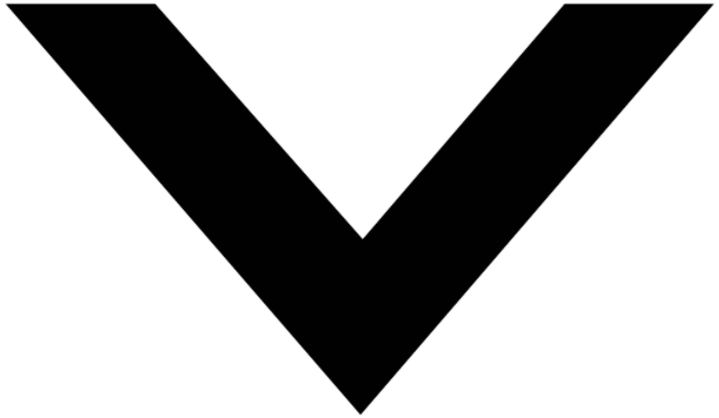


VICXER

SAP Situation Report

Q4 2019

DISCLAIMER

- This publication contains references to the products of SAP AG. SAP, R/3, SAP NetWeaver and other SAP products.
- Products and services mentioned herein are trademarks or registered trademarks of SAP AG in Germany, in the US and in several other countries all over the world.
- SAP AG is neither the author nor the publisher of this publication and is not responsible for its content. The SAP Group shall not be liable for errors or omissions with respect to the materials.

ABOUT US

*WE ARE **VICXER!***

- A company focused on securing the business-critical applications and its adjacent infrastructure (SAP, Oracle Siebel and others)
- All of our customers belong to the Fortune-500 Group
- We offer:

  Oracle & SAP Penetration Testing

  Cyber-Security Trainings

  Vulnerability Assessment and Management

  SAP Forensics & Many More!

VICXER

THE AGENDA

CHAPTER 01

Introduction

CHAPTER 02

Global Results

CHAPTER 03

Continental Results

CHAPTER 04

Conclusions

VICXER

CHAPTER 01

INTRODUCTION

SAP Situation Report Q4 2019

INTRODUCTION

VICXER

Mark of Reference

- This situation report, focuses on understanding the Internet facing SAP systems, and how these systems align to the status of SAP cyber-security in the current global market.

- We have analyzed the **Internet** facing SAP **Netweaver** systems, by applying **passive** discovering techniques, that allowed us to not only discover SAP assets (we only focused on web application servers), but their corresponding versions. It is important to clarify that ***NO active probes were executed on any of the detected systems. The collected information was obtained, by just analyzing the systems' metadata.***

- After the culmination of the data collection phase, our consultants compared the obtained SAP versions against a comprehensive set of SAP vulnerabilities (*disclosed by **SAP**, by **external** security researchers like **Vicxer** and private / semi-private vulnerabilities*)

- The **results** of this study will be divided in two, one section will contain the **worldwide** results, while the other, will outline the results per **continent**.

VICXER

CHAPTER 02

GLOBAL RESULTS

Discovering Internet Facing SAP Systems

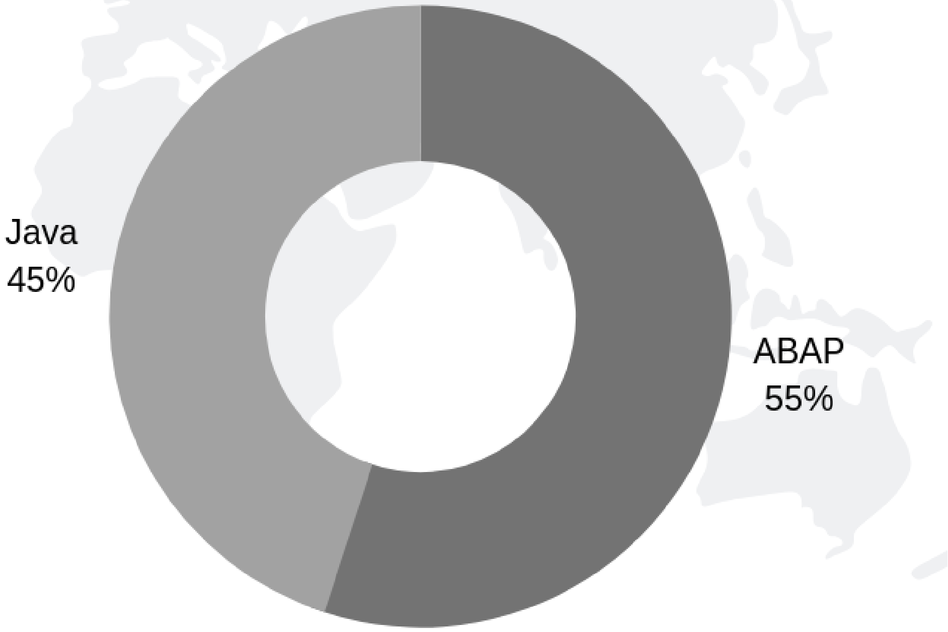
GLOBAL RESULTS

VICXER

The Big Picture

GLOBAL SAP SYSTEMS

Currently, there are more than **6339** SAP systems exposed to the Internet

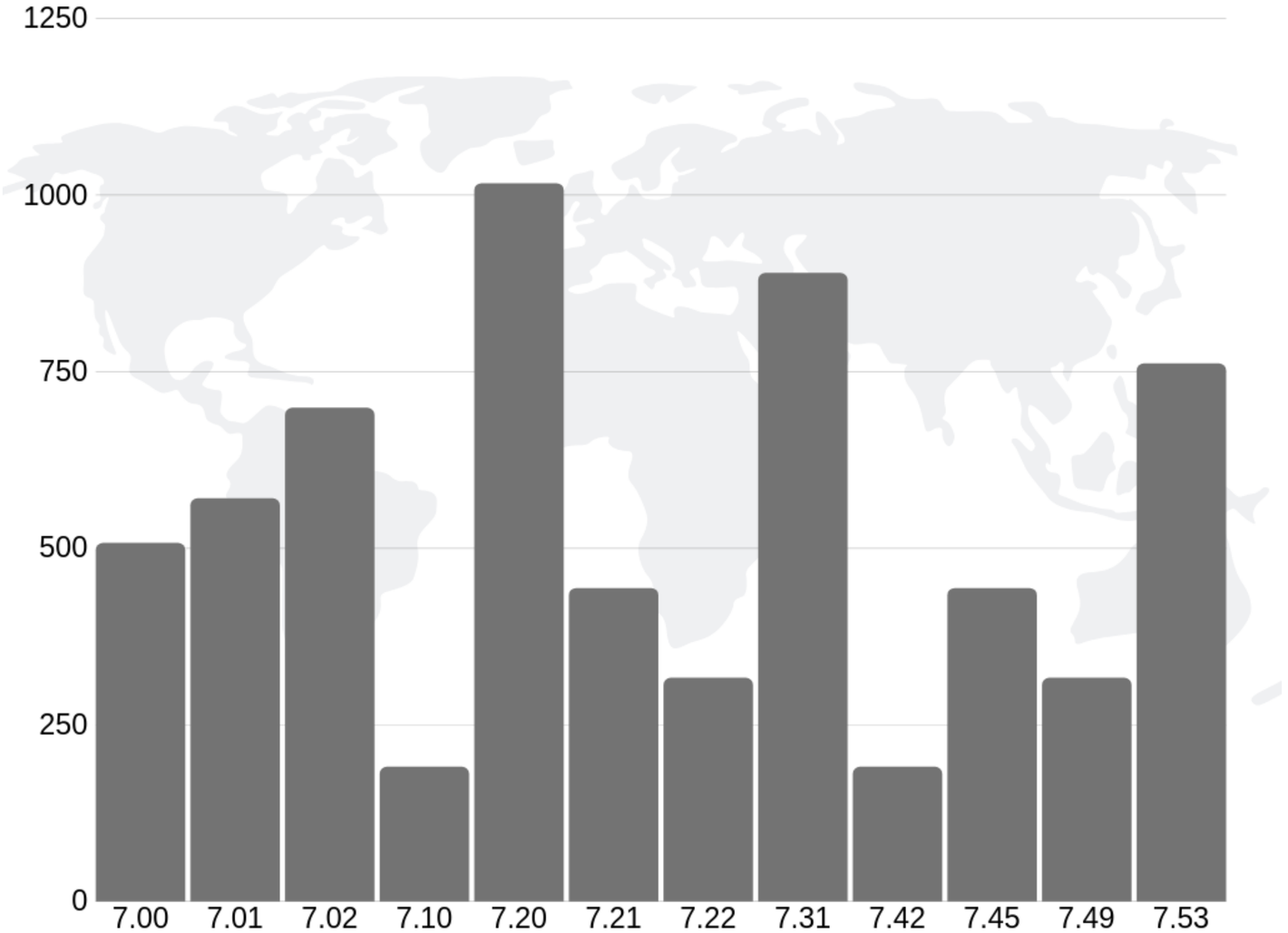


** Only SAP Netweaver systems were considered for this statistic. Current ratio might be different for non-Internet facing assets*

GLOBAL RESULTS

VICXER

The Big Picture



GLOBAL SAP VERSIONS

Exposed Web Application Servers (WebAS)

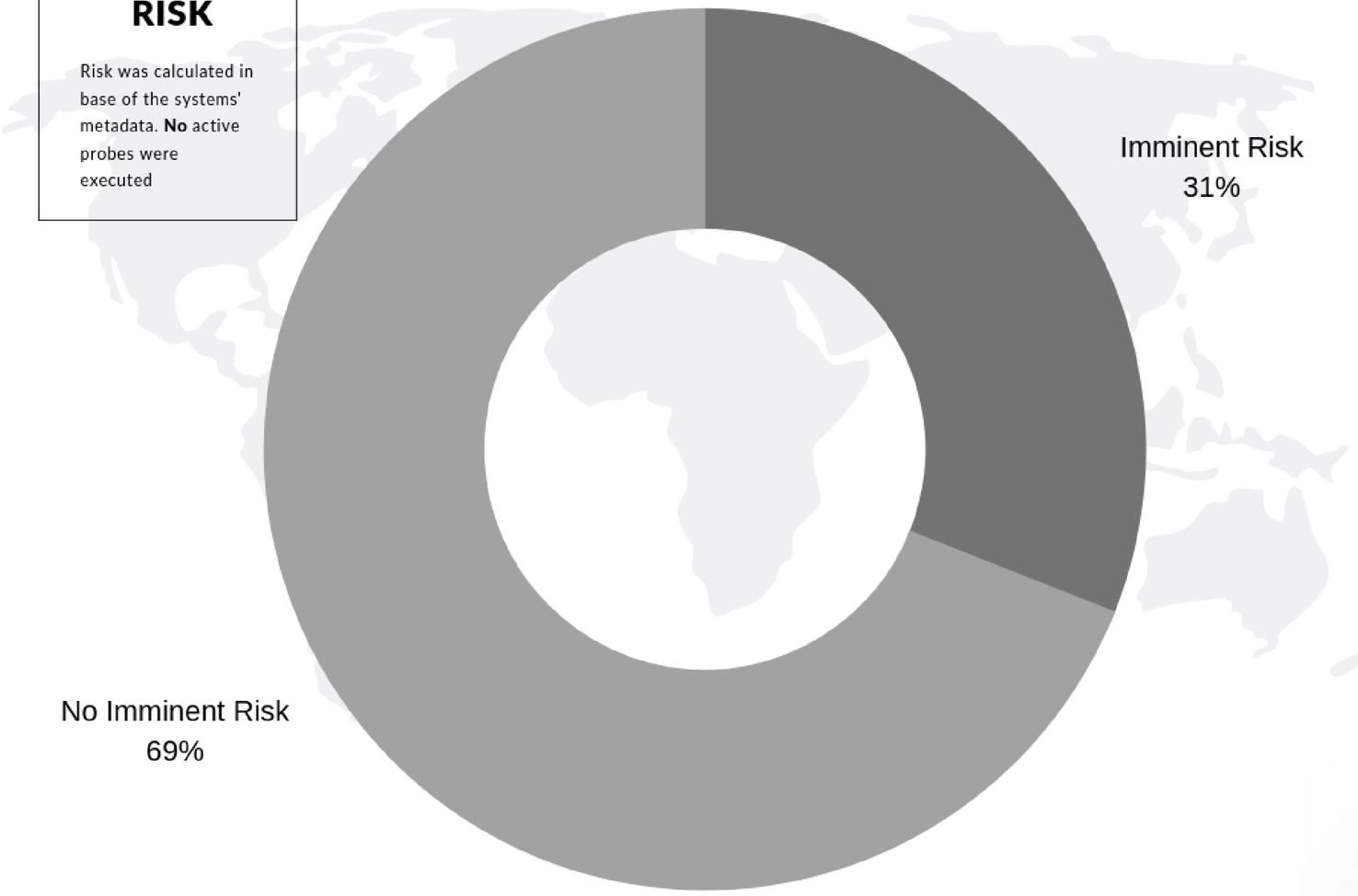
** Versions correspond to SAP WebAS*

GLOBAL RESULTS

The Big Picture

GLOBAL RISK

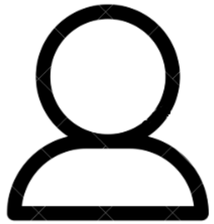
Risk was calculated in base of the systems' metadata. **No** active probes were executed



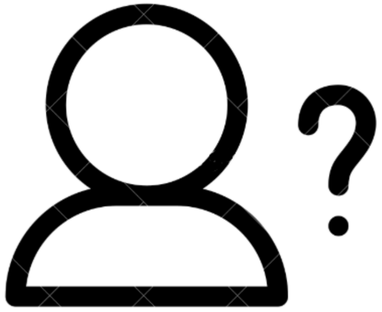
** Only SAP Netweaver systems were considered for this statistic*

GLOBAL RESULTS

The Big Picture



37.86%



62.14%

GLOBAL SAP OWNERS

Identified institutions / companies behind the assets

** To check if your company / institution is on this list and if it is at risk, please visit https://vicxer.com/research/situation.html*

CHAPTER 03

CONTINENTAL RESULTS

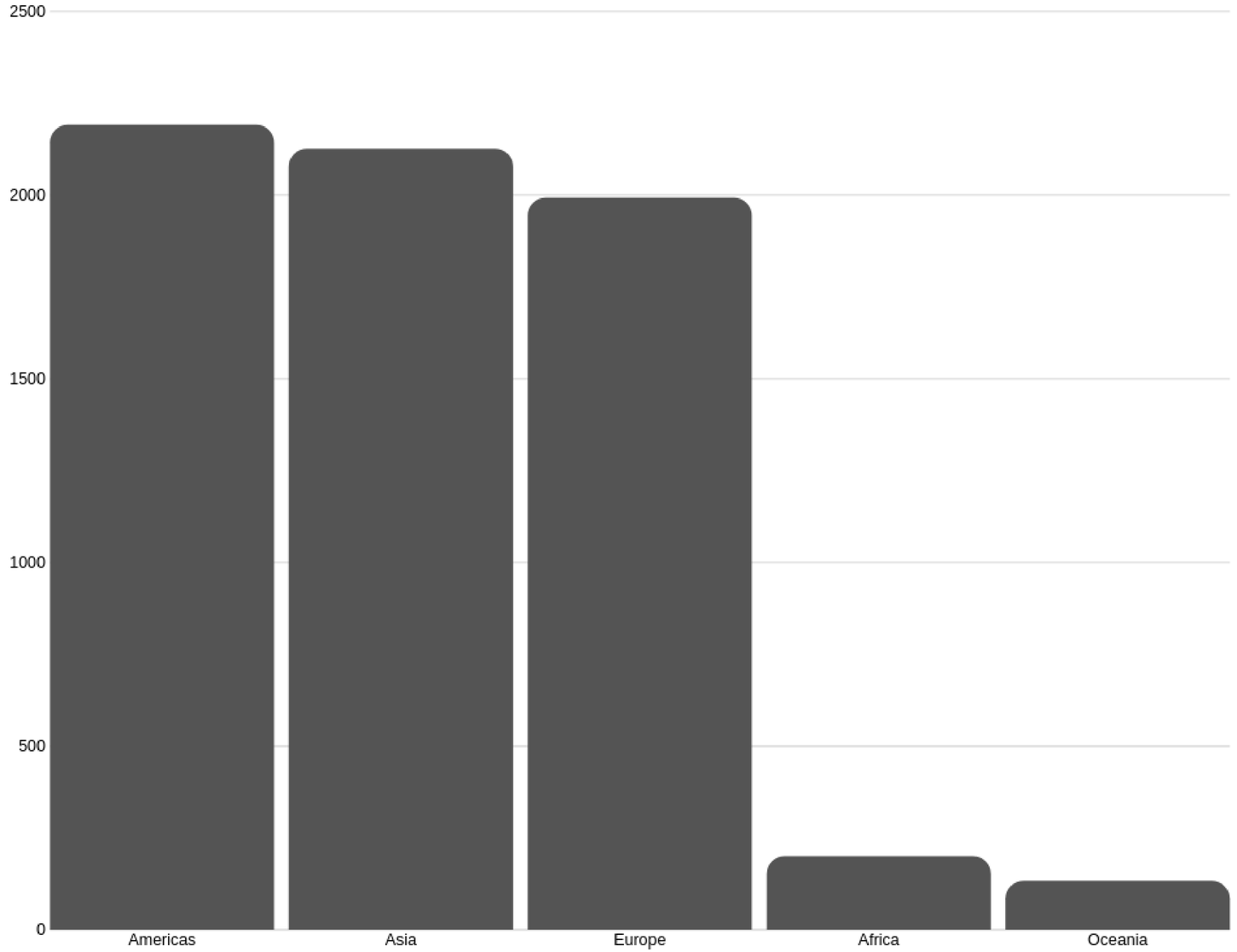
SAP Results Sorted Per Continent

CONTINENTAL RESULTS

The Sum of Everything

SAP MAP

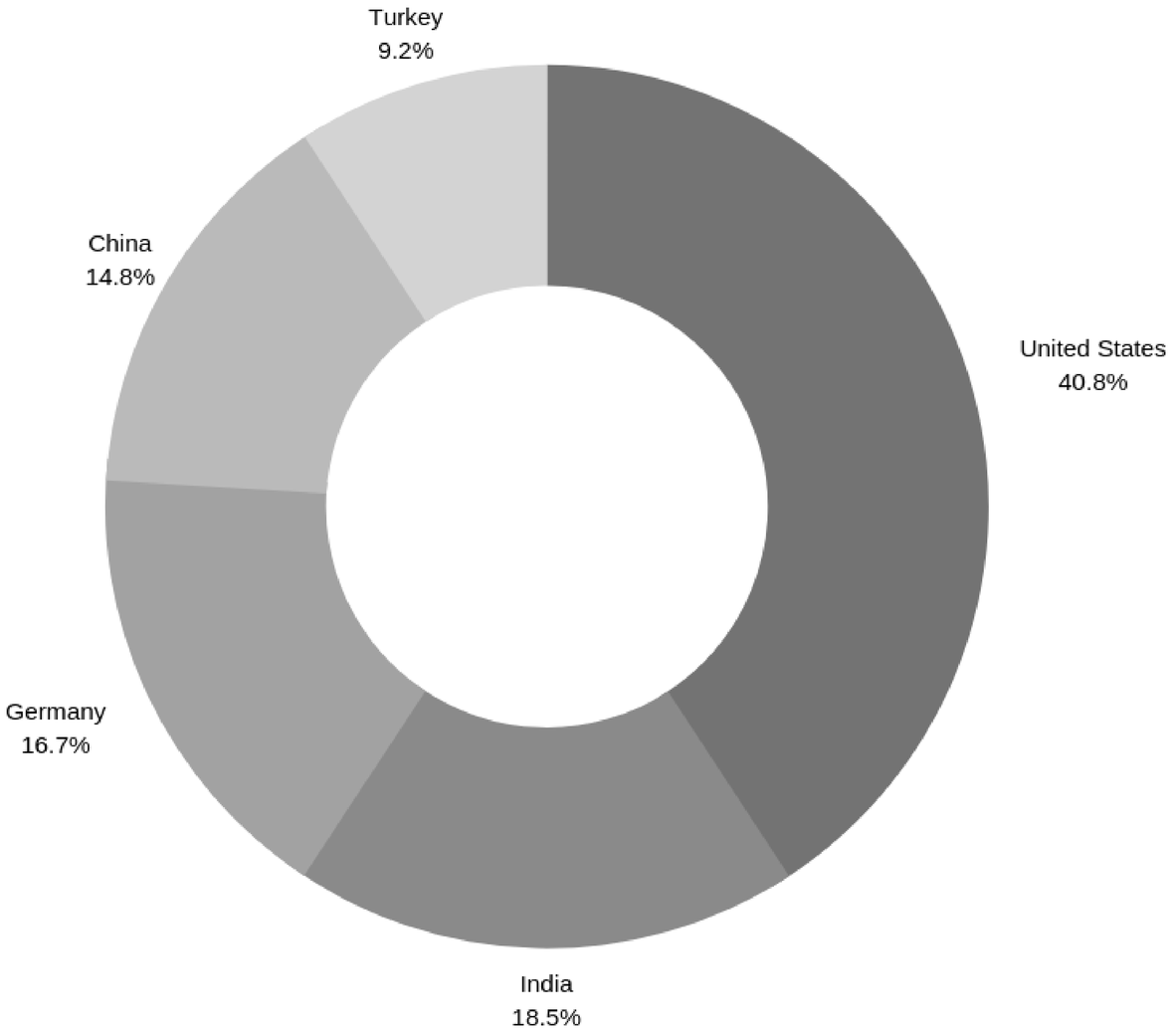
Distribution of SAP Internet facing systems per continent



CONTINENTAL RESULTS

VICXER

The Sum of Everything



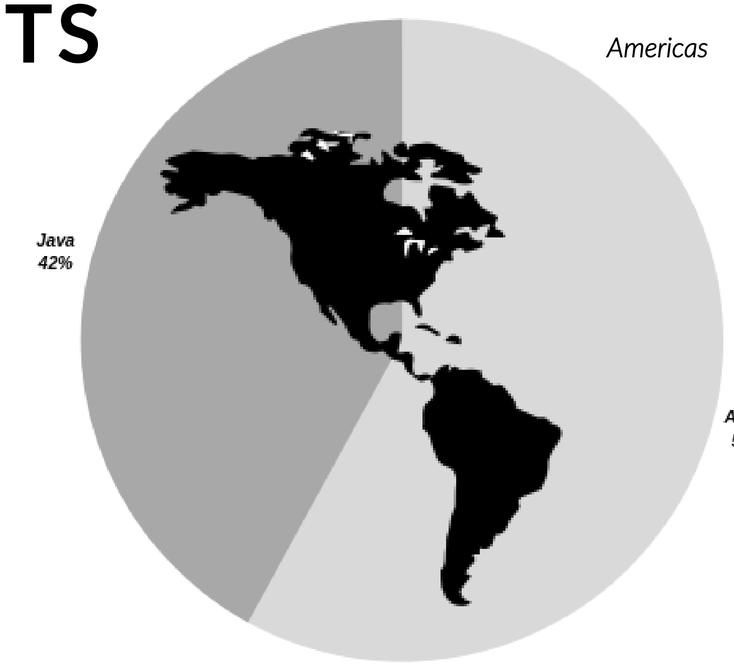
SAP MAP

Top 5 countries with the highest amount of SAP Internet facing systems

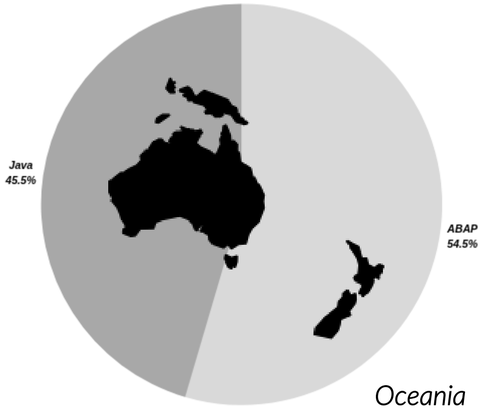
CONTINENTAL RESULTS

VICXER

The Sum of Everything



Asia



Oceania

Africa

Europe

SAP MAP

SAP Internet facing stacks per continent

VICXER

CHAPTER 04

CONCLUSIONS

*SAP Situation Report at **Q4 2019***

CONCLUSIONS

VICXER

Project Results – An Objective View

- One-third of the detected Internet facing SAP systems, are currently affected by serious vulnerabilities that could allow a **remote** and **unauthenticated** attacker, to compromise **the target SAP systems,** and possibly perform lateral movement on the DMZ / adjacent network.
- Our team **could not find any evidence** that, **expensive solutions like IDS** / **IPS** systems would have a **meaningful** impact on stopping and preventing SAP intrusions (specialized SAP solutions will be tested on the next exercise)
- Firewalls **will not stop** most of the specialized attacks either, as the SAP web application server ports need to be open and unfiltered, in order to serve the valid users / customers.
- The main critical factors are caused by the customers inability (technical or political) to upgrade to a modern SAP version, in combination with the lack of a robust and **periodic** SAP patching policy.
- As a side result, it was possible to detect that some organizations are not just exposing **productive** SAP systems to the Internet, but **development** and **quality assurance** as well.

CONCLUSIONS

VICXER

Follow Up Actions for SAP Customers

- Know your assets! more often than not, companies cannot tell exactly, how many SAP assets they own.
- If you haven't already, make sure your SAP assets are included in your general patching strategy. Appoint a technical champion to oversee the progress of this task.
- Ensure that all the SAP audit trails are enabled*
- Before investing in expensive SAP security products, perform a quick SAP penetration test, in order to understand where your SAP implementation stands in terms of cyber-security, and how it compares to similar sized organizations.

** https://www.youtube.com/watch?v=ISa8lpSkHH8*

CONCLUSIONS

VICXER

Follow Up Actions for Security Researchers

- **We have the obligation** to enrich the security of the organizations with **integrity**, **consolidated knowledge** and **empathy**, while avoiding the spread of misinformation, uncertainty and doubt.
- We need to **contribute more** to open initiatives like local meetups, technical gatherings and conferences, by sharing **novel**, **unbiased** and **relevant technical knowledge**.
- We must take a **unifying** role in the organizations running SAP, by being the nexus between the SAP team and the IT security world.

THAT IS ALL...

VICXER

QUESTIONS?

To learn more about **SAP security**, visit us at ***https://vicxer.com*** or follow us on Twitter

@VICXERSECURITY

@JSANTARSIERI