

## Introducing a new way to increase security and cut costs

### Why new challenges require new methods

The challenge for IS departments and security managers today are to juggle cost cuts and increased security threats<sup>1</sup>. At the same time there are outside threats emerging such as regulative demands and the need to control internal usage<sup>2</sup>. To top this off, IS departments are expected to support users with new frontiers of technology: smartphones, IM, social networking, software as a service, streaming services, etc<sup>3</sup>. This pushes both service grade and the security challenges to new levels.

The goal, of course, is to cut cost, maintain service levels, and if possible increase *security* while at the same time supply new services. This cannot be met through the traditional thinking of throwing resources and hardware at the problem and applying a traditional firewall “port centric” approach.

*New challenges require new methods.*

This white paper describes an alternative route, one that provides a far more powerful and flexible solution than traditional means of dealing with these issues. Plus, it also shows you an opportunity to actually cut costs dramatically: swap chunks of iron for an SLA!

### What you are facing today

As a manager in a Network Operations Center (NOC) you are typically charged with “keeping the network secure”. But what does this actually mean?

If the objective is to “keep the network secure” then obviously all NOCs have a set of firewalls. However, firewalls alone will not do the job. Therefore most enterprises are also launching efforts in the area of IDS/IPS solutions (Intrusion Detection and Prevention Systems) and log management resulting in SIEM solutions (Security Information and Event Management).

Even with a SIEM solution (firewalls, IDS/IPS and log analysis), you are still facing challenges in each individual discipline<sup>4</sup>. You have to combine the results from the individual areas and take a more user-behavioral approach of what is going on in the network. If you view them as unrelated activities you won't get the necessary big picture of the network traffic and threats.

---

<sup>1</sup> Waagstein Research, “Nordic Information Security Market 2008-2009” (Ref 1), chapters 4 and 5

<sup>2</sup> Ponemon Institute, “The Ignored Risk of Employees' Use of Internet Applications” (Ref 2), page 2; Ref 1, chapter 9

<sup>3</sup> Forrester Consulting, “Improving Application Deployments” (Ref 3), August 2007, pages 4-5

<sup>4</sup> InfoSecurity Conference 2007, Keynote, Vijay Basani (Ref 4)

## Are you making these mistakes with your firewall administration?

When a NOC operator installs a firewall, it's sometimes a one-time affair. Unpack, configure, install in server rack, take online, and touch every now and then. This leads to firewall logs being ignored and firewall administration and tuning being absent from regular NOC operations.

In a corporate environment, firewalls need to be continuously updated, tuned, re-configured, tweaked and administered. New services cause new behavioral patterns, and proactive firewall administration makes the difference between experiencing problems and having to react, or never experiencing the problems in the first place.

*"Ok, let's configure this thing. We allow inbound 25, 110, 143, 993, 995 to the mail server... 80, 443 to the web server... 53 UDP to the DNS servers... and 1723 and GRE to the VPN server... and then 3306 from the web server to the database... yeah, that should be it. I'm done now, we can take this firewall online, and we don't need to touch it ever again."*

Many NOCs don't analyze firewall logs at all, and much less react to the facts in those logs or new external network conditions. And they rarely re-tune the firewall.

## Can your business handle one million alarms per month?

Intrusion Detection and Prevention Systems are frequently installed as an additional ability to monitor traffic. These systems require active management. They need to be updated with new signatures each and every day. They need to be configured, tuned, and re-configured. Their alarms need to be analyzed; there are often several hundred thousand alarms per month, assuming the systems are well configured. If badly configured, the alarm rate can easily pass the one-million-per-month mark.

Surprisingly many NOCs invest in these systems, and then either ignore the alarms or turn them off, because the alarms are perceived to be too many to analyze, manage and understand. In effect, this is buying expensive hardware and then ignoring all the services that it provides.

## Why log management isn't a defense against external threats

Surveillance on the port level is not enough. Most large enterprises have launched initiatives to manage and handle logs generated from multiple systems, ranging from firewalls to business applications. The concept rests on the notion of understanding users' behavior – what a particular human behavior looks like in the firewall logs. For example, when people use Skype to transfer files outside the corporate network, what alarms are raised? And what happens if a specific application is used outside of their security context?

Unfortunately, these efforts are often halted by the immense challenge of managing such a large set of data, sometimes reaching levels of 100 gigabytes per month. The challenges of securing the system that constantly generates logs means you have to *save* the data and still be able to *search* the stored data and have the *tools* and *skills* to analyze it.

The result is often, in the best case, saved logs that require expensive forensic operations to restore and analyze in an after-the-attack analysis. Logs are almost never a source of proactive defense against external threats or misuse of the systems.

To manage firewalls IDS/IPS, and analyze log data means continuous surveillance, which requires skill, patience, and tenacity. Few individual NOCs bring these activities together in a SIEM solution. Even though the NOC have invested heavily in security technology, the value of that technology is still dependent on 24/7 monitoring by security specialists. These specialists have to be able to see patterns in data from multiple sources to get a full-view perspective of the security of the network.

How dangerous is it for your business for not doing this? How much would it cost if you did?

When did you last hear one of your NOC employees say **this**?

*"I had no idea reading firewall logs was this much fun! Did you know that we're being portscanned from China on average every 90 seconds? Also, there's a host in Brazil knocking on port 25 of where our mail server used to be, and in exactly 15-minute intervals. I'm betting it's an MTA trying to deliver mail and it has a stale DNS cache. Try routing that external IP to the honeypot, and we'll see what they're trying to send us."*

## How Secode can lower your cost and increase security

Secode offers you an outsourced approach, providing your business with some very obvious and tangible advantages:

- By **sharing resources and infrastructure** – your cost decreases.
- By **adding more data points and sensors** – your security quality increases.

**Sharing sources and infrastructure:** In order to maintain a proactive approach to security, 24/7 expertise is required. This, according to some of the largest Scandinavian IT departments, is not affordable! However, it is perfectly feasible to share such round-the-clock staffing with other corporations, since there is a common objective in sharing incidents and know-how in keeping threats at bay. Hence, it makes very good sense to outsource: **it adds effective resources, while at the same time cutting your costs of the security capabilities.**

**Security quality:** The threats on the Internet are global. If you have your security in-house it gives you a limited and vertical perspective of the global threat footprint. By outsourcing security monitoring to Secode, you benefit from a global eye of the current threat footprint. Secode monitors over 60 networks, located all over the globe, supporting businesses ranging from the largest Scandinavian financial institutions to small internet-based web shops. **The result is a pooled view of the network threat that all participants benefit from – a global perspective of the global threats.**

*The Secode business mission is to translate customers' security needs into an Service Level Agreement. This results in higher quality and lower costs!*

Here's what Secode can offer your business:

- **Log File Management and Analysis.** Firewalls and business applications generate large quantities of log entries. Not only do the hardware and applications need to be configured for the right amount of logging, the generated logs – sometimes millions of entries per month! – must also be retained and cataloged for regulative reasons in many industries. We provide log analysis

services with security reports monthly, daily, or in real time. Secode has developed a platform for dealing with these challenges. Our solution is flexible and can address requirements where some or all data needs to reside within your walls.

- **Intrusion Detection/Prevention Systems.** We help you identify the optimal network location for IDS/IPS hardware. Then we configure those systems, and patch them with new signatures which arrive about every other day. The threat signatures change daily, and the legitimate usage pattern changes daily. IDS/IPS hardware is not an install and forget affair. It needs to be actively managed. Secode offers you that service.
- **Security Administration:**
  - **Advisory Watch.** We listen to all security advisories and map them to your systems and needs, and act according to an SLA. We provide services ranging from easy monthly statements up to advanced reports in real time and that includes applying necessary patches to your systems.
  - **Security Hardware Configuration.** We respond to global threat changes and reconfigure firewalls and other security hardware to counter threats. This scales well, as many of our clients have similar equipment.

## Contact us today and get these benefits

These are your benefits of outsourcing **your security services to Secode:**

- **You are in control of the traffic in your network!**
- **Lower costs.** Because NOC operations scale so well, we are able to provide this at a much lower cost than you would be able to do in-house. Effectively, you are pooling analysis resources with other large corporations and taking advantage of economies of scale.
- **Higher quality**
  - Secode's SOC staff is 100% focused on Information Security. This leads to a vast amount of knowledge and constant improvement, compared to a typical in-house solution.
  - You get almost ten years of experience of developing infrastructure and methodology to deal with the challenges around the enormous amounts of data that need to be stored, analyzed and understood. This gives you an SLA that serves your network surveillance needs.
  - Global problems require global perspectives. An attack against **one** corporation means that the knowledge of the still-ongoing attack is applied to **all** corporations, including yours. In an in-house solution, you would typically be unaware of a specific attack until it hit you.

*"No more looking at network threats through a straw."*

## Summary

Secode offers your IS department the opportunity to cut costs and maintain an appropriate security level by introducing security by SLA. If you are interested – let us know, and we will come and calculate the benefits for your enterprise. No strings attached of course.