Netsurion®

Powering Secure and Agile Networks

NIST CSF Compliance Guide

How Netsurion® Can Help You Achieve and Maintain Compliance

Summary of NIST Cybersecurity Framework (CSF)

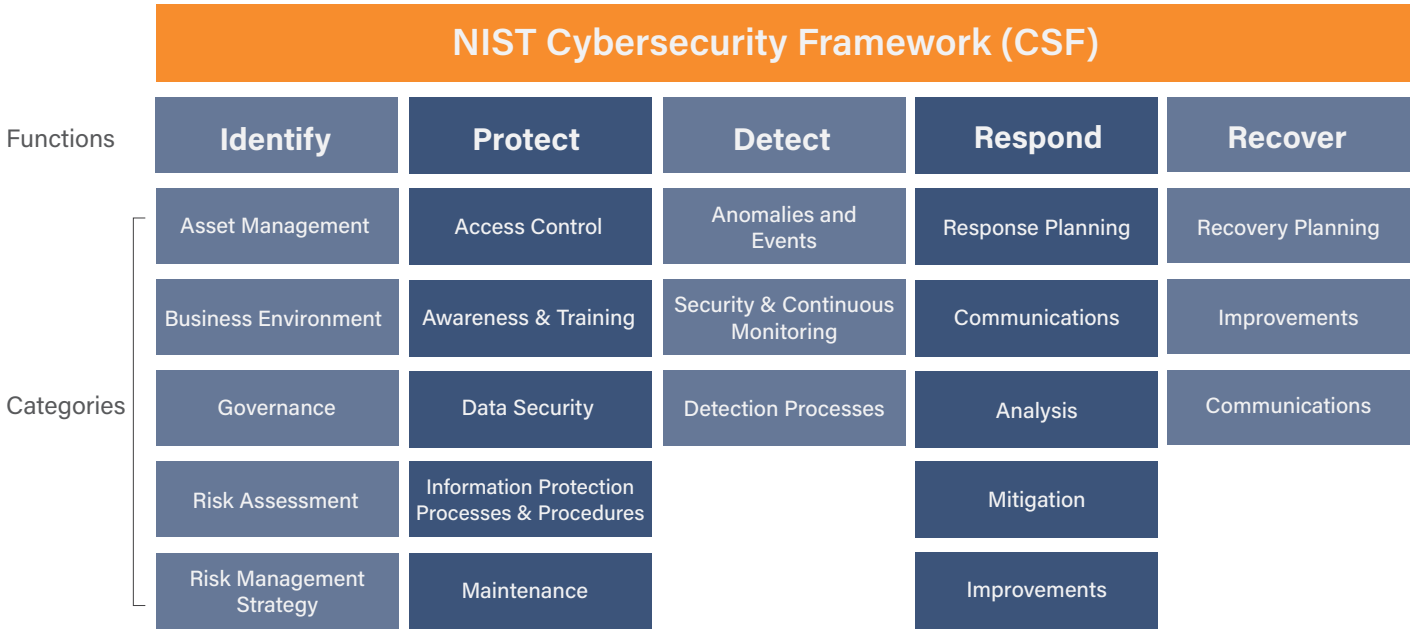
The National Institute of Standards and Technology's Cybersecurity Framework (CSF) was published in February 2014 in response to Presidential Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," which called for a standardized security framework for critical infrastructure in the United States.

The NIST CSF is recognized by many as a resource to help improve the security operations and governance for public and private organizations. While the NIST CSF is a useful guideline for transforming the organizational security posture and risk management from a reactive to proactive approach, it can be time-consuming to implement it.

These published guidelines cover many areas surrounding "access control", "audit and accountability", "incident response", and "system and information integrity". Each agency is responsible for implementing the minimum- security requirements as outlined by NIST. Agencies are periodically scored to determine their compliance level. Although compliance is currently voluntary, the government is likely to pursue passing law to enforce legal ramifications for noncompliance.

If you are new to the NIST Cybersecurity Framework, a quick overview and summary of the framework can help you accelerate your security transformation.

Here is an overview of the NIST Cybersecurity Framework:



Maximize NIST CSF Readiness

EventTracker SIEM improves security, maintains compliance and increases operational efficiency. EventTracker can be deployed on-premises for customers who prefer their equipment to reside in their data center. EventTracker is a software-based SIEM and log management solution that resides in a Windows Server environment. It may also be deployed in a virtual environment using VMware. In both cases, on-premises installation implies that the EventTracker software resides at the customer's location in some form or fashion.

For some customers, the space requirements, staffing issues, or lack of technical expertise make a cloud-hosted solution more attractive, and deployed in a Tier 1 EventTracker data center. Netsurion capabilities include the following:

- Secure Virtual Private Cloud (single tenant) environment
- Server disk space
- Installation
- Server diskspace
- Platform management
- Anti-virus installation and updates
- Windows updates
- Back-up/restore

Netsurion enables your organization to be aware of potential security risks and internal/external threats that can be identified and eliminated before they are exploited. It provides your organization with the ability to respond to a security incident and have the necessary data and tools for forensic analysis. The total time required to investigate and mitigate a security incident can be reduced by up to 75 percent, minimizing the potential exposure and costs.

Our experienced staff assumes responsibility for all SIEM related tasks including daily incident reviews, daily/weekly log reviews, configuration assessments, incident investigation support and audit support. We augment your IT team, allowing you to focus on the unique requirements of your organization, while actively leveraging our expertise.

Strong Access Control Policy and Procedures

Netsurion enables automatic, unattended consolidation of billions of events in a secure environment that is incrementally scalable to meet the needs of any size of organization. It also supports an infinite number of collection points, with each collection point able to process over 100,000 events per second. All this data is identified by the product-centric Knowledge Base, which contains detailed information on over 20,000 types of events, and automatically determines which logs are alerts, which are incidents, and which can be ignored.

Log collection includes a flexible, agent-optional architecture providing managed real-time and batch aggregation of all system, event and audit logs. EventTracker SIEM supports UDP and TCP (guaranteed delivery) log transport and is FIPS 140-2 compliant for transmission of events from agent/collection point to console.

Netsurion complies with Open Web Application Security Project (OWASP) guidelines which enforce strong authentication and authorization mechanisms in order to restrict user access. It incorporates default deny policy bringing more security to customers. It monitors changes on the file system and in the system registry of a Windows system and substantially improves corporate security and availability.

It provides customizable, role-based dashboards that allow organizations to control the information visible to a user based on their role in the organization. It also allows users to remove the information they do not want to see, and rearrange the location of the information on the dashboard. For example, a system administrator may only have access to the information on the ten servers they are responsible for maintaining, while the director of security will see the relevant information concerning the entire infrastructure.

EventTracker comprehensively monitors administrators and user's activities for all critical file and folder access on all servers. It monitors successful and failed logon attempts to all servers either locally or remotely. Each EventTracker user has specific user credentials and permissions. With the authentication and authorization mechanism implemented by the EventTracker platform, access privileges are controlled.

Ease of Deployment and Scalability

EventTracker is a comprehensive managed threat protection platform that offers several deployment options to meet the needs of small organizations with a few dozen critical systems, as well as larger organizations with thousands of systems spread across multiple locations.

Available as an option with EventTracker's built-in Behavior Analysis enables you to quickly detect and address changes in system and user behaviors. Automatic baseline learning, or flexible rules definitions, determine your thresholds for alerting on anomalies in your infrastructure. Real-time processing and correlation give you the complete picture of what's new and different that may signify something suspicious or an emerging cybersecurity threat.

Ease of FISMA Reporting and Alerting

The EventTracker platform produces specific reports, rules and dashboards to help meet the security controls detailed within FISMA-NIST. These reports, rules and dashboards can be easily and intuitively customized for specific environments.

Real-time Monitoring, Account, and Configuration Management

The file system and registry of every Windows system is ever-changing. This change may be voluntary or involuntary and happens quickly and often without the user's knowledge. Under the current Windows OS architecture there is no easy way for the user to understand change, identify change, and recover from change.

Change Management is a concept by which all system changes are intelligently tracked and reported on demand for the user to analyze, understand, and if needed, recover from change. The EventTracker platform monitors unauthorized software install / uninstall on all servers. It monitors all the sensors and configuration changes on critical file and database servers. Also enforces system and application policies on critical servers using Change Audit and periodically compare policy. It monitors all security patches and updates to servers.

EventTracker SIEM Change Audit is fully integrated into the EventTracker platform. EventTracker SIEM stores all the change audit data as both system snapshots for later comparisons and as events in EventVault. Change events can have rules written against them to trigger alerts or any other action available in EventTracker SIEM.

Protect Data and Information

As security with its first and foremost priority, EventTracker comprehensively monitors network connections on servers and firewall activity. It also monitors for changes or unauthorized access to routers and switches.

EventTracker SIEM is capabilities-rich, with key features that expand its competences beyond SIEM and log management. These include File Integrity Monitoring, Change Audit, Config Assessment, Cloud Integration, Event Correlation, and writeable media monitoring.

We safeguards data by ensuring stringent rules against unknown authentication and authorization. EventTracker monitors access to file and database servers. Also, it monitors configuration changes on critical file and database servers and alerts the responsible party to take further action. EventTracker SIEM also has an optimized, high performance event warehouse that is designed for efficient storage and retrieval of event logs. It reliably and efficiently archives event logs from across the SIEM without the need for any DBMS licenses or other overhead costs. And these logs are compressed and sealed with a SHA-1 signature to prevent potential tampering.

Statement of Compliance – NIST CSF

Identify (ID)

NIST CSF Requirement	Netsurion Capability
Asset Management (AM): The personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy. **ID.AM-1:** Physical devices and systems within the organization are inventoried. **ID.AM-2:** Software platforms and applications within the organization are inventoried. **ID.AM-3:** The organizational communication and data flow is mapped. **ID.AM-4:** External information systems are mapped and catalogued. **ID.AM-5:** Resources are prioritized based on the classification / criticality / business value of hardware, devices, data, and software. **ID.AM-6:** Workforce roles and responsibilities for business functions, including cybersecurity, are established.	EventTracker provides support for NIST-CSF control requirements ID.AM-3, ID.AM-4 and ID.AM-6 by collecting and analyzing all account management, access granting/revoking, and access/authentication logs. EventTracker's correlation rules provide alerting on account authentication failures. EventTracker investigations, reports, and details provide evidence of system account management activity (account creation, deletion, and modification), access granting/revoking activity, and account access/authentication activity. Lastly, EventTracker investigations provide evidence of authorized/unauthorized network access.
Governance (GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk. **ID.GV-1:** Organizational information security policy is established. **ID.GV-2:** Information security roles & responsibility are coordinated and aligned. ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed. **ID.GV-4:** Governance and risk management processes address cybersecurity risks.	EventTracker provides support for NIST-CSF control requirement ID.GV-1, ID.GV-2, and ID.GV-3 by collecting and analyzing all account management and access/authentication logs. EventTracker correlation rules provide alerting on account authentication failures. EventTracker investigations, reports, and details provide evidence of account management activity (account creation, deletion, and modification) and account access/authentication activity to support efforts of enforcing security policies within the organization.

Risk Assessment (RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. **ID.RA-1:** Asset vulnerabilities are identified and documented. **ID.RA-2:** Threat and vulnerability information is received from information sharing forums and sources. **ID.RA-3:** Threats to organizational assets are identified and documented. **ID.RA-4:** Potential impacts are analyzed. **ID.RA-5:** Risk responses are identified.	EventTracker provides support for NIST-CSF control requirements ID.RA-1 by collecting and analyzing all suspicious network activity or activities indicative of cybersecurity risks. EventTracker's correlation rules provide alerting on events indicative of potential cybersecurity threats or attacks on the network. EventTracker investigations, reports, and details provide evidence of cybersecurity events in support of early detection and incident response.

Protect (PR)

NIST CSF Requirement	Netsurion Capability
Access Control (AC): Access to information resources and associated facilities are limited to authorized users, processes or devices (including other information systems), and to authorized activities and transactions. **PR.AC-1:** Identities and credentials are managed for authorized devices and users. **PR.AC-2:** Physical access to resources is managed and secured. **PR.AC-3:** Remote access is managed. **PR.AC-4:** Access permissions are managed. **PR.AC-5:** Network integrity is protected.	EventTracker provides support for NIST-CSF control requirements PR.AC-1, PR.AC-2, PR.AC-3, PR.AC-4, PR.AC-5 by collecting and analyzing all account management, network access/authentication logs, remote and physical access. EventTracker's correlation rules provide alerting on account authentication failures. EventTracker investigations, reports, and details provide evidence of account access/authentication activity.
Awareness and Training (AT): The organization's personnel and partners are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements. **PR.AT-1:** General users are informed and trained **PR.AT-2:** Privileged users understand roles & responsibilities. **PR.AT-3:** Third-party stakeholders (suppliers, customers, partners) understand roles & responsibilities. **PR.AT-4:** Senior executives understand roles & responsibilities. **PR.AT-5:** Physical and information security personnel understand roles & responsibilities.	EventTracker provides support for NIST-CSF control requirement PR.AT-3 by collecting and analyzing all third-party accounts or process activities within the environment to ensure third-parties are performing activities according to defined roles and responsibilities. EventTracker correlation rules provide alerting on account authentication failures. EventTracker investigations, reports, and details provide evidence of vendor account management and authentication (success/failures) activities.

NIST CSF Requirement	Netsurion Capability
Data Security (DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. **PR.DS-1:** Data-at-rest is protected. **PR.DS-2:** Data-in-motion is secured. **PR.DS-3:** Assets are formally managed throughout removal, transfers, and disposition. **PR.DS-4:** Adequate capacity to ensure availability is maintained. **PR.DS-5:** There is protection against data leaks. **PR.DS-6:** Intellectual property is protected. **PR.DS-7:** Unnecessary assets are eliminated. **PR.DS-8:** Separate testing environments are used in system development. **PR.DS-9:** Privacy of individuals and personally identifiable information (PII) is protected.	EventTracker provides support for NIST-CSF control requirements PR.DS-1 and support for NIST-CSF control requirements PR.DS-4, PR.DS-5, PR.DS-6 by collecting and analyzing all system logs relating to the protection of data integrity, availability, and mobility. EventTracker's File Integrity Monitoring (FIM) tracks file changes, while EventTracker independently monitors and logs the connection and disconnection of external data devices to the host computer where the sensor is running. EventTracker also monitors and logs the transmission of files to an external storage device. EventTracker can be configured to protect against external data device connections by ejecting specified devices upon detection. External USB drive storage devices include Flash/RAM drives and CD/DVD drives. EventTracker correlation rules provide alerting on remote account authentication failures. EventTracker investigations, reports, and details provide evidence of remote account access/authentication activity.
Information Protection Processes and Procedures (IP): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. Security policy (that addresses purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets. **PR.IP-1:** A baseline configuration of information technology/operational technology systems is created. **PR.IP-2:** A System Development Life Cycle to manage systems is implemented. **PR.IP-3:** Configuration change control processes are in place. **PR.IP-4:** Backups of information are managed. **PR.IP-5:** Policy and regulations regarding the physical operating environment for organizational assets are met. **PR.IP-6:** Information is destroyed according to policy and requirements.	EventTracker provides support for NIST-CSF control requirements PR.IP-1, PR.IP-3, PR.IP-4, PR.IP-7, PR.IP-8, PR.IP-11, PR.IP-12 by collecting and analyzing all logs relating to change management, backups, and those in support of incident response plans. EventTracker correlation rules provide alerting on account management activities. EventTracker investigations, reports, and details provide evidence of account management and authentication (success/failures) activities.

NIST CSF Requirement	Netsurion Capability
PR.IP-7: Protection processes are continuously improved. **PR.IP-8:** Information sharing occurs with appropriate parties. **PR.IP-9:** Response plans (Business Continuity Plan(s), Disaster Recovery Plan(s), Incident Handling Plan(s)) are in place and managed. **PR.IP-10:** Response plans are exercised. **PR.IP-11:** Cybersecurity is included in human resources practices (de-provisioning, personnel screening, etc.).	
Maintenance (MA): Maintenance and repairs of operational and information system components is performed consistent with policies and procedures. **PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools. **PR.MA-2:** Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access and supports availability requirements for important operational and information systems.	EventTracker provides support for NIST-CSF control requirement PR.MA-1 and PR.MA-2 by collecting and analyzing all logs relating to critical and error conditions within the environment. EventTracker correlation rules provide alerting on critical and error conditions within the environment. EventTracker investigations, reports and details provide evidence of environment conditions as well as process and system start-ups/shut-downs.
Protective Technology (PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. **PR.PT-1:** Audit and log records are stored in accordance with audit policy. **PR.PT-2:** Removable media are protected according to a specified policy. **PR.PT-3:** Access to systems and assets is appropriately controlled. **PR.PT-4:** Communications networks are secured **PR.PT-5:** Specialized systems are protected according to the risk analysis (SCADA, ICS, DLS).	EventTracker provides support for NIST-CSF control requirement PR.PT-1, PR.PT-2, PR.PT-3, PR.PT-4 by collecting logs relating to technical security solution access management and authentication activities. Further, with the use of EventTracker's FIM allows for monitoring of removable media and other audit logging events. EventTracker correlation rules provide alerting on audit logging events (log cleared), FIM, software installations, access provisioning and authentication activities. Lastly, EventTracker investigations, reports and details provide evidence around the mentioned activities.

Detect (DE)

NIST CSF Requirement	Netsurion Capability
Anomalies and Events (AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood. **DE.AE-1:** A baseline of normal operations and procedures is identified and managed. **DE.AE-2:** Detected events are analyzed to understand attack targets and methods. **DE.AE-3:** Cybersecurity data are correlated from diverse information sources. **DE.AE-4:** Impact of potential cybersecurity events is determined. **DE.AE-5:** Incident alert thresholds are created.	EventTracker provides support of NIST-CSF control requirements DE.AE-3 and DE.AE-5, while providing support for NIST-CSF control requirement DE.AE-1, DE.AE-2, DE.AE-4 by collecting and analyzing logs related to security events throughout the network. An inherent function to EventTracker is the ability to correlate and aggregate event data across the environment. EventTracker's log analysis, investigations, details and reporting capabilities can be leveraged during a security assessment to help ensure implemented controls are functioning as intended and to potentially identify any weaknesses.
Security Continuous Monitoring (CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures. **DE.CM-1:** The network is monitored to detect potential cybersecurity events. **DE.CM-2:** The physical environment is monitored to detect potential cybersecurity events. **DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events. **DE.CM-4:** Malicious code is detected. **DE.CM-5:** Unauthorized mobile code is detected **DE.CM-6:** External service providers are monitored. **DE.CM-7:** Unauthorized resources are monitored. **DE.CM-8:** Vulnerability assessments are performed.	EventTracker provides support of NIST-CSF control requirements DE.CM-1, DE.CM-2, DE.CM-3, DE.CM 4, DE.CM-6, and DE.CM-7 by providing continuous monitoring, analysis, and reporting of network, physical access, and other events indicative of malicious cyber activities.
Detection Processes (DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events. **DE.DP-1**: Roles and responsibilities for detection are well defined to ensure accountability. **DE.DP-2:** Detection activities comply with all applicable requirements, including those related to privacy and civil liberties. **DE.DP-3:** Detection processes are exercised to ensure readiness. **DE.DP-4:** Event detection information is communicated to appropriate parties. **DE.DP-5:** Detection processes are continuously improved.	EventTracker provides support of NIST-CSF control requirement DE.DP-4 and support of NIST-CSF control requirement DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-5 by logging and monitoring around process and procedures in the environment. Further, EventTracker's correlation engine provides alerting on activities to assigned individuals. EventTracker reporting, investigations, and details provide evidence around these activities as well to support maintenance of processes and procedures.

Respond (RS)

NIST CSF Requirement	Netsurion Capability
Response Planning (RP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events. **RS.RP-1:** Response plan is implemented during or after an event.	EventTracker provides support for NIST-CSF control requirement RS.RP-1 by collecting and analyzing all cybersecurity events and providing notifications to assigned personnel. EventTracker correlation rules provide alerting on cybersecurity events while investigations, reports, and details provide evidence behind cybersecurity events.
Communications (CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from federal, state, and local law enforcement agencies. **RS.CO-1:** Personnel know their roles and order of operations when a response is needed. **RS.CO-2:** Events are reported consistent with established criteria. **RS.CO-3:** Detection/response information, such as breach reporting requirements, is shared consistent with response plans, including those related to privacy and civil liberties. **RS.CO-4:** Coordination with stakeholders occurs consistent with response plans, including those related to privacy and civil liberties. **RS.CO-5:** Voluntary coordination occurs with external stakeholders (ex, business partners, information sharing and analysis centers, customers)	EventTracker provides support for NIST-CSF control requirement RS.CO-3 and RS.CO-4 by collecting and analyzing all cybersecurity events and providing notifications to assigned personnel. EventTracker correlation rules provide alerting on cybersecurity events while investigations, reports, and details provide evidence behind cybersecurity events.
Analysis (AN): Analysis is conducted to ensure adequate response and support recovery activities. **RS.AN-1:** Notifications from the detection system are investigated. **RS.AN-2:** Understand the impact of the incident **RS.AN-3:** Forensics are performed. **RS.AN-4:** Incidents are classified consistent with response plans.	EventTracker provides support for NIST-CSF control requirements RS.AN-1, RS.AN-2, RS.AN-3 and RS.AN-4 by collecting and analyzing logs to categorize events and allow for forensics to be performed. EventTracker's correlation engine provides alerts and notifications to assigned personnel. EventTracker investigations, reports, and details provide evidence of security and other events of interest throughout the environment.
Mitigation (MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident. **RS.MI-1:** Incidents are contained. **RS.MI-2:** Incidents are eradicated. **RS.MI-3:** Newly identified vulnerabilities are mitigated or documented as accepted risks.	EventTracker provides support for NIST-CSF control requirements RS.MI-1, RS.MI-2, RS.MI-3 by collecting and analyzing logs related to incident response. EventTracker correlation engine provides alerting on vulnerabilities within the environment. EventTracker investigations, reports, and details provide evidence to support incident analysis and remediation of exposure or vulnerabilities.

Improvements (IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/ response activities. **RS.IM-1:** Response plans incorporate lessons learned. **RS.IM-2:** Response strategies are updated.	EventTracker provides support for NIST-CSF control requirements RS.IM-1, RS.IM-2 by collecting and analyzing logs related to incident response. EventTracker reports provide evidence to support incident analysis and remediation of exposure or vulnerabilities.

Recover (RC)

NIST CSF Requirement	Netsurion Capability
Improvements (IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/ response activities. **RS.IM-1:** Response plans incorporate lessons learned. **RS.IM-2:** Response strategies are updated.	EventTracker provides support for NIST-CSF control requirements RS.IM-1, RS.IM-2 by collecting and analyzing logs related to incident response. EventTracker reports provide evidence to support incident analysis and remediation of exposure or vulnerabilities.
Communications (CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors. **RC.CO-1:** Public Relations are managed. **RC.CO-2:** Reputation after an event is repaired.	EventTracker provides supplemental support of NIST-CSF control requirement RC.CO-1 and RC.CO-2 by collecting and analyzing logs relating to recovery operations. EventTracker reports provide evidence around the recovery operation events.

Reference:

https://www.nist.gov/cyberframework

How Netsurion Can Help

Not sure where to begin? Netsurion helps you reduce cyber risk, augment your IT team's skills, and spend less time on documentation and compliance readiness. Contact us and our experts can advise you on the path to achieve NIST CSF preparedness.

About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's managed platform approach of combining purpose-built technology and a team of cybersecurity experts gives customers and partners the ultimate flexibility to adapt and grow while maintaining a secure environment.

Netsurion's EventTracker cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service. Netsurion's BranchSDO delivers purpose-built technology with optional levels of managed services to multilocation businesses that optimize network security, agility, resilience, and compliance for branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit netsurion.com or follow us on Twitter or LinkedIn.