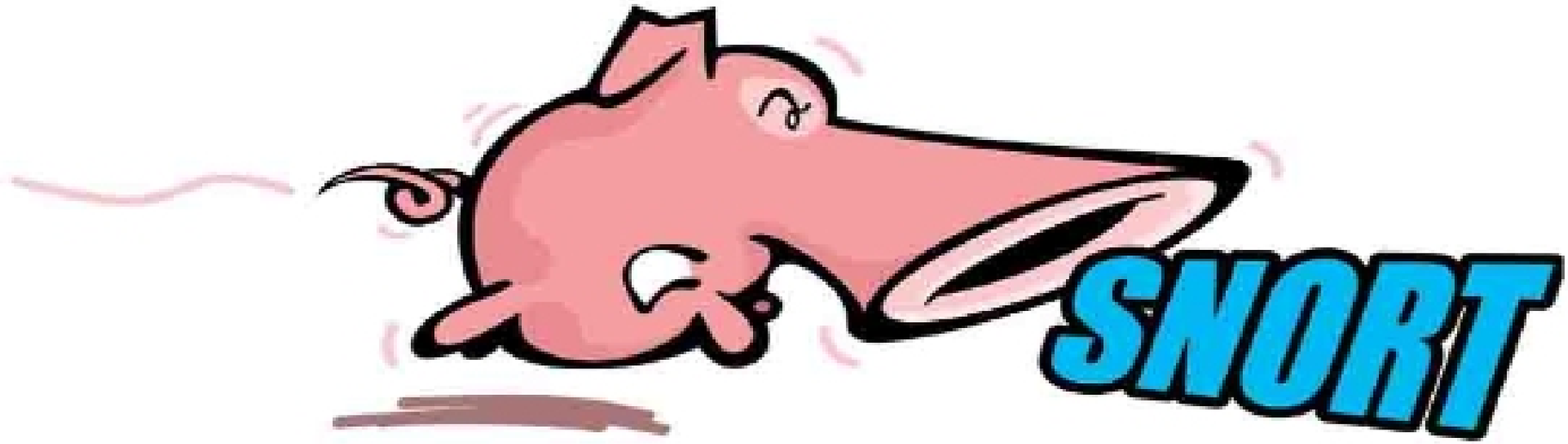


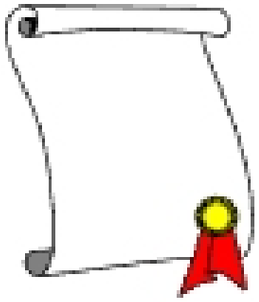
Modified slides from Martin Roesch

Sourcefire Inc.

Topics

- Background
  - What is Snort?
- Using Snort
- Snort Architecture
- Third-Party Enhancements

Background – Policy



- Successful intrusion detection depends on policy and management as much as technology
  - Security Policy (defining what is acceptable and what is being defended) is the first step
  - Notification
    - Who, how fast?

  - Response Coordination