RSAC Studio

Connect to Protect

Seven Software Security Myths:
Myth Busting Security and the Dev Cycle

Gary McGraw, Ph.D.
Chief Technology Officer
Cigital
@cigitalgem

Seven Myths of Software Security

- **Building security in** is essential for modern security
- What actually holds software security back?
- Seven myths drawn from real field data gathered @cigital

Myth #1: Perimeter Security Works

An outstanding defense…in 1535

Myth #2: A Tool Will Do It ALL

When your tool finds ten bugs, who fixes them?

Myth #3: Penetration Testing is Perfect

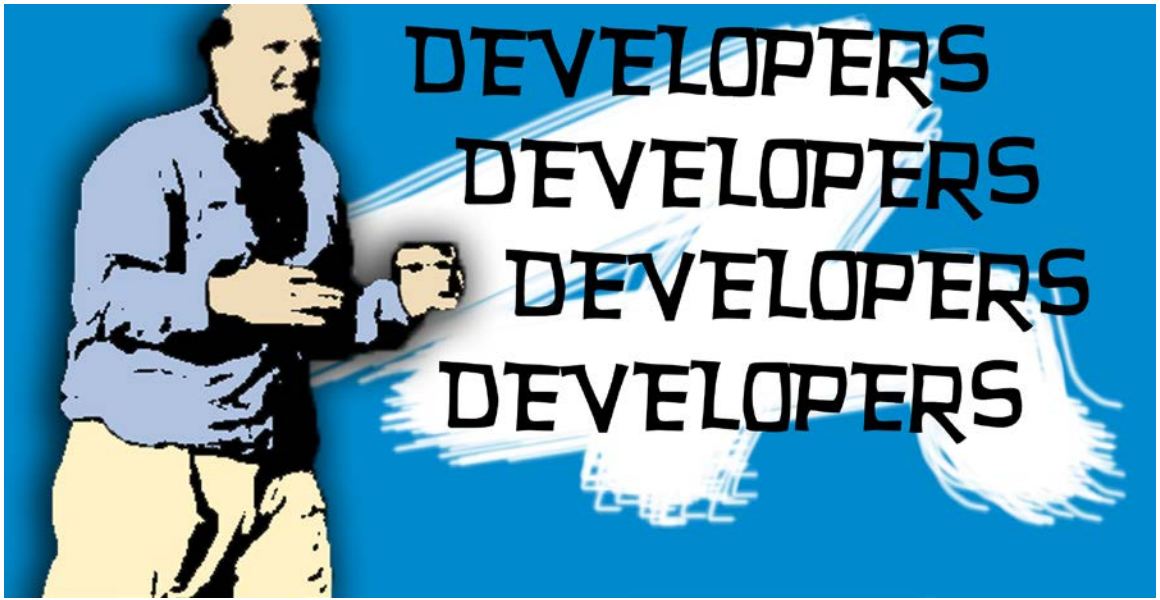
Economics shows that fixing things after they are done is dumb.

Myth #4: Cryptography is Magic

The liberal application of “magic crypto fairy dust” does not address defects.

Myth #5: Eradicate the Bug Parade

Defects come in two categories: bugs and flaws.



Myth #6: Developers Should Solve the Problem

A Software Security Group unifies security and development.

Myth #7: Focus Only on High Risk Applications

Risk management has well understood failure conditions.

What now?

BSIMM 6

- Debunk the myths in YOUR organization
- Read the original article: http://bit.ly/swsec-myths
- Get a #BSIMM measurement

Cigital
BUILDING SECURITY IN