Presenters:

-Lucian Corlan

-Gareth Dixon

OWASP

The Open Web Application Security Project

About Me

OWASP
The Open Web Application Security Project

- Lucian Corlan
  - Currently AppSec @Sage
  - Currently Supporter of OWASP London Chapter
  - Ex-Chapter Leader @Cluj-Napoca Romania
  - Working in Security since 2006
- Gareth Dixon
  - Principal Test Engineer @Sage
  - Currently UK and Ireland Lead Security Champion
  - Currently Studying MSc (DTSS in Cyber Security)

Context

OWASP
The Open Web Application Security Project

sage

40+ Security Team

170+ Security Champions (as of March 2020)

200+ Products

50+ IT Services

8 regions

15+ countries with Tech

24 total countries

3500+ Technology personnel

Why Security Champions?
Application Security Initiative maturity

- Application Security maturity is assessed as part of a drive to increase development teams' aware ness and use of security within the SDLC. In this respect, OWASP OpenSAMM and BSIMM are used for continuous Application Security Initiative Maturity improvement.
- The Security Champions are a key element of the model.

Security Satellites a.k.a. Champions

OWASP
The Open Web Application Security Project

- What is currently available
  - OWASP Security Champions Playbook HERE
  - OpenSAMM v2 (yay!)
  - BSIMM v10
  - SAFECode guide (2019) HERE
  - […?]

What is being done?

BSIMM NUMBERS OVER TIME										
	BSIMM10	BSIMM9	BSIMM8	BSIMM7	BSIMM6	BSIMM-V	BSIMM4	BSIMM3	BSIMM2	BSIMM1
FIRMS	122	120	109	95	78	67	51	42	30	9
MEASUREMENTS	339	320	256	237	202	161	95	81	49	9
2ND MEASURES	50	42	36	30	26	21	13	11	0	0
3RD MEASURES	32	20	16	15	10	4	1	0	0	0
4TH MEASURES	8	7	5	2	2					
SSG MEMBERS	1,596	1,600	1,268	1,111	1,084	976	978	786	635	370
SATELLITE MEMBERS	6,298	6,291	3,501	3,595	2,111	1,954	2,039	1,750	1,150	710
DEVELOPERS	468,500	415,598	290,582	272,782	287,006	272,358	218,286	185,316	141,175	67,950
APPLICATIONS	173,233	135,881	94,802	87,244	69,750	69,039	58,739	41,157	28,243	3,970
AVG. SSG AGE (YEARS)	4.53	4.13	3.88	3.94	3.98	4.28	4.13	4.32	4.49	5.32
SSG AVG. OF AVGs	1.37 / 100	1.33 / 100	1.60 / 100	1.61 / 100	1.51 / 100	1.4 / 100	1.95 / 100	1.99 / 100	1.02 / 100	1.13 / 100
FINANCIAL SERVICES	57	50	47	42	33	26	19	17	12	4
ISVs	43	42	38	30	27	25	19	15	7	4
TECH	20	22	16	14	17	14	13	10	7	2
HEALTHCARE	16	19	17	15	10					
INTERNET OF THINGS	13	16	12	12	13					
CLOUD	20	17	16	15						
INSURANCE	11	10	11	10						
RETAIL	9	10								

Numbers for 122 firms such as NetSuite, CapitalOne, PayPal, Fidelity, Sony and others.

GOVERNANCE								
ACTIVITY	FINANCIAL (OF 57)	ISV (OF 43)	TECH (OF 20)	HEALTHCARE (OF 16)	IOT (OF 13)	INSURANCE (OF 11)	CLOUD (OF 20)	RETAIL (OF 9)
[SM2.3]	23	21	10	7	8	6	9	4

How many businesses employ security champions per sector.

Using the Building Security In Maturity Model v10 – security champions a.k.a. Satellite Members.

6298 Security Champions in 122 companies surveyed!

Only 10 out of 20 Tech and 9 out of 20 Cloud companies surveyed employ security champions!

OWASP
The Open Web Application Security Project

How I started as a security champion...

OWASP
The Open Web Application Security Project

GOAL for Security Champions

Support the Global Security Team in all matters related to security in your assigned area – indicative % is 10% of my time

OWASP
The Open Web Application Security Project

What do Security Champions do?

Business As usual	Building Security	Security Processes	Security Tools	Vulnerability Tracking
Take security responsibility into Business As Usual work and raise to product security team when uncertain	Participate / deliver Building Security In Maturity Model assessments / gap analysis for your area of responsibility	Learn, follow and/or adapt security process – such as Security Controls evaluation, Threat Modelling and Security Definition of Done	Learn and work with security tools/reports – static code analysis, dynamic, dependency checking, automation	Vulnerability tracking - be responsible for tracking vulnerabilities in their area and ensure they are addressed in time

Champions Meetups	Trainings & Certifications	Sage Security Portal	Collaboration	Volunteering
Attend security champions meetups for products security status and knowledge sharing	Follow security training and secure one course and/or certification	Contribute to Sage Security Portal and to existing or new security documentation	Collaborate as a local and global security champion group	Participate in applicable volunteering opportunities for security champions (e.g. Digital Defenders/STEM outreach programs etc.)

The Sage story

OWASP
The Open Web Application Security Project

SYNOPSYS®

HACKSPLAINING

PLURALSIGHT

OFFENSIVE security

>_codebashing.
by Checkmarx

SECURE CODE WARRIOR

avatao

SANS

LEARNING

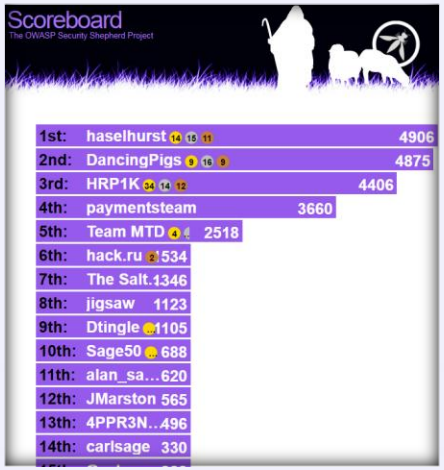
(ISC)²

CompTIA

The Sage story

OWASP
The Open Web Application Security Project

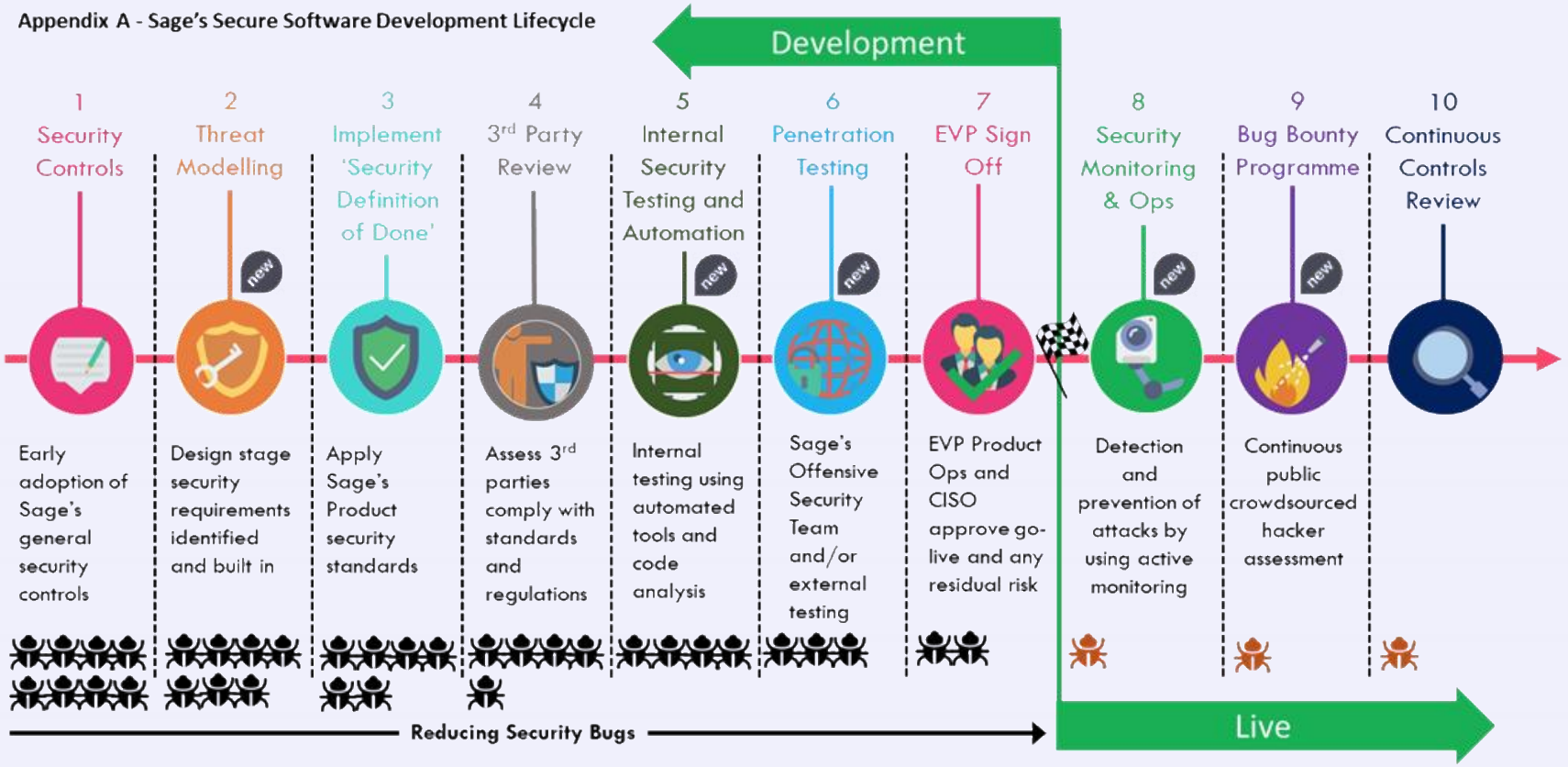
sage CTF Winner



27 teams!
1 month long event!
More than 150 people involved
Scope: UK and Ireland

The Sage story

OWASP
The Open Web Application Security Project



"Defence in Depth & Shifting Security to the Left"

Introducing…

OWASP
The Open Web Application Security Project

1. **Use of tools (Maturity levels: 1, 2, 3)**
2. **Bounty (M123)**
3. **Training (M123)**
4. **Events (M123)**
5. **Security ops (M123)**
6. **Sec Reviews / Assessments (M123)**
7. **Research (M123)**
8. **Development for security (M123)**
9. **Reporting (M123)**
10. **Threat Modelling (M123)**

Detail HERE

How to award?

Maturity one – 1 point
M two – 2 points
M three – 3 points

How to recognise?

Black belt – 15 points with 3 Maturity 3s mandatory
Green belt – 10 points with 2 M2s and 1 M3
White belt – 5 points

OWASP
The Open Web Application Security Project

Application to
Manage Security Champions
Activities / Maturity / Awards / Recognition

DEMO

Open source!

Recognition / Prizes / Swag

OWASP
The Open Web Application Security Project

Sage Coin

Vouchers, stickers and others!

Questions?

OWASP
The Open Web Application Security Project