CSA GCR 6th Congress 第六届云安全联盟大中华区大会

CSA GCR cloud security alliance GREATER CHINA REGION

基于云原生的攻击面管理

Attack surface management based on cloud native

演讲人：**万飞**

北京华云安信息技术有限公司

CSA GCR 6th Congress 第六届云安全联盟大中华区大会

目录

Contents

一. 云原生安全发展趋势

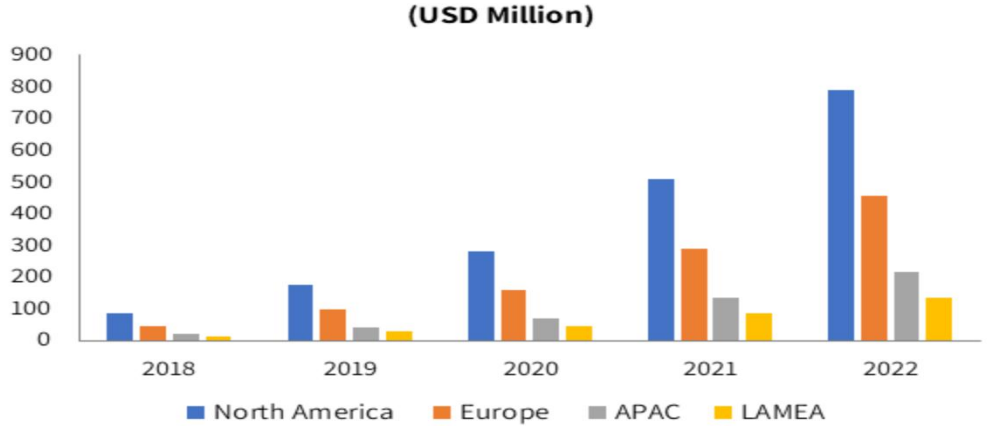
二. 云原生安全攻击面管理

三. 云原生安全落地实践分享

VUL·AI 华云安

1.1 基于云原生应用安全投入

简单看一组国外的统计数据
从2018到2022年增长趋势很明显。



2.1 云原生安全资产发现

自动发现并可视化云原生环境下运行的主机、K8s集群、pod、容器、Namespace、微服务等多种资产，基于优先级实时感知风险态势。

影响攻击面因素

未知资产

攻击面数量，随着部署SaaS应用程序资产的范围扩大而不断扩展。未知资产的危险在于网络安全风险和威胁的不可预见。

层出不穷的安全弱点

通常情况下，部署的资产越多，暴露的弱点越多，尤其未经安全团队授权安装在企业资产上的某些组建或不安全设置。

云计算技术应用

云计算迅速兴起，越来越多的资产面临外部威胁，从而进一步增加网络攻击面。

攻击面资产构成

2.2 云原生安全攻击面检测

2.2.1 云原生开发中的攻击面检测

2.2.2 云原生线上应用攻击面检测

2.2.3 云原生基础设施攻击面检测

2.2.1云原生开发中的攻击面检测

安全左移，从源头解决问题

01-03

01 CI/CD 流程深度集成,在开发过程中通过攻击面检测技术检测弱点、敏感数据及其他安全问题

02 基于镜像的弱点扫描，通过在线提供镜像扫描和多种配置扫描发现风险点

03 基于容器动态安全分析，通过安全容器沙箱技术检测高级威胁、未知恶意软件威胁等风险点

2.2.2云原生线上应用攻击面检测

容器安全

01-05

01 通过弱点扫描，检测线上应用是否存在可利用的弱点

02 通过自动化渗透，检测线上应用是否存在可利用的弱点

03 获取容器和Kubernetes运行时环境的详细审计和取证数据，以跟踪违规事件，进行合规评估

04 在沙盒环境中运行、分析容器镜像，检查和跟踪行为异常，以发现静态扫描程序无法检测到的高级恶意威胁

05 通过机器学习分析行为、识别云原生环境中符合ATT&CK框架下所有攻击行为，保证容器运行时免受各类型已知攻击威胁

2.2.2云原生线上应用攻击面检测

虚拟化安全

01-06

01 多云环境中进行VM配置核查与合规检测

02 通过弱点扫描，检测VM是否存在可利用的弱点

03 通过自动化渗透，检测VM是否存在可利用的弱点

04 通过VM实时监控，实现资产快速更新

05 通过VM入侵检测，动态监控注册表、文件系统等

06 提供取证分析，监视VM可疑活动

2.2.2云原生线上应用攻击面检测

云函数安全（Serverless安全）

01-05

01 通过弱点扫描，检测云函数是否存在可利用的弱点

02 通过自动化渗透，检测云函数是否存在可利用的弱点

03 标记过度授权，监视未使用的权限和角色来防止权限滥用

04 提供运行时保护，检测异常行为

05 通过策略授权提供可控部署，避免云函数滥用

2.2.3云原生基础设施攻击面检测

云环境安全

云环境安全是云安全的重要基础，也是攻击面检测的必要对象。通过保证云环境的安全，能够有效地降低通过利用云环境造成的攻击。

01 通过云基线进行配置核查与合规检测

02 通过弱点扫描，检测云环境是否存在可利用的弱点

03 通过自动化渗透，检测云环境是否存在可利用的弱点

04 通过云控制面行为检测，分析敏感数据变更或潜在恶意活动

05 提供自动化修复机制，根据策略进行必要的干预操作

2.2.3云原生基础设施攻击面检测

集群安全

集群是一切云计算的基础，因此也是云原生的基础设施中最核心的内容，只能通过多种技术手段实现对基础设施的攻击面检测，才能为上层应用提供可靠的安全保证。

01 提供集群配置核查与合规检测

02 通过弱点扫描，检测集群是否存在可利用的弱点

03 通过自动化渗透，检测集群是否存在可利用的弱点

04 通过可控节点部署，避免非法节点上线

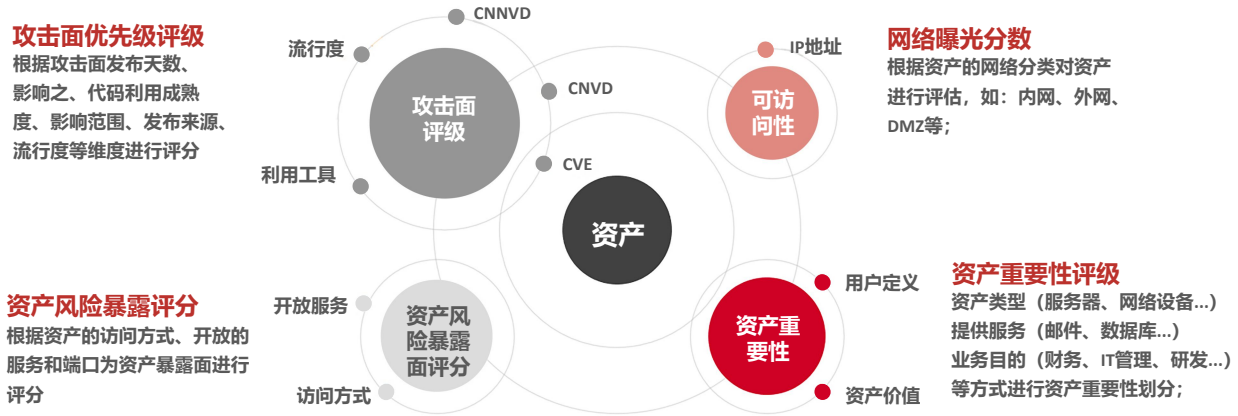
05 通过策略准入进行应用部署，避免非法应用上线

06 通过身份隔离技术，在集群内和集群之间强制执行容器级网络隔离规则

2.3 攻击面分析

攻击面优先级评估

集群是一切云计算的基础，因此也是云原生的基础设施中最核心的内容，只能通过多种技术手段实现对基础设施的攻击面检测，才能为上层应用提供可靠的安全保证。



VUL·AI 华云安

2.3 攻击面分析

攻击面情报分析
通过分析包括IoC情报、供应链情报和外部情况等类型的攻击面情报能够有效地发现各类未知风险，从而在攻击发生前掌握重要的攻击信息。

结合IoC情报分析

了解针对云原生环境的可能威胁

结合供应链情报分析

了解云原生组件供应链中的风险以及它们如何影响云原生应用

结合外部情报分析

了解黑产，仿冒APP、仿冒网站，企业信息泄露对外部信息对组织得影响

2.4 云原生攻击面响应

通过华云安产品家族，助力云原生环境安全左移，达到攻击面快速收敛和事件快速响应能力，在DevOps 基础上能够及早发现问题并快速修复它们。

提供事件跨部门协同流转

完整和开放式的流转体系，将技术和流程打通，将复杂的攻击面事件管理工作流程化和制度化，协同用户跨部门进行合作，从而完成攻击面快速处置工作。

提供SOAR人机协同：

通过SOAR完成自动化弱点验证&修复功能，通过SOAR可实现对各类工具的调度，做到攻击面快速收敛和事件快速响应

云原生原子化安全能力调度平台

核心理念

云原生统一架构实现了一个平台交付所有安全原子化能力的技术管理体系。

统一安全平台

积木式搭建产品，微服务化安全能力平台易于扩展。

云原生交付

轻松支持本地化部署、云化部署和SaaS化交付。

安全风险库

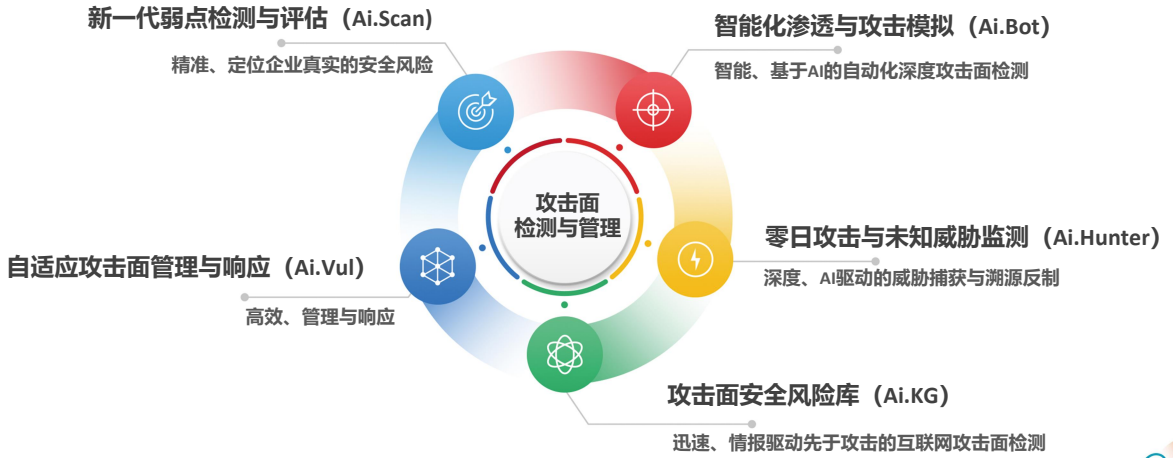
基于知识图谱的风险库，增强共享能力、提升安全防御体系的有效性。

人工智能引擎

场景化AI对抗引擎，源自国家重点研发计划，技术领先市场3-5年。

基于云原生的攻击面管理

通过云原生原子化安全能力调度平台，为云原生攻击面管理的各个环节，提供完整的解决方案。



CSA GCR 6th Congress 第六届云安全联盟大中华区大会

CSA GCR cloud security alliance GREATER CHINA REGION

THANK YOU