

TPReport™ | The Reporting System for TippingPoint

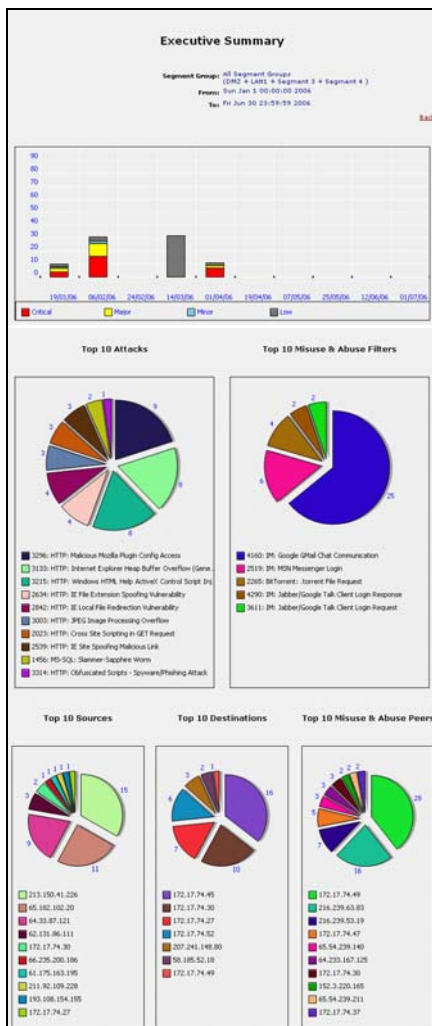
FEATURES AND BENEFITS

- Enterprise-wide Reporting and Trend Analysis
- Device Performance Monitoring
- Automatic Reporting
- One-Click Correlation
- Advance Reporting for Multiple TippingPoint System
- External Database Integration

Flexible, Powerful, TippingPoint IPS Reporting

TPReport is a handy companion tool that provides global vision and in-depth reporting to complement the embedded TippingPoint Local Security Manager (LSM).

TPReport is designed to provide immediately useful pre-packaged reports to cover the most common operational and management information that an organization would expect to see on a daily, weekly and monthly basis. TPReport features a user friendly and secure web interface that enables "big picture" analysis with trending reports, correlation and real-time graphs on traffic statistics, filtered attacks, network hosts and services, and TippingPoint IPS inventory and health.



Executive Summary

A very effective component of the TPReport is the Executive Summary. The Executive Summary provides at-a-glance event monitors for all TippingPoint systems in the network and filters behavior can be viewed and assessed.

One-Click-Correlation

A timely security information analysis is the key to remediation capabilities. TPReport's one-click-correlation is a unique feature to swiftly correlate all security incidents related to the suspicious host.

Flexible Data Field Sorting

TPReport features flexible capability to sort all displayed fields to enhance information analysis experience.

External Database Integration

Out-of-the-box support for Microsoft SQL and Oracle database enables TPReport to seamlessly integrate with any third party applications

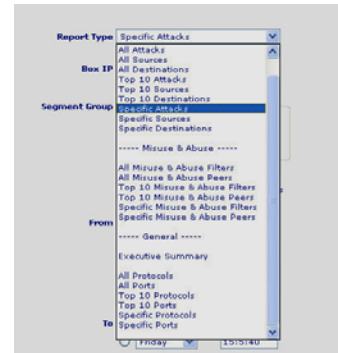
Visit Demo at:
<http://www.tippingpoint.com.sg>

SYSTEM REQUIREMENTS

- Intel Pentium-III Processor with 1GHZ and above
- Minimum 1GB RAM
- Minimum 2GB hard disk space
- Windows 2003, Windows XP with SP2
- .NET Framework 2.0
- Microsoft IIS

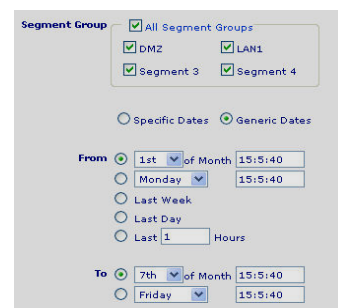
Archiving and Advanced Forensic Analysis

TPReport allows unlimited archiving of IPS events. Its easy-to-retrieve feature facilitates the continuous analysis of security incidents, system logs and network management information for immediate cyber attack containment, perpetrator location and identification, and damage mitigation.



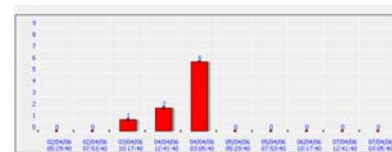
Comprehensive Reporting

While TippingPoint IPS detects and manages malicious attacks and network usage, event data automatically logs to the database of TPReport engine. A comprehensive set of security reports and graphs are made available in real time for operational decision:

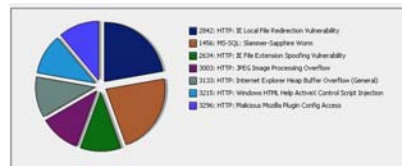


Attacks	Misuse & Abuse	General
<ul style="list-style-type: none"> • All Attacks • All Sources • All Destinations • Top 10 Attacks • Top 10 Sources • Top 10 Destinations • Specific Attacks • Specific Sources • Specific Destinations 	<ul style="list-style-type: none"> • All Misuse & Abuse Filters • All Misuse & Abuse Peers • Top 10 Misuse & Abuse Filters • Top 10 Misuse & Abuse Peers • Specific Misuse & Abuse Filters • Specific Misuse & Abuse Peers 	<ul style="list-style-type: none"> • Executive Summary • All Protocols • All Ports • Top 10 Protocols • Top 10 Ports • Specific Protocols • Specific Ports

Event Name	Attack Type	Severity	Source IP	Description	IP
2842_Http://_IE Local File Redirection Vulnerability	Block	Critical	213.191.249.229	98.189.92.89	2
1456_Http://_SslBanner/SslBanner Worm	Block	Critical	64.30.87.121	98.189.92.89	2
2424_Http://_File Extension Spoofing Vulnerability	Block	Major	213.191.249.229	98.189.92.89	2
2842_Http://_IE Local File Redirection Vulnerability	Block	Critical	193.109.194.199	372.17.74.92	1
2842_Http://_IE Local File Redirection Vulnerability	Block	Critical	64.30.87.121	372.17.74.92	1
2003_Http://_Pps/Java/Flashvars/OverFlow	Block	Major	65.182.182.20	372.17.74.92	1
2123_Http://_Internet Explorer Heap Buffer Overflow (General)	Block	Critical	65.182.182.20	372.17.74.92	1
2123_Http://_Windows HTML Help ActiveX Control Script Injection	Block	Major	213.191.249.229	372.17.74.92	1
2226_Http://_Malicious Media Plugin Config Access	Block	Critical	64.30.87.121	372.17.74.92	1



Event Name	Attack Type	Severity	Prevalence	IP
2842_Http://_IE Local File Redirection Vulnerability	Block	Critical	High	2
1456_Http://_SslBanner/SslBanner Worm	Block	Critical	High	2
2424_Http://_File Extension Spoofing Vulnerability	Block	Major	High	1
2842_Http://_IE Local File Redirection Vulnerability	Block	Critical	High	1
2842_Http://_IE Local File Redirection Vulnerability	Block	Critical	High	1
2003_Http://_Pps/Java/Flashvars/OverFlow	Block	Major	High	1
2123_Http://_Internet Explorer Heap Buffer Overflow (General)	Block	Critical	High	1
2123_Http://_Windows HTML Help ActiveX Control Script Injection	Block	Major	High	1
2226_Http://_Malicious Media Plugin Config Access	Block	Critical	High	1



Event Name	Attack Type	Severity	Prevalence	IP
2842_Http://_IE Local File Redirection Vulnerability	Block	Critical	High	2
1456_Http://_SslBanner/SslBanner Worm	Block	Critical	High	2
2424_Http://_File Extension Spoofing Vulnerability	Block	Major	High	1
2842_Http://_IE Local File Redirection Vulnerability	Block	Critical	High	1
2842_Http://_IE Local File Redirection Vulnerability	Block	Critical	High	1
2003_Http://_Pps/Java/Flashvars/OverFlow	Block	Major	High	1
2123_Http://_Internet Explorer Heap Buffer Overflow (General)	Block	Critical	High	1
2123_Http://_Windows HTML Help ActiveX Control Script Injection	Block	Major	High	1
2226_Http://_Malicious Media Plugin Config Access	Block	Critical	High	1

Copyright © 2006 Cohesion Network Technologies Pte Ltd (CNT). TippingPoint is a registered trademark of 3Com Corporation. TPReport is a trademark of Cohesion Network Technologies Pte Ltd. All other company and product names may be trademarks of their respective holders. While every effort is made to ensure the information given is accurate, CNT does not access liability for any errors or mistake which may arise. Specifications and other information in this document may be subject to change without notice.