

GroupTest: IDS/IPS MSS

There are several aspects to managed security services that have evolved over the past 10 years of their history. A decade ago, managed security services were restricted to applying the output of sensors to some sort of collection and display device. Usually this took the form – in the beginning, anyway – of a homogeneous system allowing only a single sensor type. The first evolution of that approach was the use of Snort sensors to overcome the problem of feeding the collector.

It was not long, though, before we began to see the development of translators that could take many of the most popular data sources and feed them into the collector. This forced the collector to become a correlator, taking the pressure off of the human operators and placing it on machines. When that happened, the

race for the market was on. Today's refinements are a direct result of the development of compact, high performance log correlators. These devices usually are either unified threat management systems (UTMs) or something similar to security information and event management (SIEM). In either, log feeds now are completely heterogeneous and correlation is in near real time, simplifying the job of the analyst.

We found there are a couple of approaches to today's managed security services. In one case, the services are automated and completely managed by the devices. Once the device – correlator, SIEM or other similar device – is tuned for minimum false positives, the device takes over notifying the customer of alerts.

The other case adds a significant human analyst element. In this case, there are human analysts watching

the devices and responding to alerts by tracing, analyzing sources, and performing specific actions to protect the customer network.

Today, managed security services are, de facto, services in-the-cloud in that the correlation point is remote and is accessed through a protected internet connection. Where the sensors aggregate varies from vendor to vendor, and many of the service providers are product vendors that have added managed services to their menu.


Buying managed services always has been difficult. Ten years ago, the difficulty had a lot to do with the immaturity of network security and network security tools in general. The challenges were, in part at least, technology driven. Today's technologies have addressed those issues nicely. The other problem, though, is still with us: A combination of

cost/benefit analysis and the fear of turning the organization's "crown jewels" over to an outside vendor.

When buying managed services for intrusion detection and prevention, get back to the basics. The first question regards whether managed services are appropriate for your organization in the first place. Managed security services are not for everyone. Of necessity you will lose some level of control.

More data always is better than less, and more types of data also add to the ability of your staff or the vendor's analysts to analyze events and act quickly and effectively. If your vendor can't become a part of your security team, look for another vendor.

This month was a bit different in the SC Labs. Deploying a managed service is quite different from testing an appliance.

Product	Vendor	Our verdict	URL	Rating
Clone Guard Managed IDS/IPS	Clone Systems	Excellent service with a lot of capabilities. We rate this one Recommended.	www.clone-systems.com	
Managed Protection Service	IBM ISS	A top-notch services suite based on proven technology and infrastructure. We make this one our Best Buy.	www.ibm.com	