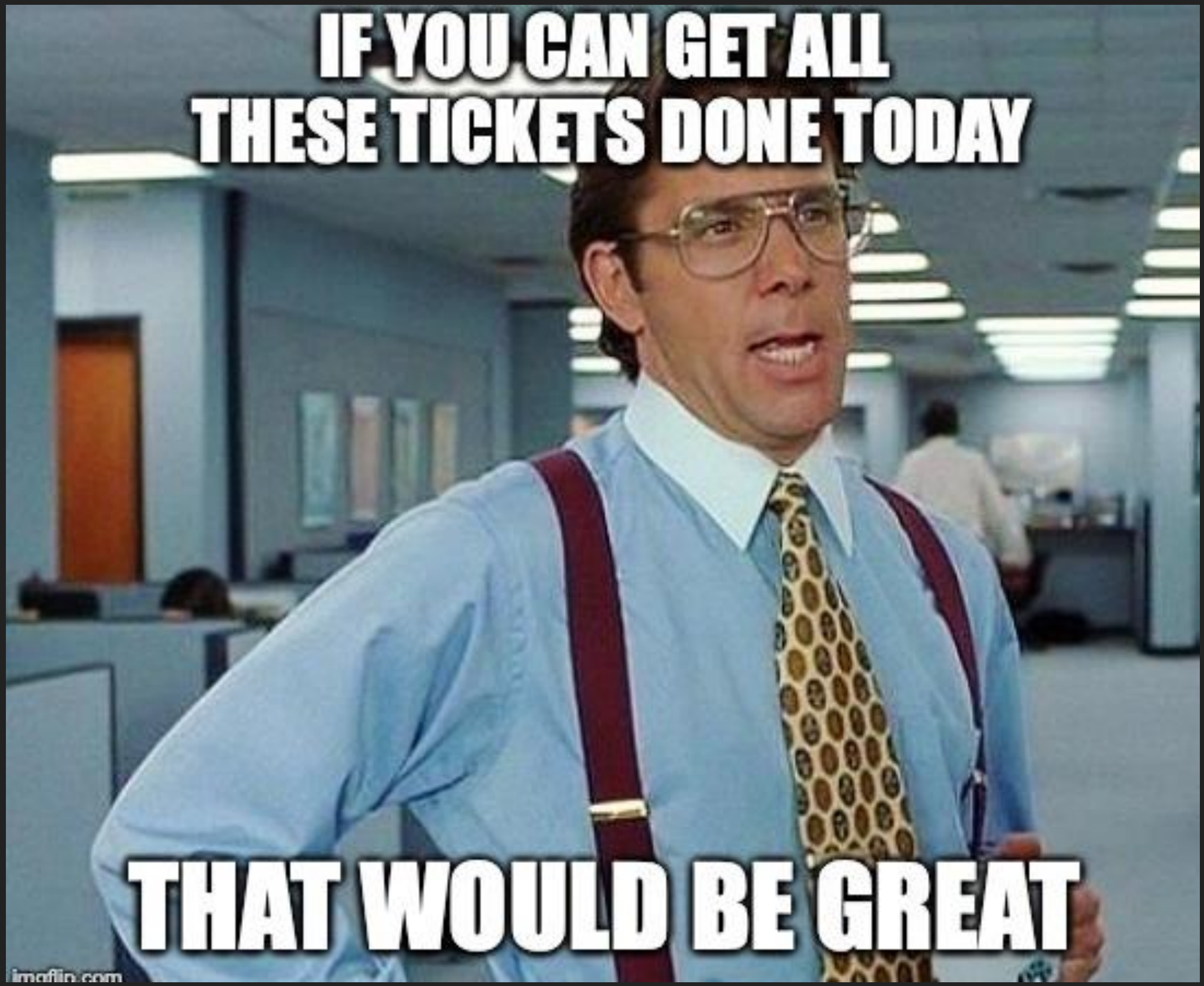
SHARED SECURITY SERVICES

HOW TO ADJUST TO AN EVER-GROWING LANDSCAPE OF SECURITY OPERATIONS CENTER RESPONSIBILITIES

ABOUT ME

- SANS Mentor and Community Instructor for MGT 512
- Run SOC program CLS International Bank. Former Infosec Manager at WarnerMedia (formerly Time Warner)
- SOC responsibilities at JPMorgan and New York Power Authority
- Sat through many painful operational SOC services meetings that went no where quick.



Type to enter a caption

WHAT ARE SOME OF THE EXISTING PROBLEMS

- Most SOCs do not just work on alerts anymore
- Many SOCs have gained responsibilities without resources being correctly allocated
- We miss an opportunity to build rapport with other teams
- Much of the team is overwhelmed with day to day work that strategic thinking is elusive

METRICS: WHAT STORY ARE WE TRYING TO TELL

- Compliance stories are important, but are they making a difference?
  - Is it good enough that remediation teams are meeting their SLAs?
  - How can we showcase just how busy we are?
- How can just meeting compliance requirements make a SOC's job easier?
  - Do the bad actors care about compliance statistics??
- Do we even know the answer to what story we are telling?

SHARING OUR “SHARED” STORY

- One set of metrics does not address everyone’s requirements, especially upper management
- Metrics for different audiences
  - Remediation teams
  - Security teams
  - Management
  - Business metrics
- How can we best communicate the new story? Just through meetings?

ARE WE GETTING CREDIT FOR WHAT WE STOP?

- Reporting on successes such as attempts to exploit our environment stopped by our efforts
- Time and effort spent working with teams to address their concerns and help them
- # of alerts or configuration changes we were able to help other teams fix?

CRUNCHING AND RELEASING THE DATA

- Are we the best qualified group to be crunching SOC data?
- Can we reach out to others within the company to help us visualize data points (AKA enabling other business units)
- Data Analytics teams are a great match for the treasure trove of security data vulnerability teams have.
- Internal communications teams may be able to help craft a story

VISIBILITY INTO WHAT WE DO - OPERATIONAL TRANSPARENCY

- Does anyone outside of Security Operations know what the security operations team does?
- Harvard Business Review - Operational Transparency (https://hbr.org/2019/03/operational-transparency)
  - "When people see the work going on behind the scenes, they value the service more."
  - "At Domino's, customers can use the company's Pizza Tracker app to watch as the kitchen workers prep, bake, and package the pizza for delivery."

VISIBILITY INTO OTHER'S THOUGHTS - FEEDBACK

- Insert customer feedback into every step of the process
  - Make the customer feel listened and enabled.
  - 5 principals of getting good feedback (http://customerthink.com/5-principles-of-getting-good-quality-customer-feedback/)
    - Personalized surveys
    - Be clear and concise
    - Always be there
    - Create Actions
    - Incentivize

ITS NOT JUST THE METRICS - OTHER WAYS OF SHARING

- Why does it **just** have to be metrics?
  - Newsletters
  - Town Hall style discussions
  - Security champions in other groups
- Be the first to tell the story. Do not let others write the story for you.

HIRING THE RIGHT TALENT

- Are we asking the right interview questions?
  - Why do we get so deeply technical in vulnerability management interviews?
- Looking at other areas of the business to help bridge people into our security program
  - Remember, people want to work for security teams!
- Foster the SOC team's growth
  - True security analysts will want diversity in their role
- Team up with red team to help learn exploitation techniques

ALIGN WITH THE RISKS OF THE ORGANIZATION

- Work with risk organization to understand the risk profile of your organization.
  - Don't just align to your critical assets. Grow past that metric
  - For example, is availability your biggest concern? Refocus alert SLAs and ratings based on the key business disrupters.
- Aligning to not only your risks, but your threats and adding them to your alerts scores through basic SOAR practices:
  - Age of IP in question
  - Vulnerabilities associated with internal IPs in question
  - Detonate malware associated with an alert

RETHINK - IN SUMMARY

- Rethink how to use your data
- Rethink how to share your data
- Rethink your communication to other teams
- Rethink your hiring
- Rethink the future of your alerts and your story