



do you know all of your weaknesses?

Many enterprises have recognised the need to be proactive in their efforts to protect themselves against internal and external threats. Vulnerability Assessments and Penetration Testing are key approaches for evaluating the security of your infrastructure. However the traditional focus for this type of testing has been a specific targeting of the network perimeter, and perhaps the DMZ. Whilst essential, this approach does not provide sufficient analysis of the efficacy of internal defences or risks, including the risks arising from user behaviours, internal threats, malfunctions, misconfigurations and administrative mistakes.

Many businesses are liable to legal or regulatory sanction due to mis-use or theft of company data, not to mention damage to their ability to execute business or their reputations. Research shows that one of the key risks now facing enterprises is inside attacks (*Ref: UK DTI Information Security Breaches Survey 2006 - 52% of large companies responded that their worst security incident had an internal cause*). The attackers range from disgruntled employees and internal data/information thieves to external attackers that are able to gain unauthorised access to internal systems via an unsecured wireless access point, modem, or other portal. Now that corporate perimeters are generally very well protected this state of affairs reinforces the need to pay extra attention to internally generated risks.

security & integrity assessment

To provide a more complete view of the risks and threats affecting your business third-i has developed a new approach, a service we call "Security & Integrity Assessment", to provide a much broader and more holistic view of the risks enterprises are facing.

Traditional Vulnerability Assessments and Penetration Tests rarely get to grips with real "inside the perimeter" threats because of the difficulty in achieving comprehensive visibility across corporate infrastructure. This is where third-i's Security & Integrity Assessment comes in. Combining traditional vulnerability assessment expertise and tools (including the latest threat evasion penetration testing techniques) with behavioural analysis, third-i is able to achieve comprehensive and more insightful risk evaluations across the entire infrastructure for our clients.

The Security & Integrity Assessment service is typically conducted over a period of five weeks and is led by an experienced Intelligence Officer who will analyse the outputs from the Security & Integrity Assessment in collaboration with the client. At the end of the engagement the Intelligence Officer will deliver detailed reporting on the findings including recommendations and the significance and potential impact of findings against the client's business logic.

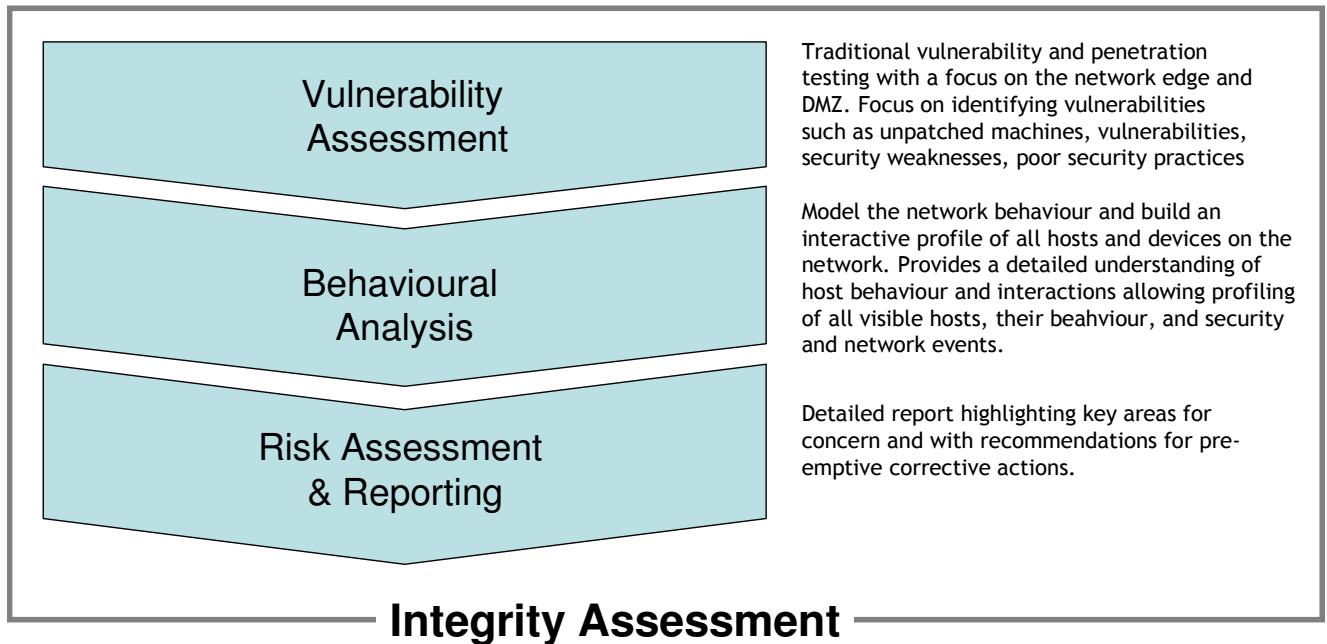
The first component of a Security & Integrity Assessment is Vulnerability Assessment and Penetration Testing with a focus on the network edge and DMZ, identifying vulnerabilities such as unpatched machines, vulnerabilities, security weaknesses and poor security practices. Edge protection devices such as Firewalls, IDS/IPS systems and remote access systems, proxies and secure mail gateways are reviewed through testing and policy/procedural analysis.

The second component - Behavioural Analysis - focuses on modelling the infrastructure behaviour and building an interactive profile of all hosts and devices on the network. This provides a detailed understanding of host behaviour and interactions allowing profiling of all visible hosts, their behaviour, and security and network events.

Collaborative consultation with the client by third-i's Intelligence Officer will yield detailed reporting highlighting key areas for concern and with recommendations for pre-emptive corrective actions.

about third-i

founded in november 2004, third-i is a leading provider of network intelligence services to enterprises which operate business critical IP infrastructure. third-i's services and solutions help our clients reduce the costs and risks of operating large complex IT infrastructure. third-i's ability to detect, alert, analyse and mitigate operations impacting events provides our clients a new level of control, availability, integrity and confidentiality.



Key Features Summary:
Vulnerability Assessment & Penetration Testing
Infrastructure Behavioural Analysis

Unpatched machines, vulnerabilities, security weaknesses, poor security practices

Model the infrastructure behaviour and build an interactive profile of all hosts and devices on the network including:

- Rogue / suspect services, e.g. P2P or unapproved messaging apps
- Rogue / suspect hosts
- Suspect usage, e.g. data theft or inappropriate access to resources
- Policy and process failures
- Misconfigurations and infrastructure failures
- Traffic analysis

Report Generation

Detailed report highlighting key areas for concern and with recommendations for pre-emptive corrective actions.

Key Business Benefits

Reduced risk and improved control of security related incidents and threats:

The powerful combination of vulnerability assessment and penetration testing (including the latest threat evasion techniques) with behavioural analysis (BA) a Security & Integrity Assessment provides comprehensive visibility of a wide range of potential threats. BA can detect malicious attacks or code propagation as changes in the network behaviour and identify source and infected hosts. Penetration and vulnerability testing will highlight potential security flaws or exploits.

Reduced risk and liability of legal or regulatory threat due to mis-use or theft of company data:

Security & Integrity Assessment BA can identify normal and abnormal patterns of traffic and application usage. Any abnormal movement or usage will be identified and analysed. Unwanted usage such as peer-to-peer traffic, unwanted programs or even misconfigured devices can be identified and targeted for remedial action.

Improved transparency and governance of IT organisation:

Security & Integrity Assessment reporting and analysis provide both IT and Management with detailed insight into key IT risks.

about third-i

founded in november 2004, third-i is a leading provider of network intelligence services to enterprises which operate business critical IP infrastructure. third-i's services and solutions help our clients reduce the costs and risks of operating large complex IT infrastructure. third-i's ability to detect, alert, analyse and mitigate operations impacting events provides our clients a new level of control, availability, integrity and confidentiality.