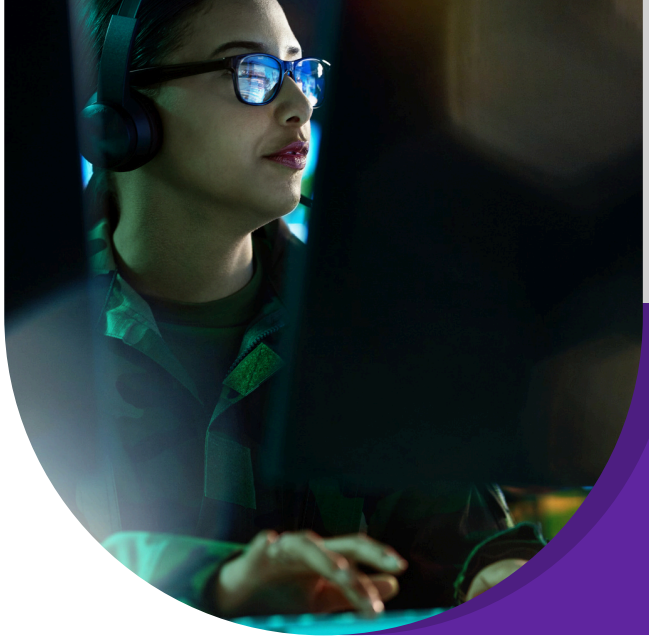

CLOUD RANGE

CASE STUDY:

NEBRASKA NATIONAL GUARD'S ANNUAL INTERNATIONAL EVENT FOR IMPROVED CYBER READINESS

2-Week Incident Response Simulation Training Event Uses Cloud Range to Strengthen Cyber Defenses and Collaboration of Military, Government, and Civilian Organizations

SUMMARY

Cyber Tatanka, a flagship cybersecurity training event led by the **Nebraska National Guard**, offers a unique platform for collaboration and skill-building in defensive cyber operations. This annual two-week event, conducted in partnership with civilian organizations and state and international partners, aims to enhance cybersecurity capabilities and foster partnerships across sectors.

Cloud Range played a pivotal role in providing a cutting-edge virtual threat environment (VTE) and multiple live-fire attack simulation exercises that facilitated immersive, hands-on training for participants from diverse backgrounds.

CYBER TATANKA

BY THE NUMBERS

- 194 participants
- 13 teams on 13 cyber ranges
- 9 live-fire simulation exercises conducted by all teams simultaneously, increasing in complexity throughout week
- Attendees from 6 states, 6 countries, 3 armed service branches, 10 government entities, 3 higher education institutions, and 10 civilian organizations
- 12 critical infrastructure sectors represented

Background

Cyber Tatanka is an increasingly popular annual two-week event designed to improve incident response capabilities and promote interoperability among military, governmental, and civilian organizations. Led by the Nebraska National Guard in partnership with multiple civilian organizations, the event provides realistic, hands-on defensive cyber training exercises in a safe, controlled environment.

With the goal of improving cyber defense for Nebraska entities – and many others through partnerships with other states and countries – Cyber Tatanka is focused on learning, real-world experience, and collaboration. It enhances cyber skills, as well as communication and collaboration between industry leaders; the National Guard; international military partners; federal, state, and local governments; and non-governmental organizations to protect critical infrastructure from cyber threats. This unique opportunity allows service members and civilian participants to train in a joint environment, enhance military readiness, build partnerships, become more cyber secure, and provide key services with lasting benefits to the community.

The world is becoming increasingly interconnected, which means the need for robust cybersecurity measures has never been more pressing.

With the event in its third year and having a record number of registrants, the organizers wanted to upgrade capabilities and refine objectives from previous years. The previous cyber range platform served their needs at

Why "Cyber Tatanka"?

"Cyber Tatanka" draws its name from the Lakota word **tȟatȟáŋka**, meaning "big beast," referring to the bison, an animal revered by the Lakota people for its life-sustaining qualities. The bison was much more than just a source of food; it provided clothing, shelter, and tools, symbolizing self-sacrifice and generosity. In Lakota tradition, the bison is a sacred symbol of the divine, embodying the spirit of giving.

Similarly, cyber systems are the lifeblood of our modern world, providing essential connectivity and protection. Just as the bison sustained the Lakota, "Cyber Tatanka" emphasizes the vital role of cyber defense in safeguarding our digital existence, highlighting the need for resilience and preparedness in today's interconnected world.

Background, continued

the time, but they needed a more sophisticated platform, more variety of simulations and tools, and a better, more stable user experience. They required a platform that could not only deliver a wide range of realistic simulations but also support a large and diverse group of participants, including military, government, and civilian organizations from multiple countries.

After an in-depth search and bidding process, Cloud Range was selected to be the new cyber range and simulation platform. Cloud Range's VTE proved to be a robust and flexible solution and was the core technology for the two-week event. The platform offered a seamless experience with missions that started on time, a broad array of tools and simulations tailored to the event's needs, and the scalability to accommodate future growth.

The overall experience with Cloud Range was overwhelmingly positive. The platform's reliability and depth allowed for smooth execution of the event, and participants gained valuable hands-on experience. This success not only enhanced the reputation of Cyber Tatanka but also generated increased interest in future iterations of the event. With Cloud Range, the organizers were able to overcome previous challenges and position Cyber Tatanka for continued growth and impact in the cybersecurity community.

> "The goal of this event is to introduce an accessible virtual training environment that serves participants globally, allowing them to improve cybersecurity capacity and preparedness through collaboration using real-life scenarios."
>
> — **RYAN CARLSON, LEAD TECHNICAL PLANNER OF CYBER TATANKA**

Event Structure: Two Weeks of Training and Simulation

Cyber Tatanka was structured into two distinct weeks to maximize learning and skill-building.

WEEK 1: TRAINING AND ORIENTATION

The first week focused on training and orientation, providing participants with the foundational knowledge needed for effective cyber defense. During this phase, attendees engaged in courses covering SOC core skills, active defense, enterprise forensics, threat intelligence, and more. They also spent time familiarizing themselves with the VTE provided by Cloud Range, adjusting the systems and tools integrated into Cloud Range's platform, and updating their alerts and procedures to prepare for the upcoming simulations.

WEEK 2: HANDS-ON SIMULATIONS

The second week was dedicated to hands-on simulations, where participants faced realistic cyber threats in a controlled environment.

- Cloud Range delivered **nine live-fire simulation exercises simultaneously to 194 participants in 13 different teams** throughout the week – two per day on Monday through Thursday, and one on Friday morning.
- The attack simulations **increased in complexity** during the week, exposing teams to a range of threats from script kiddies to insider threats.
- These exercises were **based on the MITRE ATT&CK framework** and emphasized collaboration rather than competition, allowing teams to learn from each other and improve their collective defenses. The immersive simulations **reinforced the importance of teamwork and communication**, building confidence and camaraderie among participants.

Cloud Range's Role: Crafting a Virtual Battlefield

A leading provider of virtual threat environments (VTE) and a key player in the success of Cyber Tatanka, Cloud Range used its realistic and immersive cyber range to transform the training landscape into a dynamic battlefield where participants could hone their skills in real-time.

Cloud Range's cloud-based platform was pivotal in delivering a seamless experience for the event. The VTE allowed participants to access cyber ranges through standard web browsers, eliminating the need for specialized software and enabling easy entry into the virtual battlefield. With the capacity to support myriad teams and participants at one time, Cloud Range ensured that the event could accommodate the anticipated growth and diversity of teams.

Virtual Threat Environment (VTE) Setup

- **Scalable and Accessible Platform:** Cloud Range provided a SaaS-based cyber range accessible via standard web browsers, supporting up to 20 enclaves, or teams, with up to 15 participants each. The range was designed for scalability and ease of access, eliminating the need for specialized software.

- **Pre-Event Coordination:** Cloud Range conducted an initial kickoff meeting and regular updates with exercise planners to ensure alignment and readiness. A final VTE walkthrough was conducted 15 days before the event to familiarize planners with the systems and tools.

- **Enclave Template and Topology:** Cloud Range delivered a comprehensive environment topology with customizable resources. The setup allowed for dynamic IP schema adjustments to prevent repetitive response strategies and tailored configurations for varying team sizes and skill levels.

Exercise Development and Execution

- **Scenario Library and Training Arc:** Cloud Range customized and coordinated live-fire simulations for each day of the event, following a structured training arc that got progressively complex throughout the week:
    - Day 1: Script Kiddies
    - Day 2: Hacktivists
    - Day 3: Cyber Criminals
    - Day 4: Advanced Persistent Threats (APTs)
    - Day 5: Insider Threats (half-day)

  Each scenario was mapped to the MITRE ATT&CK framework, ensuring participants encountered specifically requested real-world tactics, techniques, and procedures (TTPs) of bad actors and threat groups.

- **Dynamic and Realistic Simulation:** Cloud Range provided real-time adjustments to scenario difficulty, matching participant skill levels and simulating realistic enterprise environments. Automated Red Team activities ensured efficient threat injection and monitoring.

CYBER TATANKA 2024

WHO
Nebraska National Guard (NENG), other National Guard units, federal and state agencies, industry partners, international partners

WHAT
Conduct defensive cyber operations (DCO) to build incident response (IR) capabilities

WHEN
June 3, 2024 – June 14, 2024

WHERE
Kiewit Hall, University of Nebraska, Lincoln

WHY
Enhance understanding and capability to react to cyber incidents, build partnerships, and improve communication and support for Nebraska Emergency Management and critical infrastructure

HOW
Conduct live-fire cyber exercises within a virtual threat environment and preparatory coursework to simulate scenario-driven cyber attacks

Tools, Reporting, and Feedback

- **Cyber Defense Tools:**
  Cloud Range's platform integrates numerous licensed tools including SIEMs, firewalls, IDS's, endpoint security systems, analysis tools, and more, allowing trainees to practice using the same products they use every day. Cloud Range implemented and provided support for multiple specified tools during the event, with flexibility to offer alternatives as needed.

- **Situational Awareness and Reporting:**
  Cloud Range provided Common Operational Pictures, or simulation guides, for real-time scenario oversight, a web-based performance portal for situational reporting, and a feedback loop with Red/Purple Teams for Blue Team assessment.

- **After Action Review (AAR):**
  Daily debriefs were conducted to reinforce learning, as well as a full after-action discussion on Friday afternoon. An after-action report was submitted within 30 days, highlighting performance, strengths, weaknesses, and lessons learned.

Roles and Responsibilities

- **Red Team:**
  Automated injects and simulations using playbooks/scripts, providing inject functions checks and mission readiness confirmation.

- **Purple Team:**
  Evaluated Blue Team responses, offered feedback, and conducted daily debriefs and overall exercise AAR.

- **Blue Team:**
  Engaged in incident response, investigation activities, and documentation of evidence and situational reports.

- **White Cell/Exercise Control:**
  Oversaw overall exercise execution and coordination, ensured VTE availability, and monitored range activities.

Exercise Support

- **Opposing Forces (OPFOR):**
  Cloud Range's simulations include automated Red Team operations throughout the exercise, tracking incidents and validating Blue Team actions.

- **Training and Operations Support:**
  Cloud Range had Attackmasters, or expert instructors, available on-site for both weeks of the event. The first week, Attackmasters assisted with training, setup, and introducing participants to the platform. On exercise days during the second week, Attackmasters provided immediate assistance, necessary documentation, troubleshooting, and support for participants.

CYBER TATANKA WELCOMED PARTICIPANTS FROM:

- UNITED STATES OF AMERICA
- CZECH REPUBLIC
- UKRAINE
- ARMENIA
- CHILE
- AUSTRIA
- VARIOUS STATES
- ARMED SERVICES BRANCHES
- GOVERNMENT AGENCIES
- ENTERPRISE ORGANIZATIONS
- CRITICAL INFRASTUCTURE
- ACADEMIA

12 CRITICAL INFRASTRUCTURE SECTORS WERE REPRESENTED:

- Commercial Facilities
- Critical Manufacturing
- Dams Sector
- Emergency Services
- Energy
- Financial
- Food and Agriculture
- Government Services
- Healthcare & Public Health
- Nuclear Reactors, Materials, & Waste
- Transportation Systems
- Water & Wastewater Systems

Outcomes and Benefits

With the use of Cloud Range's VTE, Cyber Tatanka successfully delivered high-value training experiences, enhancing participants' readiness and response strategies against cyber threats. The collaborative environment fostered partnerships across sectors, resulting in increased communication and support for critical infrastructure.

KEY OUTCOMES

- **Enhanced Cyber Preparedness:**
  Participants gained valuable hands-on experience in a realistic, unclassified computing environment, improving their incident response capabilities and technical skills.

- **Successfully Completed 9 Attack Simulations using Cloud Range's VTE:**
  Cloud Range created a program of increasingly complex live-fire simulations throughout the second week of the event. It enabled participants to experience specific tactics, techniques, and procedures based on the MITRE ATT&CK framework and practice hands-on incident detection, remediation, and response in a collaborative environment.

- **Partnership Building:**
  The event strengthened partnerships among military, governmental, and civilian organizations, creating lasting relationships and lines of communication.

- **Immediate Impact:**
  Participants, such as those from Bryan Health, implemented learned skills and strategies in their networks, showcasing the event's immediate impact on organizations.

- **Confidence and Camaraderie:**
  The event instilled confidence in participants, reinforcing their career choices and building camaraderie essential for effective teamwork during cyber incidents.

> "Through the capabilities of Cloud Range's platform and library of attack simulations, the teams worked their way through a variety of realistic scenarios to help professionals identify and address gaps in incident response. With Cloud Range's support, this year's event was the largest one yet, accommodating 194 participants. We have exceeded our own expectations in creating this vibrant community, and we are excited about continuing to grow the event next year."
>
> **— RYAN CARLSON, LEAD TECHNICAL PLANNER OF CYBER TATANKA**

Conclusion

Cloud Range's VTE and training program helped Cyber Tatanka achieve its mission of enhancing cyber preparedness and fostering collaboration among diverse stakeholders. The event's success highlights the importance of hands-on training and partnership building in strengthening cybersecurity defenses.

Future Prospects

- **Expansion and Growth:**
  Cyber Tatanka is set to continue expanding, with Cloud Range committed to supporting its future iterations and evolving training needs.

- **Ongoing Collaboration:**
  The partnerships and relationships formed during Cyber Tatanka will serve as a foundation for continued collaboration and improvement in cybersecurity efforts.

LEARN MORE ABOUT CLOUD RANGE AND PRODUCTS MENTIONED

- Cloud Range Cyber Range-as-a-Service
- Live-fire attack simulation scenarios for teams
- Specialized Cyber Defense Training for Government and Military
- Cloud Range for Critical Infrastructure
- Blue team exercises
- Red team vs. blue team scenarios
- Attack simulations

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.