WHERE CYBER RANGE AND DIGITAL TWINS MEET

Through a flexible cyber range-as-a-service approach, Leidos CastleClone leverages secure replicas to enhance cyber readiness

When the SolarWinds attack wreaked havoc in late 2020, cybersecurity leaders across government and industry scrambled to protect their organizations. As cyber response teams sorted through red flags and fallout details specific to the affected organizations, they faced a monumental task. Not only did they need to understand the mechanics of a major novel threat but they also had to unravel how it would impact their own unique environments.

"I was running a response center during SolarWinds, and there were a lot of hours spent dealing with that and Log4j," says Scott Atchison, now a homeland security solutions architect at Leidos. "Half of it was spent trying to figure out somebody else's problem, then trying to find a way to apply that to my environment, and come up with alerts that were high enough fidelity that we could actually move the needle."

What if, instead, security operations teams could simulate a specific threat in their own environment and observe the impact without harming the environment? Enter CastleClone, the Leidos innovative cyber range solution that helps organizations test and strengthen their cybersecurity posture while reducing technical complications and risk.

CastleClone enables organizations to create digital twins of their environments and networks. These clones can be used for everything from penetration testing and malware analysis to training employees and new product assessments, all tailored to the organization's unique needs.

Upgrading the cyber range

A cyber range isn't a new concept, but for a long time they weren't accessible or convenient enough for widespread government use. Creating secure replicas on physical servers is expensive, and earlier cyber range models involved licensing fees and upfront costs. Sharing ranges across multiple departments can lower those costs, but results in a less customized experience.

"They were built in silos, and it was difficult to schedule time and get the cyber range to do what you needed it to do," says Seth Abrams, chief technology officer for Homeland Security Solutions at Leidos. "CastleClone is a flexible model that allows you to clone your infrastructure or set up a newer version of your infrastructure."

The key phrase being "your infrastructure," because each government agency or department's infrastructure is unique. Think of it as a cyber range-as-a-service — instead of licenses and fixed costs, users pay based on their usage to spin up clones as needed.

"You replicate an environment, you run testing on it, and you can compare it to your current environment

> **“You can simulate threats mapped to the MITRE ATT&CK framework. It gives organizations the ability to spin up a clone or a replica of their network and see how it responds. Is my network secure enough against the latest nation-state cyberattack?”**
>
> Kevin Jordan | CastleClone Platform Lead, Leidos

and make changes there,” says Meghan Good, director of the Leidos Cyber Accelerator. “You’re not hurting your production environment, but you’re exploring what’s possible in your production environment.”

The platform is “a Swiss Army Knife” in its variability of functions, describes Josh Strunk, Leidos chief cybersecurity officer for Homeland Security Solutions. It allows an organization to increase its security posture without incurring more risk. Key functions include:

Simulating and analyzing threats: Rather than relying on secondhand information about how threats impact other organizations, CastleClone helps cyber teams assess how their defenses hold up – no guesswork required.

“You can simulate threats mapped to the MITRE ATT&CK framework,” says Kevin Jordan, platform lead for CastleClone. “It gives organizations the ability to spin up a clone or a replica of their network and see how it responds. Is my network secure enough against the latest nation-state cyberattack?”

This way, cybersecurity leaders can gather information on how their tools, environments and team react to emerging cyber threats. It’s a complete people, processes and technology assessment, similar to how first responders prepare for major emergencies through disaster simulations. Bug bounties, penetration testing, red teaming and more are supported for both classified and unclassified environments, without exposing any data.

“Having these kinds of events in a controlled environment, you get to learn where you have areas of responsibility and where some of the gaps are in your response,” Abrams says. “So you can train as you fight when it comes to getting ready for the adversary.”

Testing new products and technologies: From zero trust solutions to generative artificial intelligence (AI), each step forward in innovation comes with countless tools to sift through.

“No one knows my agency like I do, so when I get pitched by a product or solution, my mind is already on, ‘How does this apply to me? Do you actually understand me?’” Strunk says. “We understand that you understand yourself best. You can use your environment with the new technology that’s being developed – whether it’s new defensive capabilities, tools, firewalls – to practice your processes as you know best.”

Whether a team is comparing new products or testing them against similar tools currently deployed in their environment, experimenting in a cloned setting saves time and effort by minimizing the likelihood of introducing security vulnerabilities and technical debt.

Training or upskilling cyber team members: Training presents something of a catch-22 situation. To protect an organization from attack, cybersecurity teams must engage in comprehensive, hands-on training and practice, but that same training can also introduce significant risk if it takes place in a production

For more on Leidos’ latest cybersecurity developments and solutions, download:

An Everything-As-Code Approach to Securing the Software Supply Chain

How to Secure Systems Without Limiting Innovation

> **“Cyber ranges have been built 100 times over, and the problem is that it’s always been someone else’s vision of a cyber range. We found a way to make a range that allows you to build what you need from your own vision instead of someone else’s idea of what your environment should look like.”**
>
> Scott Atchison | Homeland Security Solutions Architect, Leidos

environment. Practicing new skills in a replica allows for in-depth learning without the risk.

Ultimately, “we need better tools that help us get an understanding of our environments and the threats we face,” Good says. “And then we need a way to respond quickly with what we already have or with the new changes we’re adding. CastleClone is a tool that helps you do that easily.”

The future of CastleClone

Amid a shifting threat landscape, the Leidos team plans for future enhancements to CastleClone to stay ahead of adversaries. Generative AI is top of mind for government leaders as they consider “its possibilities and perils,” and the team sees applications for CastleClone.

“We’re going to be looking at incorporating deception detection, advanced honeypot deployments and ways to implement generative AI to come up with different variations of malware on the fly that exploit developers and penetration testers can use, as well as using generative AI to develop tailored training scenarios,” Jordan says.

Internally at Leidos, CastleClone has been used to test the company’s own gold image and firewall configurations, in addition to evaluating zero trust solutions and architectures, particularly in the face of evasive malware. The Leidos team also raises the possibility of incorporating CastleClone into the SecDevOps pipeline to put new code through a series of tests that go beyond typical scanning to ensure its integrity.

Amid all the possibilities internally and externally, the central promise of CastleClone is that it leverages technology to provide a fresh perspective and set of solutions to longtime challenges plaguing cybersecurity teams.

“Cyber ranges have been built 100 times over, and the problem is that it’s always been someone else’s vision of a cyber range,” Atchison says. “We found a way to make a range that allows you to build what you need from your own vision instead of someone else’s idea of what your environment should look like.”

Learn more about how Leidos is leveraging cutting-edge technologies and solutions to enhance government cybersecurity.

leidos

23-Leidos-1006-27002