Active Network Monitoring and Analysis

Services	Deliverables
• Active Network Monitoring and Analysis	▪ Pre-installation technical assessment, network sensor hardware and software installation, 24/7 collection of network traffic data, analysis of collected data, reporting to customer of network incidents with remediation recommendations or fixes.

Active Network Monitoring and Analysis

24/7 inspection of network traffic and daily analysis for malicious/damaging activities to include hacking attempts, scanning by competitors, insider threats, violations of policy, misconfigured equipment, etc. Reporting of network events to the customer's designated points of contact, to include recommended remediation courses of action.

"Better Cyber-Safe than Cyber-Sorry. Cyber-Sorry takes on new meaning daily."
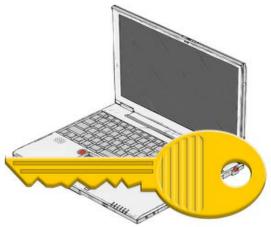

Objectives of this service:

- Satisfy several NIST 800-171 requirements to monitor network traffic for malicious activity.
- Provide expert analysis of network traffic at the flow and packet levels to alert IT staff and other company designees of potential threats and appropriate mitigation recommendations.

Upon completion the company will:

- Have satisfied the NIST 800-171 requirement 3.14.6.
- Have installed and configured a network sensor running 24/7 collection of suspected network incidents.
- Have reporting of network incidents and remediation recommendations from network analysts (analysis and reporting frequency based on customer network size, complexity, and other factors determined during the pre-installation technical assessment.)

* The service provider will maintain (as needed) and retain ownership of installed equipment.

ADVANTAGE KENTUCKY
ALLIANCE