



Many intrusion protection projects fail. Even if the system is made to work, it often fails to meet real needs. We help fit the technology to the day-to-day environment.

The Need

Companies both large and small can hit significant problems in getting a useful working system, resulting in delays, shelf-ware or a false sense of security. Building a successful IDS or IPS is possible – and any real web service would be vulnerable without one – but it requires careful planning and a realistic view of the costs and benefits.

Product Selection

The intrusion protection market has grown rapidly over the last couple of years, and the sheer number of products can be confusing. We recognise that no one product can meet all requirements: in particular, small gateways do not have the same needs as large portals. More to the point, security budgets vary wildly.

To make sure that you use the right product, we will analyse your requirements, looking at the network architecture, discussing the level of protection required and designing the intrusion protection system to fit in with the rest of the operational infrastructure.

Technical Architecture

Building on this, we will help you place sensors in the most the appropriate locations. It may be interesting at first to watch all the traffic coming in from the Internet, but the most effective solutions concentrate on networks and hosts where attempted attacks actually have some chance of succeeding.

In any large gateway, it not always easy to connect the front-end sensors to the back-end analysis components without knocking holes through the firewall. Similarly, all components need to be manageable, even if they are on isolated parts of the network. We work with the network architects and the operations staff to devise a management infrastructure that is workable without compromising overall security.

Deployment and Configuration

Successful deployment starts with planning, including the resourcing of hardware platforms and any supporting software.

We then carry out the basic installation. Given our considerable technical experience and familiarity with a number of products, this is often more cost-effective than giving the task to network staff.

Once the basic hardware and software are in place, it is necessary to set up communication between components. This includes management and control channels as well as day-to-day reporting.

Tuning

The key part of the whole deployment is tuning the system to match the underlying network. This means analysing traffic flow to find out what is expected, so that unusual packets can be flagged as a potential attack.

Similarly, it is necessary to filter out or downgrade alarms for exploits that can never succeed, for example, Microsoft IIS attacks against UNIX servers. This reduces false alarms and keeps operational staff focused on real security issues, not artefacts of a particular product.

People and Procedures

We can use our experience to help you fit the IDS or IPS into the management structure, making sure that the right people are in place for the various jobs that need to be done. These range from the more mundane aspects of software update and maintenance through to the tricky jobs of understanding what suspicious traffic actually means – and whether the organisation is at risk.

To formalise the roles and responsibilities, we can provide simple procedures covering maintenance, tuning, event handling and escalation. These can be in place as soon as the system is up and running, to ensure continuity between the initial, project-based deployment effort and the follow-on work of the operations staff. This allows for feedback before the system is locked down and the development staff move on.

Staff Training

Finally, we can undertake or organise training at all levels. This can be tailored to the particular network environment and the level of knowledge of individual staff.

Our Track Record

IDsec has been supplying intrusion detection systems to a number of customers since 1997. Our involvement ranges from supplying software only through to full management of complex IDS systems.

For a UK mobile phone operator we have installed and provided day-to-day management for dozens of sensors across a number of systems, including Enterasys' Dragon as well as ISS's RealSecure.

Feel Good About Your Network

IDsec is an independent company specialising in network security. We can assess your security and advise on long-term protection: as we have for a range of blue-chip clients since 1997.

IDsec

31-33 College Road, Harrow, Middlesex HA1 1EJ, United Kingdom
T: +44 20 8861 2001 F: +44 20 8861 3433 W: www.idsec.co.uk

All prices exclude VAT and are subject to confirmation.
Copyright © 2009 IDsec Limited

[services/intrusion/intrusion.pdf](#) 20091019 (5.09)