Threat Model Worksheet

AIAI
CPDR

Actors

Who are you defending against?

Incentives

What can someone gain by compromising you?

Assets

What are you defending?

Impact

What happens when you are compromised?

Capabilities

What can they do?

Prevention

How do you stop attacks?

Detection

How will you detect a compromise?

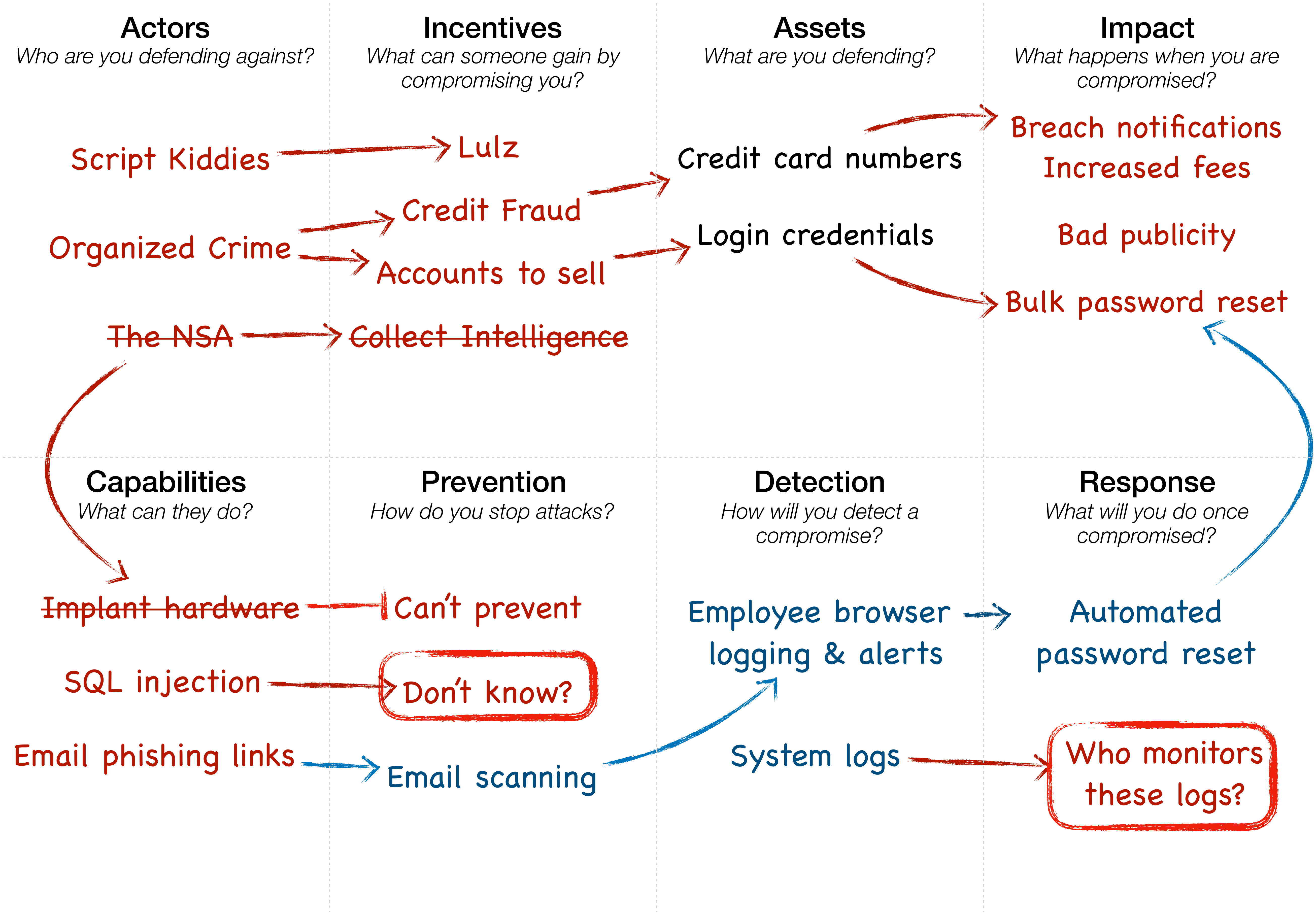
Response

What will you do once compromised?

@sweis - v4 - 27.04.18

Threat Model Worksheet

My example website



Actors

Who are you defending against?

Script Kiddies

Organized Crime

~~The NSA~~

Incentives

What can someone gain by compromising you?

Lulz

Credit Fraud

Accounts to sell

~~Collect Intelligence~~

Assets

What are you defending?

Credit card numbers

Login credentials

Impact

What happens when you are compromised?

Breach notifications

Increased fees

Bad publicity

Bulk password reset

Capabilities

What can they do?

~~Implant hardware~~

SQL injection

Email phishing links

Prevention

How do you stop attacks?

Can't prevent

Don't know?

Email scanning

Detection

How will you detect a compromise?

Employee browser logging & alerts

System logs

Response

What will you do once compromised?

Automated password reset

Who monitors these logs?

@sweis - v4 - 27.04.18