GOALS

Develop continuous monitoring techniques to improve EDS operators’ awareness of their cyber infrastructure.
- Continually monitor and measure system vulnerabilities, configuration errors, malicious events, and compliance with security policies.
- Provide data analytics that aggregate and process a broad set of data sources to determine security concerns.
- Reduce the cost of performing security assessments.
- Thoroughly test and verify the proposed technologies within realistic testbeds and in real-world systems.

FUNDAMENTAL QUESTIONS/CHALLENGES

- Cybersecurity assessments are costly and time-consuming, preventing EDS operators from performing frequent security evaluations.
- Periodic assessments provide limited assurance of security. Industry reports suggest that an adversary might compromise a system in minutes[1], but the average time to detection is 205 days[2].
- NERC CIP standards have limited requirements for security assessments and monitoring of security data, including:
  - High-impact systems require active vulnerability assessments every 36 months.
  - High/medium-impact systems require paper assessments every 15 months.
  - Checks for new security patches or changes of baseline configurations should occur every 35 days.
  - Logs reviewed every 15 days.
- Question: Can the process of assessing security and verifying that systems meet required security policies be automated and performed on a regular basis?

RESEARCH PLAN

This project will explore techniques to help EDS operators continuously monitor the cybersecurity of their systems. This requires a number of key research tasks, including:

- Identifying key security metrics
  - Identify metrics to address the current security posture of the EDS:
    - Examples include patch levels, account logins, logs collected, configurations managed, and incidents detected.

- Develop assessment techniques and protocols to collect security data
  - Extend NIST’s Security Content Automation Protocol (SCAP) to enable automated data collection.
  - Explore methods to perform data collection on heterogeneous EDS systems (e.g., credentialed scans).

- Explore assessment schedules to minimize the impact on the EDS
  - Identify the impact of assessment techniques (e.g., scanning) on a variety of EDS devices.
  - Optimize assessment strategies and schedules around inherent system redundancies.

- Develop analytical techniques to validate the system’s current security baseline
  - Correlate data from a variety of sources, including assessment results, packet captures, netflows, IDS logs, and log files.
  - Demonstrate the ability to validate compliance with security policies (e.g., NERC CIP) in real-time verification, rather than yearly basis.

- Test and validate the proposed techniques on various real-world devices
  - Evaluate the proposed technique against real software platforms (e.g., EMS, DMS) and devices within the WSU Smart City Testbed and other CREDC testbeds.

BROADER IMPACT

- Provide utilities and other EDS operators with real-time awareness of their critical cyber assets, beyond traditional intrusion alerts.
- Decrease the window of time between when a security incident occurs and when EDS operators identify the incident.
- Reduce the cost and inconvenience of periodic vulnerability assessments.
- Inform EDS operators with consistent evidence of their compliance with organization or industry standard security policies (e.g., NERC CIP).

INTERACTION WITH OTHER PROJECTS

- The project will explore collaboration with other CREDC activities focusing on:
  - Detecting cyber attacks on systems and networks.
  - Performing big-data analytics of cybersecurity events.
  - Developing cyber-physical metrics for security.
- This research will also explore industry collaboration to obtain inputs from both vendors and EDS operators on the feasibility of the proposed techniques.

FUTURE EFFORTS

- Explore techniques to identify malicious activity on smart meters and other EDS systems, combining both network and host-based analysis.
- Begin exploring security assessment content that can be collected from EDS devices.
- Test current assessment activities (e.g., scanning, credentialed analysis) on real EDS devices.