Breach Detection & Network Forensics

BACKGROUND

- The Enterprise Lacks Network Visibility
  - Alerts & reports are **not** network visibility
  - Logs are low fidelity & require configuration
  - Netflow is low fidelity
  - Full Packet capture is too heavy to be useful at scale
- Solution: BRO IDS (**Operationalized**)
  - Enhance data, add detections (file analysis, metadata based alerts)
  - Reassemble logs into readable, searchable flows
  - Add visualizations, natural language search & workflow
  - Solve scale issues

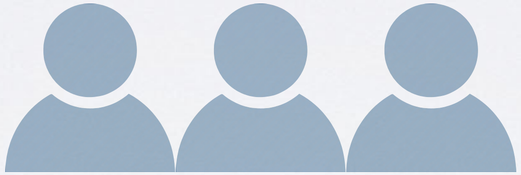
BRO @ ENTERPRISE SCALE = RSCOPE

- Clients Require Scaling to 10+ Gbps
- Reservoir Labs RSCOPE
  - Scale huge amounts of traffic on small, specialized hardware
  - Dynamic Shunting
  - Development environment
  - Test new bro scripts!
  - Research
  - Service & Tuning& Support
  - Exciting Roadmap
- A Bro-based solution that just **works**

Reduce Dollars Spent per Incident Resolved

- Dramatic reduction in time spent verifying alerts/hunting

SIEM & LOGS



45 minute average
30 hours/day
$3,000/day on IR OPEX

PACKETSLED

2 man hours per day
$200/day on IR OPEX

ALERT VERIFICATION

- Verify alerts from any alert generator
  - Was there suspicious traffic before the alert?
  - Did the machine act inappropriately after the alert?
- New threat intel
  - In my environment in the last 90 days?
- File analysis
  - Were domains or services in malware visited by this host?
  - Are those indicators on my other hosts?
- Phishing
  - Was the link clicked?

ALERT VERIFICATION

- SSH Password Guessing Alert
- Verify with logs/SIEM?
  - Do you have the logs?
  - Did the attacker delete the successful login from the logs?
    - Of course she did

PACKETS DON’T LIE

Alert Verification

What if We Could Automate?

- Synthesize the analyst’s steps in data driven decision trees
- Use dynamic data from prior stages in the next step
- Any alert, analytic, statistic, any piece of metadata can be a stage in the decision tree
- Chain disparate or low certainty events into accurate profiles of attacks

IRES

Incident Response Expert System

IRES (Incident Response Expert System)

STOP TRIAGING ALERTS,
START HANDLING INCIDENTS.*

*Requires capturing, storing and efficiently searching and viewing high fidelity network metadata

Reservoir Labs

packetsled

Questions?