March Community Meetup

THREAT MODELING CONNECT
POWERED BY IRIUSRISK

What does a mature security champion program look like?

March 24th | 11:00 - 12:00 ET

Hosted by:

Chris Ramirez
Principal Software Security Engineer | Axway

About me

Chris Ramirez
Principal Software Security Engineer
Axway

- With Axway since 2013
- **Prior experience:** system administrator, database developer, web developer, web application penetration tester, corporate compliance, POS systems
- **Current security certifications:** CISSP, CCSP, CISA, GWAPT, GCIH

Axway and BSIMM

- **Axway**
  11,000 customers
  100 countries worldwide

- **Key Industries**
  Banking and Financial Services
  Insurance
  Healthcare
  Energy and utilities
  Government
  Public sector

- **BSIMM**

Building Security In Maturity Model (BSIMM) is a study of current software security initiatives or programs. It quantifies the application security (appsec) practices of different organizations across industries, sizes, and geographies while identifying the variations that make each organization unique.

- **~20% of the BSIMM participants who publicly disclosed are Axway customers**

Axway's Security Program

- **Software Security Group**
  Manage the Axway SSDLC Program:
  - Secure coding training
  - Threat Modeling
  - Static Application Security Testing (SAST)
  - Software Composition Analysis
  - Attack Surface Analysis
  - Dynamic Application Security Testing (DAST)
  - Container Security Analysis
  - Security Reviews

- **Security Champions (SPOCs)**
  7 main development sites worldwide
  ~100 software products
  One primary SPOC is required per dev team
  Implement the SSDLC requirements

- **Champions.** Interested and engaged developers, cloud security engineers, deployment engineers, architects, software managers, testers, and people in similar roles who have an active interest in software security and contribute to the security posture of the organization and its software.

Observations/challenges with our implementation

- **Volunteered vs Voluntold:** SPOCs are required. If no SPOC selected, Eng Mgr by default.
- **Additional Training for SPOCs:** Blue Belt Training (Black Belt eventually)
- **Recognition/Reward:** Security Stars Program
- **Clear lines of responsibility:** Set up a RACI chart. SPOC Responsible. Mgr Accountable.
- **Clear lines of communication:** People know how to reach SSG for questions
- **Important to build a narrative:** Bring them on the security journey with you
- **Exec/Mgmt Support:** SSG is a support/advisory group. Execs accept the biz risk.

Discussion

- **Question 1:** How do you identify your champions?
- **Question 2:** What is a security champion expected to do in your organization? What are the goals for your security champion program in your organization?
- **Question 3:** What is the value of SC program to your organization? How do you measure and demonstrate the value?

Use "✋ Raise Hand" feature to let the hosts know you have something to share.