WINDOWS SECURITY BASICS FOR THE SYSTEM ADMIN

It's not always easy, but it is always important

FROM THE INSIDE

TO ADMIN, OR NOT ADMIN?

- Desktops? Sure … why not?
- Laptops? Might be more work than it's worth.
- You can do more with Admins than you think!

GROUP POLICY (OU POLICY?)

- Not just for Desktop Wallpaper anymore (if it ever was)!
- Lots and lots and lots of policies.
- Things of which to be aware.
- Example

FIREWALLS (YES! PLURAL!)

- Windows Firewall
- IPSEC Rules
- (Outside) Symantec Endpoint Protection
- Differences?

BITLOCKER – EASIER THAN YOU THINK

- Requires TPM to be enabled
- Does not automatically cache recovery token

- Certificates
- Login requirements

OTHER QUESTIONS

ON THE OUTSIDE LOOKING IN

- Symantec Endpoint Protection

ANTI-VIRUS / ANTI-MALWARE

MONITORING

- Splunk
- Windows logs are noisy!
- Windows logs are ugly!
- Working on it …
- Example

INVENTORY (EXCEL IS NOT ENOUGH)

- Hardware & software
- System Center Configuration Manager
- IBM Endpoint Manager
- *NO* excuse to not be using one of these tools

- security@duke.edu
- Security Liaisons
- Duke ITSO Web Site

QUESTIONS? (AKA "WHAT'D I MISS?")