Vulnerability Management – From B Movie to Blockbuster

Rahim Jina

5 December 2018

edgescan™

Rahim Jina

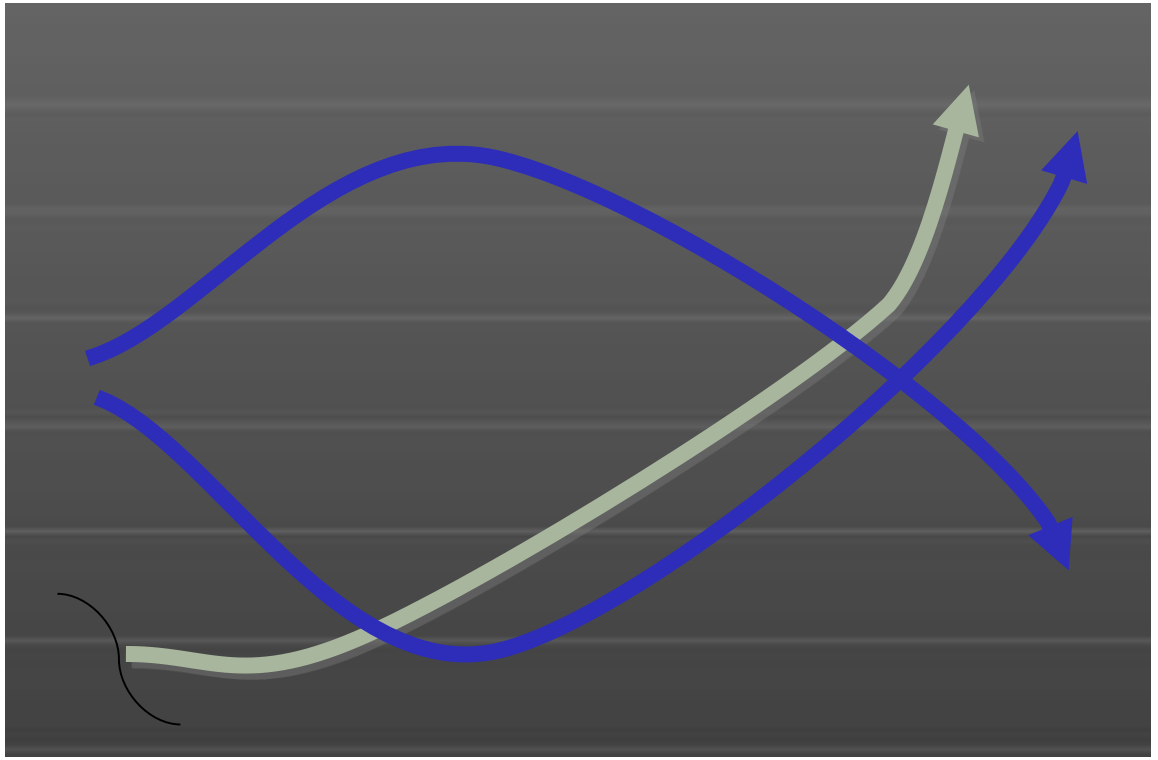
COO & Co-Founder

Edgescan & BCC Risk Advisory

@rahimjina
rahim@edgescan.com


at&t
LinkedIn
UCLA
Kiplinger
zynga
HACKED
RATFOR
GLOBAL INTELLIGENCE
UNIVERSITY
NYSE
GAWKER
BitTorrent

Its (not) the $$$$

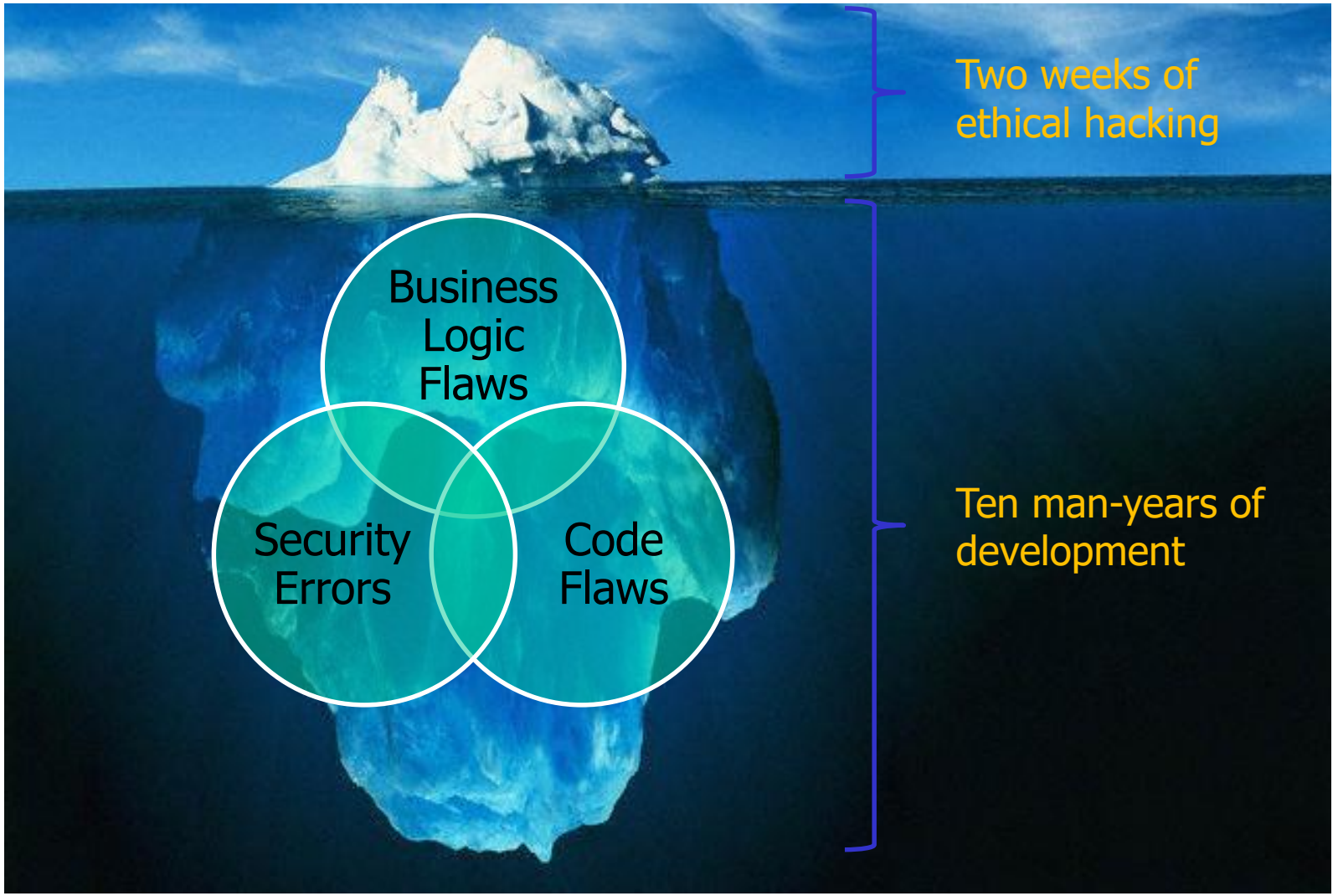


Information security spend

Security incidents (business impact)

Problem # 1
Asymmetric Arms Race

An inconvenient truth



In two weeks:

Consultant "tune tools"
Use multiple tools – verify issues
Customize Attack Vectors to technology stack
Achieve 80-90 application functionality coverage

How experienced is the consultant?

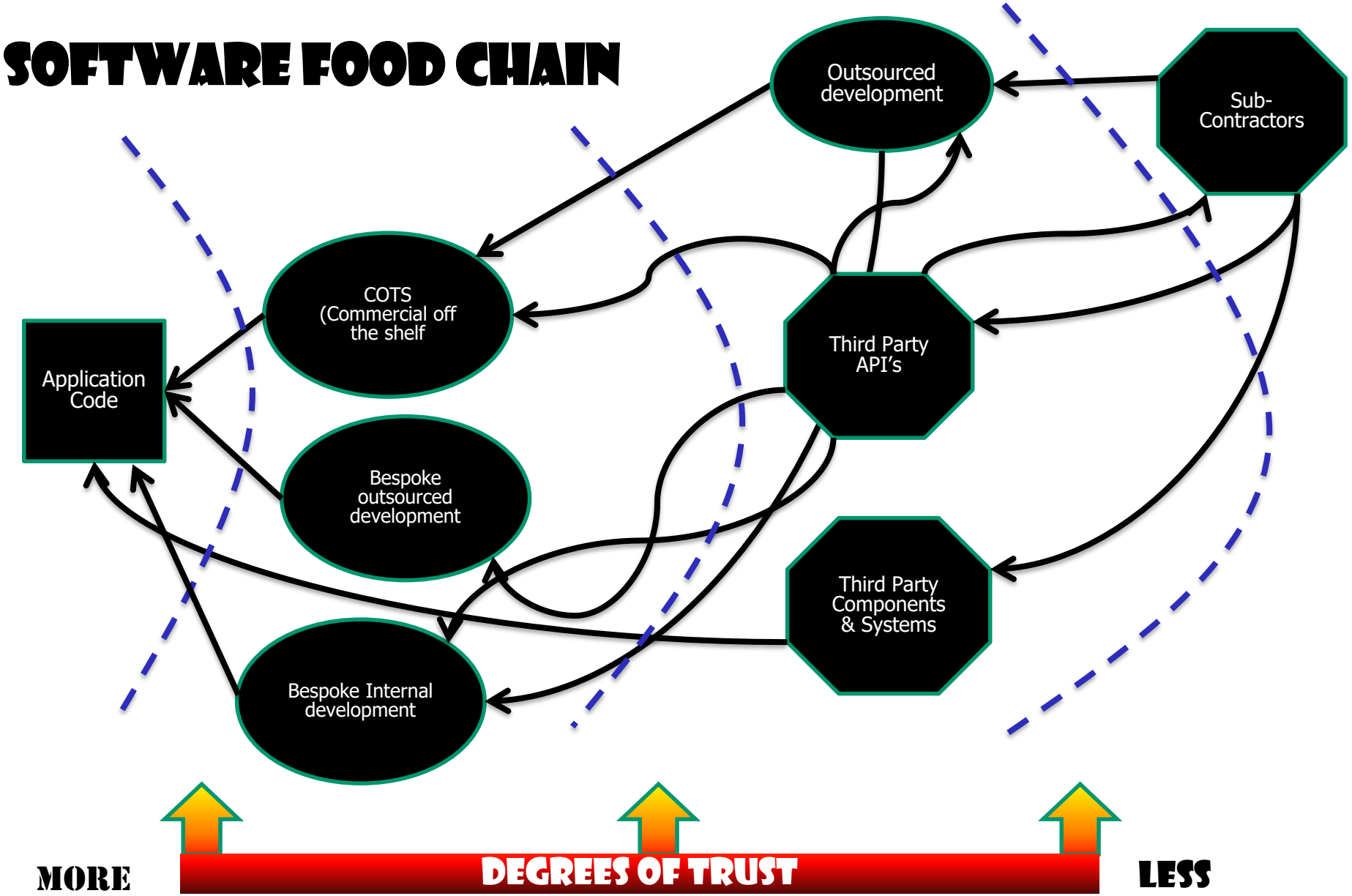
Was the environment even working properly!!

Are they as good as the bad guys?
They certainly need to be, they only have 2 weeks, right!!?

Code may be pushed to live soon after the test.
Potential window of Exploitation could be until the next pen test.
6 mths, 9 mths, 1 year?


Problem # 2
You are what you eat

SOFTWARE FOOD CHAIN



You may not let some of the people who have developed your code into your offices!!

2018 - Open Source Security Statistics.

- 23% of the Components in the Average Software Application Contain Known Vulnerabilities
- 60% of businesses do not keep a complete inventory (bill of materials) of components being used in their applications.

- edgescan statistics November 2018

Struts - application development framework : downloaded 2 million times in the last year. –

Remote Code Execution attack CVE-2017-9805

Struts 2.1.2 - 2.3.33, 2.5 - 2.5.12

https://cwiki.apache.org/confluence/display/WW/S2-052

2.1.2 – 9 years old

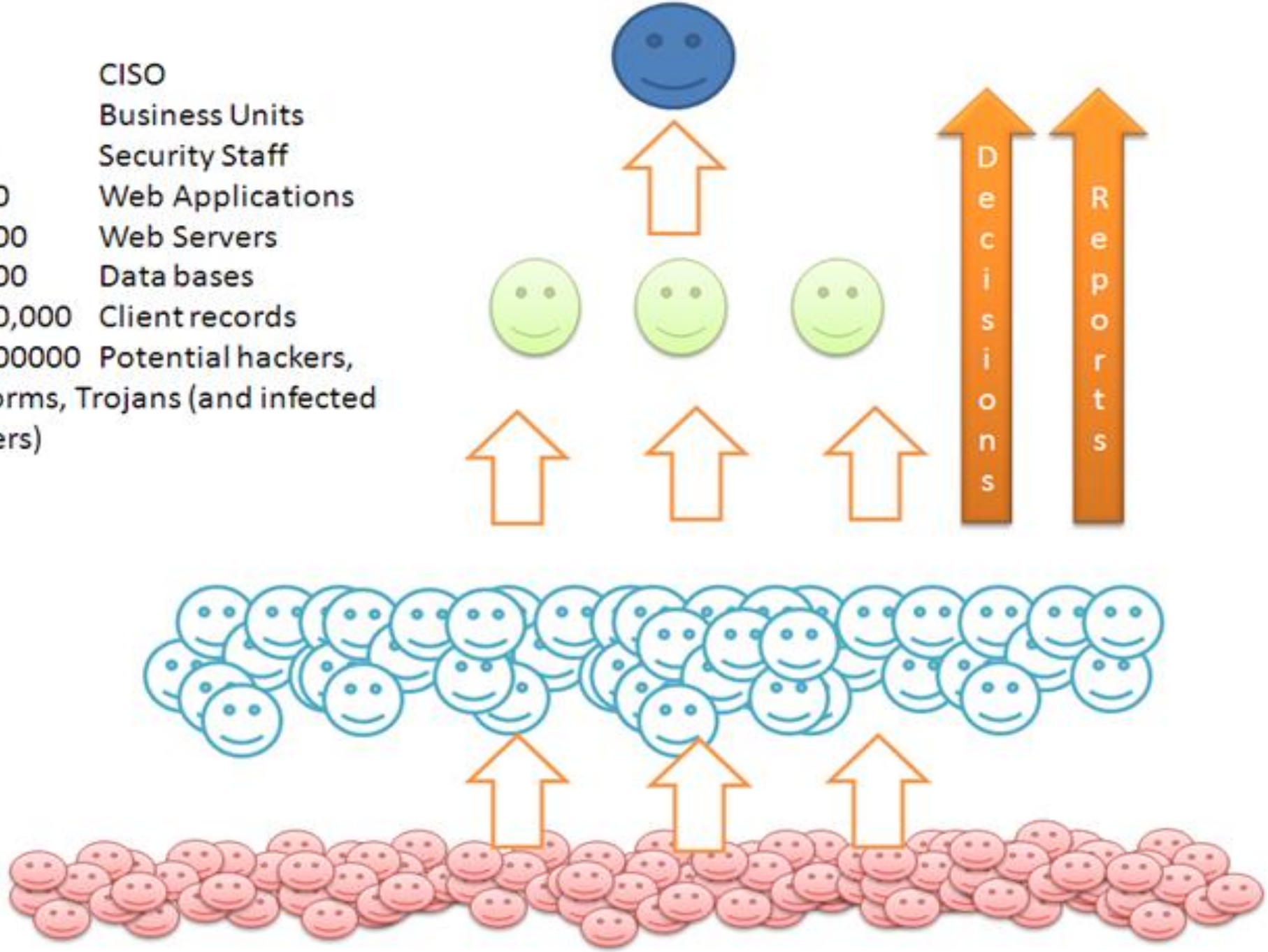
2.3.33 – July 2017

2.5.x – May 2017

https://struts.apache.org/downloads.html


Problem # 3
Bite off more than we can chew

1	CISO
10	Business Units
30	Security Staff
200	Web Applications
1000	Web Servers
2000	Data bases
100,000	Client records
1000000	Potential hackers, Worms, Trojans (and infected users)



"We can't improve what we can't measure"

Problem # 4

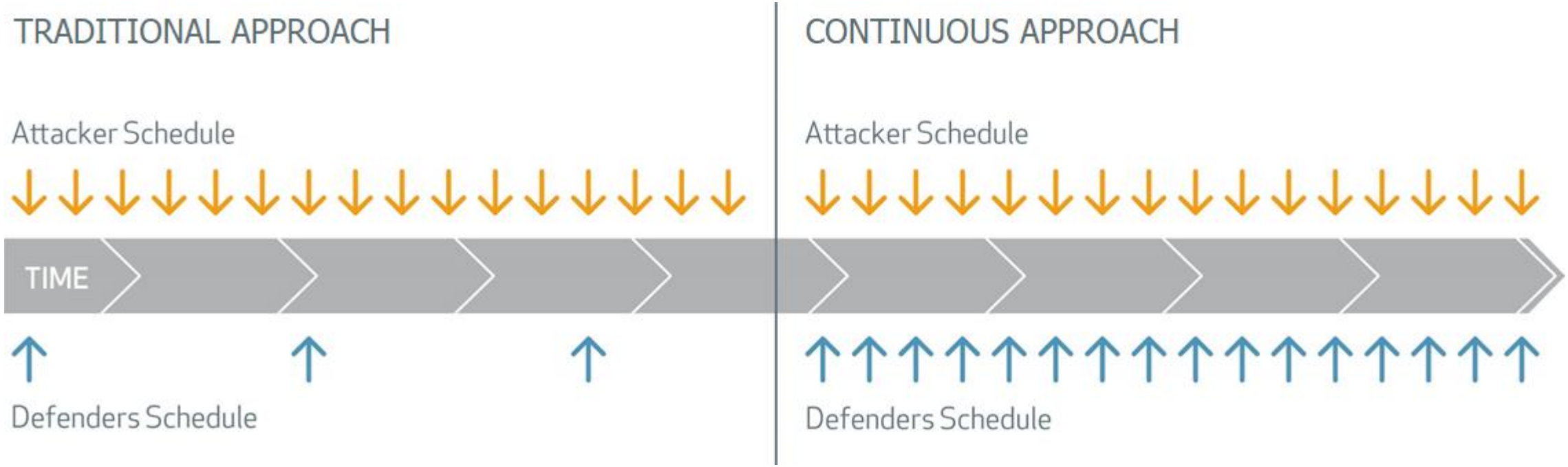
Nothing ever stands still

Challenge

- Application Layer (Layer 7) is still more vulnerable.
- Applications change more.
- Change results in Risk (CI/CD/Agile)
- Risk (may) result in vulnerability & breach.

Keeping pace with change

- “Keeping pace” with development.
- Assisting secure **deployment.**
- Catching bugs **early** – Push Left.
- Help ensure “**change**” is secure.



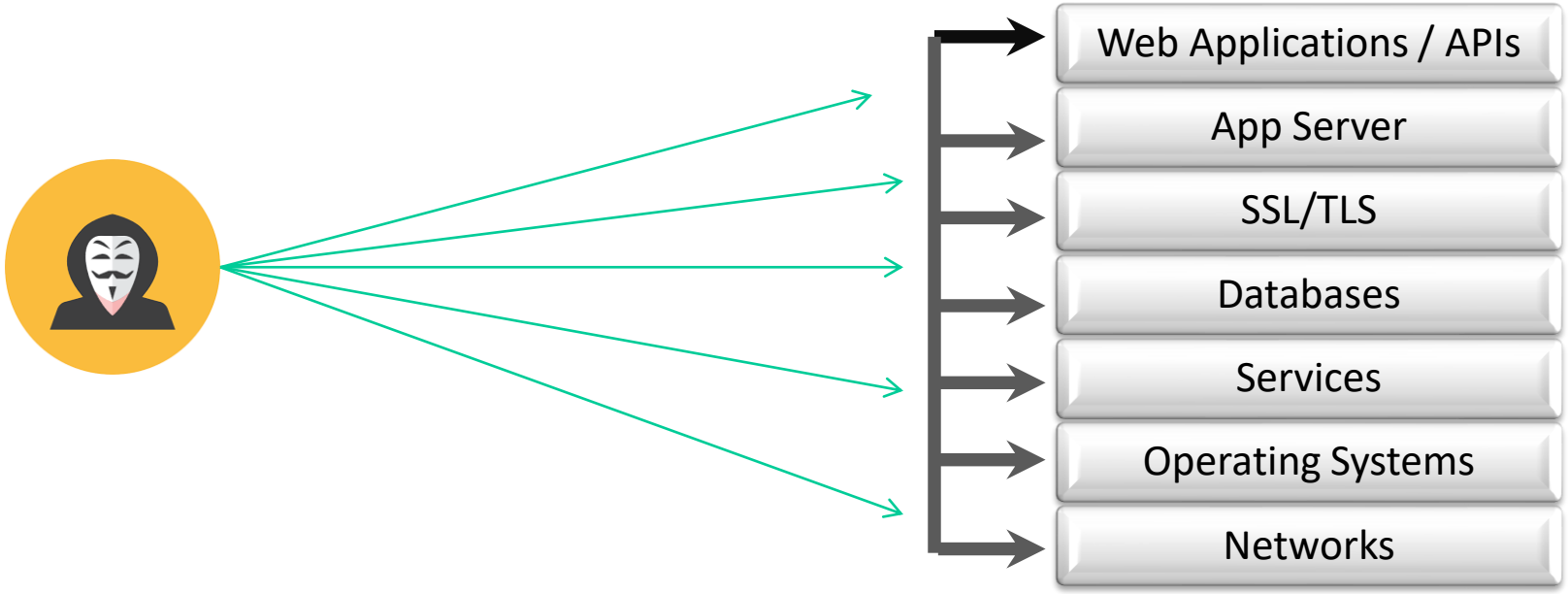
Let’s do a reality check

Where are these stats coming from?

- **edgescan™** is a sophisticated, enterprise-grade vulnerability assessment and management solution
- **edgescan™** helps from small & medium-sized to large enterprises identify and remediate known vulnerabilities
- **edgescan™** is a cloud based SaaS

#Fullstack

edgescan™



How we get the Statistical model

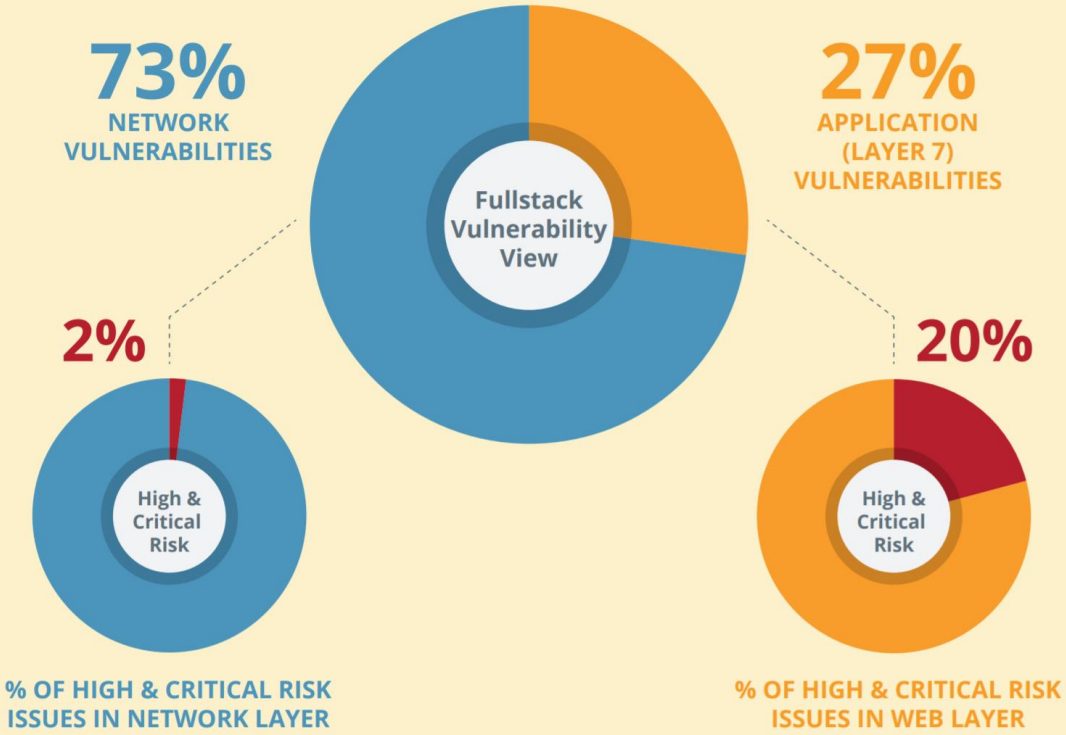
- 1000’s of vulnerability assessments globally.
- #Fullstack view of security
- False positive free (99%) ☺
- Industries: Media, Energy, Government, Pharma, Finance, Software etc….

Risk Dispersion

edgescan™

FULLSTACK VULNERABILITY VIEW

In 2017 we discovered that on average, 27% of all vulnerabilities were associated with web applications and 73% were network vulnerabilities.



Web Application Layer (Layer 7)

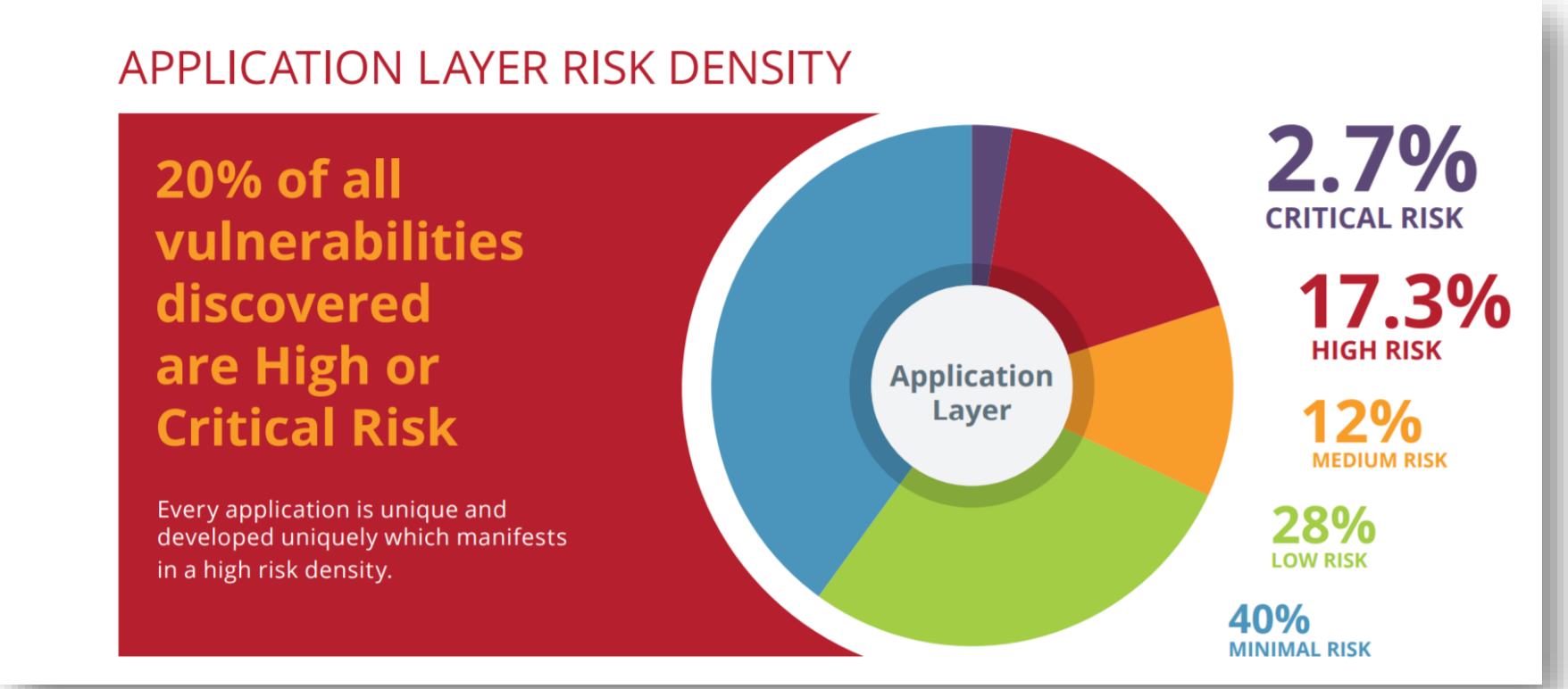
edgescan™

Lots of high or critical risk issues!!

Easily exploitable

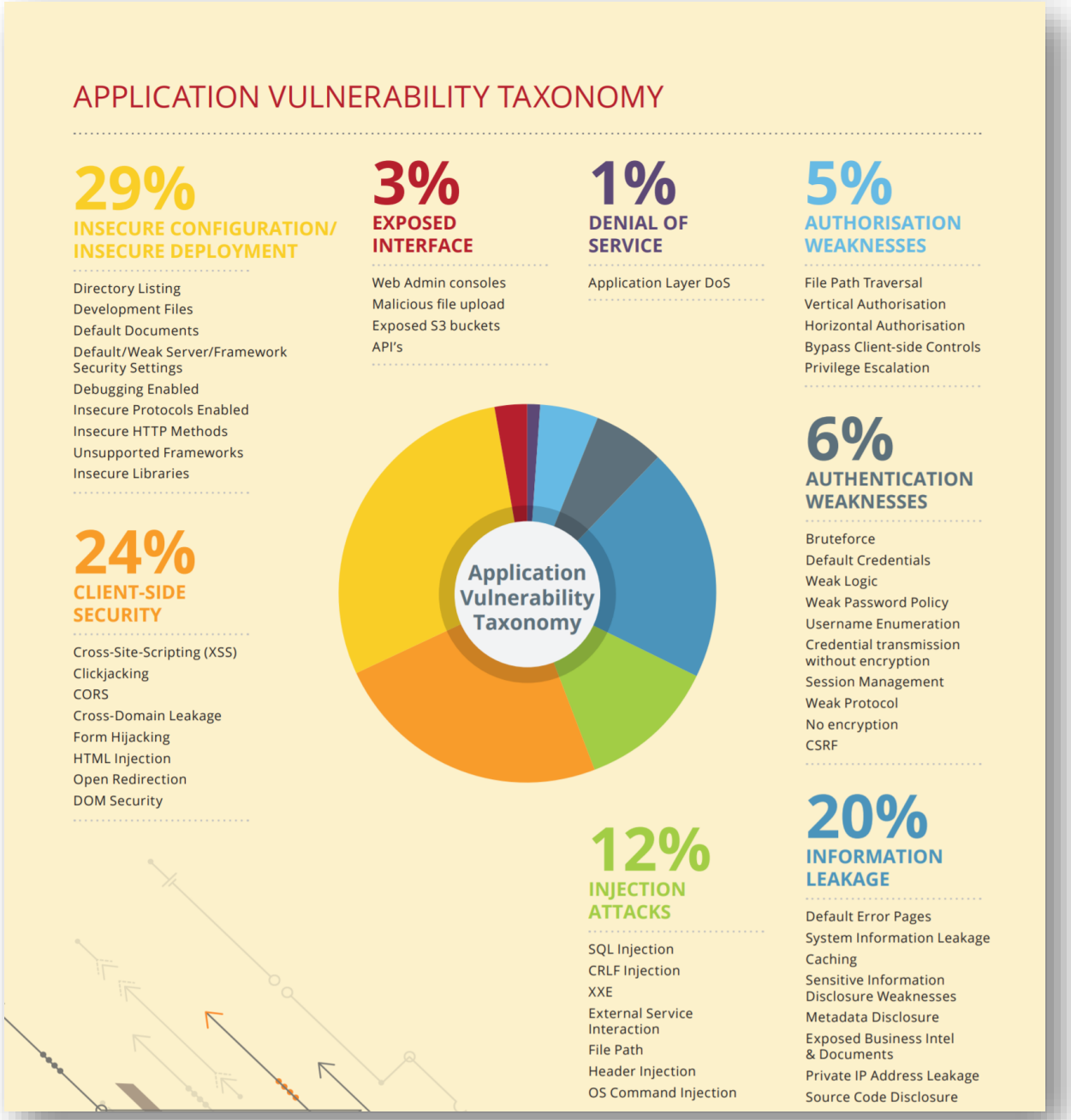
Very Damaging

Very Bad



More Detail – App Layer

- System configuration and secure deployment is a big issue.
- Client-Side security: XSS, HTML Injection, Browser based issues are still very common.



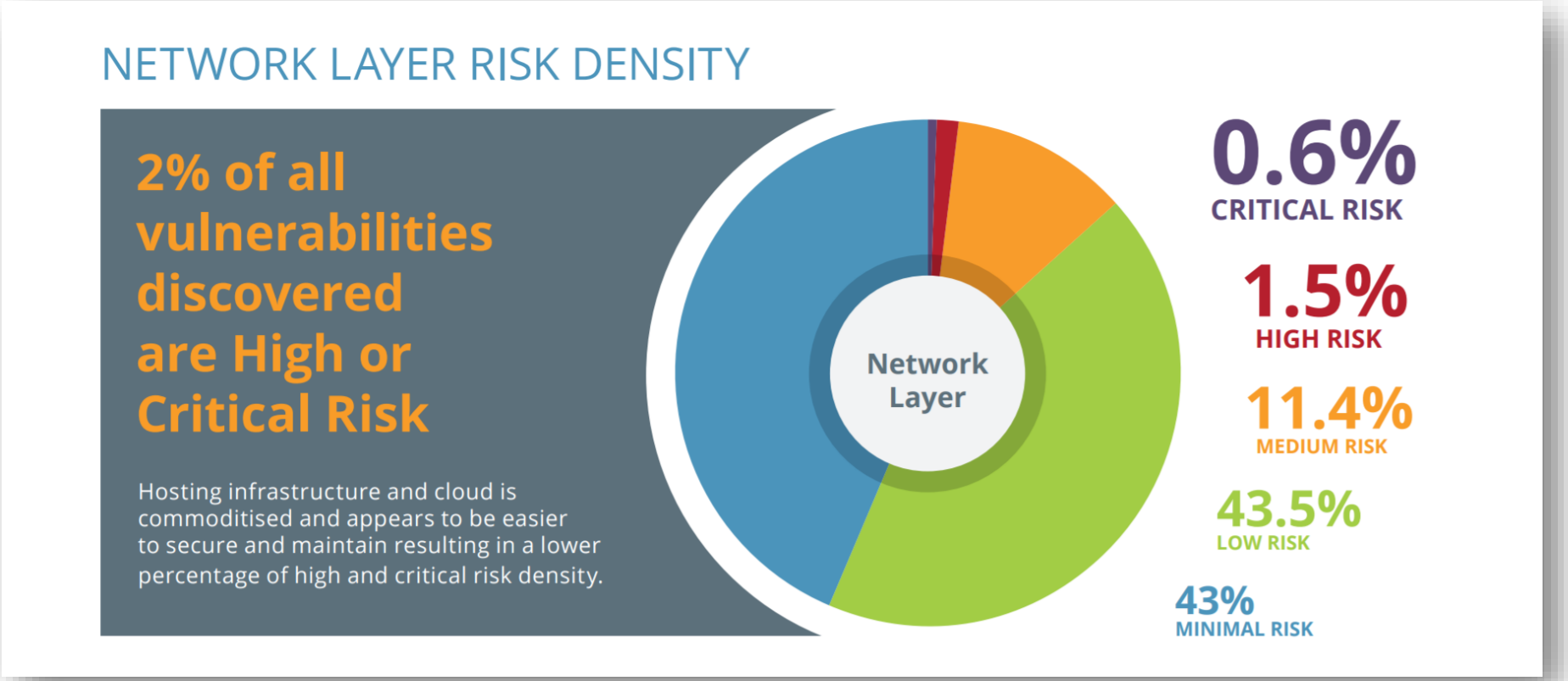
edgescan™

Infrastructure Layer (Non Web app)

Lots of vulnerabilities!!

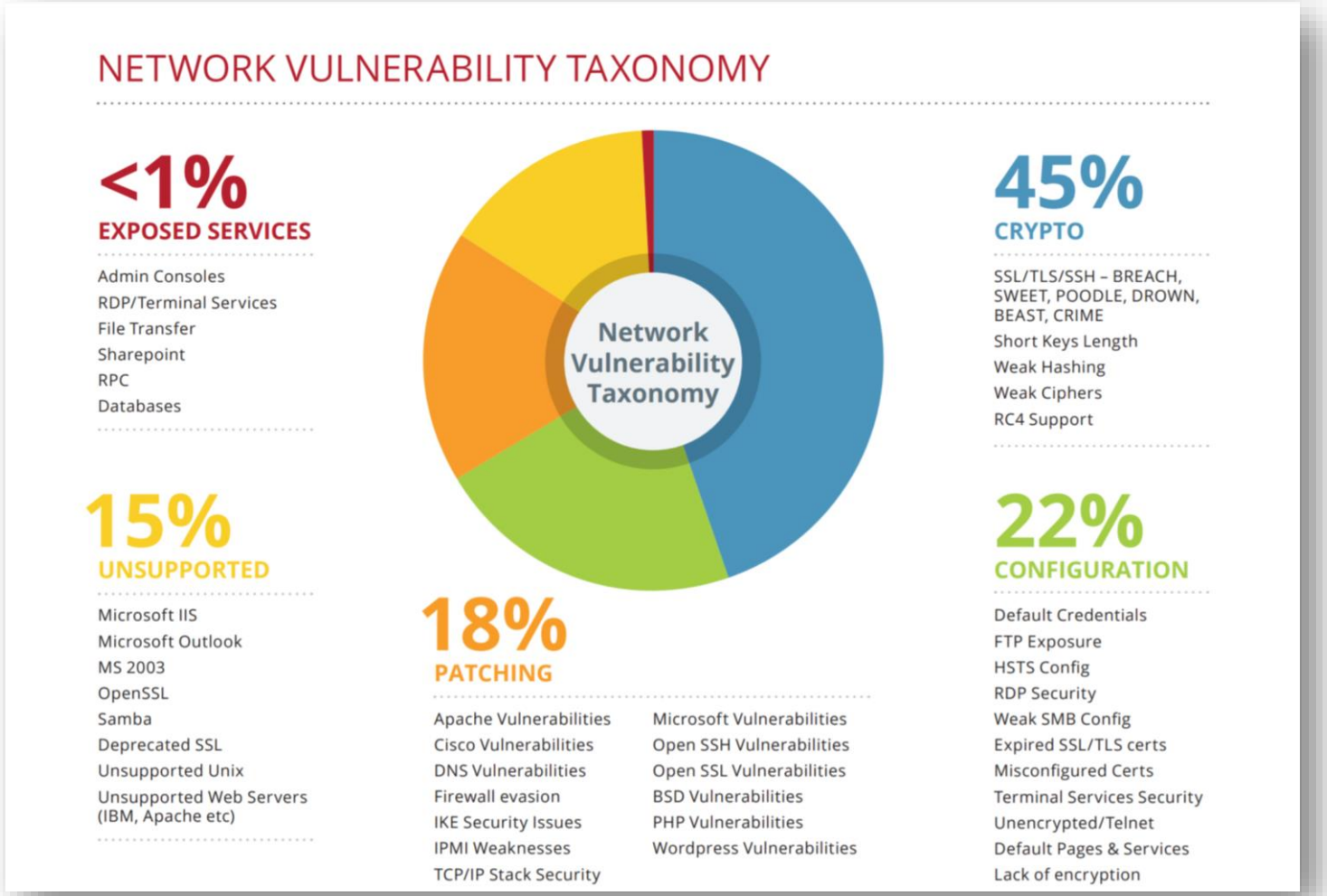
Not many high or Critical Risk.

More problems but less vulnerable



More Detail – Net Layer

- Large number of crypto-related issues: deprecated protocols, CVE's, poor implementation.
- Weak configuration / Mis-configuration



Known Vulnerabilities - Age

Patching and version maintenance is still a key part of maintaining a secure posture.

Known Vulnerabilities – Most Common

edgescan™

CVE-2004-2761

MD5 Message-Digest Algorithm is not collision resistant

CVSS: 5.0

CVE-2008-7220

Vulnerability in Prototype JavaScript framework (prototypejs)

CVSS: 7.5

CVE-2011-4969

Cross-site scripting (XSS) vulnerability in jQuery

CVSS: 4.3

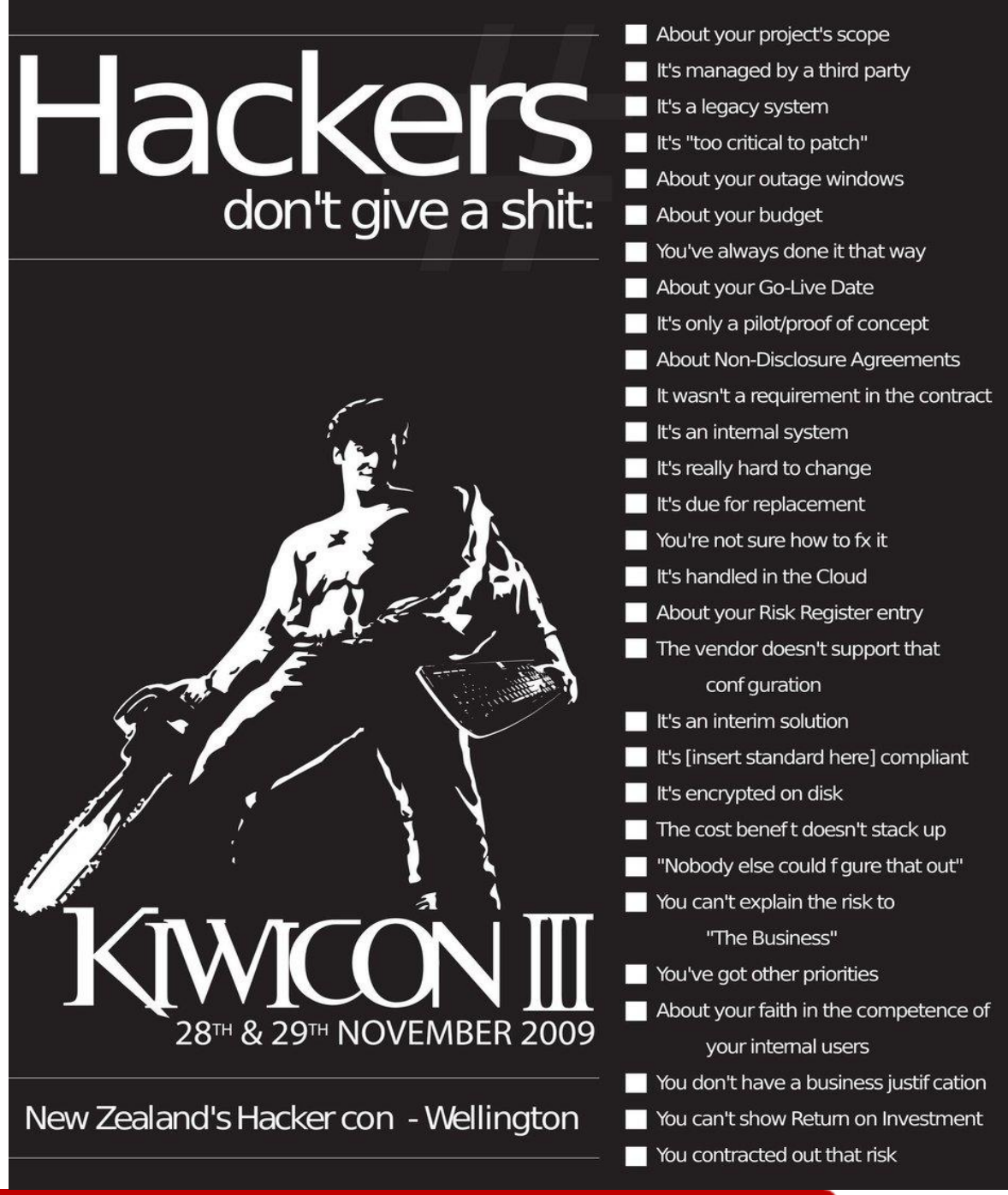
CVE-2008-5161

Error handling vulnerability in the SSH protocol

CVSS: 2.6

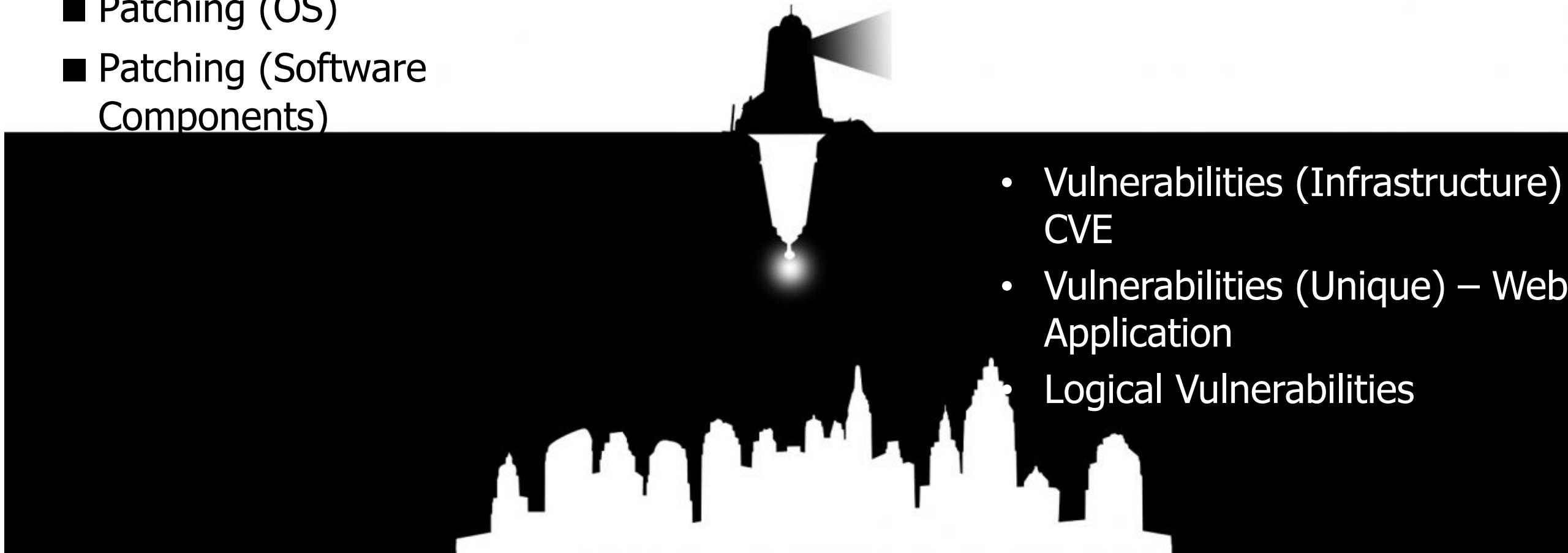
Don’t “Silo”/ Segment Risk…

Hackers don’t care where the vulnerability is!

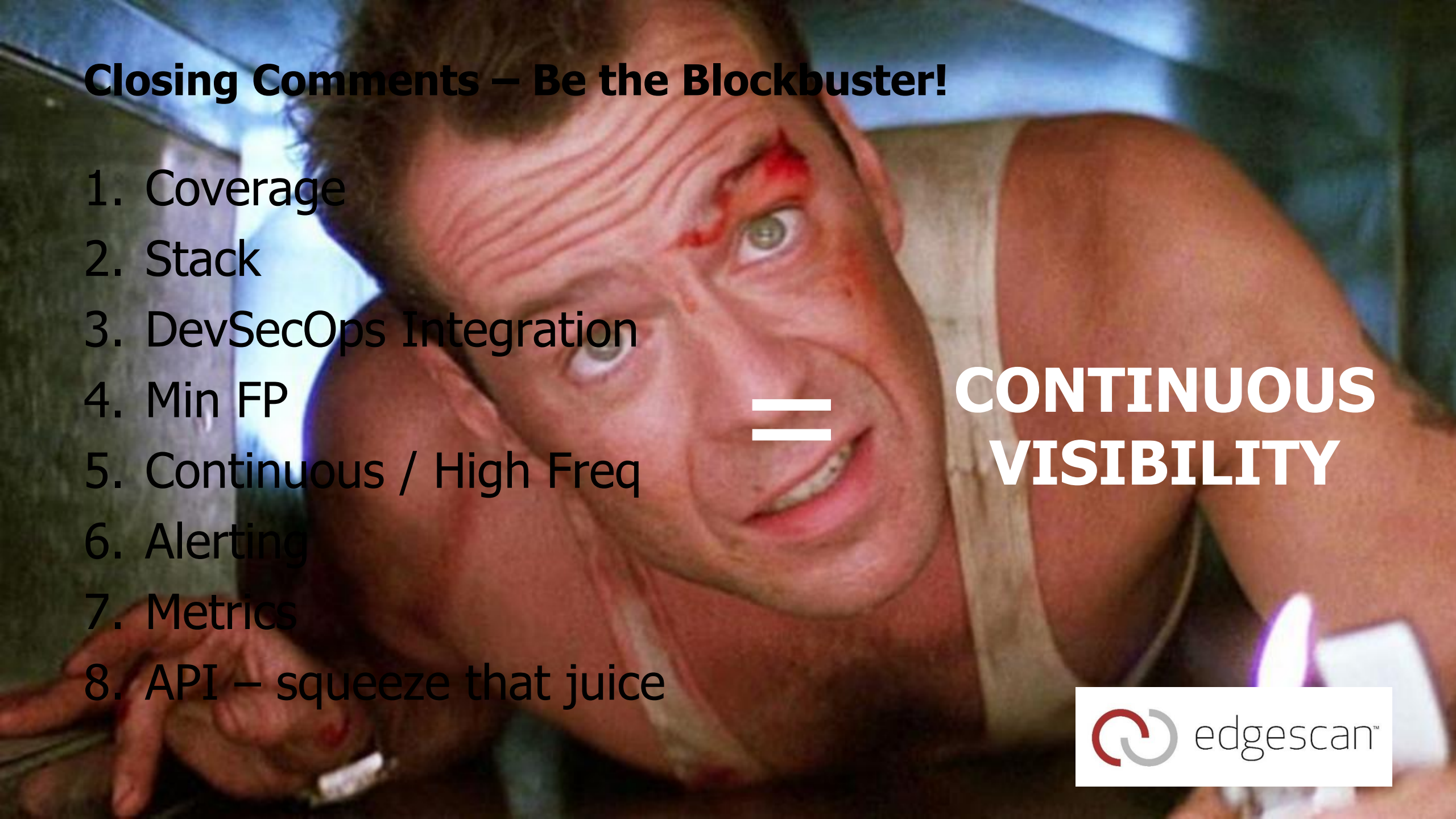


edgescan™

- Services
- Ports
- Patching (OS)
- Patching (Software Components)



- Vulnerabilities (Infrastructure) CVE
- Vulnerabilities (Unique) – Web Application
- Logical Vulnerabilities



Closing Comments – Be the Blockbuster!

1. Coverage
2. Stack
3. DevSecOps Integration
4. Min FP
5. Continuous / High Freq
6. Alerting
7. Metrics
8. API – squeeze that juice

=

CONTINUOUS VISIBILITY

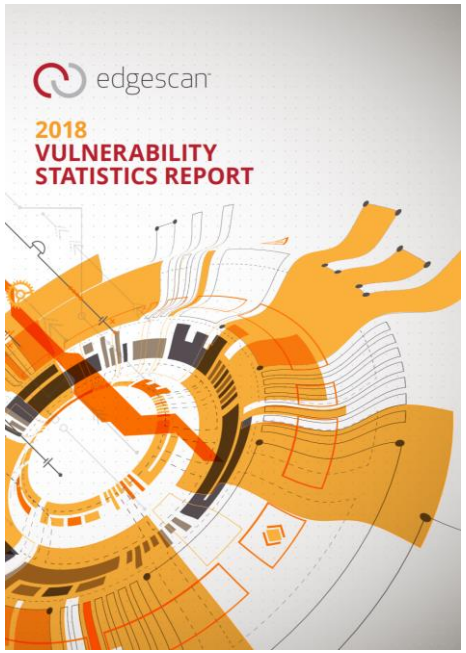
edgescan™

THANKS!

2019 Coming Soon!

edgescan™ 2018 Vulnerability Stats Report:

Available now on:
edgescan.com



rahim@edgescan.com
@rahimjina

NO ANNOYING REGISTRATION NECESSARY!

edgescan