Robert A. Kalka Metropolitan Skyport

Penetration Test Debrief

Finals-XX

Robert A. Kalka
Metropolitan Skyport

CONFIDENTIAL
DO NOT DISTRIBUTE

Team Introduction

Manager

Assistant Manager

Network Analyst

Reconnaissance Analyst

Cloud Analyst

Systems Analyst

Agenda

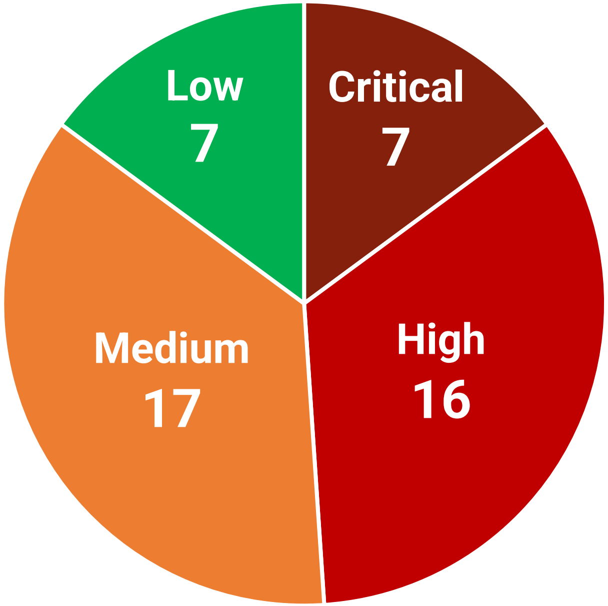
- **Summary of Engagement**
- **Findings**
  - Breakdown by Severity
  - Validate Fixes
- **Business Impacts**
- **Next Steps**
  - Remediations
  - Policy Changes

Summary of Engagement

- Followed up on our Q4 2023 penetration test
- Ensured the security of customer data
- Reevaluated vulnerabilities discovered in initial penetration test
- Identified key strengths and weaknesses of RAKMS’s security

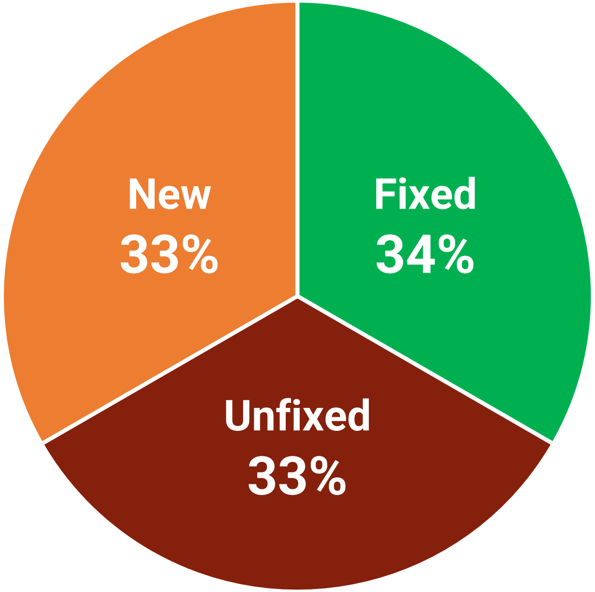
Findings

Findings and Remediations



48

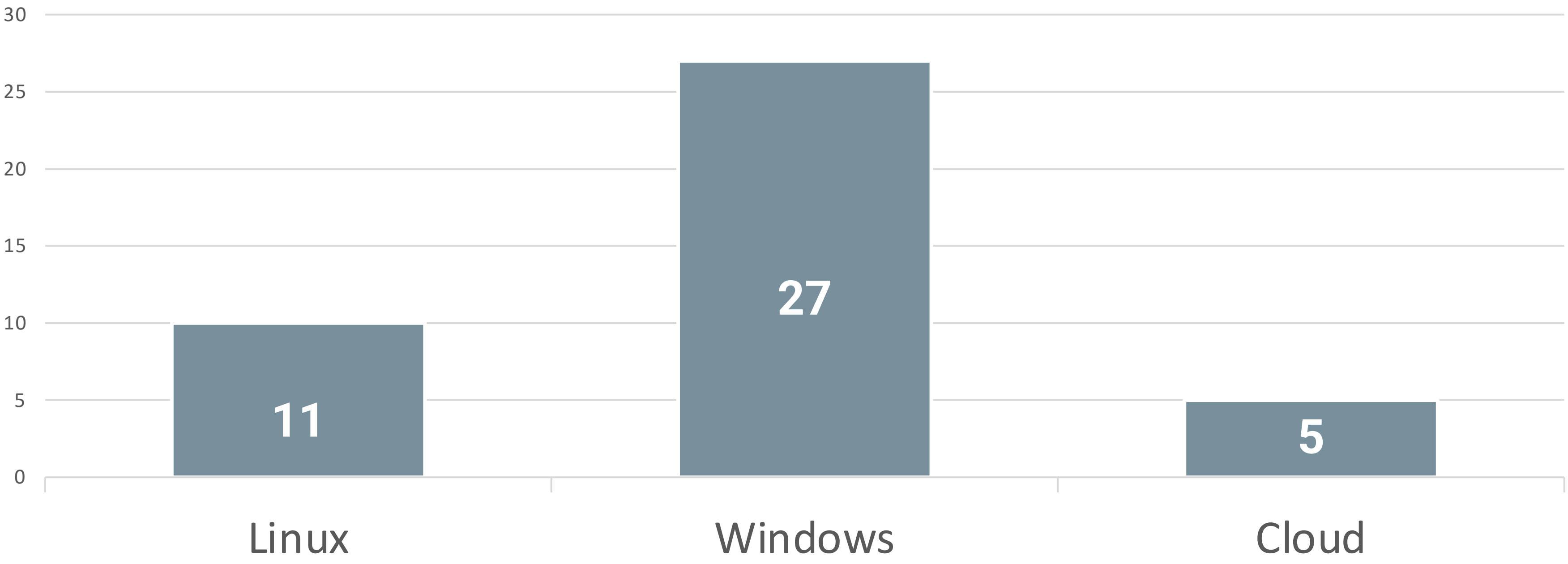
Vulnerabilities Discovered



CONFIDENTIAL

DO NOT DISTRIBUTE

Categorical Findings



CONFIDENTIAL
DO NOT DISTRIBUTE

Cloud Findings

Three custom internal applications

- Publicly exposed with no authentication.
- Policy misconfiguration allowing any user to gain privileged access.
- Arbitrarily large tool requisitions.
- Exposure of *PII* data due to insecure cloud storage including SSNs of 150 customers.

Business Impacts

Compliance

We checked our findings against applicable privacy regulations:

- **PCI DSS:** Payment Card Industry Data Security Standards *(Payment card processing)*
- **GDPR:** General Data Protection Regulation *(European Union)*
- **CCPA:** California Consumer Privacy Act
- **TSA** Emergency Amendment *(New)*
- **White House** Cybersecurity Strategy *(New)*

TSA Emergency Amendment

Critical New Legislation for Airports

https://www.tsa.gov/sd-and-ea

1. Federal Prosecution
2. Loss of Contracts
3. Emergency Changes Reflected in Report

CONFIDENTIAL

DO NOT DISTRIBUTE

Monetary Costs

$21,768,460*

Possible fine if findings are not fixed.

*Based on historical GDPR, CCPA, and PCI fines

CONFIDENTIAL
DO NOT DISTRIBUTE

Next Steps

Recommendations

We recommend continuing the following changes to further reduce risk:

1. Network Segmentation
2. Improving Access Policies
3. Software Patches + Antivirus