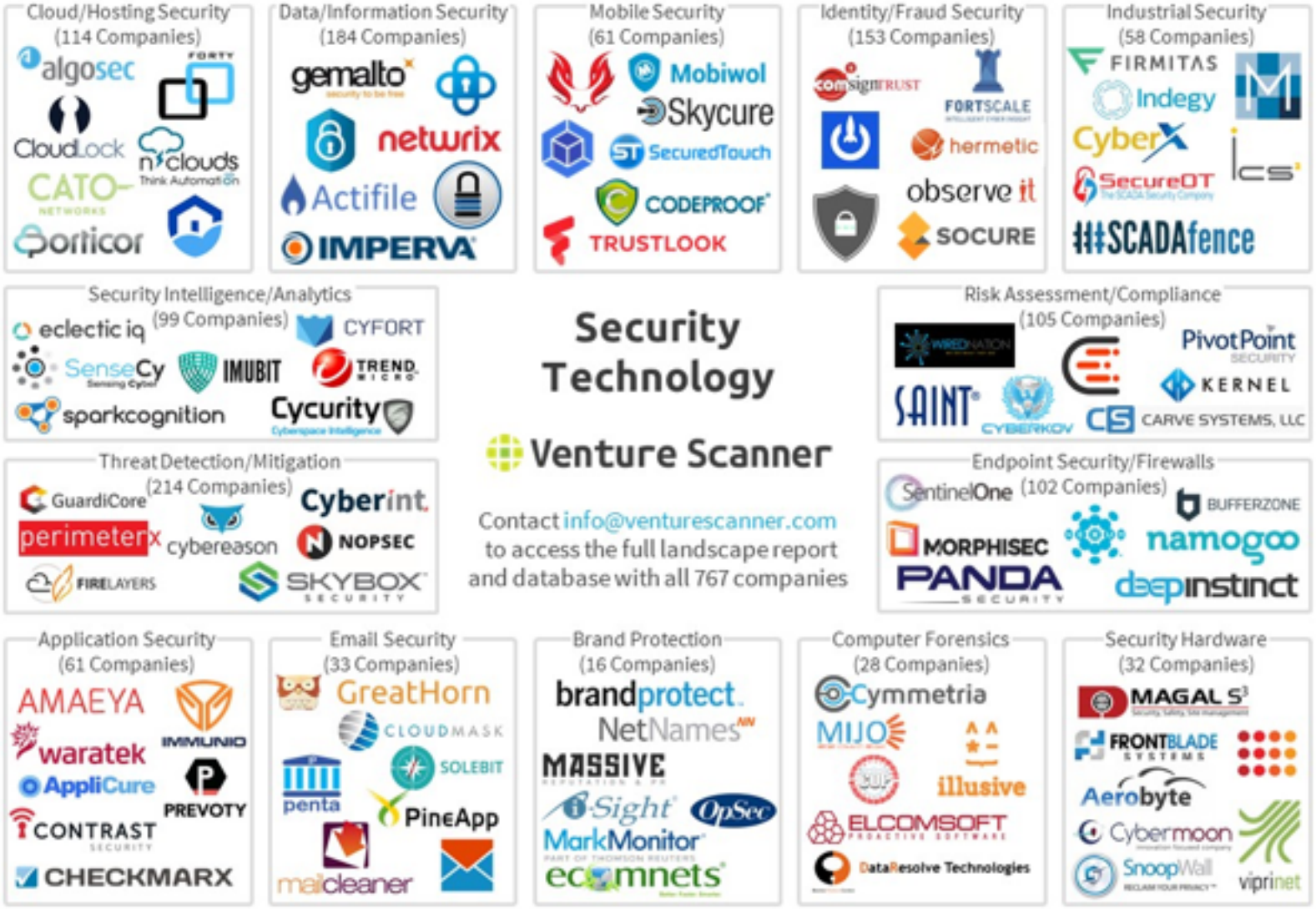
HIGH-TECH BRIDGE®
WEB SECURITY COMPANY

Application Security Strategy and AST Lifecycle

OWASP London Chapter Meeting, 2018

by
Ilia Kolochenko
High-Tech Bridge, CEO & Founder
Forbes Technology Council, Member

Are we secure now ?



State of the Art Cybersecurity ?

- **Worldwide Security Spending Will Reach $96 Billion in 2018** — Gartner
- **US Halloween spending hit record $9.1 billion in 2017** — Forbes
- **Cybercrime caused up to $109B hit to US economy in 2016** — The White House
- **Nearly seven in ten large companies identified a breach or attack** — National Cyber Security Centre, a part of GCHQ
- **Ransomware hackers purposefully target US Police Departments** — CNBC

Application Security Testing Jungles

- SAST v. DAST v. IAST v. MAST v. SCA ?
- AVC v. ASTO ?
- WAF v. NGFW v. RASP ?
- S-SDLC v. DevSecOps v. CI/CD ?
- Bug Bounties v. Private Bug Bounty v. Open Bug Bounty ?
- Crowdsourced Penetration Testing v. Crowdsourced Neurosurgeons ?
- Machine Leaning v. Artificial Intelligence ?

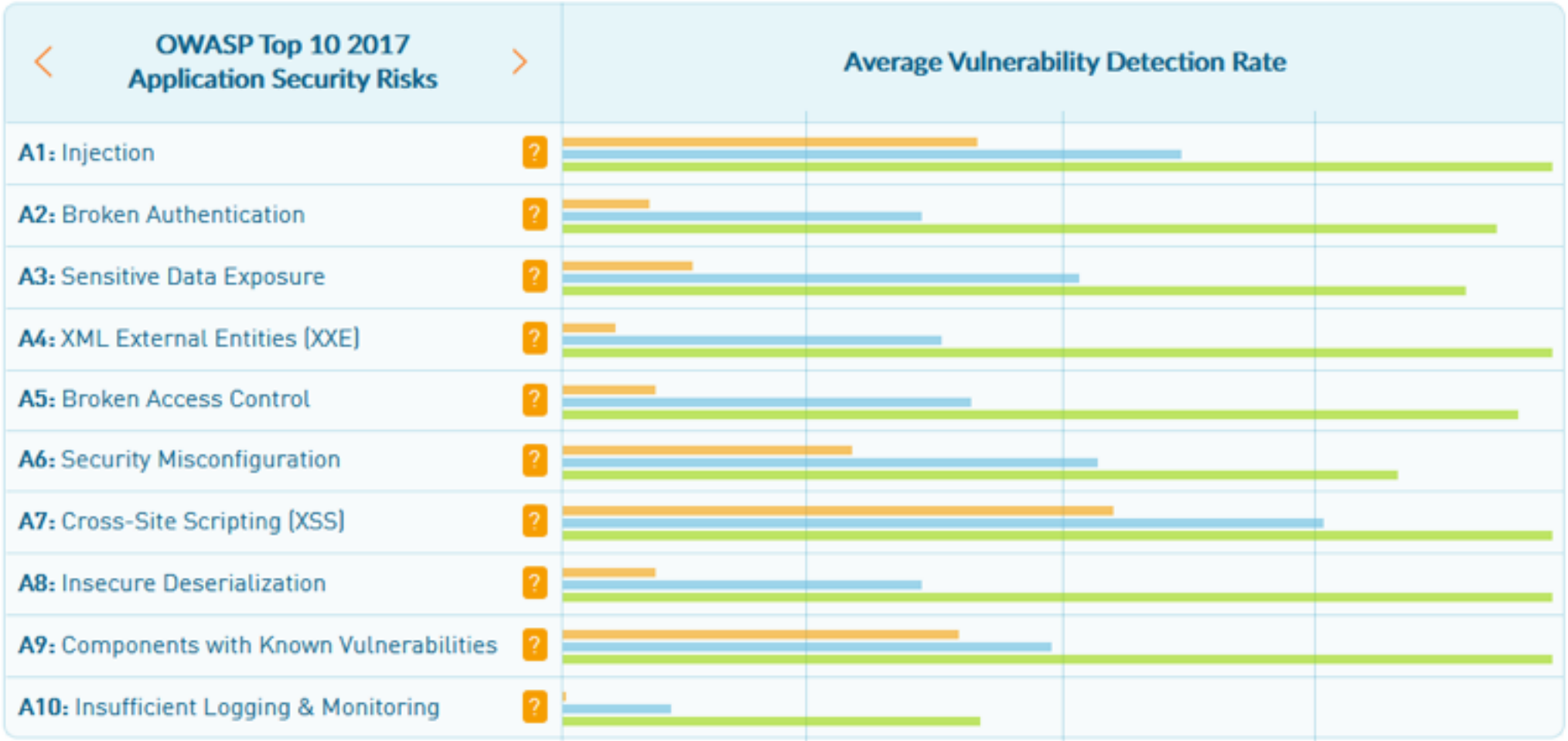
OWASP Top Ten 2013 v. OWASP Top Ten 2017 RC 1

Top 10 2013	Top 10 2017
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting
A4 – Insecure Direct Object References	A4 – Broken Access Control
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control	A7 – Insufficient Attack Protection
A8 – Cross-site Request Forgery (CSRF)	A8 - Cross-site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	A10 – Unprotected APIs

OWASP Top Ten – Collections of Marketing Slogans

- “We go far beyond OWASP Top 10”
- “We use AI to reimagine OWASP Top 10”
- “Scanners detect OWASP Top 10, we detect serious flaws”
- “Time to address human code, not just OWASP Top 10”
- “Manual testing for OWASP Top 10, Injections and RCEs”
- “Complicated Web 2.0 and HTML 5.0 vulnerability detection”

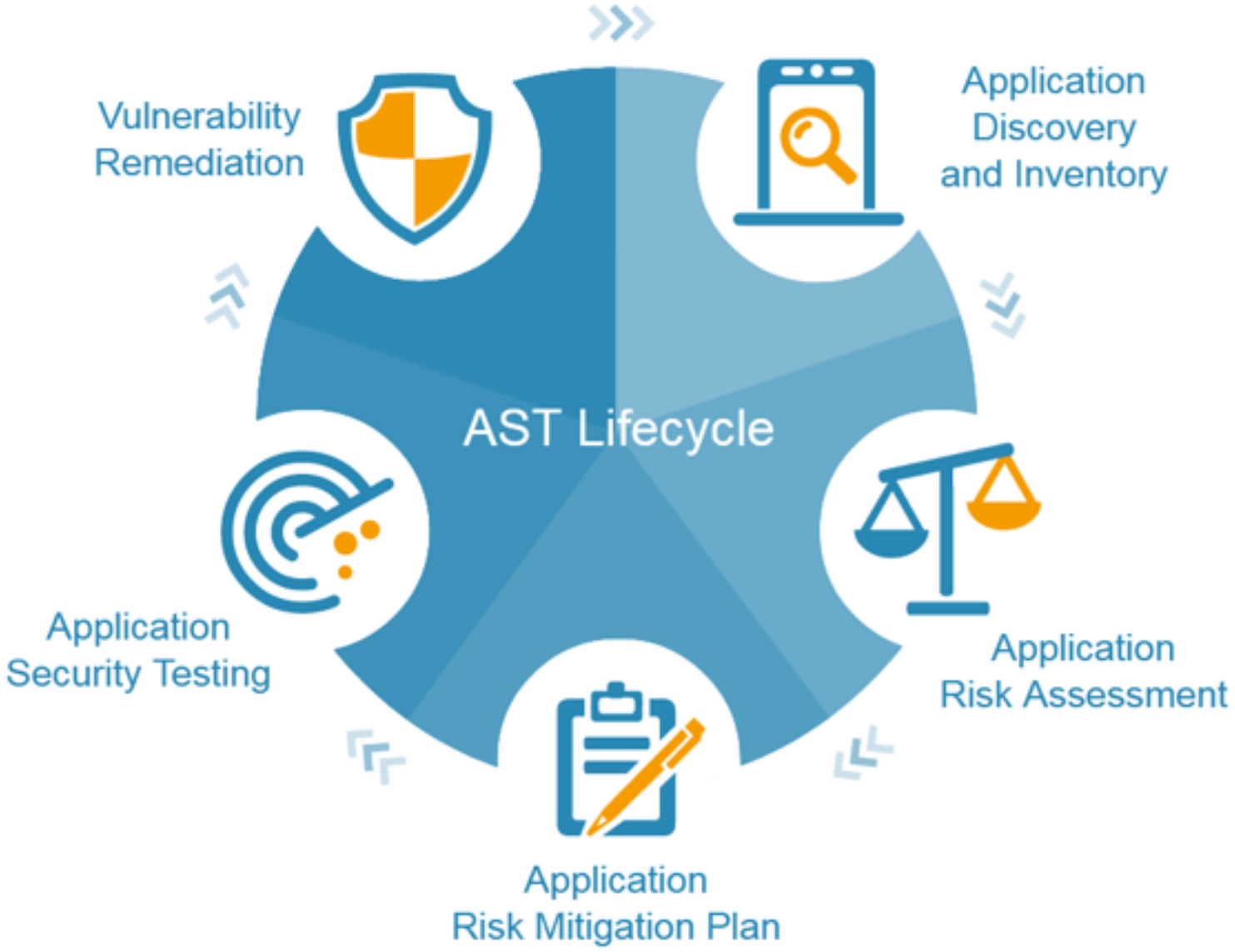
OWASP Top Ten – Overcoming the FUD



Application Security Strategy: Fundamentals

- Do we know which applications, users and data do we need to protect?
- What are the business risks attributable to our application infrastructure?
- Which compliance and regulatory requirements do we need to implement?
- Shall we use reactive, proactive or both approaches to mitigate the risks?
- Does our vendor selection process benchmark how the solution fits into our needs?
- Do we have a person responsible for every single process and procedure?
- How do we measure efficiency and effectiveness of our application security?

Vendor Neural Application Security Testing Lifecycle™



Thank you for your time!

ilia.kolochenko@htbridge.com

www.linkedin.com/in/kolochenko

www.csoonline.com/author/Ilia-Kolochenko