
ENGINEERING
TEXAS A&M UNIVERSITY


TEXAS A&M ENGINEERING
EXPERIMENT STATION

# Arming SecOps with a Special Forces Targeting Process

Andrew Stokes

@_andrewstokes

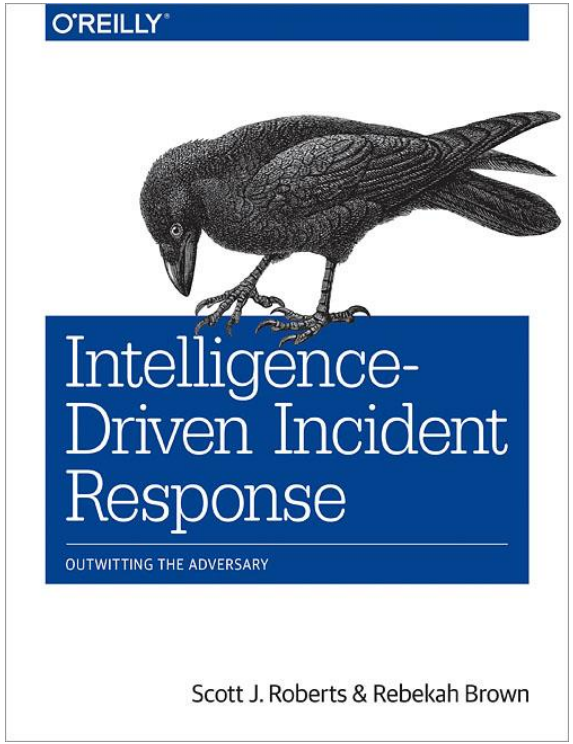
# Who Am I

- Andrew Stokes, @_andrewstokes
- Information Security Officer @ Texas A&M Engineering
- 12+ Years in Enterprise IT and Security Operations
- U.S. Marines, Operation Iraqi Freedom, Fallujah

# Inspiration

Scott Roberts & Rebekah Brown

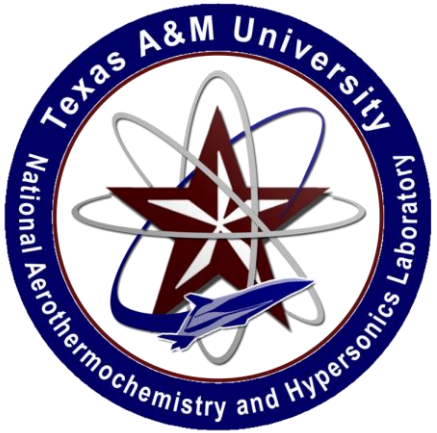
*Intelligence Driven Incident Response*



# Environment

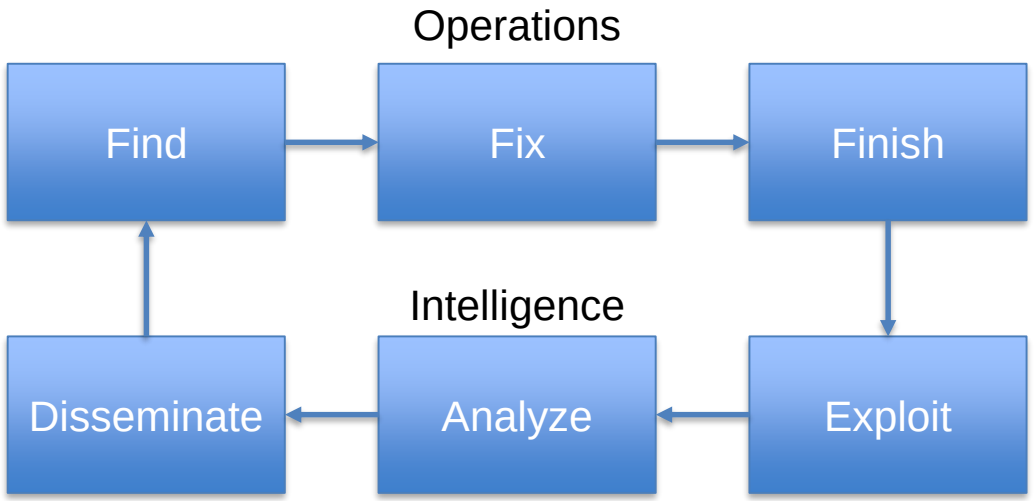
- Tier I Research Institution
- DoD and DoE Contractor
- Large and complex environment
- Many different missions
- Targeted research
- CUI, PCI, HIPAA, GDPR, ITAR, EAR, FERPA
- Academic Freedom





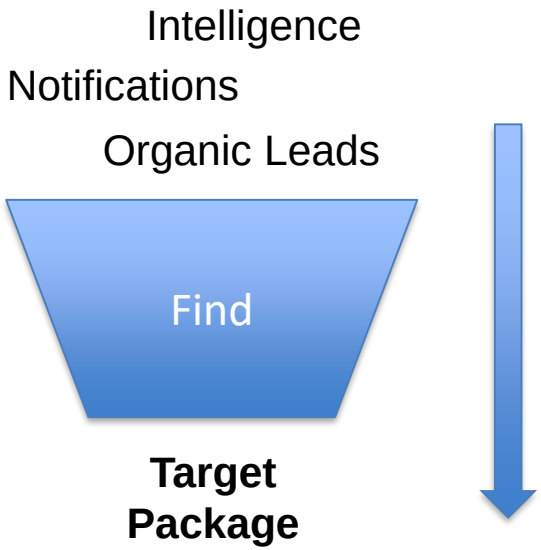

# F3EAD

- Intel from ops improves future ops
- Used by U.S. SF for targeting
- A process and a mindset



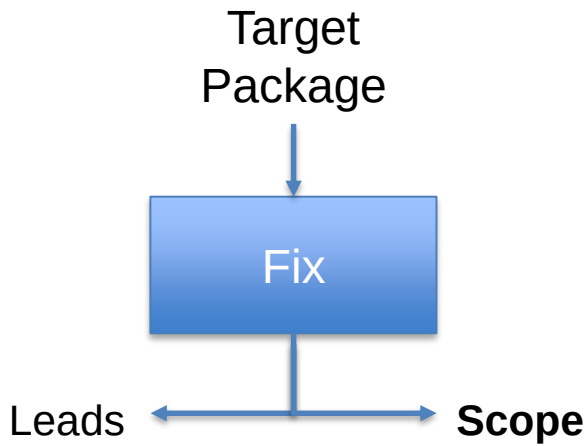
# Find: Identify the Target

- Who are we looking for?
- What do they look like?
- Start with notifications
- Prioritization is key
- QC Notifications
- Develop and improve sources
- Aim for highest value indicators
- MITRE ATT&CK Navigator



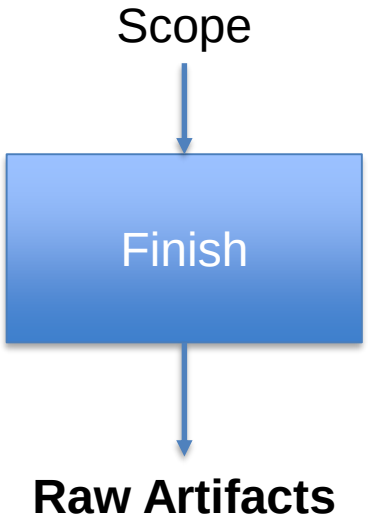
# Fix: Locate the Target Position

- OpSec
- Create detections and leverage the SOC
- Survey using EDR and network telemetry
- Scope
  - Target positions / assets affected
  - Target capabilities
  - Initial access method
  - Target objectives
- Get unrelated leads out of the way



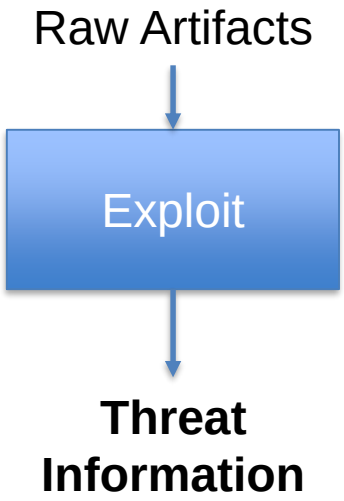
# Finish: Neutralizing the Target

- OpSec
- Make a plan
  - Mitigation
  - Prevent re-entry
  - Containment
  - Eviction
- Execute
- Report



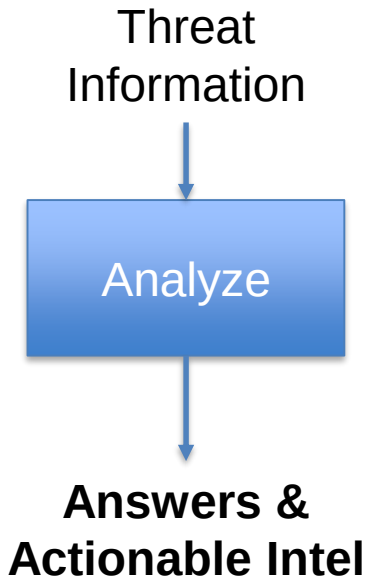
# Exploit: Collecting Additional Information

- Tailor response processes to support collection
- Make this a part of closing an incident
- Capture infrastructure data quickly
- Automate when possible
- Important for the analysis phase
- Use a standard, even if it's your own



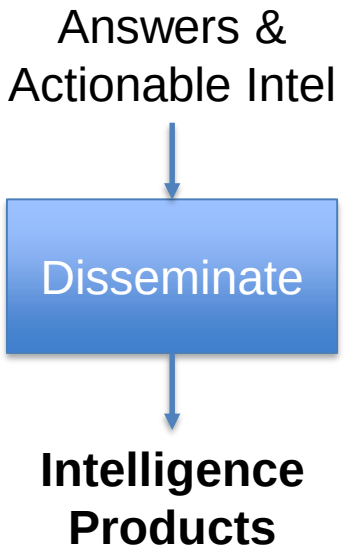
# Analyze: Creating Intelligence

- Goal: Reduce uncertainty about threats
- Start simple
- Use a standard set of intel requirements
  - What was the adversary's objective?
  - How could the attack be prevented?
  - How can we detect this adversary?
  - Have we seen this adversary before?
- Involve the team in Devil's advocate rounds



# Disseminate: Sharing Intelligence

- Consumer Priority
  - Yourself/Defense
  - SOC
  - CISO
  - Community
- Be mindful of creating demand
- Focus on clarity and consumer value
- Short stories for the CISO/CIO



# Conclusion

- Ops first, then intel
- Focus on improving lead quality vs. quantity
- Let junior analysts test drive intel analysis
- F3EAD is not only a process, it’s a mindset
- Helps prevent rabbit trails
- Increases organizational visibility and value
- Continuously improve and sensibly automate


ENGINEERING
TEXAS A&M UNIVERSITY


TEXAS A&M ENGINEERING
EXPERIMENT STATION

Questions?