



Information Exchange Policy (IEP) SIG Update

Merike Kaeo - presenter

Terry MacDonald

Paul McKittrick

Goal of IEP SIG work

IEP-SIG mission is to automate the exchange of security and threat information in a timely manner to improve the efficiency and effectiveness of the security response community, and industry.

Work Completed

- IEP 2.0 - https://www.first.org/iep/FIRST_IEP_Framework_v2.0.pdf
- Create IEP Protocol
 - Create an Information Exchange Policy protocol to enable machine-based exchange of restrictions for handling, actions, sharing and licensing of shared information.
- Create Standard IEP Policies
 - Create language around the more common policies used today for sharing threat intelligence information utilizing the IEP protocol.

Work In Progress or Starting

- Incorporate IEP into STIX/TAXII (currently in progress)
 - STIX 2.1 had been ratified as a standard. IEP 2.0 has been ratified. Work is starting towards getting IEP 2.0 into STIX 2.2.
- Promote IEP Policy Reuse (work starting)
 - Develop a suite of standard, reusable IEP Policy Files that will cover 80% of the threat intelligence sharing situations in use today.
 - A few key standard IEP Policy Files for consideration:
 - IEP-SIG TLP Policy File: <https://www.first.org/iep/2.0/first-tlp-iep.iepj>
 - IEP-SIG Unknown Policy File: <https://www.first.org/iep/2.0/first-unknown-iep.iepj>
- Create standard legal documents to match Standard IEP Policies (work starting)
 - Develop globally acceptable legal contract language that match the standard IEP policies created.

Future Work

- Create IEP selector website to ease IEP Policy selection
 - Envisaged to be a website similar to the Creative Commons 'Choose your licence' wizard.
 - It will be a series of questions that then tell the viewer which standard IEP Policy is right for them.
- Enable TAXII to use IEP requirements to auto-enroll new sharing partners
 - Aim to use IEP to automate TAXII Channel participation by automatically accepting legal agreements and restrictions between intelligence producers and intelligence consumers.

Meeting June 26, 2022

- Agreement that work in progress should be continued
- Some proposal for enhancements to IEP 2.0 may need to be considered
- Coordinate with other industry efforts that have overlap with IEP work
 - ANSI PAP
 - APWG
 - M3AAWG