

Mapping EventTracker Reports and Alerts To FISMA Requirements NIST SP 800-53 Revision 3

© Prism Microsystems, August 2009

FISMA Requirement (NIST)		EventTracker	
Family	Control	Reports	Sample Alerts
Access Control	AC-2 Account Management	<ul style="list-style-type: none"> • *Security: User Account disabled • *Security: User Account enabled • *Security: User Account locked • Active Directory: User added • Active Directory: User deleted • *Security: User added to group • *Security: User removed from group • *Security: Account rename • Solaris BSM: User management • Solaris BSM: Disable user 	<ul style="list-style-type: none"> • Domain policy changed • Excessive user lockout in your enterprise • Excessive logon failures due to bad password/username • Excessive logon attempts from a particular IP address • Excessive access failures on a specific computer • Excessive access failures by a user
	AC-17 Remote Access	<ul style="list-style-type: none"> • Windows: Account logon • Windows: Account logon failure • EventTracker: Initial User Network logon • *Security: User logon • *Security: User logoff • Active Directory: User logons • Active Directory: User logoffs • Security->Access Control (all reports) 	

FISMA Requirement (NIST)		EventTracker	
Family	Control	Reports	Sample Alerts
	AC-19 Access Control for Portable and Mobile Devices	<ul style="list-style-type: none"> • USB Device: Report Detail • USB Device: Report Failure • Exchange ActiveSync: Policy compliance • Exchange ActiveSync: User Agent 	<ul style="list-style-type: none"> • USB Insert Alert
Audit And Accountability	AU-1 Audit and Accountability Policy and Procedures	<ul style="list-style-type: none"> • Active Directory: Group Policy (all reports) • *Security: Policy Change • *Security: Audit Policy change • Checkpoint: Audit activities • Solaris BSM: Audit Policy changes 	<ul style="list-style-type: none"> • Domain Policy Changed
	AU-4 Audit Storage Capacity	<ul style="list-style-type: none"> • Disk Space Forecasting: Disk Space Availability • Disk Space Forecasting: Disk Space Status • Disk Space Forecasting: Disk Utilization Trend 	<ul style="list-style-type: none"> • Disk Full • Disk Space Critically Low
	AU-5 Response to Audit Process Failure	<ul style="list-style-type: none"> • EventTracker: CAB integrity verification • EventTracker: Collection master error • EventTracker: Collection point error • EventTracker: Disk Space low • EventTracker: Eventlog full 	<ul style="list-style-type: none"> • System Audit Log Cleared • Critical Service Not Running • Critical Service Not Started • Event Log Full • Event Log Cleared • EventTracker agent service failed • Collection Master Error • Collection Point Error • IIS Logging Shutdown • MExchange: Log disk full • System Shutdown • SQL Server: Transaction Log Full

FISMA Requirement (NIST)		EventTracker	
Family	Control	Reports	Sample Alerts
	AU-6 Audit Review	<ul style="list-style-type: none"> • Windows: Account logon • Windows: Account logon failure • EventTracker: Initial User Network logon • *Security: User logon • *Security: User logoff • Active Directory: User logons • Active Directory: User logoffs • Solaris BSM: SU failure • Solaris BSM: SU success • Solaris BSM: Failed local logon/logoff • Solaris BSM: Privileged use • NetApp Data ONTAP: Delete Access • NetApp Data ONTAP: Logon failure • NetApp Data ONTAP: Read Access • NetApp Data ONTAP: User Logon • NetApp Data ONTAP: Write Access • Exchange ActiveSync: Policy compliance • Security->Access Control (all reports) 	<ul style="list-style-type: none"> • Admin Login Failure • Admin Login Success • Solaris BSM: SU failure • Solaris BSM: SU success • Solaris BSM: User Management
	AU-9 Protection Of Audit Information	<ul style="list-style-type: none"> • File Resource Access Success:Delete Access • File Resource Access Failure:Delete Access • Active Directory:Deleted Share • Active Directory:Share Folder deleted • NetApp Data ONTAP: Delete Access • Whatchanged: Files Deleted 	<ul style="list-style-type: none"> • EventTracker CAB integrity checksum failed • Admin Login Failure

FISMA Requirement (NIST)		EventTracker	
Family	Control	Reports	Sample Alerts
Configuration Management	CM-3 Configuration Change Control	<ul style="list-style-type: none"> • WhatChanged: (all reports) • *Security: Policy Change • *Security: Audit Policy Change • Active Directory: Changed objects • Active Directory: OU change • CISCO PIX: Priv level changed • EventTracker: Service changes • File/resource Access Failure: Change property • File/resource Access Failure :Change ownership • File/resource Access Success: Change property • File/resource Access Success: Change ownership • Solaris BSM: Audit policy changes • Solaris BSM: set, create, change passwords • Syslog: Password changed 	<ul style="list-style-type: none"> • Agent not running • Audit log cleared • Directory permission change • Eventlog full • EventTracker cab integrity checksum failure • Excessive ping failures - system(s) are not reachable • Excessive file deletes on a computer • Excessive access failures on a specific computer • Excessive access failures in your enterprise
System And Information Integrity	SI-4 Information System Monitoring Tools and Techniques	<p>Too many to list, including reports on Window, UNIX, Linux, network devices including firewalls (CISCO PIX, Checkpoint) routers and switches, infrastructure applications like Citrix, IIS, databases and many more...</p>	<ul style="list-style-type: none"> • Excessive remote connections established on a local network port • Excessive logon failures in your enterprise • Excessive access failures in your enterprise • Excessive access failures on specific computer • Excessive file deletes on a computer • Excessive access failure by user • Logon Failures • Logon Failures from a specific computer • Excessive Logon failures due to bad password • Excessive remote connections established • Excessive User Lockout • ISA Server: Port Scan Detected • ISA Server: Land Attack detected • ISA Server: Out-of-bound attack • ISA Server: Ping attack • ISA Server: Spoof attack

FISMA Requirement (NIST)		EventTracker	
Family	Control	Reports	Sample Alerts
			<ul style="list-style-type: none"> • ISA Server: UDP attack • Netscreen: IDS Intrusion detected • Netscreen: Security device error • CISCO PIX: IDS Intrusion detected
	SI-7 Software and Information Integrity 8500.2: ECSD-2 DCID 6/3: 4.B.1.c(2)(b)	<ul style="list-style-type: none"> • EventTracker: Service changes • Snort: Denial of service alerts • System: Service control manager • EventTracker: Software install/uninstall • Solaris BSM: Package management 	<ul style="list-style-type: none"> • Detected Software install