Threat Model Worksheet

A C P A I D R I

Δ	ct	0	rc

Who are you defending against?

Capabilities

What can they do?

Prevention

How do you stop attacks?

Assets

What are you defending?

Incentives

What can someone gain by compromising you?

Detection

How will you detect a compromise?

Response

What will you do once compromised?

Impact

What happens when you are compromised?

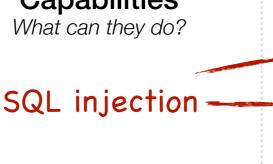
Threat Model Worksheet

My example website



Actors Who are you defending against? Script Kiddies The NSA

Capabilities







Credit card numbers

Assets

What are you defending?

Organized Crime

Email phishing links

> Implant hardware

Can't prevent

Email scanning

Incentives

What can someone gain by compromising you?

Lulz

Credit Fraud

Accounts to sell

Collect Intelligence

Detection

How will you detect a compromise?

Employee browser logging & alerts

System logs

Response

What will you do once compromised?

> Employee password reset

Who monitors these logs?

Impact

What happens when you are compromised?

Bulk password reset

Bad publicit

Breach notifications & Increased fees