Ensure prompt detection of any potential intrusion or security attack and provide the rapid response necessary to minimise the impact on your business.

Cable & Wireless Intrusion Detection and Response

If your business is unfortunate enough to have a suspected computer security breach, you will want to deal with it quickly and with the least possible impact.

Cable & Wireless Intrusion Detection and Response can help. The service detects suspected intrusions and provides around-the-clock response, giving you peace of mind.

It is provided by Cable & Wireless' Cyber Attack Team (CAT), an internationally respected team of professionals, most of whom have worked with and for governments. It is part of a wide portfolio of security solutions that protect all aspects of business IT systems.

Detection, analysis, protection

A C&W Intrusion Detection and Response solution aims to ensure prompt **detection** of any potential intrusion or security attack (internal or external), and provide the rapid **response** necessary to avert costly consequences and minimise any impact on your business. Any incidents will be investigated to determine:

- the nature of the intrusion
- the extent of any security compromise
- how to correct the gap in security and prevent the same type of attack occurring again
- mitigate the amount of damage
- identify the intruder (in many cases)

Three elements for a tailored service

Three services form the foundation of the C&W Intrusion Detection and Response offering. You can choose the elements that are right for your needs.

- **Intrusion Detection System** (IDS) scrutinises all packets on a network segment and identifies suspicious-looking ones that could be a sign of unauthorised network access attempts.
- **Content Integrity Monitoring** (CIM) alerts you if specific files on a host computer have been changed, which could be a sign of someone trying to hack your website, for example.
- **Incident Response** (IR) assesses any detected or reported incident and takes appropriate action.

IDS — checking for suspicious network activity

If an unauthorised person attempts to gain confidential information, or to access your servers or websites, or to disable your systems, there are likely to be anomalies or signatures in the network traffic patterns. If IDS identifies any such activity it issues an alert.

The Cable & Wireless Incident Response team evaluates the seriousness of the event using pre-defined criteria, agreed with you when your solution is provided.

- ***rapid detection of intrusions or security attacks***
- ***expert impact assessment***
- ***24 x 7 cover***
- ***highly qualified team***
- ***part of comprehensive security portfolio***

CABLE & WIRELESS

Cable & Wireless Intrusion Detection and Response

service info

Included in the service are hardware and software updates whenever they become available; a review of your solution every six months; access to the past 60 days' alert reports; and 40 hours of the Cable & Wireless Incident Response service.

CIM — checking for altered files

A favourite activity of hackers is to change their victims' websites, which they do by modifying files. This sort of activity can be highly damaging to an organisation's public image. Hackers may also be interested in modifying files associated with granting network access rights.

CIM protects you against this type of damage by monitoring specified files residing on a host computer, issuing alerts, and triggering incident response if you choose.

The service provides software to check files and directories. We can advise on which files and directories should be monitored, plus how critical they are and therefore how alerts should be handled. The service is best for static files and directories. We refine the service at intervals; provide access to reports; and include 40 hours of the Cable & Wireless Incident Response service.

IR — minimising your risk

How quickly security alerts are dealt with is crucial — the faster the response to any suspicious activity, the greater the chance of avoiding damage. The IR service provides assistance from highly trained and experienced security professionals.

IR services are initiated by a suspicious event or situation that indicates your digital security may be compromised. You, your IDS, CIM or other indicators may detect this event or condition.

The IR team will assess any detected or reported incident, determine whether an intrusion has occurred, determine the extent of the damage, gather evidence of the intrusion, document the damage done and secure the system against further attacks. If you authorise it, the team will take appropriate steps to identify the perpetrator and help you present the case for litigation or prosecution.

The IR activity carried out following an alert will depend upon the nature of the security incident. C&W will work with you to determine the most appropriate response. Responses may include:

- site hardening
- modification of firewall and IDS rules
- modification of the operating system security controls
- analysis of logs, system statistics and files
- collection of data and intrusion investigation
- collection of evidence and forensic analysis
- reporting and recommendations

Part of a security solution

C&W Intrusion Detection and Response should be considered part of a security solution. It is designed to work in conjunction with C&W Managed Firewall to improve the overall integrity of your C&W Managed Hosting Solution. But you can still enjoy the benefits of C&W Intrusion Detection and Response if you do not have a C&W Managed Hosting Solution.

Cable & Wireless
Registered office address:
124 Theobalds Road, London WC1X 8RX

Cable & Wireless pursues a policy of continuous development of its products and services.
This document is for guidance only and does not form part of any contract. It is subject to change without notice.

eP/05.03

For further information please ask your Cable & Wireless sales contact

www.cw.com