

0 1 1 0 0 1 0 1 0 1 0 1 1 0 1 1 1 0 0 1 0 1 1

An introduction to:
**Managed Security
Monitoring**



1
0
1
1
1
0
1
0
0
1
0
0

about dns

dns is a leading provider of information security services in the UK. Our sole focus on information security provides us with the experience and expertise needed to provide security solutions to a wide range of public and private sector organisations throughout the UK.

Headquartered in Scotland, with offices in London and operating throughout the UK and Europe, **dns** provides security services across the full security lifecycle ranging from setting strategy and policy to design and delivery of secure infrastructure, service support and 24/7 management.

contact us

head office:
83 princes street,
edinburgh eh2 2er

london office:
16 st martin's le grand
london ec1a 4en

t: 0870 085 8555
f: 0870 085 8556
e: info@dns.co.uk



our services



An introduction to: Managed Security Monitoring

table of contents

1	table of contents	3
2	introduction	4
2.1	a dangerous environment	4
3	what is Managed Security Monitoring?	5
3.1	business drivers	6
3.2	how does it work?	6
3.2.1	dnsMSS Managed Security Monitoring technologies	6
3.2.2	network Intrusion Detection and Prevention	7
3.2.3	host Intrusion Prevention	8
3.2.4	monitoring Intrusion Detection & Prevention Systems	8
3.2.5	reporting through the dns dashboard	9
3.2.6	alerting	10
4	client experiences	10
4.1	examples of success	11
4.1.1	email-borne virus	11
4.1.2	spyware	11
4.1.3	brute-force attack	12
4.1.4	privileged employee access	12
5	summary	12

COPYRIGHT 2005 DNS LTD. ALL RIGHTS RESERVED. MATERIAL CONTAINED IN THIS PUBLICATION MAY NOT BE REPRODUCED, IN WHOLE OR IN PART, WITHOUT PRIOR PERMISSION OF DNS LTD (OR OTHER COPYRIGHT OWNERS). WHILST EVERY EFFORT IS MADE TO ENSURE THAT THE INFORMATION GIVEN HEREIN IS ACCURATE, NO LEGAL RESPONSIBILITY IS ACCEPTED FOR ANY ERRORS, OMISSIONS OR MISLEADING STATEMENTS.

An introduction to: Managed Security Monitoring

2 introduction

Maintaining a strong corporate information security posture is becoming ever more complex, difficult and costly to achieve – and more important to organisations the world over. One result of this rising cost and complexity has been a shift towards partnering with specialist organisations – called Managed Security Service Providers (MSSPs) - to deliver operational security management and monitoring. This has allowed organisations to increase their access to security expertise whilst also reducing costs.

Managed Security Services (MSS) describe the provision of skilled, specialist assistance to the management and monitoring of your IT security status. The market for MSS is one of the fastest growing segments in the security arena. In fact, Gartner reports that by the end of 2005, 60% of enterprises will outsource the monitoring of at least one network security device.

This document focuses on one particular managed security service; Managed Security Monitoring. The paper will explain the service and show how it works.

2.1 a dangerous environment

Ask any IT Director or IT Manager what he needs security for, and he can describe the threats: web site defacements, corruption and loss of data due to network penetrations, denial-of-service attacks, virus and Trojans. The list of threats is endless and recent research shows that these threats are increasing. The latest DTI Information Security Breaches Survey found that:

- **The average UK business now receives roughly twenty viruses a year, and has its website scanned or probed many times.**
- **Large businesses are attacked more, receiving on average one virus a week.**
- **Two-thirds of UK businesses had a premeditated or malicious incident compared with just under half two years ago.**
- **The average UK business now has roughly one security breach a month. Large businesses have roughly one a week.**

As you can see the threats to your organisation from the outside are increasing rapidly, but it is the threat from within that has the greatest effect on organisations. The DTI survey found that inappropriate usage of systems caused the majority of security incidents faced by organisations. These internal threats can come from a range of sources such as system misuse, the breaking of corporate security policy, third parties and remote workers connecting to your network and current or past employees with malicious intent.

An introduction to: Managed Security Monitoring

It is important to understand the risks that your organisation faces but it is vital that you understand the consequence of not protecting yourself from these threats:

Theft – the first consequence is theft. Assets such as money, trade secrets, company information, digital assets and customer information are all at risk.

Productivity loss – is a very important issue. Whether this is due to corruption of data, diversion of funds or recovery and continuity expenses the end result is a big loss in productivity and therefore money. According to the DTI survey mentioned above the average cost of an organisation's most serious security incident was roughly £10,000. In large companies this was more like £120,000.

Indirect losses – include loss of potential customers, loss of competitive advantage, negative brand impact and the loss of goodwill. On the legal side you are also at risk due to failure to meet contracts, failure to meet privacy regulations and illegal user activity.

All organisations using the Internet are at risk from these threats. The challenge is to protect yourself effectively and efficiently. This means detecting, responding and protecting your organisation from threats whether they are internal or external.

3 what is Managed Security Monitoring?

Technology such as firewalls and intrusion detection systems are critical components of a security posture, providing *protection* against a range of known threats. Security protection stops some attacks dead in their tracks, but is not perfect, and cannot protect against everything. The only effective way to manage all serious risks in a fast-developing on-line world is through comprehensive *detection* of attack, married to timely and effective response. The time to detect and respond to that zero-day worm, application hack or denial-of-service attack is critical – and this is the crucial weakness in the security posture of many organisations.

Managed Security Monitoring from dns is the provision of technology, people and process to provide timely detection of security attack, and effective response to protect your critical data assets. Technology – because the sheer quantity of data produced by security devices in a corporate network would swamp even the largest team of security experts. People – because the only effective way to deal with unknown and complex threats is through the application of skilled human IT security specialists, and process – because time to act is critical, and effective, continuous and consistent analysis, action and alerting is vital.

Managed Security Monitoring also provides detailed historic and up-to-date reporting of security event activity across your network – critical data for compliance and audit requirements, and important information for analysing threat trends and behaviours.

An introduction to: Managed Security Monitoring

In a nutshell, that is Managed Security Monitoring. It operates 24 hours a day, 7 days a week, all year round, filtering, analysing, reporting on and taking action upon your IT security information. We work round the clock to record, analyse and act upon your security data, so that you don't have to.

3.1 business drivers

- **Improving security posture** – your organisation needs to be secure in order for your stakeholders to trust you and for you to be able to carry out your operations. Without 24/7 monitoring and immediate response your organisation will be at risk.
- **Reducing operational costs** – the technology, people and process required to manage and monitor your security posture 24/7 is an expensive business. For example, to monitor 24/7 you would need a minimum of 7 security professionals, as well as the complex IT technology to filter and manager the enterprise security data.
- **Avoiding the cost of a security incident** – as shown earlier the cost of a security incident is around £10,000 and more like £120,000 for larger organisations.
- **Provision of expertise** – managing and monitoring IT security systems is a skilled and intensive task. Hiring and retaining sufficient in-depth skill to do so is rarely as cost-effective as partnering with a specialist provider.
- **Regulatory compliance** – Sarbanes-Oxley, FSA regulations, BASEL II, e-Government standards and more are topics that are discussed in board rooms across the UK. The reason for this is the fact that responsibility lies with the board and the repercussions of not being compliant are serious.

3.2 how does it work?

3.2.1 dnsMSS Managed Security Monitoring technologies

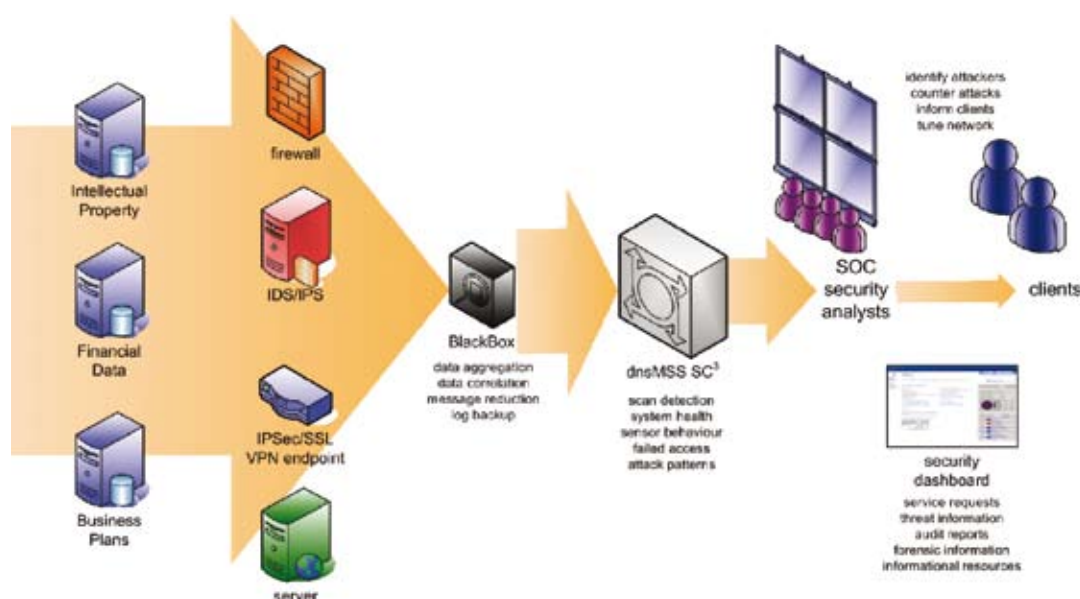
We have designed our Managed Security Monitoring (MSM) service with three primary goals in mind; flexibility, security and scalability.

Three dnsMSS proprietary technologies facilitate the delivery of our best-of-breed security monitoring and management:

- The Black Box, our low-impact management agent and event aggregation and correlation engine provides a complete view of your security data to the dnsMSS security operations team

An introduction to: Managed Security Monitoring

- The SC3 (Security Command and Control Centre), providing cross-customer correlation, data filtering and prioritisation, integrated with our ITIL-compliant ticketing and service desk
- The dnsMSS Security Dashboard, providing real-time and historical reporting on security event data, open issues and trend information, plus security intelligence, learning materials and best practice information



The dnsMSS Black Box collects, aggregates and correlates data from a broad range of security devices, including firewalls and Intrusion Detection Systems (IDS) from a range of the leading vendors. It reduces the data volume and passes back normalised events to the dnsMSS SC3 where service management and attack analysis is undertaken. Events deemed serious enough to warrant further investigation are automatically raised as tickets in the dnsMSS service desk, from where our team of 24/7 security analysts investigate and respond to security events as they happen. Together with our close person-to-person communication with our clients, our security dashboard provides detailed analysis of your security event data, historical reporting and cross-customer threat trends.

Amongst the most important device types that we analyse data from are Intrusion Detection and Intrusion Prevention Systems. These are explained below.

3.2.2 network Intrusion Detection and Prevention

A network Intrusion Detection or Prevention System (IDS/IPS) is a device which listens to raw network data as it travels through your network. It can be located outside your perimeter, on your server

An introduction to: Managed Security Monitoring

network, or on your workgroup LAN. Each of these locations demand a different detection-focus; it is important to look for worm infections on your workstations and servers, but as these bounce constantly off your perimeter it would be futile to look for them outside the firewall. It is also necessary to look for web and email-attacks. Ensuring that monitoring is tailored individually to each server and network is a demanding job, but one which is vital for an effective intrusion prevention service.

The dnsMSS™ MSM infrastructure supports any number of network Intrusion Prevention sensors.

3.2.3 host Intrusion Prevention

Whilst a network security device is extremely useful for monitoring and controlling network choke-points, it is often only on the host that direct attack may be seen and trapped. This fact has spawned a thriving industry in Host Intrusion Detection/Prevention software.

The host IPS client is a piece of software which works as a conceptual guard dog on your server, carefully watching everything that goes on. It is able to control application requests to use the file system, memory or network resources. In the event that activity is detected by the system administrator which is not explicitly allowed, the Host IPS client can be configured to deny it.

A deployment of Host IPS agents can be targeted at your servers, but it is also increasingly common – and recommended – to install Host IPS on workstations to give the Administrator unprecedented control over user activity.

3.2.4 monitoring Intrusion Detection & Prevention Systems

The single biggest obstacle which a security administrator faces in gaining Return On Investment in Intrusion Detection is the sheer amount of data they pump out, 24 hours a day, every day.

When an IDS system is first installed it lacks any awareness of its surroundings, and will raise alerts on a large volume of normal network traffic: Domain traffic, web traffic and network management traffic are only some of the traffic types which a newly installed sensor will issue alerts on. This is also the main reason why many security administrators give up on their IDS deployments shortly after installation; because the sensors throw up so many “false positives” it is both difficult and time consuming for an administrator, with little knowledge of IDS systems, to identify the real threats.

This is why after initial installation, an IDS deployment requires time to be spent on baselining and filtering. To gain real return on the investment made in IDS technologies it is vital to ensure the accuracy and relevance of alerts. The baselining process will identify all the normal ‘quirks’ which are present on all networks: Does the old legacy application use an anonymous FTP account to that old Linux server? What is the network management server, and what is the range of hosts it is expected to monitor?

Often the baselining will also identify anomalous configurations on the network which the security in-house team might not even know about: How long has that router been configured to use the insecure ‘public’ community string?

An introduction to: Managed Security Monitoring

However, once “normal” events are filtered out, they are never seen again. This can lead to later issues in a dynamic environment with malicious traffic being passed by policy. As recommended by industry guidelines we review security profiles and baselines every 3 months for suitability and correctness.

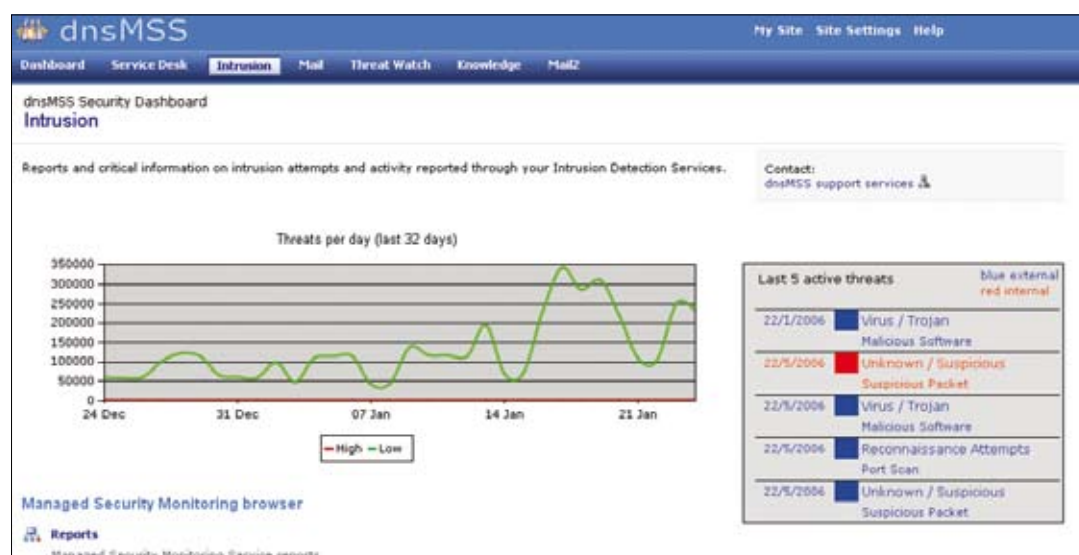
Equally important is that events are categorised and prioritised correctly when they occur. You want an internal worm outbreak to be recognised as such immediately, but you don't want non-malicious anomalies scan to tie up resources unnecessarily.

Our event classification serves a double purpose: Not only is it essential to prioritise which events are important, but it provides useful information about the state of your network; indicating where the real threats are and where it might be wise to focus future improvements in the network. The reports which you receive from dnsMSS MSM provide this data.

3.2.5 reporting through the dns dashboard

As events are stored in our MSM data centre, they are also forwarded to our reporting dashboard. The dnsMSS Dashboard is a web portal which gives you a view straight into the heart of your operations, be it Managed Firewalls, Managed Email or Managed Security Monitoring.

For Managed Security Monitoring, the dashboard displays real-time information about security events happening *right now*; details about the threat, and how the Security Analysts are dealing with the incident. It also provides historical reports: A measure of which parts of your network are most exposed, where the attacks are coming from (and going to) and a distribution of high severity Vs low severity events are only some of the graphs available.



An introduction to: Managed Security Monitoring

3.2.6 alerting

When something important happens, you will be informed immediately. 24 hours a day the **dnsMSS™** Security Analysts are analysing and investigating traffic and events. Experience has shown us that even if a network event can at first appear innocuous, a situation can rapidly escalate into a scenario that needs full attention – however, one of the primary benefits of having dedicated IDS experts at hand is that you will not be flooded with random events that are not really a threat.

Spotting the real threats in the ocean of minor data can be a real challenge, and not one that is easily resolved.

Take for instance the following scenario: An attacker uses a Web attack on your Email server. Shortly after the attack is detected by **dnsMSS**, it will be established that the destination is not vulnerable to the attack. At this point the **dnsMSS** security team will keep a closer look at traffic coming from this source, but not take any further action – yet. 20 minutes later, the attacker hits the Web server with the same attack. This time there is a potential for compromise, and the Security Analyst will run a comprehensive test of the destination server: Is it vulnerable to this attack? If the answer is no, the situation remains unchanged but a watchful eye will be kept on the situation. If the answer is yes, and there is a possibility that the web server has been compromised, we will make immediate contact with the client and recommend subsequent actions.

4 client experiences

The client whose offices are spread throughout the UK outsourced its security management to **dnsMSS™**. For the organisation this was a logical step in focusing on security.

The results have been staggering as the following shows:

Statistics over three month period:

15,000,000	security events monitored by dnsMSS™
700,000	direct attacks identified
99.92%	prevented by managed perimeter infrastructure
538	critical events investigated by dnsMSS™
87.55%	critical events dealt with without client interaction
67	events escalated for further investigation
0	Internet Security Breaches

Industry data for same sized organisation during the same period:

68%	suffered significant virus infection
39%	suffered unauthorised access by outsiders
£127,500	average cost of serious security breach

An introduction to: Managed Security Monitoring

Customer quote:

“Keeping our security in-house had always been a bit of a sacred cow, but it had to be slaughtered. I could only see security getting more complex and expensive if we tried to do it ourselves. dns give us top quality services, and we’ve built a deep trust in them on the strength of our relationship. Most importantly, we’ve seen a reduction in security threats and a benefit in the bottom line.”

4.1 examples of success

4.1.1 email-borne virus

Almost all companies are protecting themselves from viruses, but increasingly complex networks introduce an increasing number of attack vectors. In one situation our client had installed a comprehensive email virus scanning service, but on this particular morning it was behind on updating its virus signature database. An email containing a newly released virus managed to get through the filters and was downloaded to the user workstation.

The virus was detected at 09:32 through the security event data stream integrated into our Managed Security Monitoring service, and a critical alert ticket raised immediately. After being identified as a variant of the Bagle virus, the Security Analyst gathered all relevant information about the event: IP addresses of the hosts involved in relaying the virus-infected email, the IP address of the infected host and the exact timestamp for the event. This information was then sent to our client at 09:35, and we phoned to confirm receipt and offer assistance. At 09:55 we had confirmation that the workstation had been isolated and cleaned before the user had a chance to open it and potentially trigger a larger-scale virus outbreak on the internal network.

The total time taken between virus detection and the subsequent email deletion was 23 minutes.

4.1.2 spyware

One of the biggest annoyances facing computer users today is spyware. Pop-ups which appear from nowhere, your browser home page resets to some strange looking website and your PC is running noticeably slower are only some of the symptoms that your PC has been infected with spyware. Quite apart from these inconveniences and much more serious, is the fact that they frequently include malicious software which will let an external attacker full access to the host.

dnsMSS™ MSM regularly detects workstations which have been infected with spyware. When this happens, we provide our customer with all the information they need to disinfect and clean the host.

In a recent case MSM detected the Gator spyware application on one of our client’s networks and it was sending a beacon to its Internet server, raising an alert in the SOC. Within 10 minutes, we had sent our customer an email detailing the host IP address and the exact time of the event, enabling them to locate the host and remove the Spyware infection.

An introduction to: Managed Security Monitoring

4.1.3 brute-force attack

One of the most common attacks experienced is the password attack, where the attacker will try to guess privileged account passwords, either manually or by using tools which automate the process. The likelihood of success of such an attack depends on two factors; complexity of the password and time available to the attacker.

At 03:35 on a Saturday morning in January, the dnsMSS MSM service detected such an attack on a client's business-critical web portal. On receipt of the correlated attack data, the SC3 immediately delivered our security team with a critical alert ticket, comprehensive information on the attack (including the list of usernames tried, the source of the attack and confirmation that a login had been successfully achieved) and details of the specific client emergency response procedures. After investigation, which confirmed that a real attack was in progress, the emergency response was affected, and our client's IT staff notified. On their instructions, and before 25 minutes had elapsed since the initial attack, dnsMSS systematically killed all connections from the attacker to the portal system, stopping data theft or damage before it could be completed. Job done, and a potentially disastrous event avoided.

4.1.4 privileged employee access

Access to and control over systems is a basic requirement of the system administrator, and in any large organisation there will be a number of people with such rights. Patches need to be applied, and configurations need to be changed to accommodate an ever-evolving network. However it is vital to control change on critical systems; whether maliciously or through best intentions, that privileged access can be abused.

One weekend last December, the dnsMSS security team was alerted to a number of changes to a customer's critical application and database services. The nature of the files being manipulated gave the impression that patching and upgrading was underway, but when the client was consulted over their change schedule it became apparent that no maintenance work was planned for that day.

The client security manager was immediately contacted, who in turn phoned the security guard on duty in the office, revealing that a system administrator was making unauthorised, unplanned and untested changes to the client's critical application infrastructure.

5 summary

The benefits of dnsMSS™ Managed Security Monitoring are:

- Increased security posture – you can be confident in the fact that there is a team of highly trained security experts dedicated to monitoring your network 24/7. You are free to carry out your operations without worrying about potential threats.

An introduction to: Managed Security Monitoring

- Reduced operational costs – outsourcing your security management saves you money. We hire and train the staff, buy the hardware and software and monitor your security event data for you at a cost which is impossible to replicate in-house. This leaves the rest of your IT resources to focus on business critical objectives.
- Avoiding the cost of security incidents – as shown earlier the cost of a security incident is around £10,000 and more like £120,000 for larger organisations. The cost of incidents are generally avoided with successful attacks being detected and protected against in time to minimise exposure and therefore cost.
- Effective use of security infrastructure – an overwhelming amount of data is produced by IT security systems. It is vital that data is filtered, analysed and acted upon immediately to maintain your security defences.
- Return on investment – our reporting will clearly show you your return on investment. We can accurately show you the events we have stopped and estimate the damage they would have caused had the not been dealt with.
- Regulatory compliance – managed security monitoring meets crucial requirements for audit and compliance standards.