Shadow-Soft 4C's Framework Addresses Technology Attacks and Vulnerabilities

Cyber attacks happen every 39 seconds costing trillions of dollars requiring a new security framework from Cloud to Cluster to Container to Code

ATLANTA, GA, UNITED STATES, May 2, 2023 /EINPresswire.com/ -- Shadow-Soft, a Kubernetes system integrator, is drawing attention to cyber attacks that are happening every 39 seconds on average according to the non-profit Information Security Forum.

> Companies can't patch and pray. That's not a strategy. Fortunately, Kubernetes lets you build in security from Cloud to Cluster to Container to Code. Because the best defense is a good offense."
>
> *James Chinn, Shadow-Soft CEO*

James Chinn, CEO of Shadow-Soft, observed, "With supply chain businesses like manufacturing, logistics, retail, and finance increasingly reliant on digital systems, they are likely to be a significant portion of the $10 trillion cybercrime losses projected in 2025."

As malicious actors constantly evolve their tactics, targeting vulnerabilities in software, hardware, and networks, businesses rely on patching their systems which takes an average of 250 days to detect and contain a breach. Chinn remarked, "Twitter, PayPal, AT&T, T-Mobile, and even The House of Representatives experienced technology attacks this year. This defensive posture is not sustainable."

To proactively defend against attacks, Nick Marcarelli, Head of Consulting, tasked his engineering team to create a 4C's Security Framework to rethink Kubernetes security. "For every business leveraging the power of Kubernetes and especially those businesses just getting started with Kubernetes, you need to consider security at the Cloud, Cluster, Container, and Code level or what we call the 4C's" advised Marcarelli.

As part of this new paradigm, Shadow-Soft recommends:

1. Treat each Kubernetes cluster and container as its own security boundary
2. Upgrade to Layer 7 inspection/detection; Layer 4 is insufficient
3. Internal security (East-West) is as important as perimeter security (North-South)
4. Zero Trust through automation needs to be established as default

To help educate the market, Shadow-Soft is making their “Kubernetes: A CISO User Guide Using A Cloud to Code Framework” available at academy.shadow-soft.com. The Framework can guide businesses on how to think through attack vectors and how to build proactive security.

About Shadow-Soft:
Shadow-Soft is an award-winning Kubernetes system integrator, specializing in helping organizations adopt and optimize the use of open source technologies. With a team of experienced, certified consultants, and proprietary Kubernetes Frameworks, Shadow-Soft is the partner of choice for companies looking to leverage their legacy infrastructures and applications to Make Optimal Possible©.

Ross Beard
Shadow-Soft
+1 678-842-8715
email us here
