SESSION #8, Breakout #4

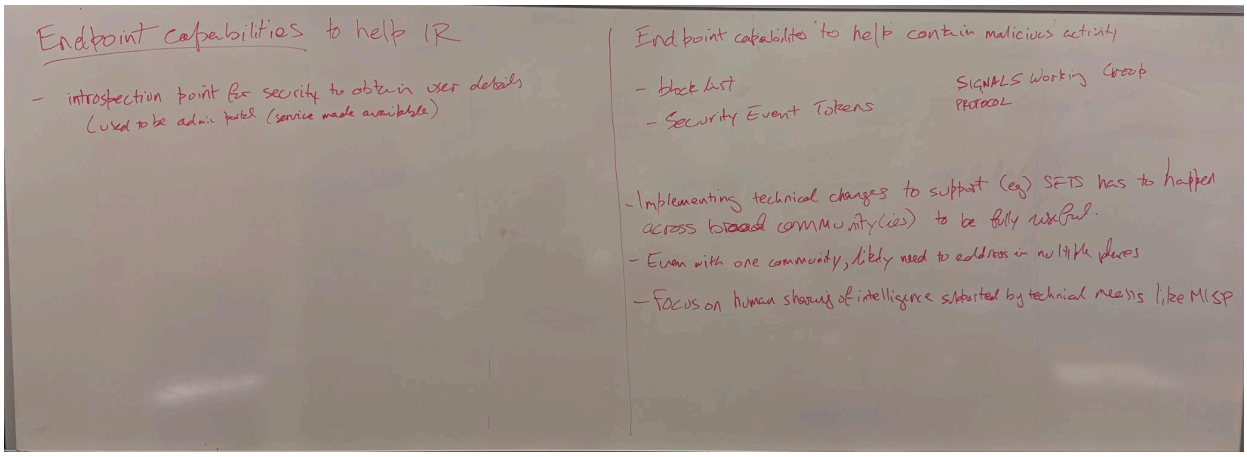
Session Title: Endpoint capabilities to support incident response
Session Convener: David Crooks
Session Notes Taker(s): Liam Atherton

Tags / links to resources / technology discussed, related to this session:

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion, action items, next steps:

What are the tools we can implement on the IdP side to help the IR process that would be available for use without building a whole process around them? Marcus had a suggestion, would it make sense that there could be an endpoint for responders to help contain malicious activity.

??What tools can we conceive of in the background so that when we need them they have been thought of??



Discussion became around

- Endpoint capabilities that could help incident response
    - Introspection point for security teams to obtain user details based on possession of a token

- Endpoint capabilities to help contain malicious activities
    - Blocklist
    - Security Event Tokens

Ultimately, the discussion ended in the finding that implementing changes to support (eg) SETs has to happen across broad community(ies) to be fully useful. Note that resources are constrained - and may well need to be focused on operational functionality without broad acceptance

Even within one community, likely that implementation would need to take place in multiple places/softwares
Focus on human sharing of intelligence supported by technical means like MISP

Mention of SIGNALS working group (I think https://openid.net/wg/sharedsignals/); potential for work on this to continue in the background at a slower cadence as the community moves forward.