VIRTUOUS CYCLES
RETHINKING THE SOC FOR LONG-TERM SUCCESS
GAP SIZE = 3 MILLION JOBS GLOBALLY

59% SAY "ORGANIZATION IS AT EXTREME OR MODERATE RISK DUE TO CYBERSECURITY STAFF SHORTAGE"

48% OF TEAMS PLAN ON INCREASING STAFF NEXT YEAR

ISC² Cybersecurity Workforce Study, 2018
AVERAGE TIME IN ANALYST ROLE...

1-3 YEARS
A tier 1 "SOC monkey" job is terrible. Most of your work can be replaced with a script. The instant you do find something that actually interests you for once, you have to immediately escalate it and completely forget about it. It's soul-sucking.

The worst thing is almost (and I mean probably like over 95% or even more) are false positives, even those escalated, as at T1 we don't have enough access (or time given number of alerts) to check what is really going on.

I think many people who go for a SOC position overestimate how much they are going to learn until they ultimately realize they're just arbitrarily sifting through data to generate metrics for management to show how good of a job you are doing.

95% of our rules are based on threat intel. If there's suspicious traffic, we won't do anything about it because the 'IP is clean'.

Soooooo true. "You were scanned by an IP that was C2 about ten years ago. This indicates there is a compromised machine on your network"

I know what you mean, Tier 1 SOC work is really boring... of course this all depends on where you work.
Burnout

- Diminished Interest in Work
- Exhaustion
- Cynicism
- Inefficiency
- Lack of Concentration
If we understand the causes of burnout we can work to prevent it.
NEED TO CULTIVATE TEAMS THAT ARE:

• INTRINSICALLY MOTIVATED
• ENGAGED
• TRUSTED
• HAPPY

BUT HOW?
THE TYPICAL APPROACH
UNFORTUNATELY, THIS DOESN’T WORK!

• $ WORKS ONLY FOR BASIC MECHANICAL TASKS
• “IF/THEN” INCENTIVES STRIP ENJOYMENT FROM LEARNING AND SOLVING HARD PROBLEMS
  • EXTRINSIC MOTIVATORS GREAT TOOL FOR COMPLIANCE
  • BAD TOOL FOR ENGAGEMENT
• WE WANT TO CULTIVATE INTRINSIC MOTIVATION
WHAT DOES MOTIVATE PEOPLE?

DANIEL PINK’S RESEARCH IDENTIFIED 3 FACTORS
USE THEM TO GUIDE AMPLIFYING INTRINSIC DRIVE
AUTONOMY

"THE DESIRE TO BE SELF-DIRECTED"
MASTERY

"THE DRIVE TO GET BETTER AT SOMETHING"
Purpose

“The yearning to do what we do in service of something greater than ourselves”
RESEARCH TO BACK IT UP:
"A HUMAN CAPITAL MODEL FOR MITIGATING SECURITY ANALYST BURNOUT"¹

SOC HUMAN CAPITAL MODEL

GROWTH

CREATIVITY

SKILLS

EMPOWERMENT

Empowerment
CREATIVITY
GROWTH
ADDITIONAL FACTORS:

"TO MITIGATE ANALYST BURNOUT, SOCS HAVE TO PAY SPECIAL ATTENTION TO THE INTERACTION OF HUMAN CAPITAL WITH 3 OTHER FACTORS"
REQUIREMENT FOR AUTOMATION: TIME FOR REFLECTION
OPERATIONAL EFFICIENCY
METRICS

SOC PERCEPTION

BUDGET
The Whole Model

TIME TO REFLECT:
WHAT TYPE OF SOC DO YOU RUN?
DO YOU OPTIMIZE FOR / PROMOTE THE VALUES IN THE HUMAN CAPITAL MODEL?

BEFORE YOU ANSWER...
ARE ANALYSTS STUCK FOLLOWING PLAYBOOKS?
ARE THEY COMFORTABLE “OFF THE MAP?”
Are analysts trusted by management?
Are they empowered to contain problems?
Can the see the data they need to investigate?
ARE PROCESSES NEEDLESSLY MANUAL?
When was the last time you had "live fire" practice?
How often do analysts get quality training?
Who trains your most advanced people?
DO ANALYSTS GET FREE TIME FOR NEW IDEAS AND TOOLS?
CAN THEY GET DISTRACTION-FREE “DEEP WORK” TIME?
CRUCIAL QUESTION: HOW DOES TIER 1 FEEL?
RECOMMENDATION 1 – SKILL IMPROVEMENT

FOCUS ON DIVERSE AND FREQUENT TRAINING OF MULTIPLE TYPES

- PURPLE / RED-TEAMING, TABLE TOP, PEER-LEAD, FORMAL

"TRAIN LIKE YOU FIGHT"

"LACK OF TRAINING BECOMES LACK OF CONFIDENCE"
RECOMMENDATION 2 – EMPOWERMENT

• LET ANALYSTS CHALLENGE THEMSELVES!
• ALLOW ANALYSTS TO ACT TO RESOLVE ISSUES!
• NO ARBITRARY LIMITS ON TOOL/DATA ACCESS
• AUTONOMY LEADS TO ENGAGEMENT
RECOMMENDATION 3 – CREATIVITY

• Give time for reflection and innovation
• Encourage learning new technology and tools
• For complex tasks: "Developer-analyst tool co-creation"
RECOMMENDATION 4 - GROWTH
OPTIMIZE FOR "GOLDILOCKS" TASKS

TOO EASY = BOREDOM
TOO HARD = ANXIETY
RECOMMENDATION 5 - AUTOMATION/OPS

• S.O.A.R. TOOLS OR SCRIPTING, JUST GET IT DONE!
• ELIMINATE REPETITIVE TASKS LIKE THE PLAGUE!
• BONUS: GIVE ANALYSTS TIME TO DEVELOP IT (CREATIVE OUTLET)
RECOMMENDATION 6 – METRICS

• Do you have analyst buy-in?
• Do they demonstrate SOC R.O.I.?
• Are they reflective of analyst effort?
• Does behavior drive metrics, or do metrics drive behavior?
• Are you pulling the right levers to change them?
Recommendation 7 – Human Capital

Run a "Human First" SOC

• Primary goal: Cultivate Human Capital
• Optimize for Challenged, Engaged and Happy Analysts
• Fewer limits, more learning = long-term SOC success
ASK YOURSELF:
WHAT TRULY PROVIDES THE BEST SECURITY?

TURNOVER AND BURNOUT WITH "EFFICIENT", "REPEATABLE" BUT MISERABLE ANALYSTS?
AN ENGAGED, CREATIVE, SKILLED TEAM WITH LONG-TERM INSTITUTIONAL KNOWLEDGE?
THANK YOU!
TWITTER: @SECHUBB
MORE INFO IN NEW CLASS:
SEC450: BLUE TEAM FUNDAMENTALS