DENIM GROUP

Building a world where technology is trusted.

Enumerating Enterprise Attack Surface

Dan Cornell | CTO

Dan Cornell

- Founder and CTO of Denim Group
- Software developer by background
- OWASP San Antonio co-leader
- 20 years experience in software architecture, development, and security

DENIM GROUP

Building a world where technology is trusted

Denim Group is solely focused on helping build resilient software that will withstand attacks.

- Since 2001, helping secure software
- Development background
- Tools + services model

How we can help:

Advisory Services

Assessment Services

Remediation Services

ThreadFix
Powered by Denim Group
Vulnerability Resolution Platform

So You Want To Roll Out a Software Security Program?

- Great!

- What a software security program ISN'T
  - Question: "What are you doing to address software security concerns?"
  - Answer: "We bought scanner XYZ"

- What a software security program IS
  - People, process, tools (naturally)
  - Set of activities intended to repeatedly produce appropriately-secure software

Challenges Rolling Out Software Security Programs

- Resources
  - Raw budget and cost issues
  - Level of effort issues

- Resistance: requires organizational change
  - Apparently people hate this

- Open source tools
  - Can help with raw budget issues
  - May exacerbate problems with level of effort

- View the rollout as a multi-stage process
  - Not one magical effort
  - Use short-term successes and gains to fuel further change

You can’t defend unknown attack surface

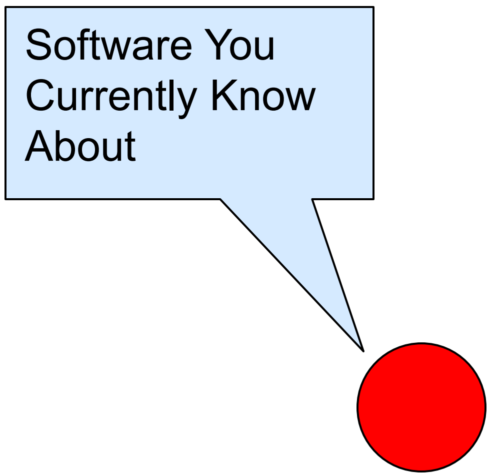
If everything is important then nothing is important

[Translation]

Find out what applications you have in your organization

Decide the relative importance of applications and treat them differently based on this

What Is Your Software Attack Surface?

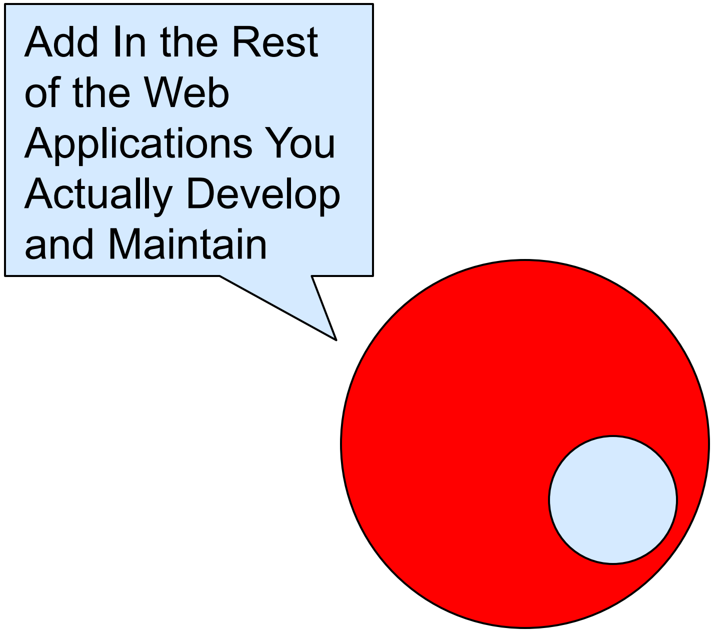


Software You Currently Know About

What?
- Critical legacy systems
- Notable web applications

Why?
- Lots of value flows through it
- Auditors hassle you about it
- Formal SLAs with customers mention it
- Bad guys found it and caused an incident (oops)

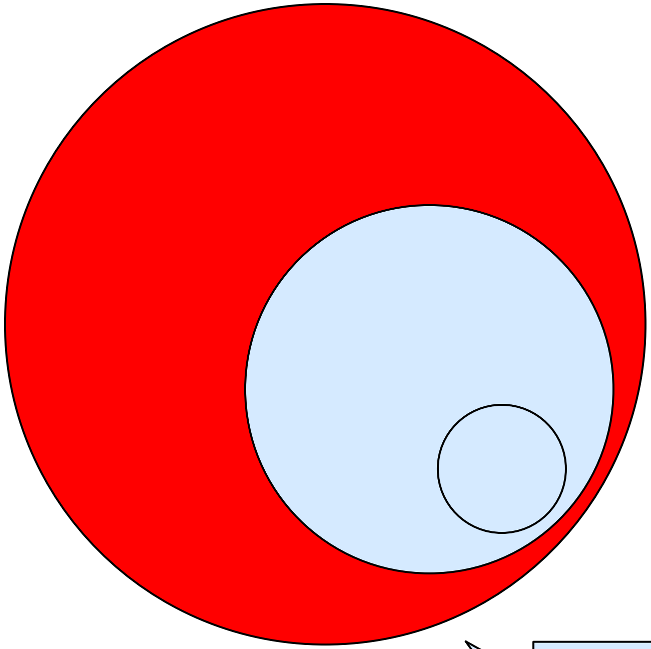
What Is Your Software Attack Surface?


Add In the Rest of the Web Applications You Actually Develop and Maintain

What?
- Line of business applications
- Event-specific applications

Why Did You Miss Them?
- Forgot it was there
- Line of business procured through non-standard channels
- Picked it up through a merger / acquisition

What Is Your Software Attack Surface?



Add In the Software You Bought from Somewhere

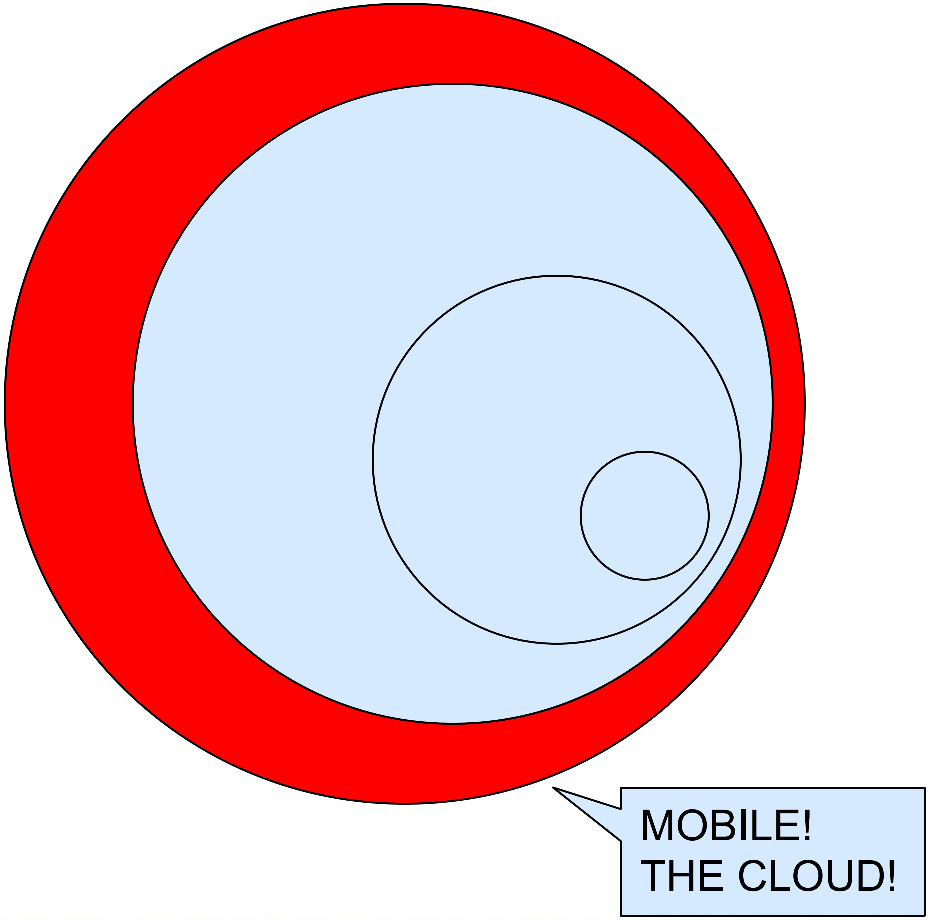
What?

- More line of business applications
- Support applications
- Infrastructure applications

Why Did You Miss Them?

- Most scanner only really work on web applications so no vendors pester you about your non-web applications
- Assume the application vendor is handling security

What Is Your Software Attack Surface?



MOBILE!
THE CLOUD!

What?

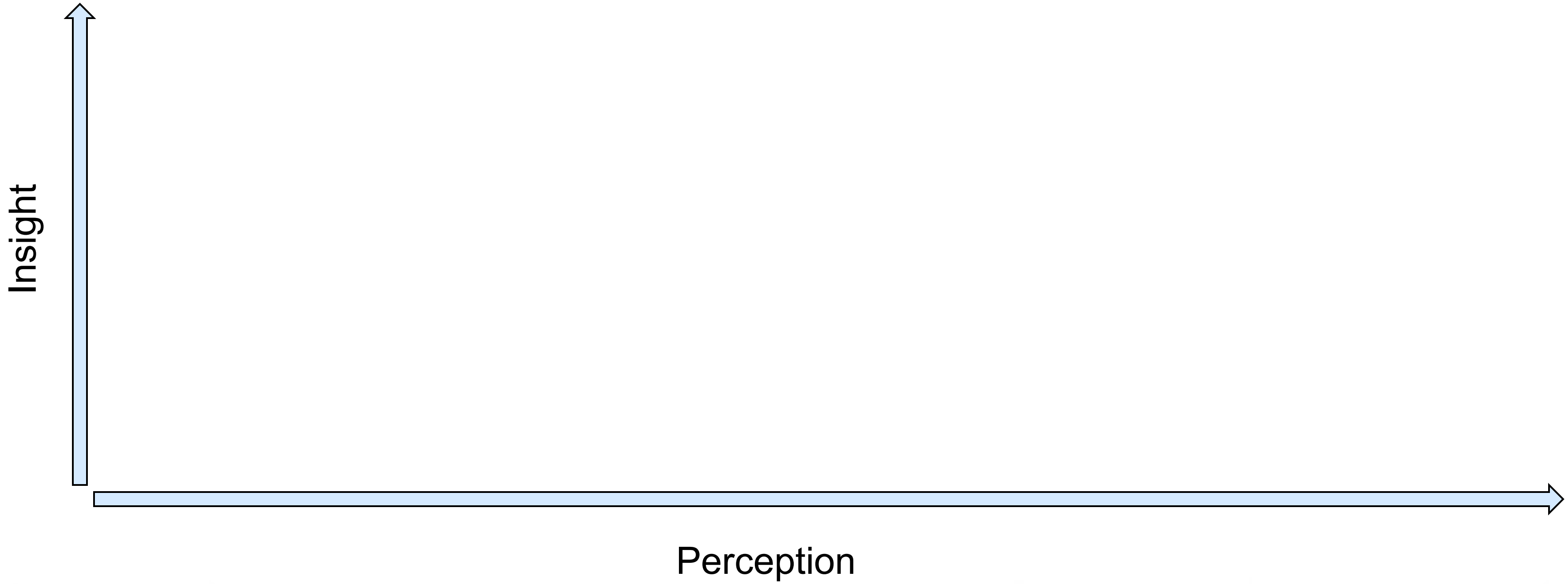
- Support for line of business functions
- Marketing and promotion

Why Did You Miss Them?

- Any jerk with a credit card and the ability to submit an expense report is now runs their own private procurement office

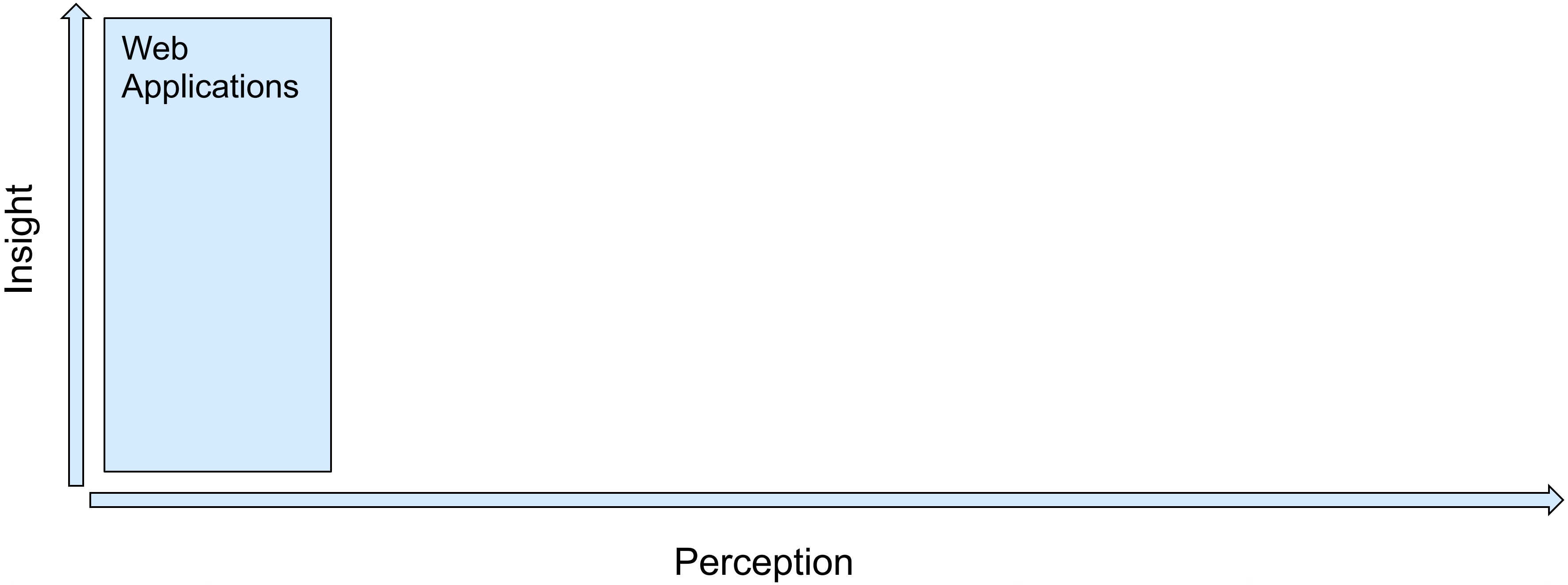
Attack Surface: The Security Officer's Journey

- Two Dimensions:
  - Perception of Software Attack Surface
  - Insight into Exposed Assets



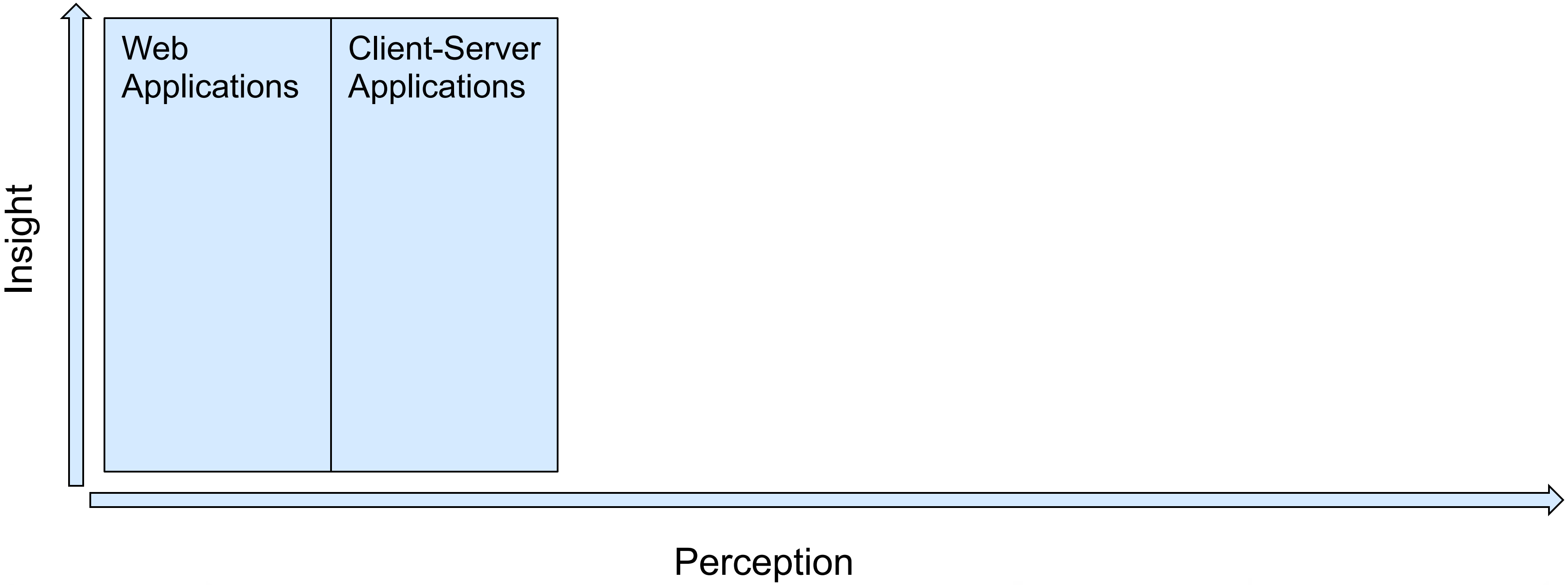
Attack Surface: The Security Officer's Journey

- As perception of the problem of attack surface widens the scope of the problem increases



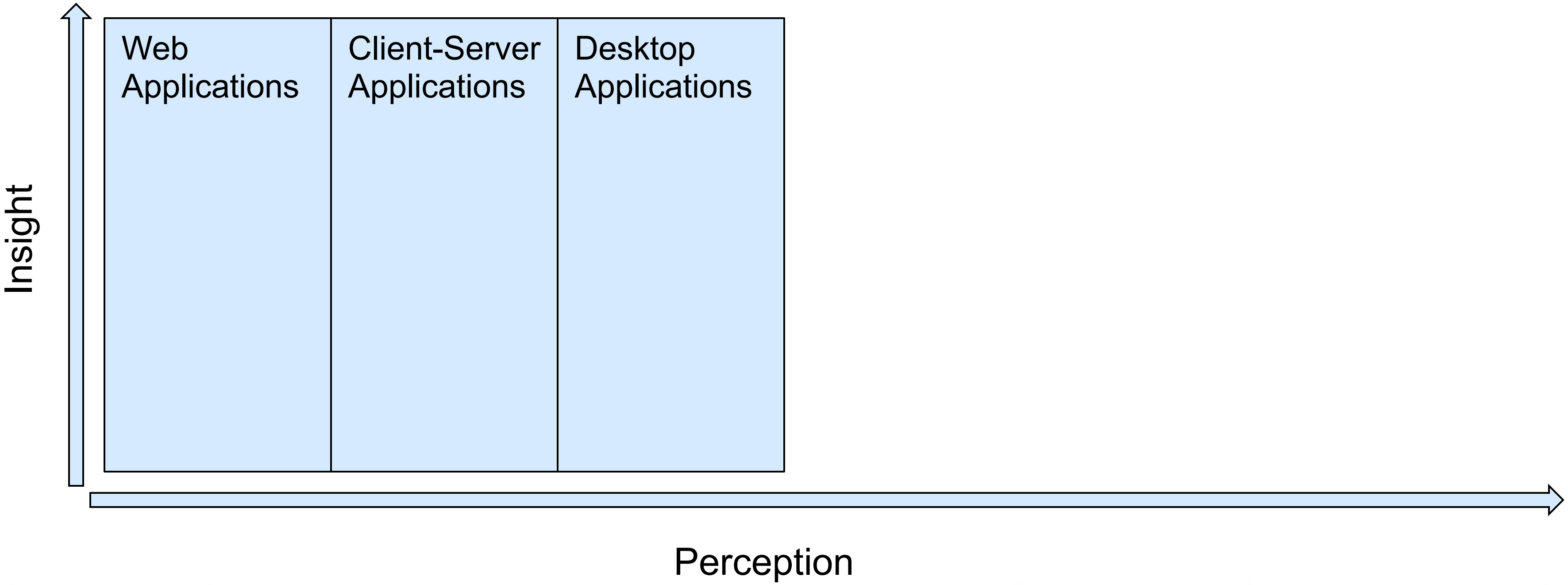
Attack Surface: The Security Officer's Journey

- As perception of the problem of attack surface widens the scope of the problem increases



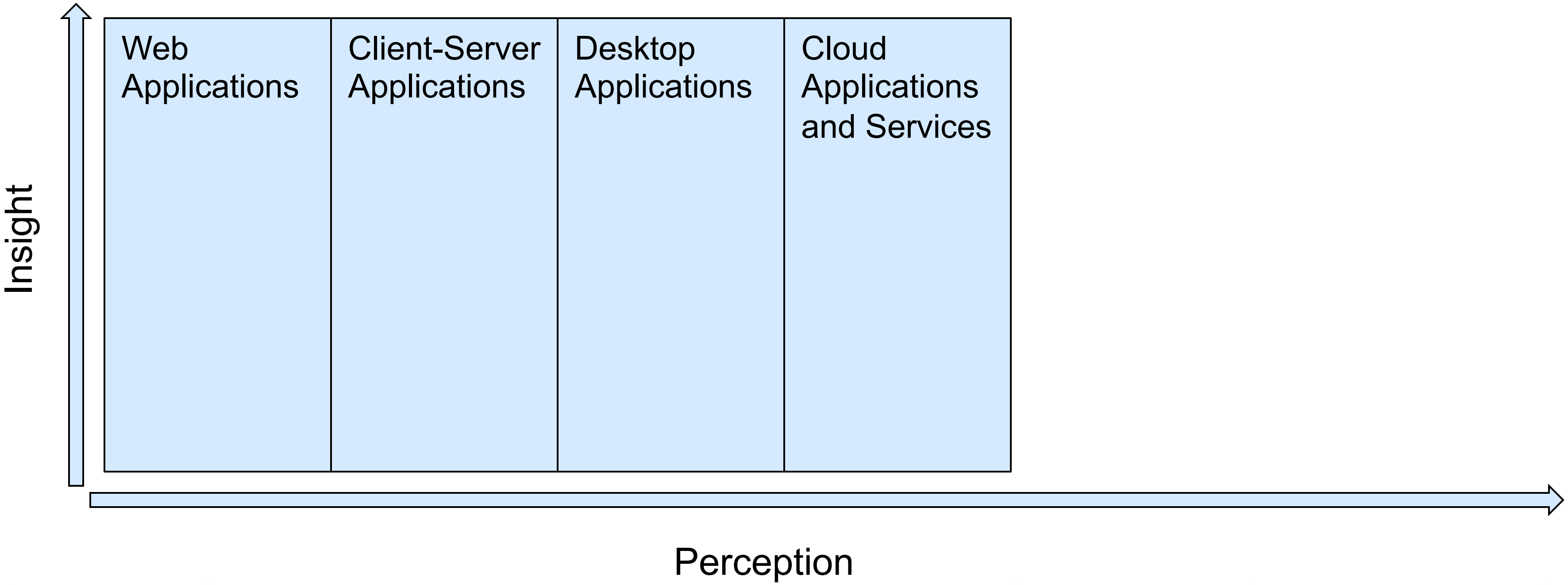
Attack Surface: The Security Officer's Journey

- As perception of the problem of attack surface widens the scope of the problem increases



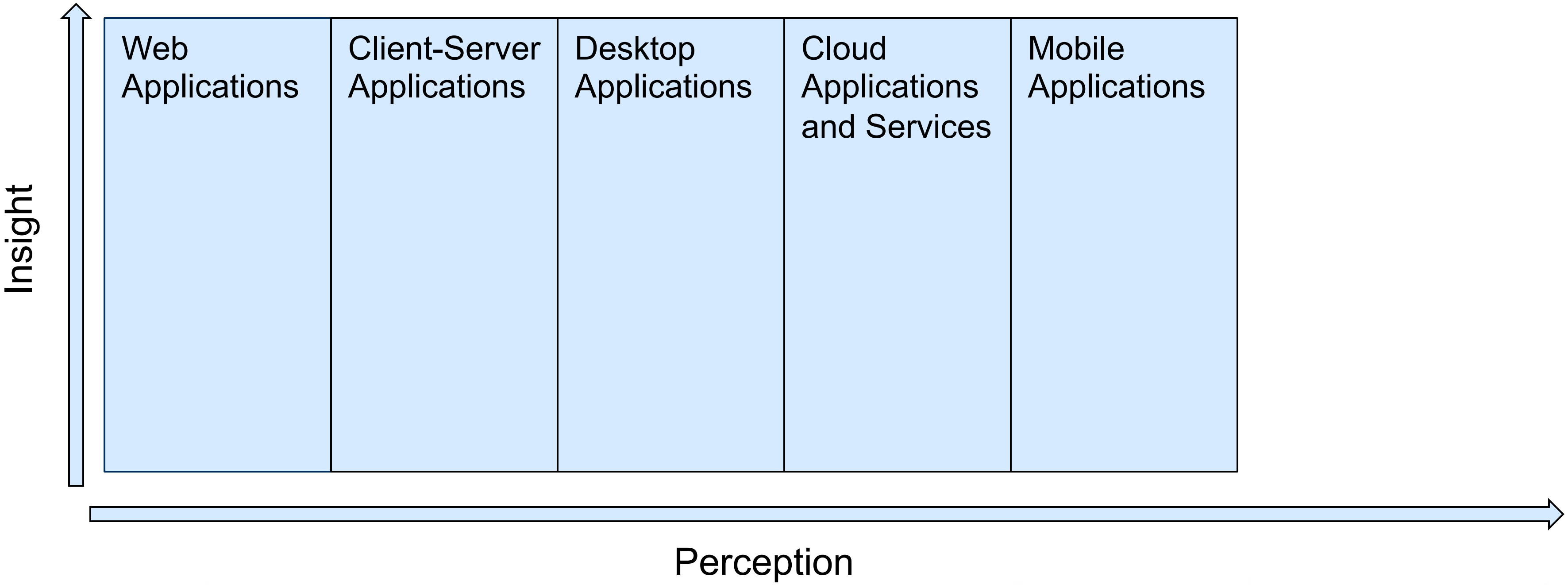
Attack Surface: The Security Officer's Journey

- As perception of the problem of attack surface widens the scope of the problem increases



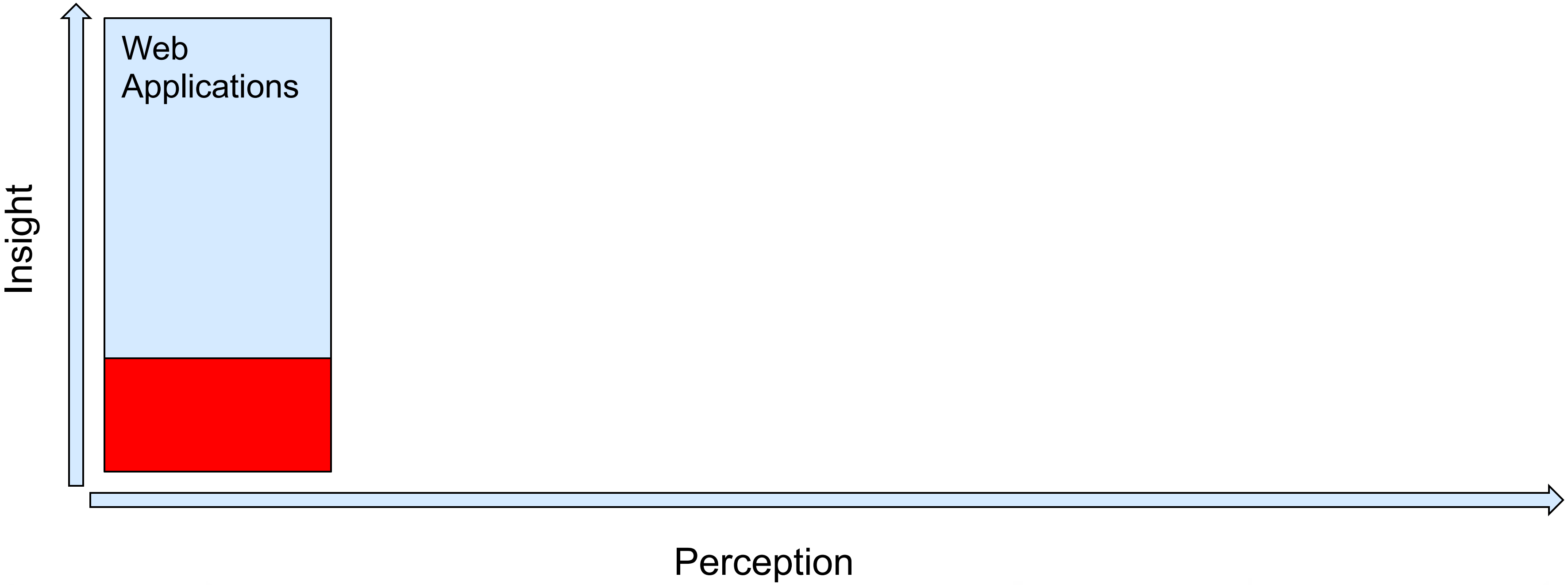
Attack Surface: The Security Officer's Journey

- As perception of the problem of attack surface widens the scope of the problem increases



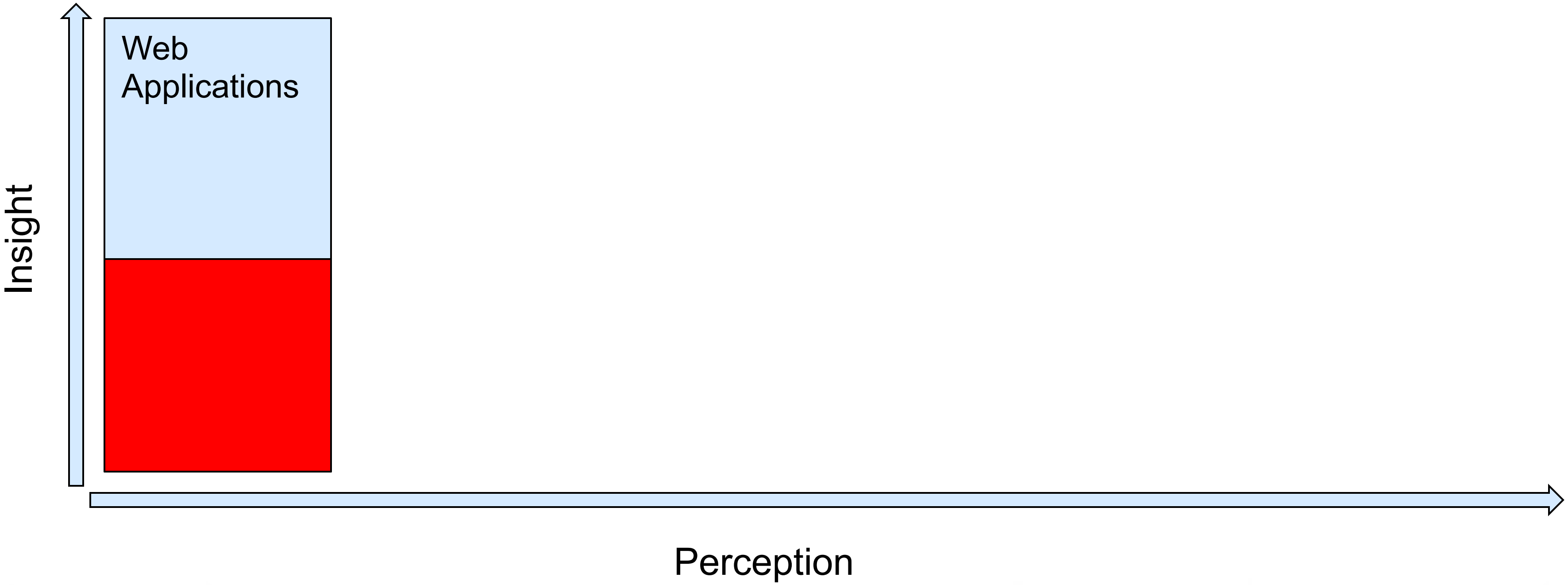
Attack Surface: The Security Officer's Journey

- Discovery activities increase insight



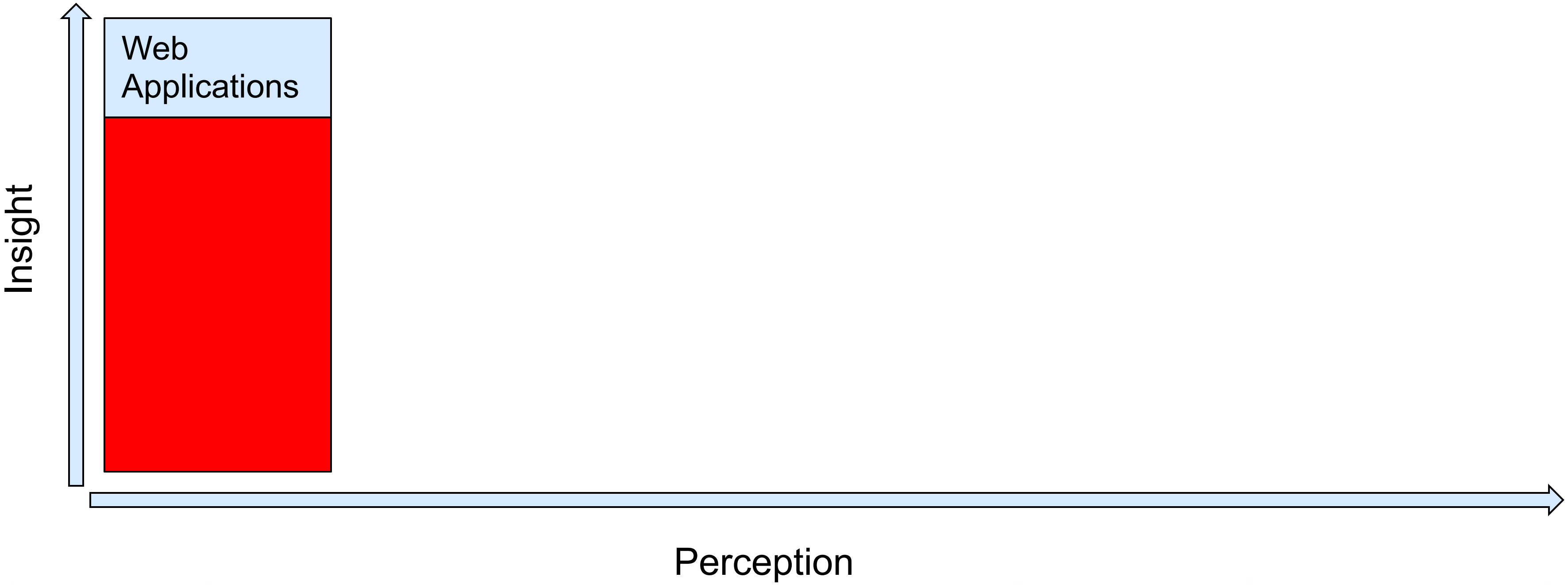
Attack Surface: The Security Officer's Journey

- Discovery activities increase insight



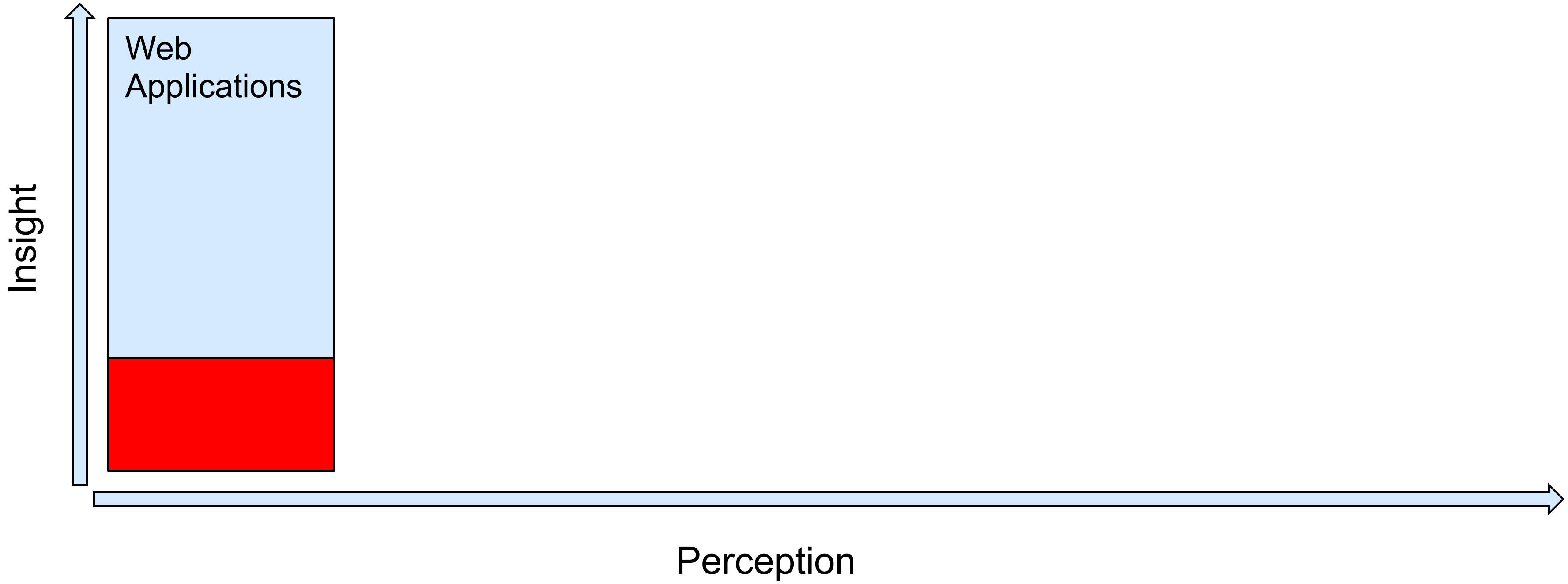
Attack Surface: The Security Officer's Journey

- Discovery activities increase insight



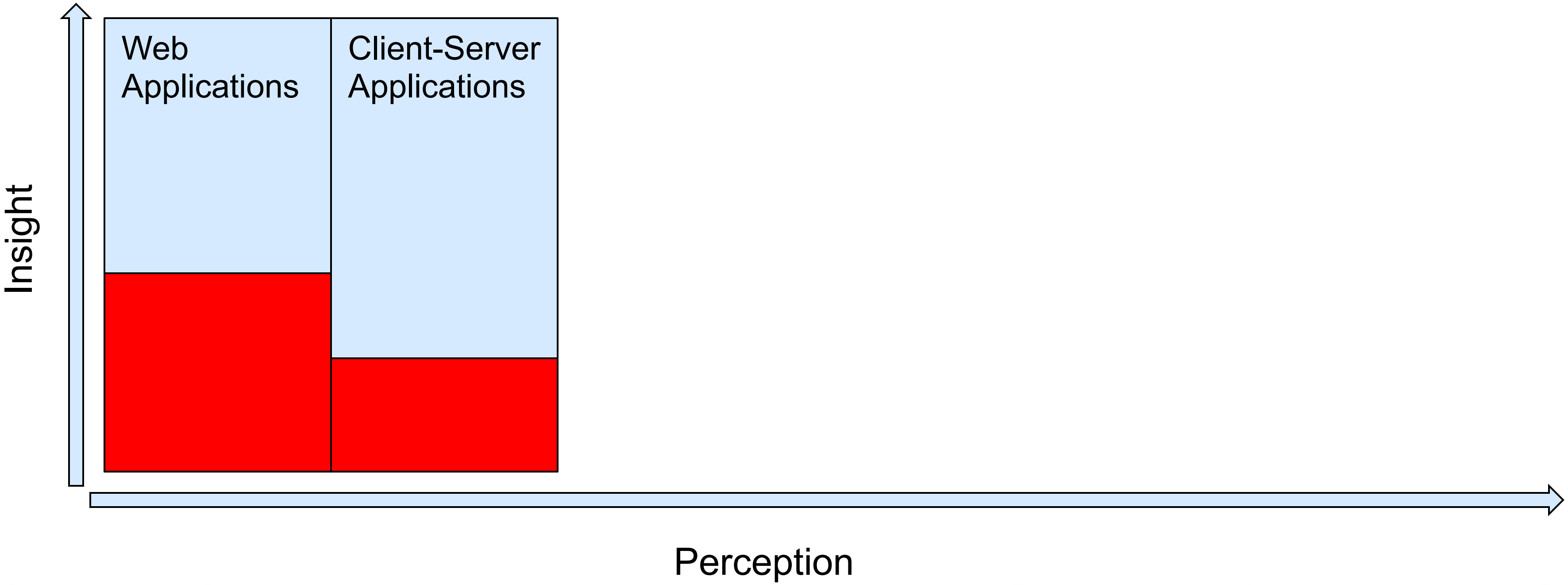
Attack Surface: The Security Officer's Journey

- Over time you end up with a progression



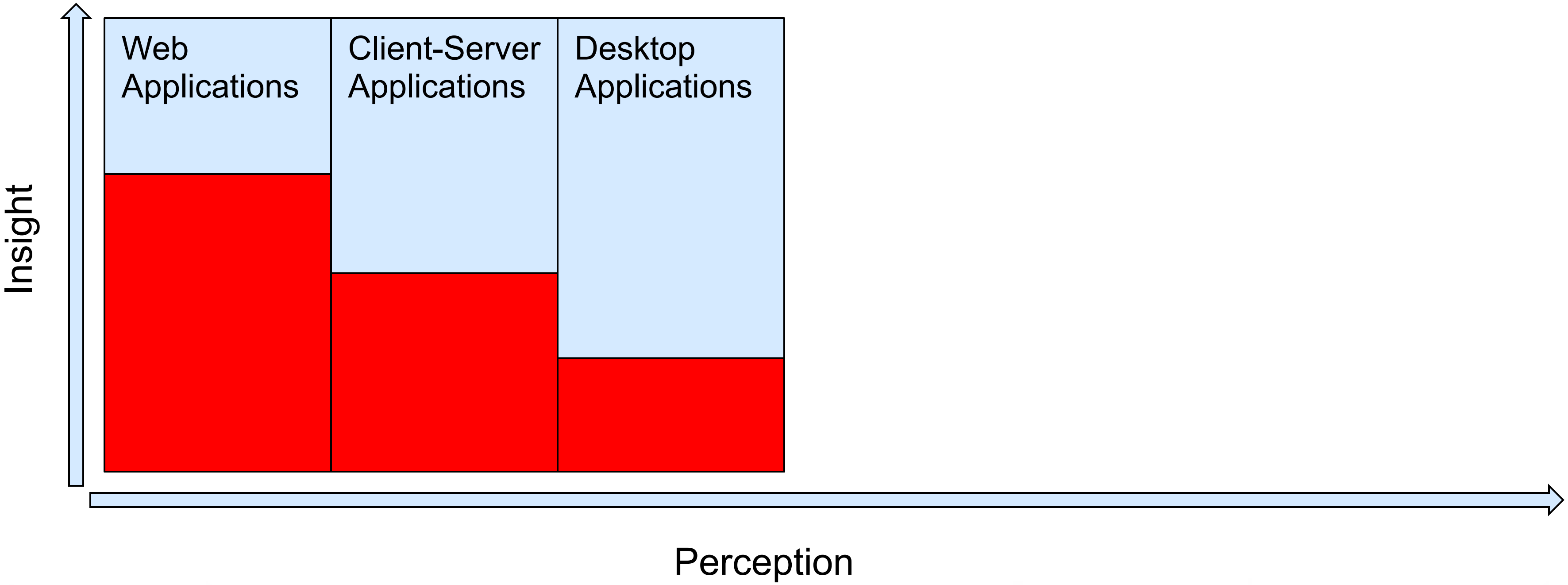
Attack Surface: The Security Officer's Journey

- Over time you end up with a progression



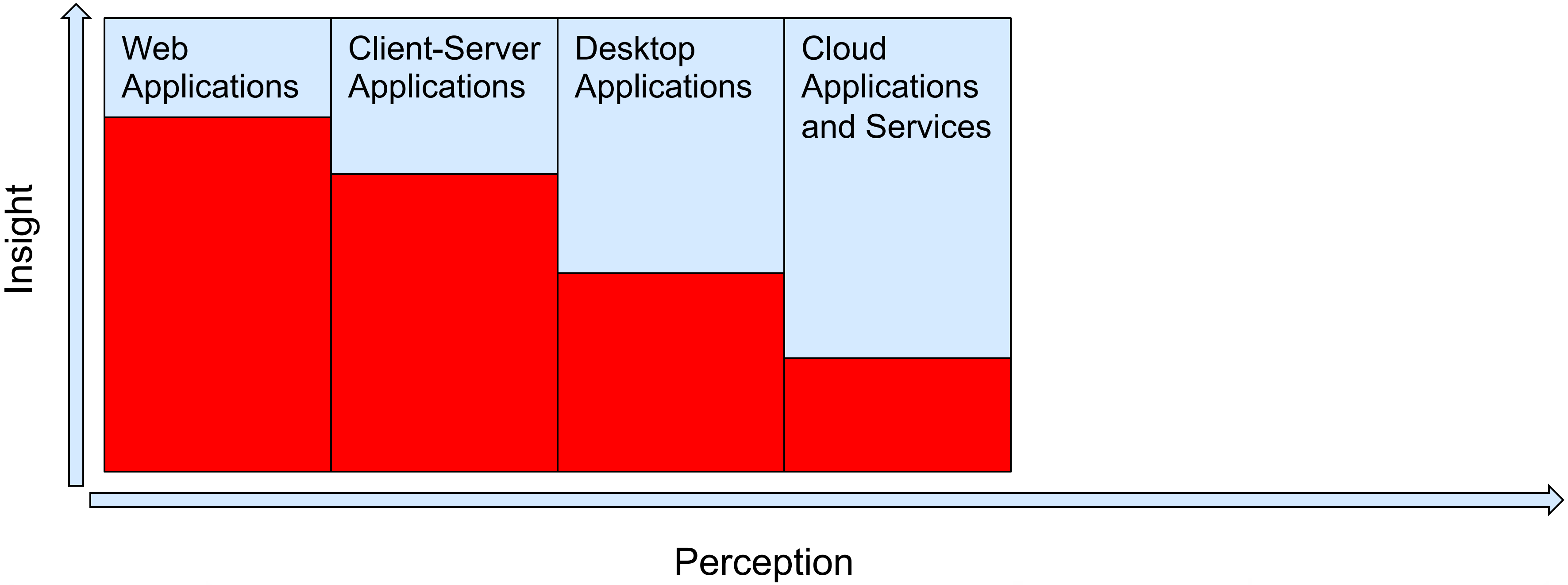
Attack Surface: The Security Officer's Journey

- Over time you end up with a progression



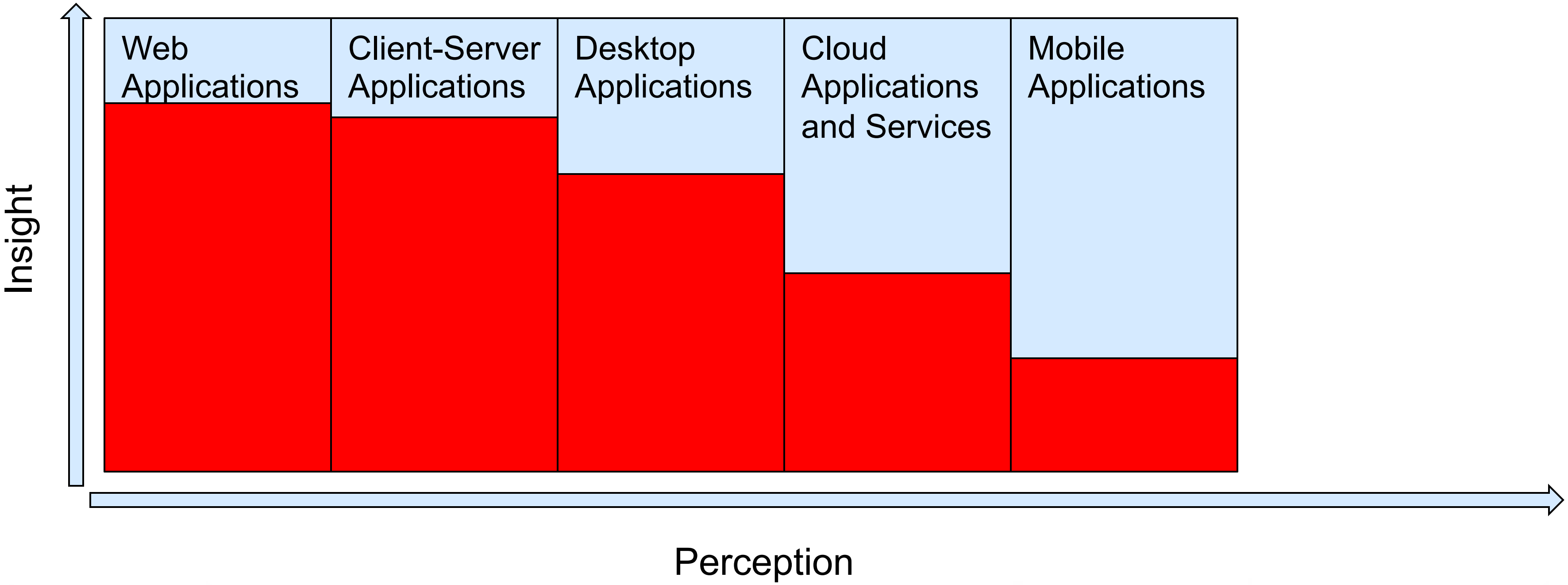
Attack Surface: The Security Officer's Journey

- Over time you end up with a progression



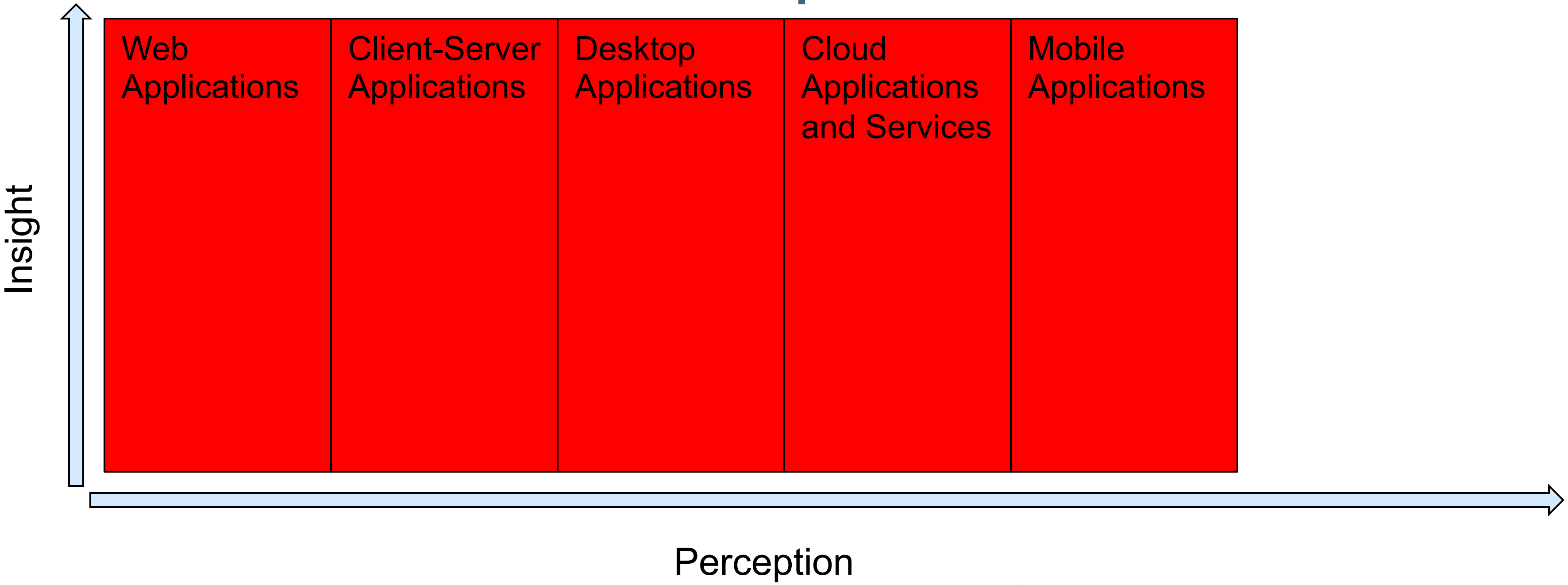
Attack Surface: The Security Officer's Journey

- Over time you end up with a progression



Attack Surface: The Security Officer's Journey

- When you reach this point it is called "enlightenment"
- You won't reach this point



Process

- Identify Application “Homes”
- Enumerate Applications
- Collect Metadata
- Repeat as Needed

So Where Are These Applications?

- Your Datacenters
- 3rd Party Datacenters
- Cloud Providers

Enumerating Applications

- Technical
  - Network inspection
  - DNS and other registry inspection
- Non-technical
  - Interviews
  - Other research

Network Inspection

- nmap: https://nmap.org/
- Look for common web server ports:
  - 80, 443, 8000, 8008, 8080, 8443
  - Others depending on your environment
  - nmap -sS -p 80,443,8000,8008,8080,8443 x.y.z.0/24
- Great for dense environments you control
  - Largely datacenters

https://www.denimgroup.com/resources/blog/2016/03/threadfix-in-action-discovering-your-organizations-software-attack-surface-web-app-edition/

DNS Inspection

- SubFinder: https://github.com/subfinder/subfinder
  - docker run -it subfinder -d target.org
- OWASP Amass: https://github.com/OWASP/Amass
  - sudo docker run amass --passive -d target.org
- DNSGrep: https://github.com/erbbysam/DNSGrep
  - https://blog.erbbysam.com/index.php/2019/02/09/dnsgrep/

IP Range Detection

- IPOsint: https://github.com/j3ssie/IPOsint

Mobile Application Identification

- Scumbler: https://github.com/Netflix-Skunkworks/Scumblr
  - Purpose of tool evolved over time
  - Not currently maintained – looking for maintainers

Interviews

- Line-of-business representatives
  - Will need to translate their definition of "application" to your definition
  - Think in terms of business processes and these can map to multiple applications and microservices
- Tech leads
  - More familiar with the deployed infrastructure and other assets

Other Research

- Disaster recover plans
- Accounting
  - Find cloud providers

Collect Metadata

- Technical: Language, Scale
- Architectural: Web, Mobile
- Exposure: Public, Partner, Internal
- Regulatory: PCI, HIPAA, GDPR

Value and Risk Are Not Equally Distributed

- Some Applications Matter More Than Others
  - Value and character of data being managed
  - Value of the transactions being processed
  - Cost of downtime and breaches
- Therefore All Applications Should Not Be Treated the Same
  - Allocate different levels of resources to assurance
  - Select different assurance activities
  - Also must often address compliance and regulatory requirements

Do Not Treat All Applications the Same

- Allocate Different Levels of Resources to Assurance
- Select Different Assurance Activities

- Also Must Often Address Compliance and Regulatory Requirements

Rinse and Repeat

- This list will change over time
- Metadata will change

- This is especially true in a world of microservices

You can’t defend unknown attack surface

If everything is important then nothing is important

[Translation]

Find out what applications you have in your organization

Decide the relative importance of applications and treat them differently based on this

Questions

SM

DENIM GROUP

Building a world where technology is trusted.

dan@denimgroup.com

@denimgroup

www.denimgroup.com