PLENARY SESSION 1: Cloud Forensics Challenges and Lessons Learned

Anil Karmel
Founder and CEO
akarmel@c2labs.com
DOE YOURcloud: A Cloud of Clouds approach brokering any organization, through any device, to any service respectful of site autonomy

INSIGHT
- Green & Business IT Smart Meters
- PortfolioStat
- Enterprise Architecture
- Data Center Consolidation

FEATURES
- Virtual Desktops & Servers
- Enterprise Application Store
- Enterprise Certification & Accreditation

*Powered by INSIGHT: Green & Business IT Smart Meters

Anil Karmel | Building YOURcloud | 2013
Key Forensics Challenges in the Cloud

Technical

• Data Ownership
• Architecture (IaaS, SaaS, PaaS)
• Logs / Time Stamps
• Transient State of the Virtual Machine or Data
• Validation of Identity
• Encryption
• Root of Trust
Key Forensics Challenges in the Cloud

Legal

- Contract Terms and Conditions
  - Data Ownership
  - Access to Underlying Infrastructure
- Jurisdiction
- Outdated Policies and Processes
  - Seizure of assets
- Retention Periods
Key Forensics Challenges in the Cloud Organization

- Lack of standard processes across organizations
- Evolving System Boundary
- Clearance/Need to Know
Lessons Learned
Cloud Forensics

• Technical
  – Validate that your architecture (IaaS, SaaS, PaaS) respects multi-tenancy with an established root of trust
  – Fork your logs to multiple entities with a baseline timestamp

• Legal
  – Establish Clear Contract Terms and Conditions
  – Update Policies and Procedures

• Organization
  – Establish clear retention periods for logs and data
  – Redefine your system boundaries
  – Ensure people that have access to government data have the appropriate clearance level