WHITE PAPER

Insider's view of Homeland Security's threat intelligence

DHS-approved Enhanced Cybersecurity Services (ECS) from Lumen offers a potent resource to federal agencies, state & local government as well as critical infrastructure organizations to combat cyberthreats.

LUMEN® TECHNOLOGIES

At no other time in history has the nation's critical infrastructure — the facilities, services and institutions upon which our way of life depends — faced a broader array of threats. From the current global pandemic to sophisticated cyberattacks, natural and manmade disasters, the companies and government agencies responsible for operating and protecting our critical infrastructures are under constant assault.

Bad actors have probed American critical infrastructure, with varying degrees of sophistication and success. The most important industries and critical infrastructures, including energy, finance, telecommunications and government services are at risk for attack without the proper cybersecurity measures in place.

This may sound extreme, but the size, scope, complexity and interconnectedness of our nation's critical infrastructure sectors put them beyond the ability of the federal government to defend alone.

That's why the Department of Homeland Security has been working directly with a handful of select internet and telecom providers to offer **DHS-authorized Enhanced Cybersecurity Services (ECS)** to State, Local, Tribal, and Territorial (SLTT) organizations, critical infrastructure companies based in the U.S and the defense industrial base. The services take advantage of the government's "secret sauce," which identifies threat signatures, network traffic patterns and other technical indicators that show hackers at work on a system.

For CEOs and executive teams responsible for safeguarding critical infrastructure facilities, ECS represents an increasingly potent resource for combatting cyberthreats.

Public-private partnership to protect the Nation and its assets

Lumen has offered Enhanced Cybersecurity Services since the program's inception in 2010. This assures SLTTs and critical infrastructure providers of the company's expertise in stopping malicious attacks.

In addition, Lumen's role in supporting the critical infrastructure has led to key roles within DHS's National Cybersecurity and Communications Integration Center (NCCIC) and Communications Information Sharing and Analysis Center (ISAC). This relationship with DHS has also put the company in a unique position to help critical infrastructure providers leverage cyber intrusion and detection services available via ECS.

Lumen built and maintains DHS Authorized classified systems which protect ECS customer networks against unauthorized access, exploitation, and data exfiltration. ECS follows a managed security service model whereby DHS shares sensitive and classified cyber threat information with Lumen. Lumen uses that information to detect and block malicious traffic from entering or exiting customer networks. ECS is the only way organizations can operationalize classified information to immediately protect their network.

Unique position

The company's ECS offering is no small accomplishment. It is one of only three communications service providers (CSPs) accredited and authorized by DHS to offer it. Lumen provides similar enhanced security protections to hundreds of thousands of federal civilian end-users under the DHS Einstein 3 Accelerated (E3A) program. The E3A program detects malicious traffic targeting federal government networks and prevents that traffic from harming those networks.

The company's E3A service is provided to federal civilian agencies by DHS. Lumen's ECS capabilities are available to state and local governments and private criticalinfrastructure companies, even if they don't get their connectivity from Lumen. ECS has been available on the company's GSA Schedule 70 procurement contract vehicle since 2016. Like E3A, ECS offers:

- Domain Name Service (DNS) Sinkholing, which blocks access to specified malicious domain names and
- Email (SMTP) Filtering, which blocks email with specified malicious criteria from entering a network.

DHS collects a lot of threat information that Lumen uses to provide protections to the critical infrastructure operators. The information is not available to them directly from DHS. They can only get it through a communications service provider. And you have to be an ECS provider authorized by DHS.

Insider perspective – unique vantage point to cybersecurity from an ISP

A significant portion of the world's internet traffic moves across Lumen's network. Lumen has one of the largest and most deeply peered IP backbones in the world, providing an expansive, global visibility into the threat landscape. The network is a differentiating factor for providing uptime, infrastructure availability and application performance. But the network can also be a differentiator to help keep data protected. Organizations cannot wait to respond to cyberattacks after they happen. For organizations to stay ahead of attacks, they must understand, identify and defend against today's dynamic threats. They must increase their visibility. The wider visibility you have, the greater the likelihood for successfully defending your IT environment.

Given the global nature of the Lumen backbone and deep network peering, our visibility provides increased opportunities to observe advanced threats, resulting in shortened response times and advanced analysis surrounding reportable events.

Since 2013, Lumen has baselined the behavior of our global backbone by ingesting and analyzing billions of data records daily and then using this baseline to detect potentially malicious anomalies.

Each day, our custom machine learning models ingest over 190 billion NetFlow sessions and approximately 771 million DNS queries. Approximately 3.6 million threats are tracked daily. We correlate these tracked threats against our NetFlow and DNS metadata to alert customers to a potential compromise.

Because of our highly distributed network edge, we efficiently shift the first line of defense closer to the threat source. Our global network acts as a proactive defense platform, blocking malicious activity before it impacts the customer environment.

The technologies we use to protect ourselves also protect our customers. By modeling threat behaviors, understanding motivations, using attacker techniques as a kernel for research and analysis and ultimately implementing disruption efforts, we built one of the world's most advanced threat research teams — Black Lotus Labs. Through our continued investment in our Black Lotus Labs division, Lumen harnesses the power of our global visibility to disrupt malicious actors.

Our network-based approach to cybersecurity is built-in to protect the critical infrastructure and perfectly aligned to combat emerging threats in cyberspace. We own and operate the network that many critical infrastructure organizations rely upon; and apply advanced analytics capabilities that hunt for unknown threats in the network.

The combination of our managed security services, strategic relationship with DHS, and professional consulting services is an important weapon for government agencies and the world as a whole to employ in defending ourselves against sophisticated, evolving, malicious cyberattacks.

To learn more about how Lumen's Enhanced Cybersecurity Services capabilities can help your agency with a critical edge in combating cyberthreats, visit our government cybersecurity page.

LUMEN® TECHNOLOGIES