Secure Network Operations Center (SNOC) Overview

Executive Summary:

The Electronic On-Ramp, Inc. (EOR) team has developed a new methodology to support an architecturally sound operations center that they have termed a SNOC (Security Network Operations Center) that consolidates both NOC (Network Operations Center) and SOC (Security Operations Center) functionality. This approach reduces the investment and overhead necessary to manage these traditionally separate aspects of enterprise security management. This also effectively increases knowledge sharing, while decreasing the mean time to response to security threats. The combined nature of gathering information from security and networking systems allows security analysts and network engineers to detect anomalies, zero day vulnerabilities, network outages, and threats as they happen rather than in a state of delay providing a convenient unification of metrics while at the same time reducing overhead.

Background:

Traditionally, network and security operations have been highly separated. Information collected from network infrastructure elements and security devices were not typically correlated causing blind spots in visibility. This leads to lack of knowledge sharing, competition for budget, distrust between operational groups, and political struggles for control over devices that provide useful information to both security and network operations. This can lead to replication of functionality and an increased budget. These departments were traditionally segregated to add a series of checks and balances, but experience has shown that the amount of information provided to security operations has diminished because of their lack of understanding of the network and operational changes that occur on a day-to-day basis.

Solution:

The EOR team came to the realization very early on in their existence that you cannot monitor what you cannot see and that you cannot secure what you cannot monitor. Because of that, the EOR team has invested heavily into developing a new level of visibility and bringing substance back into security metrics and operational procedures. This allows SNOC centers to more appropriately adapt to constantly changing threats and environments. This approach also builds the synergy between networking and security to provide an unprecedented level of cooperation and emergency response.

Outcome:

The SNOC approach designed and advocated by EOR allows for maximum flexibility in recovery from threats that could hinder the continuity of the enterprise including evolving exploit threats, worms, network outages, and the failure of specific technologies to limit damage to the enterprise.

Maryland Office
785 Rockville Pike, Unit F-131
Rockville, Maryland 20852

Direct: 240.475.6858
Phone/Fax: 800.960.2469
Website: http://www.eor.us

Virginia Office
901 North Pitt Street, Suite 105
Alexandria, Virginia 22314