Final Technical Report

PROJECT BOEING SGS

Contract ID: DE-OE0000191

Project Type: Regional Demonstration

Revision: V2

Recipient:

The Boeing Company

Principal Investigator:

Thomas E. Bell

thomas.e.bell@boeing.com

314-233-7055

December 10, 2014

TABLE OF CONTENTS

1. Executive Summary

Boeing and its partner, PJM Interconnection, teamed to bring advanced “defense-grade” technologies for cyber security to the US regional power grid through demonstration in PJM’s energy management environment. Under this cooperative project with the Department of Energy, Boeing and PJM have developed and demonstrated a host of technologies specifically tailored to the needs of PJM and the electric sector as a whole. The team has demonstrated to the energy industry a combination of processes, techniques and technologies that have been successfully implemented in the commercial, defense, and intelligence communities to identify, mitigate and continuously monitor the cyber security of critical systems. Guided by the results of a Cyber Security Risk-Based Assessment completed in Phase I, the Boeing-PJM team has completed multiple iterations through the Phase II Development and Phase III Deployment phases. Multiple cyber security solutions have been completed across a variety of controls including: Application Security, Enhanced Malware Detection, Security Incident and Event Management (SIEM) Optimization, Continuous Vulnerability Monitoring, SCADA Monitoring/Intrusion Detection, Operational Resiliency, Cyber Range simulations and hands on cyber security personnel training. All of the developed and demonstrated solutions are suitable for replication across the electric sector and /or the energy sector as a whole.

Benefits identified include:

- Improved malware and intrusion detection capability on critical SCADA networks including behavioral-based alerts resulting in improved zero-day threat protection
- Improved Security Incident and Event Management system resulting in better threat visibility, thus increasing the likelihood of detecting a serious event
- Improved malware detection and zero-day threat response capability
- Improved ability to systematically evaluate and secure in house and vendor sourced software applications
- Improved ability to continuously monitor and maintain secure configuration of network devices resulting in reduced vulnerabilities for potential exploitation
- Improved overall cyber security situational awareness through the integration of multiple discrete security technologies into a single cyber security reporting console
- Improved ability to maintain the resiliency of critical systems in the face of a targeted cyber attack of other significant event
- Improved ability to model complex networks for penetration testing and advanced training of cyber security personnel

2. Introduction

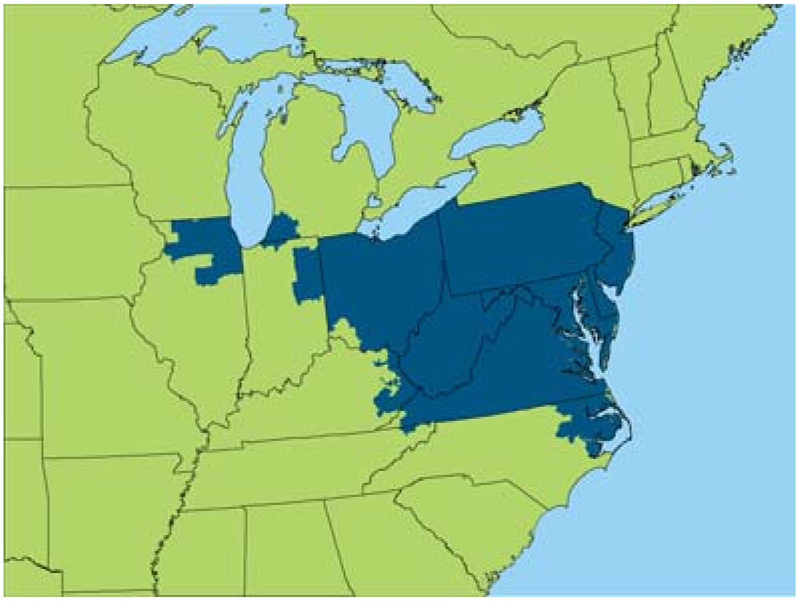
This document represents the Final Technical Report for the Project Boeing SGS Regional Demonstration. Under a cooperative agreement with the Department of Energy, Boeing and its partner, PJM Interconnection, teamed to demonstrate advanced technology solutions focused on cyber security in an energy management environment on the US regional power grid. The team has successfully tailored, and demonstrated to the energy industry a combination of processes, techniques and technologies that have been successfully implemented in the commercial, defense, and intelligence communities to identify, mitigate and continuously monitor the cyber security of critical systems.

As shown in Table 1, PJM's service territory spans all or part of 13 states serving over 60 million people. Figure 1 shows the geographical boundaries of the project region ("Project Region"). Table 1 shows specific information regarding PJM's territory, including applicable NERC reliability regions. All the solution candidates developed and demonstrated on this project have the potential for replication across the entire bulk electric system for the benefit of improved cyber security and Bulk Electric System (BES) reliability.

Table 1 - Project Boeing SGS Service Territory

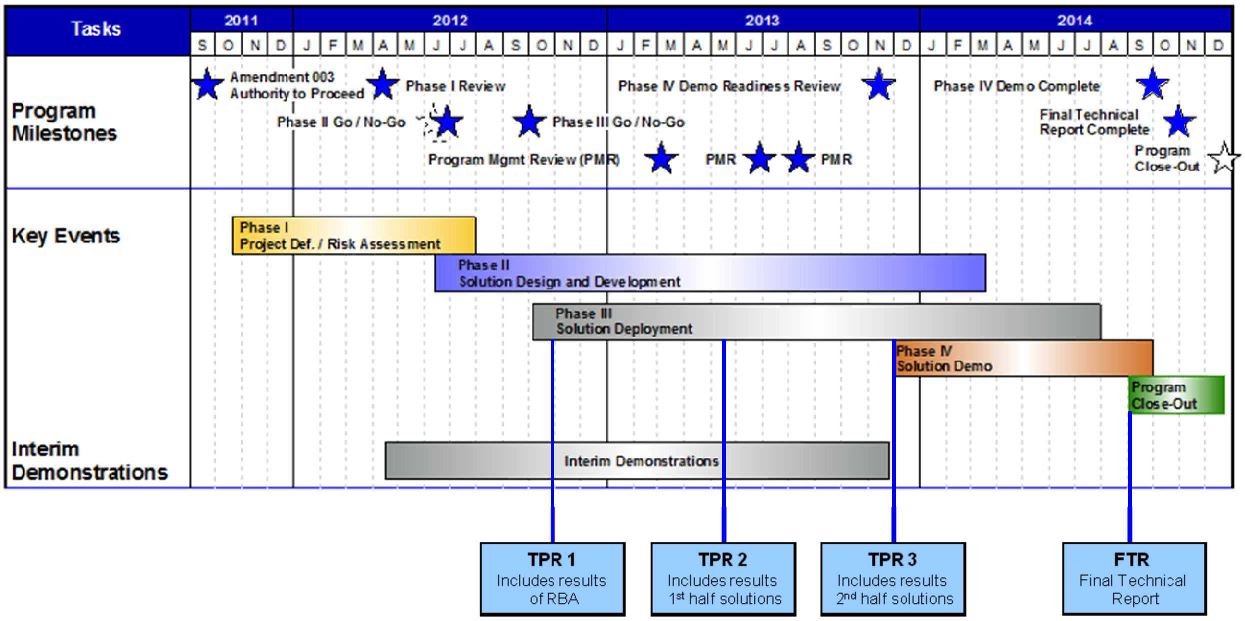
Name	Overview	Region (Square Miles)	Region (States)	Reliability Regions*	Population Served	Peak Demand Total Generation Capacity (MW)
PJM Interconnection	RTO that coordinates movement of wholesale electricity (*About PJM*)	214,000	All/part of 13 states: DE, IL, IN, KY, MD, MI, NJ, NC, OH, PA, TN, VA, WV, DC	RFC SERC	61 million	163,848 185,600

Figure 1 - Project Boeing SGS Service Territory



This project was managed and executed as illustrated in the project schedule shown in Figure 2. The project initiated with the essential Cyber Security Risk Based Assessment performed in Phase I, followed by multiple iterations of solution design, development and deployment in Phases II and III. Solution development and deployment was undertaken in a serial-parallel fashion consisting of multiple iterations of specific candidate solutions designed to improve cyber security control posture against risks uncovered during the Phase I Risk Assessment.

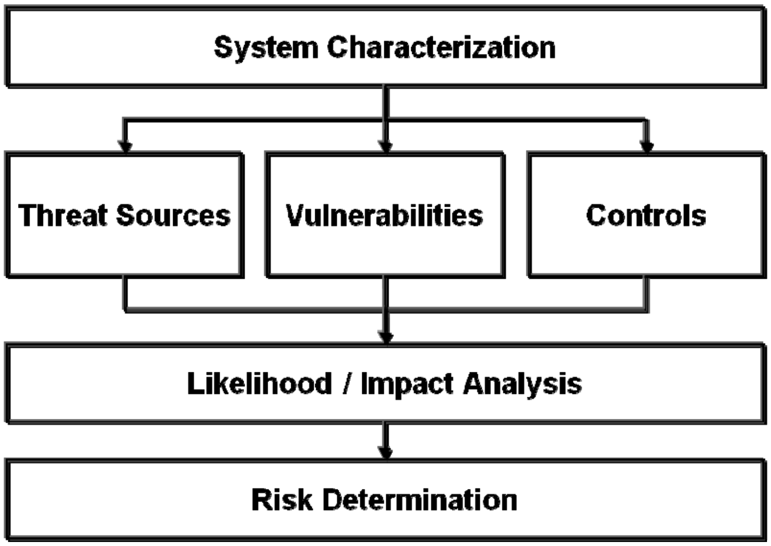
Figure 2 - Project Boeing SGS Integrated Schedule



3. Cyber Security Risk-Based Assessment

An initial Cyber Security Risk-Based Assessment was completed to determine cyber security risks to the PJM network / information system that supports the regional Bulk Electric System. Risk management of the PJM information system is essential to protecting cyber assets and thus PJM's overall mission. The risk-based assessment process identifies threat sources, vulnerabilities, and existing security controls. By pairing threat sources with vulnerabilities while considering the existing control posture, one can establish the likelihood and impact of an enterprise's true risk exposure, and begin to address solution development to reduce specific risks to an acceptable level. This section summarizes the Phase I Risk Assessment as identified in Figure 3. The scope of this assessment was constrained to high-value PJM information systems and provided the baseline for remediation efforts.

Figure 3 - Cyber Security Risk-Based Assessment Process Overview



Methodology

The risk assessment adhered to NIST Special Publication 800-30 (Risk Management Guide for Information Technology Systems) by executing each of the eight defined steps while tailoring step details for the energy sector.

Step 1 determined the portion of the PJM system to be assessed which resulted in focusing the data collection and assessment to the PJM Identified high-value systems and followed by a further narrowing to three high-value systems and their support systems.

Step 2 defined seven potential human threat-sources in two groupings: *external* (nation-state, terrorist, industrial spy/organized crime, hacktivist/hacker) and *internal* (employee, member, and vendor). The assessment focused on human threat-sources as opposed to natural and environmental threat-sources due to resource constraints and because PJM policies, standards and procedures already mitigate natural and environmental threats.

Step 3 defined applicable vulnerabilities as the 52 vulnerability categories and associated definitions in NISTIR-7628 (Guidelines for Smart Grid Cyber Security, Vol 3). This set is considered energy sector-applicable and comprehensive because it includes vulnerabilities related to policy, software/firmware, platforms, and networks. In addition, step 3 identified specific PJM vulnerabilities which were also associated with each of the 52 categories and applied in following steps.

Step 4 identified the current PJM security controls that apply to high-value systems. These controls were identified within PJM's policy, standards, and procedure documents (70 of 140 were considered applicable and reviewed). Each PJM control was associated with one of the 205 controls in the well-known standardized set from NIST SP800-53. Each standardized control was associated with one or more vulnerability categories in Step 3.

It is the 364 (7x52) pairs of threat-sources and vulnerabilities from steps 2 and 3 and associated controls in step 4 that formed the threat space for the risk evaluation.

Step 5 assigned a likelihood rating to each threat (a combination of a threat-source and vulnerability category mitigated by known controls). At the highest level, the likelihood rating is a subjective judgment of how likely a threat is to be successful against one of the three high-value systems. A modified Open Web Application Security Project (OWASP) methodology was used to determine the likelihood rating (range 0-9) where larger values represent a more likely occurrence.

Step 6 assigned an impact rating to each threat. Similar to the likelihood rating, the impact rating is an estimate of the likely damage if the threat was successful against one of the three high-value systems. A modified OWASP methodology was also used to determine the impact rating (range 0-9).

Step 7 used the likelihood rating (step 5) and impact rating (step 6) as an indicator of risk for each threat. This assessment has categorized risk into four levels: low, medium, high, and top high.

Step 8 initiated remediation response through new or modified security controls to address risks identified through this process.

Step 9 documented results.

Use of Automated Tools

Along with information gathered by Boeing during interviews with PJM Subject Matter Experts (SMEs), the deployment of automated security analysis tools contributed to the system characterization (Step 1) and vulnerability identification (Step 3) steps. For example one such tool automatically mapped network access by analyzing network device configurations, including routers, firewalls and load-balancers and then correlated network access with the findings of vulnerability assessment scans to help make better network security decisions. Another valuable tool, the Boeing Enterprise Network Sentinel (ENS) tool was also used to help identify vulnerabilities (Step 3) in the PJM information system. ENS detects malicious activity occurring within the network during any of the four phases of the typical threat life-cycle:

- Phase 1 – **Reconnaissance**: the attacker characterizes the targeted network/information system both from an external and internal viewpoint
- Phase 2 – **Intrusion**: malware attempts to compromise specific elements of the network/information system
- Phase 3 – **Communications Establishment**: malware will callback from a compromised internal host to an external command and control server
- Phase 4 – **Suspicious Data-In-Motion/Exfiltration**: unauthorized data is moved either internal to or exfiltrated from the network/information system

Risk Evaluation

Mapping potential threat actors to potential vulnerabilities resulted in specific risks being identified for potential mitigation. After analyzing the impact and likelihood values for all potential threats, Top High risks were identified. Few threat-vulnerability pairs are indicated in the "Low Risk" category due to the project focus on critical systems.

Guided by the risk assessment findings and project resources, the project team determined specific solution development activities likely to offer the greatest degree of security return relative to risk and investment. Key solution candidates included:

- Security Incident and Event Management (SIEM) Optimization
- Advanced Malware Assessment
- Continuous Vulnerability Monitoring
- Application Security
- SCADA Monitoring and Intrusion Detection
- Compass Operational Resiliency
- Cyber Range in a Box (CRIAB)

4. Security Incident and Event Management Optimization

Enhancing the level of situational awareness provided by a Security Incident and Event Management (SIEM) system typically results in highly cost effective security improvements. Ensuring that the SIEM is well integrated with all monitoring devices, event reports are well understood in context, and that operators are not overwhelmed with a large number of false or low priority events can significantly improve the value of an existing SIEM.

Initial SIEM solution development and deployment iterations focused on thorough identification and integration of all relevant monitoring devices on PJM high value systems and then achieving event correlation and reporting within their respective phase of the threat life cycle.
The life cycle of an Advanced Persistent Threat (APT) being defined as follows:

- **Phase 1 – Reconnaissance**: The period of time where the adversary is performing reconnaissance on your enterprise by doing port scans, social engineering, browsing external facing websites and servers, etc. In this period of time the adversary is also taking all the information gathered and is tailoring an attack to your defenses to achieve their objective.

- **Phase 2 – Intrusion**: The period of time where the adversary is launching its attack in an attempt to gain access to your enterprise and your data. Examples of this include spear phishing attempts, launching zero day exploits, handing out "free" infected thumb drives at conferences, attempting to hack into a system remotely, etc. –Note: Up until this point in time, the victim is not compromised; the stage is set so that they can be compromised. Also in this period of time the attack delivered executes and finds out whether or not compromise could in fact occur. Not all exploits are successful. Once compromise occurs, privileges are escalated, additional code is downloaded from the remote adversary, initial communication is established with the adversary, etc.

- **Phase 3 – Command and Control Establishment**: The period of time where the adversary and the compromised system communicate regarding its mission. Activities in this phase will include beaconing, scanning the infected system, scanning other internal systems, downloading of additional instructions from command and control server, etc.
- **Phase 4 – Mission Execution / Data-In-Motion / Exfiltration**: The period of time where the adversary executes its mission through the internally compromised machine. This includes data exfiltration, data or system corruption, launching pivot attacks, etc.

By aligning the security dashboard to register events within a specific threat phase, a significantly enhanced level of situational awareness is achieved when potential cyber security events are detected. Remediation action determination and timeliness improvements enhance the overall resiliency of the system(s) under protection.

System operational efficiency also improves as the inclusion of event filtering into the optimization process results in a security dashboard with significantly fewer, but more specifically targeted base events for evaluation. The resulting system realized a host of benefits:

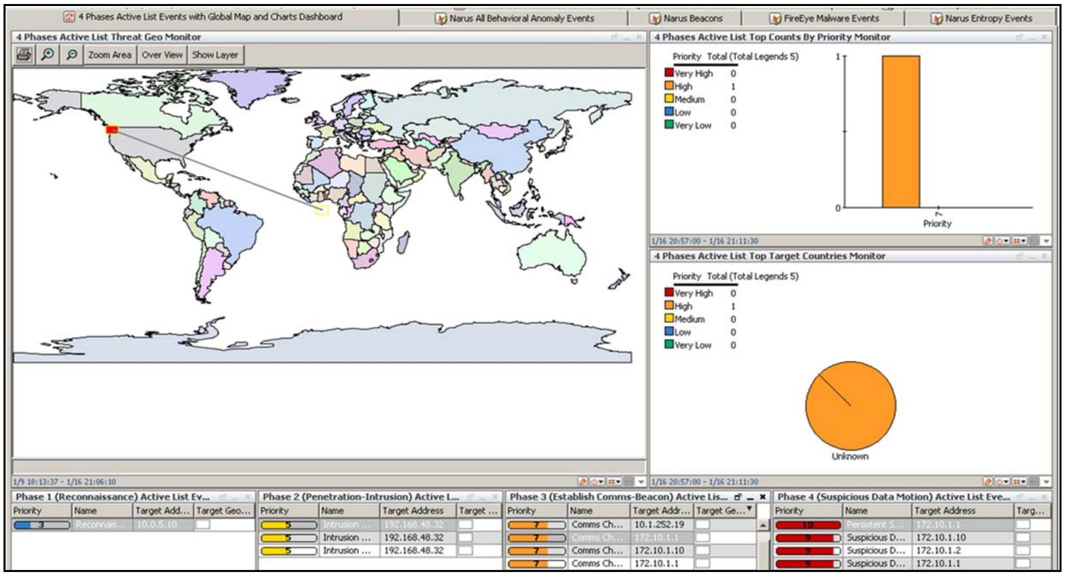
- improved operator efficiency due to a more manageable number of reported alerts
- better timeliness and precision due to reduction of noisy “false positive” alerts
- greatly enhanced situational awareness due to alert reporting within the APT threat life cycle

Achieving the above benefits required a full inventory of all potential monitoring devices and data connectors with special attention to ensuring error free parsing. As such, the SIEM has evolved into the primary cyber security situational awareness user console for information security monitoring. Figure 4 shows an example situational awareness dashboard with threat phase stratification of security alerts.

Follow-on design and development iterations served to advance the SIEM’s functional role as the security situational awareness console through the integration of reporting events from a wider set of security tools into the SIEM dashboard. Specifically, the following capabilities have been integrated and deployed to demonstrate the potential of expanded monitoring capability:

- Integrated reporting of continuous vulnerability scans down to layer three devices. This capability is described in Section 6 of this document.
- Integrated reporting of dedicated SCADA Intrusion detection and monitoring system. This capability is described in Section 8 of this document.

Figure 4 - Example SIEM Situational Awareness Dashboard


4 Phases Active List Events with Global Map and Charts Dashboard
Narus All Behavioral Anomaly Events
Narus Beacons
FireEye Malware Events
Narus Entropy Events
4 Phases Active List Threat Geo Monitor
Zoom Area
Over View
Show Layer
4 Phases Active List Top Counts By Priority Monitor
1
0
7
Priority
4 Phases Active List Top Target Countries Monitor
Unknown
1/9 18:13:37 - 1/16 21:06:10
1/16 20:57:00 - 1/16 21:11:30
1/16 20:57:00 - 1/16 21:11:30

4 Phases Active List Top Counts By Priority Monitor

Priority	Total (Total Legends 5)
🟥 Very High	0
🟧 High	1
🟨 Medium	0
🟦 Low	0
🟩 Very Low	0

4 Phases Active List Top Target Countries Monitor

Priority	Total (Total Legends 5)
🟥 Very High	0
🟧 High	1
🟨 Medium	0
🟦 Low	0
🟩 Very Low	0

Phase 1 (Reconnaissance) Active List Ev...

Priority	Name	Target Add...	Target Geo...
3	Reconnais...	10.0.5.10	□

Phase 2 (Penetration-Intrusion) Active L...

Priority	Name	Target Address	Target ...
5	Intrusion ...	192.168.48.32	□
5	Intrusion ...	192.168.48.32	□
5	Intrusion ...	192.168.48.32	□

Phase 3 (Establish Comms-Beacon) Active Lis...

Priority	Name	Target Addr...	Target Ge...
7	Comms Ch...	10.1.252.19	□
7	Comms Ch...	172.10.1.1	□
7	Comms Ch...	172.10.1.10	□
7	Comms Ch...	172.10.1.1	□

Phase 4 (Suspicious Data Motion) Active List Eve...

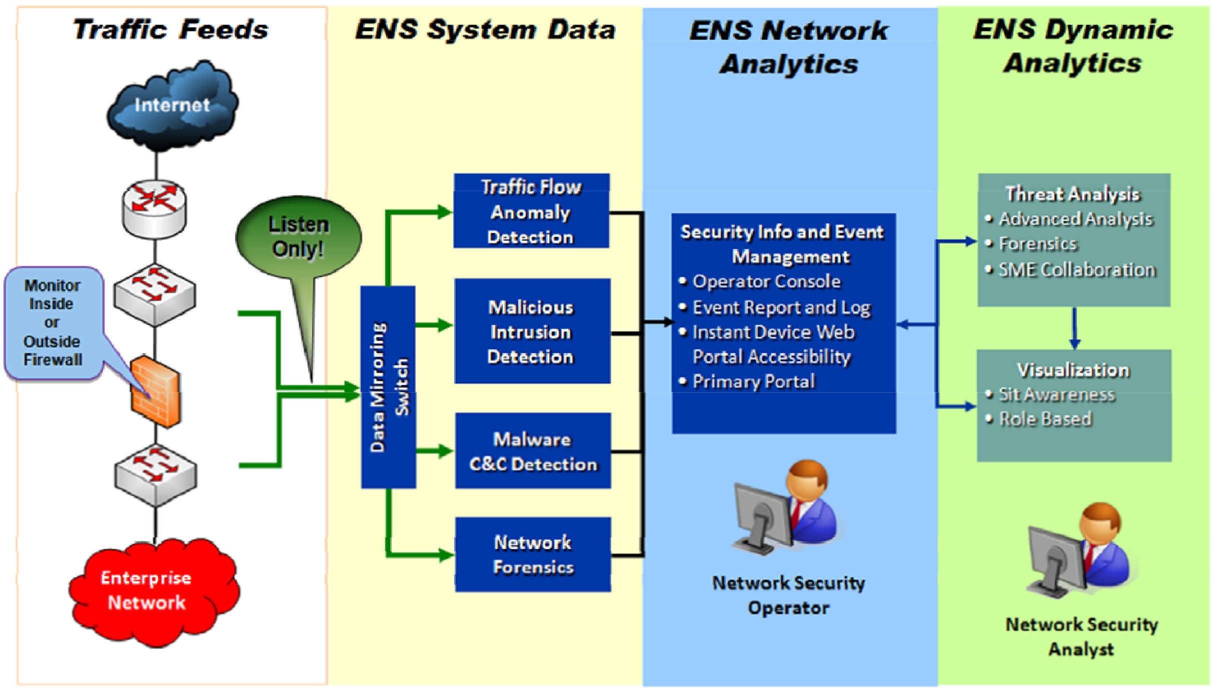
Priority	Name	Target Address	Targ...
10	Persistent S...	172.10.1.1	□
9	Suspicious D...	172.10.1.10	□
9	Suspicious D...	172.10.1.2	□
9	Suspicious D...	172.10.1.1	□

5. Advanced Malware Assessment

Several deployments of Boeing's advanced malware assessment capability, called Enterprise Network Sentinel were performed on various PJM network systems. The ENS scanned PJM's enterprise, energy management, and SCADA network environments for advanced threats. The integrated, non-signature based approach to network anomaly and malware detection, includes the ability to perform real-time forensics, advanced correlation of security events, and response work flow management. Results from these deployments were used to inform best actions toward maintaining the most robust defense possible against advanced zero-day and stealthy threats. Figure 5 illustrates an overview of the ENS capability used for these advanced malware assessments. This system may also be deployed as a continuous malware detection system with full integration into an enterprise SIEM.

Figure 5 - Advanced Malware Assessment Capability

Boeing ENS: Advanced Malware Assessment Capability



Traffic Feeds

Internet

Monitor Inside or Outside Firewall

Enterprise Network

Listen Only!

ENS System Data

Data Mirroring Switch

Traffic Flow Anomaly Detection

Malicious Intrusion Detection

Malware C&C Detection

Network Forensics

ENS Network Analytics

Security Info and Event Management
- Operator Console
- Event Report and Log
- Instant Device Web Portal Accessibility
- Primary Portal

Network Security Operator

ENS Dynamic Analytics

Threat Analysis
- Advanced Analysis
- Forensics
- SME Collaboration

Visualization
- Sit Awareness
- Role Based

Network Security Analyst

6. Continuous Vulnerability Monitoring and Management

Continuous Vulnerability Monitoring capability provides dynamic awareness of network vulnerabilities resulting from unforeseen network device configuration settings or inadvertent configuration changes that could pose a risk to a robust network security posture. Regular scanning prevents undesirable or unintended consequences resulting from architectural and operational changes by quickly detecting inadvertent or malicious system changes and enabling proactive response. This capability also facilitates effective patch management prioritization and verification.

The design, development and deployment of this capability at PJM consisted of designing the implementation architecture, deploying enhanced scanning tools, and then integrating new capability with legacy configuration management tools and scanners already in use by PJM.

Implementation at PJM resulted in successful demonstration of Layer 3 device scans capable of detecting network configuration changes in areas such as firewall settings, router or switch access control lists (ACLs), new device additions, as well as deviations from Best Practices.

The development effort also resulted in the integration of scan results to the SIEM dashboard for alert reporting to security operators, thus demonstrating the potential for enabling a greater level of situational awareness to security personnel and providing improved anomaly response time.

A few key “lessons learned” from the deployment are worth noting:

- Legacy devices may pose challenges to performing Layer 3 scans in a completely benign manner. If these devices are critical to the organization’s mission, then resource requirements to safely resolve these issues without negatively impacting operations may become significant.
- Determining optimal scanning frequency (daily, weekly, monthly) will likely be situation dependent based on the change dynamics and criticality of the subject network devices.
- Integrated vulnerability scans at the Layer 3 device level provide excellent network mapping and visualization capability which directly benefits overall network analysis capability.

7. Application Security and Application Security Maturity Model

Several iteration candidates fell under the broad topic area of Application Security. Following the results of the Phase I Risk Based Assessment, Application Security improvement opportunities were identified for prioritization to focus efforts for maximal security posture benefit. Prioritization of development action plans for Application Security leaves open the opportunity to proactively posture for future Application Security issues.

To best address Application Security issues, development of an Application Security Maturity Model specifically tailored for the unique requirements of the electricity sector was identified as a key need. Currently, electricity sector software is a mixed inventory of components acquired from external vendors and components created by internal development teams. Additionally, software acquired from vendors may be customized internally for the organization’s specific requirements. Given this mix, an appropriate maturity model needs to address both secure software development practices as well as secure software acquisition/procurement processes. This software mixture is typical of the vast majority of companies and organizations; therefore, the energy sector realized benefit from the similar maturity models and other tools that are available to industry. However, no single solution existed to meet the specific needs of the energy sector and multiple solutions create wasteful overlap and cumbersome implementation. The project undertook the effort to develop and test an Application Security Maturity Model tailored to the specific needs of the energy industry along with assessment and implementation guidelines.

To address the unique needs of the energy sector, the application security team considered nine existing maturity models and rated each candidate against eleven factors, or evaluation criteria, that a maturity model for the energy sector must address. These evaluation factors were derived based on the team’s collective experience in software development lifecycle, cyber security, and the requirements of energy sector organizations. Factors such as flexibility, tailor-ability, adaptability, and secure software development and procurement practices were used as the basis for evaluation. As a result, the application security team concluded that a hybrid Application Security Maturity Model derived from the Build Security In Maturity Model, version 4 (BSIMMv4) with augmentation and tailoring from three additional maturity models could form the basis of a robust Application Security model specifically targeted to the unique needs of the energy sector.

The resultant Application Security Maturity Model was tested and validated against PJM's needs and objectives through self-assessments and key personnel interviews. Application of this model will benefit not only PJM, but through potential replication, the electric sector as a whole.

8. SCADA Monitoring and Intrusion Detection

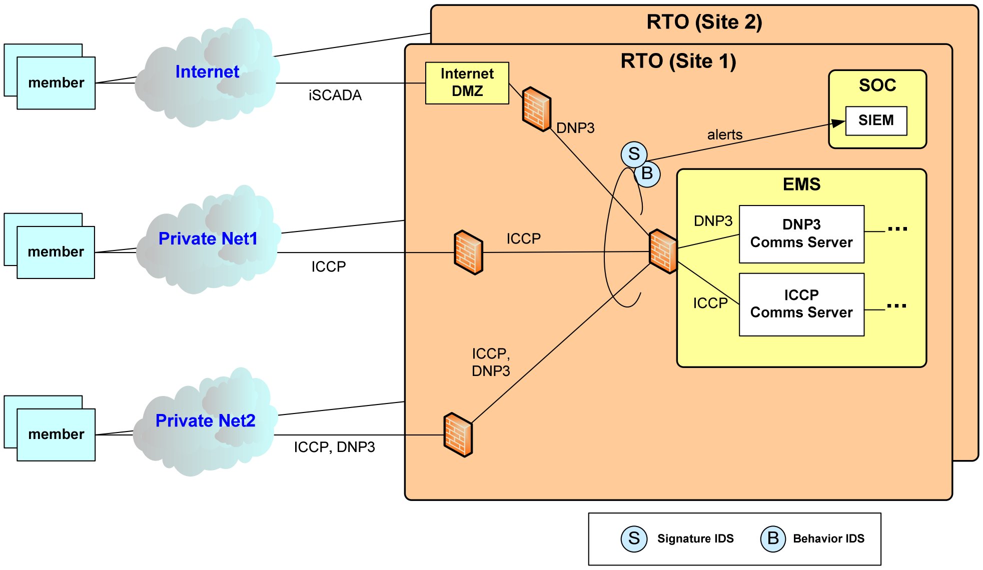
SCADA network monitoring and intrusion detection has been identified as a high value technology in the electric sector, and in general, across much of the energy sector. The maturity and availability of TCP/IP intrusion detection systems (both behavioral and signature based) has advanced rapidly in recent years, but few options exist for robust protection of SCADA networks. The objective of this solution candidate was to develop, deploy, integrate, and test robust SCADA Monitoring and Intrusion Detection System (SCADA-IDS) in PJM's representative electric sector environment.

The evolution of energy sector SCADA control systems from largely isolated, serial bus, control schemes to more interconnected TCP/IP protocols brings with it both opportunity and risk. As information systems become more interconnected, so does the potential access and risk of malicious exploitation of system vulnerabilities aimed at disrupting or degrading the performance of SCADA controlled devices. Effective intrusion prevention and detection is imperative to securing these SCADA systems and to maintaining a high level of security situational awareness which is critical to effectively mitigating or defeating an actual cyber attack.

Given the wide range of protocols used in SCADA applications, the SCADA-IDS must support a multitude of common industrial control system protocols. ICCP and DNP3 protocol compatibility was specifically developed for this implementation. Other compatible protocols include: OPC-DA, Modbus/TCP, IEC 60870-5-101/104, IEC 61850, MMS, RPC/DCOM, SMB/CIFS, and HTTP.

As depicted in Figure 6, a representative architecture was developed to serve as a template for solution development. Intrusion detection sensors positioned post firewall feed the SCADA-IDS where traffic content is screened for anomalies using both signature-based and behavioral-based detection techniques. Alerts generated by the SCADA-IDS are prioritized, sent to the SIEM, and presented to a security operator for disposition.

Figure 6 - SCADA Network and Monitoring Architecture

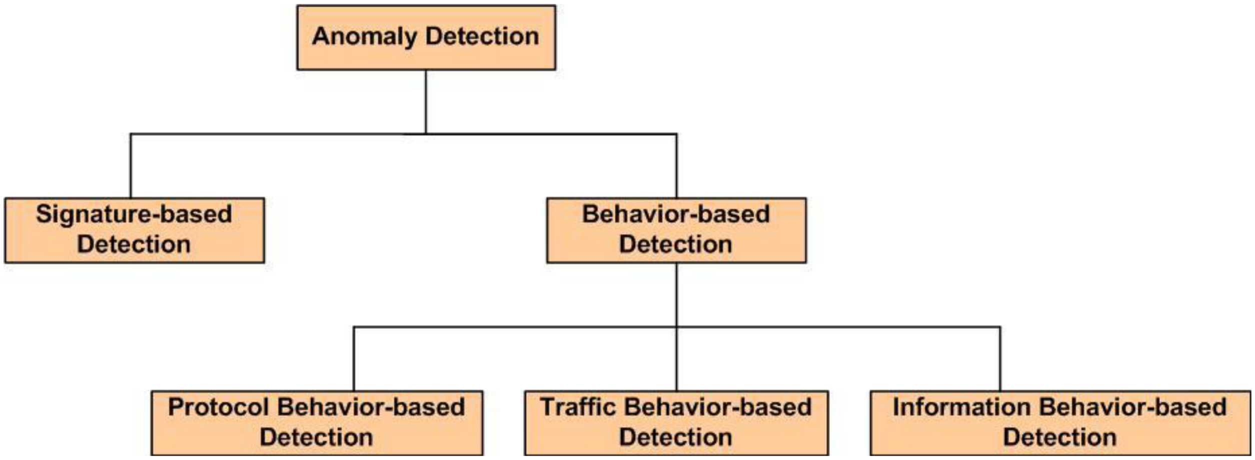


Given the general availability and maturity of signature based detection capability and the limited effectiveness of signature based defenses to zero day attacks, project requirements skewed largely toward implementing and testing complementary behavioral-based anomaly detection.

Anomaly Detection

Anomaly detection can be performed using many different detection techniques. Figure 7 illustrates an Anomaly Detection taxonomy and shows the relationship of many different techniques.

Figure 7 - Anomaly Detection Taxonomy


Anomaly Detection
Signature-based Detection
Behavior-based Detection
Protocol Behavior-based Detection
Traffic Behavior-based Detection
Information Behavior-based Detection

Signature-based techniques have been available for many years and provide the confidence to detect past known attacks. Once a vulnerability in a SCADA device has been identified, a traffic analyzer can continuously look for the set of traffic patterns (signature) to identify that exploits in the network traffic. Unfortunately, malicious actors have found ways to continuously change the traffic signature while still being able to execute the exploit and thus avoid detection. Signature-based techniques rely on vendors and vendor users to report vulnerabilities and their exploits. Often by updating the device with a patch, the vulnerability can be mitigated. However, updating SCADA devices can be problematic due to their 24x7 operation and the need to perform extensive testing before SCADA devices can be brought back on line.

Complementary to signature-based techniques are powerful behavior-based techniques that have the ability to detect abnormal traffic conditions and almost all of the signature-based exploits. Behavior-based detection suits SCADA systems well because the SCADA network traffic consists of very repetitive status and control messaging. These well-defined rhythms allow behavior-based techniques to detect small differences that indicate abnormal traffic indicative of malicious activity. Behavior-based techniques perform deep protocol inspection allowing inspection in multiple dimensions. Behavior-based detection comes in many forms but can be classified usually into one of the following categories:

- Protocol Behavior-based Detection
- Traffic Behavior-based Detection
- Information Behavior-based Detection

All these categories of behavior-based detection have been designed into the anomaly detection Sensor to provide alerts to suspicious behavior. Alerts generated by the SCADA-IDS are prioritized, sent to SIEM, and presented to the security operator for disposition.

The behavioral detection engine evaluates communication patterns, protocol specifics, message types, message fields, message values, and other parameters to detect anomalous activity patterns and then provides detailed alerts to systems security operators for in-depth analysis and timely response. The technology is self learning and can adapt to the complete range of legitimate network activity while detecting and alerting to real anomalies posed by advanced cyber attacks, human errors, or poor network configurations.

Integration to Enterprise SIEM

Integration of SCADA alert feeds into the SIEM provides situational awareness of monitored SCADA traffic and the health and performance of the detection system. Monitoring traffic using real-time displays enables more precise alerts across various categories (e.g. by member groups, geographical region, top-10 traffic sources, by protocol, by alert types, etc.). Invoking offline analyses tools enables a security analyst to investigate all details of an alert including the associated raw packet captured (PCAP) data. This capability is critical for determining response measures and /or further forensic analysis.

Operations and Testing

The SCADA-IDS has undergone testing in the PJM environment in order to refine operational configurations and end use system requirements. Given the need to test the SCADA-IDS against live threats without introducing risk to the PJM test environment, additional test facilities were required. To enable advanced testing and to further develop SCADA threat detection capability, Boeing has developed a SCADA network simulation / test bed where known SCADA exploits can be injected and evaluated in a controlled environment. New test cases can also be developed in this facility to identify and study heretofore unexploited SCADA vulnerabilities and develop remediation steps to prevent future risk of exploitation.

Non-routable Serial SCADA Network Intrusion Detection

The successful development and implementation of behavioral-based intrusion detection and monitoring for routable TCP/IP SCADA networks illuminated the fact that a significant percentage of SCADA networks remain on non-routable, serial networks. While time and resource constraints prevented a complete solution development and demonstration of non-routable serial SCADA networks, significant solution design and development was achieved through this project. As a result, the migration of this critical SCADA intrusion detection capability to non-routable serial networks is clearly feasible.

9. Compass Operational Resiliency Solution

Regardless of cyber defense posture, and proactive mitigation of known risks, no organization can ever be completely protected from a cyber attack or security breach. The Compass Resiliency Solution seeks to maximize an organization’s ability to fight through cyber or other disruptive events while maintaining maximum mission effectiveness.

An organization’s mission critical systems generally rely upon key resources comprised of people (knowledge), physical assets, and information systems. And while some ability exists to monitor and manage these resources discretely, the capability to understand the impact to an organization’s key mission functions as a result of health and status perturbations across these three fundament different domains is essentially non-existent. This is particularly true for complex organizations. The Compass Resiliency Solution provides contextual situational awareness of an organization’s health status as a function of critical resources across these three domains.

Figure 8 - Domains Impacting Mission Performance

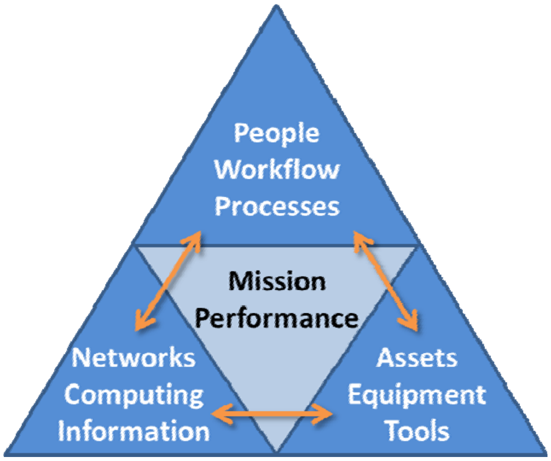
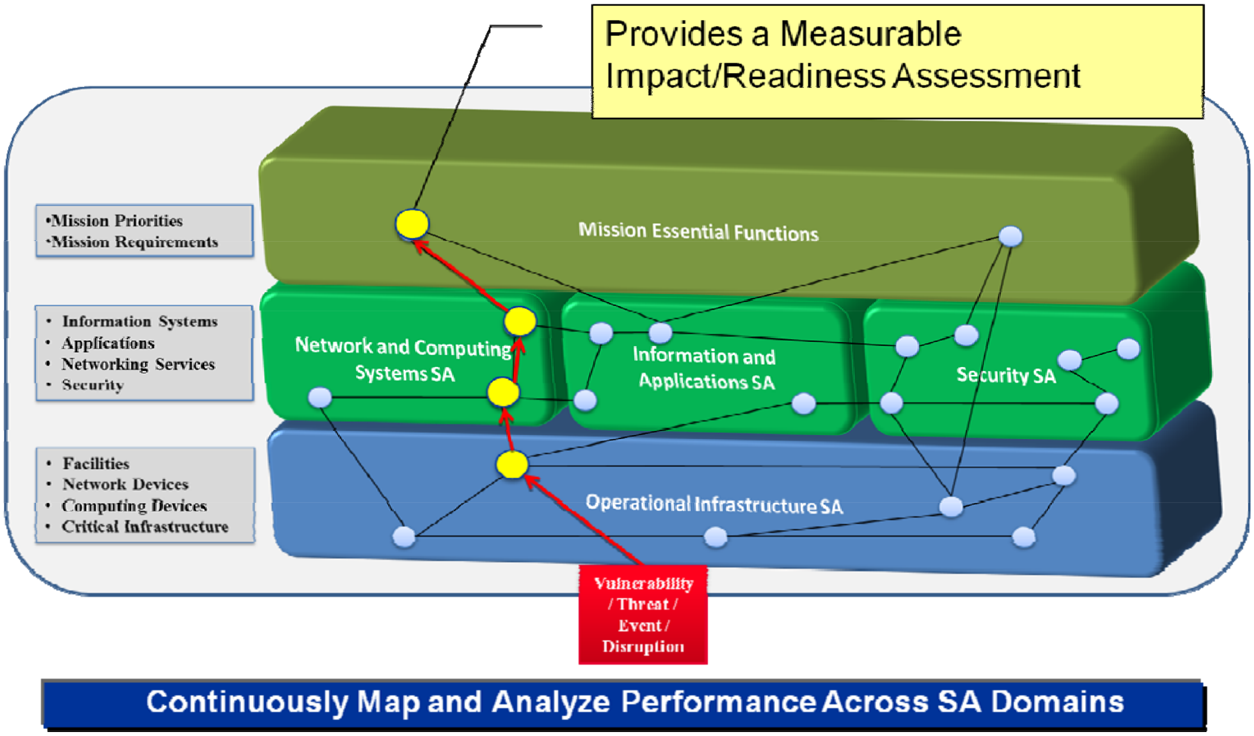


Figure 9 illustrates how the Compass Resiliency Solution integrates situational awareness across disparate domains to identify and alert to issues that may appear benign (outside of full contextual knowledge), but pose a real risk to mission performance, thus providing operators and analysts the opportunity to take proactive measures to ensure mission capability is not compromised.

Figure 9 - Compass Resiliency Solution Maps Vulnerability Paths to Essential Mission Functions



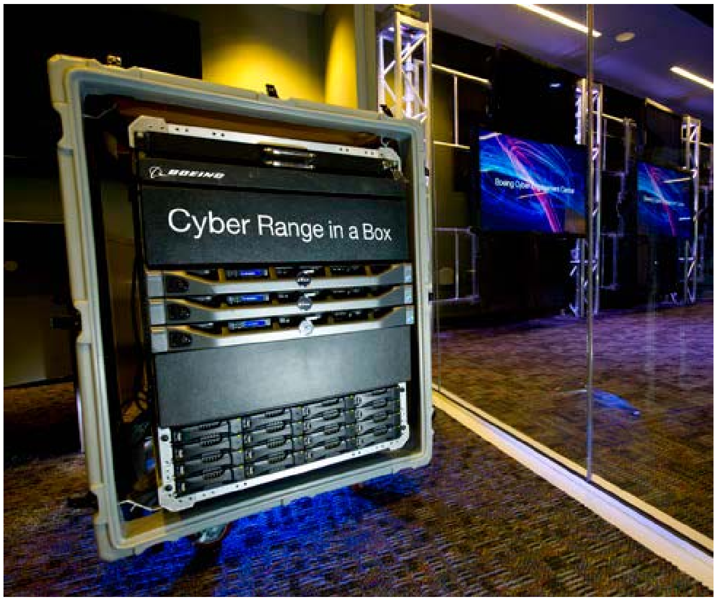
The Compass capability was prototyped at PJM to monitor the health and status of the key resources required for efficient and effective operation of energy markets. Operations and Security personnel viewed the same domain specific health and status data but contextualized to align to unique job functions, potential response actions, and criticality level.

While the prototyping exercise was successful, expanding the application of this capability across the enterprise would have required more time and resources than this project could accommodate. A complete mapping of all mission essential functions would further enhance the overall resiliency of the critical systems considered as part of this project.

10. Cyber Range in a Box (CRIAB)

Traditional network simulations used for testing and training rely upon basic network configurations, and lack the fidelity and relevance of an operational environment, and are not designed to scale for ever expanding and evolving cyber attack vectors. As part of this technology demonstration program, Boeing and PJM have considered various techniques and technologies aimed at testing cyber security solutions and training cyber security personnel in a safe yet realistic network environment.

Figure 10 - Cyber Range in a Box (CRIAB)

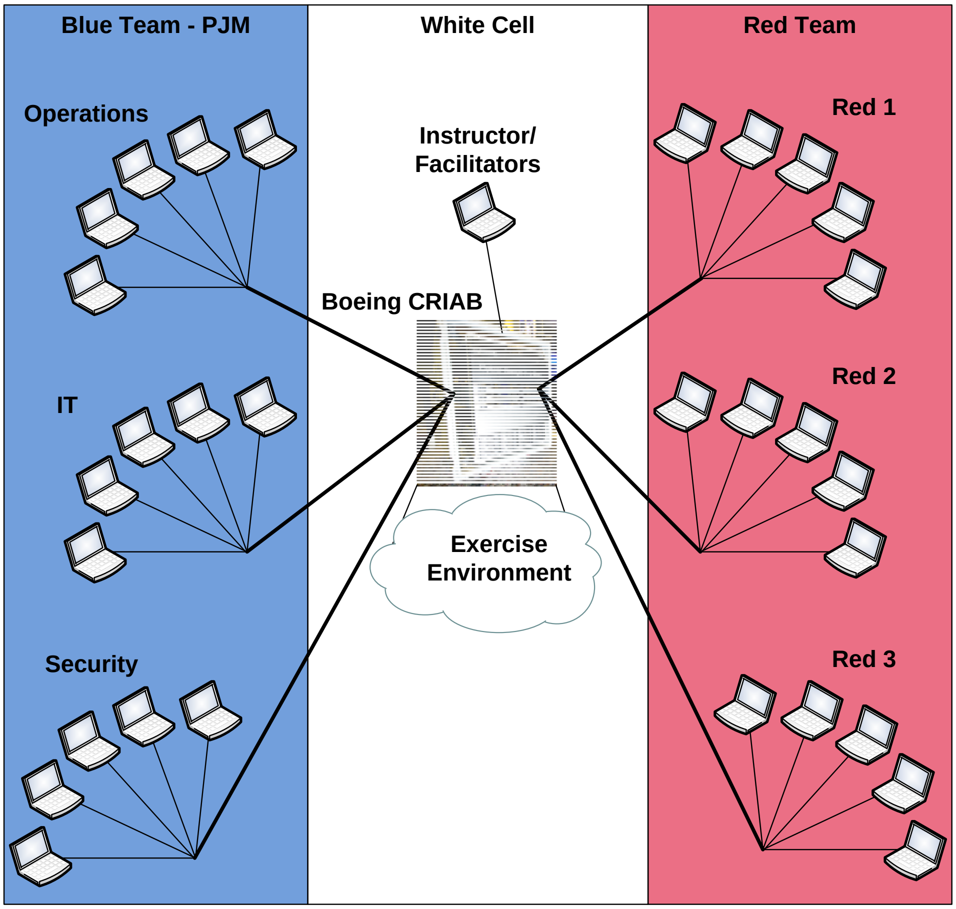


CRIAB is a compact system used to support the development, test and experimentation of cyber tools and techniques, as well as to train cybersecurity personnel. CRIAB allows modeling and simulation of complex missions and advanced threats for the creation of security solutions without putting real enterprise and operational networks at risk.

CRIAB facilitates efficient range construction and reuse through user-selectable fidelity settings for all cyber range elements. CRIAB supports the interface to external physical systems (computers, networking devices, etc.) allowing unique real-world network components to be included in the environment. The integrated Range Management Console provides CRIAB with centralized control over range operations and instrumentation. Complex network environments can be imported or are easily configured, archived for later reuse, and shared between CRIAB systems. The graphical user interface provides the flexible tools for network creation and reuse while facilitating accurate capture of simulation or training events.

Of particular relevance to this project is the capability CRIAB offers for training and experimentation, such as personnel training, threat mitigation rehearsal, and tool evaluation and improvement. Figure 11 illustrates an effective configuration for Red/Blue Team training using a mission-based training scenario to develop and measure proficiency in performing critical cyber security tasks. The training with PJM personnel consisted of a series of network attack / exploitation scenarios where the participants began with an understanding of the tools they would use during the day and then moved to hands on training to drill into tactics and techniques. The training provided a broad awareness of the tools and methods used by the "bad guys" along with mitigation and defense techniques required to protect targeted networks.

Figure 11 - Red/Blue Team Interactive Training Environment



11. Conclusion

The Boeing-PJM team has demonstrated to the energy industry a combination of processes, techniques and "defense-grade" technologies to better identify, mitigate and continuously monitor the cyber security of critical systems. Guided by the results of the Cyber Security Risk-Based Assessment completed in Phase I, the Boeing-PJM team completed multiple iterations through the Phase II Development and Phase III Deployment phases. Multiple cyber security solutions have been completed across a variety of controls as described in the preceding sections of this document. All of the developed and demonstrated solutions are suitable for replication across the electric sector and /or the energy sector as a whole. Direct benefits identified as a result of this project include the following:

- Improved malware and intrusion detection capability on critical SCADA networks including behavioral-based alerts resulting in improved zero-day threat protection
- Improved Security Incident and Event Management system resulting in better threat visibility, thus increasing the likelihood of detecting a serious event
- Improved malware detection and zero-day threat response capability
- Improved ability to systematically evaluate and secure in house and vendor sourced software applications
- Improved ability to continuously monitor and maintain secure configuration of network devices resulting in reduced vulnerabilities for potential exploitation
- Improved overall cyber security situational awareness through the integration of multiple discrete security technologies into a single cyber security reporting console
- Improved ability to maintain the resiliency of critical systems in the face of a targeted cyber attack of other significant event.
- Improved ability to model complex networks for perturbation testing and advanced training of cyber security personnel.

Grid level benefits resulting from this project include: improved electrical grid reliability through enhanced cyber security of critical systems, and improved grid resiliency through enhanced situational awareness and threat visibility enabling improved response measures to cyber attacks or other disruptive events.

<u>Boeing Technical Point of Contact:</u>

Jerry Horne, Chief Engineer
jerry.d.horne@boeing.com
(650) 316-3740

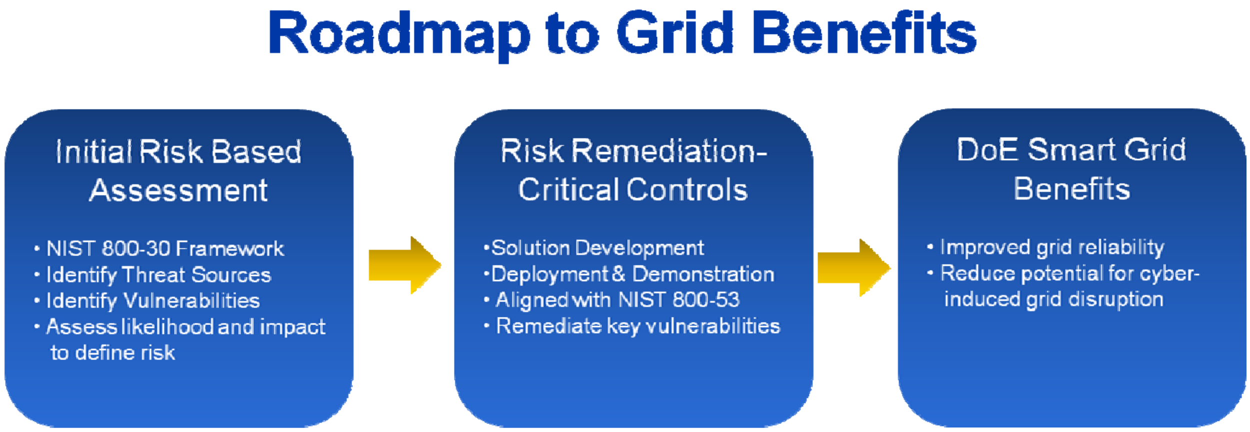
<u>PJM Technical Point of Contact:</u>

Steve McElwee, Chief Information Security Manager
steve.mcelwee@pjm.com
(610) 666-3194

Appendix A - Grid Level Benefits Summary

Enhanced protection of critical grid infrastructure from potential cyber-induced harm is a fundamental societal benefit realized through the execution of this project. Assessing the discrete cyber security risk to the electrical grid as a whole or even as a control region, such as that represented by PJM's control territory, is beyond the scope of this project. However, by focusing the project's cyber security risk-based assessment on PJM's critical systems, subsequent remediation efforts (both project funded and off-project funded) will ultimately address those vulnerabilities that are most critical to providing an effective level of cyber security for the electrical grid.

Figure A1 - Project Boeing SGS Linkage to Smart Grid Benefits



Roadmap to Grid Benefits

Initial Risk Based Assessment

- NIST 800-30 Framework
- Identify Threat Sources
- Identify Vulnerabilities
- Assess likelihood and impact to define risk

Risk Remediation-Critical Controls

- Solution Development
- Deployment & Demonstration
- Aligned with NIST 800-53
- Remediate key vulnerabilities

DoE Smart Grid Benefits

- Improved grid reliability
- Reduce potential for cyber-induced grid disruption

The key activities and outcomes of the Cyber Security Risk Based Assessment are depicted graphically in the first block of Figure A1. The risk assessment culminated in a risk matrix derived from the pairing of likely threat actors (sources) to identified critical asset vulnerabilities. The second block of Figure A1 depicts cyber security control remediation directed at identified vulnerabilities that have been the focus of solution developments and deployment undertaken by this project and described in this document. The final block depicts the Smart Grid Benefits of improved reliability and reduced potential for cyber-induced grid disruption that result both directly from activities funded as a result of this project, and indirectly, from activities funded outside of this project that result from findings of the project's risk based assessment. As shown in Figure A2, additional indirect benefits may also be realized across the electrical sector through opportunities to replicate the processes, tools, techniques and solutions developed on this Smart Grid demonstration project.

Figure A2- Smart Grid Benefit Impact Areas

Benefit Category	Benefit	Provided by Project?	Remarks / Estimates
Economic	Arbitrage Revenue (consumer)*	no	
	Capacity Revenue (consumer)*	no	
	Ancillary Service Revenue (consumer)*	no	
	Optimized Generator Operation (utility/ratepayer)	no	
	Deferred Generation Capacity Investments (utility/ratepayer)	no	
	Reduced Ancillary Service Cost (utility/ratepayer)	no	
	Reduced Congestion Cost (utility/ratepayer)	no	
	Deferred Transmission Capacity Investments (utility/ratepayer)	no	
	Deferred Distribution Capacity Investments (utility/ratepayer)	no	
	Reduced Equipment Failures (utility/ratepayer)	no	
	Reduced Distribution Equipment Maintenance Cost (utility/ratepayer)	no	
	Reduced Distribution Operations Cost (utility/ratepayer)	no	
	Reduced Meter Reading Cost (utility/ratepayer)	no	
	Reduced Electricity Theft (utility/ratepayer)	no	
	Reduced Electricity Losses (utility/ratepayer)	no	
	Reduced Electricity Cost (consumer)	no	
	Reduced Electricity Cost (utility/ratepayer)*	no	
Reliability	Reduced Sustained Outages (consumer)	yes	Potential for indirect measurement through avoidance of events
	Reduced Major Outages (consumer)	yes	Potential for indirect measurement through avoidance of events
	Reduced Restoration Cost (utility/ratepayer)	no	
	Reduced Momentary Outages (consumer)	yes	Potential for indirect measurement through avoidance of events
	Reduced Sags and Swells (consumer)	no	
Environmental	Reduced carbon dioxide Emissions (society)	no	
	Reduced SO_X, NO_X, and PM-2.5 Emissions (society)	no	
Energy Security	Reduced Oil Usage (society)	no	
	Reduced Wide-scale Blackouts (society)	no	

*These benefits are only applicable to energy storage demonstrations.

Appendix B - Risk Re-Assessment Report

Boeing Smart Grid Solution

Risk Re-Assessment Report

DOCUMENT NUMBER:	RELEASE/REVISION:	RELEASE/REVISION DATE:
	3.0	**October 23, 2014**

CONTENT OWNER:

Boeing SGS Team

All future revisions to this document must be approved by the content owner before release.

Executive Summary

Introduction

Boeing and PJM Interconnection partnered under a DoE-sponsored program to determine cyber security risks to the PJM information system that supports the regional Bulk Electric System (BES) operated by PJM. Cybersecurity risk management of the PJM information system is essential to protecting cyber assets and thus PJM's overall mission. The initial cybersecurity risk assessment identified risks and proposed steps to reduce risk to an acceptable level to three high-value PJM systems. The initial report ranked-potential cybersecurity risks as low, medium, high, and top high.

In the last two years PJM Interconnection and Boeing have implemented risk reduction measures to improve the risk posture for most of the identified top high risks. Some of the security measures were pursued by PJM independent of the DoE project as part of their overall security plan. This executive summary presents the results of re-assessing the top high risks. Although this re-assessment and associated executive summary is for the DoE project, PJM has since augmented its corporate-level risk assessment process to include periodic assessments of its cyber systems. In that sense, this summary is an interim report of an on-going process.

Methodology

The methodology used for the re-assessment was the same as the one used for the initial assessment. The initial risk re-assessment adhered to NIST Special Publication 800-30 (Risk Management Guide for Information Technology Systems) by executing each of the nine defined steps while tailoring step details for the energy sector. The re-assessment methodology focused on updates for only the top high risks.

Step 1 determined the portion of the PJM systems to be assessed which resulted in focusing the assessment on three high-value systems and their support systems. Narrowing the focus allowed trading breadth for a deeper investigation of security defense features. Even though this approach focused on three systems, the assessment should apply to many of the uninvestigated systems because these systems are part of the same architecture to which many of the same controls apply.

The re-assessment determined that there were no relevant non-security changes to the three high-value systems. There were cybersecurity control changes which are listed in step 4.

Step 2 defined seven potential human threat-sources in two groupings: *external* (nation-state, terrorist, industrial spy/organized crime, hacktivist/hacker) and *internal* (employee, member, and vendor). The top high risks only contained a subset of the seven sources. The assessment focused on human threat-sources as opposed to natural and environmental threat-sources due to resource constraints and because PJM policies, standards and procedures already provide mitigation of natural and environmental threats. The final list of human threat-sources was based on inputs from government documents, energy sector documents, and PJM operations.

The re-assessment determined that no changes were necessary for this step.

Step 3 defined applicable vulnerabilities as the 52 vulnerability categories and associated definitions in NISTIR-7628 (Guidelines for Smart Grid Cyber Security, Vol 3). For the re-assessment only 10 vulnerability categories were required based on their applicability to the top high risks. This set is considered energy sector-applicable and comprehensive because it includes vulnerabilities related to policy, software/firmware, platforms, and networks. In addition, step 3 identified specific PJM vulnerabilities which were also associated with each of the 52 categories and which applied in following steps.

The re-assessment determined that no changes were necessary for this step.

Step 4 identified the current PJM security controls that apply to high-value systems. These controls were identified within PJM's policy, standards, and procedure documents (70 of 140 were considered applicable and reviewed). Each PJM control was associated with one of the 205 controls in the standardized set from NIST SP800-53. Each standardized control was associated with one or more vulnerability categories in Step 3.

It is the 364 (7x52) pairs of threat-sources and vulnerabilities from steps 2 and 3 and associated controls in step 4 that forms the threat space for the risk evaluation. For the re-assessment the team revisited new controls implemented since the initial assessment.

Since the initial assessment report, 14 new or improved cybersecurity controls have been implemented at PJM Interconnection reducing the risk level for most of the original top high risks.

Step 5 assigned a likelihood rating to each threat (a combination of a threat-source and vulnerability category mitigated by known controls). At the highest level, the likelihood rating is a subjective judgment of how likely a threat is to be successful against one of the three high-value systems. A modified OWASP methodology was used to determine the likelihood rating (range 0-9) where larger values represent a more likely occurrence. The rating is a composite of 8 factors. Four factors are threat-source related (skill level, motive, opportunity, and size) and another four factors are vulnerability related (ease of discovery, ease of exploit, awareness, and intrusion detectable). The composite factor values are averaged to obtain the overall likelihood rating.

The re-assessment determined that four likelihood factors (skill level, motive, size, and awareness) needed no re-estimation. All other factors were re-estimated for the top high risks.

Step 6 assigned an impact rating to each threat. Similar to the likelihood rating, the impact rating is an estimate of the likely damage if the threat was successful against one of the three high-value systems. A modified OWASP methodology was also used to determine the impact rating (range 0-9). The rating is also a composite of 8 factors. Four factors are technical security related (loss of confidentiality, loss of integrity, loss of availability, and loss of accountability) and another four factors are business related (market damage, reputation damage, non-compliance, and BES reliability). The composite factor values are averaged to obtain the overall impact rating.

The re-assessment re-estimated all impact factors for the top high risks.

Step 7 uses the likelihood rating (step 5) and impact rating (step 6) as an indicator of risk for each of the top high risks. This assessment has categorized risk into four levels: low, medium, high, and top high. Each risk should be judged relative to other PJM risks and not to risks from other assessments of other information systems. Furthermore, the new values were compared to the values obtained in the initial assessment to determine changes in security posture.

Step 8 of the NIST Special Publication 800-30 provides control recommendation controls to reduce the risk for the top high risks.

Step 9 presents and documents the results of re-assessing the top high risks.

Conclusions – Risk Evaluation

After analyzing the impact and likelihood re-assessment values for all top high risks from the initial assessment, 73% of the top high risks were reduced during this project through multiple efforts including SCADA monitoring, SIEM optimization, application security procedures, advanced malware assessments, and others. PJM's ongoing security risk management approach continues to drive risks lower.

It should be noted that significant residual security value was created for PJM. Residual benefits include:

- Improved security monitoring resulting in better threat visibility, increasing the likelihood of detecting a serious event
- Improved malware detection and zero-day threat response capability
- Improved ability to systematically evaluate and secure in-house and vendor sourced software applications
- Improved malware and intrusion detection capability on critical SCADA networks including behavioral-based alerts resulting in improved zero-day threat protection
- Improved overall cyber security situational awareness through the integration of multiple discrete security technologies into a single cyber security reporting console
- Improved ability to maintain the resiliency of critical systems in the face of a targeted cyber attack or other significant event
- Advanced training of cyber security personnel

All of the developed and demonstrated solutions are suitable for replication across the electric sector and the larger energy sector.