How to Turn Your Security Operations Center Into a

THREAT HUNTING
“TOUR DE FORCE”
Meet the Presenter

Joe Moles
VP Customer Security Operations

@flyingmonkey127
joe@redcanary.com
What We’ll Cover

- Define and scope team directive
- People, process, and technology
- Building a new team vs extending/converting an existing team
- Overcoming the unique challenges of managing a threat hunting team
Your mission, should you choose to accept it...
Define Directives

- Organization risk and threat profile
- Strategic intelligence
- Specific attack type, technique, or actor
- MITRE ATT&CK™
- Kill Chain
- Focus on choke points created via preventive controls
- Validate controls, visibility & viability of detection concepts
People + Process + Technology
Threat Hunting Maturity Model

- **HMM 0 Initial**
  - Relies primarily on automated alerting
  - Little or no routine data collection

- **HMM 1 Minimal**
  - Incorporates threat intelligence indicator searches
  - Moderate or high level of routine data collection

- **HMM 2 Procedural**
  - Follows data analysis procedures created by others
  - High or very high level of routine data collection

- **HMM 3 Innovative**
  - Creates new data analysis procedures
  - High or very high level of routine data collection

- **HMM 4 Leading**
  - Automates the majority of successful data analysis procedures
  - High or very high level of routine data collection
Aspects of Technology

Visibility

- Sources that match mission
- Retention
- Accessibility
- Level of effort

Analysis

- Correlation
- Analytics
- Feedback
  - Suppression
  - Automation
process

noun

1. a series of actions or steps taken in order to achieve a particular end
It Takes a Team
...threat hunters must be dedicated to actively pursuing adversaries. These defenders add the most value when they are fixated on true threats and not restricted to responding to alerts or network maintenance issues such as patching vulnerabilities.

SANS Whitepaper, Robert M. Lee and Rob Lee
Threat Hunters Assemble:

Skills + Knowledge + Interest
Herding Cats Who Chase Squirrels
The Right Balance

- Balance various candidate aspects and skills
- Maintain focus and still be creative
- Keep the org flat
- Give everyone the opportunity to contribute to all the things
- Consider practices model to encourage leaders among equals
Variety in Hires

- Identify candidates that fill a niche or skill gap
- Multiple levels of experience
- Different career goals and growth interests
Operational Practices

- Areas of focus that improve operations
- Opportunities for growth — laterally
- Practice leads are responsible for direction and accountability
How This Looks in Practice

- Detection Engineer vs SOC Analyst
- Balance Toiling
- Practices
  - Intel
  - Engineering
  - Detection
  - Analysis
Q & A

Threat Hunting Resources:
redcanary.com/threat-hunting