SANS

US Army Gets Battle-Ready with
SANS Cyber Situational Training eXercise

CYBER STX
CYBER RANGE

"There will always be that need to have heavy armored forces and infantry soldiers to do what they need to do, but now that we are fighting in multi-domain operations, we need to have the ability to fight by air, ground, sea, space, and cyberspace,"

– Mark Esper, Former US Secretary of Army

SANS CYBER RANGES

07232021

EXECUTIVE SUMMARY

The US Army needed a way to train cyber security professionals that mirrored the kinds of threats and environments they face in the real world so they could validate their soldiers were battle-ready. They found their match in **SANS Cyber Situational Training eXercise (Cyber STX)**, which provides highly realistic exercises to ensure participants are ready to engage with very determined adversaries. With Cyber Protection Teams (CPT) of 50-100 soldiers from the first cyber brigade participating in multiple Cyber STX exercises with SANS, the Army was able to train their team, evaluate their tools, and fine-tune their Tactics, Techniques, and Procedures (TTPs).

"Being placed in a contested environment with actual adversaries offers us a chance to test new strategies, enhance our tactics, and rehearse our procedures so that we are more effective and adaptive in real-world scenarios."

– Capt. Michael Milbank

WHAT IS CYBER STX?

- Live fire, weeklong red-on-blue cyber range emulating an Advanced Persistent Threat (APT) in compromised IT and OT environments.
- Custom, detailed campaign using the TTPs and Indicators of Compromise (IOCs) of one or more APTs.
- Run anywhere, with local participants, remote participants, or mixed mode.
- Ideal training for military groups seeking in-depth training and validation, Cyber Protection Teams, government agencies responsible for defending critical systems, and large private industry organizations protecting complex infrastructure.

"There are lots of cyber ranges, but they don't have those rich training scenarios where you have an adversary that is being emulated -- a real advanced persistent threat -- and they bang away at the Cyber Protection Teams."

— John Nix, director of federal for SANS Institute

"I was very impressed by what I saw, not just with cyber but with all the capabilities and challenges presented here at this training range and what it could mean for a wide range of Army forces."

— Mark Esper, Former US Secretary of Army

CHALLENGES

As the five-day training range kicked off, there were several challenges that the team faced:

- With roughly 50 soldiers on each of the two teams, including local and remote participants, everyone began trying to share battle intelligence with everyone else all at once, clogging communications channels.
- The team has to learn dynamically how to throttle their communications and focus on the most important details.
- The Army needed their cyber soldiers validated in order to be able to go on missions, and to attain that validation, they needed the ability to get individual soldiers who were at all different levels of experience and capabilities up to the same top level.

RESULTS

- Identified leaks in the tools being used, which would send out a beacon on the network that revealed information on where Cyber Protection Teams were based.
- Produced data that was handed off to military evaluators for them to determine whether soldiers are ready to fight in real-world missions.
- Improved the soldiers' skills and helped them learn new capabilities to build up team confidence.

LESSONS LEARNED

During the After-Action Review (AAR), the teams discussed ways to better engage the adversary and work together more effectively:

- Needed to establish a battle rhythm and communication early on or else nothing was going to get done.
- Fighting with their own tools allowed them to evaluate not just their people but also their tools and their knowledge of those tools.
- Evaluated and refined their own Tactics, Techniques, and Procedures.
- Discovered they were too shy and hesitant to go on the host network and that they needed to better understand what was and was not acceptable risk.
- Identified weaknesses in soldiers' analysis kits, as SANS' red team was able to hack into their kit, pivot through it, and use its place on the network to get access to the ICS environment.

BENEFITS

The Army indicated that Cyber STX provided the most realistic exercise they had ever done. Benefits include:

- While SANS gives recommendations about what the exercise should look like, the US Army ultimately chose the adversary, one that mirrors their real-world missions.
- The US Army was able to validate that teams and individual soldiers have capabilities required by their Master Scenario Events List (MSEL), showing that they are operationally ready to go fight on missions around the world.
- With months of planning going into each Cyber STX exercise, participants are ensured the scenarios are customized to match their requirements and exercises include specific elements needed to provide the most valuable and realistic cyber range experience.

"The way things are going, every military mission — even the purely kinetic ones — will have a cyber component. That's because all of your equipment, all of your munitions, everything is networked together. And if you cannot maintain control of your computer systems, you really can't maintain control of your fighting forces."

— Ed Skoudis, SANS director for cyber ranges

"[The goal is to get operators] comfortable being uncomfortable. If we can understand all the different possibilities in ways to gain access to the network, we can better protect the network."

— John Womble, Army Cyber Protection Brigade training officer in Ft. Gordon, GA

SANS
CYBER RANGES

CYBER STX
CYBER SITUATIONAL TRAINING EXERCISE

The premiere in-depth training and validation cyber range
To learn more, visit sans.org/cyber-ranges/cyber-stx