CLOUD RANGE

CASE STUDY:

GLOBAL TELECOMMUNICATIONS COMPANY

SOC Team Continuously Improves Cyber Readiness Using Cloud Range's Attack Simulation Training Program

AT A GLANCE

CHALLENGES

- Leaders needed more confidence in team's preparedness levels
- No way to measure team members' skills and abilities
- Traditional certifications and education not enough
- Can't do on-the-job training during a cyber attack
- Team didn't have a way to train as cohesive unit
- Team members lacked confidence in their own abilities

RESULTS

- Measurably improved incident response, team performance, and communication
- Reduced noise for leadership
- Boosted culture and team
- Augmented critical thinking and problem-solving
- Elevated visibility of team leaders and security executives
- Provided actionable metrics and reporting
- Created prescriptive, customized training plans to ensure continued preparedness

9.1/10

average overall experience score of participants

100%

of participants said the cyber range and simulation training experience contributes to overall job satisfaction

100%

of participants said that doing these types of exercises will help them and their team be more prepared for future events

> “Awesome simulation! The consequences of an attack can be devastating and it is great to be able to practice handling and responding to it ahead of time.”
>
> — **MEMBER OF GLOBAL TELECOMMUNICATIONS COMPANY SOC TEAM**

Background

A global telecommunications provider faced persistent and increasingly sophisticated cybersecurity threats. The organization’s security operations center (SOC) team was made up of skilled people with impressive degrees and certifications, but there was a lack of understanding of how the team members’ training and certifications translated into actual preparedness. Was the team able to effectively and accurately handle cybersecurity incidents – especially when there is pressure and time is of the essence?

The big problem to solve with the SOC analysts, incident response team members, threat hunters, penetration testers – people of different skill levels, competencies, and backgrounds – was how to have them **work as a cohesive unit during an incident**.

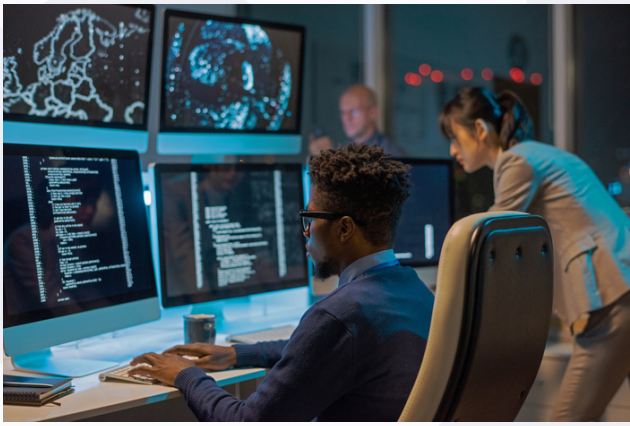
Leadership needed a way to **feel confident** about its SOC team’s readiness, which required technical skills and soft skills to ultimately decrease response times.

The company searched for a solution that would enable the group to train on both an individual level and team level to promptly identify and mitigate cyber threats and effectively interact as a unit and with company leaders.

Program Goals

After an extensive search and vetting process for a training solution, the telecommunications provider chose to implement a cyber range and simulation training program for its security team and partnered with **Cloud Range**, the leading provider of comprehensive cyber range-as-a-service solutions.

The telecommunications company saw the value and strategic advantage in using live-fire simulation to improve cyber readiness and reduce exposure to cyber risk for the entire organization. It appreciated that Cloud Range's holistic cyber readiness platform boosts technical proficiencies, enhances soft skills, and provides guidance and learning plans – all on both a team and individual level. An internal champion emerged within the telecommunications organization who helped to promote the benefits of the cyber range solution and ensure it was used effectively.



While initially interested solely in red team vs. blue team exercises, the organization broadened its focus after learning about Cloud Range's experience in, and extensive library of, cyber attack simulation scenarios for blue teams. The organization's champion of Cloud Range's cyber range simulation program understood that blue teams were the last line of defense against cyber threats and wanted to ensure those team members were prepared for whatever came their way. The champion led the way to start the program with blue team training.

The organization outlined its goals with the cyber range training program:

- Detect possible intrusions before they become incidents (convert incidents into alerts)
- Speed up creation and approval of alerts
- Develop the skills to navigate cybersecurity challenges
- Identify potential leaders

Additionally, the security leaders needed to be able to ***very quickly*** convert a large amount of detailed information into an easy-to-read format that would be relevant to executive leadership.

> "I liked the whole attack simulation. It was very engaging and informative. The collaboration aspect really kept me engaged and helped us hone in on our teamwork skills."
>
> — **MEMBER OF GLOBAL TELECOMMUNICATIONS COMPANY SOC TEAM**

A GREAT TEAM THAT GOT EVEN BETTER

Measurably improved incident response times and readiness

Accelerated onboarding and time to value of new team members

More confident, prepared team

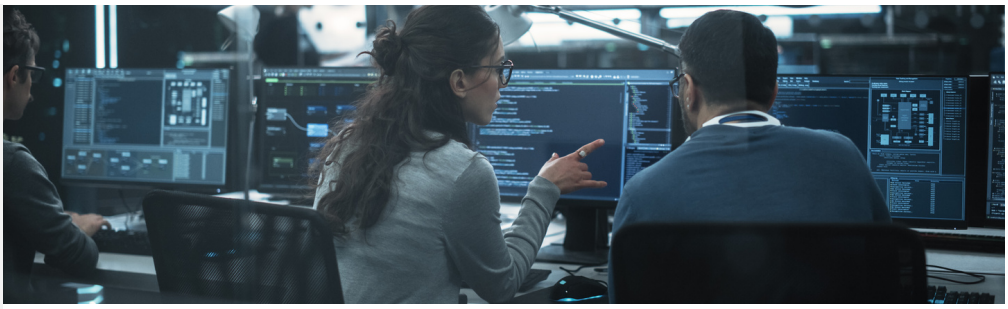
Enhanced communication among the team and between the team and leadership

Actionable metrics & results

Augmented critical thinking and problem-solving skills

Better camaraderie and more collaborative culture

Time to do what matters



The Cloud Range Solution

Cloud Range created a customized cyber readiness program to meet the organization's objectives and build on the team's existing capabilities and skill sets.

Products:

FlexRange™ Simulation Training Program

- An annual subscription of realistic cyber range exercises
- Monthly simulated live-fire cyber attack scenarios
- Each exercise led by expert Attackmasters™ – instructors who are with the team throughout the "mission" to answer questions, provide hints and counsel, debrief the team after completing the scenario, and evaluate performance
- Scenarios get more advanced as team grows in their proficiency and confidence
- All mapped to MITRE ATT&CK and NIST/NICE Frameworks

OpenRange™ cyber range access

- Designated time on virtual cyber range so the team can practice on their own

The team enjoyed the flexibility that Cloud Range provides. They found that the sweet spot for FlexRange missions was to have **5-8 active participants**, which allowed each person to take on different roles and have a chance to shine. Then, the whole group could use OpenRange to work together as a full team. The ability to **use the range in different ways** allowed them to combine guided training and self-practice, fostering both individual growth and team collaboration.

After each completed mission, Cloud Range held a **review directly with the team's leaders** to assess performance and outcomes, ensure alignment and progress toward the organization's objectives, and discuss challenges and opportunities. The leaders also received detailed metrics and analyses on an individual and group level showing ongoing improvement, which could also be used for reporting to the organization's executive leadership.

Results

Clear, success-oriented goals defined the partnership with Cloud Range, including:

- Effect measurable improvements in detection and response time
- Identify potential future leaders within the team
- Generate team enthusiasm for upcoming missions

These goals were met and exceeded, marking a significant step towards strengthening the company's cyber defense capabilities.

The professional and strategic approach of the training program significantly exceeded the goals established for the SOC team, prompting the organization to **extend its annual contract** with Cloud Range. The program has also **expanded** to add a program of red team vs. blue team training and Range365, Cloud Range's customizable, dedicated cyber range platform.

REDUCED NOISE FOR LEADERSHIP

With such a large SOC team (approximately 24 people), the organization's security leaders were concerned about the potential burden to coordinate schedules and set up the training missions. However, since the FlexRange program is full-service, Cloud Range handles all of the planning and scheduling of missions. Additionally, Cloud Range gave the team lead assistance and insights to create individual learning paths, ensuring each person on the SOC team had a training plan to continue to develop their careers.

CULTURE BOOST DURING PANDEMIC

After the first few missions, the COVID-19 pandemic pushed security team members into quarantine, preventing further onsite team training. Fortunately, Cloud Range was already equipped to deliver missions virtually to distributed security teams. Despite initial reservations about conducting the missions with a fully remote workforce, the virtual platform shift proved more beneficial than anticipated. It reignited team interactions stifled by remote work, improving communication and culture. This transition sparked renewed enthusiasm and anticipation for upcoming missions.

ENHANCED TEAM PROFICIENCY THROUGH PROGRESSIVE COMPLEXITY

The organization's SOC team, already highly skilled, saw their abilities accelerate under the program. Cloud Range's adversarial engineering team created new cyber attack scenarios and adjusted existing ones as needed to be more varied, complex, and harder to detect – keeping the team consistently engaged, challenged, and increasingly efficient.

> "Having a great instructor like the Cloud Range Attackmaster really kept me engaged and interested in the scenario we went over. Experiencing a simulated event like this one also helped me increase my technical and investigative knowledge."
>
> — **MEMBER OF GLOBAL TELECOMMUNICATIONS COMPANY SOC TEAM**

Results, continued

> "I really enjoyed this experience. I really think that this taught me a lot of what to look for as well as how to balance communications with management and technical response efforts. It was clear which parts needed improvement in our efforts."
>
> — **MEMBER OF GLOBAL TELECOMMUNICATIONS COMPANY SOC TEAM**

DETAILED METRICS AND ANALYSIS

The insightful reports and analyses from Cloud Range provided a deep understanding of the group dynamics, individual performance, and the simulation program's overall value in enhancing cyber defense capabilities. In the process, Cloud Range became a true partner, working alongside security leaders to identify and bridge gaps and tailor specific solutions for continuous improvement. The access to comprehensive metrics and key indicators simplified presentations to executive leadership and the board. These benefits not only measurably improved cyber readiness but also elevated the profile of security leaders within the organization, including the program's champion.

ESTABLISHED CAPSTONE EVENT

Cloud Range worked closely with the team lead to design a season-ending capstone event worthy of attendance by the organization's leadership. Cloud Range Attackmasters created a custom red team vs. blue team exercise that allowed the entire SOC team to demonstrate their improved technical abilities as well as their critical thinking skills and communication. Leadership saw how the training had taken the team to a new level of cyber defense capabilities, and the team ended the season feeling a sense of accomplishment.

SCALABILITY TO FIT NEEDS

The organization appreciated that Cloud Range can tailor products and services to their needs. Additionally, as goals have changed over time, Cloud Range has adapted its technologies, products and services. While Cloud Range already incorporated many fully licensed security tools, such as Splunk, CheckPoint and ArcSight, additional tools were added. To better emulate the organization's SOC within the cyber range, Cloud Range customized training by integrating IBM QRadar, FortiGate, and CrowdStrike Falcon. Additionally, as the team wanted more time with a cyber range and control over its customization, it moved to Range365, Cloud Range's hosted cyber range solution that provides an unlimited training and testing sandbox. Further, while the program started with blue team training, the organization has taken advantage of Cloud Range's holistic suite of cyber readiness solutions and incorporated additional products and services including additional live-fire team training.

Conclusion

The organization saw immediate and ongoing value in Cloud Range's unique cyber range training program. Cloud Range's solutions have helped build a strong SOC team that is measurably prepared to defend against any kind of cyber attack. The group has enjoyed learning new things, collaborating, and getting to know their teammates better. In fact, they enjoy it so much the training sessions are typically scheduled for Fridays because **they are seen as a reward**. Additionally, the leaders appreciate that the program allows them to assess and prove the effectiveness and efficiency of their security team. **The organization is more confident in its SOC team and how they work together as a unit to remediate attacks and reduce exposure to cyber risk.**

LEARN MORE ABOUT CLOUD RANGE AND PRODUCTS MENTIONED

- Cloud Range Cyber Range-as-a-Service
- Live-fire attack simulation scenarios for teams
- FlexRange cyber range training program
- Blue team exercises
- Red team vs. blue team scenarios
- Attack scenarios
- Range365 customizable, dedicated cyber range platform

ENSURE YOUR CYBER TEAM IS READY

Reduce risk with Cloud Range's customized cyber simulation solutions for teams

ABOUT CLOUD RANGE

Cloud Range, the world's leading cyber range-as-a-service, measurably decreases cybersecurity exposure and overcomes the staggering cyber skills gap by proactively preparing cybersecurity operations teams to defend against complex attacks through a customized simulation-based cyber attack training program. The full-service cyber simulation training and assessment platform includes customizable, cloud-based cyber ranges; live-fire team simulations; red, blue, and purple team and CTF exercises; 1,500+ individual skill development labs; advanced tabletop exercises; hiring assessments; IT and OT environments; and detailed reporting and analysis.