Organized Threat Hunting

Christopher Crowley
@CCrowMontance
All Rights Reserved
All Wrongs Reversed
Can’t You See I’m Hunting Here?

• Last year, Bamm Visscher said he expected to see more camouflage. I expect more blaze orange.

• So, I’m just riding along (JRA) in the Frederick Watershed...
Can’t You See I’m Hunting Here? Lessons Learned

• The unknowing ruins hunting for hunters
• Mixed-use areas where hunting is occurring results in conflict and danger
• Adversary may already be in position to hunt
• Yelling at the person with the gun isn't smart
Just because you're avant garde, doesn't mean you're going to survive or prosper.

It could be that the purpose of your life is only to serve as a warning to others. (tm Despair, Inc)
MGT517 is my expression of how to align all functions of security operations

- Presentations today will dig into technical hunting details
- Common refrain, “Operational output is a requirement"
- I'm here to explain a system that will make this happen
SOC - Functional Areas

• Steering Committee
• Control Center
• Network Security Monitoring
• Threat Intelligence
• Incident Response
• Forensics
• Self Assessment
SOC - Functional Areas

- SC, CC, NSM, TI, IR, FOR, SA
- Where does "hunting" belong?
  - Everywhere
SOC - Process Elements

- Inputs
- People
- Technology
- Process
- Artifacts
People – Train in Hunting

• Threat hunting task: know and apply the way, weather, terrain, leadership, and discipline

• Require threat hunting from staff
  • Assigned task, allocate time (2 hrs/week)
  • Artifacts: detections, methods of hunting, scripts, rules for detection systems, use cases
Process - Hunting

Network Security Monitoring

Honeypots

High value indicators

Network IDS

Wireless IDS

Host IDS

Malware Detonation

SIEM of some kind

Data for correlation

Provide alerts

Long-term analysis

Data mining

Study of interaction

Historical assessment with new IOCs

Full PCAP

Raw data for correlation and confirmation

Network Logs

Host Logs

Application Logs
Process – historical assessment with new IOCs

- IOCs, TTPs: pick your flavor, pick your weapon
- Assess at the *half-life* of data
  - You have 30 days full PCAP?
  - Run historical assessment every two weeks
Summary

• Hunting isn’t new
• Organized program for hunting is the most effective
• Security Operations requires complex data interchange
• Carefully mix hunting into your operations

• Twitter: @CCrowMontance
• This presentation: https://bit.ly/crow-th