Celerium

Cyber Threat Intelligence in Action

Top 10
Enterprise Security Solution Vendors to Watch Out in
2020

Although IT security threats have been growing for years, there is a bigger threat emerging for many large companies -- enterprise supply chain attacks. Historically, threat actors targeted large companies directly. Now, threat actors are targeting suppliers as a way to disrupt business operations of large organizations – or even entire industries. A 2017 NotPetya attack against the supply chain logistics industry (via Maersk) caused major business disruptions to enterprise supply chains. Given this, it's no longer enough to protect the enterprise; corporations must now consider the larger attack surface created by their enterprise supply chain and ecosystem. Related attacks and challenges are of great concern -- especially for enterprise supply chains supporting the U.S. defense industry.

Celerium is focused on helping companies deal with enterprise supply chain threats in two ways:

1) through their commercial line of cyber defense solutions called Cyber Defense Network, and

2) through an initiative called the CMMC Academy.

Celerium created the Cyber Defense Network (CDN) family of solutions to help address the challenge of enterprise supply chain cybersecurity. Some of the solutions are cybersecurity intelligence services and education, while others are focused on cyber threat sharing.

The entry-level CDN solution, called CDN110, is a cyber threat intelligence subscription service that is designed to help small to midsize companies. Companies can learn about threats and advisories – to help them improve their cybersecurity knowledge and effectiveness – in a very affordable way. CDN110 is a great cloud-based cyber threat intelligence solution that provides reports about recent threat activity as well as recent vulnerabilities. It also provides weekly reviews, and industry threat reports, along with information about threat actors, malware, and threat tactics.

Tommy McDowell
General Manager

> CDN is a family of solutions that helps companies and industry sectors defend against enterprise supply chain cyber threats.

CDN110 does provide a basic cyber threat sharing mechanism, but additional CDN solutions provide more advanced cyber threat sharing capabilities.

Some of these solutions allow for personal cyber threat sharing in a community via a secure portal which enables collaboration. Other solutions provide for automated sharing. These automated sharing systems use advanced machine-to-machine technology based on the power of STIX/TAXII.

Cyber threat sharing across disparate companies and partners is often exacerbated by the lack of cybersecurity staff – and the fact that existing staff is often overworked. Automated threat sharing along with automated distribution rules can be a game-changer. It can help alleviate the staffing shortage and make existing staff more effective by scaling resources across a company or an industry, allowing each participant to benefit locally from global expertise.

“Our automated machine-to-machine technology, and our secure collaboration mechanism helps facilitate sharing of threats. Each solution can be used independently, or in conjunction with each other based on the needs of the customer to defend itself and its enterprise supply chain,” says Tommy McDowell, Celerium's General Manager, a seasoned leader in cyber threat intelligence, risk management, and information security who has helped private sector and governmental organizations transform their cybersecurity understanding and practices.

Stating an instance, McDowell shares one involving a corporation with $55 billion in revenue that wanted to securely and efficiently share indicators of compromise (IOCs) among their business partners on a strictly private basis. The company was able to leverage machine-to-machine technology to automatically share IOCs and collaborate on incident response – while also taking advantage of an advanced discussion boards capability to collaborate on threats.

The U.S. Department of Defense is focused on improving the cybersecurity of the defense supply chain, which includes more than 300,000 suppliers. Their program is called CMMC, which stands for Cybersecurity Maturity Model Certification, and is an effort to enhance the protection of FCI and CUI within the defense industrial base (DIB) supply chain. Accordingly, in January of this year, Celerium launched the CMMC Academy, a free initiative for DOD Suppliers that want to comply with CMMC. The CMMC Academy is intended to help defense suppliers navigate the CMMC requirements.

For the days to come, Celerium has a broad and deep focus on supply chain cybersecurity and introducing their CDN110, an entry-level solution within the Cyber Defense Network family of solutions, created in part to help defense contractors comply with the Situational Awareness practices within CMMC.