Netsurion | EventTracker

CJIS Security Policy
Version 5.7
Solution Brief

www.netsurion.com/eventtracker

CJIS SECURITY POLICY

About Netsurion

Netsurion powers secure and agile networks for highly distributed and small-to-medium enterprises and the IT providers that serve them. In such environments, the convergence of threat protection and network management are driving the need for greater interoperability between the NOC (network operations center) and the SOC (security operations center) as well as solutions that fuse technology and service to achieve optimal results. To this end, Netsurion has converged purpose-built network hardware, innovative security software, and flexible managed services.

Netsurion's SD-Branch solution, BranchSDO, is a comprehensive network management and security solution consisting of SD-WAN, next-gen security, cellular, Wi-Fi, and PCI DSS compliance tools and support. At the heart of the solution is the CXD, Netsurion's SD-WAN edge appliance.

Netsurion's Security Operations solution, EventTracker, delivers advanced threat protection and compliance benefits in a variety of deployment options: a SIEM platform, a co-managed SIEM service with 24/7 SOC, and a managed SIEM for MSPs.

CJIS Security Policy Compliance

The Criminal Justice Information Services Division of the FBI gives federal, state and local law enforcement and criminal justice agencies-controlled access to a wide range of criminal justice information such as digital fingerprint records, arrest and stolen property reports, criminal records, and digital evidence such as dashboard and body-worn camera video. A wide variety of agencies, external organizations and individuals may need to access CJI. To that end, the CJIS has established a Security Policy defining the minimum set of security controls required for interacting with CJI. The CJIS Security Policy applies to every individual—contractor, private entity, non-criminal justice agency representative, or member of a criminal justice entity— with access to, or who administers criminal justice services and information including private contractors such as cloud service providers. All private contractors who process CJI must sign the CJIS Security Addendum, a uniform agreement that ensures the contractor's IT systems and practices are consistent with the CJIS Security Policy. While the CJIS provides uniform information security requirements, guidelines, and agreements, the Security Policy is left to the individual states and local jurisdictions to interpret. Specific administrative, technical and contractual requirements vary from state to state, and from locality to locality.

The EventTracker Control Center staff, while working closely with our end user customers, delivers SIEMphonic co-managed services. These services include SIEM administration, and continuous tuning, filtering and analysis using the EventTracker SIEM software platform. The SIEM software captures logs and event data from network and system components, such as operating system logs, application logs, logs from perimeter firewalls, IDS, Antivirus and more. It integrates and correlates inbound data with threat intelligence feeds, reputation indications, application safe-listing, and uses behavioral analysis to automatically provide direct, real-time response/remediation to notify and optionally terminate processes and/or systems that may compromise an organization's security and/or ability to demonstrate compliance with NIST and similar controls.

CJIS Security Policy Control Families

CJIS Security Section	Control Description	NIST 800-53	EventTracker Capability
5.3.2.1 Incident Handling	The agency shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Wherever feasible, the agency shall employ automated mechanisms to support the incident handling process. Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports	IR-4, IR-4(1), IR-4(3), IR-4(4), IR-8	Enable timely detection of any user actions that violate your data protection policies, across the entire IT environment. EventTracker collects, consolidates, reports and alerts on all events that occur in your IT infrastructure. Discover and investigate irregular system or data access events and other potential security incidents. EventTracker collects audit data from multiple independent sources, not just logs, and transforms that raw data into meaningful and actionable intelligence. Use preconfigured alerts to respond quickly to threat patterns that violate your corporate security policies and indicate possible cyber security incidents, including breaches of CJI or personally identifiable information. Alerts are available across multiple audited systems. Customize the predefined alerts or create entirely new ones to better address specific threats relevant to your environment and mitigate the corresponding risks.

CJIS Security Section	Control Description	NIST 800-53	EventTracker Capability
5.3.2.2 Collection of Evidence	Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).	IR-4, IR-4(1), IR-4(3), IR-4(4), IR-8	Review user access to sensitive content and data, critical system configuration changes, and other irregular or otherwise suspicious user behavior. EventTracker ensures secure collection, consolidation and long-term storage of a complete audit trail. Readily access the archived audit data at any time for security assessments, investigations and compliance processes.
5.3.4 Incident Monitoring	The agency shall track and document security incidents on an ongoing basis. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.	IR-5	Promptly detect and respond to threats to the confidentiality, integrity and availability of your sensitive data by subscribing relevant employees to reports and alerts on system configuration changes, data access events, and user behavior pattern changes across multiple IT systems and applications. Streamline investigation of incidents with full contextual information. EventTracker ensures that a complete audit trail is preserved safely for many years
5.4 Auditing and Accountability	Agencies shall implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior.		

CJIS Security Section	Control Description	NIST 800-53	EventTracker Capability
5.4.1 Auditable Events and Content (Information Systems)	The agency's information system shall generate audit records for defined events. The agency's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.	AC-9, AU-2, AU-2(3), AU-3, AU-3(1), AU-6, AU-6(1), AU-6(3), AU-12, CA-7	Use EventTracker to gain enterprise-wide visibility into what happens in your IT environment. EventTracker helps you identify measure and minimize risks to your highly sensitive data. Detect any user actions that violate your data protection policies, spot changes in user behavior patterns indicative of malicious intent and establish user accountability. EventTracker provides extensive reporting and audit search capabilities. Use overview dashboards to see what is happening in your IT infrastructure on a high level, including how often changes are made, which systems are most affected, and whether there are unusual spikes in the number of modifications and file and folder access attempts. Demonstrate the effectiveness of your data protection controls and your ability to investigate incidents with a complete, consolidated audit trail. EventTracker provides storage system that ensures reliable and cost-effective long-term storage of your audit trail.

CJIS Security Section	Control Description	NIST 800-53	EventTracker Capability
5.4.1.1 Events	The following events shall be logged: 1. Successful and unsuccessful system log-on attempts. 2. Successful and unsuccessful attempts to use: a. Access permission on a user account, file, directory or other system resource; b. Create permission on a user account, file, directory or other system resource; c. Write permission on a user account, file, directory or other system resource; d. Delete permission on a user account, file, directory or other system resource; e. Change permission on a user account, file, directory or other system resource. 3. Successful and unsuccessful attempts to change account passwords. 4. Successful and unsuccessful actions by privileged accounts. 5. Successful and unsuccessful attempts for users to: a. Access the audit log file; b. Modify the audit log file; c. Destroy the audit log file	AC-9, AU-2, AU-12, CA-7	Gain complete visibility into everything happening across the core systems in your environment. EventTracker delivers easy-to-read, noise filtered information that enables you to understand the context in which security incidents or operational problems occurred. EventTracker's core technology ensures you can track down all events listed in CJIS Security Policy area 5.4.1.1.

CJIS Security Section	Control Description	NIST 800-53	EventTracker Capability
5.4.1.1.1 Content	The following content shall be included with every audited event: 1. Date and time of the event. 2. The component of the information system (e.g., software component, hardware component) where the event occurred. 3. Type of event. 4. User/subject identity. 5. Outcome (success or failure) of the event.	AU-12	Overcome the problem of fragmented visibility by quickly gaining relevant knowledge about system configuration changes, system and data access, and events that indicate threats to sensitive data. EventTracker reports provide meaningful details about user activity, including who, what, when and where details for each change or access event, along with the before and after values.
5.4.2 Response to Audit Processing Failures	The agency's information system shall provide alerts to appropriate agency officials in the event of an audit processing failure. Audit processing failures include, for example: software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.	AU-5, AU-5(2)	Review the EventTracker system health log to identify any failures to configure audit policies or capture audit events, and any errors that occurred during processing.

CJIS Security Section	Control Description	NIST 800-53	EventTracker Capability
5.4.3 Audit Monitoring, Analysis, and Reporting	The responsible management official shall designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions. Audit review/analysis shall be conducted at a minimum once a week. The frequency of review/analysis should be increased when the volume of an agency's processing indicates an elevated need for audit review.	AU-6, AU-6(1), AU-6(3), AU-7, CA-7	Once you have met this requirement, improve the efficiency of the designated person by providing that person with the ability to quickly detect, investigate and report anomalous insider behavior and irregular access to key IT systems and data with EventTracker.
5.4.6 Audit Record Retention	The agency shall retain audit records for at least one (1) year. Once the minimum retention time period has passed, the agency shall continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes.	AU-4, AU-5(1), AU-9(2), AU-11	Demonstrate the effectiveness of your data protection controls and your ability to investigate incidents with a complete, consolidated audit trail. EventTracker provides storage system that ensures reliable and cost-effective long-term storage of your audit trail. Easily access the archived audit data at any time for security assessments, investigations and compliance processes.

CJIS Security Section	Control Description	NIST 800-53	EventTracker Capability
5.5.1 Account Management	The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The agency shall validate information system accounts at least annually and shall document the validation process. Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The agency shall identify authorized users of the information system and specify access rights/privileges. The agency responsible for account creation shall be notified when: 1. A user's information system usage or need-to know or need-to-share changes. 2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.	AC-2, AC-5, IR8	Use EventTracker reports to see enabled, disabled, expired and locked user accounts. Check each user's status against HR employee listings and coordinate with your HR department if you find any discrepancies. Periodically verify the appropriateness of user access rights by reviewing each user's assigned permissions to files and folders against HR employee listings and employee job descriptions using the Account Permissions report. Review reports that show current and past group membership; object permissions granted to user accounts; excessive access permissions; and permission inheritance breaks. Easily stay abreast of changes that could result in inappropriate permissions escalation by subscribing to appropriate reports.

CJIS Security Section	Control Description	NIST 800-53	EventTracker Capability
5.5.2.1 Least Privilege	The agency shall approve individual access privileges and shall enforce physical and logical access restrictions associated with changes to the information system; and generate, retain, and review records reflecting all such changes. Logs of access privilege changes shall be maintained for a minimum of one year or at least equal to the agency's record retention policy – whichever is greater.	AC-2, AC-2(4), AC-2(7), AC-5, AC-6, AC-6(5), AC-6(9), AC-10, RA-5(5)	Validate that your access controls are working properly in accordance with a least-privilege model and based on segregation of duties by periodically reviewing EventTracker reports that show the current state of user and object permissions, and the status of users. Control privilege delegation and access rights elevation by subscribing to daily or weekly reports showing changes to user accounts, permissions and group membership. Easily access the archived audit data at any time for security assessments, investigations and compliance processes.

CJIS Security Section	Control Description	NIST 800-53	EventTracker Capability
5.5.2.2 System Access Control	Access controls shall be in place and operational for all IT systems to ensure that only authorized personnel can add, change, or remove component devices, dial-up connections, and remove or alter programs.	AC-2, AC-2(4), AC-2(7), AC-5, AC-6, AC-6(5), AC-6(9), AC-10, RA-5(5)	Monitor access to IT systems by regularly reviewing reports that detail successful and failed system logon attempts. Closely control access by monitoring changes to Group Policy objects (GPOs) that could affect password policy and auditing all password activities across all information systems. Control privilege escalation by subscribing to daily or weekly reports showing changes to user permissions and group membership. Validate that your access controls are working properly by comparing lists of enabled user accounts with the current or historical state of permissions. Verify that no excessive access rights are assigned to employees beyond those needed for their primary job responsibilities by reviewing the Excessive Access Permissions report. Periodically review reports that provide details on all installations and removals of software applications and hardware devices, and well as reports showing the creation of potentially harmful files.

CJIS Security Section	Control Description	NIST 800-53	EventTracker Capability
5.5.2.4 Access Control Mechanisms	When setting up access controls, agencies shall use one or more of the following mechanisms: 1. Access Control Lists (ACLs). ACLs are a register of users (including groups, machines, processes) who have been given permission to use a particular object (system resource) and the types of access they have been permitted.	AC-2, AC-2(4), AC-2(7), AC-5, AC-6, AC-6(5), AC-6(9), AC-10, RA-5(5)	Review the state of accounts and permissions at present or at any particular moment in the past using EventTracker's historical reporting capability.
5.5.3 Unsuccessful Login Attempts	Where technically feasible, the system shall enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI). The system shall automatically lock the account/node for a 10 Minute time period unless released by an administrator	AC-7, IA-5(1)	Once you have met this requirement, gain visibility into failed login attempts by subscribing to EventTracker reports that deliver details about successful and failed system logon attempts, enabling prompt response. Review appropriate reports to validate that there are no multiple login instances.
5.6.1 Identification Policy and Procedures	Agencies shall ensure that all user IDs belong to currently authorized users. Identification data shall be kept current by adding new users and disabling and/or deleting former users.	IA-1, IA-2, IA-2(5)	Regularly view enabled, disabled, expired and locked user accounts by subscribing to predefined reports. Check each user's status against HR employee listings and coordinate with your HR department if you find any discrepancies. Minimize account sprawl and reduce the risk of account misuse by reviewing deactivating or deleting inactive user accounts.

References: https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center/view