IOT Security IN-ISAC - 2020

Who We Are:

The IN-ISAC provides Tier 1 management of network events through its security operations center (SOC) in West Lafayette. Additionally, the IN-ISAC handles the statewide cybersecurity training for all Executive Branch agencies and separately elected officials that opt in. The team also provides outreach services to local governments, K-12 (primarily through DOE), and other Indiana based organizations.

Our Mission:

To support IOT Security efforts through a broad, diverse range of services that include triaging of network events, provision of formalized and ad hoc cybersecurity training, and the support of state governmental entities outside the Executive branch through a variety of services.

Department: 493003

Managers:

Bryan Sacks, CISO; Tad Stahl, IN-ISAC Exec. Dir.; Nicole Needham, Training Manager; Brian Hartz, SOC shift lead

What We Do:

The IN-ISAC performs support functions for distinct audiences. The Executive branch serves as a customer for the cybersecurity training and SOC functions as well as 1175 statistical information. Other governmental organizations receive ad hoc services as requested including public speaking, the sharing of threat information, consultation, and awareness materials.

Our Products:

1175 Security - Baseline

Our Tools:

- MediaPro Cybersecurity training/PeopleSoft ELM
- FireEye NX – Network malware detections (workstations)
- FireEye HX – Hosted Based
- MS-ISAC (managed 3rd party sensor)
- Intel (McAfee) Web Gateways
- Archer
- Logging – ELK, Azure
- Microsoft ATA & Azure

Our Metrics:

The IN-ISAC tracks statistics for a number of 1175 services as well as completion metrics for the monthly cybersecurity awareness trainings and the failure rate for quarterly phishing simulations.

Our Customers:

All Executive Branch agencies, State outreach to non-Executive branch government organizations.

Our Budget: @ $600,000

Our Growth:

- SOC – adoption of new tools and additional monitoring of events
- Training completion rate – increase in monthly metric of completions, increase in number of agencies meeting target metric
- Increased presence with outreach through speaking and presentations
- Increased distribution of ad hoc and weekly cybersecurity awareness information

Major Accomplishments - 2019:

- Cybersecurity awareness program released trainings on time each month
- Completion rates increased to over 90% for nearly every agency
- Executed and reported on quarterly phishing simulations
- Used new tools at SOC to provide more thorough analysis and improved dispensation of security events

- Contributed, through the resume enhancement of SOC duties, to the employment of 5 students
- Completed the refresh of the state's acceptable use agreement
- Implemented cybersecurity onboarding training for all new hires
- Implemented script for the automatic disable of non-completions of the IRUA (post refresh) and cybersecurity onboarding modules (completed 2020)

Current Projects:

- Improved use of enhanced logging tooling (ELK)
- Implementation of new learning manager (Success Factors)
- Consideration of new awareness software
- SOC 2.0
- Strategy review for improved awareness of phishing attacks and results