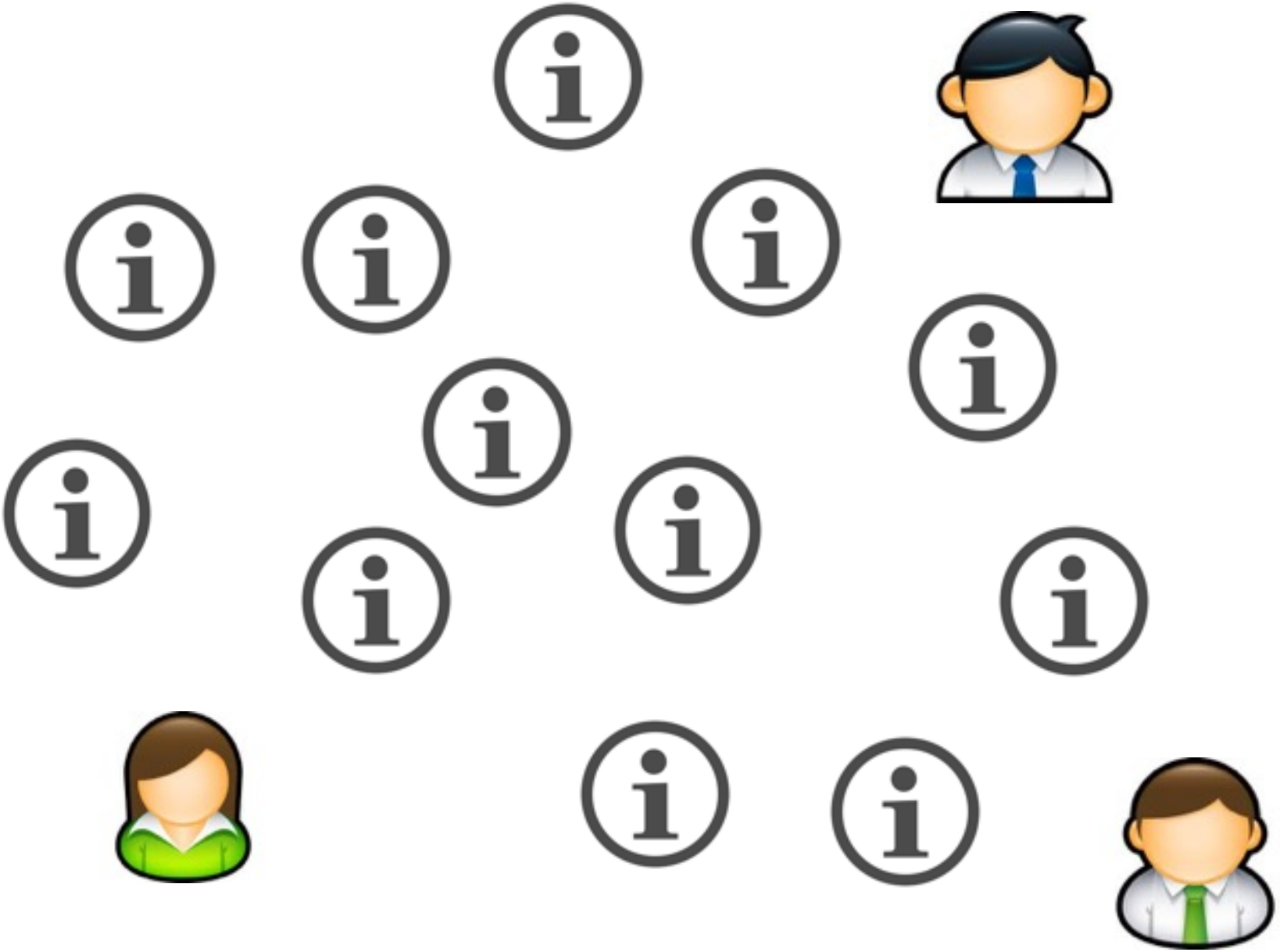
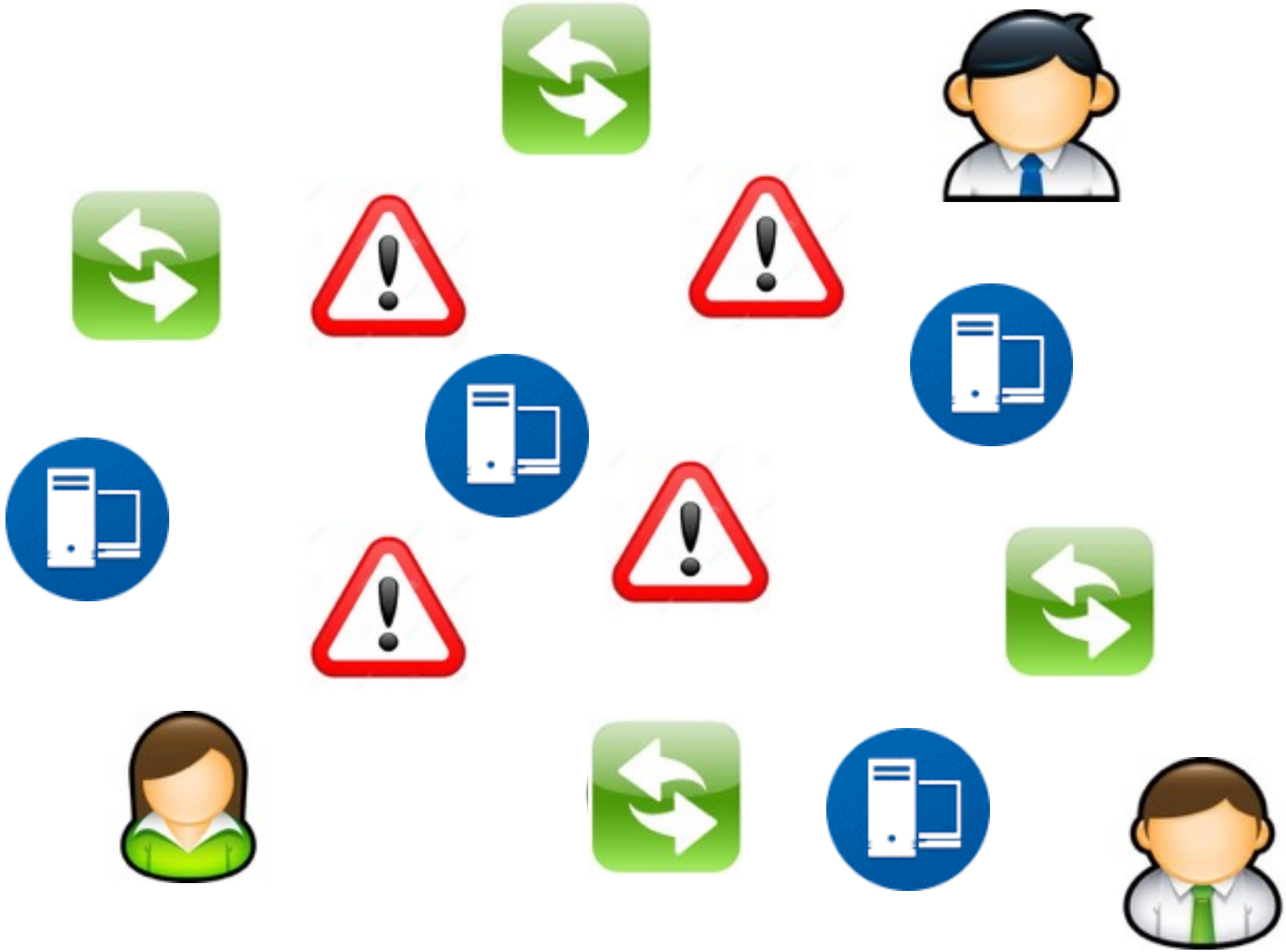
|galois|

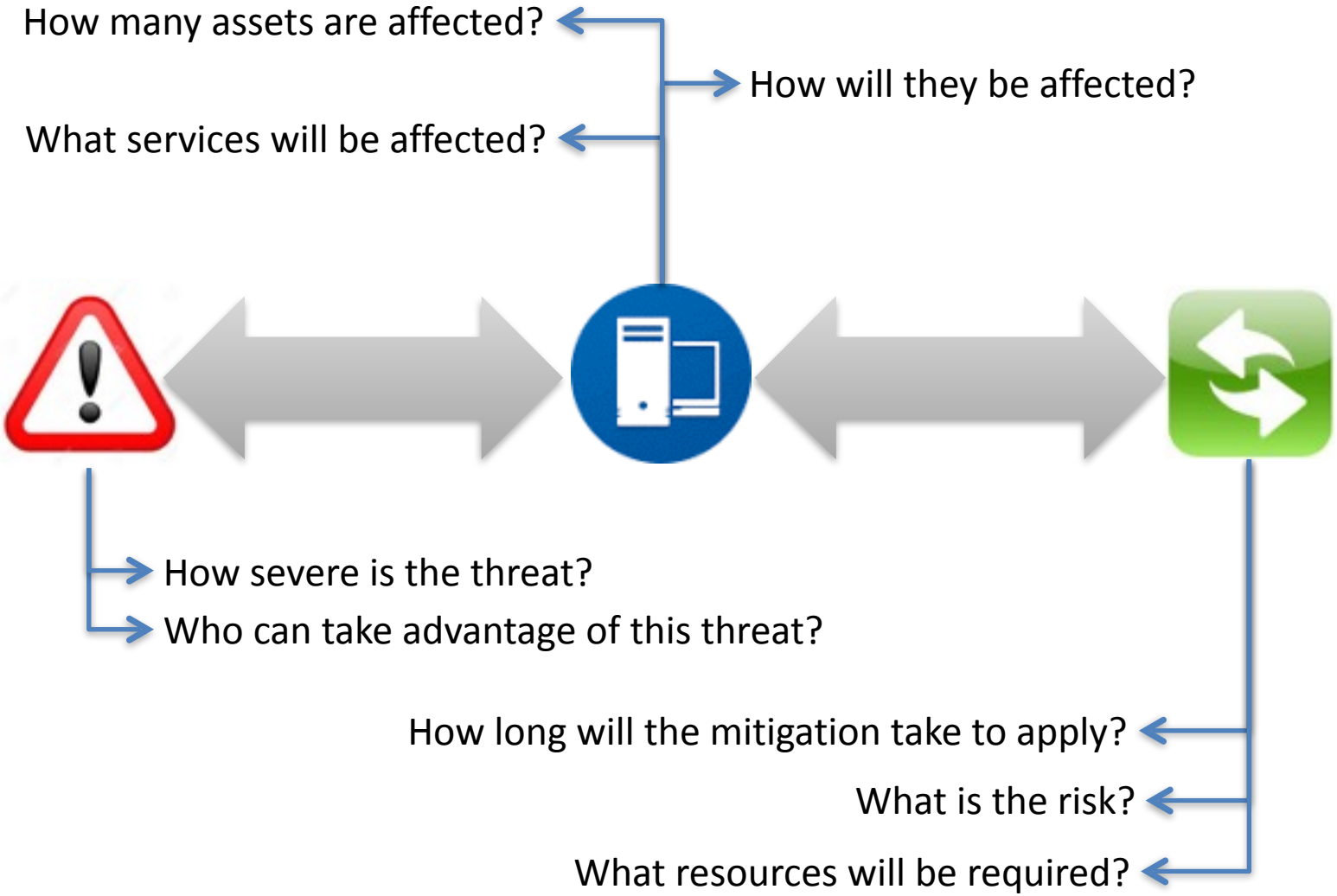
TFER: Threat Fusion & Effective Response

Galois [gal-wah] Named after French mathematician Évariste Galois

www.galois.com



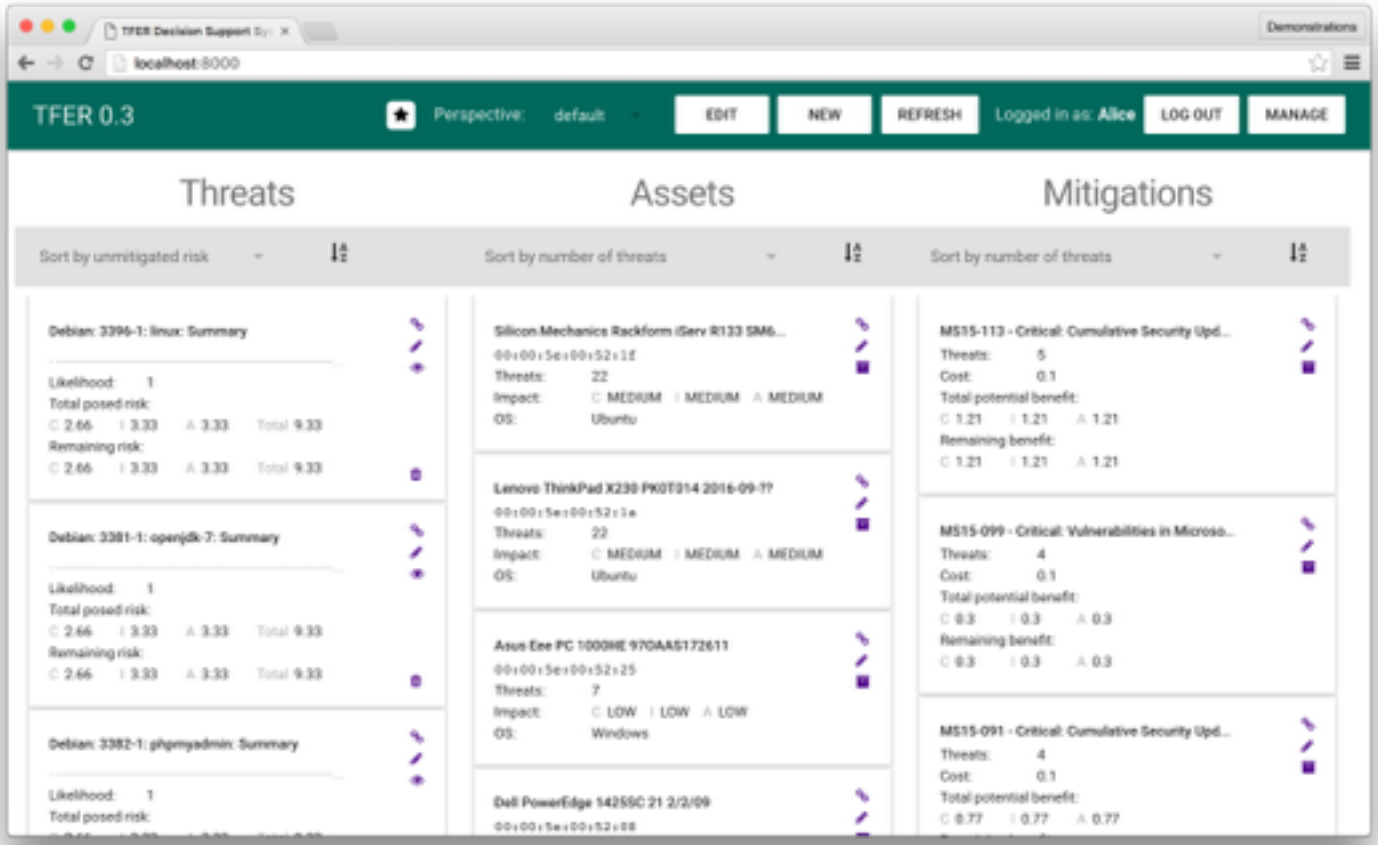


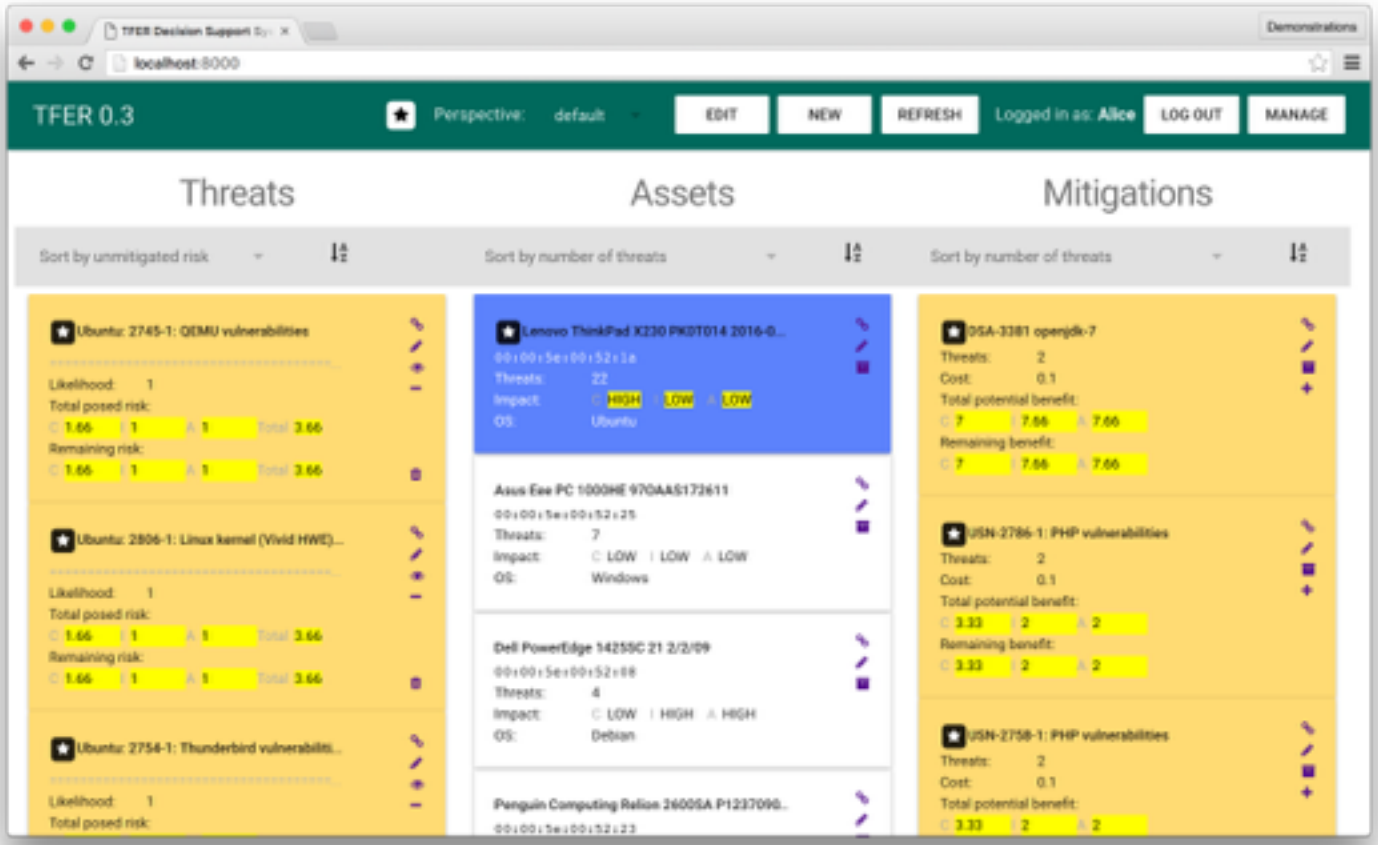


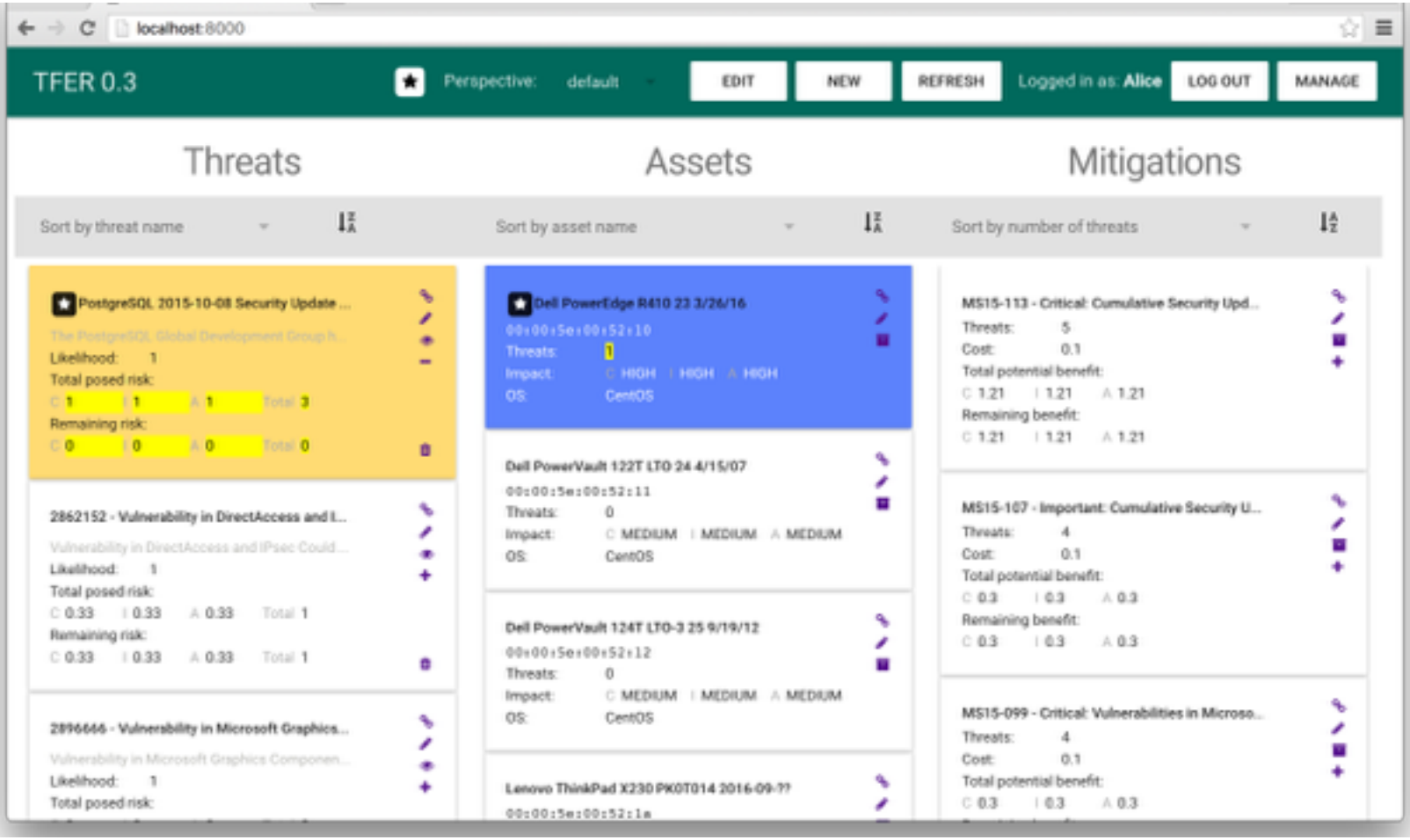
Project goals

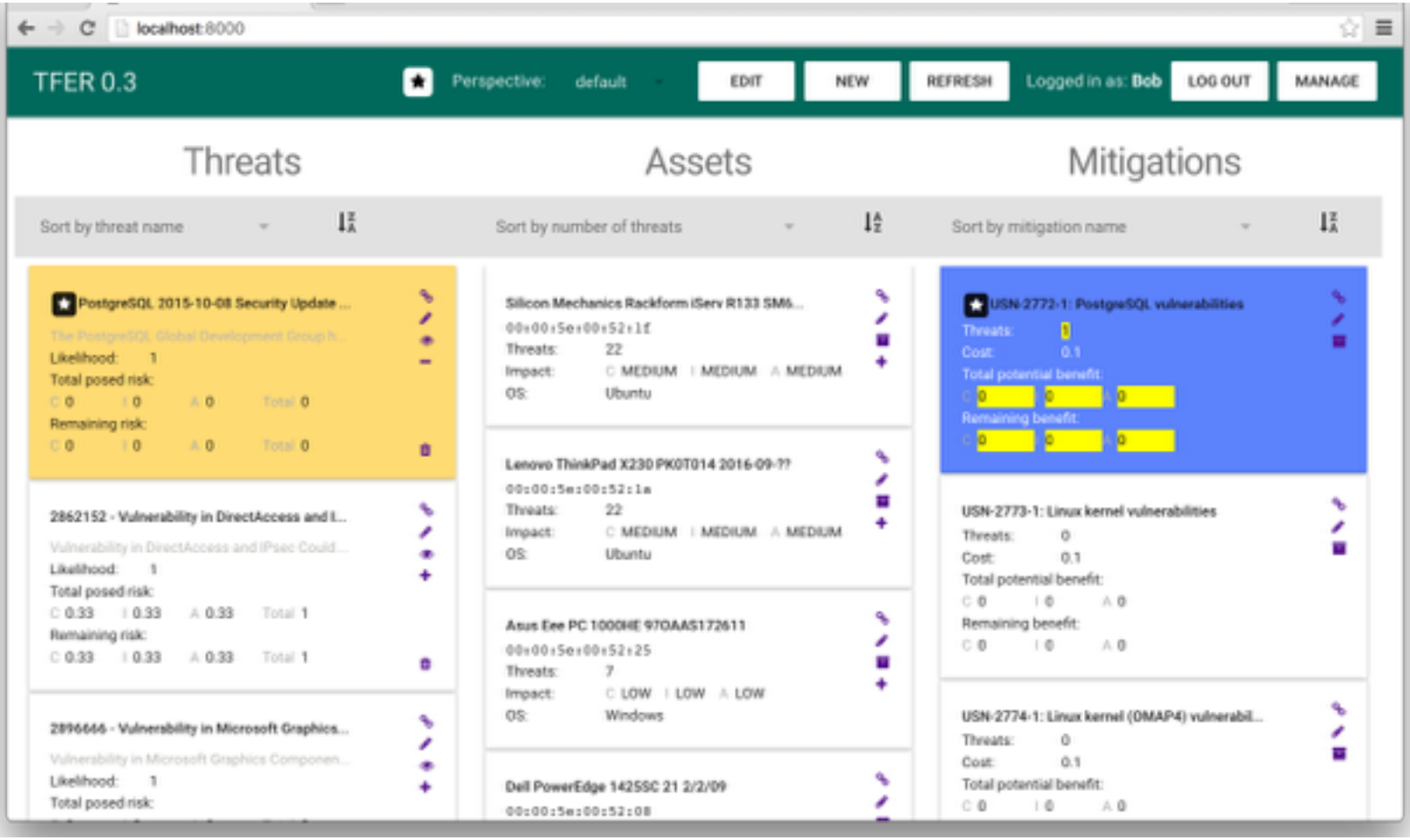
Improve analyst efficiency and collaboration by leveraging existing workflows, standards, and **state of the art automation**, resulting in an **easy-to-understand reference prototype** that links high-level threats to low-level data.

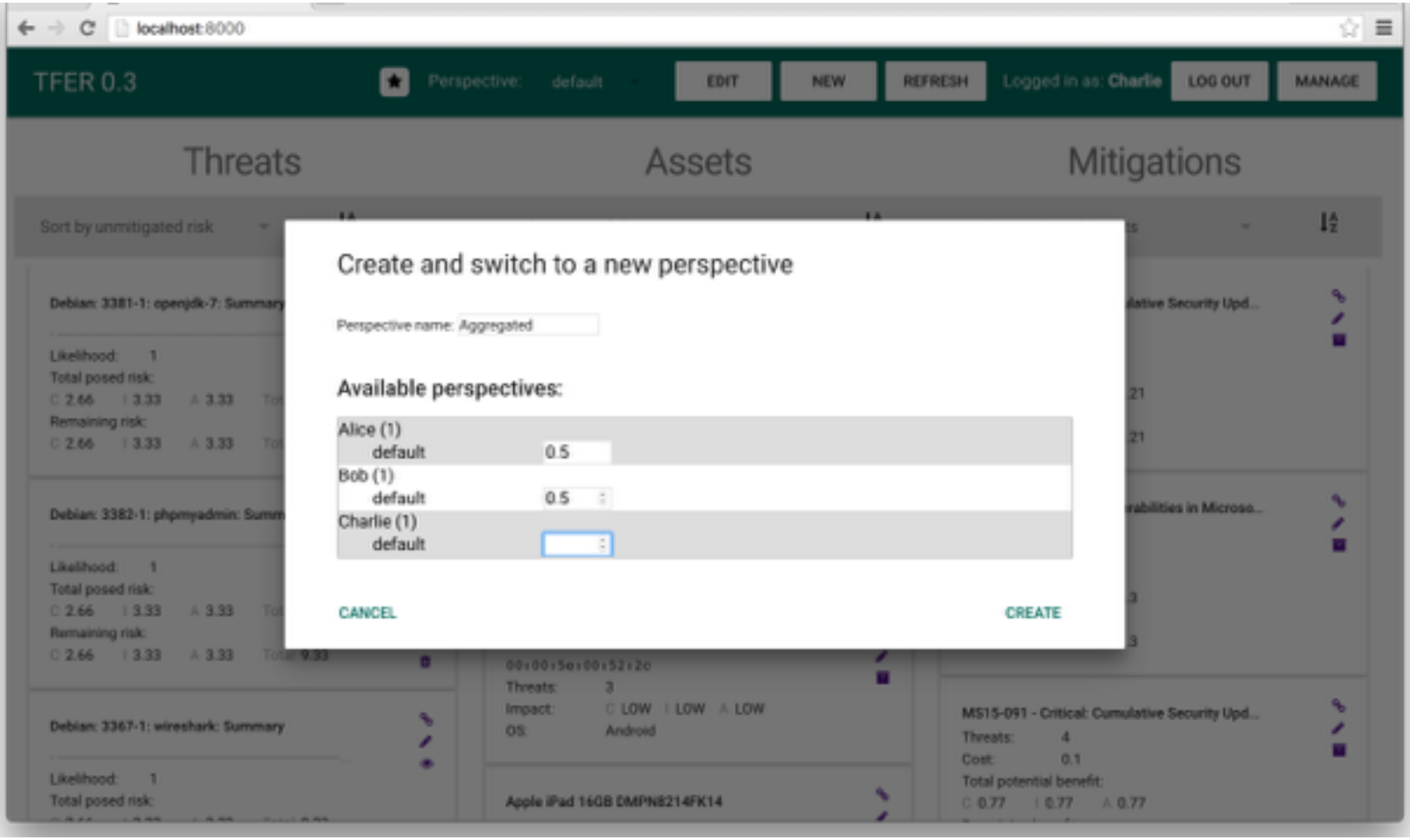
DEMONSTRATION

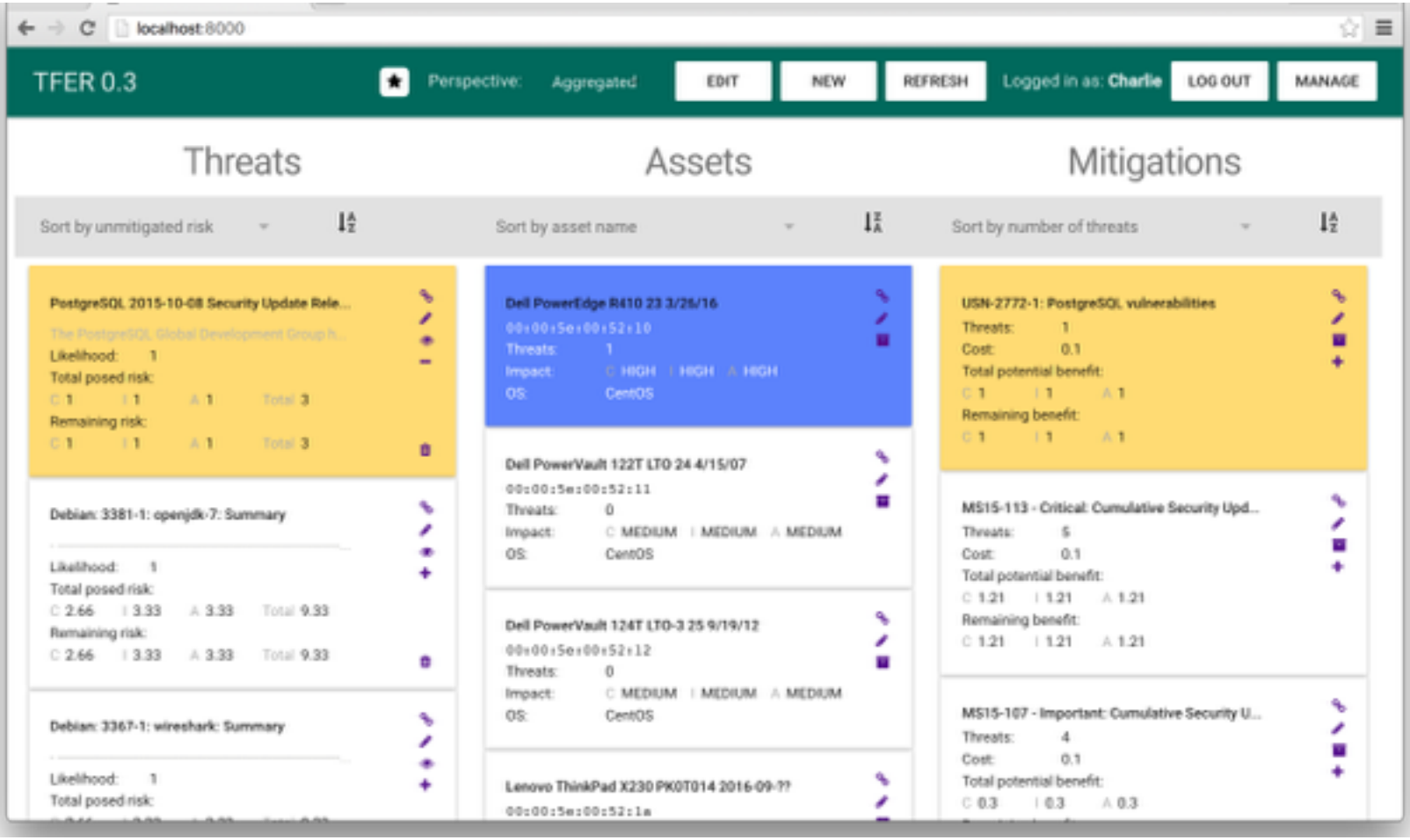


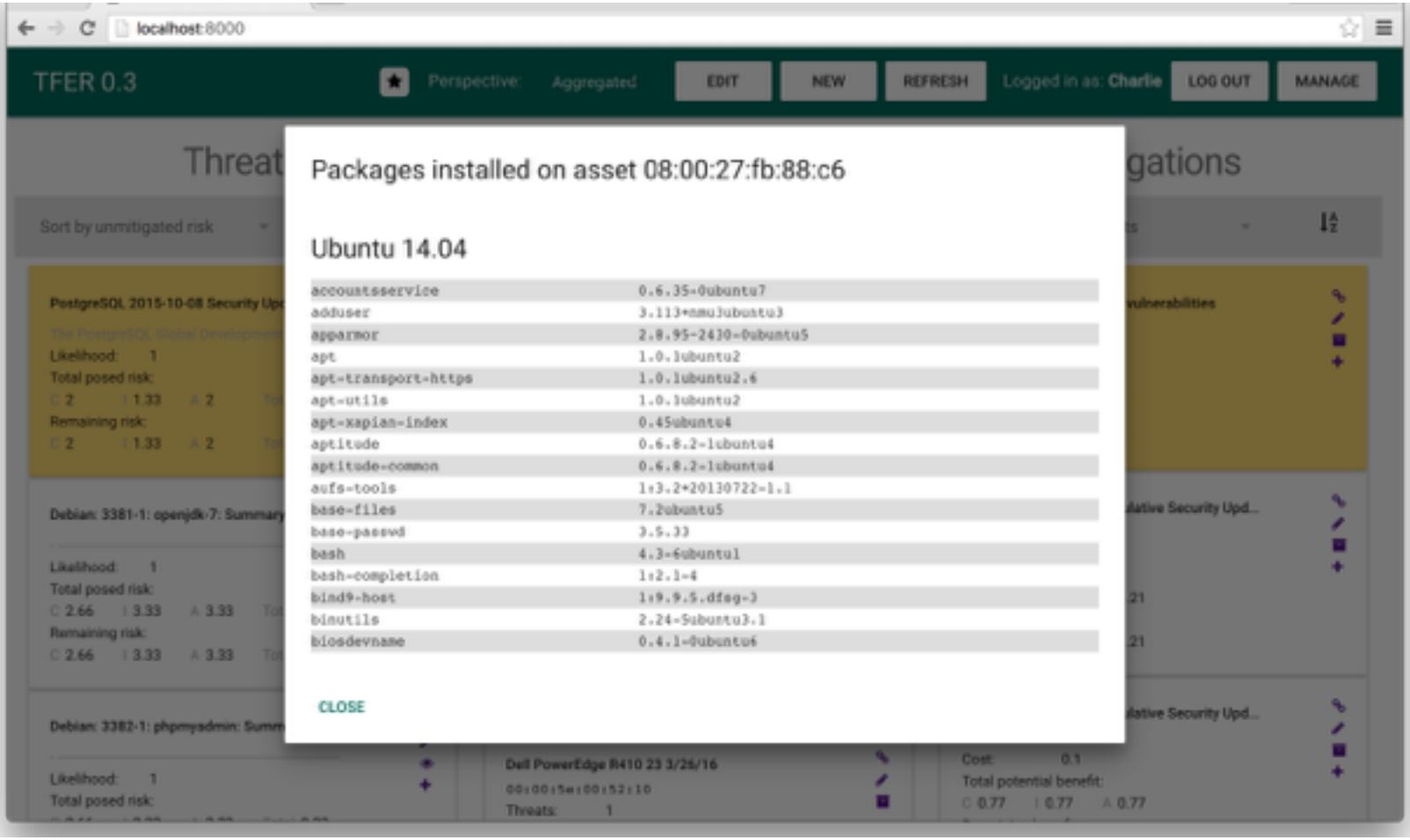


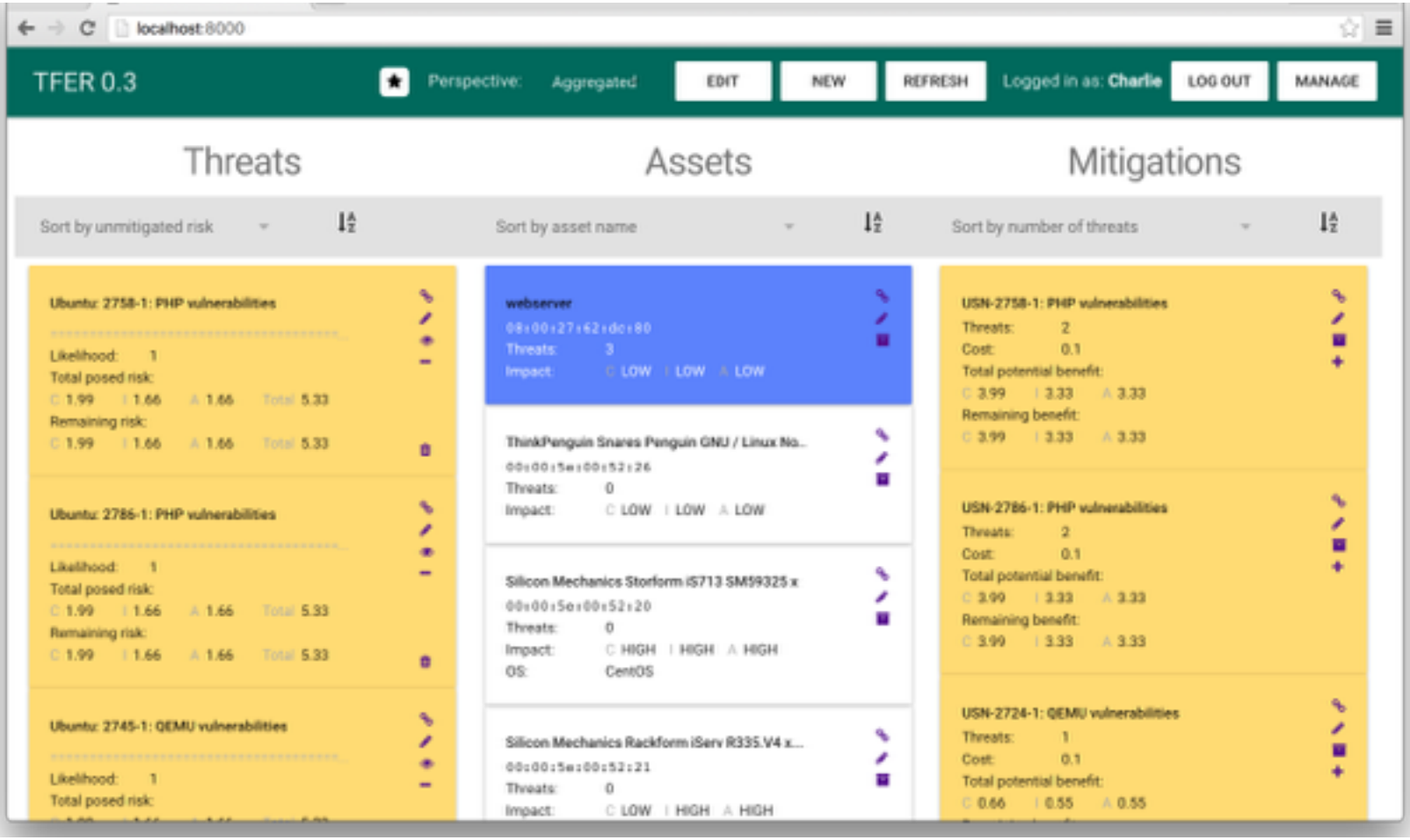


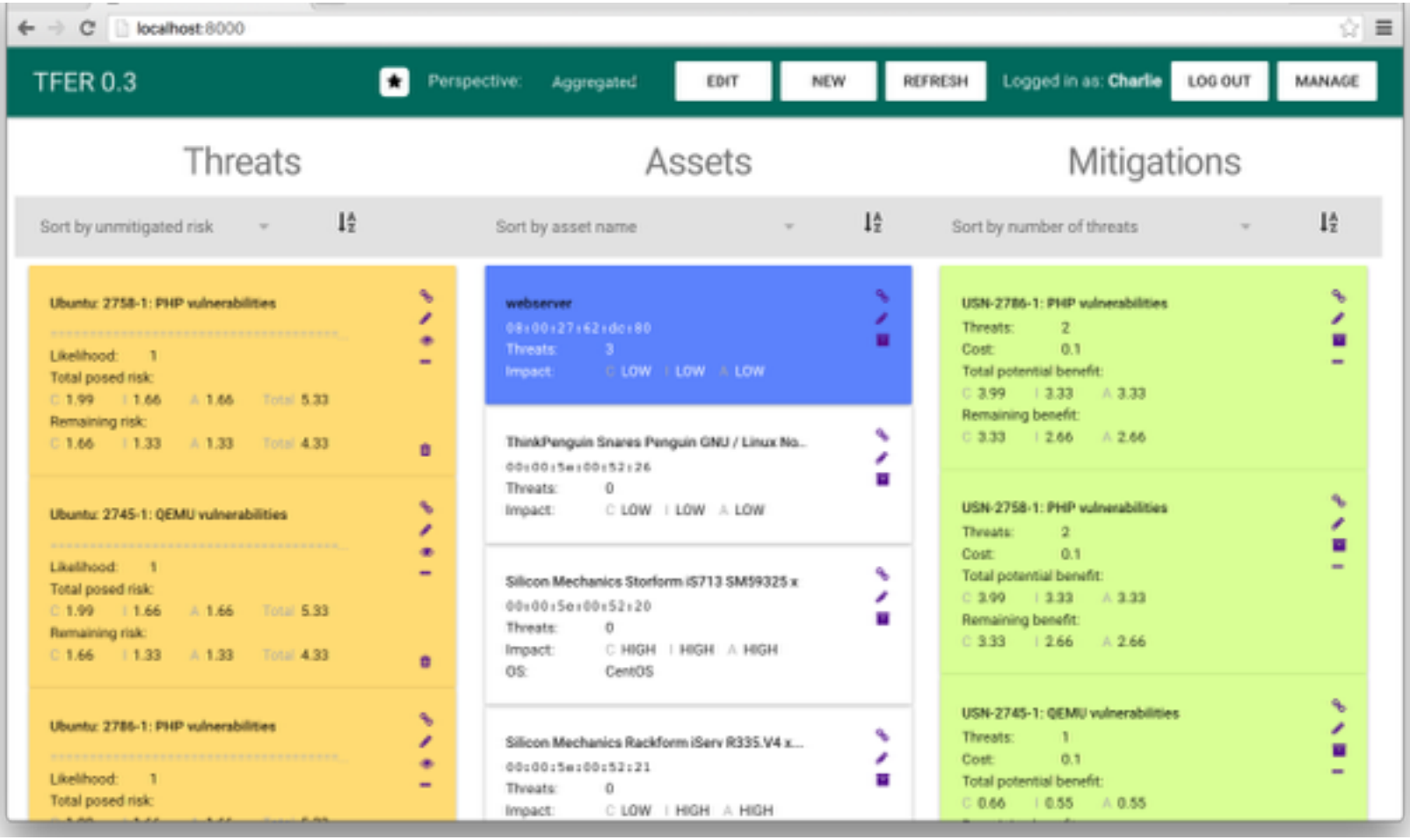












Demonstration summary

- Automated results are ready immediately
- Multiple analysts can refine results
  - Input provided according to user capability, expertise, and availability
- Conflicting input is aggregated according to:
  - Assortment of algorithms
  - Human preference
- Result:
  - View of the threat landscape in operational context
  - Prioritization of T/A/M with high risk / pay-off

TFER is a Decision Support System

- Enumerate the threats, assets, and mitigations by automatically pulling from existing sources.
- Use automated analysis to help rank and score information, so that the most important information floats to the top.
- Use manual connections from a collection of analysts to add new links and update the scoring system.
- Allow multi-user perspectives to make cross-analyst deductions work cleanly and easily.

Uncertainty & Hard Numbers

TFER ingests data from a variety of sources, and provides automatic ranking and clustering based on some hard numbers. You saw these as some of the hard numbers in the demo.

The basis for these hard numbers is an extension of Dempster-Shafer Theory, invented as a way to reason about uncertainty when combining evidence from multiple sources.

Stay tuned for David Burke's talk tomorrow to learn more.

THANK YOU.