Give Your SOC a SOUL

(Self-driven sense of Ownership, Unity and Long-term commitment)

Alissa Torres  |  @sibertor
## Give your SOC a SOUL Agenda

<table>
<thead>
<tr>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define SOC success factors</td>
</tr>
<tr>
<td>Communication patterns of a successful team</td>
</tr>
<tr>
<td>Baked-in Obstacles to SOC espirit de corps</td>
</tr>
<tr>
<td>- Evolving Technologies</td>
</tr>
<tr>
<td>- Skills/Experience/Temperrament mismatch</td>
</tr>
<tr>
<td>- Dual-Anticipated Turnover</td>
</tr>
<tr>
<td>Strategies in Motivation</td>
</tr>
<tr>
<td>- Individual incentives</td>
</tr>
<tr>
<td>- Team-based strategies</td>
</tr>
<tr>
<td>Feedback Loops</td>
</tr>
</tbody>
</table>
Define SOC Successful Factors

Possible Factors to Success
• Productivity based on metrics
• Employee retention and/or
• Employee satisfaction
• Reputation internal
• Reputation external
• Customer satisfaction

Most analysts would admit, it is a combination of the above... and an intangible element of *espírit de corps*
es·prit de corps

noun

the capacity of a group's members to maintain belief in an institution or goal, particularly in the face of opposition or hardship
Communication and its role in successful teams

- Study by MIT research team at the Human Dynamics Laboratory tracked team members with electronic recording device for a 6 week period.
- Based on the data they collected from employee interactions, they could accurately predict which teams were the most productive, most successful.

- Interactions correlated to the great teams
  - Everyone on the team talks and listens in roughly equal amounts.
  - Members face one another and their conversations and gestures are energetic.
  - Team members connect directly with one another - not just with the team leader.
  - Members carry on back-channel or side conversations within the team.
  - Members periodically break, go exploring outside the team and bring information back.

Three critical dimensions of communication

**Energy**
Number and nature of exchanges among team members

**Engagement**
Distribution of energy among team members
*High predictor of success -> engagement outside of formal meetings*

**Exploration**
Energy between a team and other teams it interacts with

Acknowledge the Moving Target

Traditional tiered system “defense-in-depth”
- Tier1 - Junior
- Tier2/3 - Intermediate/Senior
- SMEs

Rebooted SOC structure
- Technologies are changing the team composite
- Automation of repetitious tasks reduces typical junior analyst workload
- Trend towards automated workflow
the spread of discontent

“This is not what I was promised.”

“This is not what we were promised.”
How do you know negativity is brewing?

**Signs of disengagement**
- Boredom
- Carelessness
- Risk-taking behavior
- Rogue scans, unwarranted data access
- Tardiness
- Lack of official turnovers
- “Phone it in” mentality

<table>
<thead>
<tr>
<th>US Employees</th>
<th>World’s Best Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>33%</td>
<td>70%</td>
</tr>
</tbody>
</table>

ARE ENGAGED AT WORK

Gallup 2017 State of the American Workplace
“The worst thing is almost all (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.”
Commitment to Professional Development

- SOC analyst missed an alert in a customer’s environment. The early warning of the compromise having been missed, the attacker was able to move swiftly through the victim’s network, stealing upwards of 30 GB of data.
Bouncing back from major mistakes as a Security Analyst? Are mistakes really common?

---

• I'm a relatively new analyst and I improperly managed an alert last month that lead to a big issue last week. I'm not fired and haven't been harshly reprimanded since everyone understands my mistake.
• Everyone is saying it's cool and that they've made mistakes in the past but from my Jr. position, it's hard to believe that the senior analysts are even capable of making mistakes; I look up to them so much and they are just seem rock solid and incapable of messing up.
• I'm so worried about another mistake that I'm 2x as slow at my job now. How do I bounce back? Are analyst mistakes even that common or am I an idiot?
"They said lots of things in the interviews that turned out to be false."

- /u/Nibuch, Reddit
Accurately access your security operations maturity level

LEVEL 1: Random, or Disorganized
LEVEL 2: Reactive, or Tactical
LEVEL 3: Preventative
LEVEL 4: Organized, or Directed
LEVEL 5: Proactive, Comprehensive, Continuous and Measurable

Chaos of an Immature SOC

Analysts who can happily work on a well-organized, burned-in SOC may NOT be the best choice for a SOC in its foundling stages

- Growing a team too quickly can create an immature SOC
- New technologies can create a temporarily immature SOC
- Hiring mismatches can create hostile work environments
Managing Expectations

Other Common SOC Analyst Complaints

• I’m not being challenged.
  • Not touching IDA, Encase
  • No deep-dive forensics, RE, threat intel
• Op tempo is too high to document.
• Why can’t we access all of the tools in the enterprise?
• I am not getting paid what I am worth.
• Too much stress, too many tools.
• Success is not clearly defined.

Cybersecurity workers believe their performance should be evaluated by:
• How quickly they respond to a breach or security incident (43%)
• Security program maturity (30%)
• How effectively they increase employee security awareness (30%)
• How effectively they handle remediation (28%)
Expectations of Turnover

“I was drawn to the SOC by misguided youthful ideals, which have been ground into a fine powder by years of poor management and lack of support from higher-ups”

Respondent in Cyentia Institute's "Voice of the Analyst Study" 2018
A SOC manager ensures there is no single point of failure.
• Succession planning
• Building staffing redundancy
• Institutional knowledge archives

A SOC manager prepares the employee for his/her next job.
• Individual Training Plans
• Clear and defined performance objectives
• Outlined career path for advancement
Expectations for A Short Tenure

• Most analysts don’t expect (or recommend) to stay at a SOC longer than 12-18 months.

• A stint in security operations is seen as a necessary milestone along the way to a desired career.

• Many think it is sign of “failure to launch” if an analyst stays longer than 18 mths.

“A SOC is a transitional role for most people.” - kid_miracleman, Reddit
“Make the most of your time and always be developing but don't stay too long.” - Nibuch, Reddit poster

“Do not learn from people that have been there 3+ years in the same position. This is my own personal bias I admit, but this is an entry-level position for a reason. If someone has been in the SOC for 5 years, it means they're either too lazy to move on, too dumb despite how they'll talk about how they run the show there, or a mixture of both. Successful people don't waste their time associating with people who seem to be actively avoiding success.”
Strategies in Motivation
A SOC manager prepares the employee for his/her next job.
• Individual Training Plans
• Clear and defined performance objectives
• Outlined career path for advancement
• A percentage (10-20%) should be spent on advancing skills for next position, whether at the same company or elsewhere.

Initial cost upfront but potential gains
• Longer tenures for current employees
• Obvious benefits from R&amp;D, more educated workforce
• Draws external talent due to flexible, supportive workplace
Incentives

After salary & benefit requirements are met, these things matter most¹:

- Challenging and impactful work
- Demonstrated commitment to professional development
- Continuing investment in training
- “Kevin Durant effect” - desire to work with others whose talent and work they respect
- Opportunities for research & development

¹https://www.csis.org/analysis/recruiting-and-retaining-cybersecurity-ninjas Center for Strategic and International Studies
Continuing Investment in Training

- Provide foundational skills onboarding, mentoring
- Ensure vendor-specific training
- Budget for “Stretch” training, “beyond the scope of the job”
- Cross-train for different perspective of shared mission
- Provide SOC analysts opportunities to meet the profit centers
- Provide R&D funds and work hours to senior team members
Incentive Programs

• Gamification of certain SOC tasks and good analyst behaviors rewarded with cash prizes to encourage healthy competition.

• As a tangible way to support research, a program soliciting submissions for special project grants can spur creativity and push individuals and groups to achieve.

• Bonuses commensurate with contributions that have a business impact. Efficiency gains, improved visibility into environment.

1https://www.csis.org/analysis/recruiting-and-retaining-cybersecurity-ninjas Center for Strategic and International Studies
Sense of Ownership

Opportunities for analysts to be seen & heard, have their work recognized are key.
- Newsletters, presentations, lunch n’learns
- Development and maintainence of internal wikis
- Small projects to extend skillset and circles of interaction

Mentorship programs.
- New employee on-boarding training sessions
- Knowledge shares

Participation in hiring interviews, onboarding

Having a shared story.
- Hearing it. Telling it. Repetition.
• Indicates a level of employee status
• Flexible starting and ending times
• Telecommuting 1-2 days a week
• Management that supports work/life balance
• Provisioning of adequate staff to avoid burnout
Offer an individualized career development plan

- Not everyone wants to grow up to be a manager
- Individualize career milestones and measures of success
- Provide a roadmap for career progression
- Learn what motivates an individual -> Not a cookie cutter formula
- Consider relocation incentives

“Paths to other teams existed on paper, but weren't actually viable (and no one would help you follow them even if you tried).”
Feedback Loops

Solicit more feedback with increased interactions
- Quarterly performance reviews (individual)
- Quarterly team meetings with upper management
- Cross-team mentoring one-on-one sessions
- Anonymous surveys on job satisfaction
- Solicitation of great ideas
- Team, organizational level recognitions
References

• https://www.reddit.com/r/AskNetsec
• https://www.youtube.com/watch?v=QaePF_mtVbM
• Recruiting and Retaining Cybersecurity Ninjas. https://www.csis.org/analysis/recruiting-and-retaining-cybersecurity-ninjas
• (ISC)² Finds 84% of Cybersecurity Workers are Open to New Opportunities or Already Planning a Job Search in 2018, https://www.researchgate.net/publication/235270159_What_Motivates_employees_according_to_over_40_years_of_motivation_surveys
• Gallup 2017 “State of American Workplace”