



Partnering With Credit Unions to  
Address Data Security Challenges



## What does iSec® do?

- iSec® combines several of the most requested industry standard security components into a single multifaceted enterprise wide Infrastructure Security Monitoring Solution:
  - A **Network-Based Intrusion Detection System** that continually monitors traffic along the Internet perimeter of your network using the Snort® component.
  - A **Host-Based Intrusion Detection System** that collects and correlates all system event logs that a host or device creates including *user login, file access, program execution, etc.*
  - A robust **Event Log Management Solution** that gathers and stores all event logs for archival and forensic studies, as well as future retrieval and reference. All data is stored for an indefinite period of time.
  - An innovative approach to **False Positive Filtering**, to achieve a total risk analysis as it relates to your individual network – using credit union specific rules to weed through the events that present an acceptable level of risk, allowing you to drill down and focus your resources on malicious patterns and severe security risks.
  - **Alert and Event Identification and Reporting** to correlate security events with scanning, threat intelligence and asset information and present them in meaningful reports that are easily understood, and delivered to management and examiners.
  - **24x7 Security Monitoring Service** through our Secure Operations Center (SOC), where we identify attacks from tens of thousands of alerts and millions of log entries. Once an event is deemed suspicious, our team of expert Security Analysts jump into action to help maintain the safety and soundness of your infrastructure as follows:
    - Begin an investigation of the threat
    - Eliminate false positives
    - Identify follow-up activities required
    - Rank the threat on a low, medium, or high scale
    - Provide e-Mail notification to CU IT professionals
    - Assist the CU as needed with the neutralization of the threat or attack vector

## Why iSec® & not the competition?

- We do not restrict our solution to threshold-based monitoring (there is no minimum – we look at everything that could potentially be suspicious)
- We monitor host-based traffic as well as network traffic
- We monitor everything...servers, workstations, peripheral devices (routers, switches, firewalls, VPN access, web servers, SMTP logs, etc.)
- Our indexing tool is very fast & efficient for searching and reporting
- The Snort® network intrusion prevention and detection system is included in iSec!
- We can monitor up to 4 networks/interfaces through one iSec® installation
- Our pricing beats the competition – we are the cost effective solution.

(Rev. 9/11/2009)