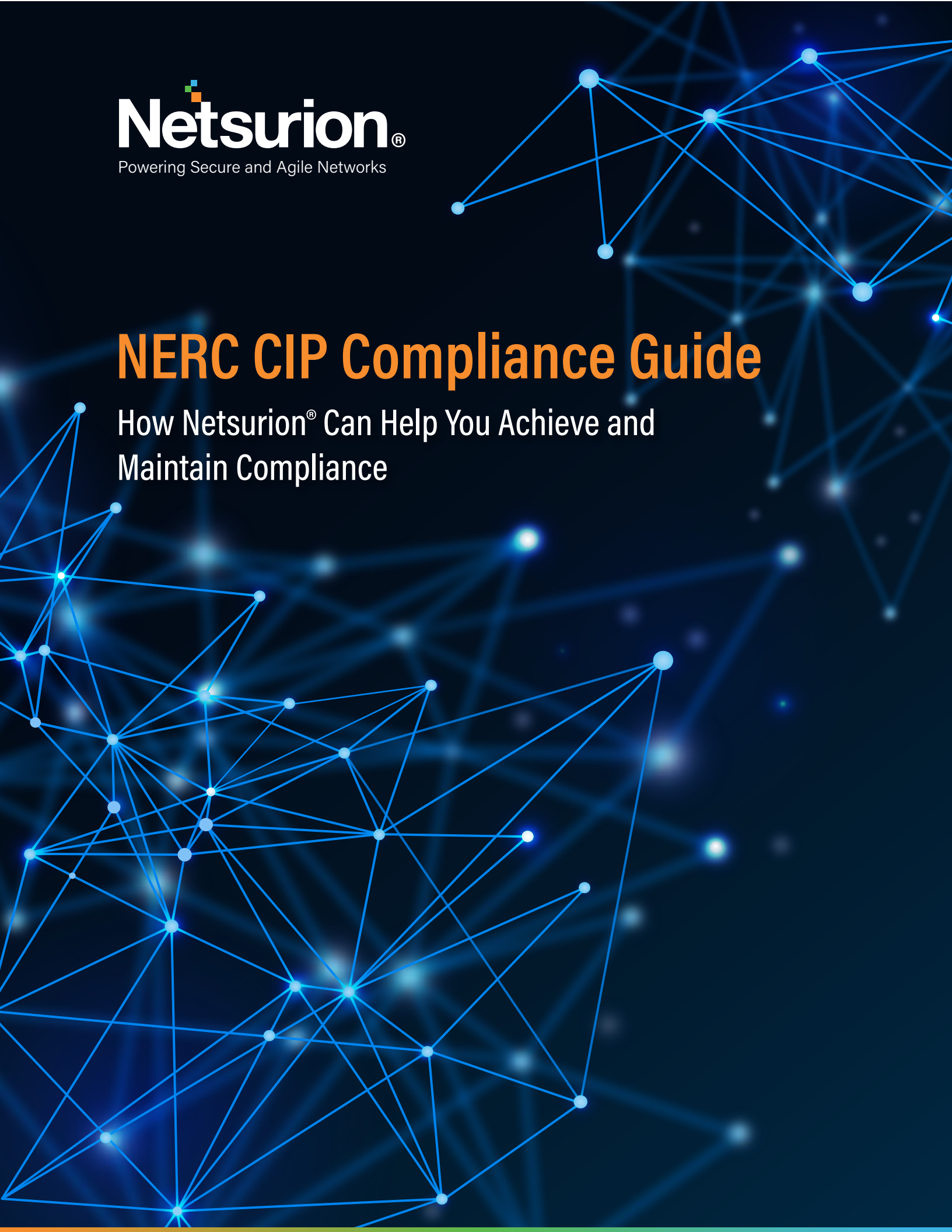
Netsurion®

Powering Secure and Agile Networks

NERC CIP Compliance Guide

How Netsurion® Can Help You Achieve and Maintain Compliance



Overview of NERC CIP

The North American Electric Reliability Corporation (NERC) was formed to assist in maintaining and improving the reliability of the bulk power system. NERC also offers a number of additional programs and resources to support owners, operators and users of the electric grid system, in their attempts to continue operating efficiently.

After several attempts and attacks, there are concerns that the severity and frequency of critical incidents directed against the infrastructure will increase in the future.

The organization also has been granted legal authority to enforce legal standards, and certify operators involved in the program known as Critical Infrastructure Program (CIP).

Since the introduction of mandatory electric reliability standards, the North American Electric Reliability Corporation (NERC) has worked to identify the best means of ensuring protection of critical infrastructure and, particularly, critical cyber assets. Practical considerations – such as lack of information, technical feasibility, and/or prohibitive cost – as well as a reluctance to impose a "one-size-fits-all" approach to a wide variety of assets have driven an iterative process.

Avoid blind spots and cybersecurity gaps across your converged infrastructure that can increase risk. NERC CIP involves the focus of controls on risk management of high-impact infrastructure and crucial assets that are required for day-to-day resiliency and operations. One of the benefits of NERC CIP is simplifying compliance and reducing the time spent on documentation and audits.

Protective Monitoring

The policy is not reproduced here and public sector bodies should obtain it from the North American Electric Reliability Corporation. However, in summary the logging requirements regarding user access to your network and systems include recording the following events:

- Unauthorized application access (where applicable)
- File access attempts to protectively marked information (e.g. RESTRICTED data).
- Unsuccessful login / logout
- Successful login / logout
- Privileged system changes (e.g. account management, policy changes, device configuration)

Logs should be kept for at least 6 months. This may include the use of backup tapes but logs should be easily available for use as part of your incident response policy, as well as help with an investigation. In practice this may need a system which maintains logs readily recoverable from any archive.

Simplify NERC CIP Compliance

The EventTracker threat protection platform improves security, helps organizations demonstrate compliance, and increases operational efficiencies. EventTracker SIEM enables your organization to be more aware of potential security risks and internal/external threats. It provides you with the ability to respond to a security incident with comprehensive data and forensic tools for analysis. The time required to investigate and mitigate security incidents can be greatly reduced, minimizing potential exposure and costs.

Our expert staff can assume responsibility for some or all EventTracker SIEM-related tasks, including system management, incident reviews, daily/weekly log reviews, configuration assessments, and audit support. We augment your IT Security team, allowing you to focus on your priorities by leveraging our expertise, discipline and efficiency.

Maximize NERC CIP Readiness

Netsurion enables automatic consolidation of thousands or even millions of audit events to meet the needs of any size organization. The inbound log data is identified by EventTracker's built-in manufacturers Knowledge Base, which contains log definitions for thousands of types of log events, and automatically identifies which events are critical to security standard.

The EventTracker platform provides real-time and batch aggregation of all system, event and audit logs from your firewalls, IDS/IPS, network devices, Windows, Linux/Unix, VMware, Citrix, databases, MS Exchange web servers, EHRs, and more.

Ease of Deployment and Scalability

EventTracker is available on premises or as a highly scalable cloud-based SIEM and Log Management solution. It offers several deployment options to meet the needs of organizations with a few dozen systems or those with thousands of systems spread across multiple locations. EventTracker Cloud is available as an AMI on Amazon EC2, Microsoft Azure or your cloud infrastructure provider of choice. It supports multi-tenant implementations for MSSP organizations serving the needs of smaller customers.

NERC CIP Compliance Requirements

Control Description	Netsurion Capability
CIP-002-5 R1: BES Cyber System Categorization Each Responsible Entity shall implement a process that considers each of the following assets i. Control Centers and backup Control Centers; ii. Transmission stations and substations; iii. Generation resources; iv. Systems and facilities critical to system restoration v. Special Protection Systems that support the reliable operation of the Bulk Electric System vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above. **1.1** Identify each of the high-impact BES Cyber Systems. **1.2** Identify each of the medium-impact BES Cyber Systems. **1.3** Identify each asset that contains a low-impact BES Cyber System.	EventTracker Support the 002-5 control objectives by allowing the organization to leverage an entity-based structure to apply the categorization of BES Cyber Systems into High, Medium and Low impacts. All components of the NERC-CIP Compliance Automation Module then apply the entity structure for easy identification of logging activities by impact.
CIP-004-5.1 R4 Personnel & Training Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access management programs that collectively include each of the applicable requirement parts in CIP-004-5 Table R4 – Access Management Program. **4.1** Process to Authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: **4.1.1** Electronic access; **4.1.2** Unescorted physical access into a Physical Perimeter; and **4.1.3** Access to designated storage locations, whether physical or electronic, for BES Cyber System Information. **4.2** Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have Authorization records. **4.3** For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	EventTracker Support control 004-5 R4 by monitoring any access provisioning activities within the environment. Further, authentication or access activities to both physical and electronic access point are monitored. Privileged accounts or groups, both by default or defined by the organization, are also monitored for access provisioning, authentication and access activities due to their impact within the environment. EventTracker module content provides reports, alerts and investigations, enabling the organization's periodic access review process.

Control Description	Netsurion Capability
4.4 Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	
CIP-004-5.1 R5: Personnel & Training Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access revocation programs that collectively include each of the applicable requirement parts in CIP-004-5 Table R5 – Access Revocation. **5.1** A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights.) **5.2** For reassignments or transfers, revoke the individual's Authorized electronic access to individual accounts and Authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access. **5.3** For terminations actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action. **5.4** For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	EventTracker Support and addresses control objectives within 004-5 R5 by alerting and reporting on access de-provisioning due to reassignment, transfer or termination. This enables the organization to measure policy adherence for timely modification or removal of access.

Control Description	Netsurion Capability
5.5 For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer period, change the password(s) within 10 calendar days following the end of the operating circumstances.	
CIP-005-5 R1 Electronic Security Perimeter(s) Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. **1.1** All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP. **1.2** All External Routable Connectivity must be through an identified Electronic Access Point (EAP). **1.3** Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	EventTracker Support objectives within control 005-5 R1 through enhanced analytics and reporting at the Electronic Security Perimeter. Advanced correlation and alerting reduce the interval to detect and respond to vulnerabilities and attacks against the network. Further analysis of uncommon or suspicious network activities is facilitated through real-time analytics, compliance reports and forensic investigations.
CIP-005-5 R2: Electronic Security Perimeter(s) Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible: **2.1** Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset. **2.2** For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System. **2.3** Require multi-factor Authentication for all Interactive Remote Access sessions.	EventTracker Support objectives within control 005-5 R2 by alerting on potentially malicious activity through VPN tunnels, wireless access points and use of unencrypted network protocols. Reports and investigations allow for detailed review of activities related to points of network access.

Control Description	Netsurion Capability
CIP-006-5 R1 Physical Security of BES Cyber Systems Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented Physical plans that collectively include all of the applicable requirement parts in CIP-006-5 Table R1 – Physical Plan. **1.1** Define operational or procedural controls to restrict physical access. **1.2** Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Perimeter to only those individuals who have authorized unescorted physical access. **1.3** Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Perimeters to only those individuals who have Authorized unescorted physical access. **1.4** Monitor for unauthorized access through a physical access point into a Physical Perimeter. **1.5** Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection. **1.6** Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System. **1.7** Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection. **1.8** Log (through automated means or by personnel who control entry) entry of each individual with Authorized unescorted physical access into each Physical Perimeter, with information to identify the individual and date and time of entry. **1.9** Retain physical access logs of entry of individuals with Authorized unescorted physical access into each Physical Perimeter for at least ninety calendar days.	EventTracker supports most objectives within controls 006-5 R1 and 006-5 R2 by alerting and reporting on access success and failure activity at the Physical Security Perimeter. Reporting and investigations can also allow operations teams to inspect suspicious physical access activities. Depending on the processes employed by the organization to regulate visitor access, EventTracker can Support objectives within 006-5 R2. The above methods of alerting, reporting and investigations can also be used to automate physical access processes.

Control Description	Netsurion Capability
CIP-006-5 R2: Physical Security of BES Cyber Systems Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented visitor control programs that include each of the applicable requirement parts in CIP-006-5 Table R2 – Visitor Control Program. **2.1** Require continuous escorted access of visitors (individuals who are provided access but are not Authorized for unescorted physical access) within each Physical Perimeter, except during CIP Exceptional Circumstances. **2.2** Require manual or automated logging of visitor entry into and exit from the Physical Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances. **2.3** Retain visitor logs for at least ninety calendar days	EventTracker supports most objectives within controls 006-5 R1 and 006-5 R2 by alerting and reporting on access success and failure activity at the Physical Security Perimeter. Reporting and investigations can also allow operations teams to inspect suspicious physical access activities. Depending on the processes employed by the organization to regulate visitor access, EventTracker can Support objectives within 006-5 R2. The above methods of alerting, reporting and investigations can also be used to automate physical access processes.
CIP-007-5 R1: System Security Management Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 Table R5 – System Access Controls. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]. **5.2** Identify and inventory all known enabled default or other generic account types, either by system, by grouped of systems, by location, or by system type(s). **5.3** Identify individuals who have Authorized access to shared accounts. **5.4** Change known default passwords, per Cyber Asset capability. **5.5** For password-only Authentication for interactive user access, either technically or procedurally enforces the following password parameters. **5.5.1** Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset **5.5.2** Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	EventTracker Support the authentication-based objectives in controls 007 R5 and 007-5 R5. Lists can be used to monitor group various groups of accounts to monitor and report on activities, enabling processes that can be easily integrated with existing account access reviews. Password maintenance protocols can also be aligned between compliance and operational systems. EventTracker provides support of controls, which concern monitoring and reporting of malicious activity at various layers of the environment. Correlation and alerting help reduce the time to detect and mitigate these threats. Further monitoring of failed authentication and suspicious activity could provide early indicators of compromised accounts.

Control Description	Netsurion Capability
5.6 Where technically feasible, for password-only Authentication for interactive user access, technically or procedurally enforce either password changes or an obligation to change the password at least once every 15 calendar months. **5.7** Where technically feasible, either: ▪ Limit the number of unsuccessful Authentication attempts ▪ Generate alerts after a threshold of unsuccessful Authentication attempts	
CIP-007-5 R2: System Security Management Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 Table R2 – Security Patch Management. **2.1** A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists. **2.2** At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1 **2.3** For applicable patches identified in Part 2.2, within 35 calendar days of evaluation completion, take one of the following actions: ▪ Apply the applicable patches; or ▪ Create a dated mitigation plan; or ▪ Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations. **2.4** For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	EventTracker Support the authentication-based objectives in control 007-5 EventTracker Support objectives in control 007-5 R2 by providing reports and detailed investigations on patches and signature updates applied within the environment. These details support existing change and patch management controls. Correlation and alerting help reduce the time to detect and mitigate these threats.

Control Description	Netsurion Capability
CIP-007-5 R3: System Security Management Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 Table R3 – Malicious Code Prevention. **3.1** Deploy method(s) to deter, detect, or prevent malicious code. **3.2** Mitigate the threat of detected malicious code. **3.3** For those methods identified in Part 3.1 that use signatures or patterns, have a process for the updated of the signatures or patterns. The process must address testing and installing the signatures or patterns.	EventTracker Support the authentication-based objectives in controls 007 R5 and 007-5 R5. EventTracker Support objectives in control 007-5 R2 and 007-5 R3 by providing reports and detailed investigations on patches and signature updates applied within the environment. These details support existing change and patch management controls. EventTracker provides support of controls 007-5 R3 and 007-5 R4, which concern monitoring and reporting of malicious activity at various layers of the environment. Correlation and alerting help reduce the time to detect and mitigate these threats. Further monitoring of failed authentication and suspicious activity could provide early indicators of compromised accounts.
CIP-007-5 R4: System Security Management Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 Table R4 – Security Event Monitoring. **4.1** Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: **4.1.1** Detected successful login attempts; **4.1.2** Detected failed access attempts and failed login attempts; **4.1.3** Detected malicious code. **4.2** Generate alerts for security events that the Responsible Entity determines necessitates, an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): **4.2.1** Detected malicious code from Part 4.1; and **4.2.2** Detected failure of Part 4.1 event logging.	EventTracker Support the authentication-based objectives in controls 007 R5 and 007-5 R5. EventTracker Support objectives in control 007-5 R4 by providing reports and detailed investigations on patches and signature updates applied within the environment. These details support existing change and patch management controls. EventTracker provides support of controls 007-5 R3 and 007-5 R4, which concern monitoring and reporting of malicious activity at various layers of the environment. Correlation and alerting help reduce the time to detect and mitigate these threats. Further monitoring of failed authentication and suspicious activity could provide early indicators of compromised accounts.

Control Description	Netsurion Capability
4.3 Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances. **4.4** Review and summarization of sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	
CIP-007-5 R5: System Security Management Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 Table R5 – System Access Controls. **5.1** Have a method(s) to enforce Authentication of interactive user access, where technically feasible.	EventTracker Support the authentication-based objectives in controls 007 R5 and 007-5 R5. Lists can be used to monitor group various groups of accounts to monitor and report on activities, enabling processes that can be easily integrated with existing account access reviews. Password maintenance protocols can also be aligned between compliance and operational systems. EventTracker Support objectives in control 007-5 R2 and 007-5 R3 by providing reports and detailed investigations on patches and signature updates applied within the environment. These details support existing change and patch management controls. EventTracker provides support of controls 007-5 R3 and 007-5 R4, which concern monitoring and reporting of malicious activity at various layers of the environment. Correlation and alerting help reduce the time to detect and mitigate these threats. Further monitoring of failed authentication and suspicious activity could provide early indicators of compromised accounts.

Control Description	Netsurion Capability
CIP-008-5 R1: Incident Reporting & Response Planning Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications. **1.1** One or more processes to identify, classify, and respond to Cyber Security Incidents. **1.2** One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from the determination of a Reportable Cyber Security Incident. **1.3** The roles and responsibilities of Cyber Security Incident response groups or individuals. **1.4** Incident handling procedures for Cyber Security Incidents.	EventTracker Supports objectives within controls 008-5 R1, 008-5 R2 and 008-5 R3 to support Incident Response activities. As previously discussed, alerts and advanced correlation help identify potentially harmful activities within the environment. EventTracker's reporting and investigations around security events allows IT and Security Operations to gather forensic data to better understand and ultimately mitigate malicious activity. The scope of security events expands from monitoring network and remote connections at the Electronic Security Perimeter to suspicious activity and compromised internal accounts. By gathering forensic data and leveraging powerful correlation across the environment, EventTracker AI Engine rules, alerts, reports and investigations provide ample details for organizations to learn and adapt to ever changing threat landscape.
CIP-008-5 R2: Incident Reporting & Response Planning Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. **2.1** Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: ▪ By responding to an actual Reportable Cyber Security Incident; ▪ With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or ▪ dsd With an operational exercise of a Reportable Cyber Security Incident.	EventTracker Supports objectives within controls 008-5 R1, 008-5 R2 and 008-5 R3 to support Incident Response activities. As previously discussed, alerts and advanced correlation help identify potentially harmful activities within the environment. EventTracker' s reporting and investigations around security events allows IT and Security Operations to gather forensic data to better understand and ultimately mitigate malicious activity. The scope of security events expands from monitoring network and remote connections at the Electronic Security Perimeter to suspicious activity and compromised internal accounts.

Control Description	Netsurion Capability
2.2 Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise. **2.3** Retain records related to Reportable Cyber Security Incidents.	By gathering forensic data and leveraging powerful correlation across the environment, EventTracker AI Engine rules, alerts, reports and investigations provide ample details for organizations to learn and adapt to ever changing threat landscape.
CIP-008-5 R3: Incident Reporting & Response Planning Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication. **3.1** No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: **3.1.1** Document any lessons learned or document the absence of any lessons learned; **3.1.2** Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan. **3.1.3** Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned. **3.2** No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: **3.2.1** Update the Cyber Security Incident response plan(s) **3.2.2** Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	EventTracker Supports objectives within controls 008-5 R1, 008-5 R2 and 008-5 R3 to support Incident Response activities. As previously discussed, alerts and advanced correlation help identify potentially harmful activities within the environment. EventTracker' s reporting and investigations around security events allows IT and Security Operations to gather forensic data to better understand and ultimately mitigate malicious activity. The scope of security events expands from monitoring network and remote connections at the Electronic Security Perimeter to suspicious activity and compromised internal accounts. By gathering forensic data and leveraging powerful correlation across the environment, EventTracker AI Engine rules, alerts, reports and investigations provide ample details for organizations to learn and adapt to ever changing threat landscape.

Control Description	Netsurion Capability
CIP-009-5 R1: Recovery Plans for BES Cyber Systems Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable requirement parts in CIP-009-5 Table R1 – Recovery Plan Specifications. **1.1** Conditions for activation of the recovery plan(s). **1.2** Roles and responsibilities of responders. **1.3** One or more processes for the backup and storage of information required to recover BES Cyber System functionality. **1.4** One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures. **1.5** One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	EventTracker Support objectives within control 009-5 R1 with alerts that provide advanced notice when critical or error events occur. These backup failures, along with successful backup operations, are also captured in reports and detailed investigations.
CIP-010-1 R1: Configuration Change Management & Vulnerability Assessments Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-010-1 Table R1 – Configuration Change Management. **1.1** Develop a baseline configuration, individually or by group, which shall include the following items: **1.1.1** Operating system(s) (including version) or firmware where no independent operating system exists; **1.1.2** Any commercially available or open source application software (including version) intentionally installed; **1.1.3** Any custom software installed; **1.1.4** Any logical network accessible ports; and **1.1.5** Any security patches applied. **1.2** Authorize and document changes that deviate from the existing baseline configuration. **1.3** For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	EventTracker Support objectives within controls CIP-010-1 R1 and CIP-010-1 R2 by working with existing change control procedures to alert and report on various types of changes occurring across the environment. Alerts can be configured across all log sources to identify when configuration/policies are changed, signatures or patches are updated, and when software installation occurs. Reports and investigations, coupled with timely alerts of changes, provide additional details to ensure change control procedures are adhered to and any deviations from standard procedures are identified. Further, in order to support CIP-010-1 R3, EventTracker integrates with ETVAS vulnerability and other scanners to indicate when vulnerability is identified by the solution.

Control Description	Netsurion Capability
1.4 For a change that deviates from the existing baseline configuration: **1.4.1** Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; **1.4.2** Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected. **1.4.3** Document the results of the verification **1.5** Where technically feasible, for each change that deviates from the existing baseline configuration: **1.5.1** Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected **1.5.2** Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	
CIP-010-1 R2: Configuration Change Management & Vulnerability Assessments Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-010-1 Table R2 – Configuration Monitoring. **2.1** Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes, differences in operation between the test and production environments.	EventTracker Support objectives within controls CIP-010-1 R1 and CIP-010-1 R2 by working with existing change control procedures to alert and report on various types of changes occurring across the environment. Alerts can be configured across all log sources to identify when configuration/policies are changed, signatures or patched patches are updated, and when software installation occurs. Reports and investigations, coupled with timely alerts of changes, provide additional details to ensure change control procedures are adhered to and any deviations from standard procedures are identified. Further, in order to support CIP-010-1 R3, EventTracker integrates with ETVAS vulnerability and other scanners to indicate when vulnerability is identified by the solution.

Control Description	Netsurion Capability
CIP-010-1 R3: Configuration Change Management & Vulnerability Assessments Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-010-1 Table R3– Vulnerability Assessments. **3.1** At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	EventTracker Support objectives within controls CIP-010-1 R1 and CIP-010-1 R2 by working with existing change control procedures to alert and report on various types of changes occurring across the environment. Alerts can be configured across all log sources to identify when configuration/policies are changed, signatures or patched patches are updated, and when software installation occurs. Reports and investigations, coupled with timely alerts of changes, provide additional details to ensure change control procedures are adhered to and any deviations from standard procedures are identified. Further, in order to support CIP-010-1 R3, EventTracker integrates with ETVAS vulnerability and other scanners to indicate when vulnerability is identified by the solution.

Reference:

https://www.nerc.com/pa/Stand/Pages/Cyber-Security-Permanent.aspx

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 NERC CIP 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.