CASE STUDY

$30B Healthcare Organization Accelerates Cyber Incident Detection and Response with Cloud Range

Contained within 48 hours

Reduced mean time by 66%

30% improvement in response time

MAY 2025

CLOUDRANGECYBER.COM

CLOUD RANGE

Overview

A leading $30 billion healthcare organization with a national presence faced a significant cyber incident involving one of its subsidiaries. Despite the complexities of responding to an attack outside their direct purview, the organization's incident response (IR) team—bolstered by Cloud Range's hands-on and real-life simulation training—demonstrated exceptional readiness, speed, and efficiency.

> "With Cloud Range, we're not just preparing for today's threats, we're preparing for whatever comes next.
>
> **VP and Chief Information Security Officer (CISO) from a $30B NA based Healthcare organization**

The Challenge

This healthcare organization was contacted by a subsidiary within their portfolio that had been hit by a cyberattack. The attack occurred at an independent entity that had its own IT and security team, but this organization was called upon to assist with recovery efforts. This situation was unique in that it required a quick, effective response from the healthcare organizations in-house incident response (IR) team, even though the cyber event was not under their immediate responsibility.

The Solution: Cloud Range Training in Action

The incident occurred in the afternoon, and **within 24 hours**, this organization's incident response team was able to **identify the "who, what, where, and when"** of the attack. This was accomplished before the third-party contracted incident response team had fully engaged with the situation.

The Chief Information Security Officer (CISO), who oversees the IR team, attributed much of the team's swift response to the comprehensive simulation training they've received through Cloud Range. *"It was no different than their simulation training,"* he said. *"The team had done so much training that when it came to real action, they knew exactly what to do."*

While the team quickly contained the attack, they faced challenges proving whether data had been exfiltrated. However, leveraging forensic training from a trusted vendor, they successfully reconstructed a **bitmap image** of the exfiltration process, confirming data theft. This experience reinforced how the right training equips teams to handle even the most complex cyber investigations

Key Results: Efficiency and Preparedness

The response time was impressive, and this team was able to contain the cyberattack quickly, thanks in large part to the team's ongoing simulation training. ***"Within 48 hours, we were confident that no further cyber activity could be conducted against that entity,"*** **the CISO explained.**

While the forensic investigation took longer to fully resolve, the team's preparedness and quick action showcased the effectiveness of Cloud Range's training. The team had developed muscle memory through countless simulation scenarios, allowing them to work efficiently and confidently under pressure. This allowed them to seamlessly integrate their response efforts with the hired third-party, ultimately ensuring that the situation was brought under control swiftly.

Key Results: Speed, Preparedness, & Efficiency

Incident Response Efficiency:
Within the first 48 hours of the incident, the team contained the cyber activity, preventing further impact and demonstrating the effectiveness of the incident response protocol.

Mean Time to Detect (MTTD) Improvement:
After implementing simulation training, **the team reduced the mean time by 66%** to detect cyber incidents from over 72 hours in past events to within 24 hours for this particular incident.

Training Participation and Impact:
Over the past year, the team participated in 12 simulation training sessions (one per month), **leading to a 30% improvement in overall incident response time** and a noticeable increase in team coordination and communication during active incidents.

The Power of Consistent, Realistic Training

The importance of realistic training became evident throughout the event. *"It's no longer just a simulation,"* the CISO noted. *"When you're facing a real attack, it feels just like what we've trained for over and over again."*

One of the standout elements of Cloud Range's training is its gamified approach, which transforms training into a competitive, engaging experience rather than a mundane test. This organization's IR team looks forward to their monthly sessions, which are integrated into their regular workflow. The gamified approach encourages consistent participation, improving team morale and cohesion.

Moreover, it helps foster communication and collaboration, which is crucial for incident response. As the CISO shared, *"Many of the brightest individuals on my team aren't the best communicators. The training forces them to communicate and collaborate, which over time has made them more effective in the field."*

Beyond Incident Response

Cloud Range's simulation training has delivered benefits beyond cyber incident response, positively impacting:

- **Team Morale & Retention –** Investing in continuous training reinforces employee development, reducing turnover.
- **Leadership Development –** Incident commanders gain valuable leadership experience and credibility within the organization.
- **Operational Readiness –** The organization continuously tracks key performance indicators like mean time to detect and respond, showing steady improvement.

Looking Ahead: Continuous Improvement

The CISO emphasized that continuous improvement is a **core value** within this successful healthcare organization. The company measures key performance indicators like mean time to detect and respond to incidents and has seen consistent improvements in those areas. The simulation training provided by Cloud Range is considered a vital component of their overall strategy for maintaining high levels of readiness. As this security team looks to the future, they plan to keep building on their strong foundation of incident response training, integrating it into every level of their team.

Get prepared. Visit **cloudrangecyber.com** to get started.

> With Cloud Range, we're not just preparing for today's threats, we're preparing for whatever comes next.
>
> **VP and Chief Information Security Officer (CISO) from a $30B NA based Healthcare organization**