September 10, 2015

Presenter Responses to Attendee Questions
NERC CIP-007-5 Patch Management: Factors for Success

NOTE: The following are responses by the webinar presenters to questions submitted online during the webinar. None of the responses below should be interpreted as compliance guidance. Only your Regional Entity can provide authoritative compliance guidance; we recommend you discuss all questions with them.

Are we entitled to run Functional Testing on Mitigation Plans?

There is no requirement in CIP-007 V5 for testing of mitigation plans. It would be a best practice to run functional testing prior to the implementation of mitigation plan.

Do you have any experience with using commercially available software to perform the "queries" of patch levels for systems on Windows OS?

Yes, Foxguard has extensive experience querying various Windows operating systems for both version and patch level of the operating system as well as installed software.

Is there a mitigation plan template out there that can be used as a starting point?

Several of the regions maintain mitigation plan forms that contain the requirements necessary for a mitigation plan. Section 6.2 of the CMEP also sets forth the information that must be included in a mitigation plan. Please email Karl (karl[at]energysec.org) if you would like an example of a template.

What do you do when you have several paths forward. Such as Checkpoint R75 and R79 or Windows 2008 and 2010?

Have a documented process and follow it.

CIP V5 requires access to devices via an intermediate system. Does FoxGuard work through intermediate systems to scan the devices for versions?

This requirement pertains to interactive remote access. Foxguard does not need this access to run a patch management program. Generally the scanning is done locally to the site, not remotely, but Foxguard can engineer the solution you require.

How will be managed that process when using Cisco component that is based on IOS version and not patches?

IOS version that has a security component must be evaluated for applicability in your environment. Cisco security “patches”, are included in the firmware IOS version, so if the security measure is required, the firmware, IOS version, will be upgraded. Many plant devices are similar in that “patches” are not published separately.

Are there patch management providers that will track non-standard products such as nmap, putty, wireshark - just to name a few?

If in your inventory of assets to be used for patch management and you employ a patch aggregator these products should be part of the patch management program. Yes, those products and many more can be included in your service.

We have requirements to evaluate and create an action plan. Do manufacturers also have compliance requirements for releasing patches?

Manufacturers are not under the jurisdiction of NERC CIP. Manufacturers may have their own internal requirements but not mandatory compliance requirements.

Normally SCADA vendors do not test firmware updates, if a vendor do not test and we have a firmware update from the Vendor Source do we really need to apply this patch? Or create a mitigation plan for it?

If a security related firmware update then the update needs to be evaluated for your environment. You will need to determine if the patch applies to your environment and if so either deploy the patch or create/modify a mitigation plan.