What are the challenges in higher education?

Monica Bush
Security Engineer
Office of Campus Information Security
University of Wisconsin-Madison
Top 5 CLMs

1) <Share yours here>

2) Telling the CISO you’ll need an additional $XXX,XXX dollars to do it right

3) One-dimensional education

4) Skimming over seemingly benign Snort alerts

5) Showing developers this picture....
What is security .............. Everything is evil
University Context

• Tier 1 research institution
• 4 Class B networks
• Rich data
• Distributed development
• Mobile app downloaded in 78 countries
• PCI-DSS, HIPAA, FERPA, 45 CFR Part 46, FISMA
Measuring Maturity

- Software Assurance Maturity Model (OpenSAMM)
- Building Security In Maturity Model (BSIMM)
Change Components

• Understand change management

• Alter situations to modify behavior

• Work with what you have
An Example Applied

- BSIMM - INTELLIGENCE: Attack Models (AM1.2): “Create a data classification scheme and inventory.”

Toys: What do you have?

Web Server Numbers by Type (3065 Total)

- Apache: 1167
- IIS: 536
- Unknown: 151
- EWS: 126
- Others: 1085
Model: What do we do with it?
Change: What is your responsibility?
A Bit About the Speaker and Contact Info

Monica Bush CISSP, GWAPT
Security Engineer
Office of Campus Information Security
University of Wisconsin-Madison
mbush@wisc.edu