RSAC Studio

CHANGE

Challenge today's security thinking

10 Tips for Running an Effective SOC - BuzzFeed Style

Jeff Caplan

V-SOC Operations Manager
Foreground Security
@lupine313

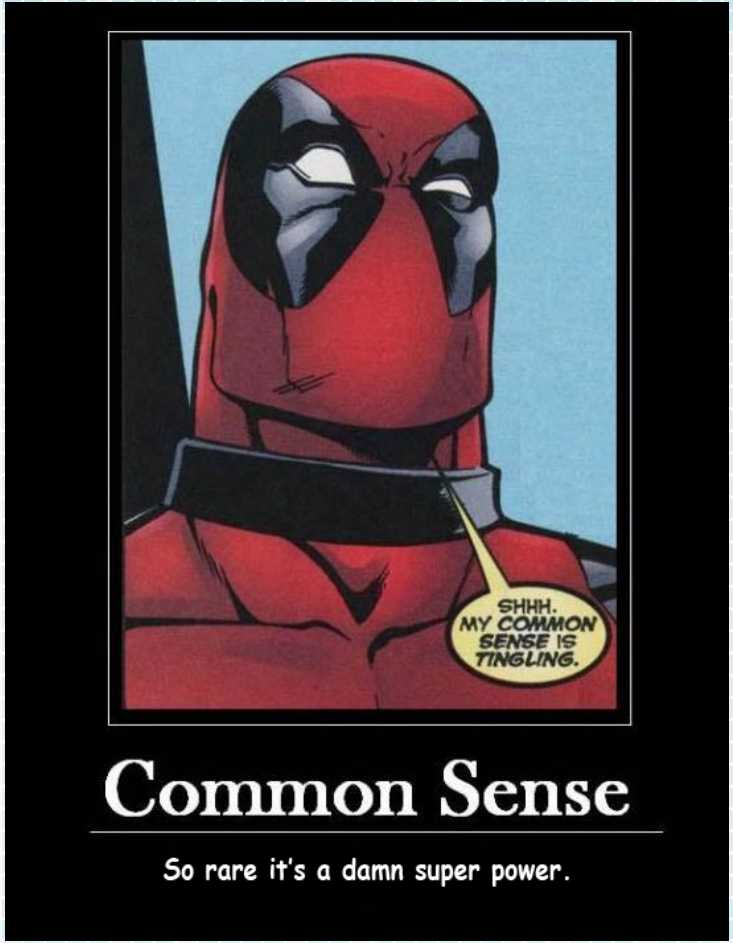
Effective you say?

- Minimize Operational Risk & Downtime
- Find Evil
- Respond to Incidents in a Timely Fashion
- Support GRC (Governance, Risk Management & Compliance)
- Provide “Value”

((Your Executive Board))

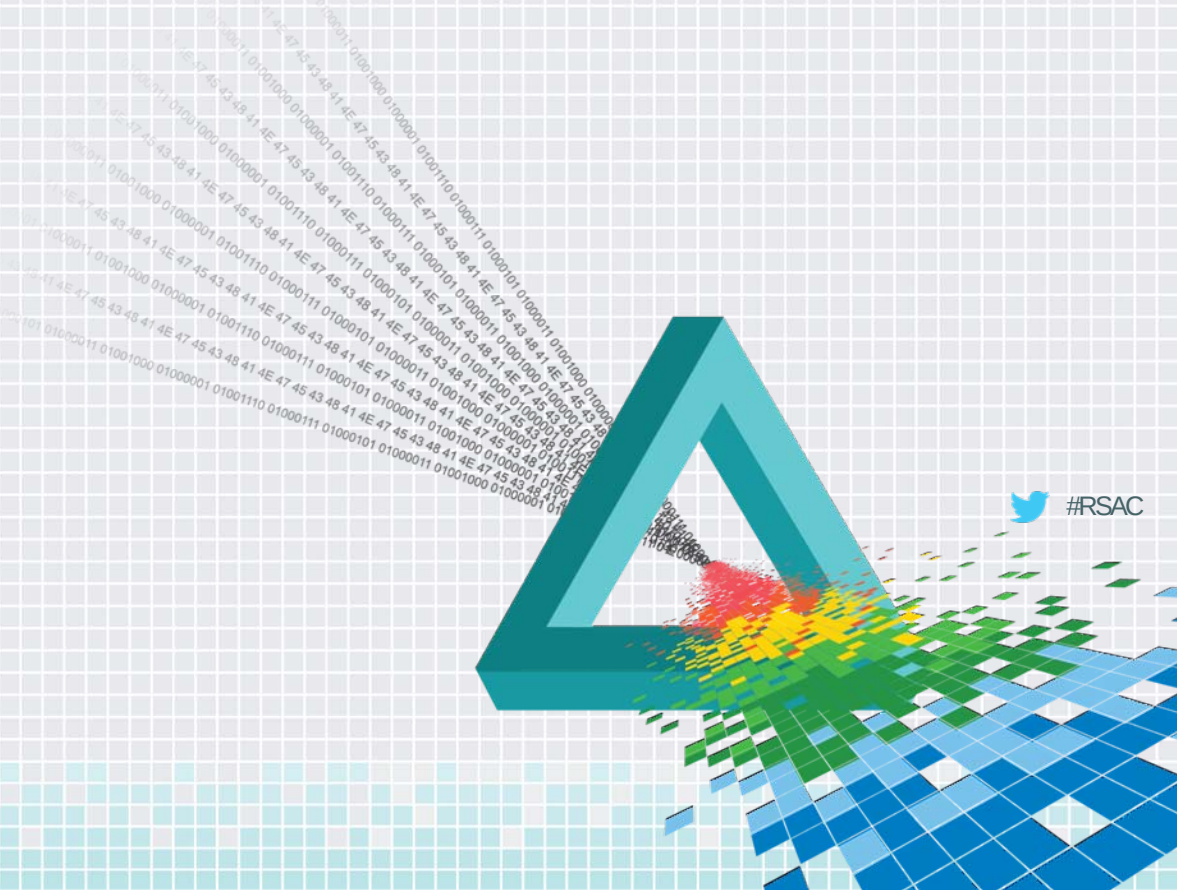
Tips you say?

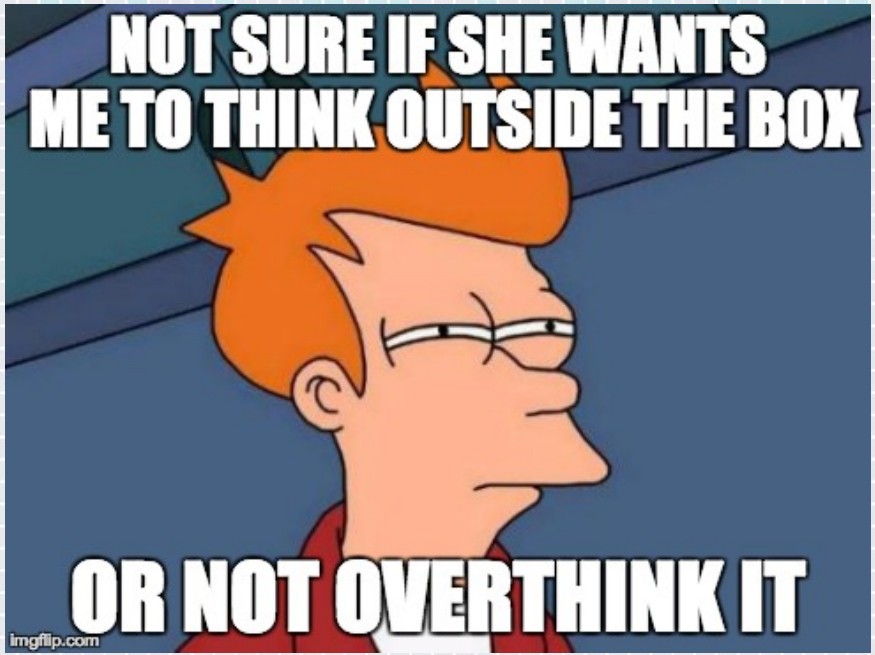
- Common Sense
- Experience
- Solid Management Strategies
- Secret Sauce (shhh!)



RSAC Studio

The List...



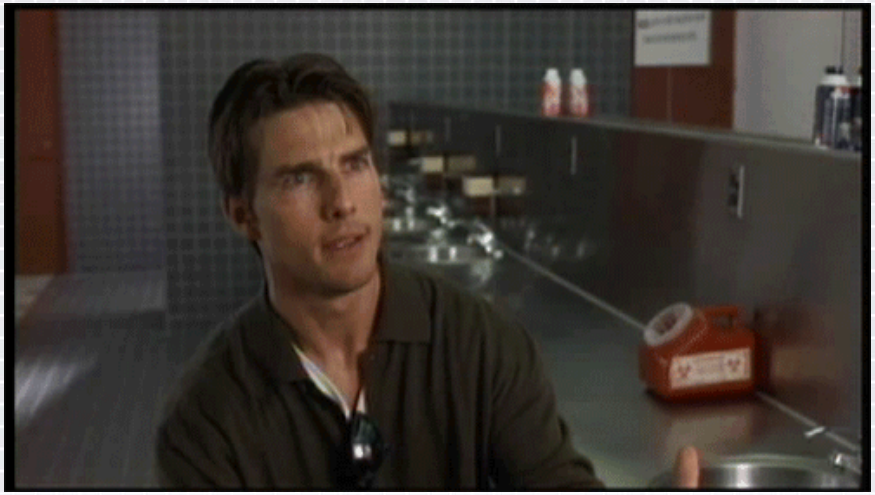

NOT SURE IF SHE WANTS
ME TO THINK OUTSIDE THE BOX
OR NOT OVERTHINK IT
imgflip.com

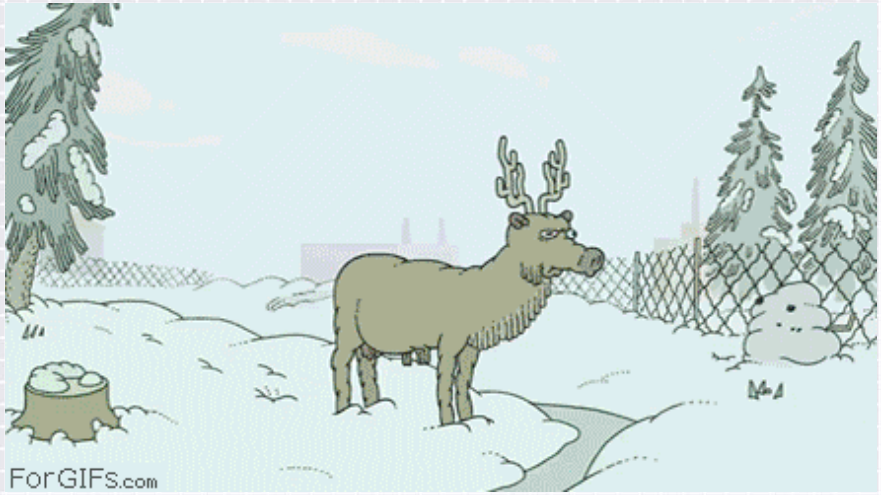
#1. Hire Smart

#2. Practice Incident Suppression

#3. Visibility is KEY

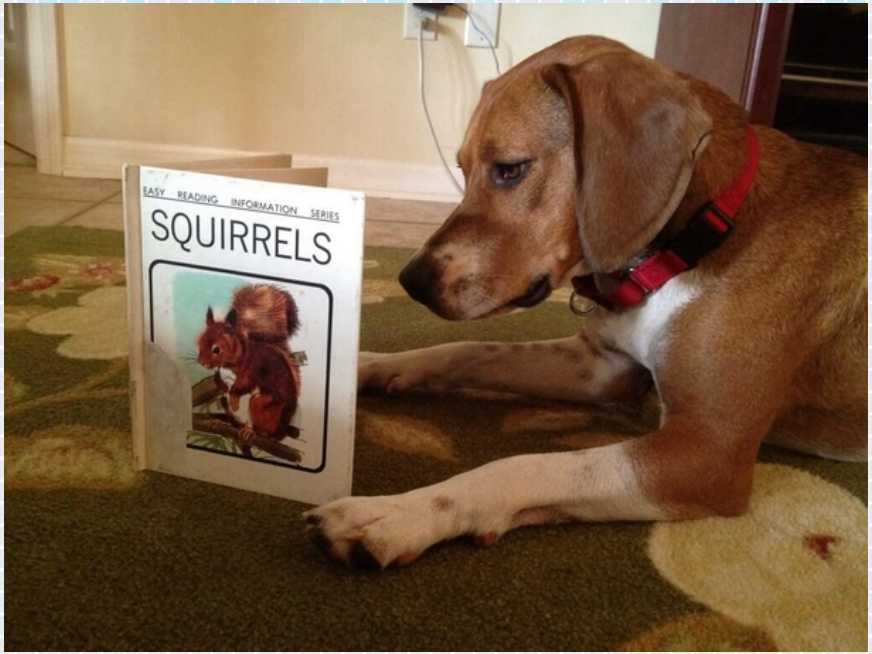
#4. Take *and Review* Notes





#5. Manage Up + The Power of Pretty!

#6. Evaluate & Apply Threat Intelligence



#7 Promote a Hunting Mindset

#8. Engage Your Team Daily

#9. Practice, Practice, Practice

#10. Communicate Effectively

Apply Liberally

- Easy Stuff:
  1. Reconsider your recruiting strategy.
  2. Implement a performance-based incentive program for your analysts or content creators.
  3. Annotate and/or take notes & ***review regularly***!
  4. Identify/evaluate all sources of threat intelligence.

Apply Carefully

- Harder Stuff:
  1. Perform a visibility assessment for your organization.
  2. Practice your IR plan - from cradle to grave.
  3. Put together a *really pretty* report template for upper management. Ensure it includes useful metrics.

Thank you!