



By the time you read this, the Soccer World Cup will be over, the winners – and losers – decided. But nowadays, such sporting events are like icebergs: the matches are only one tenth; the nine-tenths is the infrastructure which most people never see. And part of the infrastructure of the Korean side of the World Cup was Secos' *SecoShield* IDS – FIFA's official intrusion detection system. Secos is relatively unknown outside of Korea, but that is all set to change with the launch of the product in North America.

Installing *SecoShield* is extremely easy, and after installation it is clear that considerable effort has been devoted to usability. The GUI is a joy to behold, with a clearly laid out window showing the location of the network sensors, all alerts, and the audit log.

Everything is run from the Manager. This controls all of the sensors you place across the network, as well as a policy editor and the extensive reporting tools. *SecoShield* allows for many-to-many relationships between instances of the Manager and sensors, so it can be fine-tuned for the topology of virtually any network.

SecoShield is a network-based IDS with a number of surprises in store. Its network sensors can be placed anywhere

SECOS SecoShield



Version: 3.0
Supplier: Secos Inc.
Price: \$3,499 (manager/console); \$8,999 (sensor); \$1,800 (subscription)
Contact: (949) 794-0021
 info@secos.com
 www.secos.com

FOR *SecoShield* detects packets at the MAC level, ensuring that there is no performance overhead. It is also the only IDS to report on dropped packets.

AGAINST The documentation occasionally meanders – a quick-start guide or a revamp is definitely in order.

VERDICT Bursting onto the market, expect *SecoShield* to become one of the major players in the IDS arena very shortly.

Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★☆
Support	★★★★☆
Value for money	★★★★★
Overall Rating	★★★★★

***SecoShield* detects packets at the MAC level, ensuring that there is no performance overhead. It is also the only IDS to report on dropped packets.**

the administrator considers to be at risk, either side of the firewall, or even within the DMZ. This is because one of the product's strengths is its performance. Unlike some IDSes, it detects packets at the MAC level of the protocol stack, allowing real-time detection without degradation. It also employs statistical analysis to flag up abnormal network behavior, such as a denial-of-service attack. One unique feature of the product is that it registers dropped packets. This can be the precursor to an attack, but many IDSes would disregard it.

For those worried that the threat database might rapidly become out of date, Secos has addressed this concern via a licensing agreement with SecurityFocus. The company scours threat databases and reported attacks from across the world and automatically updates the signature files – there is also an option for user threat definition. This is coupled with a policy editor which allows for more detailed user input.

Given that an IDS should be an integrated part of any security policy, *SecoShield* makes this even easier by offering complete integration with Checkpoint's *Firewall-1* product. Given that one of the weakest links in any security set-up is where one application meets another, this is a definite bonus.

The product is supplied with a user guide and an installation guide. Both are generally straightforward, but there are a few occasions where things get a bit muddled; perhaps a quick-start guide or an overview would aid matters.

Currently a best-kept secret, *SecoShield* definitely deserves wider recognition. With emphasis on ease of use, this quick-to-install, simple-to-use IDS will make a fine addition to any security policy, especially in a network where performance is paramount. 