Scaling Incident Response From a 1-Person Shop to a Full SOC

Moderator: Brian Carrier

Panelists: Brian Moran
Frank McClain
Rob Wallace

Part #1: Current State

- How many companies that you deal with have an official response capability?
- For those that do, what does it typically look like in terms of size and maturity?
- What caused them to setup their first team?

Part #2: Growing Pains

- When do companies start to realize they need more?
  - Visibility to determine scope?
  - Too many alerts in the backlog?
  - Missing evidence because responders aren't looking for the right things?

Part #3: Solutions

- What do you recommend when a company is just getting started?
- How to improve visibility for scoping?
- How to reduce alert backlog and prioritize?
- How to ensure evidence is being found?
- {INSERT HERE OTHER PAIN POINTS}