

## Mapping EventTracker Reports and Alerts To PCI-DSS Requirements

© Prism Microsystems, April 2008

| PCI DSS Requirement                          |  | EventTracker Capability   | EventTracker Reports   | Sample EventTracker Alerts  |
|--|--|---|--|---|
| <b>Build &amp; Maintain a Secure Network</b> | <b>Requirement 1:</b><br>Install and maintain a firewall configuration     | 1. Network Connection Monitoring on all windows servers<br><br>2. Monitor for changes or unauthorized access to routers & switches.<br><br>3. Monitor firewall activity | 1. Compliance->Device Specific <ul style="list-style-type: none"> <li>• Check Point Analysis</li> <li>• CISCO-PIX</li> <li>• ISA Server</li> <li>• SNORT</li> <li>• Citrix</li> </ul> 2. Compliance->Incident Response <ul style="list-style-type: none"> <li>• CISCO-PIX: IDS intrusion detection</li> <li>• ISA Server: Intrusion detection</li> <li>• Suspicious Network Activity</li> <li>• SNORT: Port scan alerts</li> <li>• SNORT: Virus activity alerts</li> <li>• SYSLOG: Possible intrusion attack</li> </ul> 3. Operations->Network Traffic <ul style="list-style-type: none"> <li>• Network Connection Activity</li> </ul> | CISCO PIX: Authentication failure<br><br>CISCO PIX: IDS intrusion detection<br><br>ISA Server: All port - port scan detected<br><br>ISA Server: Excessive Winsock application open<br><br>ISA Server: Failed to start service<br><br>ISA Server: Out-of-Band attack detected<br><br>ISA Server: UDP attack detected |
|  | <b>Requirement 2:</b><br>Do not use vendor-supplied defaults for passwords |   |  |   |

| PCI DSS Requirement     |   | EventTracker Capability  | EventTracker Reports  | Sample EventTracker Alerts  |
|-------------------------|---|--|---|---|
| Protect Cardholder Data | <b>Requirement 3:</b><br>Protect stored cardholder data                                       | 1. Monitor all file server access<br><br>2. Monitor access to database servers<br><br>3. Monitor configuration changes on critical file and database servers | 1. Compliance->Incident Response <ul style="list-style-type: none"> <li>Suspicious Network Activity</li> </ul> 2. Compliance->Access Control <ul style="list-style-type: none"> <li>File/Resource access Success</li> <li>File/Resource access failure</li> </ul> 3. Compliance->System and Data Integrity <ul style="list-style-type: none"> <li>EventTracker: Device changes</li> <li>Veritas</li> <li>Solaris BSM: Device mount and unmount</li> </ul> 6. Compliance->Device Specific <ul style="list-style-type: none"> <li>SQL server</li> <li>Oracle</li> </ul> 7. Operations->WhatChanged<br>8. Operations: Disk Maintenance<br>9. Operations->Disk Space Forecasting<br>10. Operations->Veritas Backup Exec for Windows | Detected high memory usage<br><br>Disk space is critically low<br><br>SQL Server: SQL server stopped<br><br>SQL Server: Transaction log full<br><br>IIS: WWW Service Terminated<br><br>IIS: Server stopped<br><br>Oracle<br><br>Veritas Backup Exec alerts<br><br>Excessive resource access failures by an user |
|                         | <b>Requirement 4:</b><br>Encrypt transmission of cardholder data across open, public networks |  |   |   |

| PCI DSS Requirement                                |   | EventTracker Capability   | EventTracker Reports   | Sample EventTracker Alerts  |
|--|---|---|--|---|
| <b>Maintain a Vulnerability Management Program</b> | <b>Requirement 5:</b><br>Use and regularly update anti-virus software         | 1. Monitor the status of anti-virus applications, custom application logs using EventTracker log file monitor<br><br>2. Monitor anti-virus service status and restart services when required<br><br>3. Monitor all security patches and updates to servers.<br><br>4. Enforce system and application policies on critical servers using Whatchanged and periodically compare policy | 1. Operations->Antivirus<br><br>2. Operations->Service Downtime<br><br>3. Operations->EventTracker <ul style="list-style-type: none"> <li>• EventTracker: Service changes</li> <li>• EventTracker: Software Install/Uninstall</li> <li>• EventTracker : Logfile monitor</li> </ul> 4. Compliance-> Business Continuity <ul style="list-style-type: none"> <li>• System: Patches and hotfixes</li> <li>• System shutdown</li> </ul> | Critical service could not be started<br><br>Critical service not running<br><br>Detected software <Some S/W> has been installed on this system<br><br>Software Install/Uninstall<br><br>Software uninstalled from a system<br><br>System is not reachable, it may be down<br><br>System resource exhausted |
|  | <b>Requirement 6:</b><br>Develop and maintain secure systems and applications | 5. Monitor user access to all servers, activities of administrators and other privileged accounts, and changes to active directory.<br><br>6. Monitor unauthorized software install and install on all servers  | 5. Compliance->Acceptable use<br><br>6. Compliance->Access Control<br><br>7. Security-> Policy Changes<br><br>8. Security-> User Management<br><br>9. Security-> AD/Account Management<br><br>10. Compliance-> Change Management   | System Shutdown   |

| PCI DSS Requirement                      |  | EventTracker Capability   | EventTracker Reports  | Sample EventTracker Alerts                                       |
|--|--|---|---|--|
| Implement Strong Access Control Measures | <b>Requirement 7:</b><br>Restrict access to cardholder data          | 1. Monitor file and folder access on all servers<br><br>2. Monitor successful and failed logon attempts to all servers<br><br>3. Monitor all administrators' activity<br><br>4. Monitor all user activity | 1. Compliance->Access Control<br><br>2. Compliance-> Change Mangement<br><br>3. Security-> Policy Changes<br><br>4. Security-> User Management<br><br>5. Security-> AD/Account Management<br><br>6. EventTracker User Activity Viewer | Administrative log-on  |
|  | <b>Requirement 8:</b><br>Assign a unique ID to each person           |   |   | Administrative log-on failure                                    |
|  | <b>Requirement 9:</b><br>Restrict physical access to cardholder data |   |   | Domain policy changed  |
|  |  |   |   | Excessive user lockout in your enterprise                        |
|  |  |   |   | Excessive remote connections established on a local network port |
|  |  |   |   | Excessive logon failures in your enterprise                      |
|  |  |   |   | Excessive logon failures due to bad password/username            |
|  |  |   |   | Excessive logon attempts from a particular IP address            |
|  |  |   |   | Excessive file deletes on a computer                             |
|  |  |   |   | Excessive access failures on a specific computer                 |
|  |  |   |   | Excessive access failures by an user                             |

| PCI DSS Requirement                            |   | EventTracker Capability  | EventTracker Reports  | Sample EventTracker Alerts   |
|--|---|--|---|--|
| <b>Regularly Monitor &amp; Test Networks</b>   | <b>Requirement 10:</b><br>Track and monitor all access to network resources and cardholder data | 1. Monitor network and object access<br><br>2. Secure archiving of audit logs<br><br>3. Monitor changes to windows system files and registry | 1. Compliance-> Incident Response <ul style="list-style-type: none"> <li>Suspicious Network Activity</li> </ul> 2. Compliance-> Access Control <ul style="list-style-type: none"> <li>File/Resource access Success</li> <li>File/Resource access failure</li> </ul> 3. Compliance-> System and Data Integrity <ul style="list-style-type: none"> <li>EventTracker: Device changes</li> <li>Veritas</li> <li>Solaris BSM: Device mount and unmount</li> <li>EventTracker: Cab integrity verification</li> </ul> 4. Operations-> WhatChanged<br>5. Operations -> Alerts | Agent not running<br><br>Audit log cleared<br><br>Directory permission change<br><br>Eventlog full<br><br>EventTracker cab integrity checksum failure<br><br>Excessive ping failures - system(s) are not reachable<br><br>Excessive file deletes on a computer<br><br>Excessive access failures on a specific computer<br><br>Excessive access failures in your enterprise |
|  | <b>Requirement 11:</b><br>Regularly test security systems and processes                         |  |   |  |
| <b>Maintain an Information Security Policy</b> | <b>Requirement 12:</b><br>Maintain a policy that addresses information security                 | 1. Periodically compare policies enforced on all servers   | 1. WhatChanged -> Compare policy<br>2. Compliance ->Risk Management   |  |