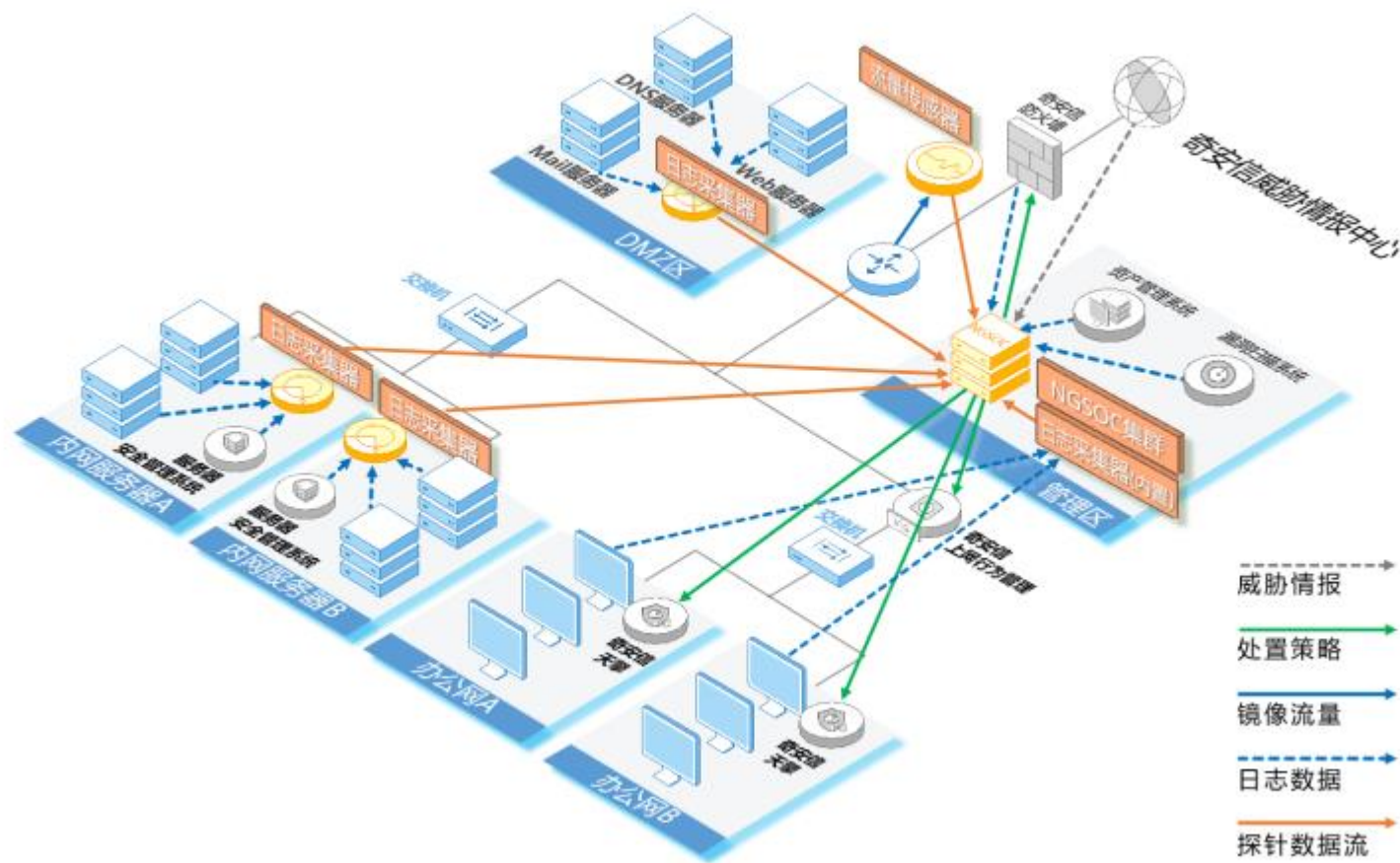


课程安排

态势感知

态势感知

实施部署:



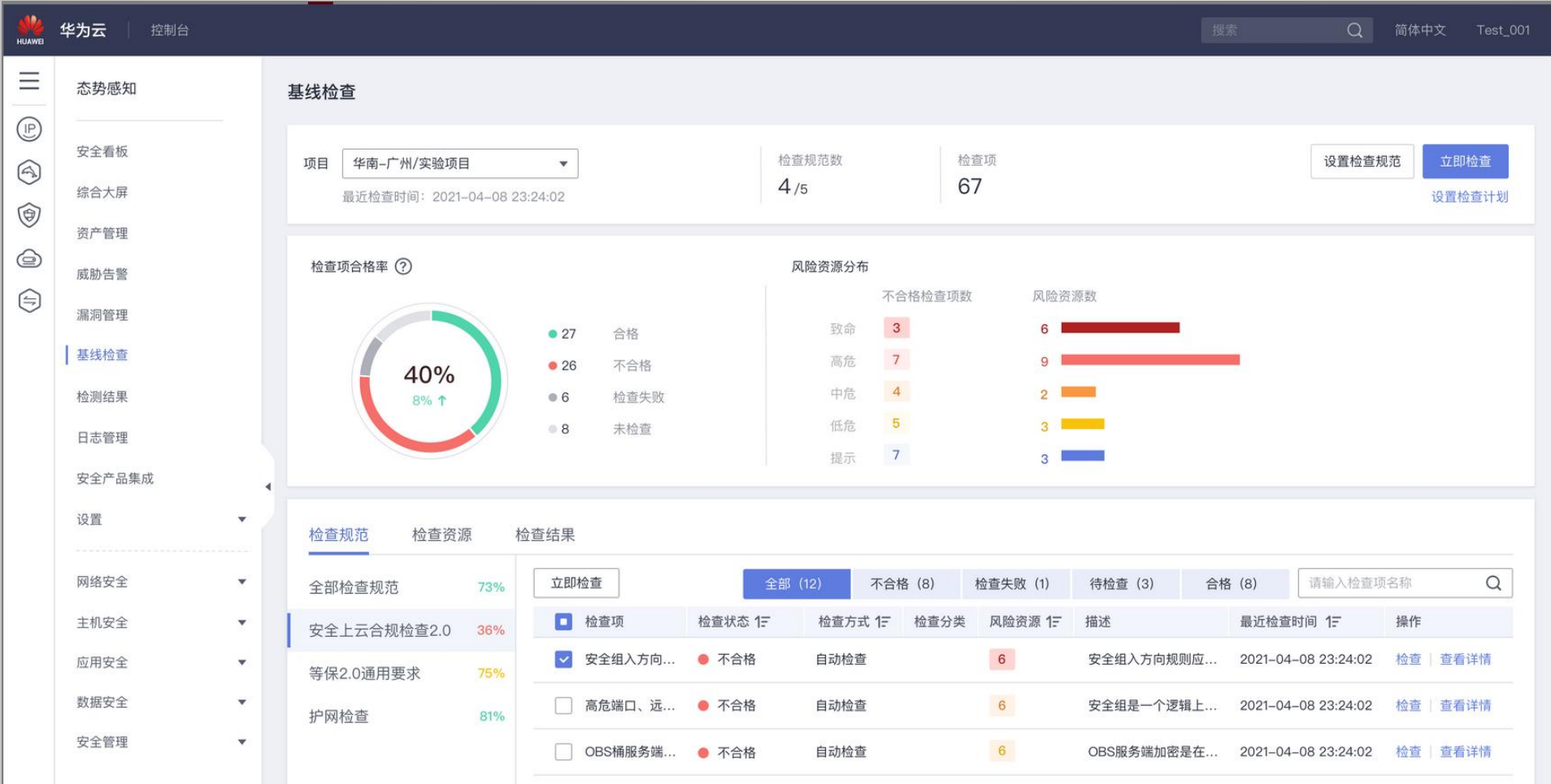
态势感知



态势感知



态势感知



课程安排

终端防护

◀ 最新动态：主机的零信任安全实践



云计算时代主机安全面临的挑战

云上的安全边界越来越模糊，依靠传统的硬件堆叠的安全防御方式已经很难解决云上的安全问题。CC、SQL注入、XSS跨站等黑客攻击以及后门、webshell等恶意代码时刻威胁企业的信息安全

云锁是中国用户总量领先的主机安全产品，在国际上率先达到Gartner定义的wapp（云工作负载保护平台）标准，兼容多种虚拟化架构和操作系统，可以高效支撑现代混合数据中心架构下的主机安全需求。

云锁基于服务器端轻量级agent，安全加固服务器操作系统及应用；云锁waf探针、rasp探针、内核加固探针能有效检测与抵御已知、未知恶意代码和黑客攻击；同时云锁融合资产管理、微隔离、攻击溯源、自动化运维、基线检查等强大功能，帮助用户高效安全运维服务器。

应对未知安全威胁

RASP

沙盒

ASVE

传统基于签名的防护手段应对未知威胁往往效果堪忧，而且会让防护架构变的愈发臃肿，云锁采用RASP、ASVE、沙盒三大基于异常行为的检测技术，可有效检测并防御未知威胁。云锁通过RASP技术对应用系统的流量、上下文、行为进行持续监控，识别及防御已知及未知威胁，能有效防御SQL注入、命令执行、文件上传、任意文件读写、反序列化、Struts2等基于传统签名方式无法有效防护的应用漏洞；云锁独创虚拟化安全域技术（ASVE），通过将应用进程放入虚拟化安全域内，限制应用进程权限，防止黑客利用应用程序漏洞提权、创建可执行文件等非法操作；云锁基于脚本虚拟机（沙盒）的无签名webshell检测技术，有效检测自种加密、变形的Webshell。

*

蜜罐设备



Linux下载

Windows下载

Docker下载

使用手册

课程安排

沙箱平台


沙箱平台



课程安排

威胁情报

威胁情报

 威胁情报中心


首页

APT全景雷达

安全研究

登录

注册

 威胁情报中心

请输入IP、域名、文件HASH(MD5,SHA1,SHA256)、证书(SKID,MD5,SHA1)

搜索

证书查询示例：①通过SKID查询证书，输入"AD 092A4E EF3B E3 963A312E A3541625764C17AB56"
②通过md5或sha1查询证书，输入"CA.md5/sha1"，如"CA:e5a51c57ecfe1a50a097e458b5d9e37fb273d945"

热门推荐

1

api.jm.taolop.com

2

165.227.65.125

3

3fae1d5f25020829edbb5e95cc7f7836

4

209.141.40.190

5

78.187.240.125

6

14.99.1.2

7

3fb5e2c05b73168c3f259d64b8978a64

8

deftsecurity.com

9

freescanonline.com

10

authentication-services.zzux.com

*

课程安排

EDR 设备

EDR 设备



[安全产品与方案](#)[行业解决方案](#)[安全服务与运营](#)[安全研究](#)[合作伙伴](#)[技术支持](#)

Q

English

绿盟终端检测与响应系统 EDR

立即咨询

视频播放

首页 > 安全产品与方案 > 基础设施安全 > 终端安全

客户价值

功能特性

产品优势

成功案例

相关资源