

Vulnerability Risk Assessment

Today's Challenges

In an effort to measure compliance against regulatory and internal service level goals, organisations face a daunting task having to identify and deal with thousands of potential vulnerabilities.

In addition to these vulnerabilities, we have to understand how these relate to network access controls across networks and more importantly how they relate to business risk.

Despite heavy investment in recent years and with an increase in awareness at board level for their responsibility to secure a company's assets, the biggest problem still remains; a lack of visibility.

Vulnerability Risk Management needs a continual assessment, prioritisation and validation process to be adopted producing prompt, accurate answers enabling IT managers to take the correct mitigating actions.

Today IT Operations spend lots of time and money patching desktops, servers, routers and databases, even though many admit they are fighting a losing battle with the sheer number of vulnerabilities they are facing.



Introducing Pentura's Vulnerability Risk Assessment (VRA)

Pentura have been working on a concept for the past three years which has been developed in close communication with key clients to solve these challenges.

The Pentura Vulnerability Risk Assessment offers a unique service to organisations by providing a holistic view of the actual business risk imposed by vulnerabilities and network access exposure to internal, external and B2B threats.

On completion of an initial assessment, Pentura will identify and report on the top 10% of high value asset vulnerabilities. Using "what-if" modelling we consult and produce a VRA Remediation Plan that provides details on the most cost effective way to mitigate these threats, reducing the total cost of remediation.

Once remediation has been completed, Pentura conduct a second assessment and are able to demonstrate a reduction in risk to actual business assets.

Pentura's VRA Service has been designed to help organisations measure the effectiveness of remediation by validating that network changes, patch deployment and other remediation steps have been successful at reducing exposure and business risk.

For governance and auditing requirements, the Pentura's VRA helps organisations demonstrate they have visibility of business risk as well as proving risk is mitigated through effective remediation planning and execution.

Key Benefits

Annual, 6-Monthly or Quarterly Service Offering

IT Security Modelling

Attack Simulation & Visualisation

Vulnerability Classification & Prioritisation

Business Impact Analysis & Risk Metrics

Remediation Planning & What-if Modelling

Regulation Compliance Risk Management

Customisable Reports

Exposure Driven Alerts

Risk Profiling & Trending

The Vulnerability Risk Assessment Process

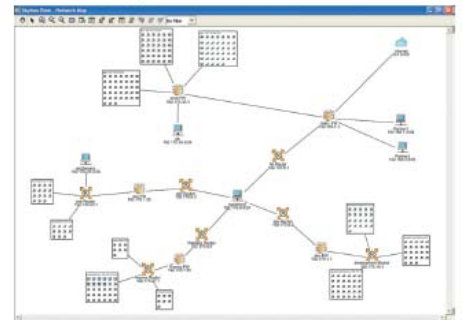
As with any project that can make such a difference to an organisation, there has to be a clearly defined process of engagement and methodology that is easy to understand. The simple logic behind Pentura's Vulnerability Risk Assessment is what makes it a success.

Step 1 - Model the Environment

Pentura builds a comprehensive model of the enterprise security environment consisting of network information, vulnerability data and business logic. A virtual representation of the enterprise is built through both collecting and importing vulnerability scanner data, routing rules and filtering rules from the IT Infrastructure. Potential threats are defined in terms of origin, skill level and likelihood of attack.

- Intelligent Collection from Existing Information Resources
- Business Logic, Asset Mapping and Threat Definition
- Integrated Security Model
- Continuous Operation and Early Warning Analysis

Network Map

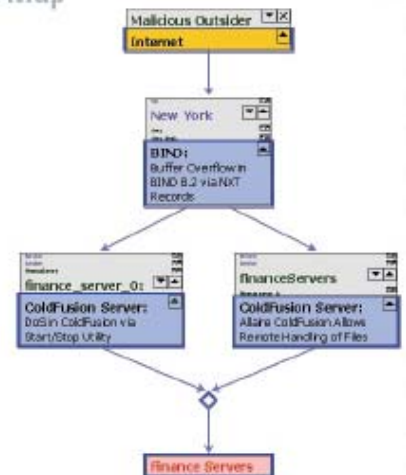


Step 2 - Simulate Attack Scenarios

In order to identify the top one to two percent of vulnerabilities that represent primary risks to critical business application, Pentura's VRA Architecture conducts exhaustive attack scenario simulations against the Integrated Security Model to measure the effectiveness of potential threats in penetrating security defences. Simulating threats that include human attackers as well as malicious code, we can determine which vulnerabilities are exploitable, which assets are at risk and which are secure.

- Access Analysis
- Vulnerability Modelling
- Attack Simulation
- Attack Visualisation

Attack Map



Step 3 - Calculate Business Risk

Business Risk is calculated by assessing both the attack likelihood and the damage potential as measured by business impact variables. The Pentura VRA Architecture determines risk factors at a detailed level — taking into account every attack scenario and vulnerability — and on an aggregated level, for business applications and threats. This step determines the current risk level for all critical applications.

Step 4 - Plan Exposure Remediation

Pentura's VRA Architecture is able to present methods for mitigating an attack scenario based on the minimum set of attacker actions which, if prevented, would prevent the entire attack. In order to speed remediation efforts, we are able to present all possible remediation measures for various attacker actions. Using powerful "what if" scenario modelling, security teams can measure the impact of various actions on overall security risk before actually applying any changes.

- Remediation Alternatives
- What-if Analysis
- Access Planning
- Remediation Workflow

Pentura's Engagement Methodology

Pentura has listened to and worked with clients to develop an engagement process whereby an organisation, with very little investment, is able to understand whether their business can benefit from a Vulnerability Risk Assessment.

The engagement process consists of the following key steps:

Step 1 - Initial Introductory Meeting

- Individual Introductions
- Client Risk Management Process Discussion (High Level)
- VRA Concept Overview
- Workshop Introduction

Step 2 - VRA Workshop

- Client Attendees – Security, Network, Desktop & Server Operations
- Pentura Attendees – Commercial & Technical Consultants
- Pentura Concept Overview
- Risk Assessment Introduction

Step 3 - Client Internal Risk Assessment

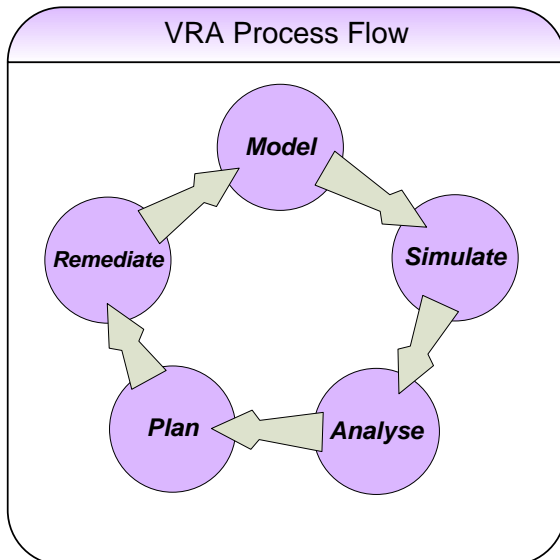
- Internal Risk Based Technical Assessment
- Focus on Key Business Assets
- Report Owned by Client Detailing Location & Value of Risk

Step 4 - Remediation Planning Workshop

- Assess Existing Remediation Tools
- Plan most Cost Effective Action i.e. patch or access filter
- Understand Change Management Workflows & Tools
- Assign Tasks & Responsibilities
- File VRA Remediation Report

Step 5 - Validation & Re-Assessment

- Validate agreed Remediation Tasks have been Completed
- Conduct 2nd Internal Risk Based Technical Assessment
- Provide Risk Reduction Report



Contact:

Pentura Limited
Diddenham Court
Lambwood Hill
Grazeley, Reading
RG7 1JS

Tel: 01189 768960
Email: info@pentura.com

