SOLUTION BRIEF

Fortinet and Cloud Range OT Simulation Cyber-Preparedness Solution

Live-Fire Cyberattack Simulation Exercises in Modeled IT and OT Environments Increases Cyber Readiness, Helps Vet Security Tools, and Mitigates Risk

Executive Summary

Fortinet and Cloud Range have partnered to provide cybersecurity teams with full-service, live-fire simulation exercises designed explicitly for operational technology (OT), IT, Internet of Things (IoT), and converged environments. It gives practitioners the capabilities and experience to protect critical infrastructure and industrial control systems (ICS) from cyber threats while maintaining uptime and safety.

Additionally, Cloud Range enables customer security teams to improve their cyber-defense skills using Fortinet solutions and tools while defending against live cyber attacks in a controlled, multi-vendor environment.

The Challenge

Organizations are increasingly integrating OT infrastructure with IT systems to comprehensively view the industrial ecosystem and equipment. That makes it easier to manage and oversee but also increases the attack surface and possibility of cyberthreats. Security teams need to understand traditional cybersecurity tactics and procedures and OT-specific ones. Sixty-seven percent of organizations say the skills shortage creates additional cyber risks.

An OT attack costs from $3 million to over $100 million. Moreover, the repercussions go beyond anything monetary, causing critical infrastructure disruption, physical damage to engineering assets, adverse environmental impacts, injury, and even death.

Joint Solution Description

Fortinet and Cloud Range have partnered to deliver an industry-leading cybersecurity simulation platform tailored to address the unique challenges faced by organizations that operate in the OT space. Cloud Range's simulated attack scenarios mimic real-world attacks, giving security practitioners hands-on experience in identifying and responding to cyberthreats, which reduces risk.

Cloud Range's virtual cyber range emulates OT and IT networks and can be customized for any industry. The one-of-a-kind simulation training allows OT incident response (IR) and ICS security teams to be immersed in and understand various attack flows, vulnerable ingress points, how to respond if a system is compromised, and how to limit cyber-physical damage. They also learn what actions they should not take and when they rely too much on IT monitoring and protocols. Team members improve technical proficiencies and soft skills, including communication, collaboration, and decision-making.

Solution Components

- Fortinet FortiGate Next-Generation Firewall (NGFW)
- FortiSIEM
- FortiSOAR
- Cloud Range for Critical Infrastructure Cyber-Simulation Exercises

Solution Benefits

- Reduce risk to cyber-physical systems (CPS)
- Recognize and understand attack flows
- Shorten detection and response times
- Prove preparedness with metrics and analysis
- Improve effectiveness and communication
- Strengthen security and operations

FORTINET FABRIC-READY

Integrating the Fortinet FortiGate NGFW and industry-leading security tools into Cloud Range's cyber ranges enables practitioners to work in a true-to-life environment and vet other tools. Plus, the range incorporates Fortinet's validated threat intelligence so customers can practice defending against real threats before they happen.

Solution Components

Cloud Range for Critical Infrastructure is a live-fire, dynamic OT and IT/OT simulation solution on a customized cyber range with OT and IT networks, including virtual PLCs, HMIs, and licensed security tools. Operational technology networks include flat models and best practices, like the Purdue model. All attack scenarios are mapped to the MITRE ATT&CK for ICS framework and can be conducted virtually or on-premises with optional live instructors.

Fortinet FortiGate NGFWs provide industry-leading threat protection and decryption at scale with a custom ASIC architecture. They also deliver secure networking with integrated features like SD-WAN, switching and wireless, and 5G. Converge your security and networking point solutions into a simple-to-use, centralized management console powered by a single operating system, FortiOS, and simplify IT management.

Fortinet FortiSIEM is designed to be the backbone of your security operations team, delivering capabilities ranging from automatically building your inventory of assets to applying cutting-edge behavioral analytics to detect and respond to threats rapidly.

FortiSOAR fully supports unique OT requirements with features such as risk-based asset and vulnerability management, MITRE ATT&CK ICS views, OT threat remediation playbooks, and full OT ecosystem integration. Whether you're extending your SOC to protect OT or growing the security capabilities of your OT control center, FortiSOAR is critical to your OT security posture, threat responsiveness, and SecOps efficiency.

Joint Solution Integration

Integrating Fortinet FortiGate NGFW, FortiSIEM, FortiSOAR, and other vendor platforms into Cloud Range allows security operations teams to learn how to utilize Fortinet and partner solutions better to enhance their cyber skills and defend against live-fire attacks.

Cloud Range's proprietary platform allows networks to be customized to meet your needs, including configurations for the technologies in an organization's stack, live traffic, and implementation of different security tools and Fortinet-specific products. Participants log in to the virtual cyber range to access the attack selected from Cloud Range's attack scenario library. Within the emulated network, the participants work together to detect and respond to the live-fire attack.

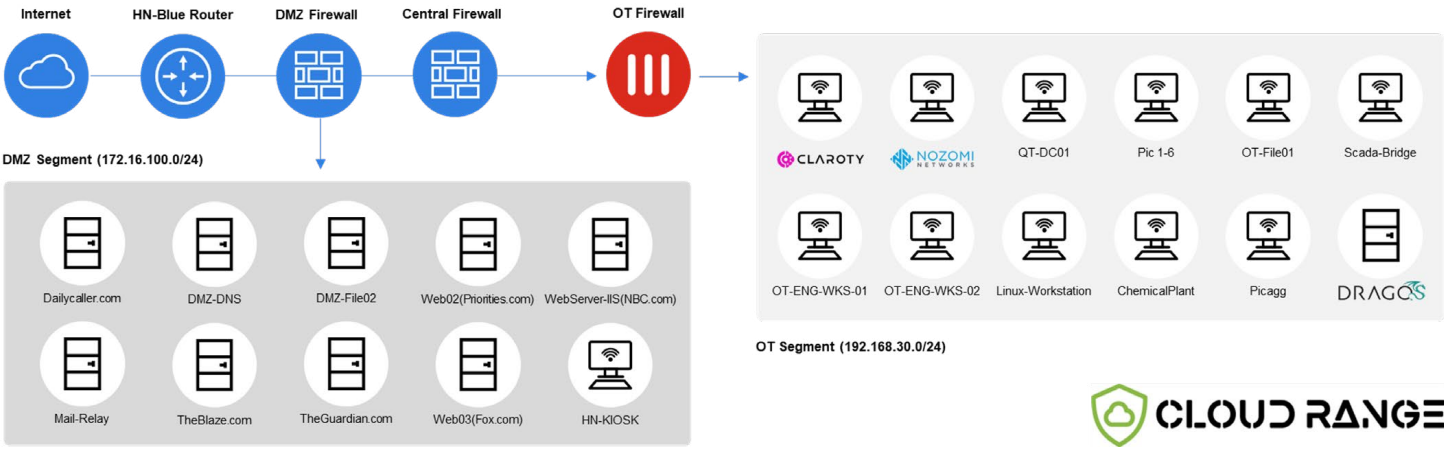

Figure 1: Cloud Range OT network cyber range, including the Fortinet FortiGate NGFW

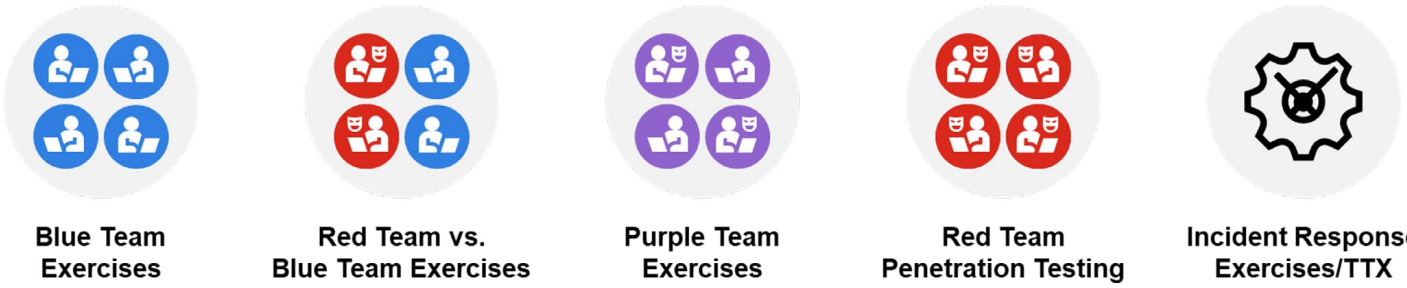

Figure 2: Cloud Range's growing library of live cyberattack scenarios for team exercises

Joint Use Case

Enterprise Customers

Cloud Range enables **enterprises** to educate, integrate, and upskill security teams in a live-fire cyber-range environment using Fortinet solutions, their preferred integrated OT visibility platforms, and a library of real-world attack scenarios.

Managed Security Service Providers

Using Fortinet solutions, Cloud Range gives **managed security service providers** (MSSPs) private access to a hosted cyber range. **Managed security service providers** can test, validate, and upskill their teams in a safe, secure, customized environment. Cloud Range helps MSSPs accelerate their SOC teams' time to effectiveness and realize a competitive advantage based on the increased expertise of their technical staff.

About Cloud Range

Cloud Range is the industry's leading cyber-readiness solution that reduces exposure to cyber risk across the organization. Organizations can accelerate the cyber-defense skills of their cybersecurity professionals using its proprietary simulation training and assessment platform, ensuring preparedness for the most complex cyber attacks.

September 2, 2023 12:59 AM

2296708-A-0-EN