
How to Turn Your Security Operations Center Into a
THREAT HUNTING "TOUR DE FORCE"
red canary

Meet the Presenter

Joe Moles

VP Customer Security Operations

@flyingmonkey127

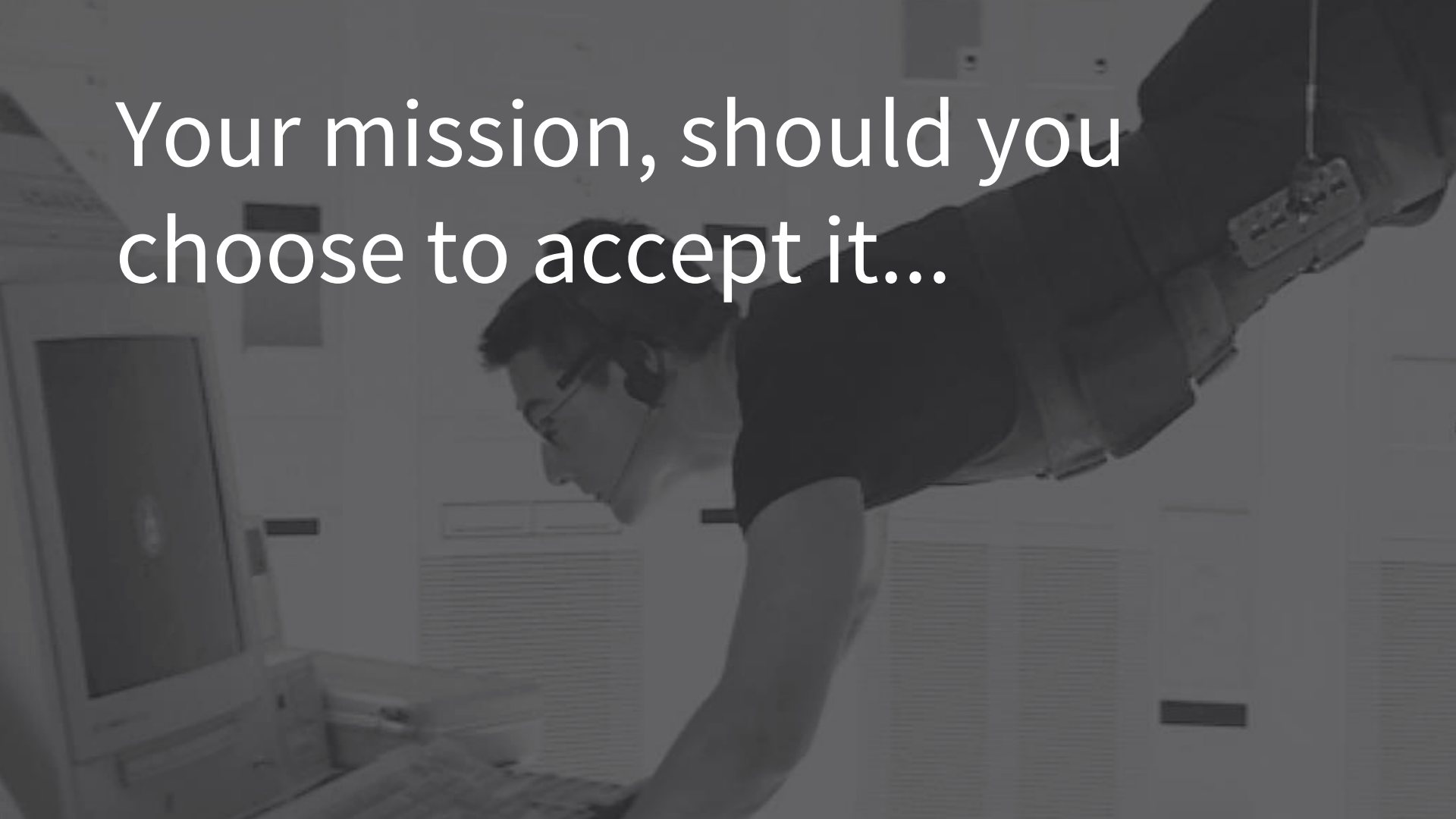
joe@redcanary.com

red canary

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

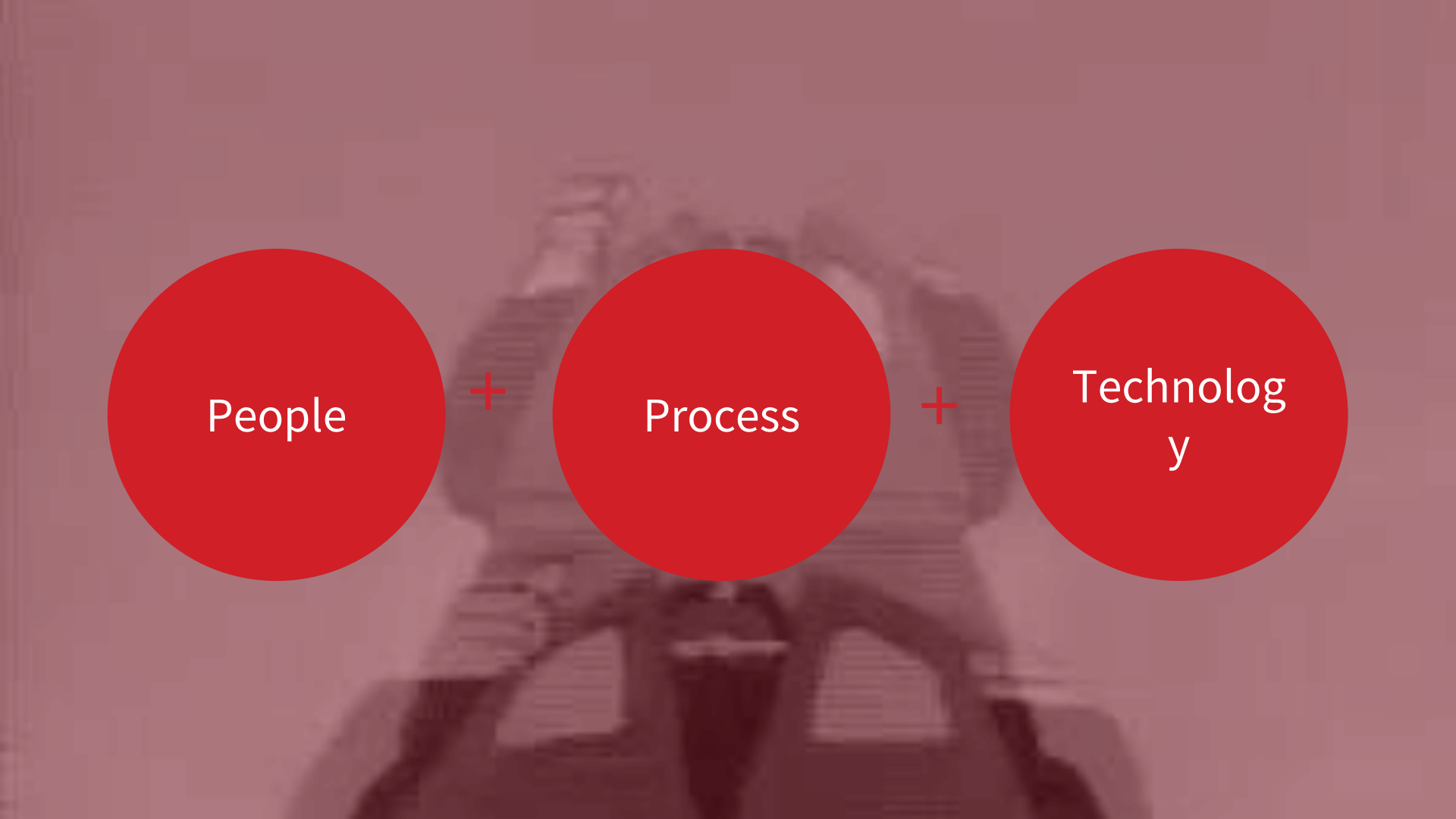
red canary


Your mission, should you
choose to accept it...

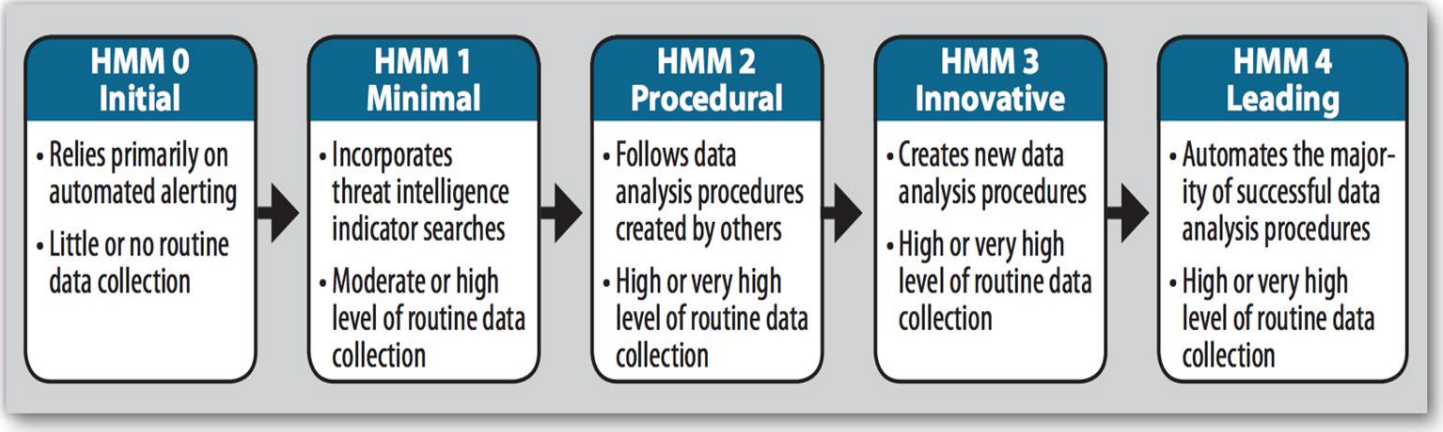
Define Directives

- 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

red canary


People
+
Process
+
Technolog
y

Threat Hunting Maturity Model



red canary

Aspects of Technology

Visibility

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

Analysis

- Correlation
- Analytics
- Feedback
  - Suppression
  - Automation

red canary

proc·ess

noun

1. a series of actions or steps taken in order to achieve a particular end


It Takes a Team
red canary

> “...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.”

The Who, What, Where, When, Why and How of Effective Threat Hunting
SANS Whitepaper, Robert M. Lee and Rob Lee

red canary

Threat Hunters Assemble:

red canary

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

red canary

Variety in Hires

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

red canary

Operational Practices

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

red canary

How This Looks in Practice

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

red canary

Q & A

Threat Hunting Resources:
redcanary.com/threat-hunting

red canary