We have tools

Are they working?

by Dan Wilkins

Who am I?

- Human
  - Husband and a father of 3
  - I ride bikes (pedal)
  - I love soccer
  - I love what I do, most days
  - Went to school for computer science
- Drone
  - Worked as helpdesk tech for 4 years in private sector
  - Work with Networking and Security primarily now in the public sector

What does MDECA do

- Shared services for school districts in Montgomery, Miami and Darke county
- We provide web filtering and other IT services beyond a typical ISP
  - We also provide student services, library services, and fiscal services.

Defining Risk

- So what is Risk?
  - How often bad things are likely to happen, and how bad are they going to be when they do happen
- Probability vs. Possibility
  - Important to distinguish the difference

credit to Jack Jones

What tools do we have now?

- Firewalls
  - Protection from the outside world
- Individual firewalls for each location
  - ACLs, Firewall Service Module, etc...
- Antivirus
- IDS/IPS
- Written policies

So why do we need more tools?

- We are missing a key component in security
  - The first three relate to physical security too
    - Preventative – Firewalls
    - Deterrent – Messages stating not to log in, physical controls
    - Detective – None
  - Attack mitigation tools
    - Corrective – AV
    - Recovery – Backups

Why we need more tools (cont.)

- Sheer volume of logs being generated

- Each source has to be checked individually
  - No centralized management

What is a SIEM

- Security Information Event Manager
  - Helps detect threats
  - Consolidates data silos
  - Meets regulation mandates
  - Real time alerting

So who did we look at?

- We demoed two companies and looked at others
  - AlienVault
    - Open source components, fairly new, very pretty but slow and not as established
  - Q1 Labs
    - Rated highly by Gardner, amazing product with availability to expand
  - Others
    - HP/ArcSight, NitroSecurity

Dashboard Tab

- Quick glance of network

Offenses Tab

- Correlation of data

Log/Network Activity Tab

- Events in real time or over chosen interval

Reports Tab

- Customized reports that can be automated

Other Tabs

- Asset Tab
  - Allows you to assign names to IP addresses
  - Allows you to set weight to devices
- Admin Tab
  - Controls user access
  - Add additional log devices

So why do we care?

- We will be able to more actively alert you to issues that may arise
- It gives districts the ability to use a tool that they otherwise cannot afford

Any Questions?