SOC TALK

what_iz

@bugg


Wat is SOC?

But first, for something completely different...

Red Team

- Atackers
- Hackerz
- Pen-Testers
- Bug-Bouty-ers
- APTs

Blue Team

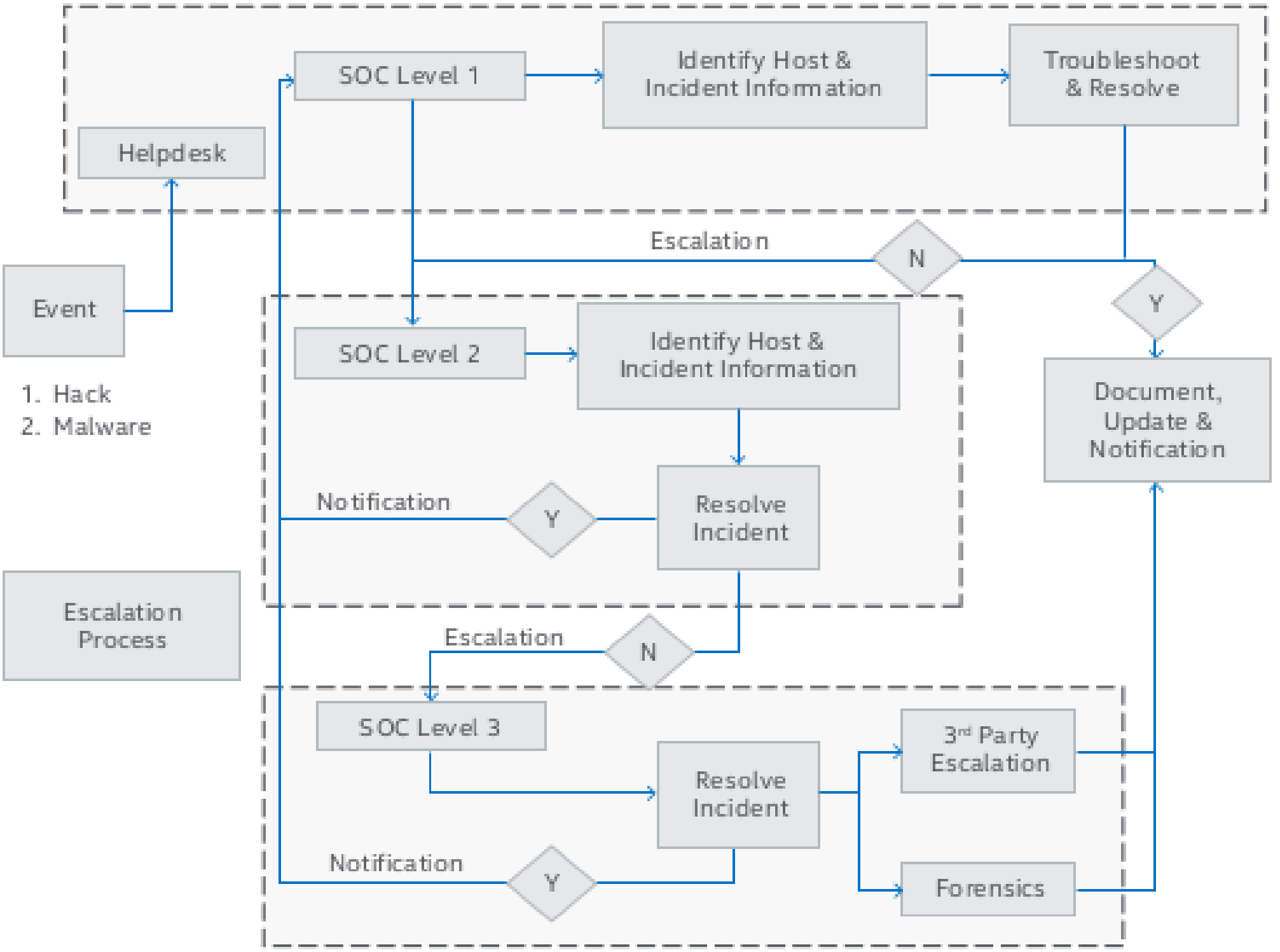
- Defenders
- Security Analysts
- Malware Researchers
- Network Security
- Sec Ops

What is a SOC?

- Where the Blue Team lives
- A Place, concentrating specialized
  - People (think YOU)
  - Tools (think software)
  - Equipment (think hardware)

People

- Tier 1 → Basic level of knowledge
  - Alert Analyst / SOC 1 Engineer / Security Analyst / etc.
- Tier 2 → Handels Escalated Incidents
  - Incident Responder / SOC 2 Engineer / etc.
- Tier 3 → Works on Advanced Threats
  - Threat Hunter / SOC 3 Engineer / Malware Reverser / Forensics Expert / etc.


SOC Level 1
Identify Host & Incident Information
Troubleshoot & Resolve
Helpdesk
Escalation
N
Event
Y
SOC Level 2
Identify Host & Incident Information
Document, Update & Notification
1. Hack
2. Malware
Notification
Y
Resolve Incident
Escalation Process
Escalation
N
SOC Level 3
3rd Party Escalation
Resolve Incident
Notification
Y
Forensics

Tools

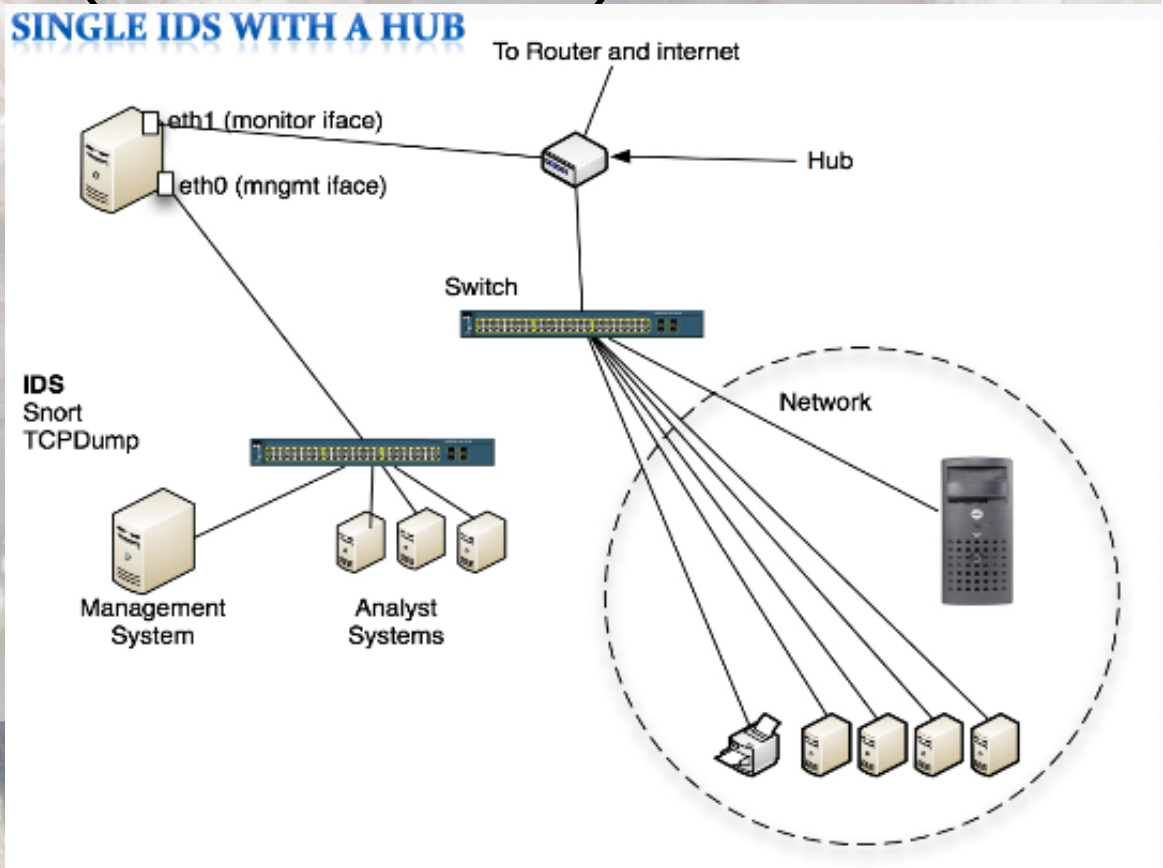
- SIEM (Security Information and Event Management)
  - The one that binds them
  - Big dashboards showing *“everything”*
- IDS/IPS (Intrusion Detection/Prevention System)
  - Directly monitors network/taps
  - Detects/Prevents bad traffic
- HIDS/HIPS (Host – IPS/IDS)
  - Directly monitors hosts
  - Detects/Prevents bad stuff (malware, etc.)
- Log Management
  - Sometimes directly part of SIEM
  - Usually integrates with SIEM (sends logs to SIEM)
- As many more as you have budget for...

Tools

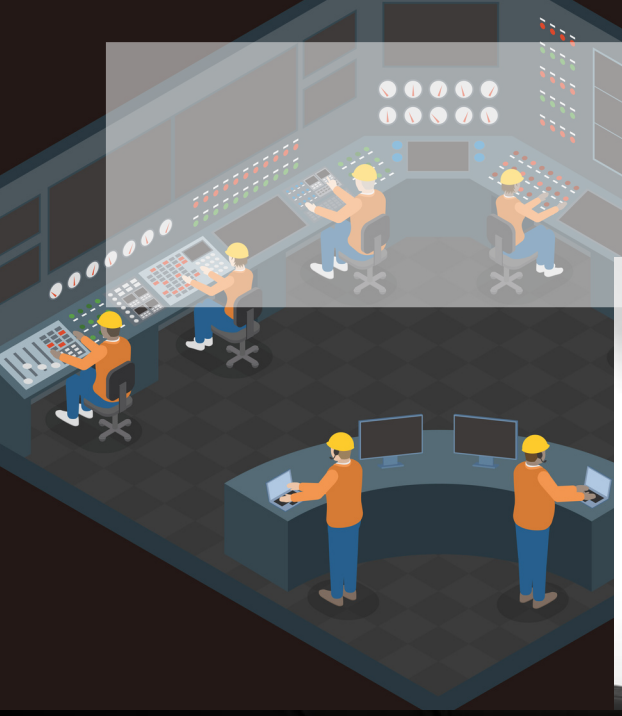
- SIEM (Security Information and Event Management)
  - Splunk
  - AlienVault
- IDS/IPS (Intrusion Detection/Prevention System)
  - Bro
  - Snort
- HIDS/HIPS (Host – IPS/IDS)
  - OSSEC
  - Defender (yes really)
- Log Management
  - ELK Stack
  - GreyLog
- As many more as you have budget for...

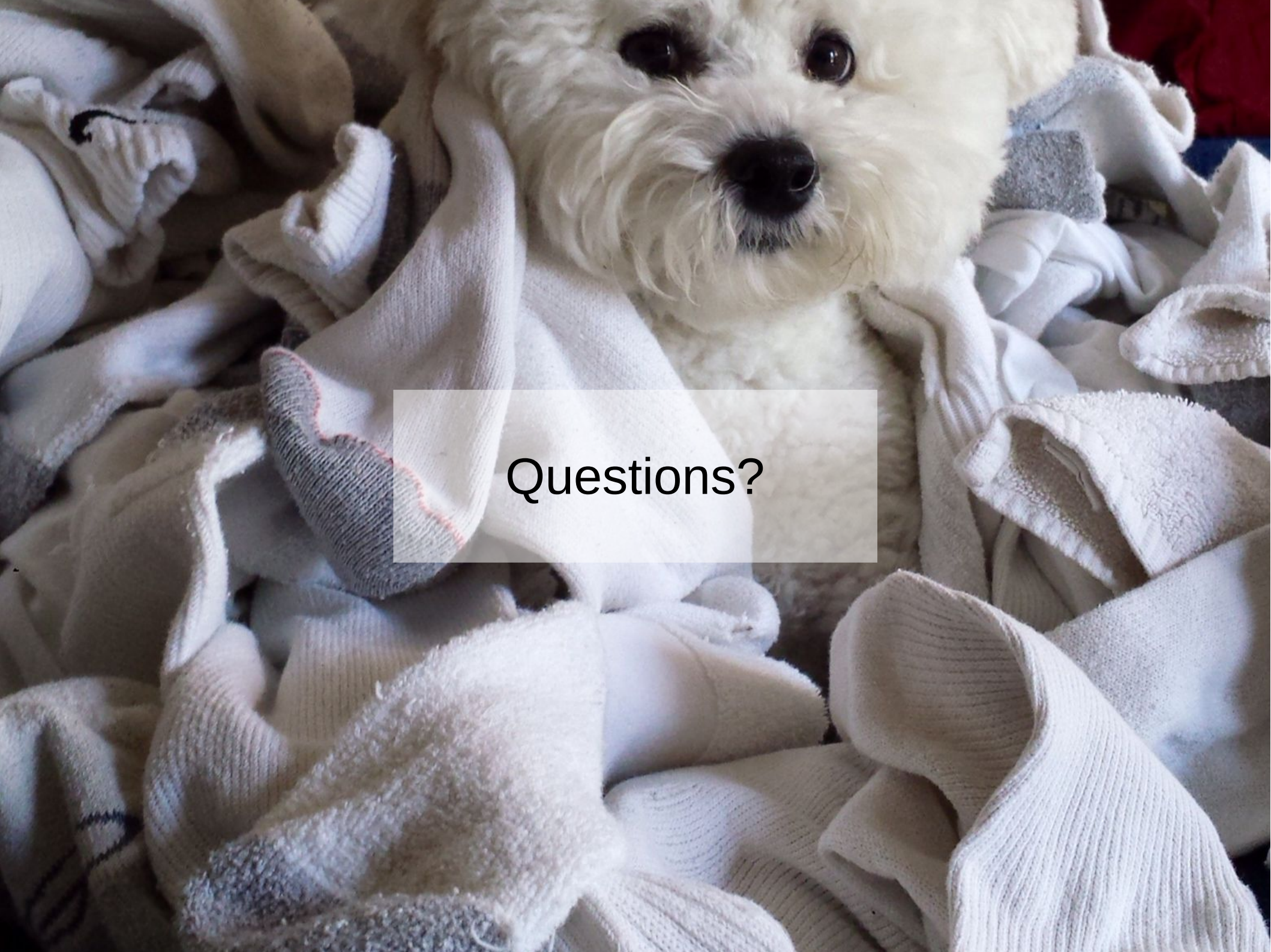
Equipment

- Desks / Chairs / Lots of pretty monitors / etc
- Protected network with Servers, Workstations
- Malware / Threat Lab (Isolated Vms)
- Network Taps



Equipment




Questions?