TAG

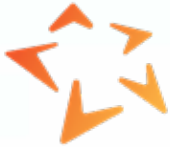
ANALYST REPORT

LIGHTS-OUT SOC?

YES, IT'S COMING (AND FASTER THAN YOU THINK)

IS THE HUMAN-AUGMENTED AUTONOMOUS SOC A CONTRARIAN IDEA OR THE NEXT BIG WIN FOR MSSPS?

DR. EDWARD AMOROSO
CHIEF EXECUTIVE OFFICER, TAG,
RESEARCH PROFESSOR, NYU



STELLAR CYBER®

LIGHTS-OUT SOC?
YES, IT'S COMING (AND FASTER THAN YOU THINK)

IS THE HUMAN-AUGMENTED AUTONOMOUS SOC A CONTRARIAN IDEA OR THE NEXT BIG WIN FOR MSSPS?

DR. EDWARD AMOROSO, CEO, TAG,
RESEARCH PROFESSOR, NYU
eamoroso@tag-cyber.com

INTRODUCTION: HUMANS AND MACHINES

Back in the mid-90s, I watched with curiosity as an IBM machine beat Gary Kasparov in chess. At the time, it felt like a fun computer science parlor trick, this interesting software machine that could hold its own against the world champion. But looking back, that moment was a clear harbinger of what we now accept as inevitable: In any domain governed by rules, data, and pattern recognition, the sad fact is that machines will eventually win.

Cybersecurity, and the Security Operations Center (SOC) in particular, is governed by just such constraints. It's rules-based, data-intensive, and increasingly reliant on pattern recognition to spot attacks. It's taken us a few decades to get here, but I believe we're now on the threshold of a full-blown transition from a hybrid model of human-machine cooperation to what we at TAG are calling a lights-out SOC, fully automated and autonomous. No humans required – at least, not in the traditional analyst sense.

But here's the twist: what some see as a threat to the SOC workforce may be one of the greatest opportunities for MSSPs. A new class of human-augmented autonomous SOC services will emerge, where MSSPs run and manage these "SOC clouds" on behalf of enterprises, providing oversight, compliance assurance, and customer-facing context while the AI does the heavy lifting.

In fact, this could be the key connection between humans and machines – a confluence that could ensure continued career paths for experts and greatly improved SOC functionality. And remember that the offense is moving in the direction of autonomous attack campaigns, run by AI-enabled weapons. Trying to handle this with human or even hybrid SOC support will not work. Let's examine this more deeply.

PHASES OF THE SOC JOURNEY

This journey to lights-out SOC operation hasn't been sudden. The first phase was purely manual. Remember Cliff Stoll chasing Markus Hess through Berkeley systems over a 75-cent accounting glitch? Or Bill Cheswick running honeypots at AT&T to trap a curious hacker named Berferd? These folks were legends, and all their work was done manually, with clever human reasoning at the core. They were the SOC.

Then came the hybrid era of security operations. HD Moore's Metasploit was a game-changer for analysts. Splunk brought better log analysis. SOAR tools boosted productivity. But the analyst still sat in the center seat. We have been calling this a hybrid SOC for the past few years, but I believe that now, AI sits at the center of the transition.

THE IMPACT OF AI

AI, through LLMs, behavioral analysis, and autonomous agent design, brings the capacity to remove the human operator from the loop entirely. Today's AI-based platforms already outperform humans in detecting and classifying malicious activity.

And they will be able to handle the onslaught of purely AI-driven attacks, one that will never stop, continually adjust, and learn from their mistakes. If this sounds terrifying, then you are on the right track in your understanding. It should help you to see why the transition to lights-out SOCs will be not only desirable but will be required.

The mistake is assuming that SOC processing tasks will always require a human interface. Autonomous decision-making is already happening at the endpoint. The SOC is next. Fighting this trend is a losing game.

But, as suggested above, there will be massive opportunities for humans to participate – but at a higher-level context, including governance, curation, and monitoring of progress in day-to-day operations. They will select the vendors, swap out automated tools, diagnose problems, and generally ensure that the defensive AI is working as expected.

And since such automation will extend to all types of companies of all sizes, and shapes, especially with MSSP involvement, it seems possible that more jobs will open up for humans in this context than exist today. Humans will be a required interface in MSSPs to connect with buyers, especially ones with less experience in SOC functions, to ensure that they are properly supported.

One could say, perhaps, that in the MSSP context, this isn't a fully "lights out" operation. MSSPs will be best placed to continue to use humans to sell to and interact with their customers in how the automation is operated, tuned, and integrated into their business.

A PROPOSED TRAJECTORY

At TAG, we thus see three phases in this SOC journey, in the context of how the actual day-to-day handling of inbound attacks will be handled:

- **Manual SOC (1985–2010): Humans ran everything.**
- **Hybrid SOC (2010–2025): Humans and machines shared control.**
- **Automated SOC (2025–2040): Machines take over, humans oversee.**

MSSPs can leverage this Phase Three by building managed autonomous SOC services that blend AI efficiency with human judgment for governance, customer trust, and strategic defense. It is comparable to SaaS capabilities, where automated platforms like M365 are often integrated into managed IT services.

THE FUTURE OF THE SOC

As we have suggested, the actual SOC operation, with its real-time data collection, on-going data processing, and live attack handling, will soon be a sealed room in the cloud, powered by autonomous AI agents running non-stop. There should be no people inside. Human roles, as we've suggested, will shift to oversight, audit, and improvement of the models.

For CISOs, we recommend the following: You should begin to rethink those plans you might have for building large SOC analyst teams. Instead, you should start planning for zero-person SOCs. For MSSPs, we strongly recommend that you start positioning yourselves as the managers of SOC clouds. You'll be that human bridge between machine speed and customer trust.

And for SOC analysts, we expect that you will soon pivot from operator to overseer, from responder to strategist. The SOC lights may go out from a day-to-day processing perspective, but with companies needing governance and MSSPs ready to step in, many new types of jobs and positions will open up, just as we've seen happen for 100% of functions that are automated.

Steve Garrison

Senior Vice President, Marketing

steve@stellarcyber.ai

THE HUMAN-AUGMENTED AUTONOMOUS SOC: CONTRARIAN OR INEVITABLE?

We see the transition as the beginning of a new era for security defense. In the coming decade, SOC operations will shift to AI-driven "defensive SOC clouds" capable of detecting, analyzing, and responding to "offensive SOC clouds" (yes, that will happen).

And MSSPs should recognize that as enterprises offload SOC operations to the cloud, these service providers can position themselves as the managers of newly emerging autonomous SOCs, tuning models, validating AI decisions, and translating automated outcomes into clear business value.

Those who can properly fend off attacks in this new model will combine AI's precision with human judgment, delivering faster, leaner, and more trusted cybersecurity as a service.

Let us know what you think.

ABOUT TAG

Recognized by Fast Company, TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights, guidance, and recommendations to enterprise teams, government agencies, and commercial vendors in cybersecurity and artificial intelligence,.