Cyber Security Operations Center

The implementation and ongoing support of security technologies and services from Windstream Enterprise is the responsibility of our own, in-house Cyber Security Operations Center (CSOC).

The dedicated staff from Windstream Enterprise provides management of the Unified Threat Management (UTM) firewall, monitoring and management of Security Information and Event Management (SIEM) and Distributed Denial-of-Service (DDoS) platforms that protect our customers' networks and data.

The CSOC augments the visibility and controls provided by digital experience within the WE Connect portal.

Stronger cyber security defenses: How it works

The CSOC uses near real-time intelligence from our partners to identify threats and potential vulnerabilities, strengthening cybersecurity defenses.

To better facilitate the correlation of security and networking events, the CSOC tightly integrates with other Windstream Enterprise customer support organizations who share management and diagnostic tools on a common trouble ticketing platform.

CSOC certified analysts and engineers employ strong security controls to protect Windstream Enterprise network services and customer information, as well as continuously verify technologies and security processes. Our experts work closely with customers from the initial configuration of the security service to ongoing operation support of their security policies.

The CSOC is organized into three teams:

Implementation

The CSOC Implementation team is responsible for the activation process for firewalls that are physically on-premises, cloud-based or running as virtual instances (i.e., Virtual Network Function) within SD-WAN edge devices. Their mission is to provide a best-in-class experience for our customers.

Capturing each customer's unique security needs and requirements must be collaborative. After the customer's security requirements and policies (i.e., rulesets) are captured, an implementation engineer will configure and deploy the firewall and apply the customer-approved policies.

Support

Post implementation, support is provided by a second specialized team within the CSOC. This team is responsible for the continuous operations of Managed Network Services (MNS) firewalls, including the management of the security components. They also provide direct customer support, including questions regarding their MNS service, issue resolution and change requests.

Customers are provided direct toll-free numbers for critical, on-the-fly requests and all other support needs. These calls are typically answered by a security expert in less than two minutes.

The service level responses for change requests and incident response times are as follows:

Standard change request:
One hour to begin addressing and within four hours to complete

Urgent change request:
30 minutes to begin addressing and within one hour to complete

Monitor

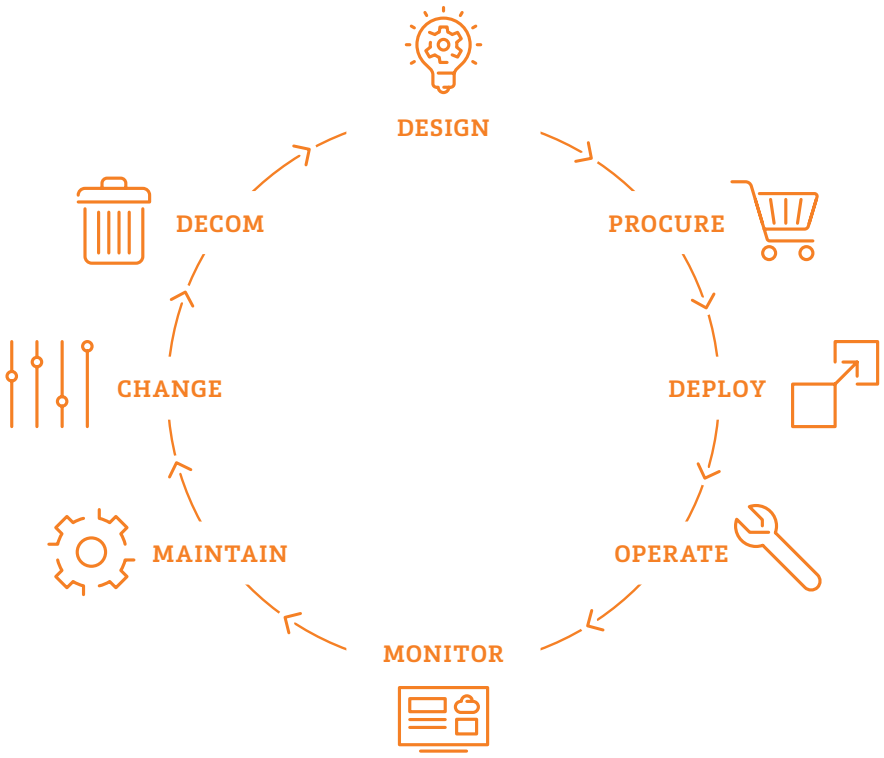
The third specialized team is responsible for proactive cybersecurity support of the Windstream Enterprise DDoS Mitigation and SIEM platforms by monitoring, detecting, validating and mitigating attacks.

For customers that use our SIEM services, this CSOC team provides 24/7 threat monitoring and incident management. Windstream Enterprise SIEM guards a network against malicious attacks that might go undetected. This is accomplished via the collection and analysis of network and security data from diverse information sources, including performance metrics, system logs, security events and changes to the configuration of monitored devices.

What are the responsibilities of the (CSOC)?

The lifecycle monitoring and management responsibilities are out tasked to the CSOC upon purchase of our cybersecurity services.

Lifecycle Support



CSOC advantages

Easy and direct anytime access to a dedicated team of security experts

People, processes and platforms with latest security threat and response information

Around-the-clock monitoring, notification and incident management with SIEM

Regular, proactive customer conversations to review security policies and overall customer satisfaction

Responsibility	Description
Design	Structured and collaborative cybersecurity policy creation
Procure	Acquisition of required vendor equipment, software and services (e.g., licenses and maintenance)
Deploy	Staging, configuration and installation of cybersecurity equipment, virtual machine and cloud-based technology
Operate	Secure, remote management of cybersecurity equipment, virtual machine and cloud-based technology
Monitor	24/7 monitoring of cybersecurity technology with redundant monitoring links
Maintain	Ongoing vendor licensing and support of deployed technology, including software patching and updates. Periodic customer review of cybersecurity features and policies
Change*	Secure and controlled implementation of changes that are requested by the customers or required to maintain optimal performance
Decom	End of lifecycle task required to remove service from operations and reclaim equipment for re-use or disposal

*Customers must have one or more employees designated as authorized security contacts that are authorized to work with the CSOC.

To learn more about Security Services, visit windstreamenterprise.com/security-compliance

WINDSTREAM ENTERPRISE