BEST PRACTICES FOR IMPLEMENTING A TRUSTED CYBERSECURITY SERVICE

To help keep pace with the rapid innovation of threat actors.

Designing and running a modern security operation requires continual assessment of foundational controls and opportunities to augment those capabilities. Identifying how and where to enhance the security stack can be a difficult decision. It's no secret that accelerated digital innovation is a double-edged sword that heavily impacts the security industry. As data becomes the new currency of our digital lives, companies must ensure the privacy and security of their intellectual property and customer information. Doing some research up front can help you successfully navigate the cybersecurity selection process.

Not sure where to start? Here's a simple guide to help.

Do you have CISA accreditation?

An accredited provider will have access to high-fidelity, classified government-furnished indicators (GFI) not available in commercial feeds to provide high confidence against emerging threats.

Can you detect emerging threats up to six months before other products and services?

The earlier the warning of an emerging threat the sooner you can break the kill chain and secure your data.

Are you a trusted government and commercial provider with long-standing partnerships with agencies like the DHS, NSA, and CIA?

This provides the credibility and experience/expertise required to design and operate a secure network product and service to support national security.

Do you offer a high-touch low friction threat detection and response service?

You want a service with high fidelity, actionable alerts with rapid counters to attacks to help reduce the dwell time of an actor in your system and that can provide your team with more support to mitigate the issue if needed.

READY TO SECURE YOUR DATA?
HERE ARE ADDITIONAL CONSIDERATIONS:

Operationalized Classified Intel

Make sure your service can operate sensitive and classified Government Furnished Indicators (GFI) in commercial and civilian environments to detect and stop advanced persistent threats capable of bypassing your existing security technology stack.

Low Integration Effort

Make sure that your service can monitor, manage, maintain, and configure an exclusive well-rounded operations center that will give you additional time and resources to meet your other business needs.

Increased Visibility

Make sure your service can detect attacks inside your network, such as ones that enter your supply chain and are hiding in plain sight. In addition, they should have the ability to see call-out, beacons, or other ingress and egress activity that commercial solutions can't see.

WE'RE HERE TO HELP

Visit **viasat.com/tcs**, email **tcs@viasat.com**, or call **888.842.7281**