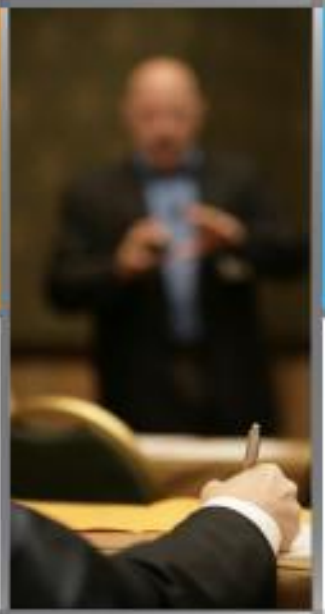
@CSOevents
#CSO50

CSO50 CONFERENCE+AWARDS

Aligning Proactive Security with Modern Threats



May 1-3, 2017

The Scottsdale Resort
Scottsdale, Arizona

PRODUCED BY
CSO
FROM IDG

CSO 50 CONFERENCE +AWARDS

Share All the Indicators

Preston Werntz

Chief of Technology Services, National Cybersecurity and Communications Integration Center (NCCIC)

Department of Homeland Security

@werntzp

Automated Indicator Sharing (AIS)

- The goal of AIS is to rapidly and widely share machine-readable cyber threat indicators and defensive measures at machine-speed for network defense purposes
- AIS fulfills the requirement in the Cybersecurity Information Sharing Act of 2015 for DHS to have a capability to automatically receive, process and share indicators
- AIS is about volume and velocity of sharing indicators, not human validation

AIS Technology Stack

- AIS is built upon the **STIX** (Structured Threat Information Expression) and **TAXII** (Trusted Automated Exchange of Indicator Information) specifications
- STIX and TAXII were initially developed by DHS, but in 2015 were turned over to OASIS (Organization for the Advancement of Structured Information Standards)
  - https://www.oasis-open.org/committees/cti/

Context

- Through AIS, we share **technical context** about the indicators
  - When did you see this IP? Is it a C2 node or part of a DDOS? What critical infrastructure sector is impacted? What phase of the kill chain?
- We do not share **cyber threat intelligence context**
  - Linking indicators to a particular campaign or threat actor

Privacy

- Our goal is to remove any personal information not required to understand the cyber threat through a mixture of automated processes and human review
- Privacy Impact Assessment and Privacy Guidelines located at https://www.us-cert.gov/ais

Where We are Today

- DHS has connected 94 non-Federal and 33 Federal entities to the AIS server (many of these entities can further re-distribute the indicators to their customers and members)
- Since March 2016, over 277,000 unique cyber threat indicators have been shared
- A recent In-Q-Tel threat feed study found the indicators in AIS tend to show up earlier than in several commercial feeds and contain high quality, low false-positive data

Takeaways, Challenges and Next Steps

- Properly measure indicator timeliness, quality and value
- Help organizations that are not sharing to overcome technical, resource or cultural hurdles
- Fully operationalize the indicators through automation and orchestration
- Continuously improve the technological infrastructure
- Tackle tough problems involving confidence, risk scoring, revocation and duplication