Lancaster University

Measuring Discrepancies in Attack Surfaces Generated By Internet Intelligence Platforms

Martin Price

m.g.price@lancaster.ac.uk

Nicholas Race, Paul Smith

Background

- In 2024, half of all UK businesses faced a disruptive cyber attack, even more recent with M&S
- Organisations and Policymakers are searching for solutions
- To understand the risk faced, the attack surface of an organisation must be known
- Motivated by previous work with the NCSC who wanted to understand an attack surface and vulnerabilities at a sector-wide scale.

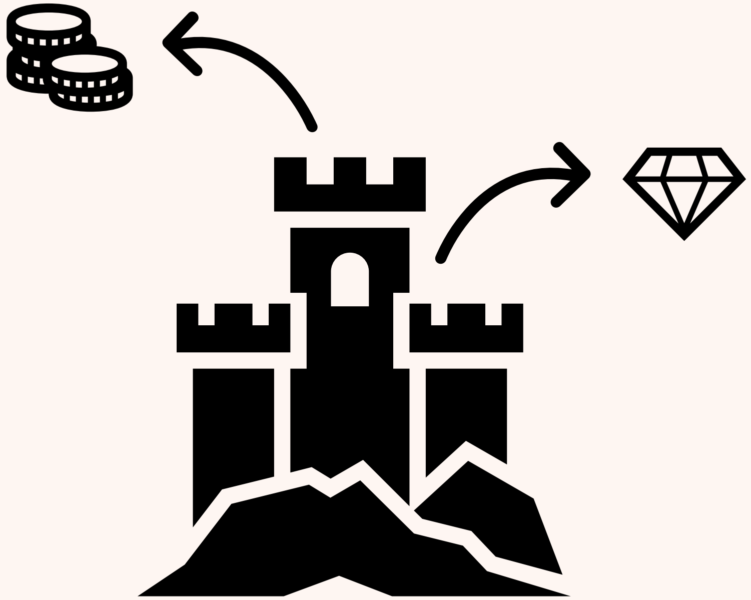
The External Attack Surface

- “Assets or services that are publicly reachable online” – NCSC [1]
- We quantify this as the IP addresses of the assets or services, such as a webpage host.
- Theoretically, it is easy to discover the surface, just ask the Regional Internet Registry
- All your services run on your assigned addresses, inside your ‘castle’

[1] ‘ACTIVE CYBER DEFENCE 2.0 Attack surface management experiments’, National Cyber Security Centre, Mar. 2025. Accessed: May 16, 2025. [Online]. Available: https://www.ncsc.gov.uk/files/Active-Cyber-Defence-2-ASM-experiment.pdf

The External Attack Surface

- Cloud Computing and Third-Party hosting has made it difficult to map
- Services are being hosted externally
- Crucial services are no longer within your managed network, moved outside your ‘castle’
- Manually discovering this surface is problematic, there is no ground-truth
- EASM tools attempt to mitigate this



Internet Intelligence Platforms

- Also known as Internet Search Engines or Web Spiders…
- Continually scans the internet, grabbing as much data as possible, such as TLS certificates and Domain Names
- Integral in current attack surface research [1,2]
- Their difference in scanning methods could result in discrepancies

Shodan	
Country	America
Background	Product
Pricing	Subscription
Cost	$69 - $1099
Approach	Proprietary

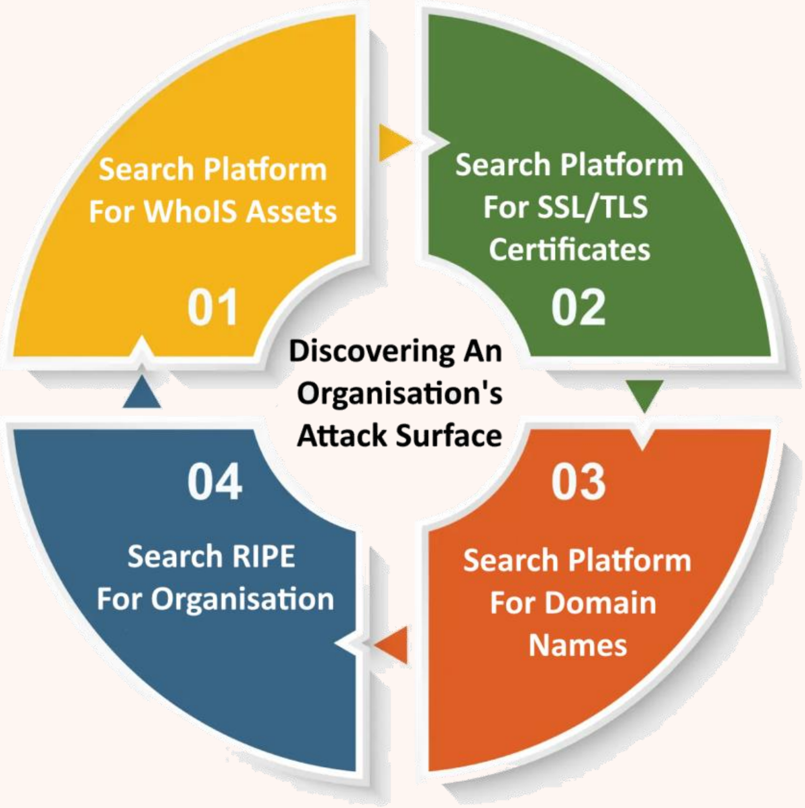
Censys	
Country	America
Background	Research
Pricing	Credits
Cost	$100 - $7200
Approach	ZMap

ZoomEye	
Country	Hong Kong
Background	Product
Pricing	Credits
Cost	$19 - $1099
Approach	???

[1] T. Ashley, S. N. G. Gourisetti, N. Brown, and C. Bonebrake, Dec. 2022, doi: 10.1016/j.cose.2022.102939.
[2] C. Harry, I. Sivan-Sevilla, and M. McDermott, doi: 10.1093/cybsec/tyae032.

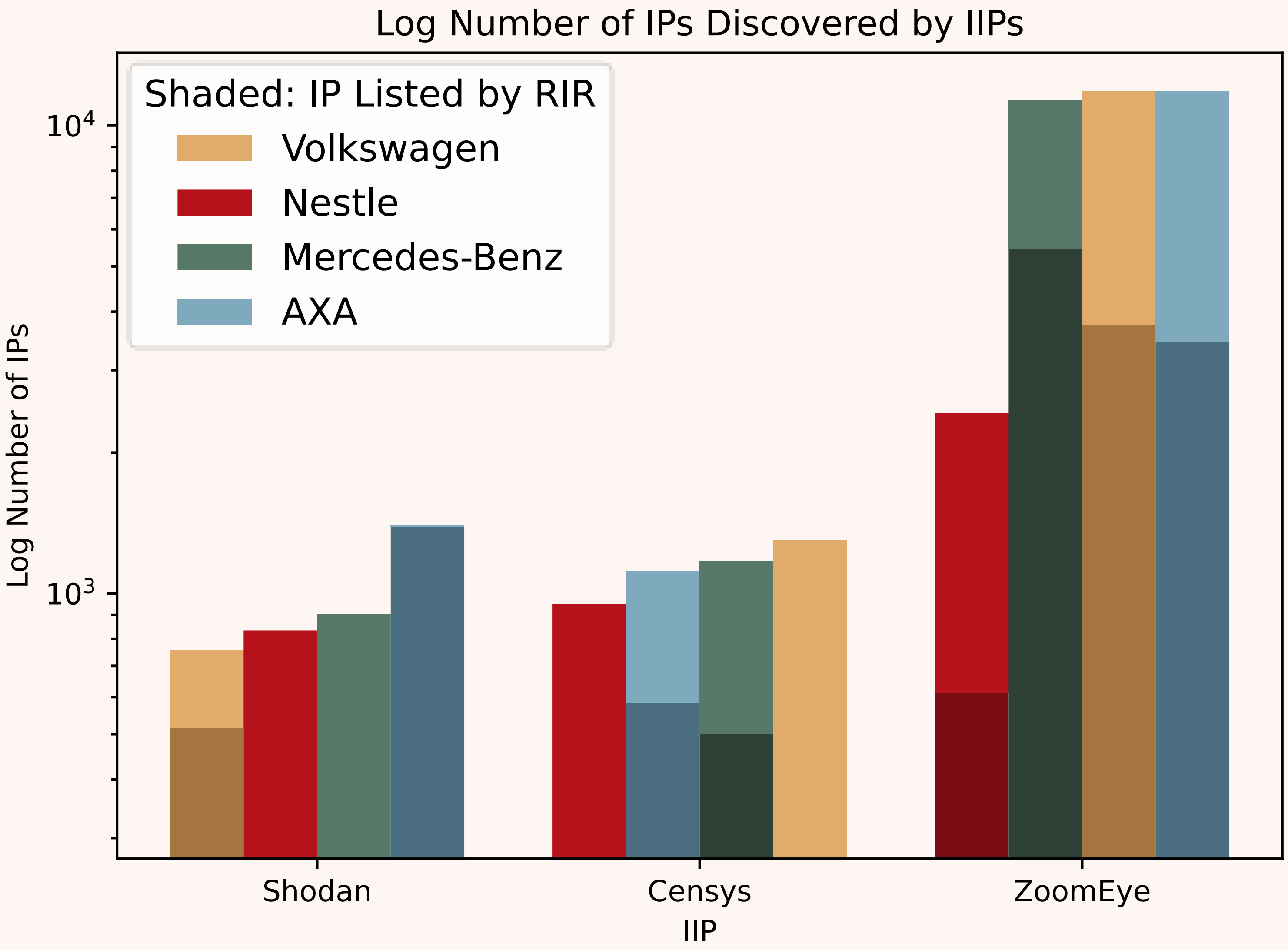
Measuring The Discrepancy

- How significant are these discrepancies?
- Generated an attack surface using each platform
- To account for externally hosted assets, we can use TLS certificates and Domain Names
- Four organisations from the EU500 used in previous research [1]

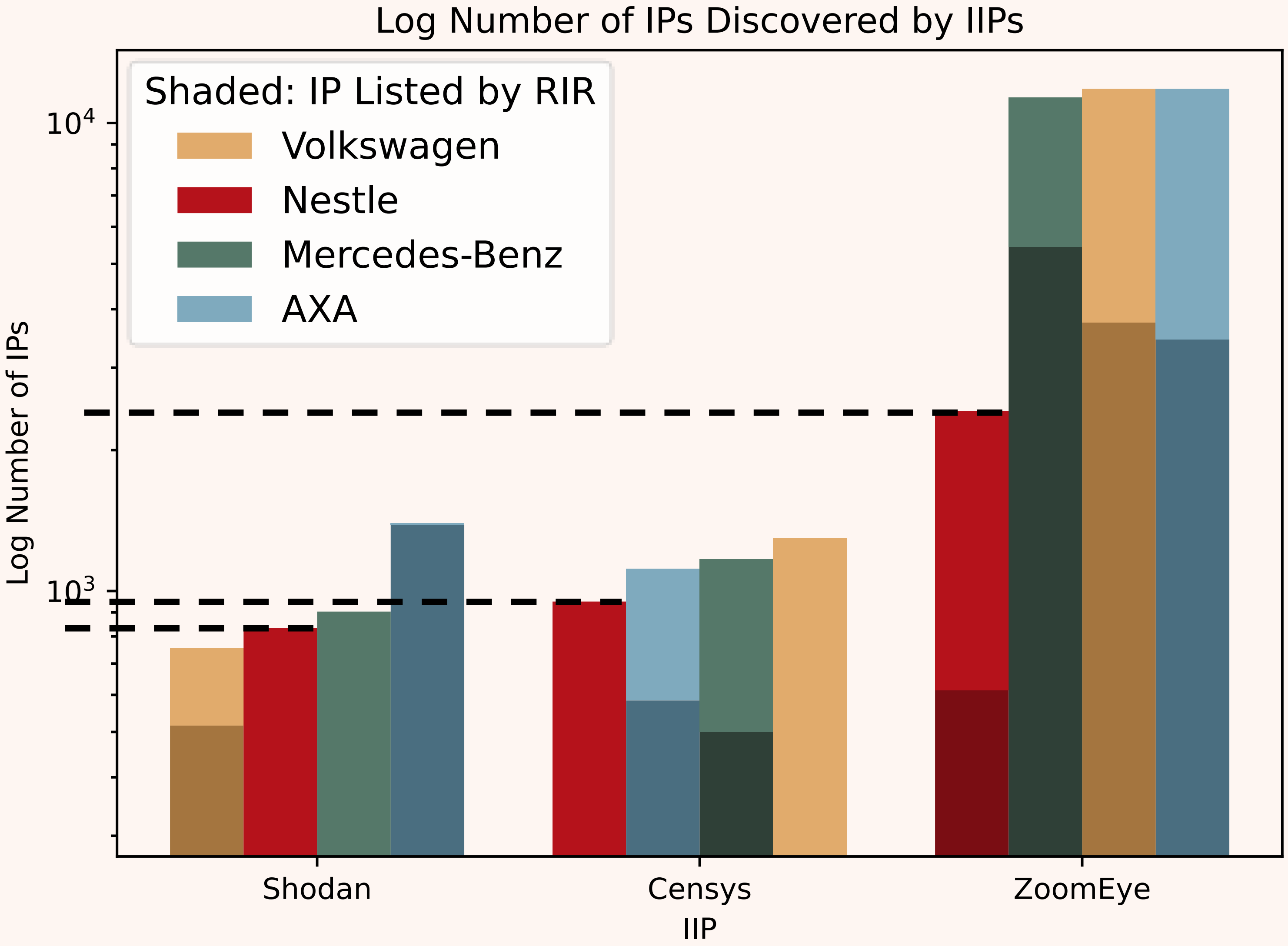

Search Platform For WhoIS Assets
01
Search Platform For SSL/TLS Certificates
02
Discovering An Organisation's Attack Surface
03
Search Platform For Domain Names
04
Search RIPE For Organisation

[1] N. Gelernter, H. Schulmann, and M. Waidner, 'External Attack-Surface of Modern Organizations, doi: 10.1145/3634737.3656295.

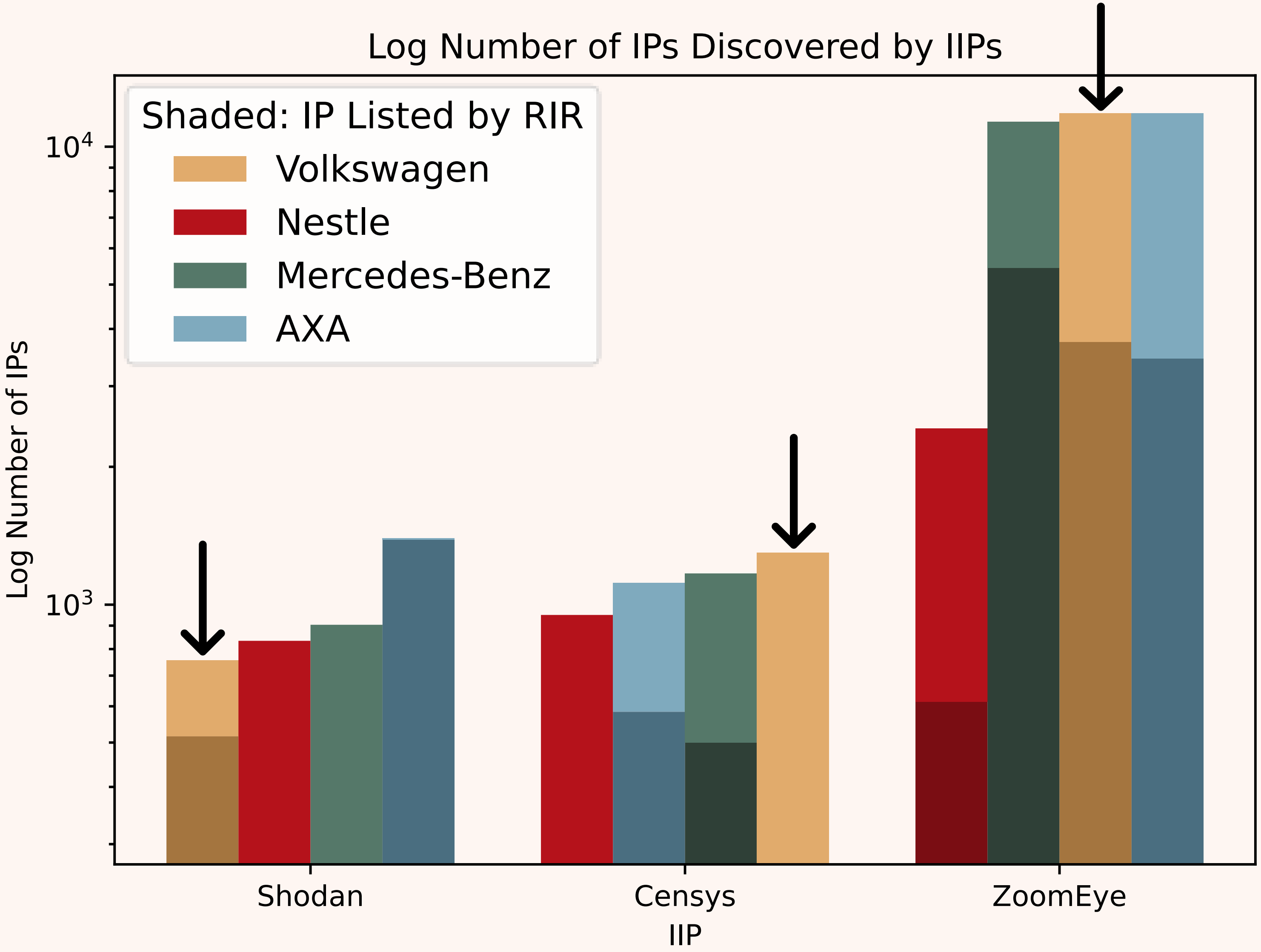
No Platform Agrees



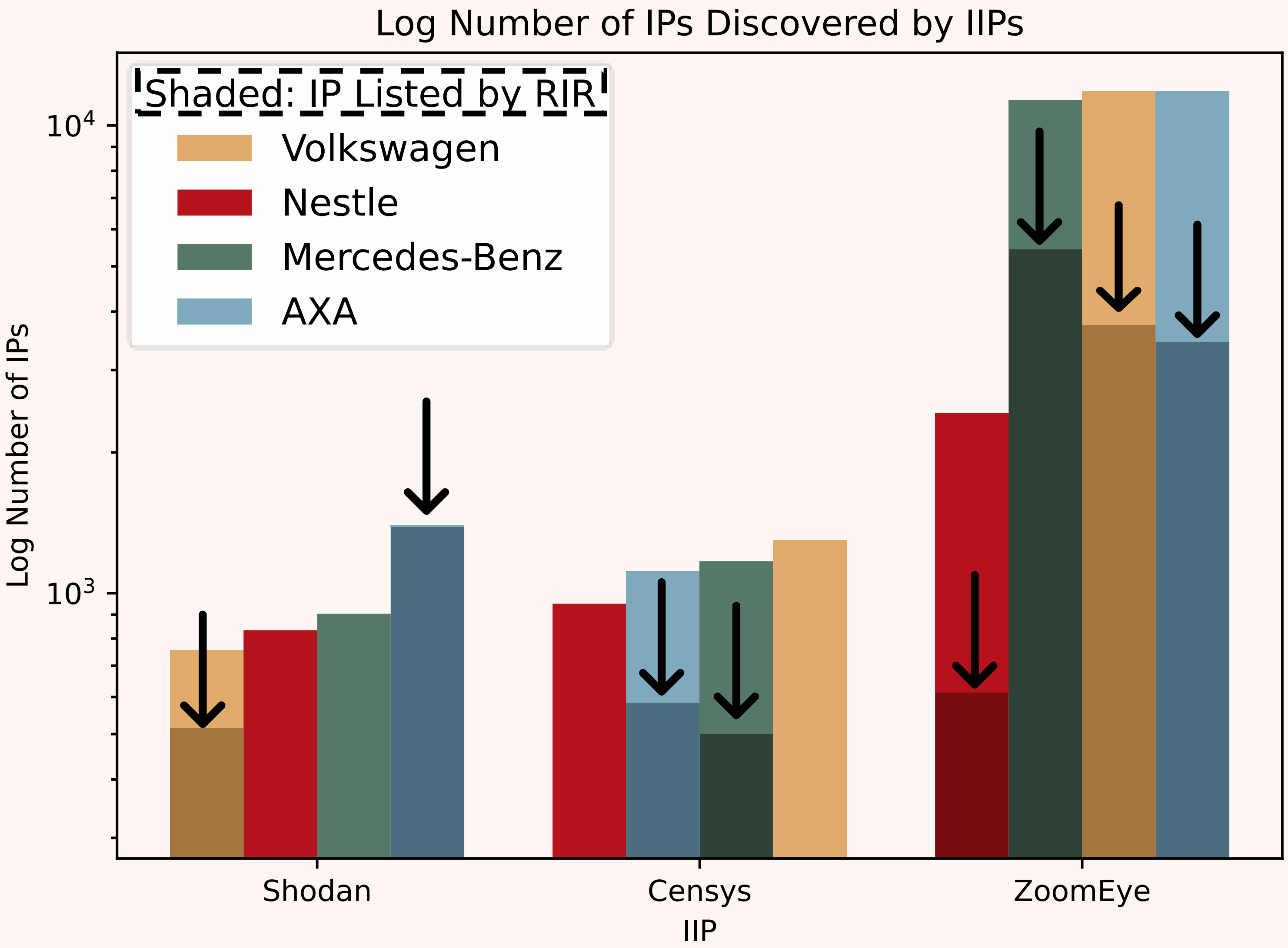
No Platform Agrees



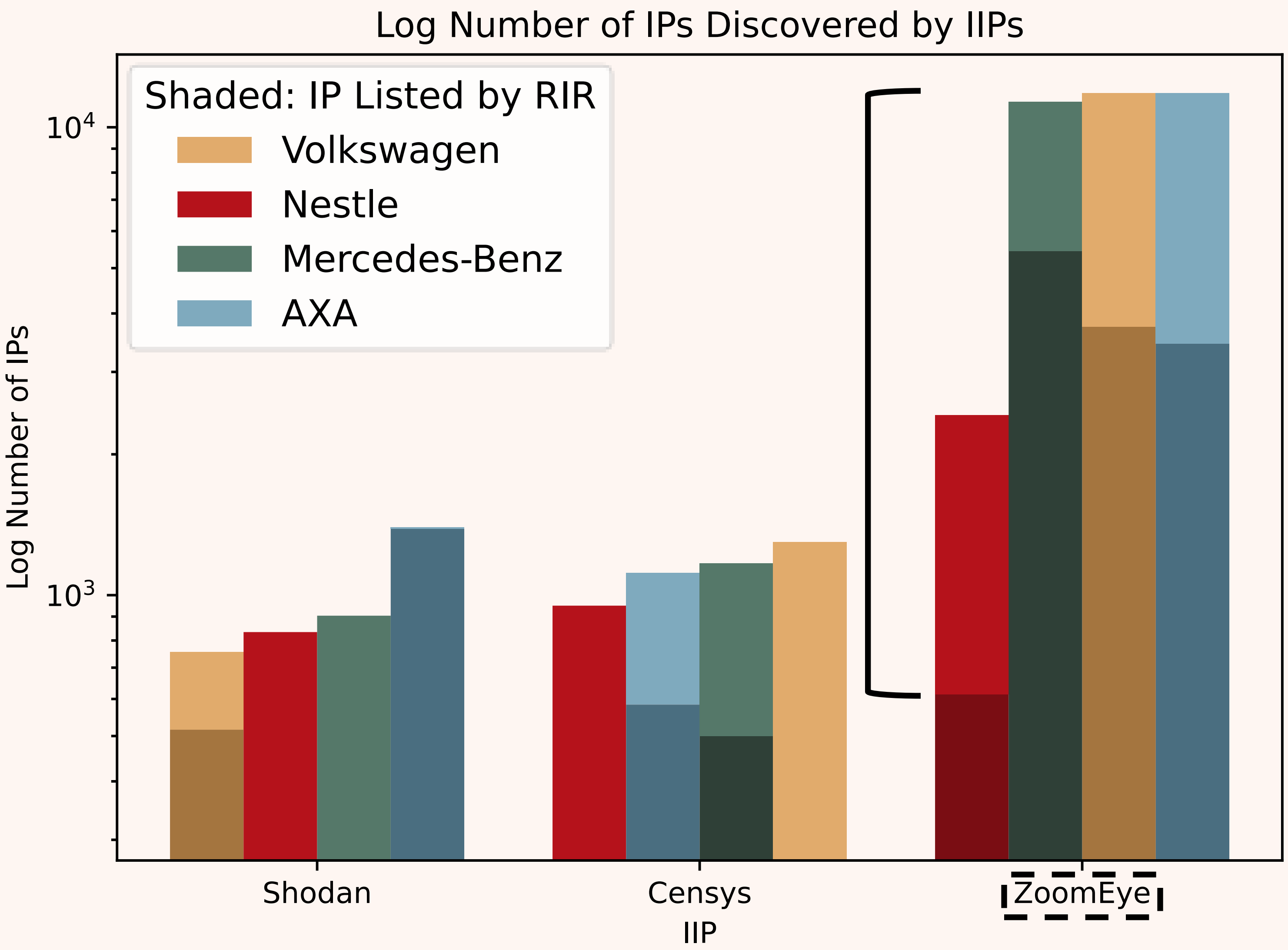
No Platform Agrees



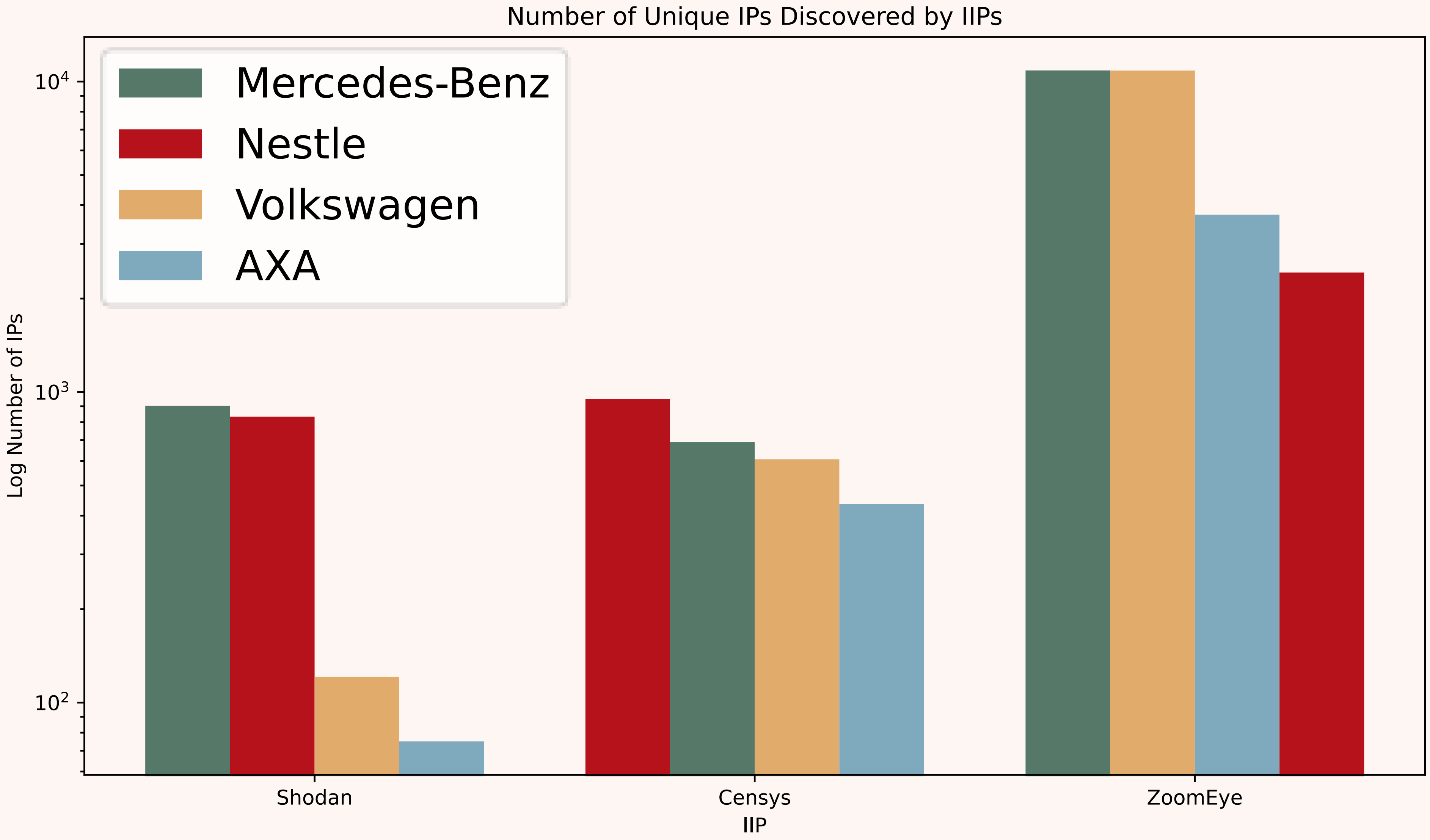
No Platform Agrees



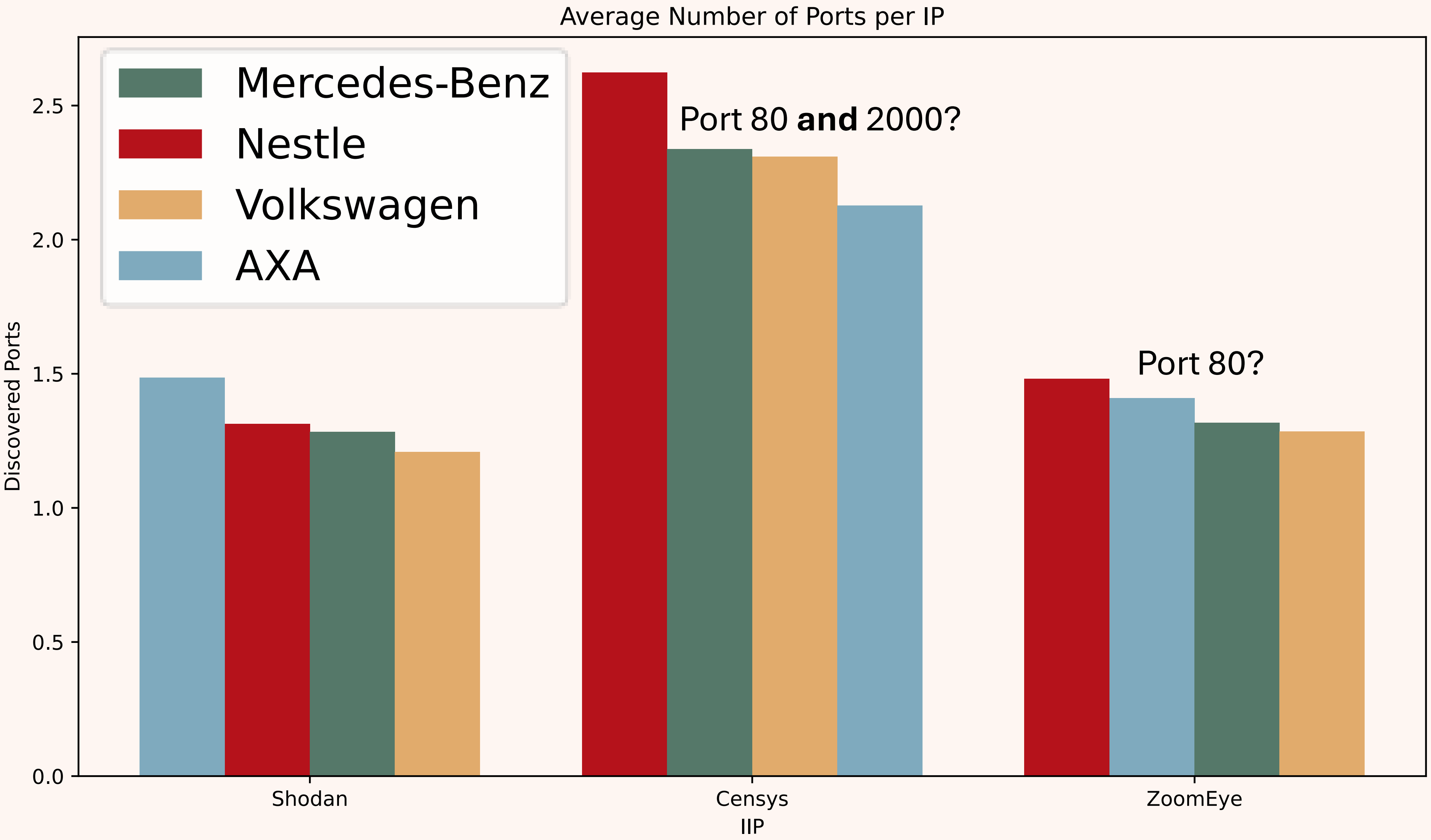
No Platform Agrees



Each Platform Has Unique Discoveries



No Platform Is Superior



Key Findings

- Depending on the platform, you will get different attack surfaces
- Platform disagree on which organisation has the biggest surface
- Using only RIRs is insufficient to create modern attack surfaces
- Omitting a single platform leads to an incomplete attack surface
- Are the results actual valid, or are they filled with bloat
- No indication of which is best, Censys discovers more ports but disagrees on attack surface size

Conclusion

- How can you know which, or how many, platforms to use?
- Multiple can be costly, especially for large-scale surfaces
- Reliance on a single platform leads to customers being misinformed about the true risk faced
- These attack surfaces are used to find vulnerabilities
- What is the ground truth? How can we be confidence in the results from the platforms?
- This is what my PhD will focus on!
- If you would like to know more, there is a SIGCOMM poster

Questions?