Hewlett Packard
Enterprise

HPE Security ArcSight Logger CIP for NERC

Software Version: 1.0

Solutions Guide

September 28, 2016

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

HPE Security ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Support

Contact Information

Phone	A list of phone numbers is available on the HPE Security ArcSight Technical Support Page: https://softwaresupport.hpe.com/documents/10180/14684/esp-support-contact-list
Support Web Site	https://softwaresupport.hpe.com
Protect 724 Community	https://www.protect724.hpe.com

Contents

Overview

The 2005 US Energy Policy Act (EPAct) legislated that an Electric Reliability Organization (ERO) be created to establish and enforce reliability standards for the bulk power system, due to the following factors:

- Potential vulnerabilities to a cyber attack on North American electric utility systems.
- Potential for computer systems play a role in power disturbances.
- Concern that a cyber attack or computer system failure could cause a wide spread power outage.
- Increased public awareness about the risks associated with the bulk power system.

In 2006, the Federal Energy Regulatory Commission approved the North American Electric Reliability Corporation (NERC) as the Electric Reliability Organization (ERO). The mission of NERC is to ensure the reliability of the bulk power system in North America.NERC defines a set of Critical Infrastructure Protection (CIP) standards to help ensure the protection of electric utility operations and cyber assets.

ArcSight Logger CIP for NERC

ArcSight Logger Compliance Insight Package (CIP) for NERC facilitates compliance with the NERC V5 standard using Logger's reporting, alerting, and dashboarding capabilities. Logger CIP for NERC addresses the NERC standard by providing:

- Detailed reports which cover the 10 NERC Critical Infrastructure Protection standards.
- Alerts that monitor incoming events in real time and notify NERC analysts when events of interest are detected.
- Dashboards which show a detailed overview of the NERC requirements.

The Logger Compliance Insight Package for NERC helps demonstrate the following to stakeholders and auditors:

- Implementation of NERC controls for your company.
- Due diligence in complying with NERC standards, as well as security policies and best practices.
- Real-time monitoring and notification of potential hazardous events, harmful user activity, network vulnerabilities, and configuration changes on critical BES cyber assets.
- Reporting that shows compliance to NERC CIP Standards.
- Graphic tools to display security events, which enables analysts to quickly analyze situations.

NERC CIP Standards Addressed

The Logger Compliance Insurance Package for NERC addresses the following NERC Critical Infrastructure Protection standards:

CIP #	Title	CIP Version
002	Cyber Security : BES Cyber System Categorization	5.1
004	Cyber Security : Personnel & Training	6
005	Cyber Security : Electronic Security Perimeter(s)	5
006	Cyber Security : Physical Security of BES Cyber Systems	6
007	Cyber Security : System Security Management	6
008	Cyber Security : Incident Reporting and Response Planning	5
009	Cyber Security : Recovery Plans for BES Cyber Systems	6
010	Cyber Security : Configuration Change Management and Vulnerability	2
011	Cyber Security : Information Protection	2

Reports, alerts, and dashboards for each standard are discussed in detail in the following sections.

Logger CIP for NERC Architecture

NERC CIP operates on events in Common Event Format (CEF), an industry standard for the interoperability of event or log-generating devices. CEF events can come from a device that is already configured to post events in CEF, or they can come from any network device whose events are first run through an ArcSight SmartConnector. NERC CIP operates on events received from devices on the network in CEF. NERC devices that are not already CEF-ready must be run through an ArcSight SmartConnector.

For more information about CEF events and how they are used, see the *ArcSight Logger Administrator's Guide*.

Limiting the Events Processed

If only some of your devices are subject to NERC CIP compliance, you can limit the events processed by the reports, alerts, and saved searches to improve Logger system performance and report more accurate and NERC CIP-relevant information.

You can limit the events processed in one or more of the following ways, depending on how your environment is set up and how you want to organize your Logger CIP for NERC compliance program.

- Create an NERC CIP-specific *device group* and only process events from devices in that group.
- Use an NERC CIP-related *storage group* to limit the events processed by the Logger CIP for NERC reports, alerts, and saved searches. This is only appropriate if an additional storage group (in addition to the Default Storage and Internal Event storage groups) was created during the Logger initialization process. Note that after the Logger initializes, you cannot allocate additional storage groups. For details, see the *ArcSightLogger Administrator's Guide*.
- Process events from specified devices only.

Tip: Reducing the amount of data a resource has to process improves performance. If only a small subset of the overall data feeding into Logger is subject to Logger CIP for NERC compliance, using a different storage group to store events from NERC CIP-related devices yields the best performance results.

To limit the events processed by the NERC CIP reports, alerts, and saved searches, implement one or more of these limiting strategies by following the configuration steps provided in the following sections.

- Classify NERC-related devices in a NERC device group. See "Classifying NERC CIP-Related Devices in a Device Group" on the next page.
- Create a NERC filter that constrains the events processed by the alerts and reports. See "Creating a Filter to Limit Events Processed" on the next page.
- Limit the events that an alert processes by either applying the NERC filter to the alert or adding the condition directly to the alert. See "Limiting Events Processed by Alerts" on page 8.
- Apply the NERC filter to the entire NERC CIP report category or specify at report run time. See "Limiting Events Processed by Reports" on page 9.
- Focus a saved search on NERC-related events only. See "Limiting Events Processed by Saved Searches" on page 10.

Processing Events

NERC CIP reports and saved searches process all events received by the Logger and no configuration is required.

NERC CIP alerts are configured to process all events except events that are stored in the Internal Event Storage Group. Some alerts require configuration with site-specific information; for details, see "NERC Alerts" on page 16.

If only some of your devices are subject to NERC CIP compliance, you can limit the events processed by reports, alerts, and saved searches. For more information, see "Limiting the Events Processed" on the previous page.

Classifying NERC CIP-Related Devices in a Device Group

If you plan on using a Device Group to limit the events processed by reports, alerts, and saved searches, create an NERC CIP device group and classify the NERC CIP-related devices into it as described in following procedure. After the NERC CIP-related devices are categorized, you can use the device group to focus on alerts and reports. For example, you can create a filter that only returns events from devices listed in the NERC CIP Device Group filter and then configure alerts and reports to use that filter to limit the events processed.

To classify NERC CIP-related devices into an NERC CIP Device Group:

1. Select **Configuration** on the top-level menu bar, and then click **Device Groups** in the **Data** section.
2. Click **Add**.
3. In the **Name** field, enter a name for the new device group, such as `NERC CIP`.
4. In the **Devices** field, click to select devices from the list. To add additional devices to the selection, press and hold the **Ctrl** key when selecting more devices.
5. Click **Save** to create the new Device Group.
6. Create a filter to limit the events processed, as described in "Creating a Filter to Limit Events Processed" below.

For more about device groups, see the *ArcSight Logger Administrator's Guide*.

Creating a Filter to Limit Events Processed

You can create a filter that identifies the NERC -related events for your environment, and use the filter to limit the events processed by NERC alerts and reports. A filter can limit events as follows:

- **Using an NERC CIP-related device group**: Only those events from devices listed in the device group are processed.
- **Using an NERC CIP-related storage group**: Only those events stored in the specified storage group are processed.
- **By specific devices**: Only events from specific devices are processed.

For example, you can create any of the following filters:

- A filter called `NERC CIP Device Group Filter` which returns events from devices categorized as Logger CIP for NERC devices.
- A filter called `NERC CIP Storage Group Filter` which returns events that are stored in a designated storage group.
- A filter called `NERC CIP Devices Filter` which returns events from specified devices.

- A filter called `NERC CIP Storage Group and Devices Filter` that returns events stored in a designated storage group (such as an `NERC CIP` Storage Group) or from a set of specific devices.

To create a filter:

1. Select **Configuration** on the top-level menu bar, and then click **Filters** in the **Search** section.
2. Click **Add**.
3. In the **Add Filter** page, enter the following information:

Field	Description
Name	Enter a name for the filter that identifies it with NERC CIP and identifies the purpose of the filter, such as `NERC CIP Device Group Filter` or `NERC CIP Storage Group Filter` or `NERC CIP Devices Filter`.
Type	From the drop-down menu, select **Search Group**. A filter of type *Search Group* can be used by reports to constrain events. A filter of type *Regex* can be used by alerts to constrain events. A filter of type *Unified* can be used by saved searched to constrain events.

4. In the Query field, construct a query, using one of the following options:
   - In the **Query** field, directly enter a regular expression, for example: `storageGroup(Default Storage Group)|deviceGroup(NERC CIP Device Group)`
   - Use the *Constrain search by* dialog: Select the ✎ icon. In the *Constrain search by* dialog, select from one of the following options:
     - Focus alerts to only process events from devices listed in the device group: Click **Device Groups**. Select a device group from the list and click **Submit.**
     - Focus alerts to only process events saved in a designated storage group: Click **Storage Groups**. Select a storage group from the list and click **Submit**.
     - Focus the alerts to only process events from individual devices subject to Logger CIP for NERC compliance: Select devices from the lists and click **Submit**. To select more than one device, press and hold the **Ctrl** key while selecting more devices.
5. Click **Save**.
6. Use the filter you created to limit the events processed by reports. See "Limiting Events Processed by Reports" on the next page

Limiting Events Processed by Alerts

To limit the events that an alert processes, either add a filter or add a Query Term to the alert.

Note: You can enable a maximum of 25 alerts on Logger at one time. Configure only the alerts that you plan to enable.

To add a filter to the alert:

1. Select **Configuration** on the top-level menu bar, and then click **Realtime Alerts** in the **Data** section.
2. Click **Add**.
3. In the **Filters** field, select the filter you created in "Creating a Filter to Limit Events Processed" on page 7 that limits the events processed by the alert.
4. Click **Save**.

To add a Query Term to the alert:

1. Select **Configuration** on the top-level menu bar, and then click **Realtime Alerts** in the **Data** section.
2. To edit the alert, click the NERC CIP alert in the Name column.
3. On the top-level Query Term field, click the Add (+) icon.

   A new empty Query term displays.
4. In the new Query Terms field, add a condition to the alert, using one of the following methods:
   - In the Query Terms field, directly enter a regular expression, for example: `storageGroup (Default Storage Group)|deviceGroup(NERC CIPDeviceGroup)`
   - Use the *Constrain search by* dialog. Select the ✎ icon and select from one of the following options in the *Constrain search by* dialog:
     - Focus alerts to only process events from devices listed in the device group: Click **Device Groups**. Select a device group from the list and click **Submit**.
     - Focus alerts to only process events saved in a designated storage group: Click **Storage Groups**. Select a storage group from the list and click **Submit**.
     - Focus the alerts to only process events from individual devices subject to NERC CIP compliance. Select devices from the list and click **Submit**. To select more than one device, press and hold the **Ctrl** key while selecting more devices.
5. Click **Save**.

Limiting Events Processed by Reports

You can limit events processed by the NERC CIP reports either with a filter, or at report runtime.

To limit the events using a filter:

1. Select **Report > Report Category** filters from the top-level menu bar.
2. On the **Report Category Enforced Filter** page, apply a report category (search group) filter to a whole report category.

To limit events at report runtime, run the report using the **Run** or **Quick Run** option. In the **Data** section, under **Devices, Device Groups,** or **Storage Groups,** select the appropriate constraint.

For more information about report category filters and scheduling reports, see the *ArcSight Logger Administrator's Guide*.

Limiting Events Processed by Saved Searches

To limit the events that a saved search processes, focus the saved search on NERC-related events.

To limit events processed by a saved search:

1. Select **Configuration** from the top-level menu bar.
2. Click on the **Saved Searches** tab
3. To edit the saved search, click the NERC saved search in the **Name** column.
4. In the query section, click **Advanced**
5. Do one or more of the following:

- Focus Saved Searches to only process events from devices listed in the Device Group: Click **Device Groups.** Select a Device Group from the list and click **Submit**.
- Focus Saved Searches to only process events saved in a designated Storage Group: Click **Storage Groups.** Select a Storage Group from the list and click **Submit**.
- Focus the Saved Searches to only process events from individual devices subject to NERC compliance: Select devices from the list and click **Submit**. To select more than one device, press and hold the Ctrl key while selecting more devices.

When finished, click **Save**.

Installation & Uninstallation

You can install Logger CIP for NERC on a Logger Appliance or a Software Logger.

Installation

Follow the appropriate installation procedure below for your Logger type.

To install Logger CIP for NERC on the Logger Appliance:

Download the Logger CIP for NERC .enc file (for example, `ArcSight-ComplianceInsightPackage-Logger-NERC.x.x.nnnn.0.enc`) to the computer where you plan to log into the Logger user interface. Check the Release Notes for the exact version of the file.

1. Log into the Logger user interface.
2. From the Logger top-level menu bar, click **System Admin.**
3. From the **System** section, select **License & Update.**
4. Click **Browse** to locate and open the .enc file you downloaded.
5. Click **Upload Update.** A dialog displays indicating that the update process might take some time.
6. Click **OK**. A message displays indicating that the update is progressing. After the contents of the .enc file are installed, another message displays indicating that the update is a success. The .enc file installs Logger CIP for NERC reports, saved searches, parameters, queries, dashboards, and alerts.

Verify that the content is installed, as follows:

- To view the installed alerts, click **Configuration** on the top-level menu bar, and then click **Alerts** in the **Data** section.
- To view the installed reports, click **Reports** on the top-level menu bar, and then click **Report Explorer** in the **Navigation** section. Click the arrow to the left of NERC to see the NERC report categories, and then click a category to see the list of reports.
- To view the installed dashboards, click **Dashboards** on the top-level menu and you should see NERC Dashboards.

To install Logger CIP for NERC on the Software Logger:

1. Log into the system running the Software Logger with the same ID that you used to install the software version of Logger.

2. Download the Logger CIP for NERC .bin file (for example, `ArcSight-ComplianceInsightPackage-Logger-NERC.x.x.nnnn.0.bin`). Check the Release Notes for the exact version of the file.
3. Go to the directory that contains the .bin file.
4. Change the permissions of the .bin file to be executable:

```
chmod +x ArcSight-ComplianceInsightPackage-Logger-NERC.x.x.nnnn.0.bin
```

5. Run the installer:

```
./ArcSight-ComplianceInsightPackage-Logger-NERC.x.x.nnnn.0.bin
```

6. Follow the instructions provided by the installer. When prompted to choose an installation folder, enter the same directory you specified when you installed the software Logger. For example, if when installing the Software Logger you specified the `/opt/logger` directory, specify `/opt/logger` as the installation folder. The .bin file installs the Logger CIP for NERC reports, parameters, queries, dashboards, and alerts.

Verify that the content is installed, as follows:

- To view the installed alerts, click **Configuration** on the top-level menu bar, and then click **Realtime Alerts** in the **Data** section.
- To view the installed reports, click **Reports** on the top-level menu bar, and then click **Report Explorer** in the Navigation section. Click the arrow to the left of **NERC** to see the NERC report categories, and then click a category to see the list of reports.
- To view the installed dashboards, click **Dashboards** on the top-level menu.

Uninstallation

To uninstall Logger CIP for NERC, you must delete each resource individually.

To delete the reports, queries, and parameters:

1. Delete each report, query, and parameter in the NERC report category:
   a. From the **Reports** top-level menu bar, click **Category Explorer** from the **Navigation** section.
   b. Right click on **NERC**.
   c. Click **Delete**.

To delete the alerts:

1. Delete each NERC CIP alert individually:
   a. From the **Configuration** top-level menu bar, click **Alerts** from the **Data** section.

b. For each NERC CIP alert, click the **Remove** (✖) icon.

c. In the confirmation dialog, click **OK** to complete the deletion.

To delete the dashboards:

1. Delete each NERC CIP dashboard individually:

   a. From the **Configuration** top-level menu bar, click **Dashboards**.

   b. For each NERC CIP dashboard, click **Tools > Delete Dashboard**.

   c. In the confirmation dialog, click **OK** to complete the deletion.

To delete saved searches:

1. Delete each NERC CIP saved search individually:

   a. From the **Configuration** top-level menu bar, click **Saved Searches** from the **Search** section.

   b. For each NERC CIP saved search, click the **Remove** ✖ icon.

   c. In the confirmation dialog, click **OK** to complete the deletion.

NERC CIP Resources

NERC CIP provides alerts, queries, reports, and dashboards.

Alerts

Alerts monitor incoming events in real time and notify analysts when events of interest are detected. All NERC CIP alerts are disabled by default.

You can view the list of NERC CIP alerts by selecting **Configuration** on the top-level menu bar, and then clicking **Realtime Alerts** in the **Data** section. To enable an alert, click the **Disabled**  icon.

Alerts are described under "NERC Alerts" on page 16.

For information about creating alert destinations and sending notifications, see the *ArcSight Logger Administrator's Guide*.

Queries

NERC CIP queries are invoked by the NERC CIP reports and have similar names as the reports themselves. You can view the queries by clicking **Reports** on the top-level menu bar, and then clicking **Query Explorer** in the **Navigation** section. For information on configuring queries, see the *ArcSight Logger Administrator's Guide*.

Queries are not described in this guide.

Dashboards

The dashboards provide a quick high level overview of the compliance status of different controls on the organization in various chart formats to help you demonstrate appropriate risk management and monitoring practices. You can view the dashboards by clicking **Dashboards** on the top-level menu bar.

Dashboards are described under "NERC Dashboards" on page 23.

Reports

NERC CIP reports consist of the following:

- **Standard Reports**

  NERC CIP standard reports are optimized to provide information that can be used to satisfy monitoring and reporting requirements of NERC. You can view the NERC CIP standard reports by clicking **Reports** on the top-level menu bar, and then clicking **Report Explorer** in the **Navigation** section. Each standard report has a SQL query associated with it that queries the database for the specified conditions. Certain reports prompt you to provide site-specific information at run time; this information is passed from the report to the query via parameters. Some queries contain default values, which you can customize to match conditions relevant to your environment.

- **Drill-down Reports**

  Some standard reports are enabled with additional investigative links that drill down to other reports and provide a different perspective about the behavior of an item on the network. For example, drilling down can provide more detail or generate a higher level overview about a certain event. Some drill-down reports are designed to be accessed by reference only from the reports that provide special hyperlinks to them. Other drill-down reports are top-level reports called entry drill-downs. Run these entry drill-downs first and use them to drill down to the other drill-down reports to avoid generating reports with a large number of pages. During an investigation, however, you might want to run a drill-down report directly; for example, to investigate a specific host or event name.

Reports are described under "NERC Reports" on page 30.

For information about running, formatting, publishing, and scheduling reports, see the *ArcSight Logger Administrator's Guide*.

NERC Alerts

NERC-002 Alerts

Alert Name	Alert Description	CIP-002 Requirement ID
NERC - New Host	Triggers when a new host is detected on the network.	R2 2.1
NERC - Microsoft Computer Account Created	Triggers when a new Microsoft computer account is created.	R1 1.1|R2 2.1
NERC - Microsoft Computer Account Deleted	Triggers when a Microsoft computer account is deleted.	R2 2.1

NERC-004 Alerts

Alert Name	Alert Description	CIP-004 Requirement ID
NERC - Anonymous User Activity	Triggers when anonymous user activity is detected.	R3.1
NERC - Modified User Group	Triggers when a user Group is modified, where user group is configuration variable. Configuration : On duser=GROUP_NAME Replace the GROUP_NAME string with the group you want to monitor	R4.3|R4.1
NERC - User Added to Group	Triggers when a user is added to group name ,where group name is configuration variable. Configuration : On cs6=Group_Name Replace the Group_name string with the group you want to monitor	R4.3|R4.1
NERC - Windows User Added to Privileged Group	Triggers when received Windows event which indicate that a user is added to privileged group.	R4.3|R4.1

NERC-005 Alerts

Alert Name	Alert Description	CIP-005 Requirement ID
NERC - Traffic Anomaly	Triggers when a network traffic anomaly is detected.	R1.5 /CIP-007-6 R4.1
NERC - Email Attacks	Triggers when an email attack is detected.	R1.5/ CIP-007-6 R4.1
NERC - Redirection Attacks	Triggers when redirection attack is detected.	R1.5/ CIP-007-6 R4.1
NERC - Information Interception Events	Triggers when information interception is detected.	R1.5/ CIP-007-6 R4.1
NERC - Covert Channel Activity	Triggers when covert channel activity is detected.	R1.5/ CIP-007-6 R4.1
NERC - Insecure Services Detected	Triggers when an insecure service, such as FTP, TFTP, telnet, POP3, or NetBIOS is identified.	R1.5/ CIP-007-6 R1.1

NERC-006 Alerts

Alert Name	Alert Description	CIP-006 Requirement ID
NERC - Failed Building Access Attempts	Triggers when a failed building access attempt is detected.	1.7

NERC-007 Alerts

Alert Name	Alert Description	CIP-007 Requirement ID
NERC - Anti-Virus Disabled	Triggers when an anti-virus disabled action is detected.	R3.3
NERC - Anti-Virus Failed Update	Triggers when a failed anti-virus update event is detected.	R3.3
NERC - Brute Force Attacks	Triggers when a brute force attack is detected.	R4.2.1
NERC - Code Injection Attacks	Triggers when a code injection attack is detected.	R4.2.1
NERC - Directory Traversal Attacks	Triggers when a directory traversal attack is detected.	R4.2.1
NERC - DoS Attacks	Triggers when a Denial of Service attack is detected.	R4.2.1

NERC-007 Alerts, continued

Alert Name	Alert Description	CIP-007 Requirement ID
NERC - Excessive Failed Administrative Actions	Triggers when an excessive number of failed actions occur by administrative user accounts. Default Match Count: 20 Default Threshold (Sec): 300	R4.1/R5.7
NERC - Excessive Failed Administrative Logins	Triggers when an excessive number of failed login attempts occur by administrative user accounts. Default Match Count: 10 Default Threshold (Sec): 300	R4.1/R5.7
NERC - Excessive Failed User Actions	Triggers when an excessive number of failed actions occur by non-administrative user accounts. Triggers for any accounts that are not listed as an administrative account in the alert. Default Match Count: 20 Default Threshold (Sec): 300	R4.1/R5.7
NERC - Excessive Failed User Logins	Triggers when an excessive number of failed login attempts occur by non-administrative user accounts. This alert is triggered for any accounts that are not listed as an administrative account in the alert. Default Match Count: 10 Default Threshold (Sec): 300	R4.2.2/R5.7
NERC - Excessive Successful Administrative Actions	Triggers when an excessive number of successful actions by administrative user accounts occur. Default Match Count: 300 Default Threshold (Sec): 300	R4.1
NERC - Excessive Successful Administrative Logins	Triggers when a large number of successful logins by administrative user accounts occur. Default Match Count: 10 Default Threshold (Sec): 300	R4.1
NERC - Excessive Successful User Actions	Triggers when a large number of successful actions occur by non-administrative user accounts. Triggers for any accounts that are not listed as an administrative account in the alert. Default Match Count: 2000 Default Threshold (Sec): 300	R4.1
NERC - Excessive Successful User Logins	Triggers when a large number of successful logins by non-administrative user accounts occur. Triggers for any accounts that are not listed as an administrative account in the alert. Default Match Count: 30 Default Threshold (Sec): 300	R4.1
NERC - Failed User Logins	Triggers when a failed user login event is detected.	R4.2.2

NERC-007 Alerts, continued

Alert Name	Alert Description	CIP-007 Requirement ID
NERC - Failed User Logins on BES Cyber Systems	Triggers when a failed user login event is detected on BES Cyber Systems. Configuration : On dst=BES_CYBER_SYSTEMS replace the BES_CYBER_SYSTEMS string with a regular expression that specifies a range of IP addresses for machines in the BES CYBER SYSTEMS For example, the following regular expression could be specified in the Query Terms field: dst=(172\.168\.(1[6-9]|2[0-9]|3[0-1])\.) This regular expression matches addresses in the range of 172.168.16-31.	R4.2.2
NERC - Information Leakage	Triggers when an information leakage is detected.	R4.2.1
NERC - Malicious Code Detection	Triggers when malicious code is detected.	R4.2.1
NERC - Privilege Escalation Attacks	Triggers when a privilege escalation is detected.	R4.2.1
NERC- Scan Attacks	Triggers when a scan attack (such port scanning, IP scanning , or service scanning) attack is detected	R4.2.1
NERC - Spoofing Attacks	Triggers when a spoof is detected.	R4.2.1
NERC - Excessive Failed Database Access	Triggers when an excessive number of failed database access attempts occur. Default Match Count: 100 Default Threshold (Sec): 300	R4.2.2
NERC - Excessive Successful Database Access	Triggers when an excessive number of successful database access attempts occur. Default Match Count: 100 Default Threshold (Sec): 300	R4.1
NERC - Detected Removable Storage	Triggers when a removable storage is detected on specific host name. Configuration : On dhost=HOST_NAME replace the HOST_NAME string with regex of the host names you want to monitor	R1.2
NERC - Data Written to Removable Storage Device	Triggers when a data written to removable storage device from specific host name. Configuration : On dhost=HOST_NAME replace the HOST_NAME string with regex of the host names you want to monitor.	R1.2
NERC - User Account Enabled	Triggers when a Windows user account enablement event is detected.	R4.2

NERC-007 Alerts, continued

Alert Name	Alert Description	CIP-007 Requirement ID
NERC - Interactive Login of System Accounts	Triggers when a Windows interactive login of system account event is detected.	R4.2
NERC - Changes by Un-Authorized Users on BES Critical Systems	Triggers when changes by unauthorized users detected on BES critical systems. Configuration : On suser=UNAUTHORIZED_USERS replace the UNAUTHORIZED_USERS string with regex of the unauthorized users you want to monitor. On dst=BES_CRITICAL_SYSTEMS replace the the BES_CRITICAL_SYSTEMS string with regex of the BES Critical systems you want to monitor	R4.2
NERC - Freak Attack Vulnerability Detected	Triggers when a freak attack vulnerability detected.	R4.2.1
NERC - GHOST glibc library Vulnerability Detected	Triggers when a GHOST glibc library vulnerability detected.	R4.2.1
NERC - Heartbleed Vulnerability Detected	Triggers when Heartbleed vulnerability detected.	R4.2.1
NERC - Microsoft Schannel Vulnerability Detected	Triggers when Microsoft Schannel vulnerability detected.	R4.2.1
NERC - POODLE Vulnerability Detected	Triggers when POODLE vulnerability detected.	R4.2.1
NERC - Shellshock Vulnerability Detected	Triggers when shellshock vulnerability detected.	R4.2.1

NERC-008 Alerts

Alert Name	Alert Description	CIP-008 Requirement ID
NERC - Suspicious Events	Triggers when there are events that are categorized as suspicious behavior, hostile behavior, or a compromise.	R1.1/CIP-007-R4.2.1

NERC-010 Alerts

Alert Name	Alert Description	CIP-010 Requirement ID
NERC - BES Cyber Systems with Vulnerabilities	Triggers when vulnerability detected on BES Cyber Systems. Configuration : On dst=BES_ADDRESSES Replace the BES_ADDRESSES string with a regular expression that specifies a range of IP addresses for machines in the BES CYBER SYSTEMS For example, the following regular expression could be specified in the Query Terms field: dst=(172\.168\.(1[6-9]|2[0-9]|3[0-1])\.) This regular expression matches addresses in the range of 172.168.16-31.	R3.1
NERC - Firewall Configuration Changes	Triggers when changes to a firewall's configuration file are reported.	R2.1/R1.1
NERC - Windows Domain Policy Changed	Triggers when a change to Windows Domain Policy is detected	R2.1/R1.1
NERC - Microsoft Audit Log Cleared	Triggers when the Microsoft Audit Log is cleared.	R2.1/R1.1
NERC - Network Equipment Configuration Changes	Triggers when changes to a network device's configuration file are reported.	R2.1/R1.1
NERC - Operating System Configuration Changes	Triggers when change to the operating system are reported	R2.1/R1.1

NERC-010 Alerts, continued

Alert Name	Alert Description	CIP-010 Requirement ID
NERC - VPN Configuration Changes	Triggers when changes to the VPN are reported	R2.1/R1.1
NERC - Vulnerability with High CVSS Score on BES Cyber Systems	Triggers when vulnerability with high CVSS score is detected on BES Cyber Systems. Configuration : On dst=BES_ADDRESSES Replace the BES_ADDRESSES string with a regular expression that specifies a range of IP addresses for machines in the BES CYBER SYSTEMS For example, the following regular expression could be specified in the Query Terms field: dst=(172\.168\.(1[6-9]|2[0-9]|3[0-1])\.) This regular expression matches addresses in the range of 172.168.16-31.	R3.1
NERC - New Process	Triggers when a new process is created on the system. Configuration : On dhost=HOST_NAME Replace the HOST_NAME string with a regular expression that specifies the host names you want to monitor. On dproc=PROCESS_NAME Replace the PROCESS_NAME string with a regular expression that specifies the process names you want to monitor.	R2.1|R1.1

NERC Dashboards

NERC CIP-002 Asset Creations and Modifications Dashboard

Panel	Title	Saved Search	Description	Type	Requirement ID
1	Created Assets per Day	NERC - Created Assets per Day	Shows asset creation events for the last 7 days.	Column	R2 2.1
2	Top Modified Assets	NERC - Top Modified Assets	Shows the top modified assets for the last day.	Column	R2 2.1
3	Modified Assets per Day	NERC - Modified Assets per Day	Shows the asset modification events for the last 7 days, grouped by day.	Column	R2 2.1

NERC CIP-004 Personel Security Dashboard

Panel	Title	Saved Search	Description	Type	Requirement ID
1	Top Anonymous User Activity by User	NERC - Anonymous User Activity	Shows top anonymous user activity events, by user.	Column	R3.1
2	Top Users Authorization Changes	NERC - Top Users Authorization Changes	Shows top users authorization change events, by user.	Column	R4.1
3	Last 20 Terminated Users	NERC - Last 20 Terminated Users	Shows the last 20 terminated users.	Table	R5
4	Top Anonymous User Activity by IP Address	NERC - Top Anonymous User Activity by IP Address	Shows the top anonymous user activity, by IP address.	Column	R3.1

NERC CIP-005 Network Communications Dashboard

Panel	Title	Saved Search	Description	Type	Requirement ID
1	Top Traffic to Public Addresses by Destination Address	NERC - Top Traffic to Public Addresses by Destination Address	Shows top traffic to public addresses, by destination address.	Column	R1.1

NERC CIP-005 Network Communications Dashboard, continued

2	Top Traffic to Public Addresses by Source Address	NERC - Top Traffic to Public Addresses by Source Address	Shows top traffic to public addresses, by source address.	Column	R1.1
3	Blocked Firewall Events per Day	NERC - Blocked Firewall Events per Day	Shows all blocked firewall events per day.	Column	R1.3
4	Top Traffic to Public Addresses by Network Device	NERC - Top Traffic to Public Addresses by Network Device	Shows top traffic to public addresses by network device.	Column	R1.1

NERC CIP-005 Network Attacks Dashboard

Panel	Title	Saved Search	Description	Type	Requirement ID
1	Top Redirection Attacks Events	NERC – Top Redirection Attacks Events	Shows top redirection attack events.	Column	R1.5
2	Covert Channel Activity Events	NERC - Covert Channel Activity	Shows top covert channel events.	Column	R1.5
3	Top Interception Events	NERC – Top Interception Events	Shows top interception events.	Column	R1.5
4	Top Email Attacks Events	NERC - Top Email Attacks Events	Shows top email attack events.	Column	R1.5

NERC CIP-005 Traffic Anomaly Dashboard

Panel	Title	Saved Search	Description	Type	Requirement ID
1	Top Network Layer Anomaly Events	NERC - Top Network Layer Anomaly Events	Shows top network layer anomaly events.	Column	R1.5
2	Top Transport Layer Anomaly Events	NERC - Top Transport Layer Anomaly Events	Shows top transport layer anomaly events.	Column	R1.5
3	Top Application Layer Anomaly Events	NERC - Top Application Layer Anomaly Events	Shows top application layer anomaly events.	Column	R1.5
4	Network Anomaly Events per Hour (Last 7 Days)	NERC - Network Anomaly Events per Hour	Shows all network anomaly events per hour.	Column	R1.5

NERC CIP-006 Physical Security Activity Dashboard

Panel	Title	Saved Search	Description	Type	Requirement ID
1	Failed Physical Facility Access Attempts at 15 Minute Intervals (Past Day)	NERC - Failed Physical Facility Access Attempts	Shows all failed physical facility access attempts at 15-minute intervals for the past day.	Column	1.6/1.1
2	Top Physical Access Event Reporting Devices (Past Day)	NERC - Physical Access Event Reporting Devices	Shows top devices reporting physical access events.	Column	1.6
3	Top Failed Physical Facility Access Users (Past Day)	NERC - Top Failed Physical Facility Access Users	Shows top users who most frequently failed to gain physical access.	Column	1.6/1.1
4	Last 5 Failed Physical Facility Access Attempts (Past Day)	NERC - Last Failed Physical Facility Access Attempts	Shows last 5 failed physical facility access attempts for the past day.	Table	1.6/1.1

NERC CIP-007 Ports Dashboard

Panel	Title	Saved Search	Description	Type	Requirement ID
1	Top Addresses Serving Ports	NERC - Top Open Ports by Address	Shows top addresses serving ports.	Column	1.1
2	Top Unsecured Ports	NERC - Top Unsecured Ports	Shows top unsecured ports.	Pie	1.1
3	Top Addresses Serving Unsecured Ports	NERC - Top Addresses Serving Unsecured Ports	Shows top addresses which are serving unsecured ports.	Column	R1.1
4	Top Dynamic Ports	NERC - Top Dynamic Ports	Shows top dynamic ports.	Pie	1.1

NERC CIP-007 Anti-Virus Activity Dashboard

Panel	Title	Saved Search	Description	Type	Requirement ID
1	Top Anti-Virus Disabled Events by Host	NERC - Top Anti-Virus Disabled Events by Host	Shows top anti-virus disabled events by host.	Column	R3.3
2	Top Failed Anti-Virus Updates by Host	NERC - Top Failed Anti-Virus updates by Host	Shows top failed anti-virus updates by host.	Column	R3.3
3	Anti-Virus Clean or Quarantine Attempt Events per Hour	NERC - Anti-Virus Clean or Quarantine Attempt	Shows all anti-virus or quarantine attempt event per hour.	Line	R3.1
4	Top Hosts Attacked by Viruses	NERC - Top Hosts Attacked by Viruses	Shows the top hosts attacked by viruses	Column	R3.1

NERC CIP-007 Login Activity Dashboard

Panel	Title	Saved Search	Description	Type	Requirement ID
1	Top Failed User Login by System	NERC - Top Failed User Login by System	Shows the top failed user logins by system.	Column	R4.1.2
2	Top Failed User Logins by User	NERC - Top Failed User Logins by User	Shows top failed user logins by user.	Column	R4.1.2
3	Infrequent Successful User Access	NERC - Rare Successful User Accesses	Shows all rare successful user accesses.	Line	R4.1.1
4	Top Failed Administrative Logins Events	NERC - Top Failed Administrative Logins Events	Shows top failed administrative logins events by name.	Column	R4.1.2

NERC CIP-007 Malicious Code Activity Dashboard

Panel	Title	Saved Search	Description	Type	Requirement ID
1	Malicious Malware Activity by the Hour	NERC - Malicious Malware Activity by the Hour	Shows malicious malware activity by the hour.	Line	R4.2/3.1
2	Worm Infected Systems by the Hour	NERC - Worm Infected Systems by the Hour	Shows worm-infected systems, sorted by hour.	Line	R4.2/3.1

NERC CIP-007 Malicious Code Activity Dashboard, continued

Panel	Title	Saved Search	Description	Type	Requirement ID
3	Top Worm Infected Systems by Address	NERC - Top Worm Infected Systems Events	Shows top worm-infected system events, sorted by address.	Column	R4.2/3.1
4	Top Worm Infected Systems Events	NERC - Top Worm Infected Systems Events	Shows top worm-infected system events, sorted by name.	Column	R4.1.2

NERC CIP-008 Incident Response Dashboard

Panel	Title	Saved Search	Description	Type	Requirement ID
1	Top Attacked Hosts	NERC - Top Attacked Hosts	Shows all top attacked hosts.	Column	R1.1
2	Top Attackers	NERC - Top Attackers	Shows the top attackers.	Column	R1.1
3	Top Attack Events	NERC - Top Attack Events	Shows the top attack events.	Column	R1.1
4	Attack Events per hour	NERC - Attack Events per hour	Shows attack events for each hour.	Column	R1.1

NERC CIP-010 Configuration Changes Dashboard

Panel	Title	Saved Search	Description	Type	Requirement ID
1	Top Firewall Configuration Change Events	NERC – Firewall Configuration Changes	Shows the top firewall configuration change events.	Column	R2.1/R1.1
2	Top Network Equipment Configuration Change Events	NERC – Network Equipment Configuration Changes	Shows the top network equipment configuration change events.	Column	R2.1/R1.1
3	Top VPN Configuration Change Events	NERC – VPN Configuration Changes	Shows the top VPN configuration change events.	Column	R2.1/R1.1
4	Top Application Configuration Change Events	NERC - Application Configuration Changes	Shows top application configuration change events.	Column	R2.1/R1.1

NERC CIP-010 Vulnerability Overview Dashboard

Panel	Title	Saved Search	Description	Type	Requirement ID
1	Top IP Addresses with CVSS Score Vulnerabilities of 4 or More (Past 30 Days)	NERC– Top IP Addresses with CVSS Score Vulnerabilities of 4 or More	Shows the top IP Addresses with CVSS score vulnerabilities greater than or equal to 4.	Column	R3.1
2	Top Critical Vulnerability Events by CVE, CVSS, and Destination Address (Past 7 Days)	NERC - Top Critical CVEs	Shows the top critical vulnerability events by CVE, CVSS, and destination address for the past 7 days.	Column	R3.1
3	Vulnerability Scanner Events by Device Vendor (Past 3 Days)	NERC - Vulnerability Scanner Events per Device Vendor	Shows vulnerability scanner events by device vendor for the past 3 days.	Pie	R3.1
4	Top Vulnerability Events by Vendor Signature (Past 14 Days)	NERC - Top Vulnerability Events by Vendor Signature	Shows the top vulnerability events by vendor signature for the last 14 days	Column	R3.1

NERC CIP-010 Vulnerability Types (Top Addresses) Dashboard

Panel	Title	Saved Search	Description	Type	Requirement ID
1	Top Vulnerable Addresses to Overflow Vulnerabilities	NERC - Top Vulnerable Addresses to Overflow Vulnerabilities	Shows the top addresses which are vulnerable to overflow attacks.	Column	R3.1
2	Top Vulnerable Addresses to CSRF Vulnerabilities	NERC - Top Vulnerable Addresses to CSRF Vulnerabilities	Shows the top addresses which are vulnerable to CSRF (cross-site request forgery) attacks.	Column	R3.1
3	Top Vulnerable Addresses to XSS Vulnerabilities	NERC - Top Vulnerable Addresses to XSS Vulnerabilities	Shows the top addresses which are vulnerable to XSS attacks.	Column	R3.1
4	Top Vulnerable Addresses to SSL Vulnerabilities	NERC - Top Vulnerable Addresses to SSL Vulnerabilities	Shows the top addresses which are vulnerable to SSL attacks.	Column	R3.1

NERC CIP-010 Vulnerability Types (Per Month) Dashboard

Panel	Title	Saved Search	Description	Type	Requirement ID
1	Overflow Vulnerabilities per Month	NERC - Overflow Vulnerabilities per Month	Shows overflow vulnerabilities by month.	Line	R3.1
2	CSRF Vulnerabilities per Month	NERC - CSRF Vulnerabilities per Month	Shows CSRF vulnerabilities by month.	Line	R3.1
3	SSL Vulnerabilities per Month	NERC - SSL Vulnerabilities per Month	Shows SSL vulnerabilities by month.	Line	R3.1
4	XSS Vulnerabilities per Month	NERC – XSS Vulnerabilities per Month	Shows XSS vulnerabilities by month.	Column	R3.1

NERC Reports

NERC-002 Reports

Report Name	Report Description	CIP-002 Requirement ID
NERC - Host Modification Events by Host	Displays all modifications on a host detected by traffic analysis systems.	R2 2.1
NERC - Modified Hosts	Displays all modified hosts on the network detected by traffic analysis systems.	R2 2.1
NERC - New Hosts	Displays all new hosts on the network detected by traffic analysis systems.	R2 2.1
NERC - New Hosts on High-Impact BES System Networks	Displays all new hosts on the high-impact BES system networks detected by traffic analysis systems, where high-impact BES systems are defined by the parameter HIGH_IMPACT_BES_CYBER_SYSTEMS.	R2 2.1
NERC - New Hosts on Low-Impact BES System Networks	Displays all new hosts on the low-impact BES system networks detected by traffic analysis systems, where low-impact BES systems are defined by the parameter LOW_IMPACT_BES_CYBER_SYSTEMS.	R2 2.1
NERC - New Hosts on Medium-Impact BES System Networks	Displays all new hosts on the medium-impact BES system networks detected by traffic analysis systems, where medium-impact BES systems are defined by the parameter MEDIUM_IMPACT_BES_CYBER_SYSTEMS.	R2 2.1
NERC - New Services	Displays all new services detected on the network by traffic analysis systems.	R2 2.1
NERC - New Services by Host	Displays all new services detected on a host by traffic analysis systems.	R2 2.1

NERC-004 Reports

Report Name	Report Description	CIP-003 Requirement ID
NERC - Anonymous User Activity	Displays all anonymous user activity, where anonymous users are defined by the NERC_ANONYMOUS_ACCOUNTS parameter.	R3.1
NERC - Anonymous User Activity on High-Impact BES Systems	Displays anonymous user activity on high-impact BES systems, where anonymous users are defined by the NERC_ANONYMOUS_ACCOUNTS parameter, and high-impact BES systems are defined by the HIGH_IMPACT_BES_CYBER_SYSTEMS parameter.	R3.1
NERC - Anonymous User Activity on Medium-Impact BES Systems	Displays anonymous user activity on medium-impact BES systems, where anonymous users are defined by the NERC_ANONYMOUS_ACCOUNTS parameter, and high-impact BES systems are defined by MEDIUM_IMPACT_BES_CYBER_SYSTEMS parameter.	R3.1
NERC - Authorization Changes	Displays authorization changes made on systems and the number of events per host name.	R4.1
NERC - Privileged Account Changes	Displays all changes made to privileged accounts, such as password changes, by user and number of changes. Privileged accounts are defined by the NERC_ADMIN_USERS parameter, and can be modified at runtime.	R4.1|R4.3
NERC - Removal of Access Rights	Displays the number of events on each host indicating the removal of access rights, user account, and group deletion.	R4.1|R4.3
NERC - Terminated User Activity	Displays all terminated user activity.	R5
NERC - Terminated Users	Displays all terminated users.	R5
NERC - User Account Creation	Displays the user, host, and zone information from user account creation events, sorted by events per zone.	R4.1|R4.3
NERC - User Account Deletion	Displays events indicating that user accounts have been removed from a system.	R4.1|R4.3
NERC - Windows Users Added to Privileged Group	Displays Windows users added to privileged groups including Time, Subject, Object, Domain info, and Group.	R4.3|R4.1
NERC - Windows Users Removed from Privileged Group	Displays Windows users removed from privileged groups including Time, Subject, Object, Domain info, and Group.	R4.3|R4.1
NERC - User Group Creation	Displays all events for creation of user groups.	R4.3|R4.1
NERC - User Group Deletion	Displays all events for deletion of user groups.	R4.3|R4.1

NERC-004 Reports, continued

Report Name	Report Description	CIP-003 Requirement ID
NERC - User Group Modification	Displays all events for modification of user groups.	R4.3|R4.1
NERC – Users Added to Groups	Displays all events for additions to user groups.	R4.3|R4.1
NERC – Users Removed from Groups	Displays all events for removal of users from user groups.	R4.3|R4.1

NERC-005 Reports

Report Name	Report Description	CIP-005 Requirement ID
NERC - BES Systems to External - All	Displays BES systems that are communicating directly with external systems. This traffic should be justified.	R1.1
NERC - Blocked Firewall Traffic - All	Displays the number of blocking events generated by devices that have blocked traffic.	R1.3
NERC - Blocked Firewall Traffic from High-Impact BES Systems	Displays the number of blocking events generated by devices that have blocked traffic from high-impact BES systems, where high-impact BES systems are defined by the HIGH_IMPACT_BES_CYBER_SYSTEMS parameter.	R1.3
NERC - Blocked Firewall Traffic from Medium-Impact BES Systems	Displays the number of blocking events generated by devices that have blocked traffic from medium-impact BES systems, where medium-impact BES systems are defined by the MEDIUM_IMPACT_BES_CYBER_SYSTEMS parameter.	R1.3
NERC - Blocked Firewall Traffic to High-Impact BES Systems	Displays the number of blocking events generated by devices that have blocked traffic to high-impact BES systems, where high-impact BES systems are defined by the HIGH_IMPACT_BES_CYBER_SYSTEMS parameter.	R1.3
NERC - Blocked Firewall Traffic to Medium-Impact BES Systems	Displays the number of blocking events generated by devices that have blocked traffic to medium-impact BES systems, where medium-impact BES systems defined are by the MEDIUM_IMPACT_BES_CYBER_SYSTEMS parameter.	R1.3
NERC - Clear Text Password Transmission	Displays clear text password transmission events.	R1.5
NERC - Covert Channel Activity	Displays a count of events identified as covert channel activity, sorted by target zone. These events are generated by IDS devices and may indicate the use of a 'loki' or other tool designed to establish an undetected channel either to or from an organization.	R1.5

NERC-005 Reports, continued

Report Name	Report Description	CIP-005 Requirement ID
NERC - Email Attacks Events	Displays information about email attacks.	R1.5
NERC - External to BES Systems - All	Displays all external systems that are communicating directly with BES systems. This traffic should be justified.	R1.1
NERC - Firewall Event Review by Device	Displays the number of different events that were triggered on NIDS systems, sorted by device.	R1.5
NERC - Firewall Open Port Review	Displays the destination ports accepted through firewalls. Includes a pie chart showing the most commonly-used destination ports.	R1.3
NERC - Inbound Traffic from Public IP Addresses to the High-Impact BES systems	Displays inbound traffic from public IP addresses to high-impact BES systems, where high-impact BES systems are defined by the HIGH_IMPACT_BES_CYBER_SYSTEMS parameter.	R1.1
NERC - Inbound Traffic from Public IP Addresses to the Medium-Impact BES systems	Displays inbound traffic from public IP addresses to medium-impact BES systems, where medium-impact BES systems are defined by the MEDIUM_IMPACT_BES_CYBER_SYSTEMS parameter.	R1.1
NERC - Information Interception Events	Displays the date, source, and destination information from information interception events.	R1.5
NERC - Insecure Services	Displays systems providing insecure services such as FTP or Telnet. The chart displays the number of times each system provided an insecure service.	R1.5/ CIP-007-6 R1.1
NERC - NIDS Event Review by Device	Displays the number of different events that were triggered on NIDS systems, sorted by device.	R1.5
NERC - Outbound Traffic from the High-Impact BES Systems to Public IP Addresses	Displays outbound traffic from high-impact BES systems to public IP addresses, where high-impact BES systems are defined by the HIGH_IMPACT_BES_CYBER_SYSTEMS parameter.	R1.1
NERC - Outbound Traffic from the Medium Impact BES Systems to Public IP Addresses	Displays outbound traffic from medium-impact BES systems to public IP addresses, where medium-impact BES systems are defined by the MEDIUM_IMPACT_BES_CYBER_SYSTEMS parameter.	R1.1
NERC - Redirection Attacks Events	Displays information about redirection attacks.	R1.5
NERC - Traffic Anomaly on Application Layer Events	Displays the date, source, and destination information from application layer anomaly events.	R1.5

NERC-005 Reports, continued

Report Name	Report Description	CIP-005 Requirement ID
NERC - Traffic Anomaly on Network Layer Events	Displays the date, source, and destination information from network layer anomaly events.	R1.5
NERC - Traffic Anomaly on Transport Layer Events	Displays the date, source, and destination information from transport layer anomaly events.	R1.5
NERC - Traffic Between Zones - Protocol	Displays communication protocols which are passed between different zones.	R1.1
NERC - Traffic - Inbound on Disallowed Ports	Displays the number of attempted connections (successful and failed) for inbound traffic on disallowed ports on BES systems. Allowed ports are specified at runtime using the NERC_ALLOWED_PORTS parameter. By default, the ports 80 and 443 are specified. BES Systems are specified at runtime using the BES_CYBER_NETWORKS parameter.	R1.5
NERC - VPN Access Summary	Displays a summary of VPN access by users.	R2.2

NERC-006 Reports

Report Name	Report Description	CIP-006 Requirement ID
NERC - Failed Building Access Attempts	Displays all failed building access attempts including user name, ID, and badge reader number.	R1.1 /R1.6
NERC - Failed Building Access Attempts after Work Hours	Displays all failed building access attempts after Work Hours including user name, ID, and badge reader number.	R1.1/R1.6
NERC - Failed Building Access Attempts during the Weekends	Displays all failed building access attempts including user name, ID, and badge reader number.	R1.1/R1.6
NERC - Physical Access Event Reporting Devices	List of physical access events reporting devices.	R1.6
NERC - Physical Access System Account Creation	Shows all new accounts added to physical access systems sorted by user name for the time period you specify when you run the report.	R1.1
NERC - Physical Access System Account Deletion	Shows all deletions of accounts from physical access systems.	R1.1
NERC - Physical Access System Account Modification	Shows all modifications made to accounts on physical access systems.	R1.1

NERC-006 Reports, continued

Report Name	Report Description	CIP-006 Requirement ID
NERC - Physical Facility Access Attempts – All	Displays all authentication verification events (badge-ins) involving physical access systems.	R1.8
NERC - Physical Facility Access Attempts by User	Displays specific user authentication verification events (badge-ins) involving physical access systems.	R1.8
NERC - Physical Reporting Devices Configuring changes	Displays the date, time, event name, and host information from all events indicating a configuration change has been made on physical device equipment.	R1.1
NERC - Successful Building Access Attempts	Displays all successful authentication verification events (badge-ins) involving physical access systems.	R1.8
NERC - Successful Building Access Attempts after Work Hours	Displays all successful building access attempts after work hours including user name, ID, and badge reader number.	R1.8
NERC - Successful Building Access Attempts during the Weekends	Displays all successful building access attempts during the weekends including user name, ID, and badge reader number.	R1.8
NERC - Events by Device	Designed as a drill-down report ,shows different events fields by device Address.	N/A

NERC-007 Reports

Report Name	Report Description	CIP-007 Requirement ID
NERC - Account Activity by User	Displays all the events with the specified destination user name, defined at runtime.	R4.1
NERC - Account Lockouts by System	Displays incidents of user accounts locked out by the system, sorted by system name. The chart displays a trend of the number of such incidents per day.	R5.7
NERC - Account Lockouts by User	Displays incidents of user accounts locked out by the system, sorted by user name. The chart displays a trend of the number of such incidents per day.	R5.7
NERC - Anti Virus Update Summary	Displays all anti-virus software updates.	R3.3
NERC - Anti Virus Update Summary by Update Result	This report designed as drill down of "Anti Virus Update Summary" report to show Anti Virus updates by result.	R3.3

NERC-007 Reports, continued

Report Name	Report Description	CIP-007 Requirement ID
NERC - Confidentiality and Integrity Breach Sources – Count	Displays the sources for confidential and integrity attacks and the number of attacks associated with each source. The chart displays the number of such events identified initiated in each zone.	R3.1
NERC - Database Access - All	Displays all login attempts to all database systems.	R4.1
NERC - Database Access – Failed	Displays all failed login attempts made to database systems.	R4.1.2
NERC - Detailed Anti-Virus Report	Displays a detailed listing of anti-virus events (routine maintenance and remediation events) ordered according to zone, IP address, and virus name.	R3.1
NERC - Detailed Anti-Virus Report per Host	This report was designed as a drill-down report. Displays a detailed listing of anti-virus events (routine maintenance and remediation events) for a specific host, ordered according to time.	R3.1
NERC - Dynamic Ports by Address	Displays all the dynamic ports by address.	R1.1
NERC - Event in Network	This report was designed as a drill-down report. Displays the hosts that were targeted by a specific event and the number of times they were targeted.	N/A
NERC - Failed Administrative Logins by System	Displays all failed administrative logins, by system.	R4.1.2
NERC - Failed Administrative Logins by User	Displays all administrative users that failed to log into systems, the number of failed logins and the number of distinct systems that were attempted to log into.	R4.1.2
NERC - Failed Administrative Logins per System - Detail	Displays all the failed administrative logins into a particular system. The chart shows the number of failed administrative logins for each product.	R4.1.2
NERC - Failed Administrative Logins per System - Summary	Displays all the administrative users that failed to login into each system and the number of such failed logins.	R4.1.2
NERC - Failed Administrative Logins per User - Detail	Displays all failed logins for the selected administrative user. The chart shows the number of failed logins per product.	R4.1.2

NERC-007 Reports, continued

Report Name	Report Description	CIP-007 Requirement ID
NERC - Failed Administrative Logins per User - Summary	Displays all the systems that the selected administrative users failed to login into, and the number of such failed logins.	R4.1.2
NERC - Failed User Logins by System	Displays all failed non-administrative logins by system.	R4.1.2
NERC - Failed User Logins by User Name	Displays all non-administrative users that failed to log into systems, the number of failed logins and the number of distinct systems that were attempted to log into.	R4.1.2
NERC - Failed User Logins per System - Detail	Displays all the failed non-administrative logins into a particular system.	R4.1.2
NERC - Failed User Logins per System - Summary	Displays all the non-administrative users that failed to login into each system and the number of such failed logins.	R4.1.2
NERC - Failed User Logins per User Name - Detail	Displays all failed logins for the selected non-administrative user.	R4.1.2
NERC- Failed User Logins per User Name - Summary	Displays all the systems that the selected non-administrative user failed to login to, and the number of such failed logins.	R4.1.2
NERC - HIDS Event Review by Device	Displays all events that were triggered on HIDS systems and the number of times each event occurred.	R3.1
NERC - Host Event Count	This report was designed as a drill-down report. Displays the number of events different events that targeted a specific host.	N/A
NERC - Malicious Code Sources	Displays the count of malicious code events from particular hosts.	R3.1
NERC - Not Allowed Registered Ports by Address	Displays all the not allowed open ports by IP address, the allowed ports are configured using this parameter <NERC_ALLOWED_PORTS>.	R1.1
NERC - Open Ports - All	Displays all open ports in the organization.	R1.1
NERC - Open Ports by Address	Displays all the open ports by address.	R1.1

NERC-007 Reports, continued

Report Name	Report Description	CIP-007 Requirement ID
NERC - Stopped or Paused Anti-Virus Events	Displays all anti-virus disabled events as reported by Microsoft systems.	R3.3
NERC - Successful Administrative Logins by System	Displays all successful administrative logins, by system. The chart displays a summary of the number of all administrative logins by product.	R4.1.1
NERC - Successful Administrative Logins by User	Displays all administrative users that successfully logged into systems, the number of successful logins and the number of distinct systems that were logged into.	R4.1.1
NERC - Successful Administrative Logins per System - Detail	Displays all the events where administrators successfully logged into a particular system.	R4.1.1
NERC - Successful Administrative Logins per System - Summary	Displays all the administrative users that successfully logged into each system and the number of such logins.	R4.1.1
NERC - Successful Administrative Logins per User – Detail	Displays all successful logins for the selected administrative user.	R4.1.1
NERC - Successful Administrative Logins per User - Summary	Displays all the systems that the selected administrative users successfully logged into, and the number of such successful logins.	R4.1.1
NERC - Successful Brute Force Logins	Displays the time, user, and host information from successful brute-force logins.	R3.1
NERC - Successful Password Changes	Displays which users have changed their passwords and when.	R5.6
NERC - Successful User Logins by System	Displays a count of all successful non-administrative logins for each system.	R4.1.1
NERC - Successful User Logins by User Name	Displays all non-administrative users that successfully logged into systems, the number of successful logins and the number of distinct systems that were logged into.	R4.1.1
NERC - Successful User Logins per System - Detail	Displays all the events where non-administrators successfully logged in into a particular system.	R4.1.1

NERC-007 Reports, continued

Report Name	Report Description	CIP-007 Requirement ID
NERC - Successful User Logins per System - Summary	Displays all the non-administrative users that successfully logged in into each system and the number of such successful logins.	R4.1.1
NERC - Successful User Logins per User Name - Detail	Displays all successful logins for the selected non-administrative user.	R4.1.1
NERC - Successful User Logins per User Name - Summary	Displays all the systems that the selected non-administrative users successfully logged into, and the number of such successful logins.	R4.1.1
NERC - Suspicious Activity in Wireless Network	Displays events defined as suspicious activity, such as port scanning in the wireless network. The wireless network is defined by the 'wirelessNetwork' parameter and can be changed at runtime. The chart displays a count of the different events that were defined as suspicious.	R3.1
NERC - Trojan Code Activity	Displays all trojan activity.	R3.1
NERC - Unsecured Ports by Address	Displays all unsecured ports by address.	R1.1
NERC - User Logins and Logouts	Displays the time, name, destination, and user information from user login and logout events.	R4.1| R5.2
NERC - Virus Summary By Host	Displays systems infected with viruses and the number of infections for each system.	R3.1
NERC - Virus Summary By Virus	Displays detected viruses on systems and the number of such detections, ordered by the viruses that were detected most times.	R3.1
NERC - Worm Activity	Displays all worm activity.	R3.1
NERC - Data Written to Removable Storage	Displays data written to removable storage using Windows 2012/2008 events.	R1.2

NERC-007 Reports, continued

Report Name	Report Description	CIP-007 Requirement ID
NERC - Removable Storage Devices Activity	Displays removable storage devices activity using Windows 2008/2012 events.	R1.2
NERC - New External Device was Recognized by the System	Displays new external devices which recognized by Windows 2016 and Windows 10 events.	R1.2
NERC - Windows Remote Access User Logins by System	Displays a successful Windows Remote (Terminal Services, Remote Desktop Remote Assistance or connections to shared folder) logins by system, where system host name is provided at run-time. Default is all the systems.	R4.1|R5.1

NERC-008 Reports

Report Name	Report Description	CIP-008 Requirement ID
NERC - Attacked Hosts - Top 20	Displays the 20 hosts that were the target for the largest number of events identified as attacks. The chart displays the number of events identified as 'attacks that targeted each destination IP address.	R1.1
NERC - Attackers - Top 20	Displays the 20 hosts that were the source for the largest number of events identified as attacks. The chart summarizes the number of events identified as attacks per source IP address.	R1.1
NERC - Attack Events - Top 20	Displays the 20 most common attack event names in the report's time frame.	R1.1
NERC - Attacks - High Impact to Medium Impact BES Cyber Systems	Displays the number of events per day categorized as attacks, originating from the high-impact BES network and targeting the medium-impact BES network. The high and medium and target networks are defined by parameters and can be set in runtime.	R1.1
NERC - Attacks - Hourly Count	Displays the number of attacks that targeted BES Cyber IP addresses each hour.	R1.1
NERC - Attacks - Medium Impact to High Impact BES Cyber Systems	Displays the number of events per day categorized as attacks, originating from the medium network and targeting the high network. High and medium impact networks are defined by parameters and can be set in runtime. The chart displays the number of such incidents per day.	R1.1
NERC - Attacks Targeting BES Cyber Assets	Displays all events with category significance of 'Recon', 'Compromise', 'Hostile', or 'Suspicious' that target a BES Cyber IP address.	R1.1

NERC-008 Reports, continued

Report Name	Report Description	CIP-008 Requirement ID
NERC - BES Cyber Systems Reconnaissance - Top 20 Events	Displays the top events identified as BES cyber systems reconnaissance events, such as port scanning activity. BES Cyber System are defined by parameters and can be set in runtime.	R1.1
NERC - BES Cyber Systems Reconnaissance - Top 20 Sources	Displays the 20 hosts that were the source of most BES cyber systems reconnaissance events, such as port scanning activity. BES Cyber Systems are defined by parameters and can be set in runtime.	R1.1
NERC - BES Cyber Systems Reconnaissance - Top 20 Targets	Displays the 20 hosts that were the target of most BES cyber systems reconnaissance events, such as port scanning activity. BES Cyber Systems are defined by parameters and can be set in runtime.	R1.1
NERC - Denial of Service Sources	Displays all the sources involved in Denial of Service activity.	R1.1
NERC - High Risk Events	Displays source and destination information from all events with an agent severity of High or Very High.	R1.1
NERC - High Risk Events by Zone	Displays the number of High or Very High severity events, sorted by zone.	R1.1

NERC-009 Reports

Report Name	Report Description	CIP-009 Requirement ID
NERC - Availability Attacks	Displays a count of Denial of Service and other availability attacks on the network. The chart displays the number of availability attacks in each zone.	R1.1|CIP-007 R3.1
NERC - Information System Failures	Displays a count of failures that occur on machines in the network, such as the failure to start a service or denial of an operation. The chart summarizes the number of failures on each host.	R1.1
NERC - Resource Exhaustion	Displays a count of events indicating resource exhaustion on particular hosts.	R1.1

NERC-010 Reports

Report Name	Report Description	CIP-010 Requirement ID
NERC - All CVE Vulnerabilities per Host	Displays all the CVEs and their CVSS Score by specific host. Default is all hosts.	R3.1
NERC - Application Configuration Modifications	This report displays events that are categorized as application configuration modifications such as an update of a license file or a program setting change. The chart displays the number of such incidents per day.	R2.1/R1.1
NERC - Audit Log Cleared	This report displays the date, time, system, and user information from all events indicating an audit log has been cleared.	R2.1
NERC - Changes to Operating Systems	This report displays modifications to operating systems such as account changes or change to the security options, and the number of the times these events happened. The chart displays the number of such events per host.	R2.1/R1.1
NERC - CVSS Score Vulnerabilities equal or greater than 8	Displays all the CVSS Score vulnerabilities per specific host equal or greater than 8, default all hosts.	R3.1
NERC - Firewall Configuration Changes	Displays all firewall configuration changes.	R2.1/R1.1
NERC - Misconfigured Systems	This Report shows all the misconfigured systems events.	R2.1/R1.1
NERC - Network Equipment Configuration Changes	Displays all network equipment configuration changes, including changes to routers and switches.	R2.1/R1.1
NERC - Security Patch Missing	Displays all the missing security patch events.	R2.1/R1.1
NERC -Top 20 Vulnerabilities	Displays the 20 most common vulnerabilities on systems, the number of systems on which they are found, and additional information regarding the vulnerability.	R3.1
NERC -Top 20 Vulnerable Assets	Displays the 20 systems with the most vulnerabilities as reported by vulnerability scanners.	R3.1

NERC-010 Reports, continued

Report Name	Report Description	CIP-010 Requirement ID
NERC - VPN Configuration Changes	Displays all configuration changes made to NERC related VPN devices.	R2.1/R1.1
NERC - Vulnerabilities on Host per Scanner	This report was designed as a drill-down report.Displays all the vulnerabilities on a host for a specific scanner.	R3.1
NERC - Vulnerabilities per Host - All - Drill Down-	This report was designed as a drill-down report. Displays all the vulnerabilities for a certain host name.	R3.1
NERC - Vulnerability Count per Scanner	This report was designed as a drill-down report. Displays the number of vulnerabilities found by each scanner that scanned the host.	R3.1
NERC - Vulnerability in Network	This report was designed as a drill-down report. Displays all the hosts with the selected vulnerability.	R3.1
NERC - Vulnerable Hosts per CVE	Displays all the vulnerable hosts per specific CVE, default all CVEs.	R3.1
NERC - Cross Site Request Forgery Vulnerabilities	Displays cross site request forgery vulnerabilities where IP Address and Host Name input parameters can be modified at runtime default all the systems. The query uses a full text search on different fields (both indexed and un-indexed fields) and this could lead to some slowness when running this report.	R3.1
NERC - Overflow Vulnerabilities	Displays overflow vulnerabilities (like buffer and head overflows) where IP Address and Host Name input parameters can be modified at runtime default all the systems . the query is using a full text search on different fields (both indexed and un-indexed fields) and this could lead to some slowness when running this report.	R3.1
NERC - Scada Vulnerabilities	Displays potential SCADA vulnerabilities where IP Address and Host Name input parameters can be modified at runtime default all the systems . the query is using a full text search on different fields (both indexed and un-indexed fields) and this could lead to some slowness when running this report.	R3.1
NERC - SSL Vulnerabilities	Displays SSL vulnerabilities where IP Address and Host Name input parameters can be modified at runtime default all the systems . the query is using a full text search on different fields (both indexed and un-indexed fields) and this could lead to some slowness when running this report.	R3.1

NERC-010 Reports, continued

Report Name	Report Description	CIP-010 Requirement ID
NERC - Windows Group Policy Changes	This report displays changes to Microsoft Active Directory.	R2.1|CIP-007 5.5
NERC - Windows Domain Policy Changes	This report displays changes to Microsoft Domain Policy.	R2.1
NERC - New Processes	Displays all the new processes by system, user and process name, where system ,user and process name are parameters which configured at run-time ,by default displays all the new processes on the organization.	R2.1
NERC - Vulnerabilities per Host	Displays vulnerabilities by specific host. Default all hosts and all vulnerabilities. Drill downs : Destination Host Name: Shows All the Vulnerabilities on this Host Name Signature ID: Shows All the hosts vulnerable to this Signature ID CVE ID -> Shows All the hosts vulnerable to this CVE ID CVSS Score -> Shows all the CVEs which have a CVSS Score equal or greater than 8 on this specific host.	R3.1

NERC-011 Reports

Report Name	Report Description	CIP-011 Requirement ID
NERC - Insecure cryptographic storage	Displays insecure cryptographic storage detected on your systems.	R1.2
NERC - Systems Providing Unencrypted Services	Displays systems that provide unencrypted communications and the number of such events recorded. Unencrypted communication is defined as using one of the following services: telnetd, ftpd, in.rexecd, rexec, pop3, rsh, imapd; or is performed on the following ports: 20, 21, 25, 110, 143, 23. These values are defined in the query and can be adjusted according to the customer's definitions.	R1.2

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Solutions Guide (Logger CIP for NERC 1.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arc-doc@hpe.com.

We appreciate your feedback!