Adapting security into engineering culture!

How to make friends and influence people

Introduction!

Paul Moreno

- Pinterest Security Engineering Lead
- Focused on federating all the things
- Likes unicorns and cats

Agenda

- Building credibility instead of insisting authority
- Performing discovery before taking action
- Confrontation and compromise
- Taking advantage of incidents

Building credibility instead of insisting authority

- Low hanging fruits
  - SSO or LDAP Integration, less freakin' passwords!
  - Basic monitoring through desktop management
  - Actually fix shit, don't just find it

Performing discovery before taking action

- Passive monitoring
    - Taps are hella cheap and most switches can port mirror without hassle
    - Build a baseline off of your users behavior
- Start with simple alerts
    - Things like ssh tunnels out of the US
    - Signature based malware alerts

Confrontation and compromise

Confrontation and compromise

- Have data to back up recommendations
  - Use real world examples
  - Proof of attack or an actual compromise
- Nobody is perfect
  - Deal with it

Storytime!

Taking advantage of incidents

- Never waste a good incident
  - Heartbleed... fuck.
  - Able to prove without a doubt exploitation
- Because of incidents we have been able to:
  - Change a number of things within the stack
  - Develop an IR plan
  - Influence employees to follow an IR plan

Bringing it all back

- Build credibility instead of insisting authority
- Fix shit, no seriously
- Justification instead of arguments
- Don’t be an asshole
- NEVER WASTE AN INCIDENT!

Q&A

Contact me after the talk if you would like to hear more trials and tribulations!