Humans Are Dynamic — Our Tools Should Be Too

The success of Security Operation Centers (SOCs) depends on combining good tools and processes with efficient and effective analysts. During four years of anthropological study of SOCs, the authors discovered that successful SOC innovations must resolve multiple internal and external conflicts to be effective and efficient. Their research indicates conflict resolution is a prerequisite for continuous improvement of SOCs in both human and technological aspects. Failure to do so can lead to adverse effects such as analyst burnout and reduction in overall effectiveness.

Sathya Chandran Sundaramurthy
University of South Florida

Michael Wesch
Kansas State University

Xinming Ou
University of South Florida

John McHugh
RedJack

S. Raj Rajagopalan
Honeywell Labs

Alexandru G. Bardas
Kansas State University

The frontline of digital warfare is a showcase of contradictions. A wall of vibrant LED screens broadcasts a steady stream of updates about potential threats. On one large screen the Earth slowly rotates as beams of light shine off of it to indicate the number of events sourced from particular locations, while at its side the real events stream through a big white backdrop. A nearby ticker indicates which analyst has been assigned to each incident. The wall feels alive and exciting in a way that the analysts sitting in front of the wall do not.

There are about a dozen analysts in the room, staring silently at the computer monitors in front of them. Adam is one of them; he looks dull and bored as he starts yet another day in the Security Operation Center (SOC). He spots an alert that just showed up in one of his displays and desultorily looks up the SOC run-book to take the next step in the course of action. He dispatches the machine for a re-image while feeling guilty subconsciously for his inability to pursue an alternate better mitigation plan – he has to go by the book. With no perceivable variation in facial reaction, he processes some 20 more events. There really isn't much he needs to do for these events – if it's too hard, he escalates it so the upper-tier SOC can take care of it; if it's easy he processes it and puts in another ticker in his scoreboard for the day.

It's not that Adam doesn't want to do any real work; he tried when he first started, but whenever he needed to check anything he was also told "no access." So he figured it would be better for him to just escalate anything that requires any real investigation – the upper-tier SOC folks must have more access. After all, in the end it's the number of events he can close in a given day that is his trophy book, so why bother spending too much time on each event? He started his shift at 6 a.m. and four hours later he's already putting up a sore face. A cup of

 Published by the IEEE Computer Society 1089-7801/17/$33.00 © 2017 IEEE

triple-shot espresso and a nerdy joke with one of his co-workers refreshes him and he is back to grinding more events. Something catches his eye; finally, an interesting alert to work on, he feels energetic now. He quickly runs a search for some data in a log server and tries to look up some contact information in another database. The first search timed out and the second one didn't return any results. This isn't the first time the tool has failed him. He has mentioned this to his manager before, but all he was told was "document that." Adam puts down his head in frustration, checks his watch, finds that it's almost the end of his shift, and walks out of the SOC.

Mundane and relatively insignificant events like these are manifestations of the core contradictions in a SOC. Depending on how well they're understood and managed, these contradictions can be the driving force of innovation and change, or a source of perpetual problems and conflict. If the management realizes these contradicting factors and take steps (and some risks) to resolve them, it can lead to positive changes and technical innovations that help human capital development.[1,2]

The Right Thing vs. the Required Thing

The SOC's primary objective is to mitigate security threats targeted toward the parent organization. But the SOC also has a second objective — justifying its value to higher management. This contradiction at the center of the SOC's objectives — as an organization that must be useful by mitigating security threats but also adept at demonstrating that it's useful — is just one among many connected contradictions operating in a SOC. To achieve this second objective, SOCs typically generate metrics that are supposed to show the value the SOC brings to the organization. The metrics are crucial for a SOC to secure funding by showing the return on investment (ROI) the parent organization extracts by investing in the SOC. Analysts are hence asked to adhere to certain norms such as closing a certain number of tickets per day and working on only specific projects that management perceives as important. This adherence can conflict with the creative mindset of an analyst, as it prevents the analyst from working on technical problems that actually matter to the SOC and its fundamental goal of keeping the organization secure. This duality creates a tension within the analysts because they're conflicted between doing the right thing versus the required thing.

This isn't just abstract theorizing. These contradictions have real effects in the lived experience of analysts, and we discovered them by living the life of analysts ourselves. After years of trying to understand SOCs through interviews and short visits, we turned to an anthropologist to train five students with computer science backgrounds in the method of participant observation.[1-3] Our students then took jobs in a variety of SOCs in universities and corporations. Before we set foot into a real SOC, we didn't know that what awaited us would be so different from what we anticipated. As the frontline of digital warfare, we expected to find exciting time-pressured investigations at the SOC that would require quick teamwork and creative problem solving. We expected to find analysts calling upon a vast array of high-tech tools to aid them in their quest. We certainly didn't expect to find what became so painfully obvious within just a few short weeks: boredom.

Within a few weeks our first fieldworker was frustrated and burned out. He had been tasked with the menial job of handling malware incident response. He found himself tediously scanning through 70 gigabytes of daily log data to find correlations between various data silos, trying to find out when and where an event might have happened. Each event took about 10 minutes to correlate. He was processing at least 15 events per day, using up 2–3 hours of precious work time. There was nothing particularly stimulating or glamorous about this task; rather, it required a peculiar blend of intense focus without any real creativity.

You would think that there would be automation for this kind of low-level work, but the tools are often chosen because they satisfied compliance requirements, not because they were useful or effective. In other words, they were also in service of the required thing, rather than the right thing. And so we find this core contradiction between the right thing and the required thing operating at all levels of the SOC, from managers to analysts and even in the tools (see Figure 1).

During our four years of fieldwork at two academic and three corporate SOCs, we would find these contradictions operating in such a way as to create a recurring pattern, and our

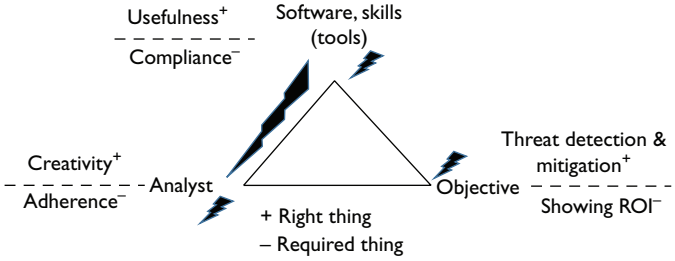

Figure 1. Tension among analyst(s), tools, and the objective. At all levels of Security Operation Centers (SOCs), often there are core contradictions between the right thing and the required thing. ROI stands for return on investment.

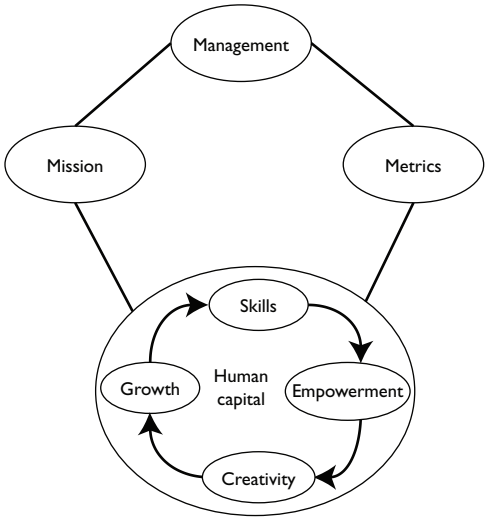

Figure 2. The right thing versus the required thing—managing a SOC's human capital. Four central factors influence the creation and maintenance of efficient human capital: skills, empowerment, creativity, and growth.

opening scene featuring Adam's frustrations is a composite of such accounts. Perhaps unsurprisingly, we soon discovered that burnout is a major concern across the industry among analysts and management alike.

Mission vs. Metrics: A Human Capital Model

From the management perspective, if these contradictions are identified and effectively dealt with, they can provide opportunities for positive changes. On the other hand, if they aren't recognized and managed, the contradictions can turn into perpetual problems in the SOC. Figure 2 shows the dynamics of SOC management and the workers inside. In theory, a SOC's management tends to the real mission of the SOC, which is to do its best with the given resources to protect the parent organization. In reality, the SOC management must show its value (ROI) to the parent organization's higher management, which it does using a variety of metrics. In essence, SOC management must tend to both of these conflicting goals in managing the SOC's workforce.

The human capital model was first postulated in economics by Adam Smith.[4] The theory holds that the investment made in education and training of individuals in a society is a resource in itself, more important than capital and natural resources. Our model[1] indicates that there are four central factors that influence the creation and maintenance of efficient human capital, as Figure 2 shows: skills, empowerment, creativity, and growth.

Skills

Security analysts need to possess the right skills to do their job. The dynamic nature of security threats means the analysts have to undergo periodic training. If the analysts aren't adequately skilled, it affects their confidence in dealing with security alerts. Over time, the lack of confidence will manifest itself as frustration, especially when their job demands them to do more than their skills level permits.

Empowerment

Analysts need to be adequately empowered to perform their job efficiently. The analysts' skill level influences the level of empowerment that management is willing to grant them. For example, only skilled analysts are trusted to be careful and are provided privileged access to user accounts.

Creativity

Creativity refers to the ability of analysts to handle an operational scenario that differs significantly from those they have encountered so far. The human capital model in Figure 2 indicates that empowerment directly affects analysts' creativity. Analysts must be empowered by their managers to deviate from norms. Otherwise, this will lead to analysts just executing the procedures and failing to react appropriately to a novel operational scenario.

Growth

Growth in the context of the SOC refers to an increase in the intellectual capacity of the analysts. An analyst, by handling different types of security incidents, learns new skills and improves his knowledge on security analysis. This learning improves his morale, because it provides a sense of purpose and accomplishment. As Figure 2 shows, growth is directly influenced by creativity, and it enhances the analysts' skillset.

How to manage the human capital in a conflicting environment such as SOCs is a challenging question to answer. Our research shows that without a conscious effort to understand and manage these conflicts, the environment tends to naturally gravitate toward the negative side of interplaying factors — the SOC's objective devolves to merely generating metrics to satisfy upper management, tools are acquired merely to demonstrate compliance, and analysts adhere to the predefined processes in their job, and in the process burn themselves out. As we found out in previous work, this is a self-inflicted problem by a mismanagement of human capital in this critical environment.[1] Instead of us managing the contradictions and tensions therein, we're managed by them.

From Contradictions to Innovations — Continually Evolving

When we first entered the SOC, we weren't aware of these contradictions. All we knew was that the job was far more tedious than it needed to be. We found that analysts were spending more time gathering the basic information (for example, the host name and location of the device in question) than actually using their human gift of creativity for higher-level analysis. Our realization was that tools must gather and deduce information along the four basic dimensions of information (what, who, when, and where) so that the analysts can spend most of their time on cognitive effort along the analytical dimensions (how and why).

Working with the analysts, we built an utterly simple incident response portal based on this insight.[5] We used a database to store log information and collected and parsed logs using periodically executed scripts. The tool correlates the information stored in the database automatically and presents the analyst with a filled-in incident ticket with all the required information such as the user of the infected device and proof of contact (POC).

The tool took a tedious 10-minute process and reduced it to 10 seconds. But more importantly, it mitigated the fundamental conflict within the analyst. Analysts were able to process the incoming malware alerts in a timely manner as required by their manager, satisfying the SOC's ROI requirement. Furthermore, analysts have more time to dedicate to more sophisticated analytical tasks that require creative thinking. Thus, the key to mitigating the burnout problem in this specific case was to resolve the conflict between the analyst and the tools they use.

Conflict Resolution Is a Continuous Process

But we would soon discover the importance of understanding the interconnectedness of these contradictions throughout the organization. The introduction of our tool had ripple effects throughout the organization and workflow. Security analysts don't act in isolation; they work collaboratively with other analysts, managers, and end users. On observing the tool's ease of use, the SOC manager required the not-tech-savvy compliance analyst to also perform malware incident response using the tool. The compliance analyst was conflicted on two fronts. First, malware incident response wasn't part of his job description and he wasn't comfortable performing the task because it was outside his expertise. Second, the tool was still too technical for him, something that isn't admitted easily. In effect, the tool turned out to be more adversarial than useful!

On the positive side, introducing the tool opened new possibilities that didn't exist before. Prior to our tool's deployment, there was only one analyst responding manually to malware incidents. With the deployment of this tool, even the compliance analyst was able to expand his capabilities, which in effect contributed to growth in his skill set. We then worked with the compliance analyst and adapted the tool's user interface so that every analyst in the SOC could use it easily to respond to malware alerts. Thus, we need to be alert to the possibility that conflict resolution can engender new conflicts, and new conflicts ought to be looked upon as opportunities for improving efficiency rather than as deterrents to change.

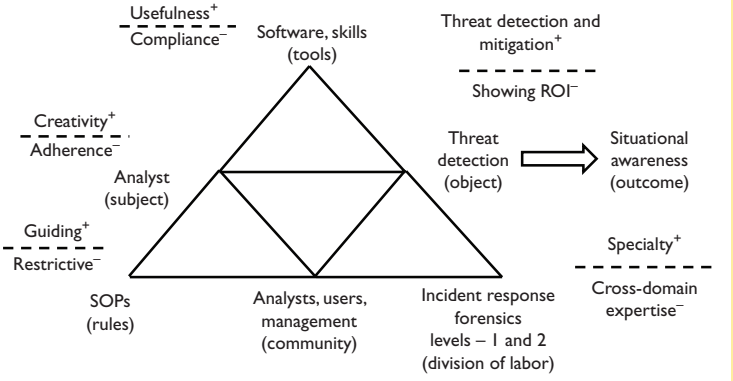

Figure 3. Activity theory (AT) model of SOCs. Low levels of empowerment lead to lower creativity, which in turn lead to lower growth and skills. SOP stands for standard operating procedures.

Understanding Burnout

As long as a positive causality exists among the human capital model factors — skills, empowerment, creativity, and growth — the analysts' morale will remain high. Burnout occurs when a SOC gets stuck in a vicious cycle of negative causation involving the same factors. This leads naturally to the question of what causes a vicious cycle and how can it be prevented. The contradictions we introduced in the previous section explain this. For instance, SOC management has to operate the SOC under two conflicting goals: protecting the organization and justifying the SOC's own existence (Figure 2). This forces them to generate metrics to satisfy upper management, so that the SOC is perceived to be delivering value. Because generating the metrics has the most immediate impact (for example, on an operating budget), management will tend to focus exclusively on metrics while ignoring the other factors in the system. This will start to create a vicious cycle among the factors in Figure 2, which eventually leads to burnout.

To take an example, standard operating procedures (SOP) are present in every SOC. SOPs are helpful in team coordination and act as guidelines for incoming analysts. But they can quickly become restrictive as analysts mature, if analysts aren't allowed to question or deviate from them as threats evolve. This dual nature of SOPs extends our model of SOC operations as we begin to consider the relationship between analysts and managers, and how this relationship is often mediated by rules and SOPs (see Figure 3).

Low levels of empowerment lead to lower creativity, which will in turn lead to lower growth and skills. Since the skill level of analysts remains low in the process, this leads to a vicious cycle of low empowerment, low creativity, and low growth (lower part of Figure 2). Burnout sets in and analysts start to feel that they're not accomplishing anything in their job and the resulting repetitiveness of the job leads to exhaustion.

This situation is unfortunate, because management everywhere wants their analysts' skill set to progressively improve through on-the-job experience, but the negative causality among the four factors makes any learning nearly impossible for analysts. Thus, it's clear that burnout is a human capital mismanagement problem. This is rooted in the lack of awareness of the conflicting factors that are at play in an SOC environment, and if left unattended they often lead to a vicious cycle for human capital development.

Turning the Vicious Cycle into a Virtuous One

Burnout mitigation can start at any of the four nodes in Figure 2, although a SOC manager can bring a significant change by taking the first step. A manager can gradually empower the less-skilled analysts; after a few positive cycles the analysts have accumulated enough new skills that the manager can now empower the analysts with privileges that they were previously denied. This will in turn encourage creativity and growth converting the cycle into a virtuous one. It's possible that even after the cycle is taken in a positive direction, the analyst's job can become too repetitive. One way to deal with the repetitiveness is by providing new opportunities for analysts to stay creative. Throughout our fieldwork at different SOCs we observed that because security threats evolve rapidly, creative analysts are paramount for a SOC's success. For example, in responding to phishing campaigns we noticed that the attack techniques used by the attackers changed almost on a weekly basis. When the analysts are stuck in repetitive tasks, only the so-called low-hanging fruit are harvested while the more dangerous threats, such as Advanced Persistent Threats (APTs) that require more skill and effort to detect, are ignored.

A key factor that ensures a virtuous cycle is automation. Automation in a SOC refers to software tools that aid analysts' jobs and improve

operational efficiency. Automation can range from complex software such as Security Information Event Management (SIEM) to simple scripts written in Python or Ruby. Software tools can be extremely efficient in performing repetitive tasks that stifle creativity. By automating repetitive tasks, skilled human analysts will have more freedom to engage in more sophisticated investigations. This has been demonstrated by our intervention with the incident response portal in one of the SOCs we studied.

During the fieldwork, we discovered that effective automation takes place only if a process called *reflection* takes place within and among the analysts. Reflection in a SOC is usually done by periodically reviewing the procedures with the goal of identifying operational bottlenecks that can benefit from automation.

There's no debate that a tool can't entirely replace human wisdom and expertise. However, tools need to be built and rebuilt on a frequent basis to enable analysts to engage in creative endeavors, by resolving the constantly emerging conflicts in the analysts' workflow using reflection. Because the conflicts are continuously evolving, the tools must continually evolve as well.

SOC as an Activity System

At a theoretical level, what we discovered in SOCs has been understood for a long time in the framework called activity theory (AT), which can model practically any organized human activity. The theory originated during the 1920s and 1930s in the works of the Russian psychologists Aleksei Leontiev[6] and Lev Vygotsky,[7] and was later extended by Yrjö Engeström.[8]

When using AT, we must examine the larger picture of systemic relations between people, tools, rules, organizational structure, and organizational culture. Engeström developed a triangular structure to model any human activity that we utilized throughout this article to explain what we observed. The full explication of this is in Figure 3. We placed Engeström's original elements in parenthesis and our own application of his insights right above them. Following Engeström insight, in a complex system such as a SOC, the participants have different points of views, and competing and conflicting goals and interests; this is represented at the bottom of the triangle. When we zoom out to see the larger organizational structure in which a SOC operates, we find that the SOC itself has different views, goals, and interests from other business units within the parent organization. These differences can create new contradictions or exacerbate existing ones. The triangular structure lets us show the potential tensions by showing how the elements are related and "mediate" one another. For example, at a most basic level, an organization includes a subject (the analyst) pursuing an object or objective (to mitigate threats), but this task is mediated by the tools they have (top of the triangle). The analyst is also part of a larger community that includes management, a relationship mediated by the SOP (lower lefthand corner). Each node or element has its own set of contradictions by virtue of its relation to other elements in the system. We identified a core contradiction for each of the nodes, and as our analysis has shown, these tensions never really go away completely even as they're mitigated. Tools or policies designed to mitigate one tension might create another tension or contradiction. Being aware of the overall dynamics of an organization and where to locate core contradictions can help us exploit these tensions as opportunities for innovation.

Our findings and insights from four years of anthropological study of SOCs show that useful innovations often occur by identifying and resolving certain tensions within and between the various interplaying factors. We found that AT is a useful framework to explain the phenomena we saw in SOCs, in particular the burnout problem. Our analysis shows that to keep improving a SOC's operation, the various contradictions in it must be constantly identified and addressed on an ongoing basis. As a result, tools used in SOCs must be dynamic and constantly adapted to address newly emerging conflicts. Identifying and working with the contradictions underlying the manifested tensions is a key requirement for running successful SOCs.

Acknowledgments

This research is supported by the US National Science Foundation under grants 1314925 and 1622402. Any opinions, findings, and conclusions or recommendations

expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation. This article is based on the contents presented in two SOUPS papers published in 2015[1] and 2016,[2] with additional study and data analysis since their publication.

References

1. S.C. Sundaramurthy et al., "A Human Capital Model for Mitigating Security Analyst Burnout," *Proc. 11th Symp. Usable Privacy and Security*, 2015, pp. 347–359.
2. S.C. Sundaramurthy et al., "Turning Contradictions into Innovations or: How We Learned to Stop Whining and Improve Security Operations," *Proc. 12th Symp. Usable Privacy and Security*, 2016; www.usenix.org/conference/soups2016/technical-sessions/presentation/sundaramurthy.
3. S.C. Sundaramurthy et al., "An Anthropological Approach to Studying CSIRTs," *IEEE Security & Privacy*, vol. 12, no. 5, 2014, pp. 52–60.
4. A. Smith and J.S. Nicholson, *An Inquiry into the Nature and Causes of the Wealth of Nations*, T. Nelson and Sons, 1887.
5. S.C. Sundaramurthy, "Designing Forensic Analysis Techniques through Anthropology," tech. report, Computing and Information Sciences Dept., Kansas State Univ., 2013; https://sathyacs.github.io/papers/tr-2013-1.pdf.
6. A.N. Leontiev, "The Problem of Activity in Psychology," *Soviet Psychology*, vol. 13, no. 2, 1974, pp. 4–33.
7. L.S. Vygotsky, *Mind in Society: The Development of Higher Psychological Processes*, Harvard Univ. Press, 1980.
8. Y. Engeström, *Learning by Expanding: An Activity-Theoretical Approach to Developmental Research*, Orienta-Konsultit Oy, 1987.

Sathya Chandran Sundaramurthy is a PhD candidate in computer science and engineering at the University of South Florida. His current research interest is studying security operation centers (SOCs) using anthropological methods. Sundaramurthy has a BS in computer science and engineering from Anna University, India. Contact him at sathyachandr@mail.usf.edu.

Michael Wesch is an associate professor of cultural anthropology at Kansas State University. His research examines the complex relationships between technologies and humans. Wesch has a PhD in anthropology from the University of Virginia. He has won several major is awards for his work, including the US Professor of the Year Award from the Carnegie Foundation, the *Wired* Magazine Rave Award, and he was named an Emerging Explorer by *National Geographic*. Contact him at mwesch@ksu.edu.

Xinming Ou is an associate professor of computer science and engineering at the University of South Florida. His research is primarily in cyberdefense technologies, with focuses on human factors in cyberdefense, intrusion/forensics analysis, cloud security and moving-target defense, mobile system security, and cyber-physical system security. Ou has a PhD in computer science from Princeton University. He's a member of ACM. Contact him at xou@usf.edu.

John McHugh recently retired from RedJack, where he served as senior principal and chief analyst. He's currently an adjunct professor of computer science at the University of North Carolina, Chapel Hill. His research includes computer security and software engineering. McHugh has a PhD in computer science from the University of Texas. He's a Life Senior Member of IEEE. Contact him at mchugh@cs.unc.edu.

S. Raj Rajagopalan is a senior principal research scientist at Honeywell Labs, where he leads the cybersecurity research effort aimed at designed-in security for Honeywell's vast control system product portfolio. His research includes computer security, including software engineering techniques for training software development teams in security practices. Rajagopalan has a PhD in computer science from Boston University. He's a member of IEEE. Contact him at siva.rajagopalan@honeywell.com.

Alexandru G. Bardas is a visiting assistant professor in the Department of Computer Science at Kansas State University. His research interests focus on cybersecurity – moving target defenses, cloud security, and bringing anthropology into cybersecurity. Bardas has a PhD in computer science from Kansas State University. He's a member of the Usenix Association, ACM, and the Honor Society of Phi Kappa Phi. Contact him at bardasag@ksu.edu.

myCS *Read your subscriptions through the myCS publications portal at* **http://mycs.computer.org.**