MARCH 2015 ENERGY PROVIDER COMMUNITY (EPC) MEETING

Date	**3/24/2015**
Time Start-End	**2:00-3:00 PM**
Attendees	Landon Roeder (NESPower) Leslie DeAnda (PG&E) Steve Sage (Project Performance Company) Mike Prescher (Black & Veach) Irene Gasko (Florida Power and Light) Ralph King (EPRI) Nadya Bartol (UTC) Jim McCarthy (NCCoE) Don Faatz (NCCoE) Harry Perper (NCCoE)

Discussion

- Jim McCarthy reviewed the status of the IdAM Use Case build. All core IdAM products have been installed. Integration among products begins this week with RSA IMG and Alert Enterprise Guardian. The current IdAM build schedule is:
  - March 27, 2015 – Complete core IdAM product installation
  - April 15, 2015 – Complete initial integration of IdAM products
  - May 15, 2015 – Draft practice guide provided to EPC for review and comment
- Meeting participants asked if the IdAM integration is dependent on specific products.
  - No, the IdAM integration is dependent on specific capabilities, identity management workflow, an identity store, and identity / access provisioning not specific products. Two different instances of identity management workflow and identity store are being built, one based on RSA products and one based on CA products. Both of these depend on the Alert Enterprise product to provision Industrial Control System devices. Alert Enterprise is the only IdAM CRADA partner that provides ICS provisioning capabilities, however, there may be other products that could provide this capability.
- Meeting participants asked if IBM was an IdAM CRADA partner as IBM has products that might provide ICS provisioning capability.
  - IBM is not an IdAM CRADA partner, however NCCoE has had discussions with IBM.
- The April EPC meeting will be joint meeting with the IdAM build team. The date of that meeting is still to be determined.
- Jim McCarthy reminined EPC members that NCCoE will hold an Energy Sector Situation Awareness workshop on Monday afternoon, April 20th, in San Francisco, CA during the RSA conference. All EPC members are invited to attend. If possible, NCCoE will offer remote workshop participation via WebEx. Jim McCarthy will provide additional details once finalized.
  - Meeting participants noted that some RSA conference attendees will not be arriving in San Francisco until Monday evening and will be unable to attend the workshop
- NCCoE presented three Situation Awareness scenarios that combine information from physical security monitoring, cybersecurity monitoring, and operational monitoring. These scenarios are candidates for guiding work on the NCCoE Energy Sector Situation Awareness Use Case. EPC members were asked to comment on the relevance of each scenario to their organization.
  - In the first scenario, gunshots were detected at a substation and power flow at that substation was interrupted. Personnel in the area of the substation were notified of the threat via text messages on their phones. Energy operations was made aware of the threat so employees responding to the power interruption would be aware of the potential danger.
    - Meeting participants observed that personnel in the area of the substation when shots were fired would likely be very aware of the threat. Further, notification via text message, which could cause an audible announcement from a cell phone, would put those personnel in additional danger by disclosing their location. Text message notification seemed best suited to personnel who were not already at the substation but needed to know about the threat.

  - In the second scenario an engineer performs remote management of SCADA devices. Policy requires this remote management be done from the energy operations center. However, a check of physical access logs indicates the engineer is not in the energy operations center. This triggers a series of response actions by physical security, cybersecurity, and operations.
    - Meeting participants explained that, while policy might require remote management from the energy operation center under normal circumstances, during emergencies this requirement would likely be suspended.
    - Meeting participants noted that there is ongoing discussion across the energy sector about remote SCADA management techniques. Some have suggested the need to be able to 'maintain SCADA from the bedroom at 3:00 AM.' There are many different opinions and policies regarding remote SCADA management.
    - Meeting participants suggested considering a variant of the scenario where remote SCADA management is permitted from mobile devices.
  - In the third scenario an energy operations center dispatcher is investigating the cause of a tripped relay at a substation. The dispatcher uses a combination of SCADA, IT, and physical security log data to determine if the event is the result of a physical breach or a cyber attack.
    - Meetings participants expressed concern that examining this data could be time consuming and affect response time. Automated analysis would need to be employed to assist the dispatcher.
    - Meeting participants explained that, while relay trips are a common event, Situation Awareness software may not be able to provide meaningful assistance to dispatchers as the number of causes and relationships among causes and responses is very large – larger than is common in IT. The diversity of networks in the power sector could require specific event correlation capabilities for each event type such as a relay trip.
    - Some particpants felt that event correlation might still be useful to identiy attempts at deception wherein, for example, a physical attack at one substation is used to divert attention from a cyber attack at another substation.
- Jim McCarthy asked participants if events such as weather conditions and first-responder actions should be included in situation awareness.
  - Meeting participants felt that existing operations procedures and existing coordination with outside groups adequately addresses this and it would not be needed in the situation awarenss use case.
  - Meeting participants commented that when you start defining situation awareness, you may not know all the events and conditions that should be handled. Utility companies are beginning to combine their disaster recovery activities across silos to get better response.
  - Meeting participants observed that situation awareness needs to capture the "seeds" that may grow into events/incidents.
- NCCoE requested participants consider how converged situation awareness information should be presented to the different silos. Physical security monitoring, cybersecurity monitoring, and operational monitoring have existing presentation capabilities for the conditions they monitor. Converged situation awareness information needs to be presented in a way that enhances current capabilities.

Conclusion/Closing Notes or Need to Follow Up