Do You Have a Scanner or a Scanning Program?

OWASP

The Open Web Application Security Project

About Me

OWASP
The Open Web Application Security Project

Dan Cornell
Founder and CTO of Denim Group
Software developer by background (Java, .NET, etc)
OWASP San Antonio
15 years experience in software architecture, development and security

Who Has Purchased an Automated Scanner?

OWASP
The Open Web Application Security Project

Static or Dynamic? (Or Both?)

Desktop, Enterprise or Cloud
(Or All the Above?)

Who Here Is Happy With Their Scanner?

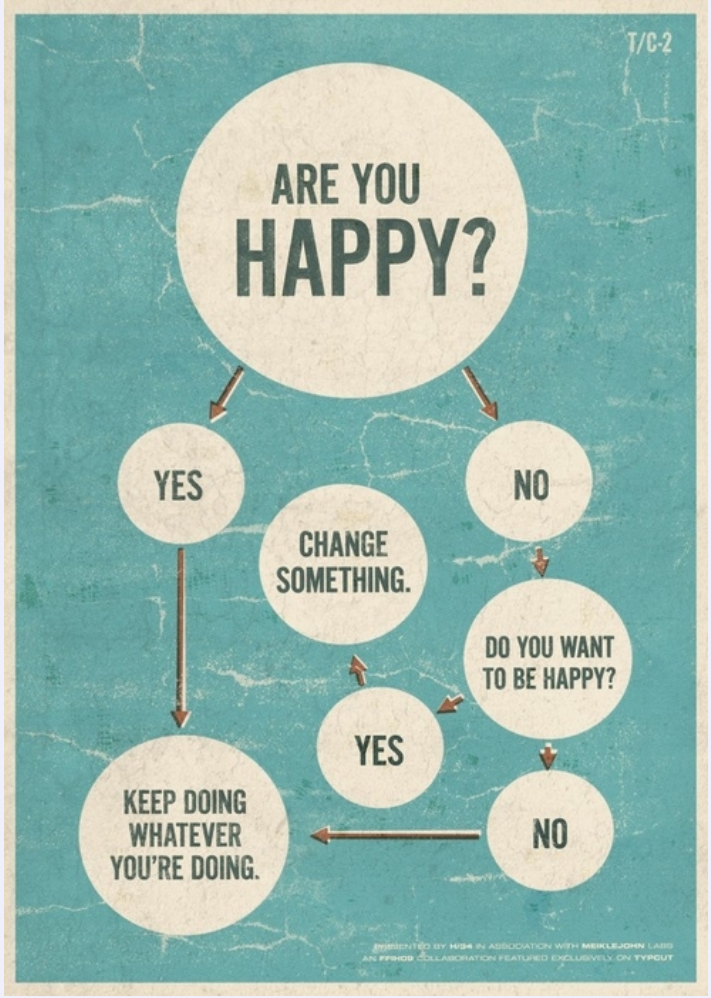
OWASP
The Open Web Application Security Project

Yes

No

Kind Of

Not Sure



OWASP
The Open Web Application Security Project

Why or Why Not?

Successful Software Security Programs

OWASP
The Open Web Application Security Project

Common Goal

Reduce Risk by…

- Reliably Creating Acceptably Secure Software

Obligatory “People, Process, Technology” Reference

Anybody got a good Sun Tzu quote?

I’d settle for a von Clausewitz…

Or perhaps we need to look at Dalai Lama quotes (topic for a different day)

Common Activities

Implementation must be tied to the specific organization

What Part Does Scanning Play?

OWASP
The Open Web Application Security Project

OpenSAMM - Automated scanning is part of both the “Security Testing” and “Code Review” Security Practices within the Verification Business Function

- Dynamic scanning and static scanning, respectively

Common starting point for many organizations embarking on software security programs

- There are lots of commercial and freely available products that can be used in support of this activity

RED FLAG:
Q: What are you doing for software security?
A: We bought [Vendor Scanner XYZ]

***** BEWARE FOSTERING A CHECKBOX CULTURE *****

Scanning Program: Anti-Patterns

OWASP
The Open Web Application Security Project

"Dude With a Scanner" approach
    Can also be implemented as the "lady with a scanner" approach

"SaaS and Forget" approach

Scanner Program Metrics

OWASP
The Open Web Application Security Project

Breadth

Depth

Frequency

Is Your Scanner Missing Something?

OWASP
The Open Web Application Security Project

Breadth “Misses”

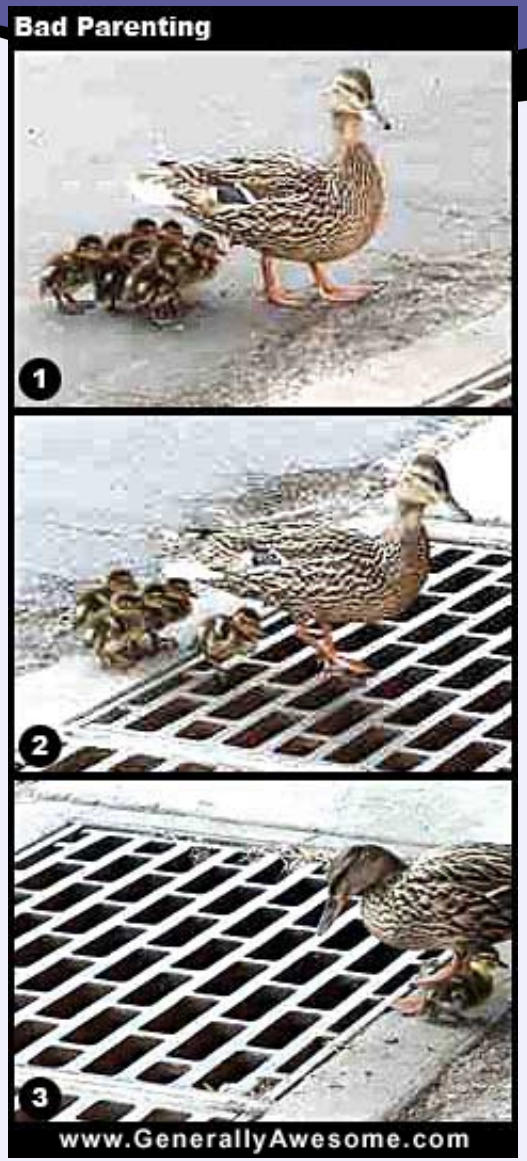
- Inadequate application portfolio
- Applications not being scanned

Depth “Misses”

- Ineffective crawling ignores application attack surface
- False negatives resulting in ignorance of legitimate vulnerabilities
- Excessive false positives causing results to be ignored

Frequency “Misses”

- Applications not being scanned often enough



Security Testing: Better Patterns

OWASP
The Open Web Application Security Project

Breadth-First Scanning
- You want a scanning program, not a scanner

Deep Assessment of Critical Applications
- Automated scanning, manual scan review and assessment

Understand that scanning is a means to an end
- Not an end in and of itself
- Start of vulnerability management

What Goes Into a Good Scanning Program?

OWASP
The Open Web Application Security Project

Solid Understanding of Attack Surface

Realistic Concept of Scanner Effectiveness

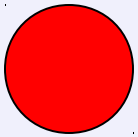
Disciplined History of Scanning

Prioritized Testing Efforts

What Is Your Software Attack Surface?

OWASP
The Open Web Application Security Project

Software You Currently Know About



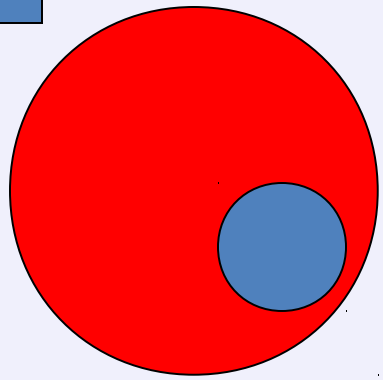
What?
- Critical legacy systems
- Notable web applications

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?

OWASP
The Open Web Application Security Project

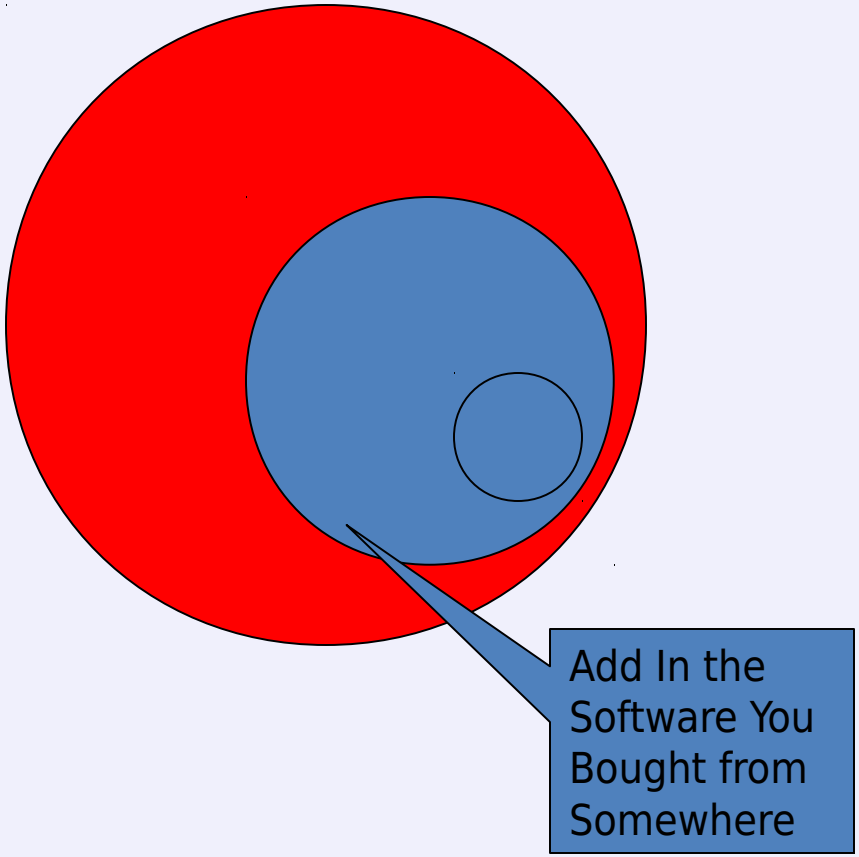
Add In the Rest of the Web Applications You Actually Develop and Maintain



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?

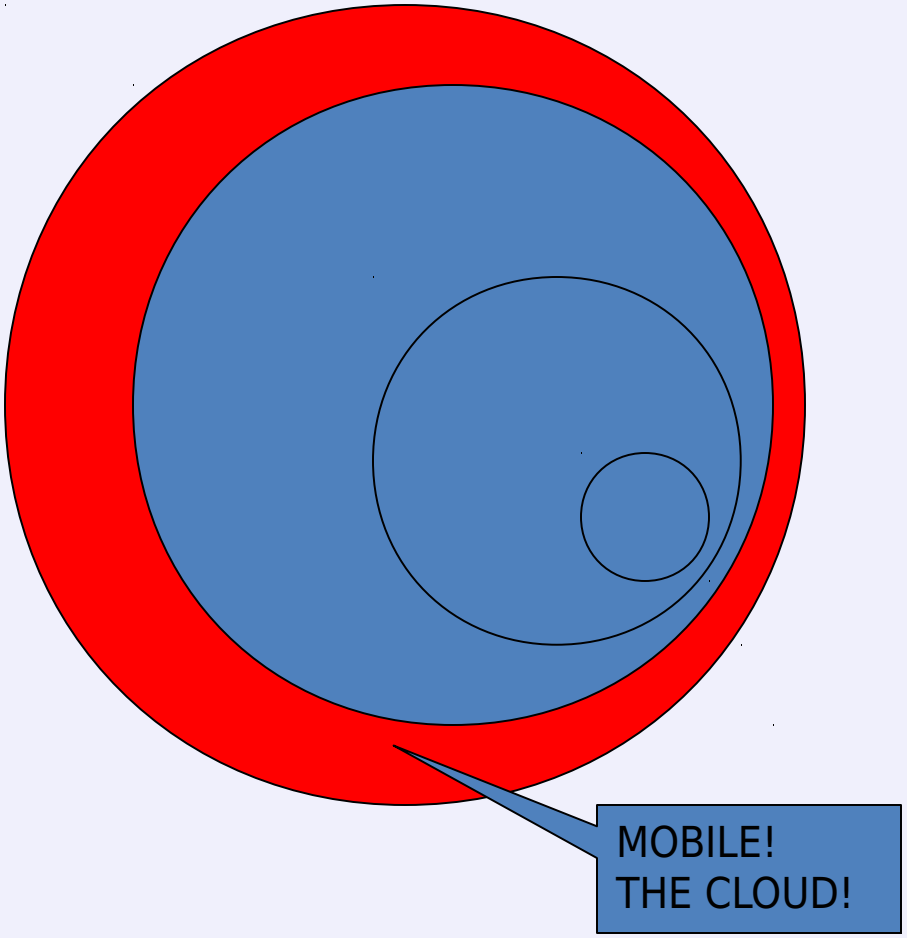


What?
- More line of business applications
- Support applications
- Infrastructure applications

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?

OWASP
The Open Web Application Security Project



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

OWASP
The Open Web Application Security Project

Two Dimensions:

Perception of Software Attack Surface

Insight into Exposed Assets

Attack Surface: The Security Officer's Journey

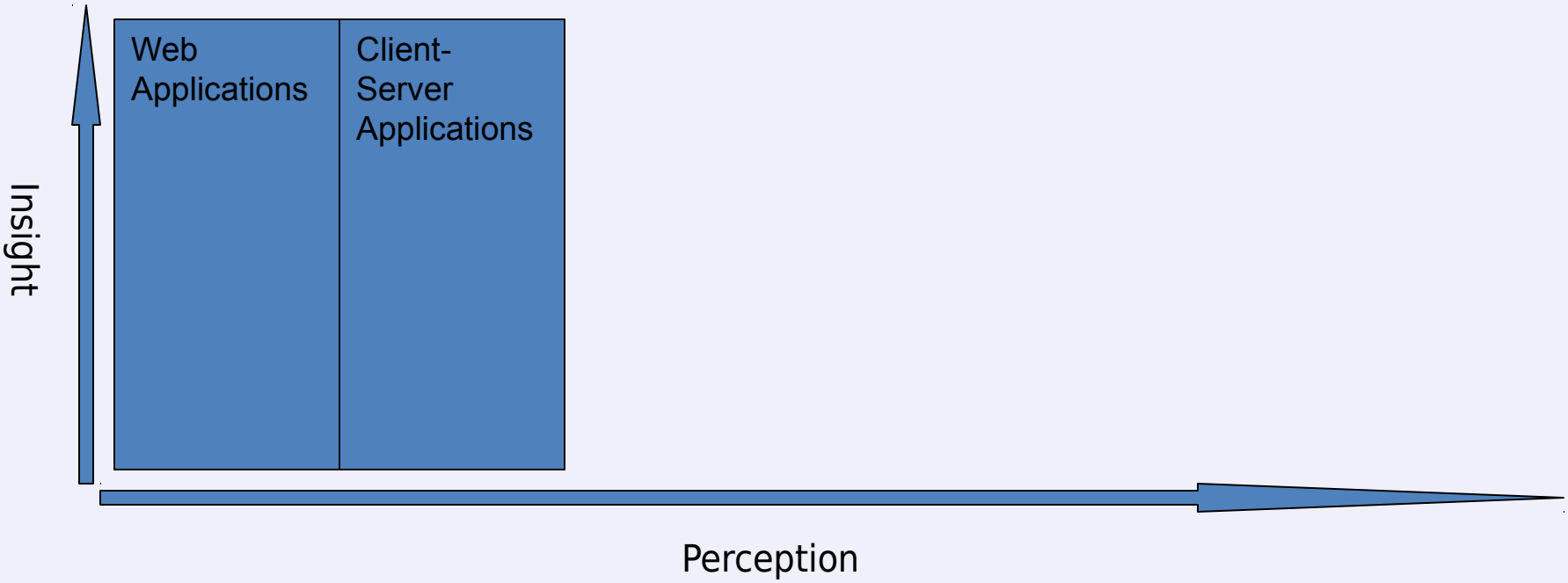
OWASP
The Open Web Application Security Project

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

Attack Surface: The Security Officer's Journey

OWASP
The Open Web Application Security Project

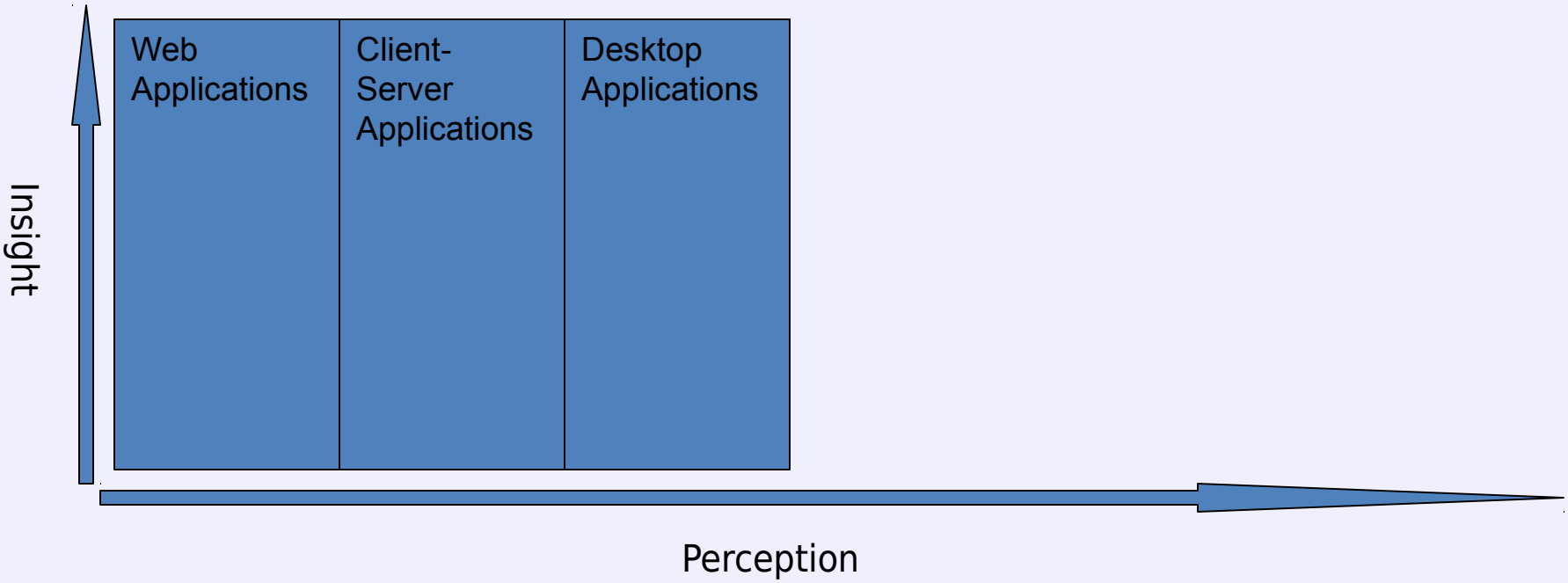
As perception of the problem of attack surface widens the scope of the problem increases



Attack Surface: The Security Officer's Journey

OWASP
The Open Web Application Security Project

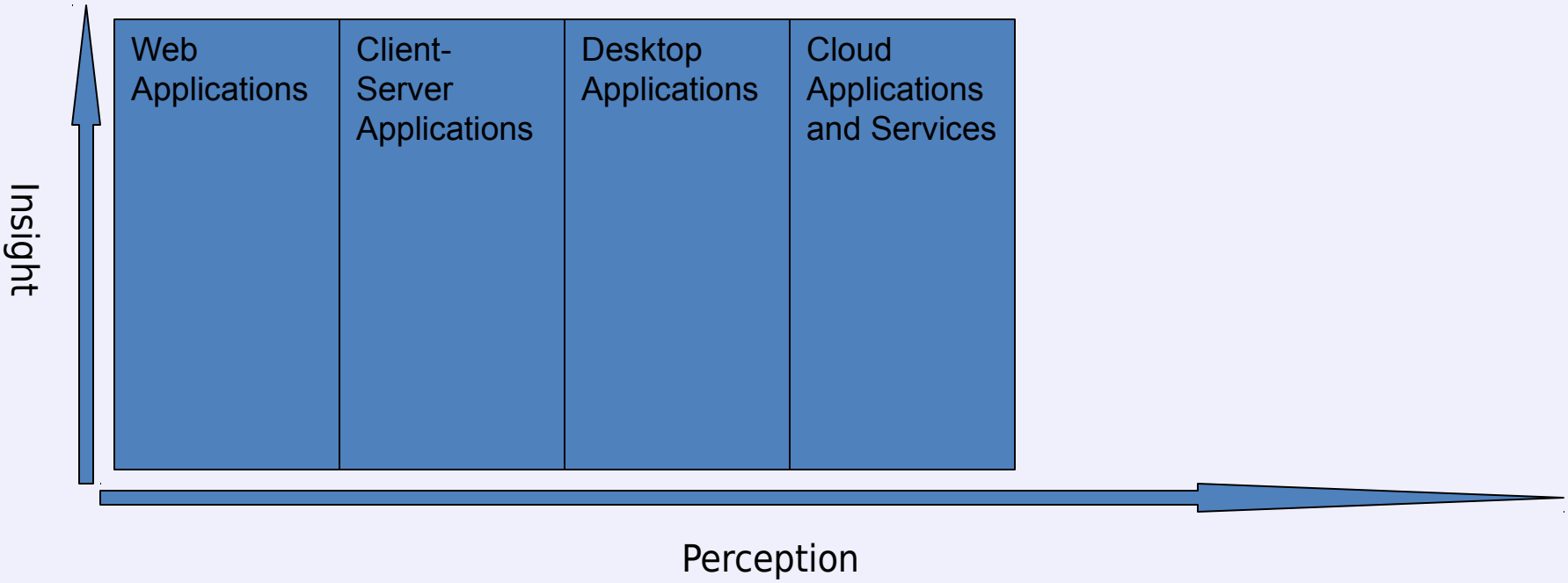
As perception of the problem of attack surface widens the scope of the problem increases



Attack Surface: The Security Officer's Journey

OWASP
The Open Web Application Security Project

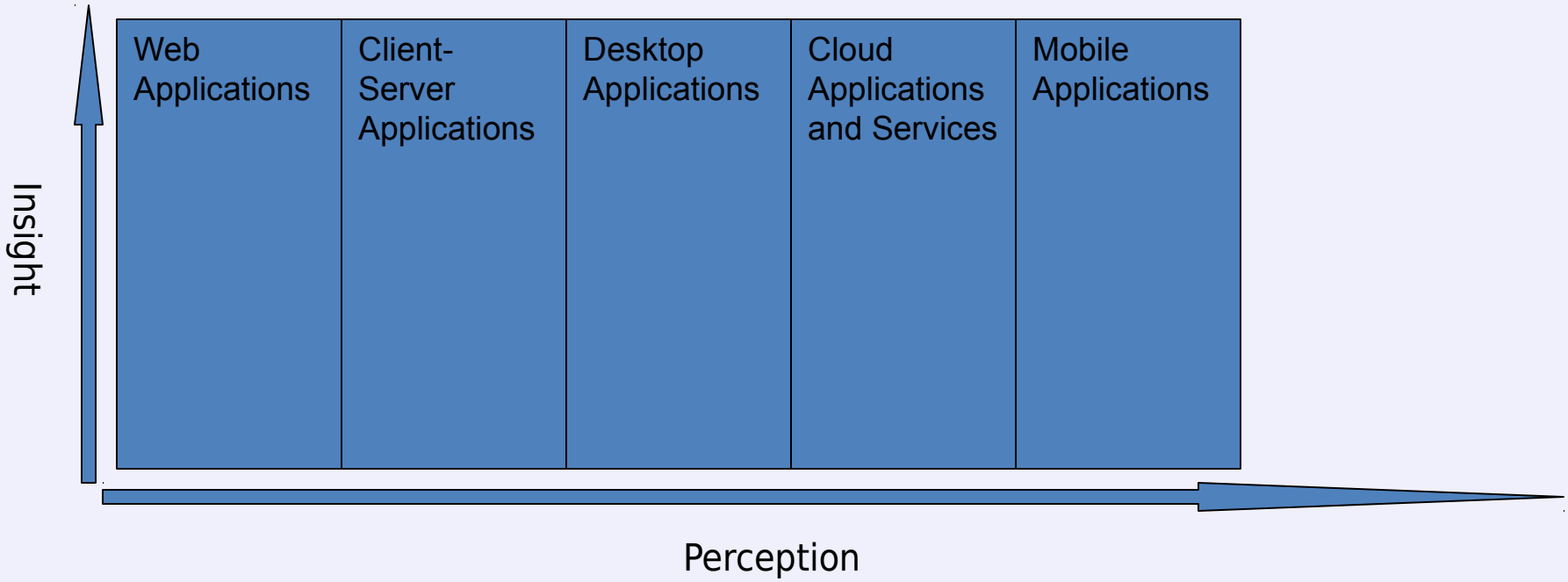
As perception of the problem of attack surface widens the scope of the problem increases



Attack Surface: The Security Officer's Journey

OWASP
The Open Web Application Security Project

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



Attack Surface: The Security Officer's Journey

OWASP
The Open Web Application Security Project

Discovery activities increase insight

Attack Surface: The Security Officer's Journey

OWASP
The Open Web Application Security Project

Discovery activities increase insight

Attack Surface: The Security Officer's Journey

OWASP
The Open Web Application Security Project

Discovery activities increase insight

Attack Surface: The Security Officer's Journey

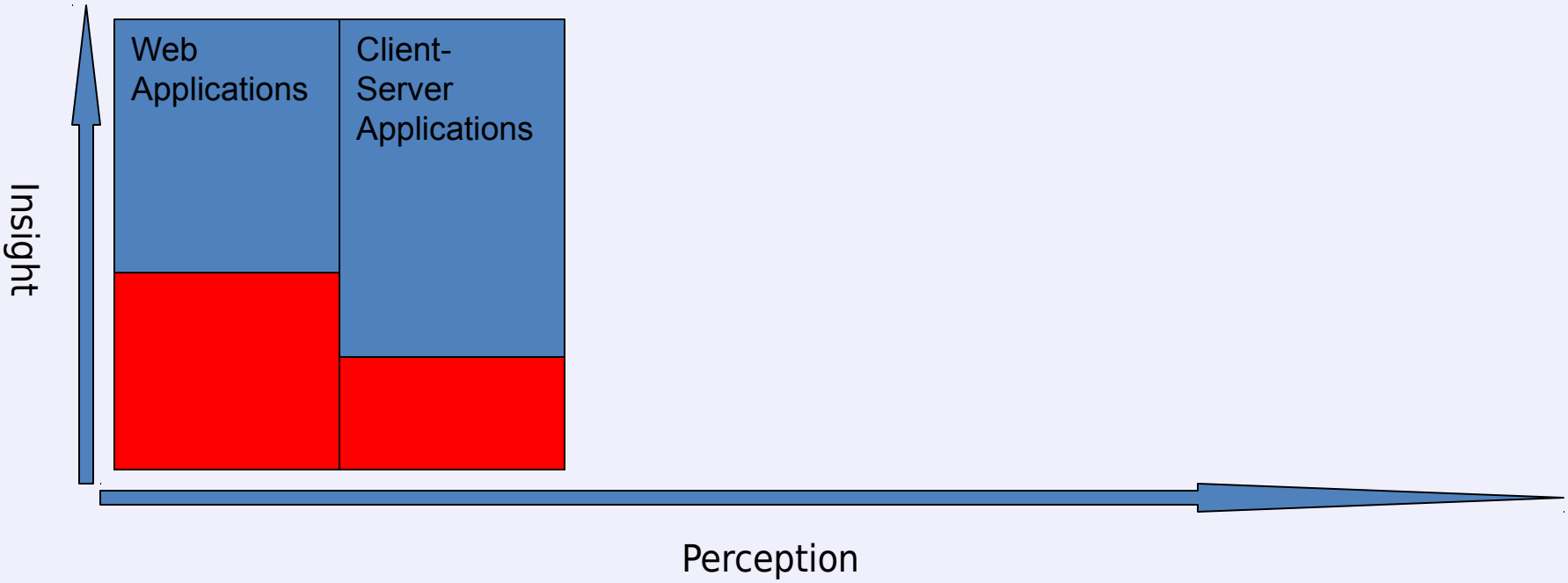
OWASP
The Open Web Application Security Project

Over time you end up with a progression

Attack Surface: The Security Officer's Journey

OWASP
The Open Web Application Security Project

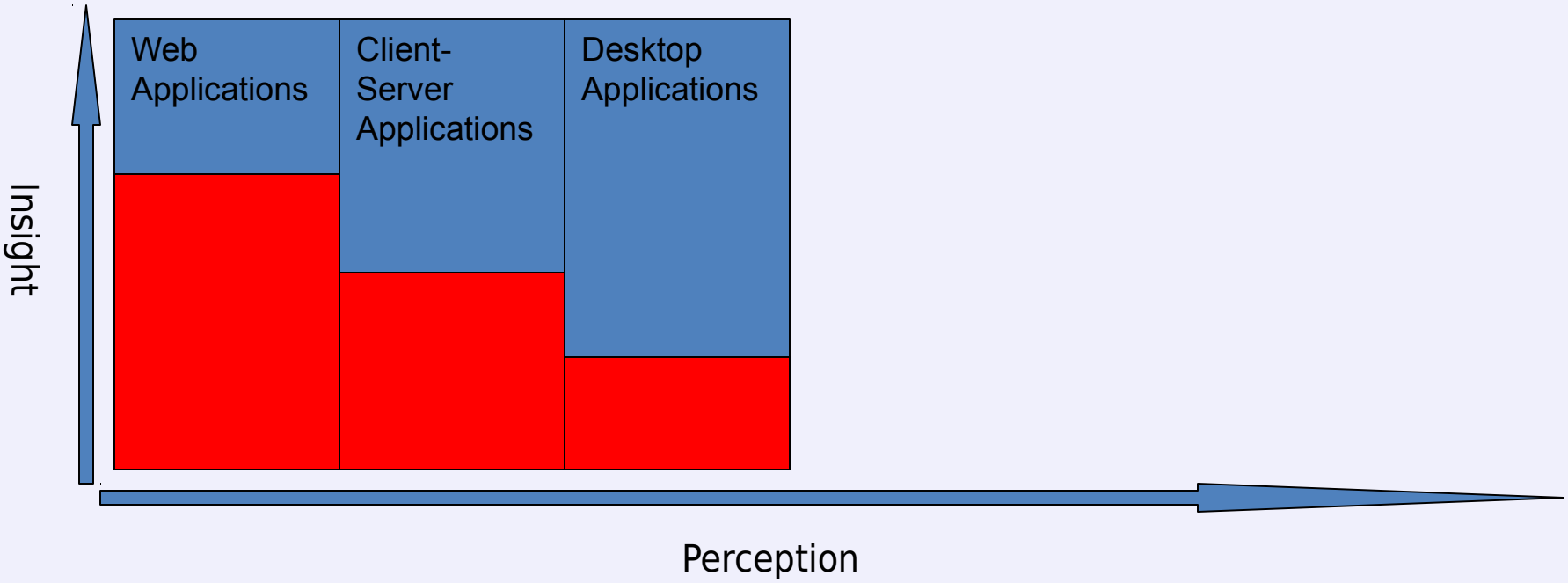
Over time you end up with a progression



Attack Surface: The Security Officer's Journey

OWASP
The Open Web Application Security Project

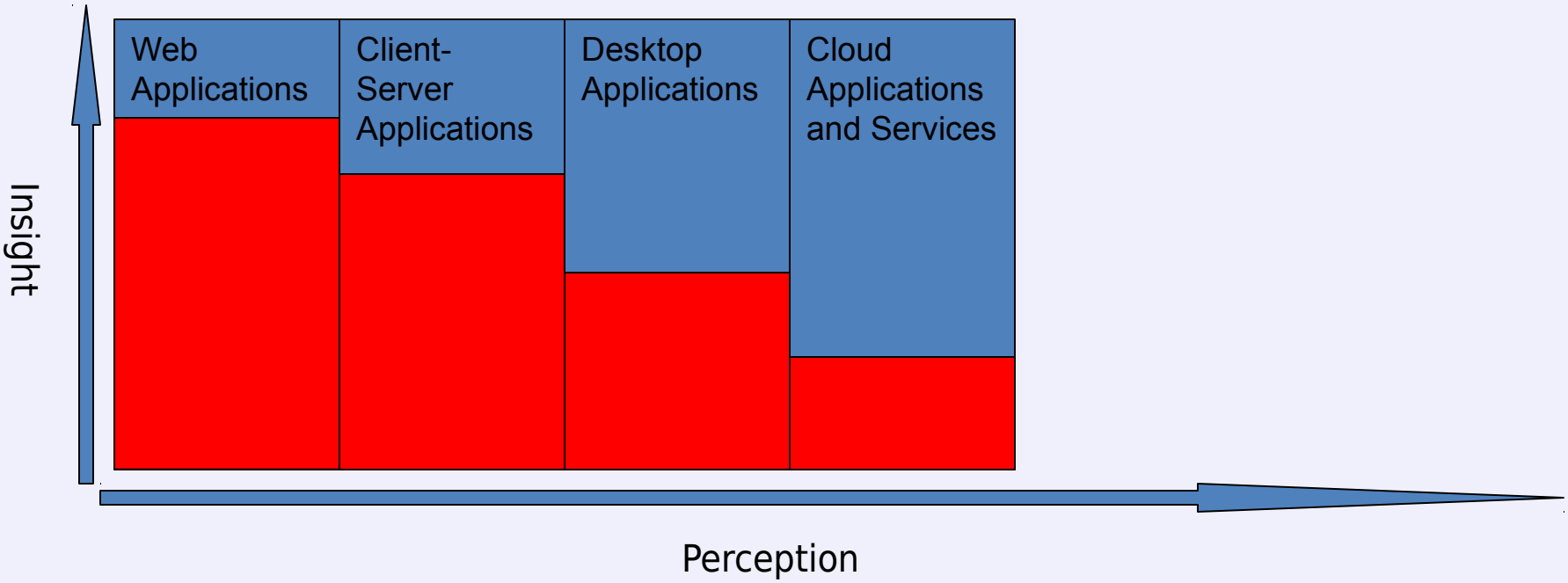
Over time you end up with a progression



Attack Surface: The Security Officer's Journey

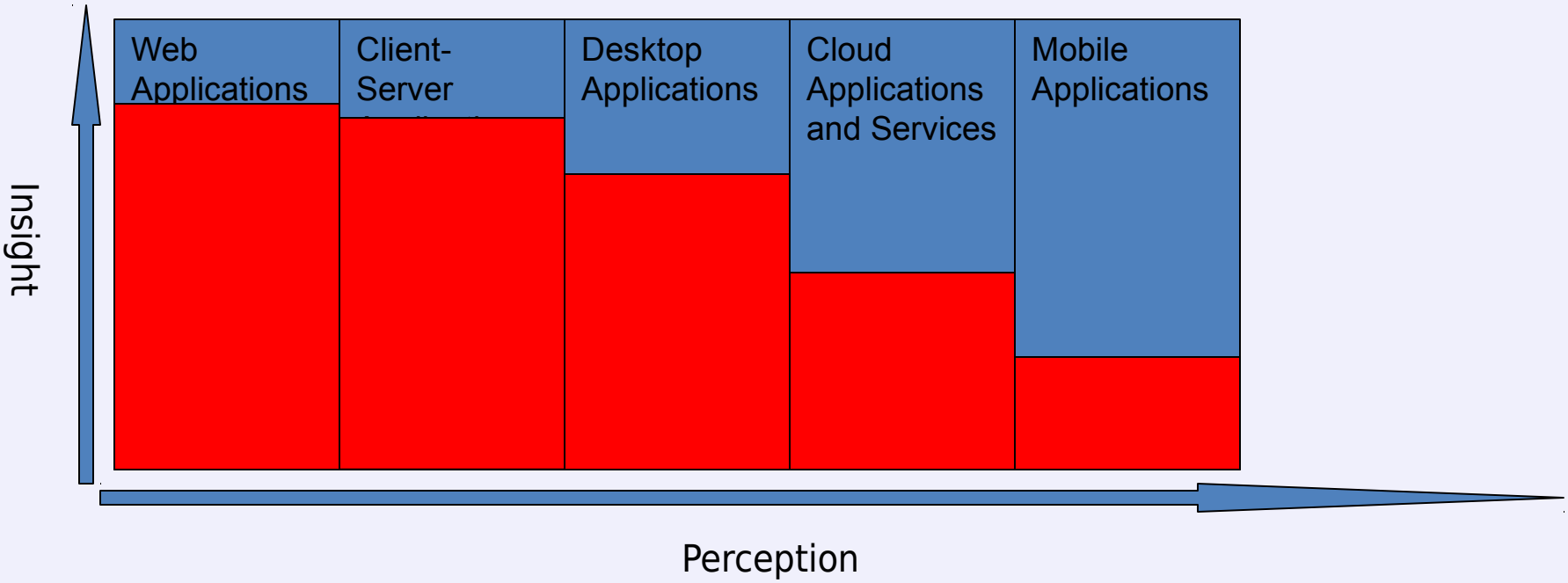
OWASP
The Open Web Application Security Project

Over time you end up with a progression



Attack Surface: The Security Officer's Journey

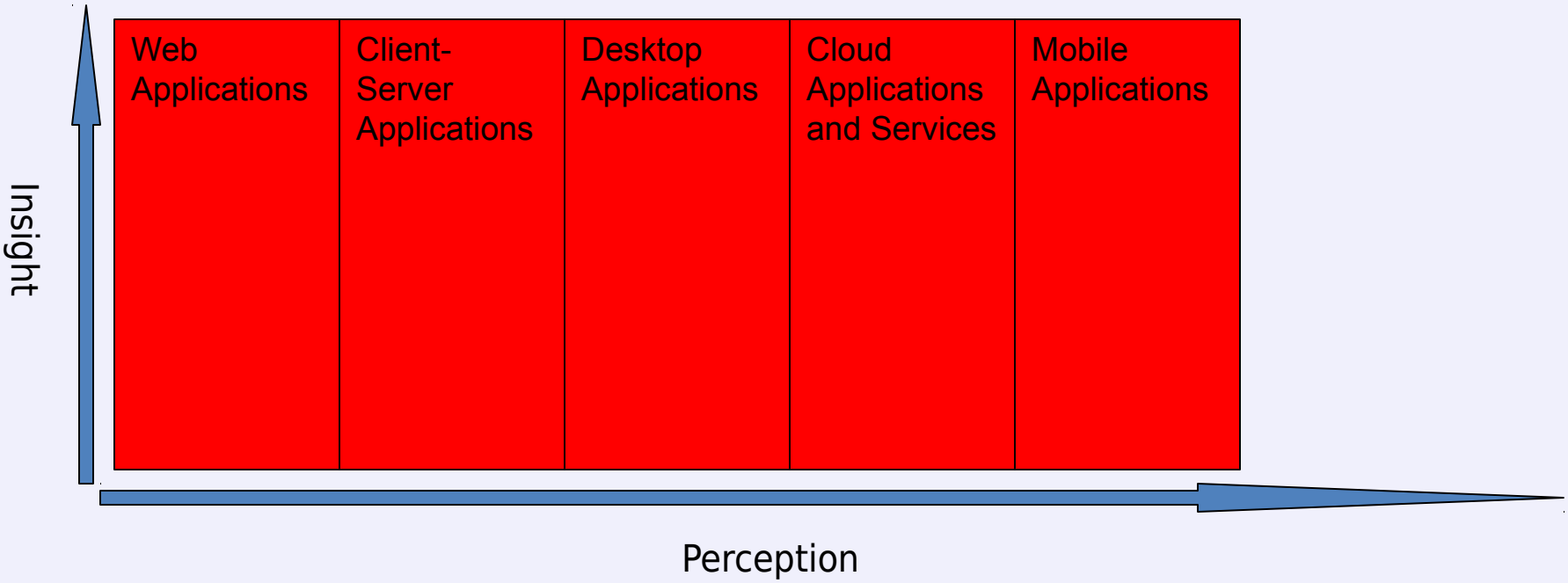
Over time you end up with a progression



Attack Surface: The Security Officer's Journey

OWASP
The Open Web Application Security Project

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



What Goes Into An Application Test?

OWASP
The Open Web Application Security Project

An Application Test

What Goes Into An Application Test?

OWASP
The Open Web Application Security Project

Dynamic Analysis

Static Analysis

What Goes Into An Application Test?

OWASP
The Open Web Application Security Project

Automated Application Scanning

Manual Application Testing

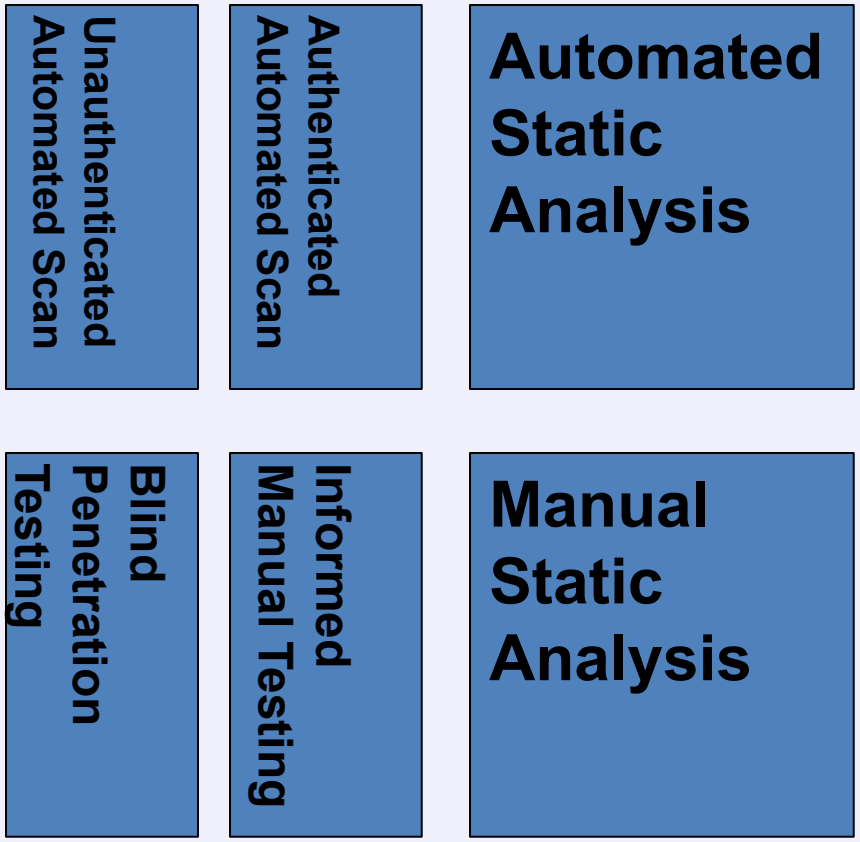
Static Analysis

What Goes Into An Application Test?

OWASP
The Open Web Application Security Project

Automated Application Scanning	**Automated Static Analysis**
Manual Application Testing	**Manual Static Analysis**

What Goes Into An Application Test?



What Goes Into An Application Test?

OWASP
The Open Web Application Security Project

Automated Binary Analysis	Manual Binary Analysis
Automated Source Code Scanning	Manual Source Code Review
Authenticated Automated Scan	Informed Manual Testing
Unauthenticated Automated Scan	Blind Penetration Testing

Value and Risk Are Not Equally Distributed

OWASP
The Open Web Application Security Project

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

OWASP
The Open Web Application Security Project

Allocate Different Levels of Resources to Assurance
Select Different Assurance Activities

Also Must Often Address Compliance and Regulatory Requirements

The ThreadFix Approach

OWASP
The Open Web Application Security Project

Free / Open Source vulnerability management and aggregation platform:

Allows software security teams to reduce the time to remediate software vulnerabilities

Enables managers to speak intelligently about the status / trends of software security within their organization.

Features/Benefits:

Imports dynamic, static and manual testing results into a centralized platform

Removes duplicate findings across testing platforms to provide a prioritized list of security faults

Eases communication across development, security and QA teams

Exports prioritized list into defect tracker of choice to streamline software remediation efforts

Auto generates web application firewall rules to protect data during vulnerability remediation

Empowers managers with vulnerability trending reports to pinpoint team issues and illustrate application security progress

Benchmark security practice improvement against industry standards

Freely available under the Mozilla Public License (MPL) 2.0
Download available at: www.denimgroup.com/threadfix
Code available at: https://code.google.com/p/threadfix/

ThreadFix Demonstration

OWASP
The Open Web Application Security Project

Building Your Application Portfolio

Storing Scanning Results Over Time

Reporting

- Trending
- Vulnerability Remediation Progress
- Scanner Benchmarking
- Portfolio Status

Steps for Improvement

OWASP
The Open Web Application Security Project

Build Your Application Portfolio

Characterize the Effectiveness of Efforts Made to Date

Build a Plan for Coverage

Monitor Progress

Questions?

OWASP
The Open Web Application Security Project

Dan Cornell
Principal and CTO
dan@denimgroup.com
Twitter @danielcornell
+1 (210) 572-4400

www.denimgroup.com
blog.denimgroup.com