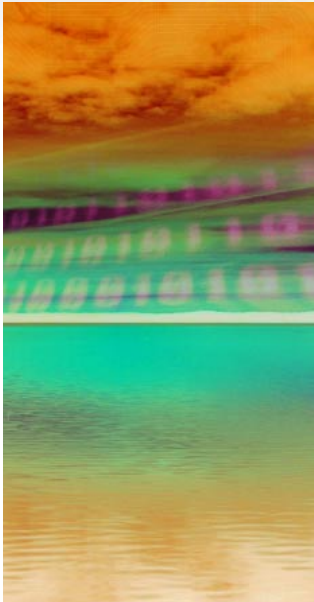


our successes

On the Path to Commercialization



Threatening (Cyber) Skies

New software solution extends company product offering

The odds of being struck by lightning in Canada are roughly 1 in 1,000,000 annually, and for most of us harried by our daily lives, the Internet security threat is as central to the mind as the lightning threat.

But lurking beneath the vast benefit of the Internet is a dark underworld of viruses, phishing, SPAM, trojans, spyware, and hacking, and security professionals who take the threat (typically on our behalf) seriously...very seriously.

Manitoba-based Seccuris Inc. currently offers 24x7 managed IT security services to customers who have elected to outsource their IT security monitoring and management. A key component of Seccuris' managed services solution is the *Seccuris Citadel*. Installed between the client's network and the Internet, the Seccuris Citadel manages all monitoring, collection and log transmission activities for the various computing devices on the network. The Citadel aggregates and normalizes log data and alerts through encrypted channel to the client's security devices. Data mining and correlation activity allow Seccuris Information Security Analysts to remotely analyze data for anomalies and signs of malicious activity. All communication between the Seccuris Citadel and the SOC is encrypted using a system that protects both the integrity and confidentiality of the data being transferred. Confidentiality and integrity services are provided through a VPN service that implements a hybrid cryptography system (symmetric and asymmetric encryption), including SHA 256, RSA, AES-128, and HMAC. Seccuris has implemented a set of tools to automate filtering, analysis and reporting of the information stored in their event database.

A discussion between Seccuris and TRILabs staff researchers identified the potential for research and development of a **Behaviour Anomaly Sensor** that could prove to be a useful addition to Seccuris' Managed Security Services toolset.

The TRILabs research team built a computer model that learns and characterizes 'normal' system behavior - which is a beneficial benchmark that can be evaluated in combination with trigger information from traditional IT security sensors to help better identify conditions for IT security event escalation. Construction of the model required computer interfacing, and programming and statistical and behavioural modeling activities. The Behaviour Anomaly Sensor operates with the information captured by the Seccuris Managed Security Services (MSS) database.

TRILabs Research Scientist Dr. Paul Card describes the results as "excellent." "This project has given the opportunity for TRILabs researchers to work with top industry research staff to produce a new innovative technology."

"This being our first engagement with TRILabs, we were very pleased with the process of initiation, research and development relating to the project," says Renée Riglin, Director, Managed Services. "Although the solution has not yet been deployed into production, we have every confidence that the solution will result in increased efficiency and accuracy for our core service."

"Security is, I would say, our top priority because for all the exciting things you will be able to do with computers - organizing your lives, staying in touch with people, being creative. If we don't solve these security problems, then people will hold back. Businesses will be afraid to put their critical information on it because it will be exposed."

Bill Gates, 2005

www.seccuris.com