

Cyber Security Operations Continuum

Broad Range of Security Solutions

The Northrop Grumman CSOC offers a full range of information security services to protect its customers' networks and data, including:

- 24 x 7 x 365 security monitoring of networks, servers, and desktops
- Computer security incident response and investigations, including containment, analysis, and restoration of operations
- Digital forensics investigative services

- Threat assessment report of threat risks to programs, technologies, or systems, based on open and intelligence sources
- Program threat and risk assessment, including 24 x 7 monitoring
- Secure code review of applications
- Vulnerability management services, including vulnerability and patch assessment, war dialing, scans of externally facing servers, and Web, database, and operating system vulnerability scans

Contact Us

For more information on the Northrop Grumman CSOC and the services it offers, or to schedule a tour of the facility, please contact the CSOC.

Northrop Grumman Information Systems

Cyber Security Operations Center
 2691 Technology Drive
 Annapolis Junction, MD 20701
 877-615-3535
 SIAC@ngc.com

▼ Cyber Security Operations Center (CSOC)

Comprehensive Cyber Threat Detection and Response



A Sophisticated Response to Increasingly Complex Cyber Threats

Cyber attacks by hostile organizations such as nation-states and organized crime are on the rise, threatening governments, corporations, and individuals by attempting to extract technical, financial, strategic, and national security information. Increasingly sophisticated and aggressive methods used in these attacks require that equally assertive measures be taken to detect, respond, and adapt quickly to new cyber threats in order to protect critical information assets.

By combining the latest cyber security technologies with expertise in information security and intelligence operations, Northrop Grumman's Information Security organization has created a Cyber Security Operations Center (CSOC) dedicated to protecting Northrop Grumman and its customers' networks and data through intelligence gathering, threat detection, incident response, digital forensics, and security monitoring.

Building for the Future – State of the Art Facility

Located in the National Business Park Conference Center in Annapolis Junction, Md., the CSOC is a 6,300 square foot state-of-the-art facility. The Conference Center building has a large classified conference facility and secure connectivity to numerous customer networks.

The heart of the CSOC is the security operations center floor, where analysts use customized tools to monitor and process over 1.5 billion daily cyber events that occur on the Northrop Grumman network.

- An Executive Heatmap provides situational awareness for management to view events of interest
- An integrated knowledge management system provides tracking, notification, and escalation of events
- Headwater 2 is an internally designed array of threat detection sensors that enable the CSOC to identify information of interest from diverse data sources and determine the extent and nature of suspicious activity



Cyber Security Operations Center (CSOC) Command Center



The CSOC's capabilities and tools can be exhibited from the CSOC floor, demonstration area, or the executive conference room. The conference room within the CSOC has full HD video teleconferencing capabilities.

In addition to connectivity to the Northrop Grumman Global Network (NGGN) and its customers, the CSOC maintains connections to Northrop Grumman's Transformational Research, Integration and Demonstration Network (TRIAD) (a network of information technology laboratories used for research and development) and information sharing capabilities with our government and defense industry partners.

Identifying and Mitigating Advanced Cyber Threats

The CSOC blends traditional operational functions (such as security monitoring) with competitive intelligence collection and analysis in a collaborative environment in order to more effectively identify and mitigate advanced cyber threats.

Security monitoring: The CSOC is staffed 24 hours-a-day, seven days-a-week, providing security monitoring for over 105,000 clients and 10,000 servers worldwide.

Incident response: Incident handlers respond to suspected security incidents, providing containment of incidents, detailed root-cause analysis and restoration of services.

Digital forensics: Computer forensic examiners collect and analyze evidence from digital media and present their findings in reports that can be admissible in court.

Technical security solutions: A technical team develops and deploys solutions and systems used within the CSOC.

Computer threat analysis and intelligence: Intelligence operators analyze and report on internal and external threats. Cyber network defense experts design and develop security capabilities that can identify advanced threats.

The CSOC currently provides these functions for Northrop Grumman's global intranet, other internal customers (such as TRIAD) and external customers. Using expertise developed by supporting internal Northrop Grumman customers, the CSOC applies best practices and lessons learned to its external customer base.

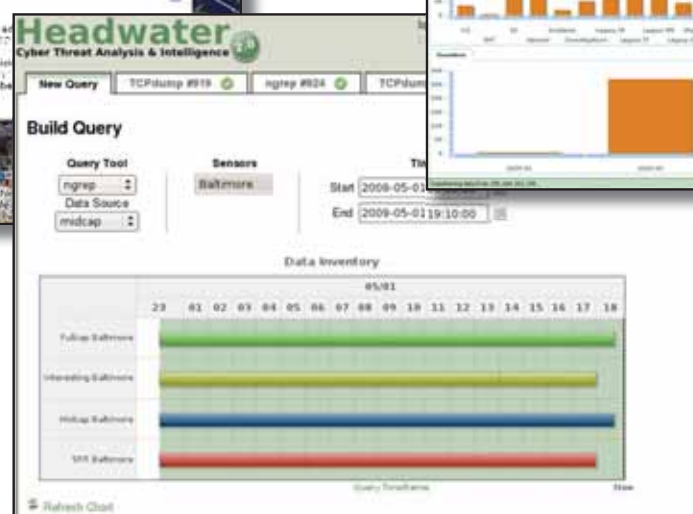
Staffed by Award-Winning Professionals

- Member of FIRST (Forum of Incident Response and Security Teams), the premier organization and worldwide recognized leader in incident response
- 2008 Mid-Atlantic and North American Security Executive "Project of the Year" award
- Recognized by the National Security Agency and the Air Force Office of Special Investigations as best-in-class among defense contractors entrusted to deliver national security solutions

Executive Heatmap of Events



Incident Tracking/Status Metrics



Headwater 2