CLOUD RANGE

CASE STUDY:

STATE OF FLORIDA IMPROVES CYBERSECURITY INCIDENT RESPONSE

2-Week Statewide Incident Response Simulation Training Program Results in Significant Improvement

AT A GLANCE

CHALLENGES

- Uncertainty in decision-making during cyber incidents.
- Lack of real-world experience among team members.
- State agency teams didn't have a way to train as cohesive units.
- Teams and team members had varying levels of experience and skills.
- No opportunities to gain experience in live cyber defense.
- Lack of familiarity with threat vectors and vulnerabilities that could impact each agency.
- Leaders needing more confidence in team's preparedness levels.

REQUIREMENTS

- Information security managers and incident response teams from state agencies required by statute to participate in an annual ISM/CSIRT training exercise provided by the Florida Digital Service.
- Training involved all members of the CSIRT, including non-technical members.
- Incident simulation and response mimicking real world actions, to include team members working remote and in office.

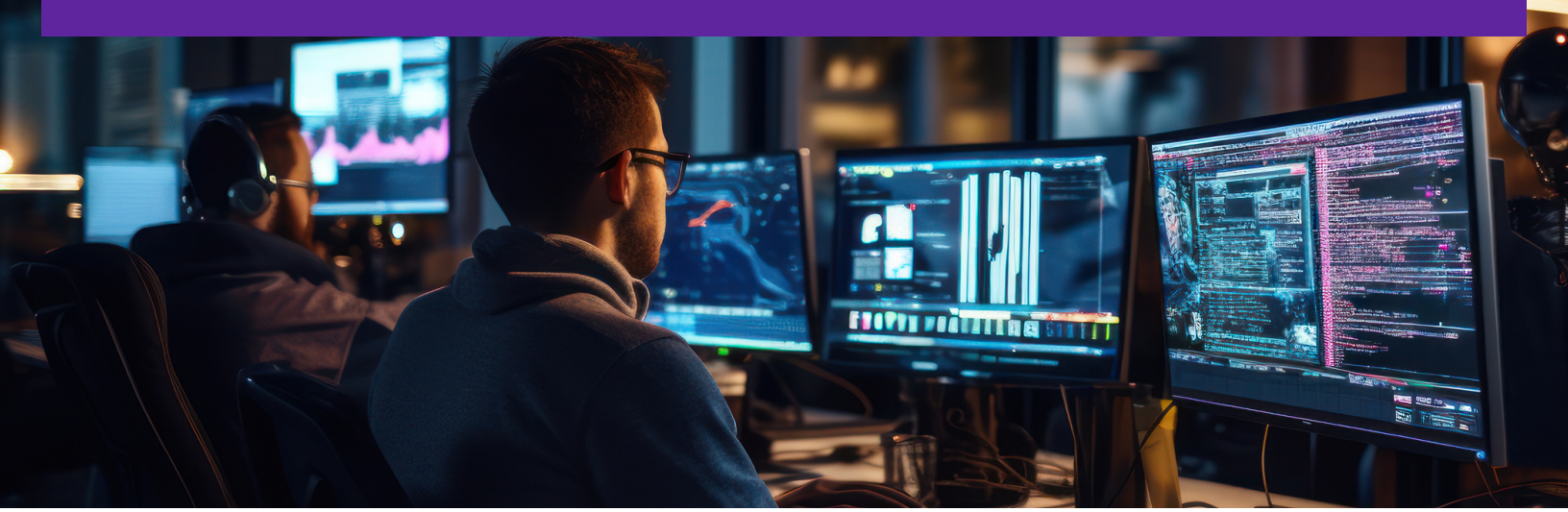
RESULTS

- 34 state agencies gained technical skills and experience detecting and responding to simulated cyber-attacks using Cloud Range's cyber-attack simulation exercises.
- 32 exercises were conducted over 8 business days, plus an additional pilot exercise that was held prior to this intensive training blitz.
- A standardized, cohesive structure to the annual ISM/CSIRT training exercise was established.
- Teams were able to adapt training based on skills and experience using Cloud Range's library of live-fire simulations.
- Teams improved communication and collaboration by working together to understand and respond to potential threat vectors.
- Actionable scoring evaluated technical proficiencies and soft skills during detection and remediation of cyber-attacks.
- Cloud Range provided recommendations for training plans for each person and team.

9/10
average overall experience score of participants

96%
of participants said that doing these types of exercises will help them and their team be more prepared for real-life events

91%
of participants said the cyber range and simulation training experience contributes to overall job satisfaction



Background

Recognizing the critical need for enhanced cybersecurity, the Florida Legislature initiated a comprehensive cyber training program aimed at fortifying state agencies' resilience. This decision aligned with the broader context of escalating cyber threats, as highlighted by recent findings – **a notable 40% increase in attacks against government agencies and public sector services**, per BlackBerry Cybersecurity's August 2023 Threat Intelligence Report. Such statistics underscore the **urgency**, not just in terms of frequency of attacks but also in the diversification of attackers' tools and methods. The Legislature's goal is to ensure that state agencies are well prepared to quickly stabilize and shut down cyber events when they occur.

About Florida Digital Service

Founded in 2020 and housed within the Department of Management Services (DMS), the Florida Digital Service (FL[DS]) is dedicated to delivering enhanced government services and transparency to Floridians. FL[DS] focuses on several critical areas including cybersecurity, data interoperability, procurement reforms, cloud adoption, and digital modernization. As the state's leading entity in cybersecurity, FL[DS] is charged with establishing and operating Florida's first enterprise cybersecurity operations center.

To further support this cybersecurity initiative, FL[DS] implemented a unique grant opportunity. **Unlike traditional grant programs that primarily provide funding, this initiative offered capabilities, enabling FL[DS] to collaborate directly with state agencies and local governments across the state in incident response.** The primary objective is to empower personnel with the resources and expertise needed to effectively respond to and mitigate cyber threats, ensuring operational continuity and state-wide cyber resilience.

> "I am happy with the exercises and had a fun time. I'll look forward to hopefully having more in the future."
>
> **— MEMBER OF STATE OF FLORIDA AGENCY CYBERSECURITY TEAM**

Proactive Cyber Training

In a significant stride towards bolstering state cybersecurity, the Florida Digital Service, in 2022, partnered with Cloud Range to launch its first-ever experimental cybersecurity simulation training program statewide. This collaboration capitalizes on Cloud Range's cutting-edge cyber range solutions, aimed at not only strengthening cybersecurity across Florida but also at upskilling the state's cybersecurity workforce.

The decision to partner with Cloud Range was driven by Cloud Range's proven capability to design and implement a versatile and comprehensive training program, tailored to the diverse roles and skill levels of the hundreds of cybersecurity professionals within Florida's state agencies. This initiative came at a crucial time, with the ever-expanding threat landscape and the global shortfall in cyber skills increasingly pressing concerns. Cloud Range addressed these challenges head-on, offering an innovative training platform that equips cyber professionals, students, and those in transitioning careers with realistic, hands-on experience. This approach is pivotal in bridging the skills gap, providing practical skills essential for navigating today's complex cybersecurity environment.

> "I liked everything about the exercise. Deep Dive. Think outside the box."
>
> — **MEMBER OF STATE OF FLORIDA AGENCY CYBERSECURITY TEAM**

"REAL-WORLD SIMULATION IS THE MOST ADVANCED AND EFFECTIVE APPROACH TO CYBER TRAINING, which is crucial because cyber attacks are in fact modern warfare. Cloud Range's goal is to reduce the chances of potentially detrimental cyber attacks throughout the state while ultimately creating a 'training pipeline' from grade school all the way through to the workforce. We want to look back in 15 years and see someone who was introduced to the cyber range in elementary school, high school, or a cybersecurity workforce program, and is now working for a public or private sector partner," said Cloud Range CEO Debbie Gordon. "In short, **FL[DS] is using Cloud Range's comprehensive cyber training platform to help change lives through pragmatic and valuable skill development.**"

2023 ISM/CSIRT Event

In alignment with Florida Statute 282.318, the Florida Digital Service (FL[DS]) collaborates with the Cybercrime Office of the Florida Department of Law Enforcement (FDLE) to provide essential training. This aims to bolster the cybersecurity acumen of state agency information security managers (ISMs) and computer security incident response team (CSIRT) members. The focus is on current threats, trends, and best practices in cybersecurity.

EVENT OBJECTIVES

Historically, there was a lack of consistency in how ISM/CSIRT training exercises were conducted. Recognizing this, in 2023, FL[DS] and Cloud Range embarked on a mission to design a standardized event for ISMs and CSIRTs across the state. Utilizing Cloud Range's cloud-based cyber range and live-fire attack simulations, the event aimed to:

- Enhance detection and response capabilities to cyber attacks.
- Deepen understanding of potential threat vectors.
- Provide experiential learning in the tactics, techniques, and procedures (TTPs) used by threat actors to more effectively detect and respond.
- Develop role-specific skills.
- Foster team coordination and collaboration.
- Evaluate and refine incident response plans and processes.
- Sharpen decision-making and leadership skills.
- Boost overall awareness and preparedness for the evolving threat landscape.

> "Cloud Range's Attackmaster was an outstanding and charismatic instructor. I appreciated the direction he offered during the exercise while still permitting us room to figure things out."
>
> — **MEMBER OF STATE OF FLORIDA AGENCY CYBERSECURITY TEAM**

TRAINING WITH LIVE-FIRE ATTACK SIMULATIONS

Over two weeks, all 34 of Florida's state agencies engaged in tailored simulation exercises from Cloud Range's extensive attack scenario library. These scenarios, reflecting a wide range of cyber attacks, were conducted remotely, with participants immersing themselves in live cyber attacks through a virtual environment. Each exercise was part of Cloud Range's comprehensive ransomware preparation program, **Path to Ransomware**.

2023 ISM/CSIRT Event, continued

EVALUATION AND REPORTING

The exercises were observed and evaluated by Cloud Range's Attackmasters™ and Florida's Inspectors General. With each CSIRT team including an Inspector General, cross-agency observation was facilitated, enriching the IG community's insights and enabling their participation in their respective agency's exercise.

Evaluations included:

- Individual and team performance in responding to live-fire exercises, including time to detect and respond to the attack.
- Technical proficiencies and use of various cybersecurity tools and technologies.
- Communication and coordination within teams.
- Adherence to incident response plans and protocols.
- Overall cyber readiness.

Following exercises, Cloud Range provided detailed reports on each simulation, complemented by IG observation reports. Cloud Range's reports included metrics and analyses on each "mission," or cyber attack simulation exercise. FL[DS] then compiled all information into a comprehensive after-action report, encompassing scores, analyses, and recommendations.

> "Each different range simulation exercise hits on bits of new areas to learn in."
>
> — **MEMBER OF STATE OF FLORIDA AGENCY CYBERSECURITY TEAM**

CANDACE WYNN, STATE OF FLORIDA CYBER COMMUNITY OPS MANAGER, HIGHLIGHTED THE EVENT'S IMPACT:

"It was exciting to witness our agencies' cybersecurity teams engaging with real cyber attacks in Cloud Range's dynamic environment. Notably, 20 agencies were first-time users of the Cloud Range's virtual cyber range, and the enthusiasm for more exercises is exciting. We've established a standardized method for ISM/CSIRT exercises, and our teams are increasingly adept and confident in handling cyber incidents. Our collaboration with Cloud Range has been exceptional, and we eagerly anticipate further exercises and an even more impactful event in 2024."

2023 ISM/CSIRT Event, continued

A SUCCESSFUL EVENT

This groundbreaking collaboration between FL[DS], FDLE, Inspectors General, and Cloud Range marked a significant advancement in securing Florida's critical infrastructure. It was the first time the ISM/CSIRT training was conducted with a uniform, structured approach, ensuring equitable training opportunities for all agencies. The event's success was largely attributed to the trust established between FL[DS] and the state agencies, as well as between FL[DS] and Cloud Range.

TORI HUGHES, CLOUD RANGE DIRECTOR OF CUSTOMER SERVICE, COMMENDED THE EFFORTS OF THE FL[DS] TEAM:

"A big reason this event was so successful and received full agency participation is due to the work of Candace and the FL[DS] team. They worked with each agency individually – especially those who had not engaged in a dynamic cyber-attack simulation before – to explain what the event was about and how it would work. They were an extension of Cloud Range's white-glove service, ensuring participants enjoyed and saw the benefit of our live-fire missions and that the event produced the desired results."

The Cloud Range Program

The ISM/CSIRT event is part of the ongoing cyber readiness program that Cloud Range created for FL[DS] to ensure cyber defenders could gain the skills and real-world experience they need to protect organizations and critical infrastructure against detrimental and potentially deadly cyber-attacks. The realistic and customizable cyber range is a safe training environment that mimics actual infrastructure and technology and gives trainees hands-on experience in detecting and mitigating real attacks.

Products in FL[DS]'s program:

FlexRange™ Team-Based Simulation Training Program

- A planned series of simulated live-fire cyber attack scenarios customized to the team's skills and learning objectives
- Each "mission" led by expert Attackmasters – live instructors available throughout the exercise to answer questions, provide counsel, conduct a post-scenario debrief, and evaluate performance
- Scenarios get more advanced as teams grows in proficiency and confidence
- All cyber range exercises mapped to MITRE ATT&CK and NIST/NICE Frameworks

OpenRange™ Cyber Range Access

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

Anatomy of an Attack Events

- Two-hour interactive events
- Real-world attacks on the cyber range completely guided by an Attackmaster via input from participants
- Ideal for Help Desk, Network Admins, Server Admins, ISSOs, App Team, and any Executives and C-Suite who would be involved in an escalated incident

FlexLabs™ Cyber Skills Development

- Hundreds of on-demand, tutorial-based exercises that focus on specific knowledge and skill sets
- Realistic environments and exercises give users the hands-on experience needed for today's threat landscape
- FlexLabs augment the FlexRange team simulation exercises by helping team members upskill as needed, creating learning paths for team members of any maturity, fulfilling prerequisites for various attack missions, and outlining post-mission opportunities for improvement

Range365™ Custom Cyber Range Platform

- An unlimited, customized, private hosted cyber range

BENEFITS

Measurably improved incident response and readiness

Accelerated onboarding and time to value

More confident, prepared team

Tested and validated playbooks

Enhanced communication

Actionable metrics & results

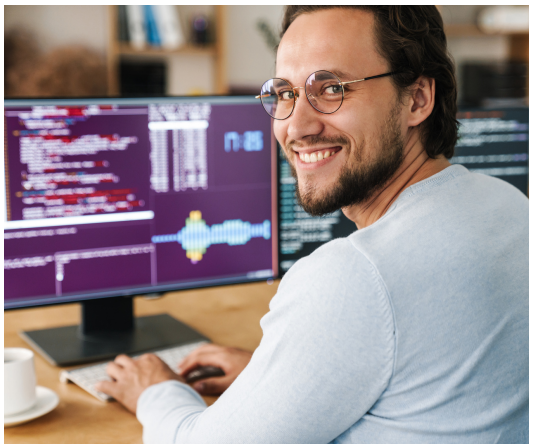
Augmented critical thinking and problem-solving skills

Quicker, more detailed response

Time to do what matters

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
- Attack simulations
- 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.