

Mapping EventTracker Reports and Alerts To The Consensus Audit Guidelines

© Prism Microsystems, April 2009

| Consensus Audit Guidelines | EventTracker Capability | EventTracker Reports | EventTracker Alerts |
|--|---|---|---|
| Control 1 - Inventory of Hardware | 1. Continuously ping all the systems where agent has been installed. 2. Monitor USB and other external devices added to the network | 1. EventTracker: Ping Status 2. EventTracker: Device Change | Excessive ping failures – system(s) are not reachable. USB insert Alert USB device disabled |
| Control 2 - Inventory of Software | 1. Monitor software install/uninstall 2. Monitor USB and other external device usage 3. Monitor critical file system and registry changes | 1. Operation->Software Maintenance <ul style="list-style-type: none"> • Software install/uninstall 2. Operation ->WhatChanged <ul style="list-style-type: none"> • Critical System Changes • Summary of File Changes • Summary of Registry Changes 3. EventTracker: Device Change | Software install/uninstall USB insert Alert EventTracker: USB device disabled |

Mapping EventTracker to the CAG

| | | | |
|---|--|--|--|
| <p>Control 3 - Secure Configurations for Computers</p> | <p>1. Monitor unauthorized software install and uninstall on all servers</p> <p>2. Monitor All the Agents</p> <p>3. Monitor configuration changes on critical file and database servers</p> <p>4. Enforce system and application policies on critical servers using Whatchanged and periodically compare policy</p> <p>5. Monitor all security patches and updates to servers.</p> | <p>1. Compliance-> Change Management</p> <p>2. EventTracker: EventTracker Agent Changes</p> <p>3. Operations->WhatChanged</p> <ul style="list-style-type: none"> • Critical system changes • Operating system changes <p>4. Compliance-> Business Continuity</p> <ul style="list-style-type: none"> • System: Patches and hotfixes • System shutdown <p>5. Compliance-> Change Management</p> <p>6. Compliance->Device Specific</p> <ul style="list-style-type: none"> • SQL server • Oracle • MS Exchange • ISA Server • Altiris <p>7. Operations: Disk Maintenance</p> <p>8. Operations->Disk Space Forecasting</p> <p>9. Operations->Veritas Backup Exec for Windows</p> <p>10. Operations->Service Downtime</p> <p>11. Operation->Device Change</p> <p>12. Compliance->Asset Management</p> | <p>Software Install/Uninstall</p> <p>EventTracker agent configuration changed.</p> <p>Audit log is cleared/Event log full</p> <p>Disk space is critically low</p> <p>Spyware</p> <p>System resource exhausted</p> <p>System shutdown</p> <p>System is not reachable and it may be down</p> <p>USB insert Alert</p> <p>USB device disabled</p> <p>Critical service could not be started</p> <p>Critical service is not running</p> <p>Detected Software has been installed on this system</p> <p>Directory permission changed</p> <p>Domain policy changed</p> <p>Group policy processing error</p> |
|---|--|--|--|

Mapping EventTracker to the CAG

| | | | |
|--|--|---|--|
| <p>Control 4 – Secure Configurations of Network Devices</p> | <p>1. Monitor configuration access to all network devices and firewalls</p> <p>2. Monitor configuration changes to network devices and firewalls</p> | <p>1. Compliance->Incident Response</p> <ul style="list-style-type: none"> • Suspicious Network Activity <p>2. Compliance->Device Specific</p> <ul style="list-style-type: none"> • Checkpoint Analysis • CISCO IOS • CISCO PIX • CISCO VPN • Citrix • Fortigate • Netscreen • Snort | <p>CISCO PIX: Access Denied</p> <p>CISCO PIX: Authentication failed</p> <p>CISCO PIX: Intrusion detection</p> <p>CISCO PIX: Failover Message</p> <p>CISCO VPN: Admin Access - Authentication Failure</p> <p>CISCO VPN: Admin Access - Authorization failure</p> <p>CISCO VPN: Memory Allocation Failed</p> <p>CISCO VPN: Admin Access-Access Control Lookup Failure</p> <p>Netscreen: Authentication failure</p> <p>Netscreen: IDS intrusion detection</p> <p>Netscreen: USB storage device attached/detached</p> <p>Netscreen: Security device error</p> <p>Netscreen: Spam found</p> <p>Netscreen: System configuration erased</p> |
|--|--|---|--|

Mapping EventTracker to the CAG

| | | | |
|--|---|---|--|
| <p>Control 5 - Boundary Defense</p> | <p>1. Monitor all tcp and udp connections opened modified and closed.</p> <p>3. Monitor suspicious network activity</p> | <p>1. Operations->Network Traffic</p> <ul style="list-style-type: none"> • Network Connection Activity • Suspicious Network Activity <ol style="list-style-type: none"> a. Most Active Ports b. Most Active Systems c. Open and Listening Ports d. Possible Infections e. Suspicious Ports <p>2. Operations->Checkpoint</p> <p>3. Operations->Checkpoint Analysis</p> <p>4. Operations->Netscreen Firewall Reports</p> <p>5. Operations->VPN Usage</p> <p>6. Operations->CISCO PIX</p> <p>7.Operations-Device Specific</p> <ul style="list-style-type: none"> • CISCO IOS • Citrix • Fortigate • Snort • ISA Server <p>8. Compliance->Incident Response</p> <p>9. Operations->Intrusion Detection System</p> | <p>Ports: Spoof Sites</p> <p>Spyware</p> <p>CISCO PIX: Intrusion detection</p> <p>ISA Server: All port - port scan detected</p> <p>ISA Server: Excessive Winsock application open</p> <p>ISA Server: Failed to start service</p> <p>ISA Server: Land attack detected</p> <p>ISA Server: Network communication device may be down</p> |
|--|---|---|--|

Mapping EventTracker to the CAG

| | | | |
|---|--|--|---|
| <p>Control 6 - Security Audit Logs</p> | <p>1. Enforce audit policies on all critical servers</p> <p>2. Back up Windows Event viewer logs using the EventTracker agent</p> <p>3. Import all audit data (log files other than .evt) using EventTracker Direct Log Archiver</p> | <p>1. Operations->EventTracker</p> <ul style="list-style-type: none"> • Cab integrity verification • Direct Archiver • Windows log backup and clear <p>2. Operations->WhatChanged</p> <ul style="list-style-type: none"> • Eventlog location change • Group policy change <p>3. Compliance->Risk Management</p> <p>4. Compliance->System and Data Integrity</p> <p>5. Operations->Platform Specific->Windows</p> <ul style="list-style-type: none"> • All Security Events • All Audit Events <p>5. Operations->Platform Specific</p> | <p>Domain policy changed</p> <p>Eventlog cleared</p> <p>Eventlog full</p> |
|---|--|--|---|

Mapping EventTracker to the CAG

| | | | |
|---|---|--|--|
| <p>Control 7 - Application Software Security</p> | <p>1. Enforce application software policies through EventTracker Change</p> <p>2. Monitor changes to file and registry systems on all critical servers</p> <p>3. Schedule daily policy comparison</p> | <p>1. Compliance->Access Control</p> <ul style="list-style-type: none"> • File/Resource access Success • File/Resource access failure <p>2. Operations->WhatChanged</p> <ul style="list-style-type: none"> • File changes summary • Registry changes summary • ODBC changes • Windows startup change <p>3. Operations->Device Specific</p> <ul style="list-style-type: none"> • Altiris • Doubletake • SQL Server • Oracle • MS Exchange • ISA Server <p>4. Operations->Platform specific->Windows</p> <ul style="list-style-type: none"> • Application: Dr. Watson's events • IIS • FTP • Certificate services • IMAP4 • File replication <p>5. Compliance->Business Continuity</p> | <p>IIS: Logging shutdown</p> <p>McAfee virus scan enterprise: update failed</p> <p>SQL server stopped.</p> |
|---|---|--|--|

Mapping EventTracker to the CAG

| | | | |
|---|--|---|--|
| <p>Control 8 - Use of Admin Privileges</p> | <p>1. Monitor all administrators' activity</p> | <p>1. Compliance->Access Control 2. Security-> Policy Changes 3. Security-> User Management 4. Security-> AD/Account Management 5. Compliance-> Change Management 6. EventTracker user activity viewer • Admin Activity 7. Compliance->Acceptable Use 8. Operations->VPN Usage</p> | <p>Administrative log-on Administrative log-on failure Domain policy changed</p> |
|---|--|---|--|

Mapping EventTracker to the CAG

| | | | |
|---|---|---|---|
| <p>Control 9 - Access Based on Need to Know.</p> | <ol style="list-style-type: none"> 1. Monitor file and folder access on all servers 2. Monitor successful and failed logon attempts to all servers 3. Monitor all administrators' activity 4. Monitor all user activity | <ol style="list-style-type: none"> 1. Compliance->Access Control 2. Compliance-> Change Management 3. Security-> Policy Changes 4. Security-> User Management 5. Security-> AD/Account Management 6. EventTracker User Activity Viewer 7. Compliance->Acceptable Use 8. Operations->Whatchanged 9. Operations->User Activity 10. Operations->VPN Usage | <p>Administrative log-on</p> <p>Administrative log-on failure</p> <p>Domain policy changed</p> <p>Excessive user lockout in your enterprise</p> <p>Excessive remote connections established on a local network port</p> <p>Excessive logon failures in your enterprise</p> <p>Excessive logon failures due to bad password/username</p> <p>Excessive logon attempts from a particular IP address</p> <p>Excessive file deletes on a computer</p> <p>Excessive access failures on a specific computer</p> <p>Excessive access failures by a user</p> |
|---|---|---|---|

Mapping EventTracker to the CAG

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

Mapping EventTracker to the CAG

| | | | |
|---|--|---|--|
| <p>Control 11 - Dormant Account Monitoring</p> | <p>1. Monitor all user log on and log off activity</p> <p>2. Configure alerts for any activity detected for dormant accounts</p> <p>3. Monitor all failed user logon attempts and failed access to files and folders</p> | <p>1. Operations->User Activity</p> <p>2. Security->User Management</p> <p>3. Operations->VPN Usage</p> <p>4. Operations->User Logon Failure Report</p> | <p>Excessive logon failures in your enterprise</p> <p>Excessive logon failures due to bad password/username</p> <p>Excessive logon attempts from a particular IP address</p> <p>Excessive file deletes on a computer</p> <p>Excessive access failures on a specific computer</p> <p>Excessive access failures by an user</p> |
|---|--|---|--|

Mapping EventTracker to the CAG

| | | | |
|--|---|--|---|
| <p>Control 12 - Anti-Malware Defenses</p> | <p>1. Monitor the status of anti-virus applications, custom application logs using EventTracker log file monitor</p> <p>2. Monitor anti-virus service status and restart services when required</p> <p>3. Monitor all security patches and updates to servers.</p> <p>4. Monitor unauthorized software install and install on all servers</p> <p>5. Monitor USB and other external device usage</p> | <p>1. Operations->Antivirus</p> <p>2. Operations->Service Downtime</p> <p>3. Operations->EventTracker</p> <ul style="list-style-type: none"> • EventTracker: Service changes • EventTracker: Software Install/Uninstall <p>4. Compliance-> Business Continuity</p> <ul style="list-style-type: none"> • System: Patches and hotfixes • System shutdown | <p>Critical service could not be started</p> <p>Critical service not running</p> <p>Detected software <Some S/W> has been installed on this system</p> <p>Software Install/Uninstall</p> <p>Software uninstalled from a system</p> <p>USB insert Alert</p> <p>EventTracker: USB device disabled</p> |
|--|---|--|---|

Mapping EventTracker to the CAG

| | | | |
|---|--|--|--|
| <p>Control 13 - Control of Ports, Protocols and Services</p> | <ol style="list-style-type: none"> 1. Monitor network activity. 2. Monitor new sockets created 3. Monitor all suspicious network activity | <ol style="list-style-type: none"> 1. Operations->Network Traffic <ul style="list-style-type: none"> • Network Connection Activity • Suspicious Network Activity <ol style="list-style-type: none"> a. Most Active Ports b. Most Active Systems c. Open and Listening Ports d. Possible Infections e. Suspicious Ports 2. Security->Incident Response 3. Operations->Intrusion Detection System | <p>Ports: Spoof Sites</p> <p>Spyware</p> <p>CISCO PIX: Intrusion detection</p> <p>ISA Server: All port - port scan detected</p> <p>ISA Server: Excessive Winsock application open</p> <p>ISA Server: Failed to start service</p> <p>ISA Server: Land attack detected</p> <p>ISA Server: Network communication device may be down</p> |
|---|--|--|--|

Mapping EventTracker to the CAG

| | | | |
|--|--|--|--|
| <p>Control 14 - Wireless Device Control</p> | <p>4. Monitor all USB and other external devices plugged into the network</p> <p>5. Enforce remedial action to disable unauthorized USB devices in the network</p> | <p>1. Operations -> USB Device Report</p> <p>2. Operations->USB Device Disabled Report</p> <p>3. Operations->EventTracker</p> <ul style="list-style-type: none"> • USB or Other Device Monitoring • Remedial action | <p>USB insert Alert</p> <p>EventTracker: USB device disabled</p> |
|--|--|--|--|

Mapping EventTracker to the CAG

| | | | |
|--|---|--|--|
| <p>Control 15 - Data Leakage Protection</p> | <ol style="list-style-type: none"> 1. Monitor network and object access 2. Secure archiving of audit logs 3. Monitor changes to windows system files and registry 4. Monitor all USB and other external devices plugged into the network 5. Enforce remedial action to disable unauthorized USB devices in the network | <ol style="list-style-type: none"> 1. Operations -> USB Device Report 2. Compliance-> Access Control <ul style="list-style-type: none"> • File/Resource access Success • File/Resource access failure 3. Compliance-> System and Data Integrity <ul style="list-style-type: none"> • EventTracker: Device changes • Veritas • Solaris BSM: Device mount and unmount • EventTracker: Cab integrity verification 4. Operations-> WhatChanged 5. Operations -> Alerts 6. Operations->USB Device Disabled Report 7. Compliance->System and Data Integrity 8. Operations->Veritas Backup Exec 9. Operations->NetApp Data ONTAP 10. Operations->Device Specific <ul style="list-style-type: none"> • Altiris • Doubletake | <p>USB insert Alert</p> <p>EventTracker: USB device disabled</p> <p>Directory permission change</p> <p>EventTracker cab integrity checksum failure</p> <p>Excessive file deletes on a computer</p> <p>Excessive access failures on a specific computer</p> <p>Excessive access failures in your enterprise</p> |
|--|---|--|--|