INVESTIGATING CYBER TERRORISM AJU 447 / AJU 6647

Mississippi College
A CHRISTIAN UNIVERSITY

Cyber Threat Hunting

vs.

Incident Responses

SANS Threat Hunting & Incident Response 2016

Keynote: Threat Hunting as a Culture (HaaC)

By Ben Johnson
Published on Apr 15, 2016

Threat Hunting as a Culture (HaaC): Moving Your Cyber Defenses Towards an Aggressive, Proactive Style

SANS Digital Forensics Incident Response

KEY POINTS

- Hunt the insider
- Move from response model to continuous scanning/recording
- Efficiency is the key

INCIDENT RESPONSE VS. HUNTING

Incident Response

- Response to a cyber threat
- Reactionary
- Location & teams may vary

Cyber Threat Hunting

- Looking for the threat before it happens
- Pervasive
- Location & teams more consistent

INCIDENT RESPONSE AND HUNTING

PREPARATION

- Risk Assessment
- Personnel / Teams
- Tools
- Plans
- Tactics
- Communication
- Logistics
- Training

INCIDENT RESPONSE AND HUNTING

Military Framework to Cyber Threat Intelligence (F3EAD)

- **Find** - bad actor/malware
- **Fix** – location of bad actor/malware
- **Finish** - contain or eradicate threat
- **Exploit** – Acquire intelligence and data
- **Analyze** – trends, bad actors, tactics, after-action reports, etc.
- **Disseminate** – Communicate with team, C-suite, & stakeholders

Incident Response and Hunting

OUTCOMES

- Contain and/or Eradicate Threat
- What are the gaps (security, response, equipment, Deploy and decay etc.)
- What are the strengths (personnel, equipment, tools, etc.)
- Where to hunt or search for
- What to hunt or search for
- What is the threat landscape

ASSIGNMENTS

1. **Research paper OUTLINE due April 12, 2018 – (10%)**
2. **No Class on April 12, 2018: MC Cyber Security Summit**
3. **Research paper due April 24, 2018**
4. **Final Exam on May 1, 2018**