



24/7 MANAGED SECURITY SERVICES

## IDS/IPS 24/7 – Network Profiling

Protecting your enterprise from cyber-threats requires 24/7 vigilance using advanced security mechanisms and methods. Effective security monitoring is a very demanding task, regardless size of your organization, and requires advanced technology, skilled security specialists and scalable processes. Secode’s Managed Security Services protects your business from intrusions, frauds, down-time, loss of money and provides you with continuous control, expertise and damage prevention.

**The challenges that the Network Profiling service address:**

- The challenge of effectively providing “Anomaly based intrusion detection”.
- The challenge of maintaining a “Graphical overview of your network”.

Although signature based intrusion detection protects from most common attacks, many intrusions go undetected by commercial IDS/IPS systems. These intrusions can often only be detected by investigating anomalies that occur in your network.

Typically these intrusions result in some form of abnormal network behavior, such as the company webserver suddenly making outbound access attempts towards the Internet. The anomalies triggered by a compromised system will be different for different networks.

By visualizing the traffic patterns of your network, *Network Profiling* will make it easy to define network flows that are expected. This is known as profiling, where expected traffic flows are collected and summarized as stable profiles. This enables effective exception monitoring of selected or entire parts of your network by labeling profiles as “locked”. Any anomalies will be detected and reported instantly.

The visual overviews will also highlight and clearly show remote site dependencies, such as partner VPN-connections.

**The service provides:**

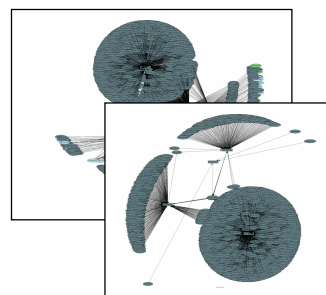
- 24/7 monitoring for security anomalies.
- Graphical representation of selected network segments.
- Ability to track policy enforcement
- Reduced risk of data leakage.
- Well-defined content for the services specified in the SLA (Service Level Agreement).

**Reporting**

The service includes incident reports and a monthly summarizing report, presented to the customer by a security specialist.

**Result**

The Network Profiling service provides state of the art technology to provide anomaly based intrusion detection.



Ticket	#10000
Environment	ENR-EXPRESS-476
Title	SECURITY
Priority	High
Description	<p>The internal host, 10.1.1.100 (client) can not find triggered a flag amount of UDP sessions towards seemingly random internet hosts. The sessions are accepted by the</p> <pre> 14-09-04 08:00:01 10.1.1.100:50000 -&gt; 194.124.208.170:42425  UDP  100 14-09-04 08:00:01 10.1.1.100:50000 -&gt; 197.140.100.100:80  TCP  100 14-09-04 08:00:01 10.1.1.100:50000 -&gt; 197.140.100.100:80  TCP  100 14-09-04 08:00:01 10.1.1.100:50000 -&gt; 197.140.100.100:80  TCP  100                     </pre> <p>The SOC recommends that Client immediately disconnects the host from the network to determine the cause of the incident. If the host is found to be infected, a full removal is suggested.</p>
Feedback was received by S&S at 2009-09-03	
The activity was verified to be caused by the user of the Skype application by J&S.	

Secode is the leading Digital Security Company in the Northern Europe. The vision is that the Internet and IT shall be secure for business, transactions and information exchange. The Company offers surveillance and protection services (24/7 Managed Security Services) from two Security Operations Centres in Gothenburg and Arendal. In combination with Secode Security Consulting, companies and organizations gain increased insight, competence and thereby control over their operations from a complete IT security perspective. Secode today has customers within all industries. Find more information on [www.secode.com](http://www.secode.com)

Secode Råsundavägen 12 SE-169 67 Solna Sweden Tel +46 8 564 875 00 Fax +46 8 564 875 29 [www.secode.se](http://www.secode.se) [info@secode.se](mailto:info@secode.se)