CYBER DEFENSE SOLUTIONS

Celerium Announces New Cyber Defense Network Solution for Critical Supply Chains

CDN Supply Chain Will Focus on Enterprise Supply Chains in Defense, Aviation, Automotive, and Energy Sectors

EL SEGUNDO, Calif., -- Celerium Inc., a leader in innovative cyber defense solutions, today announced its plans for Cyber Defense Network (CDN) Supply Chain, a community solution designed to improve the security posture for supply chains of critical enterprises in the defense, aviation, automotive, and energy sectors.

Celerium, which was previously the cyber business unit of NC4, has a rich, 13-year history of supporting cyber threat sharing in areas such as the financial services, defense, aviation, and automotive industries.

According to some estimates, up to 80% of cyber breaches occur in the supply chain. The escalation of supply chain threats and attacks has increased at a higher frequency and complexity than previously observed. In response to this growing threat, the Cybersecurity and Infrastructure Security Agency (CISA) created a task force working group, and Congressional actions such as the Federal Acquisition Supply Chain Security Act of 2018 have been initiated.

Celerium's CDN Supply Chain allows industrial organizations to strengthen the cyber defense posture of their suppliers at all levels – from large, top-tier suppliers to small and mid-size suppliers. It will offer a variety of solutions for enterprise organizations that wish to strengthen the cyber defense of their supply chains, including:

> **Informational Solutions:** The CDN Academy will provide expert videos to evolve the awareness and skill set of enterprise suppliers. Interviews and panel discussions will address basic and advanced cybersecurity issues, along with insights into the intersection of cybersecurity and supply chain operations. CDN also will provide periodic industry updates and special coverage of new cyber supply chain threats and critical events. These online informational solutions are designed to address the critical labor shortage in cybersecurity as well as the specific needs for supply chain cybersecurity knowledge and skills.
>
> **Cyber Threat Sharing:** CDN will provide mechanisms for industrial organizations (for example, "OEMs" in the automotive industry, and "primes" in the defense industry) to share cyber threat intelligence information among their suppliers. CDN provides community dashboards to enable cyber threat

situational awareness and action such as automation bots that allow suppliers to respond quickly to ever-changing threats.

“Cyber threats are increasing in their danger and ability to cause serious disruptions within key supply chains,” said Aubrey Chernick, founder of Celerium. “CDN Supply Chain will help an organization protect and defend its supply chain by empowering its cyber defenders to learn, engage, and collaborate.”

“Information and sharing should be a key part of any cyber defense strategy, and it is especially important for those companies that rely on a community of suppliers and dealers,” said Tommy McDowell, vice president of strategy for Cyber Defense Network. “The combination of insights provided via CDN Academy, and the tools that facilitate cyber threat sharing and collaboration make CDN Supply Chain an essential solution for any enterprise supply chain organization.”

CDN Supply Chain solutions will be available on October 16.

About Celerium
Celerium protects important industry sectors and their members by augmenting and leveraging cyber threat intelligence to defend against cyber threats and attacks more actively. Celerium's CDN Supply Chain is a unique solution for critical enterprise supply chains. Celerium also powers the next generation of information-sharing organizations, including ISAOs and ISACs. Relied on by government agencies, enterprise risk management teams, CISOs, and SOC analysts, Celerium supports all critical infrastructure and market sectors. Learn more at www.celerium.com.

MEDIA CONTACT:
Celerium
Lyndsi Stevens
(850) 582-5351
lstevens@celerium.com