CSA云原生应用保护平台调查报告 – 解读

汇报人：谢奕智

CSA大中华区云原生安全工作组

CSA大中华区云原生安全工作组旨在提升云原生类产品技术，帮助更多安全从业人员解决在规划、实施和维护云原生安全体系架构时遇到的问题，针对云原生安全体系中涉及的每类技术制定相应标准。

目录

CONTENTS

背景介绍

以更好地了解业界对 CNAPP
的知识了解、态度和意见

1

- 确定云安全的优先级事项和面临挑战

2

- 行业对CNAPP采用的熟悉度和成熟度

3

- 了解安全态势管理、云工作负载保护和DevSecOps方面的当前方法和挑战

CSA《云原生应用保护平台调查报告》

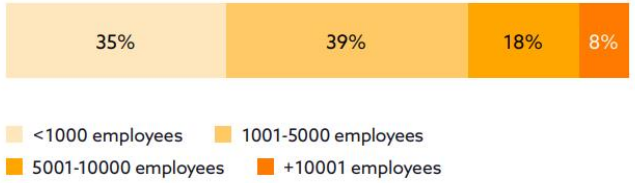
调查的创建和方法

调查由CSA于2023年4月在网上进行，收到了来自不同规模和地点的IT和安全专业人员的1201份回复。CSA的研究分析师进行了数据分析和解释。”

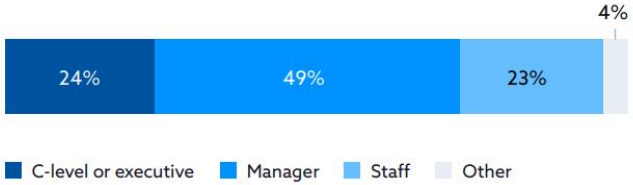
创建调查	数据收集	分析和报告
• 开发问题库 • 完善最终调查问卷	• 2023年4月份分发在线调查 • 收到1201份调查回复	• 研究团队对回收数据进行分析 • 找出3~5点重要的发现 • 基于分析的数据结果撰写报告

样本说明

What is the size of your organization?

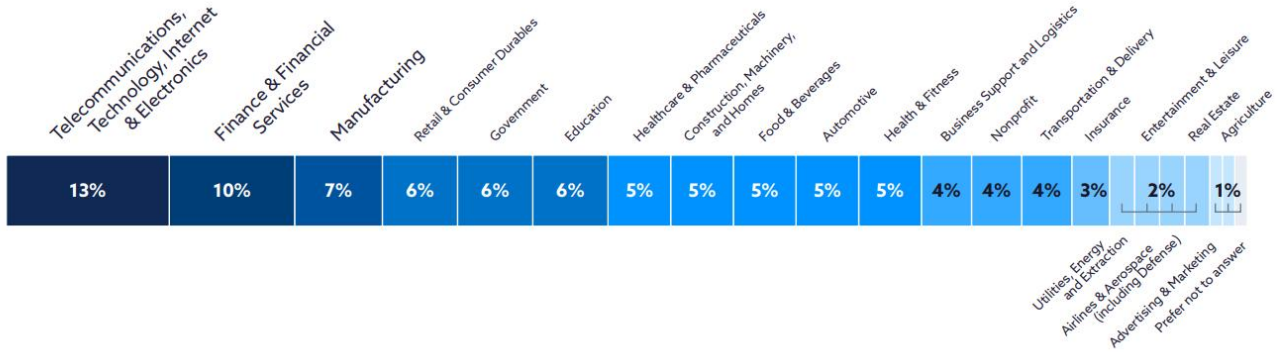


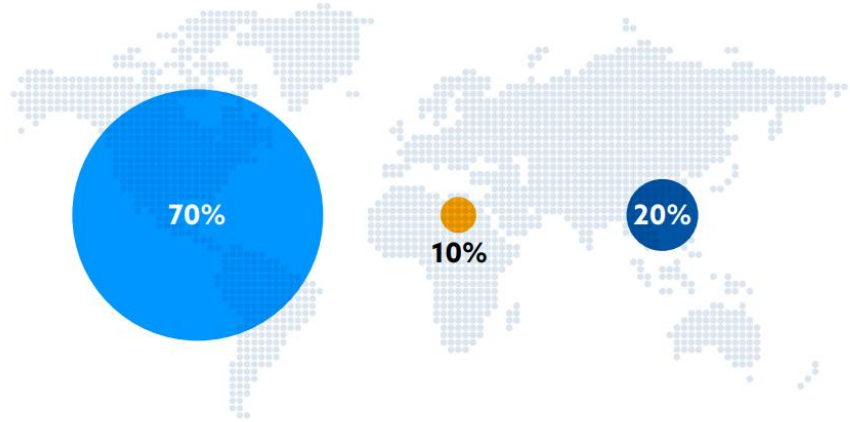
What is your job level?



What region of the world are you located in?

Which of the following best describes the principal industry of your organization?



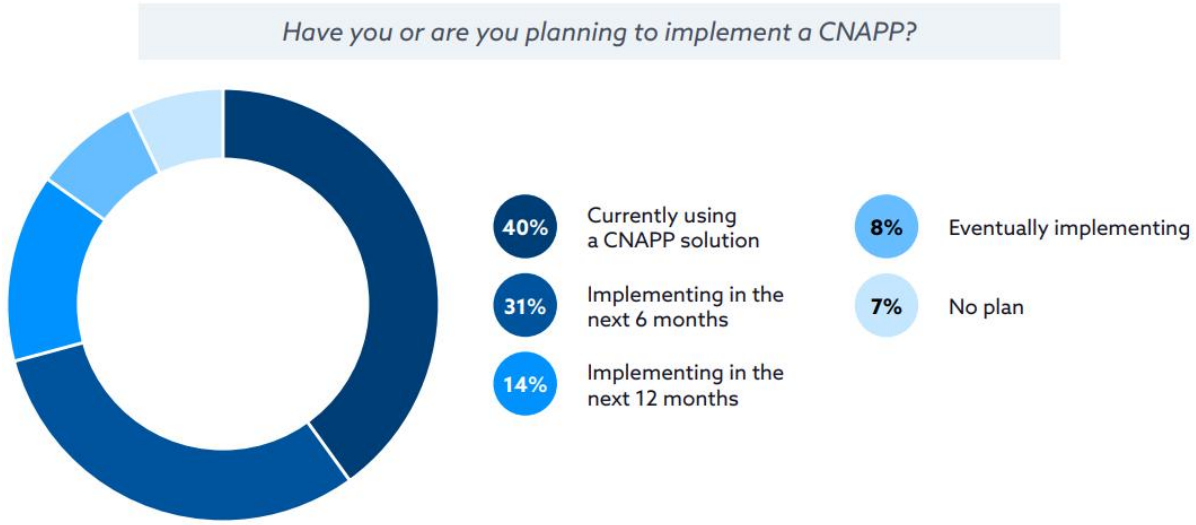


关键发现1：CNAPP

3 / 4的组织计划使用CNAPP来保护多云环境

对CNAPP有高兴趣的的主要原因

- 84%的组织使用2个及以上数量的云
- 提供跨多个云环境(例如，CSPM、CIEM、CWP)的覆盖的安全工具较少
- 提供核心功能
  - CSPM – 25%
  - security posture visibility – 42%



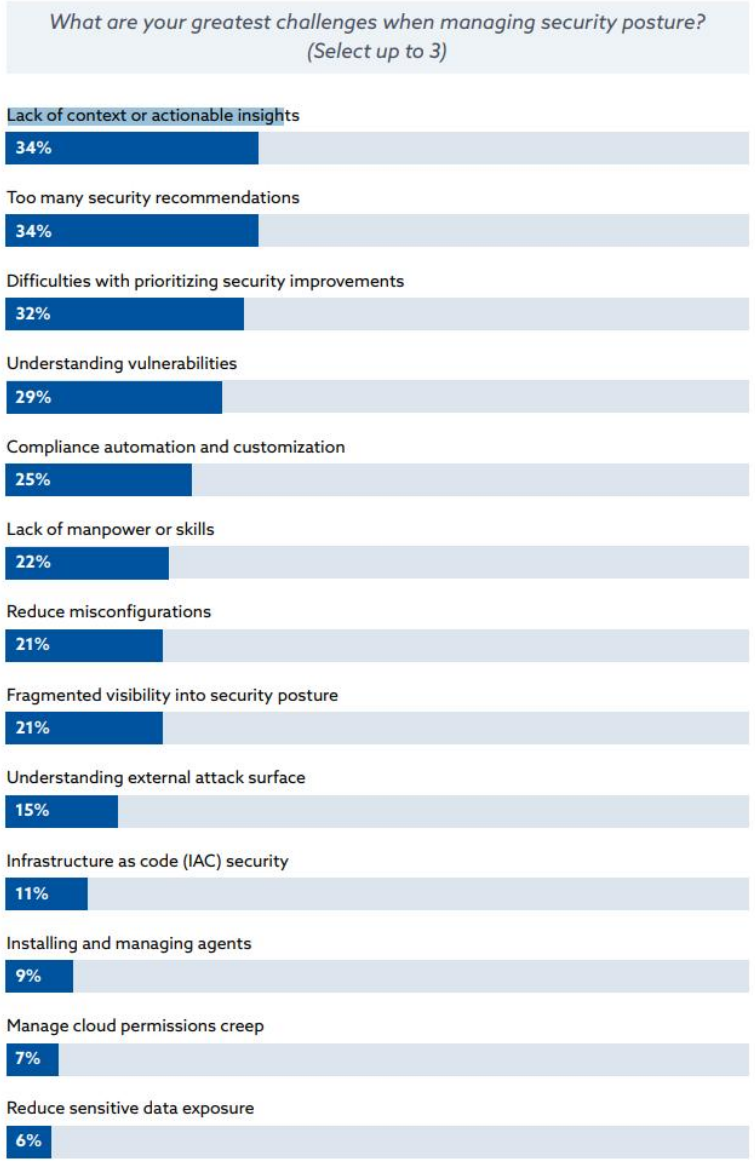
关键发现2：CSPM

安全团队要求的信息不明确，优先级不合理

32%受访者陷入安全优先级改善

被不准确或者不充分的信息淹没
- 太多安全建议 – 34%
- 缺乏上下文信息 – 34%

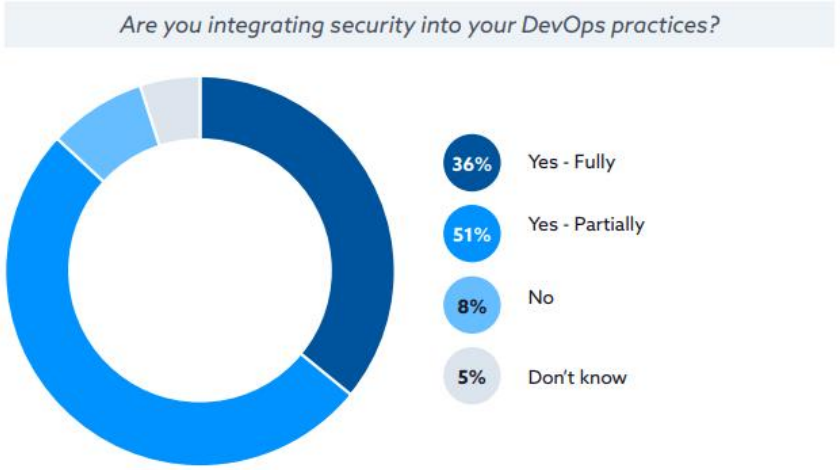
监控方式受到技术厂商影响
- agent方式 – 33%
- agentless方式 – 37%

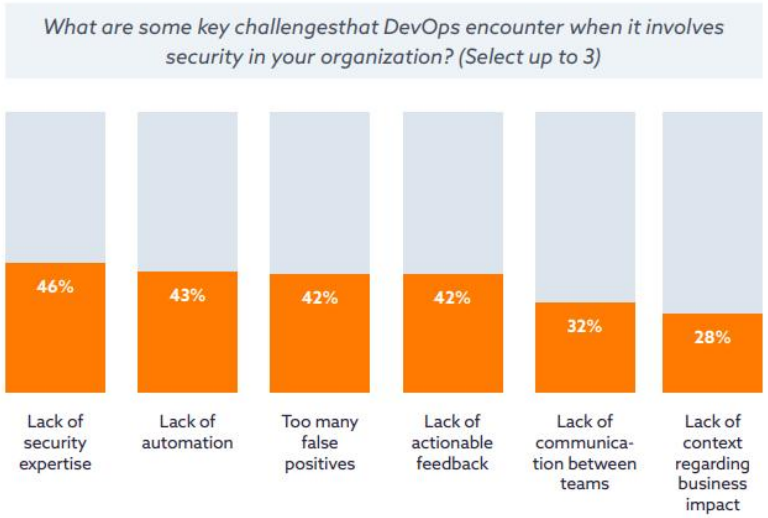


关键发现3:DevSecOps

越来越多的人认识到DevSecOps的重要性，但专业知识和人才的短缺阻碍了进展

- 51%进行中，35%完成集成
- DevSecOps面临挑战1：人才
  - 缺乏安全知识 – 46%
- DevSecOps面临挑战2：技术
  - 自动化程度不高 – 43%
  - 无告警数量多 – 42%
  - 缺乏可操作反馈

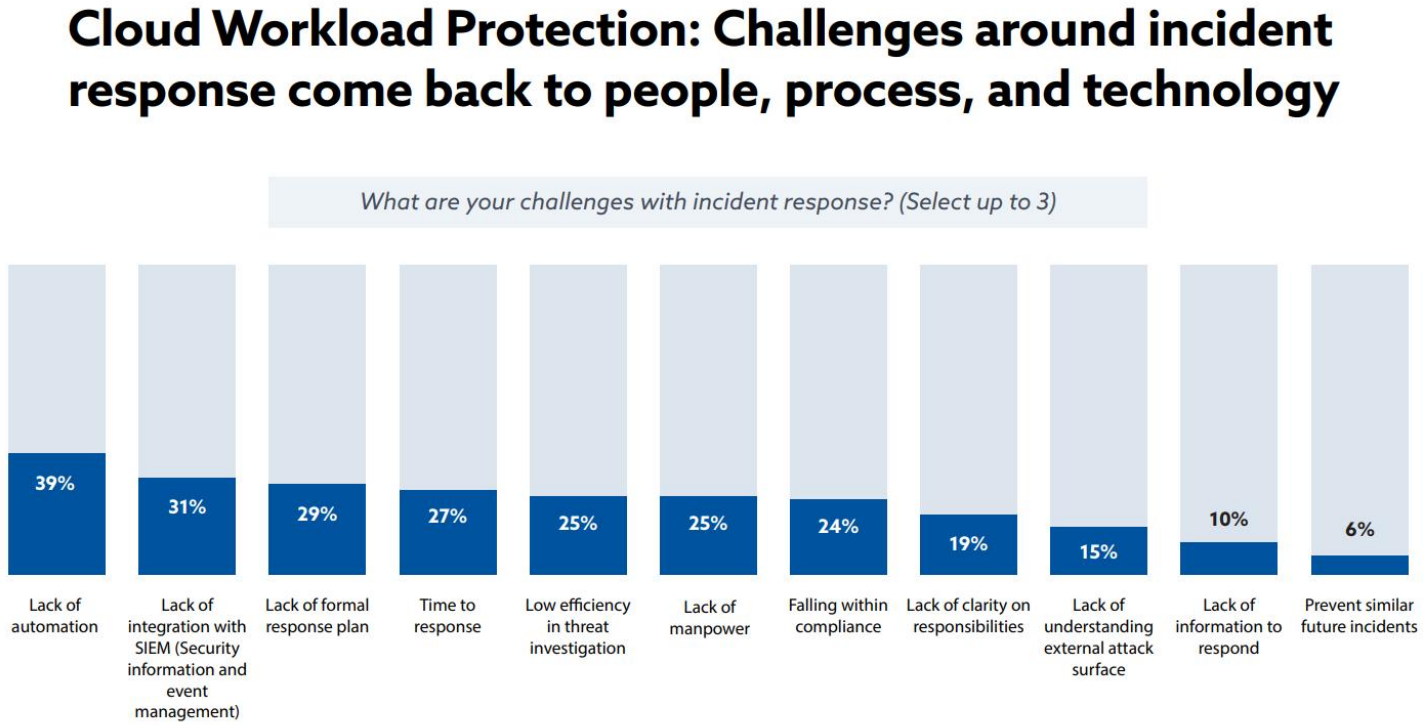




关键发现4:CWP

事件响应的挑战又回到了人员、流程和技术

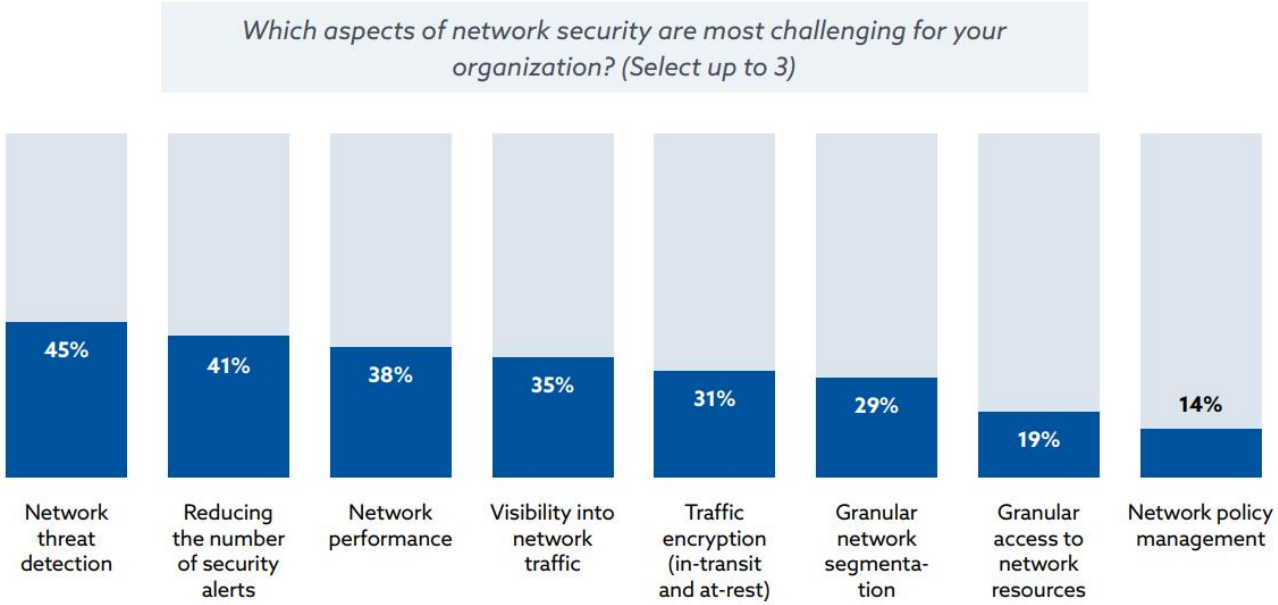
- 人员 – 缺乏人力 – 25%
- 流程 – 缺乏规范响应计划 – 25%
- 技术 – 缺乏自动化 – 39%



关键发现4:Network Security

最成熟的一个领域，但威胁检测仍然是一个挑战

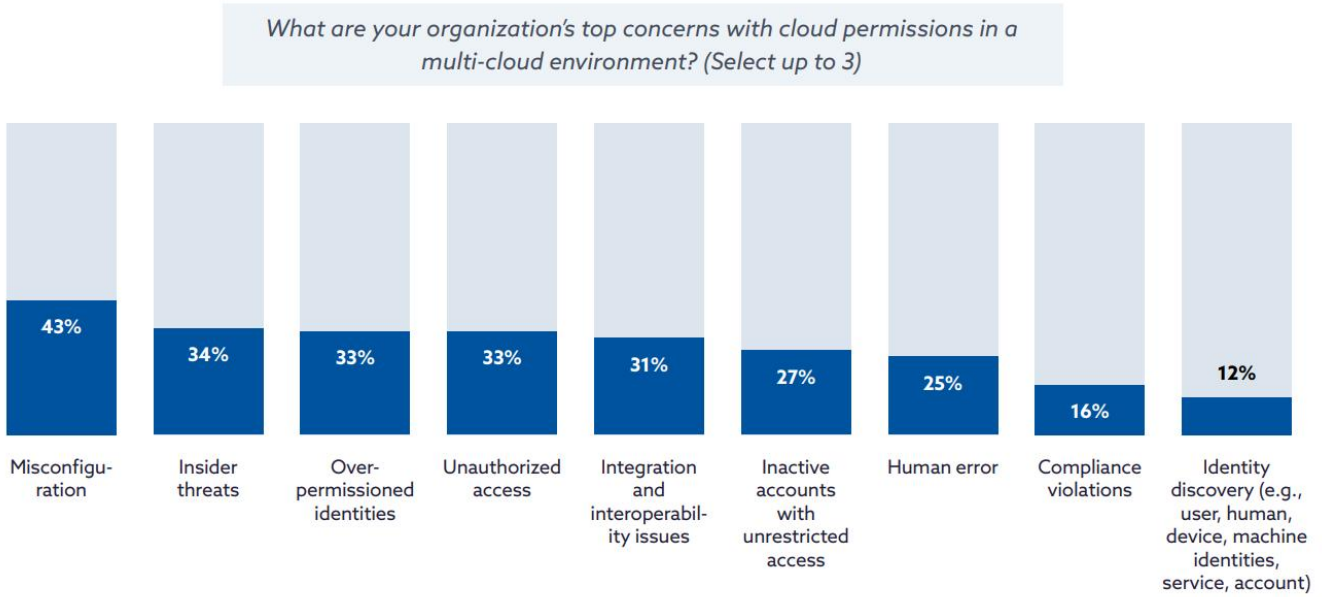
- 43%受访者反馈在多云环境中完全集成了网络安全– 25%
  - 相比之下，CSPM的使用率为28%
- 网络安全面临主要挑战
  - 威胁检测 – 45%
  - 减少安全告警 – 41%



关键发现5:CIEM Cloud Infrastructure Entitlement Management

关注多云环境下的权限配置不当问题

- 43%受访者表达对不当配置的担忧
- 不当配置可能导致其他关键问题，例如未授权访问(33%)或泄露敏感数据



THANKS

0755-86548359 info@c-csa.cn https://www.c-csa.cn/ 广东省深圳市南山区粤海街道北京航空航天大厦9楼905