

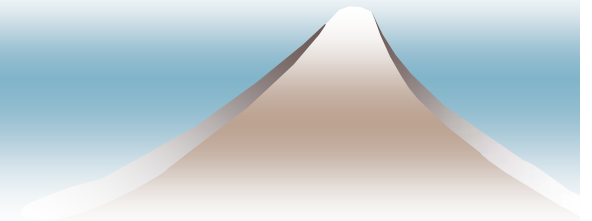
An Architecture for Tracing *Incidents* across the Internet

Glenn Mansfield Keeni

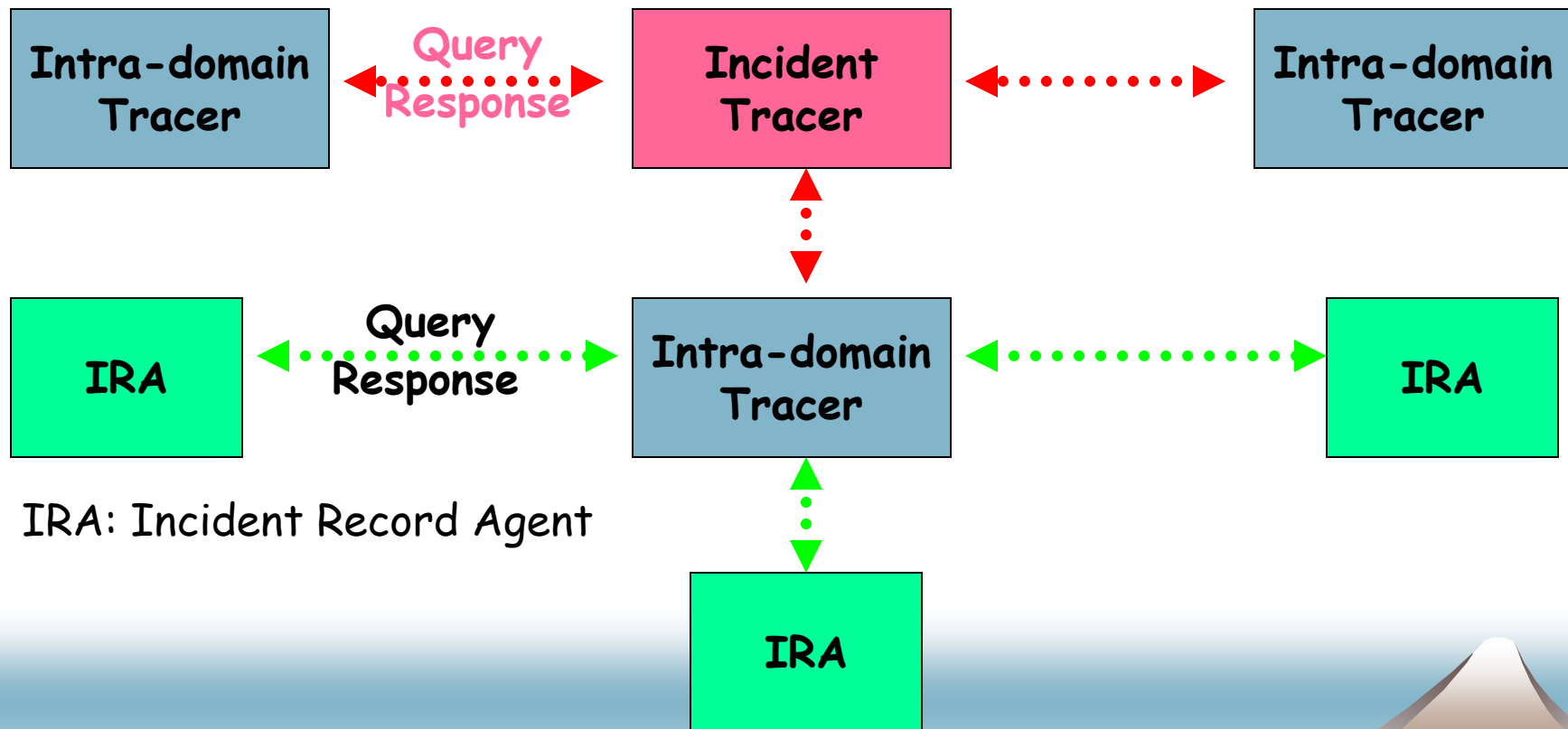
 *Cyber Solutions Inc.*

Inch-wg, IETF-61

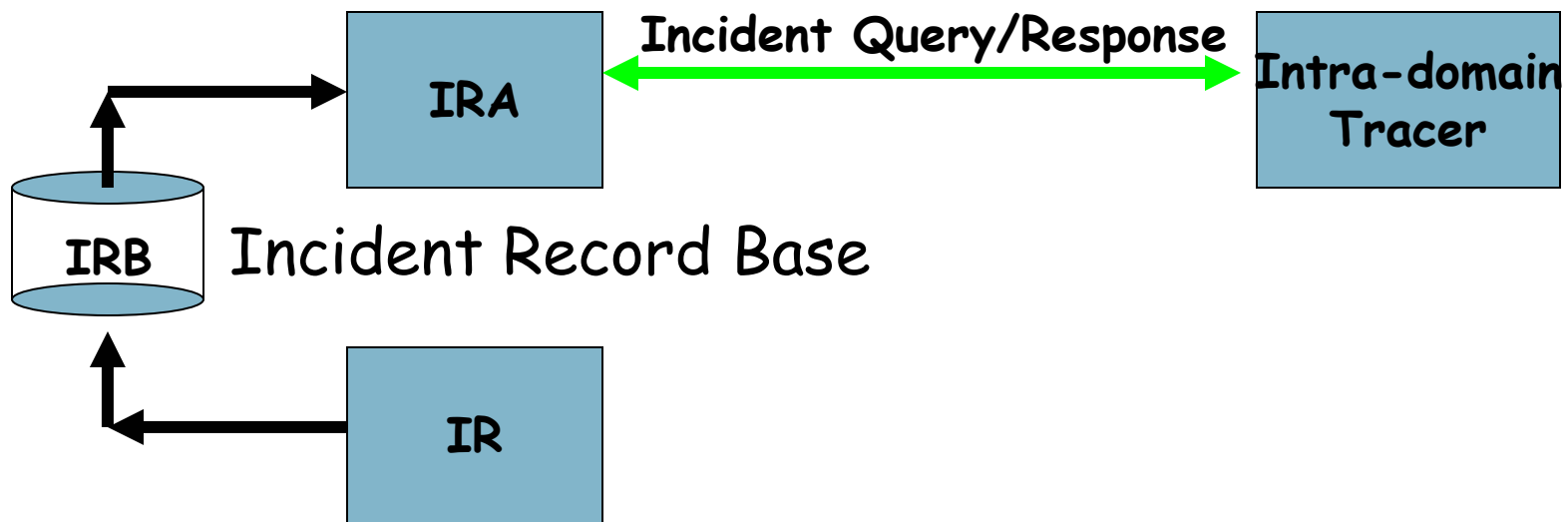
November, 2004



The two-tier Architecture

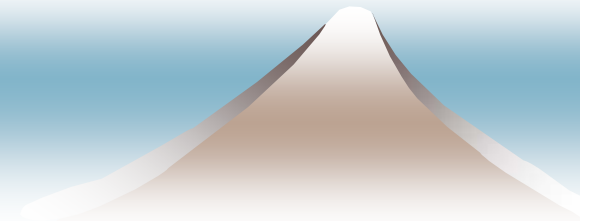


The Intra-domain Architecture



Inter-Domain Incident Tracing Protocol

- ◆ Specify the Incident *Identifier (attributes)*
 - ◆ *Unique Identification* for incident
- ◆ Return matches from local database
 - ◆ *Common format* for incident description
- ◆ Authenticated
- ◆ Privacy, Integrity
- ◆ Non Repudiation



Incident Record Protocol

Mapping: IncidentRecord ↔ Incident Identifier



Requirements: Incident Record Protocol

Recorder

Incident Report



Transform
Tr (Incident Report)



Incident Record Base

Additional Data

Incident Record Agent

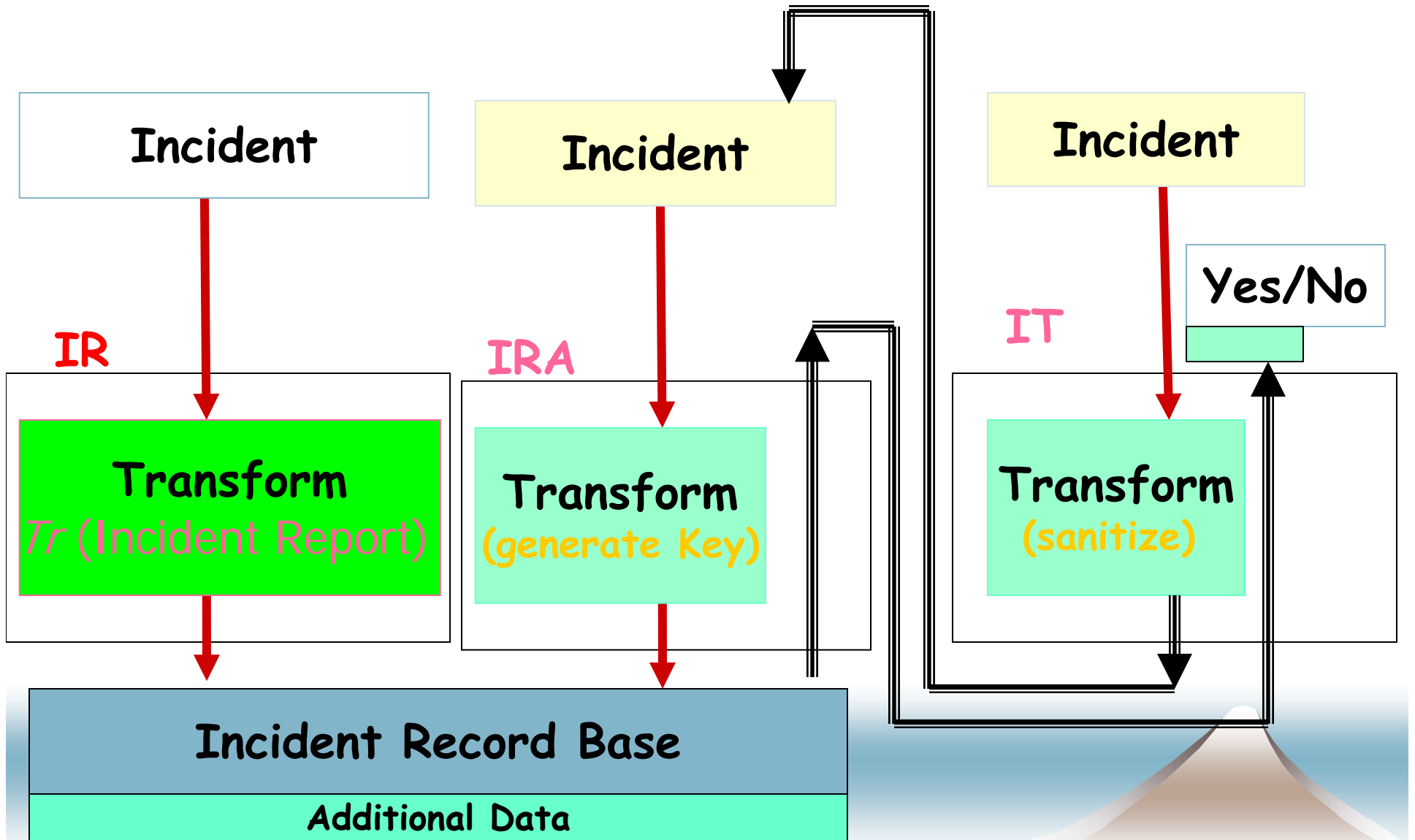
Incident Report



Transform



The Intra-domain packet tracing Process:



[draft-glenn-ippt-arch-01.txt](#)

