

**SECURITY
MESSAGE
STANDARDIZATION**

MOVING SECURITY MESSAGES THROUGHOUT “THE ETHER”

**COLLABORATIVE DATA-DRIVEN SECURITY
FOR HIGH PERFORMANCE NETWORKS**

CLAIMID.COM/WESYOUNG

THE PROJECT

- Argonne Labs (DOE)
- Computer Security Incidents WG (I2)
- Research and Education Networking Information *SHARING* and Analysis Center (DougBot and GabeBot)

HISTORICALLY...

- Inter and Intra Federation Messages
 - Mailing Lists
 - IRC
 - Wiki's
- BotTracker (Unisog)
- StormWorm (there's a nanog pres somewhere on this)
- the WAM project
- ArcSight+RTIR
- FedMod

PROTOTYPING

- Requirements moving forward
 - Code needs to be modular and open!
 - Concentration on developing the relationships and standards
 - Allow the tools to be created to fit unique environments
 - Develop standard set of expectations (Creative Commons style)
- Importance of open standards
 - Well thought out, defined basic standards (IDMEF, IODEF, XML)
 - Allow for easy implementation and proprietary extensions
 - If they don't fit, FIX OR EXTEND THEM!
- Extending existing tools, RT+IR
 - Handles ACL/UI/Basic workflow
 - Mature code base (5+ years)
 - Fairly large customer base
- Why RT+IR, where does it allow the SES project to go?
 - Prioritize, index and transactional-ize security data
 - Closest thing to your inbox (replace mailing list?)
 - Automate trust based relationships

MOVING FORWARD

- Federated Meta-bases
- Large Scale (high-volume correlation)
- Integration with existing data correlation venues (SIE, ATLAS, Shadow, etc...)
- Put “Big Red” to work for security
- Global Security Backbone
- Twitter?

claimid.com/wesyoun

WHAT PROBLEM ARE YOU TRYING TO SOLVE?

- Different Organizational Policies
- Different Priorities / Goals
- Different Standards
- Different Laws
- Different Languages

claimid.com/wesyoun