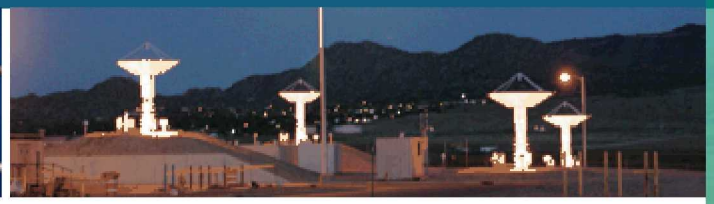
SAND2019-9516PE

Cybersecurity Research in Commercial Cloud



PRESENTED BY

Sandia civilian cyber research team

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

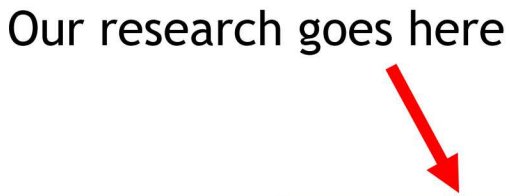
Problem - Commercial Cloud has functionality underutilized by security

Commercial cloud computing presents new delivery models with enhanced functionality, including:

- On-demand permissions
- Rapid redeployment
- Elastic capacity
- Regional delivery
- Serverless application hosting
- Simplified versioning and new application roll-out
- Strong templating and reuse
- Aggregated telemetry
- Etc.

These new options are being readily adopted by developers, solutions architects, and operations personnel to increase application efficiency and performance. However, cybersecurity tools still struggle to leverage these new paradigms to enhance protections.

Approach



NIST Cybersecurity Framework: Identify, Protect, **Detect**, **Respond**, Recover

First step in our research is to collect information and perform threat discovery. Next, we'll determine responses based on those threats which are optimized to leverage cloud capabilities.

Anticipating and Accounting for Emerging Technology Trends

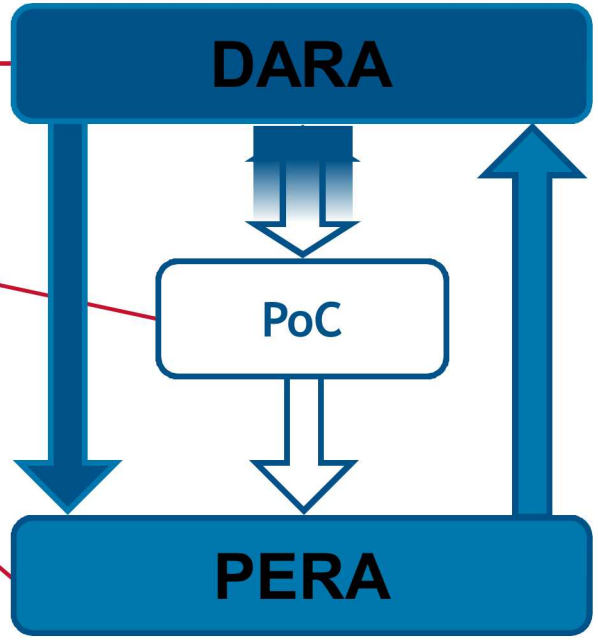
Goal: Identify disruptive cybersecurity trends (with a focus on cloud computing), evaluate their potential impacts on the civilian cyber environment (including through experimentation and evaluation of commercial product offerings with a threat-aware emphasis), and propose solutions based on emerging technology.

Value Add

Data Aggregation Reference Architecture
cloud-based architecture for ingesting cloud security logs from multiple tenancies

Aggregation Proof of Concept
Establishes feasibility of Architecture and captures lessons learned

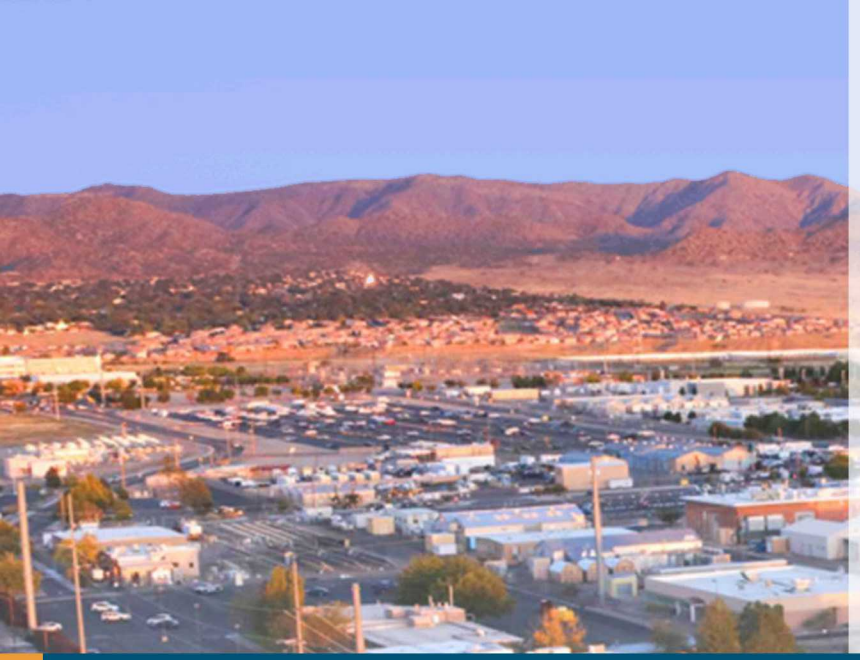
Protected Entity Reference Architecture
Provides protected entities with guidance for interacting with Data Aggregation Reference Architecture



Ongoing research

After threat discovery –so what now?

- Automated tipping of white/black lists
- On-demand trust modification
  - Connectivity
  - Permissions
  - Versioning
  - Redeployment
  - Traffic Shaping
- Protected Entity variable risk tolerance and demand for tenant self-service tools



Questions?