OWASP 中国 Open Worldwide Application Security Project

OWASP 中国 | 北京分会 Open Worldwide Application Security Project

网安加社区

探真科技 TensorSecurity

开源网安 SECZONE GROUP

BrainAu 脑动极光 BRAINAU

多云安全下一跳
云安全态势管理与LLMs

何诣莘

2024 OWASP中国安全技术论坛
全球视野下的网络安全趋势

目录
CONTENTS

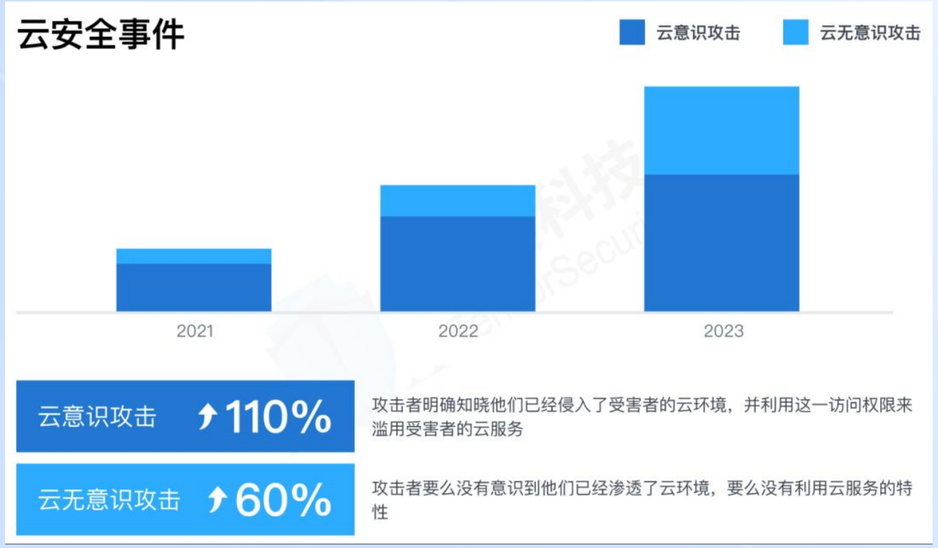
01

云上风险点的转变

云上风险点的转变

云上攻击事件逐年持续增长

《2023年全球网络安全威胁报告》中指出，2023年，云相关的网络攻击**增加了48%**，平均每个企业**每周遭受1,157次云端攻击**，79%的企业经历过至少一次严重的云安全事件



传统攻击手段

SQL注入	XSS	暴力破解
逃逸	命令执行	反序列化
解析漏洞	提权	文件包含
路径遍历	文件上传	后门病毒

针对云攻击手段

Secret泄漏	存储桶公开	子账号权限控制不严
元数据泄露	敏感端口公开	存储桶ACL提权
userdata写入	IAM账号提权	云账号弱口令

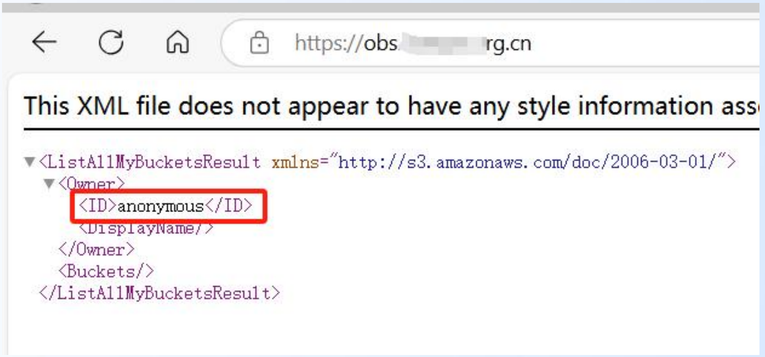
云上实际数据泄露案例

探真安全研究团队

敏感信息收集

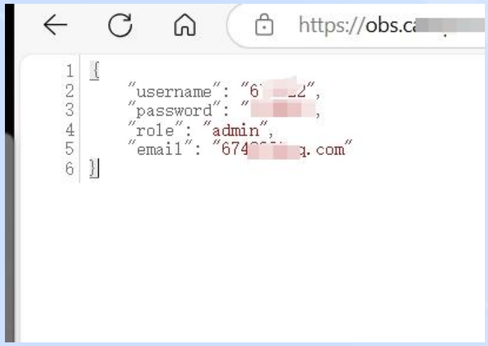
发现某客户使用华为云obs存储桶

发现存储桶未鉴权



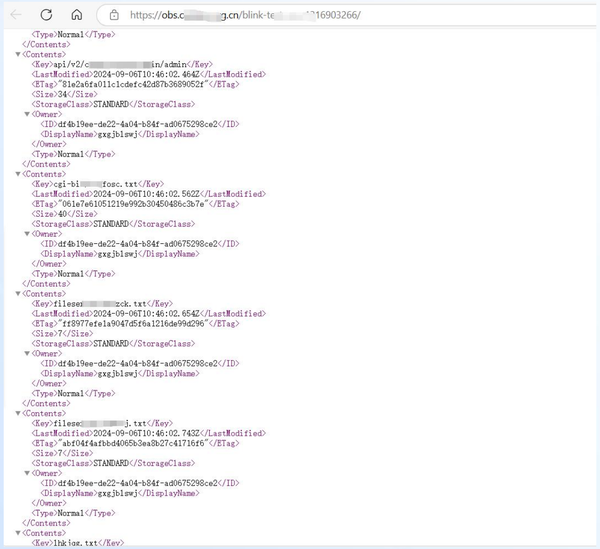
公开可访问的存储桶

通过空间搜索引擎发现多个公开的桶



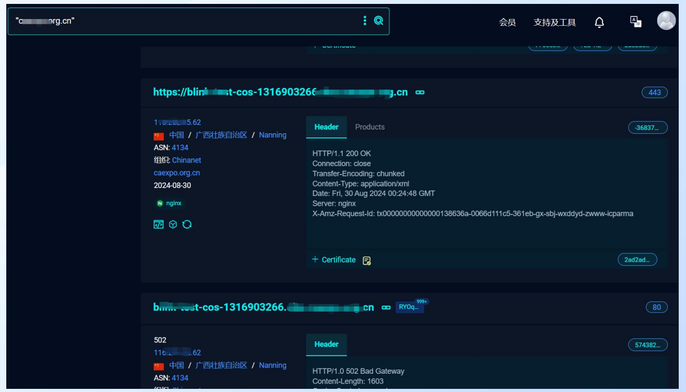
账密/邮箱信息泄露

打开user.txt



3w+可被直接下载的文件

通过桶名拼接访问对应桶内容



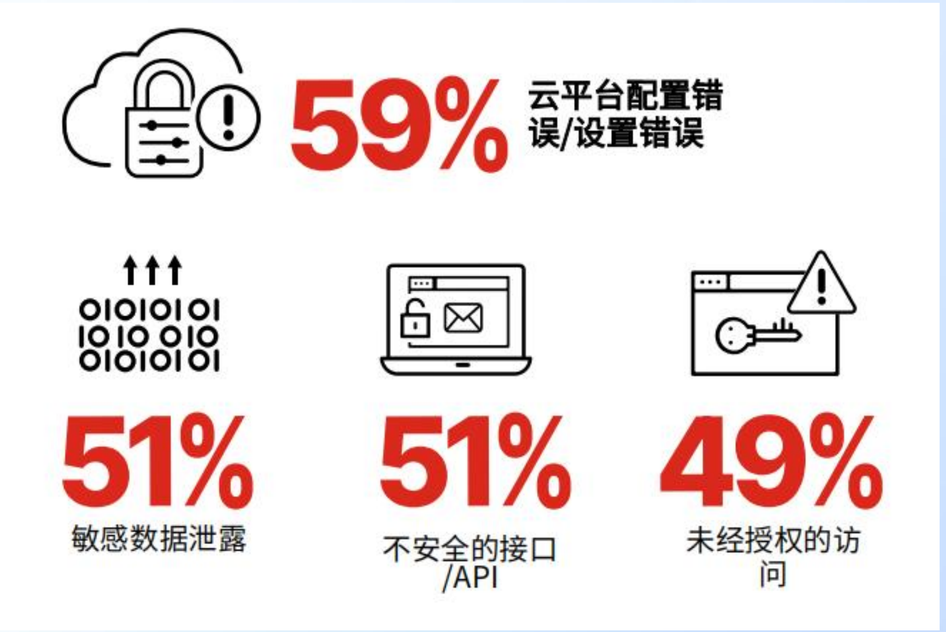
空间搜索引擎获得桶名

云上安全事件分布

公司/事件	时间	问题	损失/影响
Tesla	2018年	开放的 S3 存储桶	企业secret 泄露，导致大量研发信息和敏感数据暴露
Health Net	2017年	错误的存储配置	错误的存储配置
GitHub	2020年	配置错误的 API 密钥	机密数据暴露，引发了安全漏洞的广泛披露
T-Mobile	2023年	错误配置的 API 密钥	涉及 3800 万用户数据泄露，造成巨额损失
Twitter	2023年	开放的存储桶	攻击者访问了大量用户数据，导致数据泄露和声誉受损
Coinbase	2022年	错误的 API 配置	导致用户账户数据泄露，造成约 2.2 亿美元的损失
Uber	2016年	配置错误	5,700 万用户数据惨遭泄漏，被罚处 1.48亿美元
Microsoft	2019年	云服务错误配置	2.5 亿条客户服务信息被泄漏

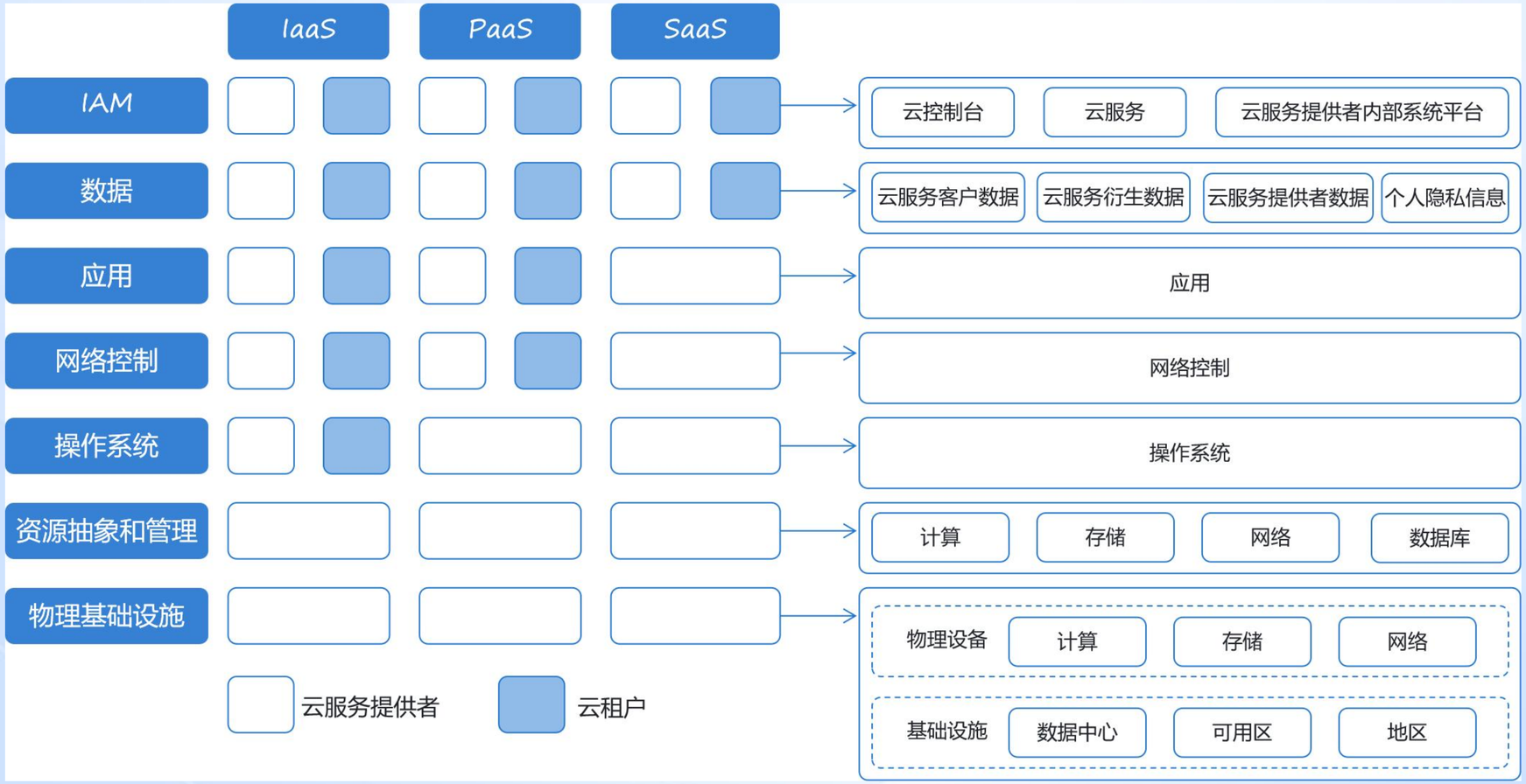
根据对全球752 名网络安全专业人员进行的一项调查：

59% 的受访者认为，在所有发生的云上安全事件中，配置错误导致的问题仍占据榜首



责任共担模型

云上责任共担模型



云服务提供商负责确保基础设施的安全，而用户则负责保护其在云中运行的应用程序和处理的数据。

02

多云安全运营的困扰

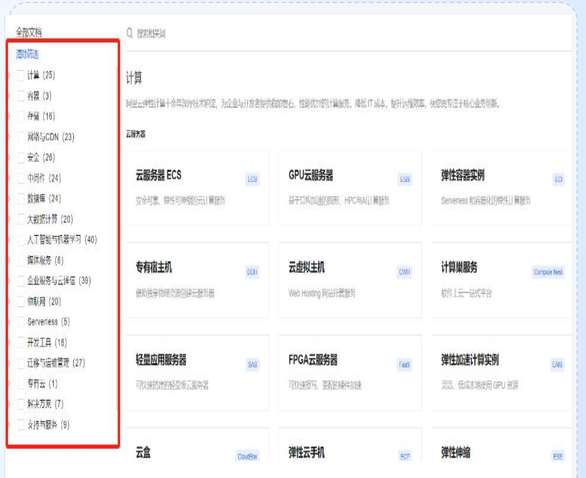
缺乏对云上安全盲点的感知能力

平均每个企业使用了20种以上的云服务，但超过80%的企业云用户难以回答以下问题：

- 我的组织使用哪些云服务?
- 谁对云资源进行了更改?
- 他们做出了哪些改变?
- 变化是什么时候发生的?
- 我的云环境中存在哪些云配置错误?
- 我的组织是否存在合规性要求?

AWS

306类云服务
10w+页文档



阿里云

336类云服务
10w+页文档

多云安全统一管控能力不足

缺乏云间一致性

不同云之间，云服务、操作、最佳实践均存在差异，很难统一安全合规和控制策略

缺乏统一可见性

不同云之间，平台各自相对独立，缺乏整体的、统一的视角对不同平台的信息进行分析管理

重复性手工配置

不同云之间，运营人员每天需要登录到各个不同云进行大量重复性工作，效率底下

云上风险治理复杂

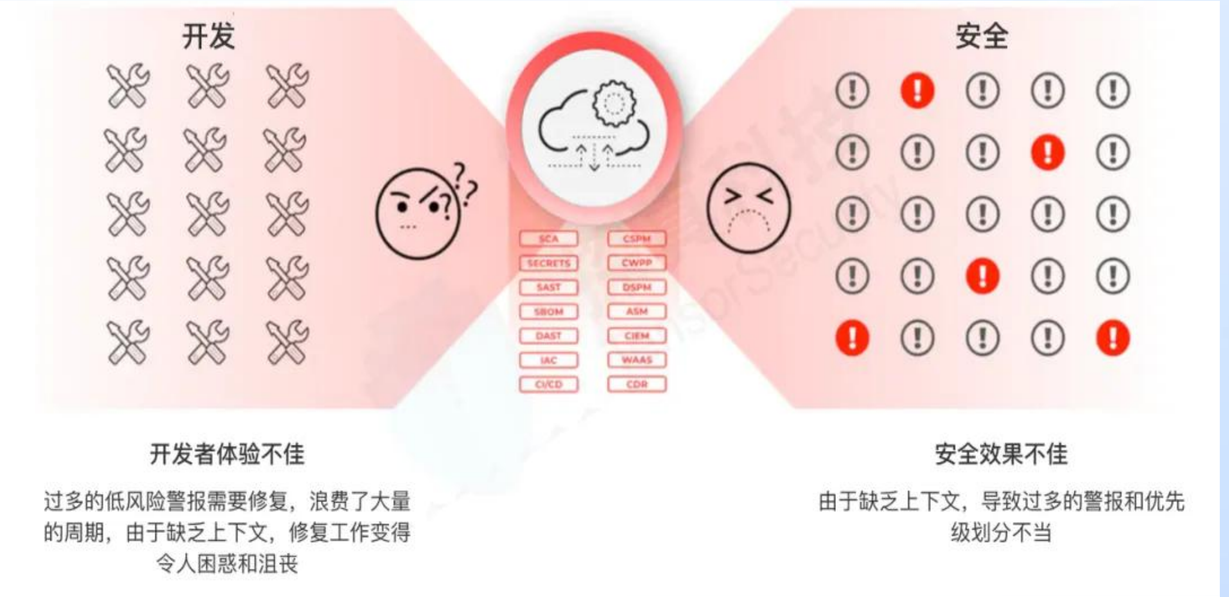
专业人才稀缺、成本高昂

具备多云安全技术能力的人员匮乏，招聘困难，且成本高昂，一个具备较强云安全技术能力的工程师平均薪资大概在**50w以上**

告警/漏洞泛滥，研判困难

各类安全工具多噪音大，导致告警研判复杂度变大，研判效率低，基于传统的CVSS评分的漏洞评级体系无法满足企业对于优先级修复的需求

Gartner 表示，“安全团队被认为正在减慢现代 DevOps 模式的开发速度。”



03

多云安全态势管理

什么是CSPM（云安全态势管理）

Gartner 定义的 CSPM（云安全态势管理），是一款持续地自动识别和管理云中风险的工具，主要负责识别云基础设施中的错误配置和合规问题

CSPM 在 CNAPP 中的角色集中在确保云基础设施的配置和操作符合最佳实践、企业安全政策和合规性要求。

早期 CSPM VS 新一代 CSPM 功能差异

	多云支持	云配置检查	合规性检查	工作负载风险检测	数据风险检测	基于上下文的风险洞察	修复优先级推荐	AI 赋能运营
早期 CSPM	✓	✓	✓	×	×	×	×	×
新一代 CSPM	✓	✓	✓	✓	✓	✓	✓	✓

CSPM可以干哪些事

CSPM核心能力

云资产自动发现

支持识别虚拟机、容器、无服务器函数、Kubernetes集群等多种资源和服务，为用户提供一个统一的视图来管理和保护云资产。

持续的配置错误及风险监控

CSPM通过持续监控云配置，帮助用户识别和修复可能导致数据泄露的配置错误。它根据业界认可的最佳实践标准，自动审查用户的云资源配置，一旦发现配置与最佳实践不符，系统会立即通知用户。

无代理风险评估

CSPM 通过深度结合云平台的能力，通过快照等方式，提供了一种有别于传统的无代理漏洞扫描模式。快速识别云工作负载和风险态势，检测配置错误和漏洞，且不影响业务运行。

基于上下文的风险洞察

CSPM 超越了简单的漏洞和配置错误识别；它结合用户活动、资产信息、云环境、数据敏感度和威胁情报等数据，提供基于上下文的洞察，帮助组织全面了解每个问题的影响范围。

合规性监控

使用 CSPM 自动化监控云环境的合规性，确保遵守行业标准和法规。它持续扫描云配置，检测不合规情况，并提供审计报告。

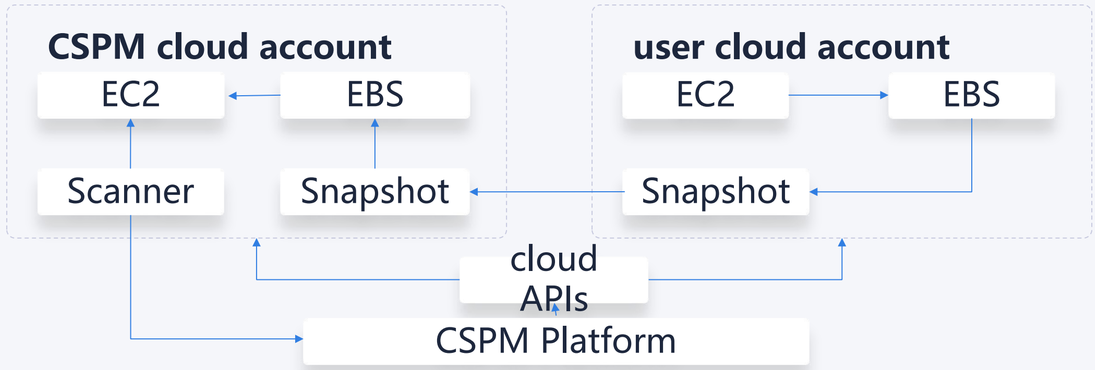
引导式修复

CSPM 不仅擅长检测潜在的安全问题，还能提供引导式修复措施，即：不仅会提醒用户有关问题，还会提供有关如何修复问题的详细指导。

无代理风险评估

典型CSPM产品架构

无代理工作负载扫描

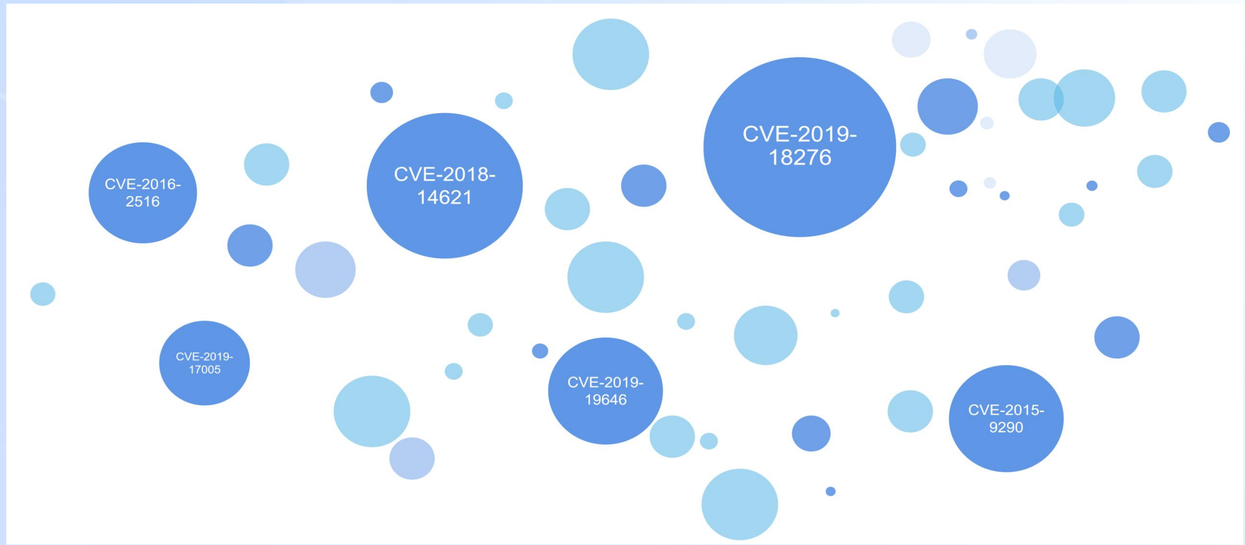


特点	Agentless	Agent
接入形态	API	agent
云负载漏洞检查	有	有
云资产清点	有	有
接入速度	快	较慢
云服务配置检查	有	无
业务影响	不影响	影响
实时攻击拦截	无	有

基于上下文的风险洞察

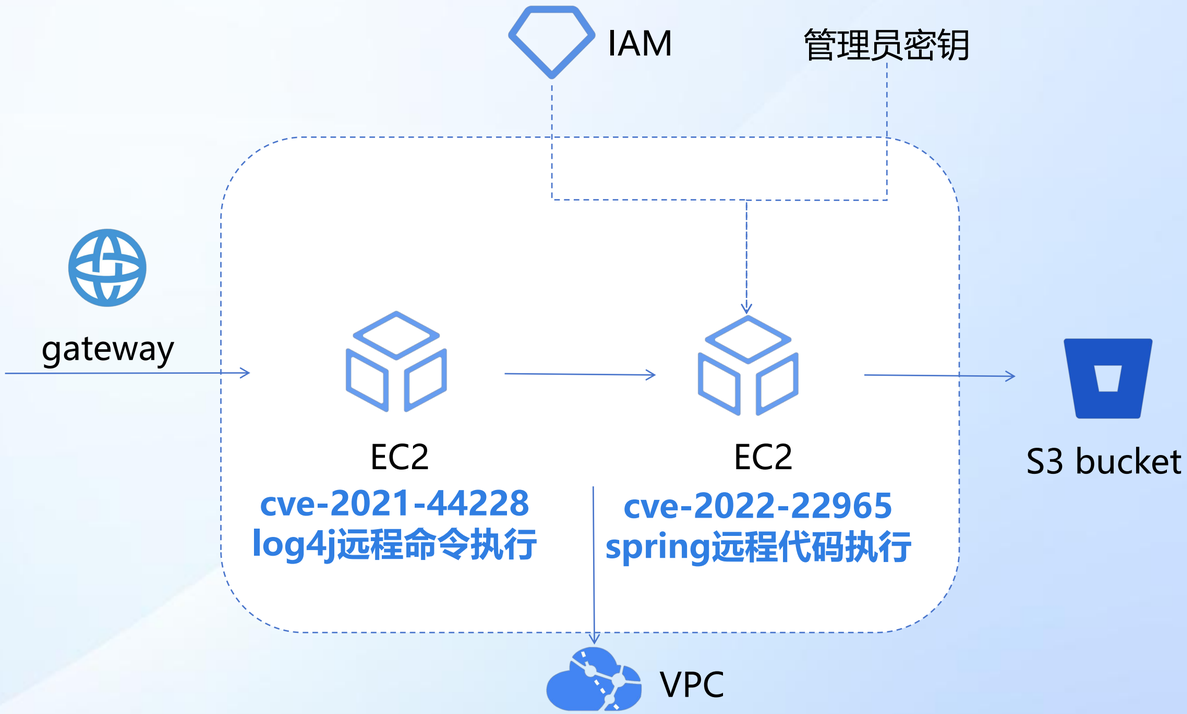
以漏洞评级修复漏洞

根据调查发现，在每年新发现的近20000个漏洞中，即使安全团队修补了所有高危和严重漏洞，也不过**只修复了24%的可利用漏洞**，而这更意味着，安全团队修复的**76%的漏洞是短期内几乎无风险**。更糟糕的是，有**44%的短期可被利用的漏洞被评为中低风险**，而很可能被忽略掉。



以脆弱链视角修复漏洞

根据扫描到的信息和脆弱性，以攻击者思维，推测入侵路线，确定修复优先级



04

多云安全与LLMs

大模型应用方式的变化

1

统一中央大模型

Transformer、GPT、Diffusion、Attention Mechanism

2

提示词、RAG、微调

GraphRAG、Prompt Engineering、Fine-tuning， GenAI

3

分布式Agent、自动化

大模型能给云安全带来什么

- 安全知识问答?
- 攻击自动识别?
- 病毒样本分析?
- 威胁情报查询?
- POC自动生成?

虚拟安全运营团队

负责和用户交互、固化经验、下发任务。

负责提供特定安全领域的专业知识和操作建议。

自动化

模拟实际的安全运维人员，处理常见安全告警。

智能化

负责维护和改进LLM模型，确保模型的持续学习和准确性。

OWASP 中国 Open Worldwide Application Security Project

OWASP 中国 | 北京分会 Open Worldwide Application Security Project

网安加社区

探真科技 TensorSecurity

开源网安 SECZONE GROUP

BrainAu 脑动极光 BRAINAU

THANKS

感谢您的观看

2024 OWASP中国安全技术论坛

全球视野下的网络安全趋势