

## Security Posture Manager

The Security Posture Manager associates the information together into a single, centralized management console, harnessing data from isolated security assessment tools that were never designed to be integrated. By consolidating security posture information and automating security functions like host configuration management processes and vulnerability assessment, security managers no longer need to manually correlate facts across reports, tools and networks using email and spreadsheets as their primary management tools.

The Security Posture Manager (SPM) is an ASP.NET application front end to the Security Posture Manager Database. The system is designed to manage security risks of a company. The system has very sophisticated management mechanisms, tools to record and manage reports by various vulnerability factors. The SPM allows end users to view and edit data within the SPM DB via an HTML browser such as Internet Explorer or Firefox. The system can be used by an IT department of a large corporation.

"Vulnerability assessment and security configuration management are required components of a vulnerability management process," said Mark Nicolett, research vice president at Gartner, Inc. "An enterprise-wide view of the state of the network and its configurations and vulnerabilities is needed to support the vulnerability shielding and mitigation work that will make the environment more secure."

The following features are key to the entire SPM:

- Security (users should only see and do what they are allowed to)
- Easy to use
- Speed
- Graphically rich
- Integration (SDK for 3<sup>rd</sup> party applications)
- Browser agnostic

Technologies employed: ASP .NET, MSSQL

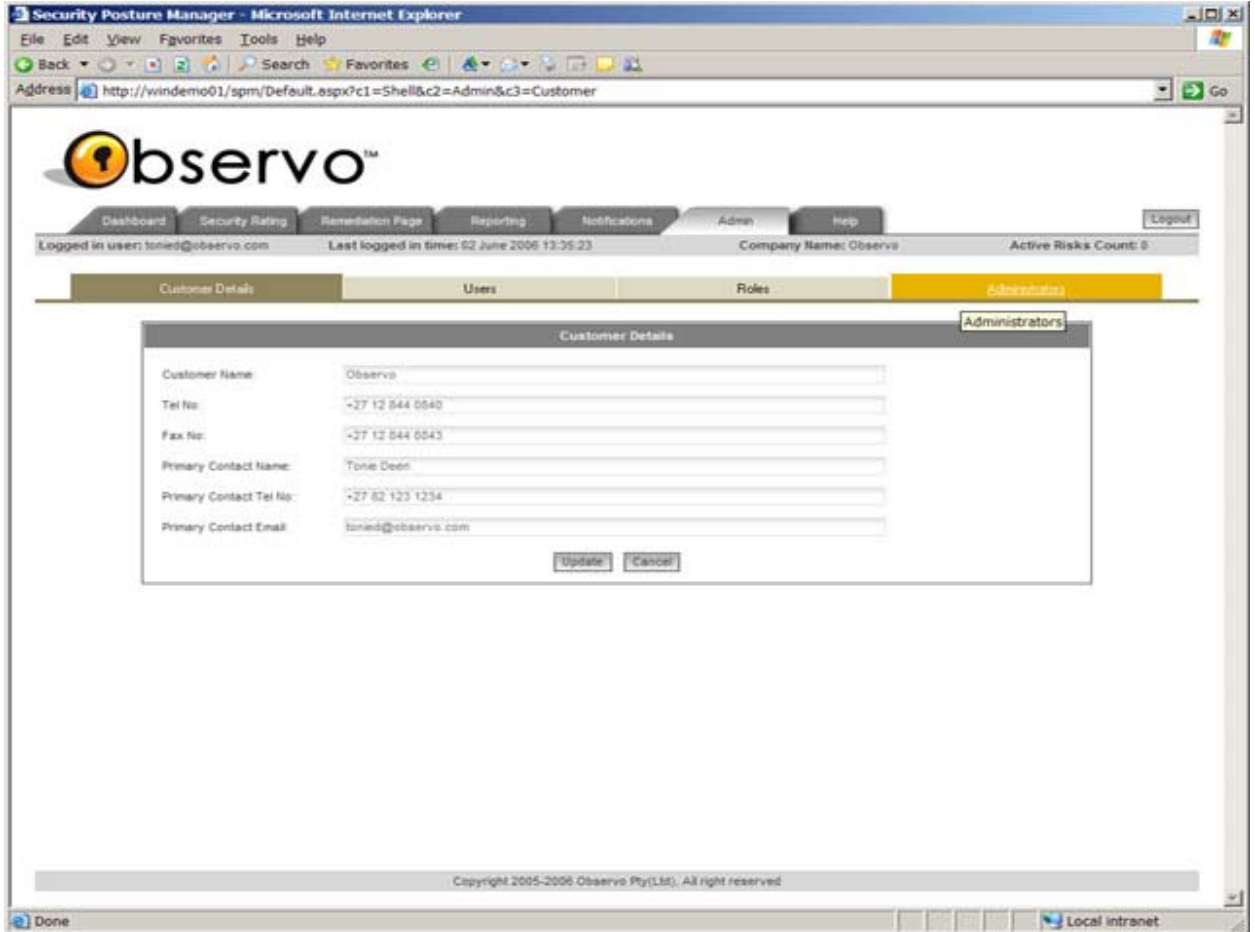
Customer: **Observe Ltd**

Year: 2005-2006

Demo: <http://windemo01.ru.enterra-inc.com/spmdemo>

URL: <http://www.observe.com>

## Screenshots



## Admin



Dashboard

The screenshot shows the Observo Security Posture Manager interface in a Microsoft Internet Explorer browser window. The page title is "Security Posture Manager - Microsoft Internet Explorer". The address bar shows the URL: http://windemo01/spm/Default.aspx?c1=Shell&c2=Remediation. The Observo logo is prominently displayed at the top left. Below the logo is a navigation menu with tabs for Dashboard, Security Rating, Remediation Page (selected), Reporting, Notifications, Admin, and Help. A "Logout" button is located on the far right of the navigation menu. Below the navigation menu, a status bar indicates the user is logged in as tonied@observo.com, last logged in on 02 June 2006 at 13:35:23. The company name is Observo, and the active risks count is 8. A filter section allows filtering by IP, Hostname, Severity, and Risk Status. The main content area is titled "Remediation" and contains a table with the following columns: Old IP Address, Hostname, Severity, Risk Name, Risk Status, Due Date, and Custodian. The table lists 23 items, each with a risk ID (e.g., E013), an IP address (e.g., 192.168.0.1), a hostname (e.g., ObWin3k), a severity level (e.g., High), a risk name (e.g., Permissions for the Everyone group should be restricted), a risk status (e.g., Active), a due date (e.g., 3/22/2006), and a custodian email (e.g., tanab@observo.com). The table is paginated, showing page 1 of 2 with 23 items displayed.

Old IP Address	Hostname	Severity	Risk Name	Risk Status	Due Date	Custodian
E013	192.168.0.1	ObWin3k	High	Permissions for the Everyone group should be restricted	Active	3/22/2006 tanab@observo.com
E043	192.168.0.1	ObWin3k	Critical	All unnecessary applications should be removed from production servers	Fixed	3/22/2006 tanab@observo.com
E074	192.168.0.1	ObWin3k	Critical	A stronger password policy needs to be implemented	Countered	3/22/2006 tanab@observo.com
E042	192.168.0.2	ObLinux	Low	Auditing should be enabled on the host	Fixed	3/22/2006 mytestacc@observo.com
E090	192.168.0.2	ObLinux	Informational	Move Your Web site to a Non-System Volume	Active	3/22/2006 mytestacc@observo.com
E014	192.168.0.1	ObWin3k	Medium	Do Not Display Last User Name in Logon Screen	Fixed	3/27/2006 tanab@observo.com
E011	192.168.0.1	ObWin3k	Informational	Remove or Secure FrontPage Server Extensions	Fixed	3/30/2006 tanab@observo.com
E012	192.168.0.1	ObWin3k	Informational	Map IS File Extensions to 404.dll	Accepted	3/30/2006 tanab@observo.com
E048	192.168.0.1	ObWin3k	Critical	Cumulative Security Update for Internet Explorer is not installed	Countered	3/30/2006 tanab@observo.com
E017	192.168.0.2	ObLinux	Informational	Allow log on locally setting should be secured	Countered	3/30/2006 mytestacc@observo.com
E018	192.168.0.2	ObLinux	High	Windows HTML Converter HR Align Buffer Overflow Vulnerability Found	Active	3/30/2006 mytestacc@observo.com
E020	192.168.0.2	ObLinux	High	Latest Service Pack for Windows 2003 Server Gold is not installed	Active	4/2/2006 mytestacc@observo.com
E034	192.168.0.1	ObWin3k	Medium	Windows Kernel Elevation of Privilege and Denial of Service Vulnerability was found	Active	5/2/2006 tanab@observo.com
E042	192.168.0.1	ObWin3k	Low	Auditing should be enabled on the host	Active	4/3/2006 tanab@observo.com
E089	192.168.0.1	ObWin3k	High	MSXML 4.0 Service Pack 2 has not been installed	Fixed	4/3/2006 tanab@observo.com
E024	192.168.0.1	ObWin3k	High	ActiveX Authenticode Verification Bypass Vulnerability was found	Fixed	4/3/2006 tanab@observo.com
E018	192.168.0.2	ObLinux	Critical	Execute permissions revoked from public on stored procedures msdb.dbo.sp_get_dtspackage	Countered	4/3/2006 mytestacc@observo.com
E063	192.168.0.2	ObLinux	Low	Administrative shares are available on the host	Accepted	4/3/2006 mytestacc@observo.com
E067	192.168.0.2	ObLinux	Low	Access to share granted to Everyone	Accepted	4/6/2006 mytestacc@observo.com
E068	192.168.0.2	ObLinux	Medium	Account Lockout Policy needs to be set	Accepted	4/6/2006 mytestacc@observo.com

## Remediation



## Reporting