Intelligence-driven Approaches to False Positive Reduction
Polling the Pain

- Who relies heavily on vendor-supplied rules?
- Who has to disposition events?
- Who has had to tune rules?
- ...and how has that worked out for you?
Step 1: Forget What You Know

- Vendor-provided rules & outsourcing security
- True Positives versus False Positives
- DBU vs RTU
- Difficulty of rule creation, management, and tuning
Let’s Be Intelligent! (Mike’s Rules for False Positive Reduction)

1. Prioritize with the Kill Chain
2. Link to actors/campaigns/intrusion sets
3. Build “stable” detections
4. Leverage first contacts
5. Favor what you know
6. Classify what you’re given
Kill Chain Crash Course

- Deterministic process
- Describes stages of a single intrusion
- “Compromise” is successful completion
- Seven opportunities to detect & defend
Classify every detection accordingly
Priority directly proportional to stage
Build workflows based on
  - Stage
  - Technique
Endow what you’ve been given
Measure your coverage
  - Count of detection, KC phase
  - Prioritize development of weak areas
Link to Campaigns

- Understanding adversary adds context
- Classify detections based on campaign
- Prioritize based on
  - Your threat landscape
  - Whether attribution is known
- On new detections:
  - Seek campaigns with no detections
  - Measure count per KC phase for each campaign
  - Build to weaknesses
Qualifies actions on detections
Prioritizes response
Side-steps “fidelity folly”
ALL detections should have an assigned maturity
Experimental Detections

- Under active development
- Are unproven
- High or unknown FP rate
- Unlikely to include TP
- Do not drive any response actions
Functional Detections

- Partially mature
- May include TP
- Often stimulate some response:
  - TP results in intrusion analysis
  - FP results in rule tweaking
- “Burn-in” before next evolution
- Abandoned if constant maintenance required
Stable Detections

- Near-zero FP rate
- Fully mature detections
- Require little to no maintenance
- Always stimulate some response
- Indicators, detections now in **Mature** state
Inform

- Construction of new detections
- Existing composite detections

- Not indicative of intrusion
- May in aggregate indicate intrusion
- Add semantic meaning to activity
Pulling the Models Together

Priority of detection = Distance from (0,0,0)
Mike’s requisite controversial statement:  
*False Positives are worse than False Negatives!*

- FPs desensitize analysts
- Accepting FNs to reduce FPs increases confidence
- Start with specific
  - *Why not* build a signature specific to what you absolutely know?
- Slowly open aperture
- Stop when FP rate too high
First Contact

- Is informational
- Notifies of new events
- Identifies detection candidates
- Only fires once
- Is constrained
  - “IDS events”
  - “AV detections”
First Contact Example

IDS Event

Add to list

New? Y

New IDS Event Detected

Analysis

Build EXP correlation rule

Add to STB IDS Event List

No Action

Previously-seen

useful on its own

useful in context
Detection Favoritism

- All detections **NOT** created equal!
- Your intel >> Others’ intel
  - Higher confidence
  - Specific to YOUR threat landscape
  - Availability of contextual data
  - Knowledge of next steps / “so what?”
- Mature shops rely on internal more than external
  - Strive for this!
Classify What You’re Given

- Detection + context = intelligence
- Turn external detections into intelligence
- Do not accept blindly what’s given to you
- Manually vet, or de-prioritize
- Discard detections without context

*External intel without context is just data*
How do I get there from here?

- **START NOW!**
  - Begin with new detections
  - Prioritize context over no context
  - Approach iteratively
  - Endow existing rules as detections fire
    - Re-write sigs
    - Leverage SIEM: Build rules around sigs
- Work through old incidents
- Leverage detection names to add context
- Rely on first contact lists
Let’s Be Intelligent! (Mike’s Rules for False Positive Reduction)

1. Prioritize with the Kill Chain
2. Link to actors/campaigns/intrusion sets
3. Build “stable” detections
4. Leverage first contacts
5. Favor what you know
6. Classify what you’re given
If you get nothing else from my presentation, please take away this:

**Ultimately, we should be dispositioning intrusions, NOT events.**

Thank you!

(e) mike@cloppert.org
(t) @mikecloppert