Choosing between an internal or third-party Cyber Vulnerability Assessment

While the NERC CIP Security Standards stipulate the minimum requirements to verify during a Cyber Vulnerability Assessment (CVA), they do not state by whom this verification must be completed. One dilemma facing entities is whether to conduct a CVA in-house or to hire a third-party to execute the assessment on their behalf. Some issues that may lead an entity to choose a third-party are:

- Lack of clear understanding of what information will be required to complete the CVA or lack of a documented CVA methodology,
- Concern regarding "checks and balances" within the entity where the same personnel that completed the work are the only ones equipped to execute the CVA in order to assess the work,
- Lack of clear understanding of how the documentation at the conclusion of the CVA may affect a NERC CIP audit, or
- Limited resource availability.

If the decision is made to proceed with a third-party to execute the CVA, selecting which third-party can be the difference between a successful NERC CIP audit and one with Potential Violations (PVs).

N&ST’s approach: There’s No Substitute for Experience

N&ST has developed a flexible, proven approach to executing CVAs that gets tailored to the needs and unique architecture of the entity. Led by senior consultants who have conducted CVAs with numerous entities across multiple regions, N&ST will walk the entity through identifying which baseline evidence is needed and what options exist for collecting current environment information prior to starting the CVA. Each approach to collecting current information has its pros and cons, as well as timeframe required to complete. With guidance from N&ST senior consultants, choosing the most appropriate approach while minimizing the time needed from the entity resources ensures an efficient, cost-effective CVA. And while no two CVAs are exactly the same, N&ST and its clients have successfully defended each at NERC CIP audits.

N&ST consultants will ensure interpretations and documentation match the entity’s needs and expectations.

“WILL MY CVA PASS A NERC CIP AUDIT?”

No two Cyber Vulnerability Assessments are the same

One Key to Success:
Know what and where to document CVA notes and results for the NERC CIP audit.
Every CVA begins with the identification and collection of baseline information. While this baseline information is required evidence for the NERC CIP standards under their respective sub-requirements, many times this information is not stored in a central location. Depending on whether the CVA to be executed is for CIP 005 R4 or CIP 007 R8, N&ST senior consultants will ask the right questions to ensure that all baseline information needed is provided, such as:

- Do the firewall rulesets and/or router/switch access control lists, for access points to each electronic security perimeter (ESP), have justifications listed?
- Do the system ports and services lists for applicable cyber assets include justifications for each? For all IP protocols, including TCP and UDP?
- Do the shared and/or default account lists for access points to each ESP and applicable cyber assets include those for the operating system and all applications? Including both local and centralized accounts?

Proper and timely execution of the CVA is dependent on the baseline information being complete and available at the start of the engagement.

**OPTIONS TO COLLECT CURRENT ENVIRONMENT INFORMATION**

**Direct Collection:**
This method requires having logical access to the cyber assets to extract the information needed using either command-line interface commands or navigating through the cyber asset’s graphical user interface. The benefit of using this method includes assurance that the information collected is accurate and complete. The cost, however, is that this method is time consuming as each cyber asset must be accessed individually.

*Examples of direct information collection include:*

- Commands such as `netstat` to extract a cyber asset’s listening ports,
- Access to *Users* and *Groups* lists in the operating system’s settings, and
- Access to network device firmware configuration to identify SNMP settings.

**Active Collection:**
This method requires having remote access to the cyber assets to extract the information needed using third-party tools. The benefit to this method includes efficiency in that the information can be collected in batches. The cost, however, is that if it is not executed correctly, there is a risk the information may be incomplete.

*Examples of active information collection include:*

- Using a port scanner to identify a cyber asset’s listening ports,
- Using an enumeration tool to collect user lists and group lists, and
- Using an SNMP browser to verify community strings.