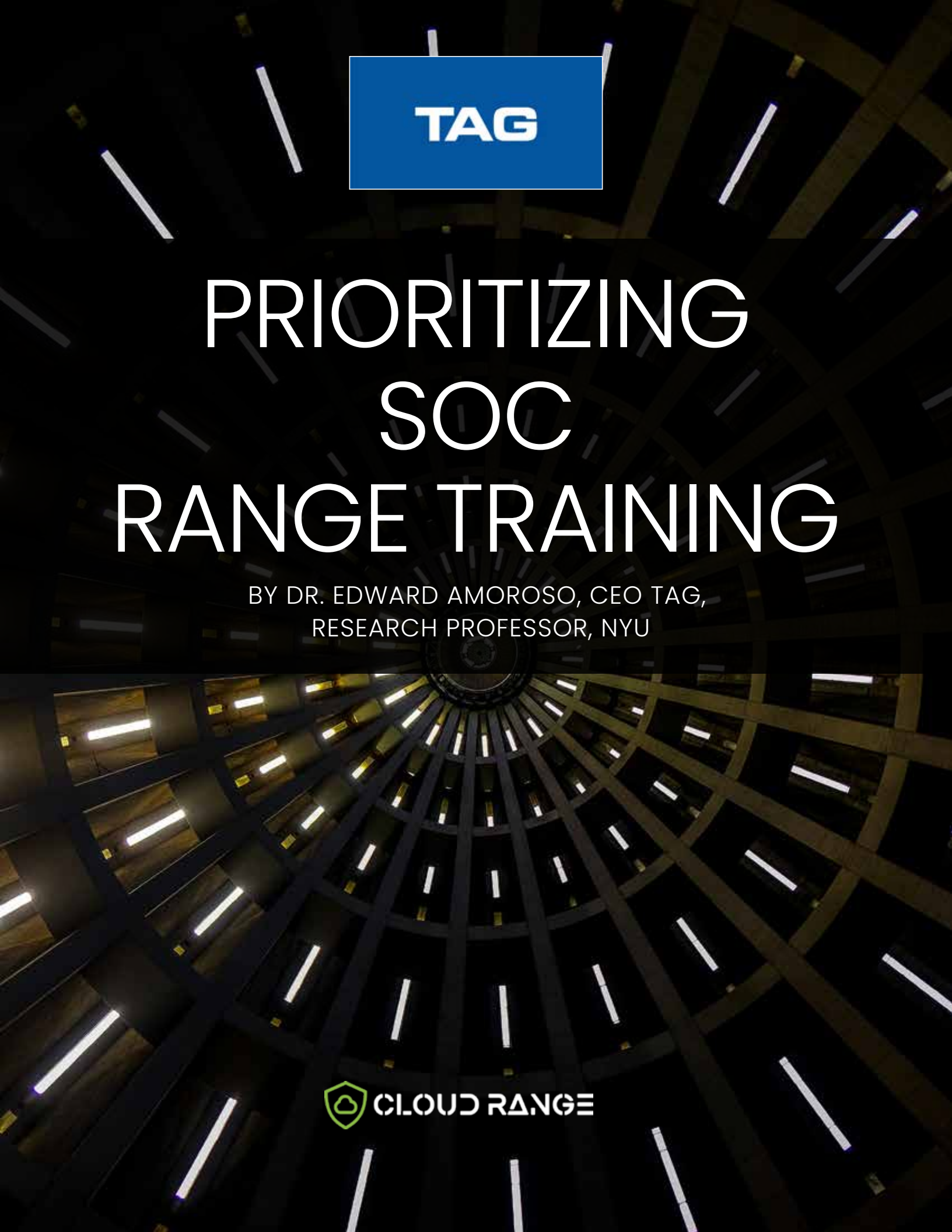

TAG

PRIORITIZING SOC RANGE TRAINING

BY DR. EDWARD AMOROSO, CEO TAG,
RESEARCH PROFESSOR, NYU

CLOUD RANGE

PRIORITIZING SOC RANGE TRAINING

BY DR. EDWARD AMOROSO, CEO TAG,
RESEARCH PROFESSOR, NYU

CLOUD RANGE
cloudrangecyber.com

IT'S TIME TO PRIORITIZE SOC RANGE TRAINING

Range training for the SOC is no longer an option, but rather an imperative and highly prioritized component of any security program.

INTRODUCTION

Our analyst team at TAG strongly recommends that all Security Operations Center (SOC) teams take the time to practice, preferably with support from a commercial vendor, developing realistic, live-fire scenarios and simulations. The decision to train should be obvious to any trained observer, but we reinforce the point mostly because we want to help security leaders ensure proper support and funding for this essential learning function.

THE SHIFT FROM OPTIONAL TO ESSENTIAL

Historically, we watched as SOC training began with passive learning, such as reading manuals, attending lectures, or watching webinars. While this approach was (and is) necessary, it falls short in preparing teams for the dynamic situations they will face during actual incidents. Live-fire simulation offers an immersive environment where teams can practice detecting, responding to, and mitigating real-world cyber threats without the associated risks.

BOARDROOM RECOGNITION

One excellent advance that we have observed is that the benefits of range training have found their way into many boardroom discussions. Boards and senior leadership teams (SLTs) are increasingly aware that cybersecurity is not just a technical issue but a business-critical concern. They understand that a well-trained SOC team can significantly reduce the organization's risk profile, protect its reputation, and ensure business continuity. This is a good trend, indeed.

MANAGEMENT AND PRACTITIONER BUY-IN

Perhaps the greatest challenge is that middle management and frontline practitioners must be guided to recognize the value of range training. Despite budget challenges, managers must be encouraged to value driving team readiness and identifying skill gaps in the SOC. Practitioners certainly appreciate the opportunity to hone their skills, gaining confidence that

improves performance during real incidents. The objective is the ensure that this translated to budget.

RISK REDUCTION THROUGH PREPAREDNESS

Having reviewed, participated, and helped to design many SOC range training engagements for our TAG enterprise and government customers (across all segments sectors, sizes, and scopes), we can summarize the primary operational and cost benefits of the process as consisting of the following – and we hope these benefits are woven into security budget-related discussions in 2025 and beyond:

- **Identify Weaknesses:** Simulations can reveal vulnerabilities in systems, processes, and team coordination that might otherwise go unnoticed until exploited by adversaries. This results in reduced likelihood of incidents going unmitigated, which can reduce response costs considerably.
- **Enhance Communication:** Real-time exercises improve communication channels within the team and with other departments, ensuring a cohesive response during actual incidents. This will also ultimately reduce the high costs of dealing with significant incidents.
- **Refine Processes:** Teams can test and refine incident response plans, ensuring that protocols are effective and well-understood. Our experience is that this can also help to streamline investments in technology, which is an important component of budget rationalization.

We see the deployment and use of these platforms within the security operations center to be no longer an option, but rather an imperative

CLOUD RANGE: A CASE IN POINT

In our estimation, experienced vendors such as Cloud Range have developed sophisticated platforms that provide realistic, customizable cyberattack simulations. We see the deployment and use of these platforms within the security operations center to be no longer an option, but rather an imperative and highly prioritized component of the overall program. Specifically, the Cloud Range platform offers these advantages:

- **Flexibility:** Cloud Range includes tailored scenarios that match the organization's specific threat landscape and infrastructure.
- **Comprehensive Training:** Exercises from Cloud Range cover the spectrum of attack vectors, including phishing, ransomware, and advanced persistent threats.
- **Performance Metrics:** Detailed analytics from Cloud Range will help assess team performance and guide future training efforts.

CONCLUSION

It should be obvious from this brief article where we stand on this issue at TAG: Organizations must prioritize range training as an integral part of their cybersecurity strategy. Period. By doing so, they not only enhance their defense capabilities but also demonstrate a proactive approach to risk management that will resonate with stakeholders at all levels. If you are a stakeholder or decision-maker for any SOC team, I hope you will act on this immediately.

INVEST IN PLATFORMS, BUT DON'T FORGET YOUR PEOPLE

Just as organizations invest in and optimize their security technology, they also have to continue investing in and optimizing their people.

INTRODUCTION

Ask any CISO or security leader today about their investments in cybersecurity, and you'll likely get a rundown of the latest tools they've added: Endpoint Detection and Response (XDR), Next-Generation Firewalls, or perhaps some brand-new AI security guard rail. These are necessary, for sure, but there's a misconception that far too many organizations still make – namely, that technology alone can mitigate major cyber threats.

The uncomfortable truth is that even the best security stack is only as good as the people who operate it. And it is our belief at TAG that unless organizations make sufficient investments in the continuous training and development of their expert security teams, particularly through real-world simulation exercises, their cyber technology investments will fail to reach their full protective potential. Let's dig into this deeper.

THE RATIONALE BEHIND PEOPLE-FIRST INVESTMENT

We can start with a positive trend: Today's boards and senior leadership teams (SLTs) are clearly beginning to understand the business value of investing in security. But with that attention has come a new financial reality: These executives, despite understanding the growing threat from adversaries such as nation states, are beginning to review investment levels to determine the optimal spend.

One observation of note is that leadership of the many different companies that TAG covers in its research and advisory work, has begun to demand rationalization of cybersecurity budgets. This means that every dollar spent on security must map clearly to some measurable reduction in risk. That's precisely why investment in human performance can no longer be considered a luxury, but rather a budgetary necessity.

A new SIEM won't magically detect an advanced persistent threat unless the analysts monitoring it know what anomalies to look for, how to pivot across datasets, and how to escalate appropriately – even in the presence of AI-assisting co-pilots.

Practitioners already understand this requirement intuitively. They can tell you from experience that no matter how interesting the tool, it still takes skill and judgment to use it effectively under pressure. A new SIEM won't magically detect an advanced persistent threat unless the analysts monitoring it know what anomalies to look for, how to pivot across datasets, and how to escalate appropriately – even in the presence of AI-assisting co-pilots.

WHY LIVE-FIRE SIMULATIONS CLOSE THE GAP

This is where the use of live-fire cyber range exercises come in, and we strongly recommend the solution offered by Cloud Range. World-class simulation platforms will immerse SOC teams in authentic, high-pressure attack scenarios designed to test and strengthen their ability to perform the following vital tasks in their day-to-day work (and this includes both virtual and non-virtual security support). Here are some specific benefits:

- **Telemetry Interpretation** – Training helps SOC team learn to better interpret the telemetry that comes from their disparate security tools.
- **Collaborative Work** – The need for SOC teams to work collaboratively across shifts and functional silos is reinforced during simulations and exercises.
- **Decision-Making** – Good training will help SOC teams make rapid decisions, even in the presence of imperfect information.
- **Dynamic Adapting** – Training guides SOC teams to follow their incident response playbooks while adapting dynamically to evolving threats.

Live-fire SOC range training like this builds operational muscle memory that simply cannot be replicated through passive learning methods or product demos. It ensures that people understand not just what the tools do, but how to wield them when it matters most. And we are confident that when this level of maturity is reached, the benefits extend across all aspects of the security program.

BUDGET OPTIMIZATION THROUGH READINESS

Yes – we understand that training, regardless of whether it is for employees, experts, or teams does cost money. But from a budget optimization standpoint, the logic is crystal clear – namely, that significant value comes from the investment. Here are some commonly cited qualitative and quantitative returns on SOC range training that we hear from our enterprise customers at TAG frequently:

- **Reduce Tool Wastage:** Well-trained teams ensure that expensive security platforms are fully utilized and properly tuned. This helps to rationalize budgets.
- **Shorten Response Times:** Teams that have practiced together in live-fire scenarios respond faster and more effectively, limiting dwell time and blast radius.
- **Lower Breach Costs:** Studies consistently show that trained, coordinated SOC teams can significantly lower the cost of a breach when it occurs.
- **Prove Readiness to Auditors and Regulators:** Increasingly, regulators want evidence not just of security tooling, but of human readiness. Live-fire exercises produce the kind of tangible metrics that satisfy these expectations.

LESSONS FROM OTHER HIGH-RISK DOMAINS

We often suggest to senior leadership, whenever the topic of expert training emerges, that they take a moment to ponder the situation in comparable high-risk situations. For example, if you review the training profiles in industries such as aviation, healthcare, or military defense, which are all sectors where lives are on the line, then you will find a serious and disciplined approach to training.

More specifically, the leaders of these industries tend to invest most heavily in simulation training. Pilots, for example, don't just read about engine failures – rather, they experience them in simulators. Similarly, surgeons don't just study textbooks. They practice on lifelike models. Cybersecurity should be no different. The threats are real, the stakes are high, and simulation is the only way to ensure that teams are ready to perform when needed.

CONCLUSION

If your cybersecurity budget only covers technology and not people, then you are leaving your organization vulnerable. Investment in live-fire simulation training must be treated as a core security control, no different from endpoint detection or network security. Companies like Cloud Range offer powerful, practical ways to make that investment count. We believe that training your SOC team is not optional. It's a baseline requirement for real cyber resilience.

WHEN YOU TRAIN YOUR SOC, DON'T FORGET THE AI

Team simulation training requires inclusion of Artificial Intelligence (AI) security platforms to address emerging threats.

INTRODUCTION

In the last couple of years, our team at TAG seen a massive surge in the adoption of AI-based security technologies. Enterprises are purchasing AI-driven threat detection, AI-based risk analysis, and AI-generated incident response recommendations, and this is an exciting development in our industry. But the reality is that buying an AI platform doesn't automatically make your SOC team ready to use it effectively.

Just as with any powerful new technology, mastery comes through practice. That's why today's live-fire simulation training must evolve to explicitly incorporate AI-based security platforms. Enterprise security leaders need to invest the time and energy to train their human defenders not only to recognize traditional threats but also to operate, trust, validate, and at times override AI recommendations.

THE RISE OF AI IN THE SOC

It is not always easy to spot trends as they are occurring, but in the context of AI, we find that identification of on-going decisions, changes, and issues have been relatively easy to spot. In particular we have noticed that most SOC teams now have at least one or two AI-enhanced platforms in their

stack, which implies the need to understand how to use such technology. Specifically, these systems are capable of the following functionality:

- **Prioritizing SOC alerts using machine learning.**
- **Suggesting the best possible response actions in real time.**
- **Automatically correlating events across vast datasets.**
- **Even recommending policy changes based on behavioral analytics.**

While these capabilities are valuable, they introduce new complexities. Analysts must understand how these AI models reach their conclusions. They must recognize when a model's recommendation is spot-on, and when human judgment must override automation to avoid catastrophic errors. Our view is that SOC training become an essential element of the equation in dealing with this new challenge from AI.

SIMULATION TRAINING: THE MISSING PIECE

SOC teams tend to train their analysts to react to threats manually, without the assistance (or complication) of AI input, and that's a gap that must be closed.

Unfortunately, most traditional training exercises have not accounted for these realities – and this is understandable given the relatively recent introduction of AI to the SOC. As such, SOC teams tend to train their analysts to react to threats manually, without the assistance (or complication) of AI input, and that's a gap that must be closed. Forward-looking platforms like Cloud Range have recognized this and are evolving their exercises to support the following:

- **Inject AI Decision Points:** Teams must decide when to trust AI recommendations versus when to dig deeper.
- **Simulate AI Errors:** Exercises include scenarios where the AI suggests incorrect actions, training teams to spot and correct these issues.
- **Model Adversarial AI Attacks:** Simulations where attackers attempt to poison or manipulate AI models, preparing teams for emerging threats.

LEARNING TO WORK WITH (NOT AGAINST) THE MACHINE

The most effective SOC teams in the coming years will be those who know how to partner with AI in order to achieve the following key operational objectives, each of which we believe will soon characterize a new normal in SOC support:

- **Understand Bias and Limitations:** Teams must grasp that AI models are only as good as their training data and that biases can creep in.
- **Validate and Corroborate:** Analysts must learn to validate AI-generated alerts against independent telemetry before acting.
- **Tune the Models:** Security engineers must practice adjusting AI thresholds and feedback loops based on organizational needs.

All of these skills can, and should, be developed through live-fire range exercise, and our observation at TAG is that Cloud Range does a particularly effective job in each of these important areas.

THE RISK OF BLIND TRUST

Blindly following AI outputs without human scrutiny is a recipe for disaster. Adversaries already recognize this and are developing attack strategies aimed at tricking or manipulating AI systems. Through targeted range training, SOC teams can learn how to:

- **Spot adversarial manipulation attempts.**
- **Recognize when AI is being used against them.**
- **Maintain vigilance and critical thinking even in an automated environment.**

CONCLUSION

When we are honest, we must acknowledge that the future of cybersecurity will not be purely human or purely machine. Rather, it will be a hybrid model where skilled people leverage powerful AI tools. But that synergy doesn't happen automatically. It requires deliberate, structured training, and SOC management would be wise to understand this new requirement in the immediate term.

Organizations must now prioritize live-fire simulation exercises that include AI decision-making dynamics. Platforms like Cloud Range are leading the way, offering environments where SOC teams can learn how to co-pilot security operations with AI. In the end, our best defense will come not from the machine alone, but from trained humans who know how to partner with it wisely.

CYBER ATTACKS DON'T WAIT. MAKE SURE YOUR SOC TEAM IS TRAINED

It is not possible to predict when a serious attack will hit your organization, so make sure you take time to do the advance training for your experts.

INTRODUCTION

> f there is one thing I've learned in my four decades in cybersecurity, it is that our adversaries operate on their own schedule. It would be nonsense, for example, to imagine them sitting around and waiting for your SOC team to be ready. And they certainly will not wait for then to finish onboarding a new analyst or complete their quarterly compliance training. Instead, they are active *when they choose to engage.*

This means that your team must be ready, and not just in theory. At TAG, we've observed repeatedly that the difference between a contained event and a full-blown breach often comes down to whether the SOC team has had hands-on, live-fire simulation training.

ATTACK TIMELINES VS. READINESS TIMELINES

One of the more common findings from our enterprise security support and our assessments is a dangerous mismatch between the pace of cyber-attacks and the preparation cycles of SOC teams. Many organizations schedule training sporadically, or worse, assume new hires will "pick it up on the job."

Meanwhile, attackers continue to innovate, automate, and launch attacks at scale. The simple truth is this: If your SOC team is not proactively training on realistic threat scenarios, then you're betting the farm on something that does not need to be so broken.

We recommend aligning training cadence with threat cadence. That means SOC teams should be running simulations monthly or quarterly. It also means adjusting exercises to reflect current threat intelligence, something that advanced platforms like Cloud Range have made easy to implement.

THE FALSE COMFORT OF TECHNOLOGY ALONE

Some will assume that tools can compensate for team inexperience, but our research shows otherwise. Even the most advanced EDR or SIEM platform won't defend your enterprise unless the human operators know how to interpret alerts, connect data, and make decisions. Too often we find that SOC teams freeze during early incident response, not because they lack intent, but because they lack muscle memory.

Live-fire range training creates this muscle memory. It immerses analysts in simulated attacks, allowing them to learn by doing, not by watching. This is particularly vital during the first few minutes of an attack when time, not tools, is the most precious resource.

REAL-TIME SKILLS ARE NON-NEGOTIABLE

Importantly, it's designed to mimic not just technical threats, but also the real pressure SOC teams experience when making decisions under stress.

Through dozens of enterprise and government simulations we've reviewed or participated in, TAG has found that well-run SOC range training consistently produces the following measurable benefits in the following areas:

- **Faster Initial Response** – Simulations reduce hesitation and help analysts trust their instincts during the first few minutes of an alert.
- **Stronger Coordination** – Live exercises reinforce cross-team communication that often breaks down during real attacks.
- **Increased Alert Fidelity** – Teams that train on telemetry interpretation improve their ability to prioritize real threats over noise.
- **Lower Escalation Errors** – Practice helps teams escalate the right alerts, to the right people, at the right time.

CLOUD RANGE AS A TACTICAL ENABLER

We believe that Cloud Range is one of the few platforms capable of delivering continuous, customized simulation at the scale enterprises require. Their range training supports a variety of attacker tactics, keeps pace with threat trends, and provides measurable feedback on analyst performance. Importantly, it's designed to mimic not just technical threats, but also the real pressure SOC teams experience when making decisions under stress.

CONCLUSION

Your SOC preparation should not be left to ad hoc checklists or quarterly tabletop exercises. Live-fire simulation should be a core control, not an optional benefit. The attackers are active now, so your team must be trained now. At TAG, we urge every cybersecurity leader to recognize this reality and ensure their teams have the tools and the training they need to succeed when the next threat hits.

BEYOND THE TECH, SKILLED EXPERTS ARE STILL KEY TO SECURITY

Regardless of what happens with technology evolution, your skilled experts are still the primary means by which you engage in an effective defense.

INTRODUCTION

As we continue our enterprise research and field engagement at TAG, one pattern keeps re-emerging: organizations are beginning to rely a bit too much on the future promise of automation and tooling to solve their problems today.

This is a mistake, and it can lead to underinvesting in the people who must ultimately wield those tools. We fully acknowledge the power of artificial intelligence (AI) and we are excited for its possibilities. But the immediate-term truth is simple and perhaps uncomfortable: Cybersecurity remains today a mostly human-centered discipline.

We all know that the platforms and tools we have today, many of which are becoming AI-enabled, provide an awesome hybrid arrangement, as we have written so many times in our work at TAG. But without expert operators in the SOC, the operation as it stands will not work. Instead, the path to resilience today runs directly through your people. And the best way to strengthen your people is through hands-on SOC range training.

TALENT SHORTAGES AREN'T THE ONLY PROBLEM

Much has been written about the shortage of trained cybersecurity professionals. But at TAG, we believe there's a deeper problem, one that affects even fully staffed SOC teams. The issue is that many analysts are not properly trained.

Yes, they've taken SANS courses, watched vendor demos, or learned attack techniques on YouTube. But mist haven't practiced reacting to the chaotic, multi-threaded incidents that define modern attacks today. This training gap can lead to two undesirable outcomes:

These exercises teach judgment, pattern recognition, and teamwork, which are skills that no platform or product alone can provide.

1. **Over-reliance on Tools** – Teams might defer to dashboards they barely understand instead of learning the threat context.
2. **Slow Escalation** – Analysts can take too long to act because they haven't experienced similar scenarios in a low-risk setting.

SOC range training addresses both gaps. By putting analysts into realistic attack environments, these exercises teach judgment, pattern recognition, and teamwork, which are skills that no platform or product alone can provide.

TRAINING AS A MULTIPLIER FOR TECHNOLOGY

We hope that you are investing in AI-based detection, SOC orchestration, and behavior-based anomaly tools. But TAG's view is that every one of those platforms becomes more valuable today, and more cost-effective today, when operated by a trained team. Consider these simple training-induced multipliers:

- Improved Tuning – A well-trained analyst can calibrate false positives and false negatives better, making platforms more precise
- **Faster Playbook Execution** – Analysts who've practiced incident response will execute workflows more efficiently.
- **Better Analyst Retention** – Practicing real-world threats increases confidence, morale, and retention, which are important in a competitive hiring market.

That's why Cloud Range has earned our endorsement: Their platform not only supports SOC technical development but also drives measurable operational improvements, with feedback loops that show how skills are improving over time.

A REMINDER FROM OTHER DISCIPLINES

We often remind executives of one of the simplest truths from other high-stakes industries: Simulation works. Fighter pilots, trauma surgeons, and astronauts all train through rigorous simulation. Why? Because when failure has high consequences, preparation must be realistic. Cybersecurity is no different.

And yet, too many SOC leaders still prioritize their tooling over training. At TAG, we think that's backwards. Your stack is only as good as your team's ability to respond, and SOC range training is how that ability is forged.

CONCLUSION

Security vendors will continue innovating, especially in AI, and that's good. But we must not lose sight of the fact that skilled people remain the foundation of effective cybersecurity. The reality today is that our tools amplify human effort. SOC leaders should be looking forward, but they also must acknowledge that to deal with their problems today, they must prioritize range training as a frontline investment, not a discretionary one.

If your security plan for this year doesn't include structured, realistic team training, then it's incomplete. We strongly recommend a commercial platform like Cloud Range, which offers a mature, flexible, and proven approach to preparing SOC analysts for the reality they face every day – not in theory, but in practice.

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,.


TAG
PRIORITIZING
SOC
RANGE TRAINING
CLOUD RANGE