Security Monitoring

Ron Simmons, CISSP, GCIA, GCIH, GCFA
Incident Response and Forensics Lead

Agenda

- The Challenge
- The Security Solutions
- The Key Words
- The Impacts
- What it looks like
- Some Thoughts
- The Solution
- In the End

The Challenge

- Multiple Networks
  - A few ICS networks
    - All run by different groups
  - The Corporate Network
- Too many different security products
- Skillset
- Rolling the data up into a single view

The Security Solution

- Enterprise Solution
- Each ICS vendor or integrator has a recommendation
  - IDS/IPS
  - Logging
  - Security Monitoring

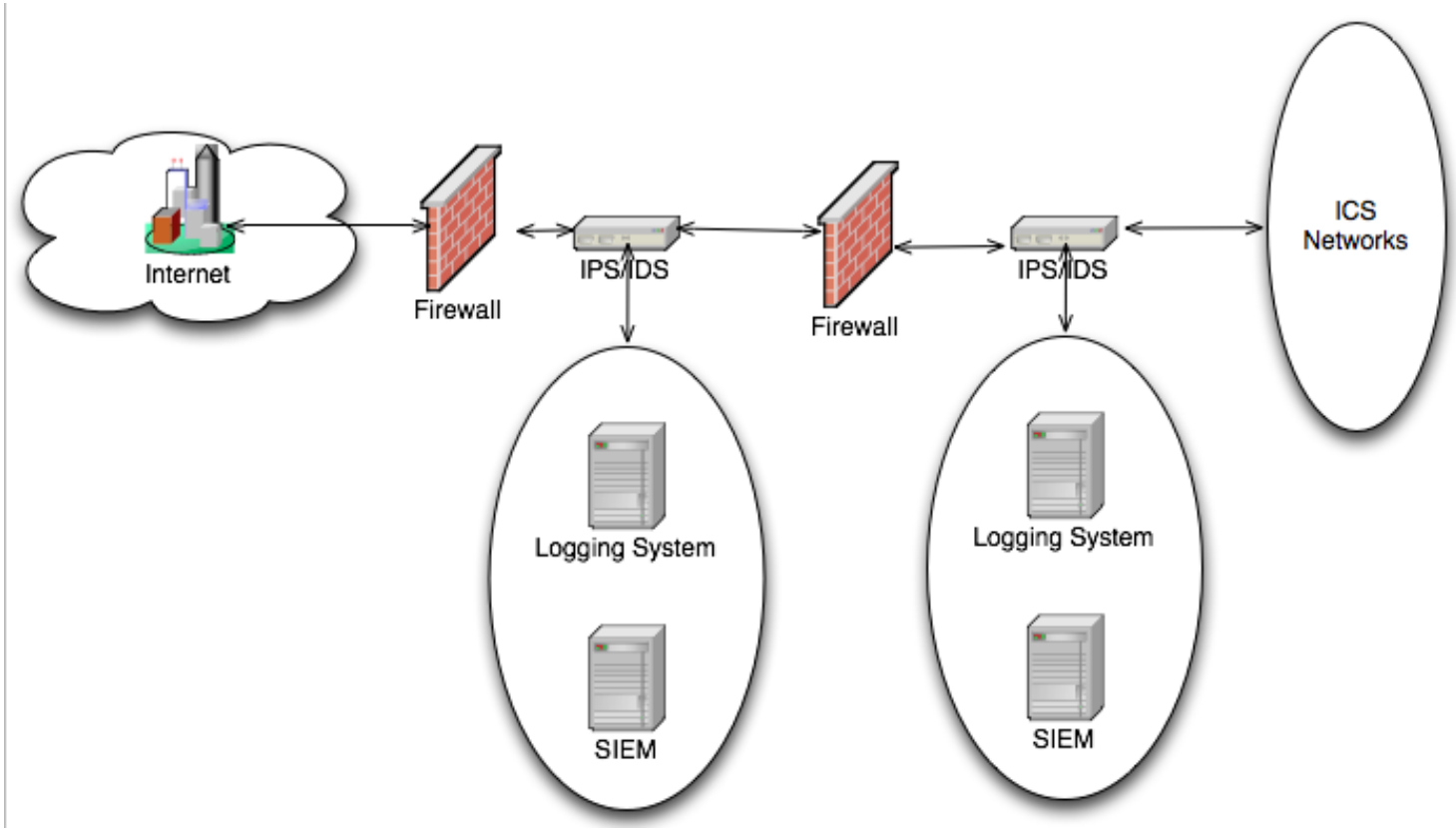
The Key Words

- We are NERC
  - Certified
  - Compliant
- We work with your ICS
- Other Utilities use this in their ICS environment
- We are Vendor X's preferred solution

The Impacts

- Financial impact (Multiple Solutions)
  - Support and Maintenance
  - Personnel
- Complexity for Operators, IT and Security Ops
  - Multiple systems
- Correlation with other systems
  - ICS Networks
  - Enterprise systems
- Visibility becomes a concern

What It Looks Like



Some Thoughts

- How are they getting in
  - Application
  - Web
  - Email
- Pivoting (Proxy) through the network
- Interconnected Systems
  - ICS with the Enterprise
  - Regulatory bodies
  - Vendor Support

The Solution

- A Single Enterprise solution
- Configuration simplicity
  - One parser language
  - Less Clients to Deploy
- Single vendor
- Event correlation with all log sources
  - Corporate and ICS
  - Email and Web
  - Proxy and Firewall

In The End

- Look at the big picture
- Less cost to the utility
- Ease of use for Staff
- Unified Security Monitoring

Questions?

- Ron Simmons
- rsimmons@sempra.com