Cerebrate

A quick intro into the current dev version of Cerebrate

Andras Iklody

Plan for this session

- Quickly go over what is there in Cerebrate currently
- Implementation details
- The future

Current scope

- Basic UI and API systems (we'll talk about this later)
- First iteration of ContactDB
- Early version of the Trust Circles
- Basic User management and ACL
- Basic public lookup interface

ContactDB

- Repository of organisations and individuals
- Their relationships to one another (an individual can be affiliated with a set of organisations)
- Encryption keys associated with either
- Basic public lookup interface

Trust Circles

- Repository of sharing groups
- Sharing groups have metadata about their purpose and a list of member organisations
- Slightly simplified compared to MISP, this might change though
- Cerebrate sharing groups are not editable by anyone besides the source (up for discussion)
- They always have a primary owner

User management

- Users are tied to an individual - but not all individuals are users
- Authentication happens via username+password or an API key
- We can extend this in the future with other auth providers (for example LDAP) and optionally take this responsibility out of Cerebrate
- Users are tied to roles that can be custom defined
- Currently their affiliation to an organisation happens through the individual - though I will probably change this
- Users can have a set of API keys with different expirations / use-cases (based on MISP discussions this week we will enhance this further)

Public lookup interface

- Still more of a proof of concept
- The idea is that administrators can decide to open up a fully public interface for lookup services
- Currently the Individual and Organisation registries are optional parts of this system
- The plan is to be able to mark a list of orgs/individuals for the public lookups
- Separate url routing makes additional allow/deny lists on the URL easy to implement

Internals

- Largest part of the work was transitioning MISP APIs to a more modern stack
- UIs are generated by a diverse list of custom factories
- Everything is parametrised and standardised internally
- MISP's API libraries have been converted and modernised
- Same with the ACL libraries

Deployment

- Installation instructions are already available on github
- Very simple, low number of requirements
- Should run on a potato

Main Next steps

- Many things to do within the existing scopes
- Cerebrate to Cerebrate communication connections
- Automatic exchange of information
- Trust relationships
- Integration layer to instruct local tools