When a SOC is more than a SOC

- Why is this person standing in front of you?
- Introduction to Aon Risk Services Company (ARC)
- What is the SOC role?
- Toughest challenges

Who am I?

- IT Security professional since 2010
- Primary experience with Regional Engineering, Cyber and Business Continuity and Advisory industries
- Currently leading a team of 20 technicians for Aon Risk Services
- Currently managing the SOC Security Operations Center (SOC)
- Participating Board seat in ISO 27001
- A digital, Social, etc.
- Backend/Cloud/Network

Yahya Ebrahimi - Aon Risk Services Company

- A creative team across the globe
- Just added a new member today
- Prepping for another exciting year
- Blanks and more
- Digital, Social, etc.
- Security operations, cloud security, Aon/ISO 27001

IT Security challenges under the Surface
Disclaimer

All views and opinions expressed are my own. I am not a spokesperson for Saudi Aramco or Aramco Overseas Company.
When a SOC is more than a SOC

- Who is this person standing in front of you?
- Introduction to Aramco Overseas Company (AOC)
- What is the AOC SOC?
- Toughest challenges
Who am I?

- IT Security professional since 1993
- Primary experience with financial, engineering, automated food manufacturing and defense industries
- Currently leading a team of 10 rock stars for Aramco Overseas Company for our Security operations Center
- Published with lots of certs- CISSP, MCDBA, C|EH, ArcSight, CheckPoint, etc.....
- I get paid for my hobby
Introduction to Aramco Overseas Company

- A services company primarily for Saudi Aramco
- Just celebrated 61 years young
- Primary EMEA materials sourcing for Saudi Aramco
- Global joint venture recruitment
- Expat recruitment EMEA based for Saudi Aramco
- Quality control and management of supply chain and sourced goods
- Global logistics
- IT Services including digital security for global the Aramco Overseas Company network
IT Security challenges under the surface
Diverse and Dispersed

Multiple types of business units
Multiple physical locations
  Joint ventures and project teams sharing networks with direct competitors
  Locations in far-flung areas
  Drastically different privacy and data protection regulations
Global network - network coverage in every country with a commercial presence except USA, Canada and Saudi Arabia
Challenges

- Lack of a common framework to exchange security intelligence information in a sanitized manner
- Although many in the oil, gas and energy industry are competitors on different levels we suffer many of the same risks and adversaries
- Some limited top level sharing of information doesn't translate well to IT operations for monitoring corporate or PCN networks
Proposed Solutions

- Operational collaboration between similar industry
- Usage of existing CERT information exchange standards for the industry wide threats and risks
- Active operational participation among operations groups, Incident response and CERT/CSIRT teams
- Operational, ground level approach

ENISA calls for better data sharing and interoperability among “Digital Fire Brigades” to...

Date: Nov 20, 2013
when a SOC is more than a SOC

- What is this person standing in front of you?
- Introduction to Aramco Overseas Company (AOC)
- What is the SOC? (IC)
- Immediate challenges

Who am I?

- IT Security professional since 2003
- Prior experience in finance, engineering, and defense industries
- Currently leading a team of 10 security for Aramco
- Co-founder and CEO of a Security solutions firm
- Published in the CIO, CIO MAGAZINE, 2018, as well as others
- CISO of CNT, etc.
- Lead, escalate, etc.

IT Security challenges under the surface

- Cybersecurity
- Information security
- IT Security
- CISO
- CIO
- CEO
- Board
- Compliance
- Regulations
- Laws