GEO-IP Blocking

June 13, 2018
Critical infrastructure is a higher profile target

- Nation states are increasing their attacks.
- Password spraying has become an effective tool to compromise user accounts.

PJM recognizes member feedback must be incorporated into security approaches
PJM’s Response to Cyber Threats

More restrictive cybersecurity controls

Block network traffic from outside the U.S. and Canada via Geo-IP blocking

www.pjm.com
PJM’s Approach to Geo-IP Blocking

- Analyze network traffic by country
- Analyze the use of authenticated services by authorized user
- Correlate service use against analysis of traffic by country
- Build up whitelisting for valid, correlated network traffic
- Monitor whitelisting
- Successively block groups of countries based on risk/use
PJM’s Support/Response Approach

- Communicate change process
- Response process for member-related problems
- Regular meetings to review process effectiveness

Collecting the right feedback to quickly determine username, source IPs, services being accessed, error information, etc.

An escalation process in place to quickly respond to problems
What Has PJM Done to Date?

PJM has begun implementing Geo-IP blocking with:

• High risk countries
• Limited access to internet SCADA