

IT Security Monitoring

With today's escalating requirements for Information Technology Security Solutions, credit unions need the peace of mind that their critical IT assets and data are secure from predators both externally and internally. Firewalls and virus protection will continue to be the first line of defense against would be intruders, but as regulations for tighter security increase so must the overall Credit Union security posture. Real-time detecting and the thwarting of potential intruders is the next step in this high stakes arena.

A credit union must have the ability to detect would be attackers and quickly respond to their threats. IT professionals must have the ability to forensically evaluate potential threats and utilize that data to strengthen their Credit Union Security Policies and Procedures. CRI Solutions has developed a Best in Class approach to enterprise wide IT Infrastructure Security Monitoring by releasing its newest technology product, **iSec v2.0**

iSec v2.0 is "Best in Class" because it combines several of the most requested industry standard security requirements into one state of the art, technically advanced, fully managed system. In the past you would have to employ the services and goods of several vendors, and recruit a highly skilled IT professional to obtain all of these features.

CRI Solutions had developed **iSec v2.0**, to incorporate the following products into a single multifaceted enterprise wide IT Information Security Monitoring Solution:

- Network-based Intrusion Detection System (IDS):
- Host-based Intrusion Detection:
- Event log Management
- False Positive Filtering
- Alert and Event Reporting
- 24x7 Security Monitoring Service:

Network-based Intrusion Detection System:

A network-based Intrusion Detection System or IDS continually monitors traffic along the Internet perimeter of your network. All Internet-based traffic destined to enter your network is monitored and logged electronically and collected for future reporting, alert generation and for forensic study. For this task we incorporated Snort[®], the most widely deployed IDS/IPS technology worldwide, as the IDS component.

Host-based Intrusion Detection:

A local Host-based Intrusion Detection System collects and correlates all the system event logs that a host or device creates. Examples of host-based activity include user logins, file access, program execution, etc. The volume and size of these logs differs by Credit Union, depending on the number of devices and their utilization. When we add up all of the Hosts and Devices that a credit union might have, you can see the tremendous amount of data that will need to be aggregated, filtered, parsed, correlated and then reviewed and reported on. ISec continually gathers this information for you 24x7 and delivers it to our security analysts for review and analysis so we can take action to protect your infrastructure.

Event Log Management:

The collection, aggregation, storage and retrieval of event logs is an added benefit of the **iSec v2.0** Platform. Event log management is the process of gathering and storing event logs for archival and forensic studies. ISec collects and stores the event logs for all of your hosts and devices so we can produce over 100 different types of reports to fully meet your needs. We will also assist you in your forensic studies should the need arise. You are not alone with **iSec v2.0** and CRI Solutions, Inc.

Reporting on Events, Alerts and end user Alert Notification:

The gathering and correlating of all this data requires advanced technology which aggregates, filters and correlates events from virtually any security device or critical information asset. Our iSec Platform correlates security events with scanning, threat intelligence and asset information to present over 100 useful reports for IT professionals, credit union management and board members alike. iSec also creates Alert events that trigger an E-mail and/or the generation of a text message if the situation warrants immediate action.

24x7 Security Monitoring Service:

Finally the best part: CRI Solutions Secure Operations Center (SOC) Monitoring Service.

Identifying potential threats and possible attacks from thousands of event alerts and hundreds of thousands of log entries is no easy task. In addition, eliminating false positives and accurately prioritizing threats requires a significant effort. Through the CRI Solutions Secure Operations Center, (SOC) our team of expert Intrusion Analysts provide a 24x7 Information Security Monitoring service for your credit union. CRI Solutions' technology platform, iSec and security experts analyze the data from your critical information assets to thwart known and unknown threats in real-time. Our Analysts possess deep experience and have handled millions of events and thousands of incidents on behalf of our clients.

Small and medium Credit Unions face the same security threats that large Credit Unions face, but often lack in-house security resources to mitigate the risk. Our approach to assessing vulnerabilities, implementing solutions and providing ongoing support delivers a secure infrastructure that is both **risk-appropriate and affordable**. With our new CRI Solutions **iSec v2.0 Platform**, Enterprise IT Infrastructure Security Monitoring is now available to everyone. Here is a list of the available features and benefits of choosing CRI Solutions **iSec v2.0**:

Supported Hosts and Devices:

CRI Solutions' robust **iSec v2.0** Platform is completely vendor neutral and can integrate with virtually any critical device, such as firewalls, IDS/IPS, routers, servers and applications. This flexible platform enables CRI Solutions to support your current and future security monitoring needs. iSec has the ability to monitor devices and Hosts on your Perimeter Network, on your DMZ Network and across your routed WAN to each branch.

This list outlines just some of the hosts and devices that iSec has the ability to monitor:

- ✓ CISCO PIX/ASA
- ✓ Other CISCO Routers and Firewalls
- ✓ Nortel VPN appliances
- ✓ Windows Server 2000 & 2003

Supported Operating Systems and Software Applications:

iSec can monitor the event logs generated by Windows based operating systems and the following software applications:

- ✓ MicroSoft ISA
- ✓ MicroSoft IIS
- ✓ MicroSoft Exchange
- ✓ Symantec AntiVirus
- ✓ MicroSoft Active Directory
- ✓ Other 3rd Party Security Applications
- ✓ Windows Workstations MS XP Pro / MS 2000
- ✓ Syslog generating devices
- ✓ Existing IDS or IPS
- ✓ Existing Security Appliances

24x7 Monitoring Services:

As stated earlier, CRI Solutions has a Security Operations Center that is staffed with a team of expert Security Analysts. Through a combination of technologies and man power your enterprise solution is monitored 24x7. This advanced technology combines the data from both the Network-based IDS and the Host-based IDS, and analyzes this data against known threats and known attack vectors. Moreover, with a technology we have titled *Total Attack Context*, the iSec Platform has the ability to determine possible unknown attacks and previously unknown attack vectors. This technology has the ability to actively identify and prevent false positives and accurately prioritize incidents to thwart attacks and potential attacks before damage is done. This results in every event or series of events being thoroughly analyzed and presented to the Security Analysts with actionable, prioritized information. Plus, with our fully managed solution, all updates, scheduled maintenance and modifications to the system are included. Fully managed means that you do not have to dedicate ITS personnel to these crucial security tasks.

Reporting Functions:

The iSec Platform provides robust reporting including asset-based views, trending and comparative analyses, as well as detailed reports. There are more than 100 reports available for your review and reference, and due diligence. Reports are all based on real-time information and can be created at any time, based on any period of activity. The suite of reports can be used for your own internal tracking, for auditing purposes, and Board of Directors level reporting as well. All reports are stored within the system on-site at the Credit Union for retrieval as well as off-site at the CRI Security Operations Center as a backup. You can even make yearly copies of all reports for archival and forensic studies. The weekly and monthly reports can be scheduled to be sent via secure email.

Alerting Functions:

As mentioned previously, hundreds of thousands of events and data points are collected and analyzed monthly; most data is informational only. As the advanced technology within iSec parses through all this data, iSec has the ability to take two or more events or data points and assess whether or not the result is a false positive, a potential threat or a real threat. The real threats make their way into Alerts of varying degree either to be reported on or acted upon. Should an Alert be deemed suspicious, several things will happen:

- The Security Operations Center will be notified and begin an investigation of its own.
- The Security Analysts will eliminate the possibility that it is a false positive.
- The Security Analysts will identify it as a potential threat to be followed up on.
- The Security Analysts will identify it as a real threat and rank it accordingly.
- Based on the threat level an E-mail or a page can be routed to IT professionals at the CU.
- The Security Analysts will work with the CU to neutralize the threat or Attack Vector.

iSec was designed with credit unions in mind and based upon the most requested Security Technologies of IT professionals, Security and Compliance Officers, and ITS Security Auditors/Examiners, including the NCUA. In this day and age, having just one part of this multifaceted product just won't satisfy the requirements. The **iSec v2.0** Enterprise IT Infrastructure Security Management System gives you confidence in your ITS Security posture because your critical IT assets are all communicating through one Security Information Management tool, **iSec v2.0**. This product will give your credit union the tools necessary to combat today's most advanced predators and hackers, and more importantly, it will bring you peace of mind.

Take a good hard look at your existing security monitoring platform. All of your servers, firewalls and other peripheral devices continuously create the data that you need. Are you utilizing that data to the fullest? Does your existing Security Information Management tool have all the features that iSec does, and is it monitored 24x7? Does it come with a team of Expert Security Analysts? You work hard and so does your security infrastructure...now with **iSec v2.0** we can all start working together and mitigate the security risks your CU is continuously exposed to.