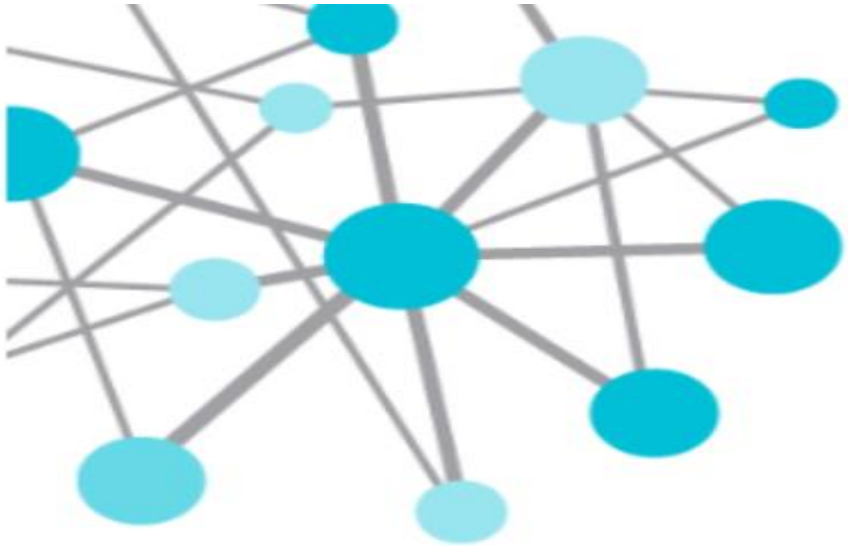
OSIsoft.



OSIsoft.
T&D USERS GROUP 2014
The Power of Data

ALBANY SEP 10-12 NEW YORK

DECISION READY IN REAL-TIME

Presented by

NERC CIP Version 5 and the PI System

Bryan Owen PE – OSisoft Cyber Security Manager

Agenda

- Update on OSIsoft Cyber Initiatives
- War Story
- CIP Version 5 Electronic Security Perimeter
- Research for PI System
- Conclusions

OSIsoft Security Engagements

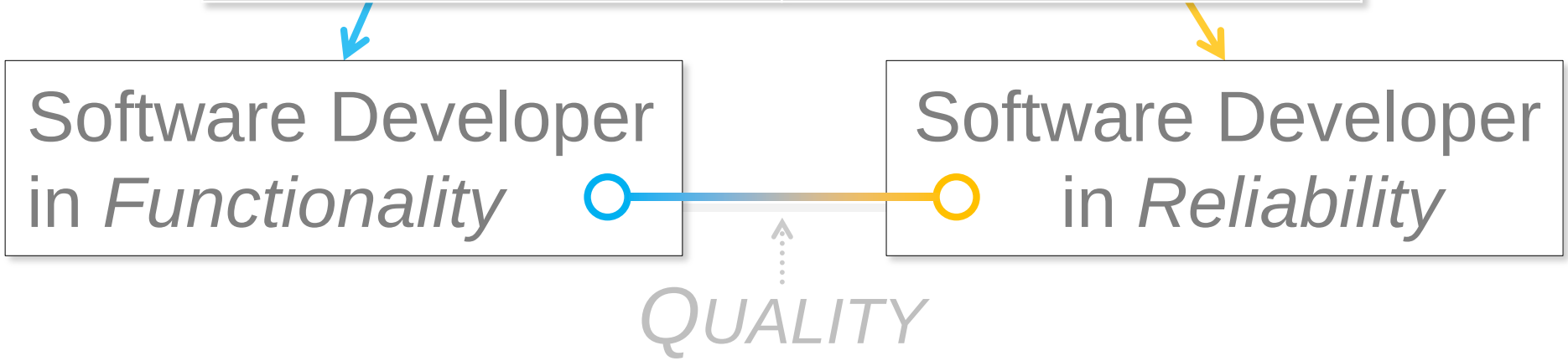
- **Idaho National Lab**
  - 2005 Assessment
  - 2008 vCampus Live!
  - 2009 vCampus Live!
  - 2011 Cooperative Research
  - 2012 vCampus Live! “Detect & Defend”
- **US Army NetCom**
  - 2009 CoN #201006618
  - 2013 CoN (recertified)
- **US NRC**
  - 2010 DISA, NIST
- **SAP QBS Certification**
  - 2012 Veracode
  - 2013 Veracode
- **Azure Penetration Testing**
  - 2014 PI Cloud Connect (Utility Partner)
  - 2014 PI Cloud Access (IOActive)
- **Microsoft Information Security Consulting**
  - 2009 PI Server
  - 2010 PI Agent
  - 2011 PI Coresight
  - 2011 PI AF
  - 2012 PI ProcessBook
  - 2012 Products in Design (3)
  - 2013 Engineering Management
  - 2013 Products in Design (3)
  - 2013 SDL for Security Champions
  - 2013/2014 Defensive Programming (Cigital)
- **Windows Logo Certification**
  - 2008 Windows 2008 Server Core
  - 2011 Windows 2008 R2 Server Core
  - 2012 Windows 2012 Server Core

OSIsoft SDL Leadership

- 4 Security Advisors (Core Team)
  - Incident response commanders
- 35 Security Champions
  - Senior Engineers
  - Every product represented
- IT Security Team
- Customer Support Security Team
  - NERC CIP Personnel Surety Program and Procedures

HEALTHY TENSION

Role 1	Role 2
Doing the “right things”	Doing “everything right”
Building innovative features	Making sure the product works
Generating user value	Preventing bad surprises
Writing a sustainable product architecture	Creating a sustainable infrastructure
Planning for future capabilities	Identify current/future threats
...	...
Focused on Functionality	Focused on Reliability



A Short ‘War’ Story

Technical Support Case of “Web Attack”

Somewhere in the galaxy PI, in the year 2013…

An intrusion prevention system detected

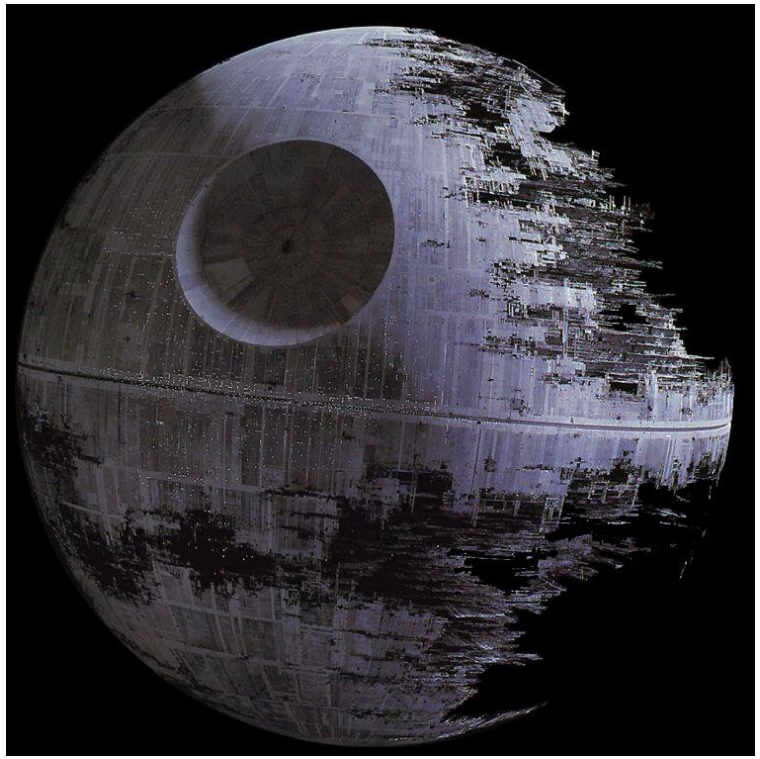
“Web Attack” on PI Webparts

Naturally, everyone was concerned.

What follows is an epic tale…

‘War’ Story

- Critical Infrastructure Environment
  - NERC CIP compliance
  - Access for external users
  - Intrusion prevention appliance
- Technical support activated incident response
  - False positive determination
  - Unresponsive IPS vendor
    - IPS signature development ‘outsourced’
  - Months to resolution

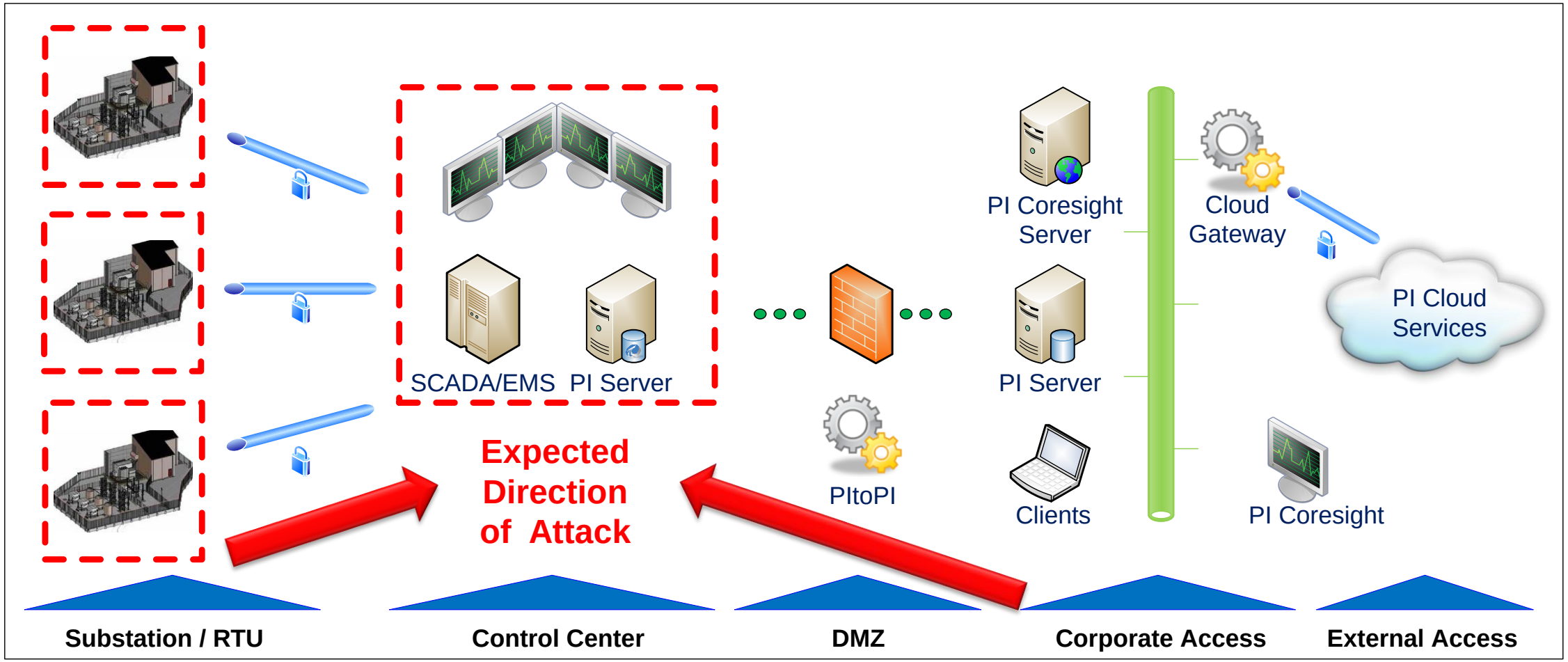


Lessons Learned

- Technical Support
  - Please do call on detections related to the PI System
  - Alert semantics matter “Web Attack”
- Signature based IPS
  - Automatic signature updates can ‘break’
  - False positive and false negative prone
- Blacklisting
  - Unsustainable approach

CIP-005-5
Electronic Security Perimeter

High Level T&D Solution Architecture



Electronic Security Perimeter

CIP-005-5 Table R1 – Electronic Security Perimeter		
Part	**Applicable Systems**	**Requirements**
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.

What is ‘malicious communication’?

HARMFUL PURPOSE

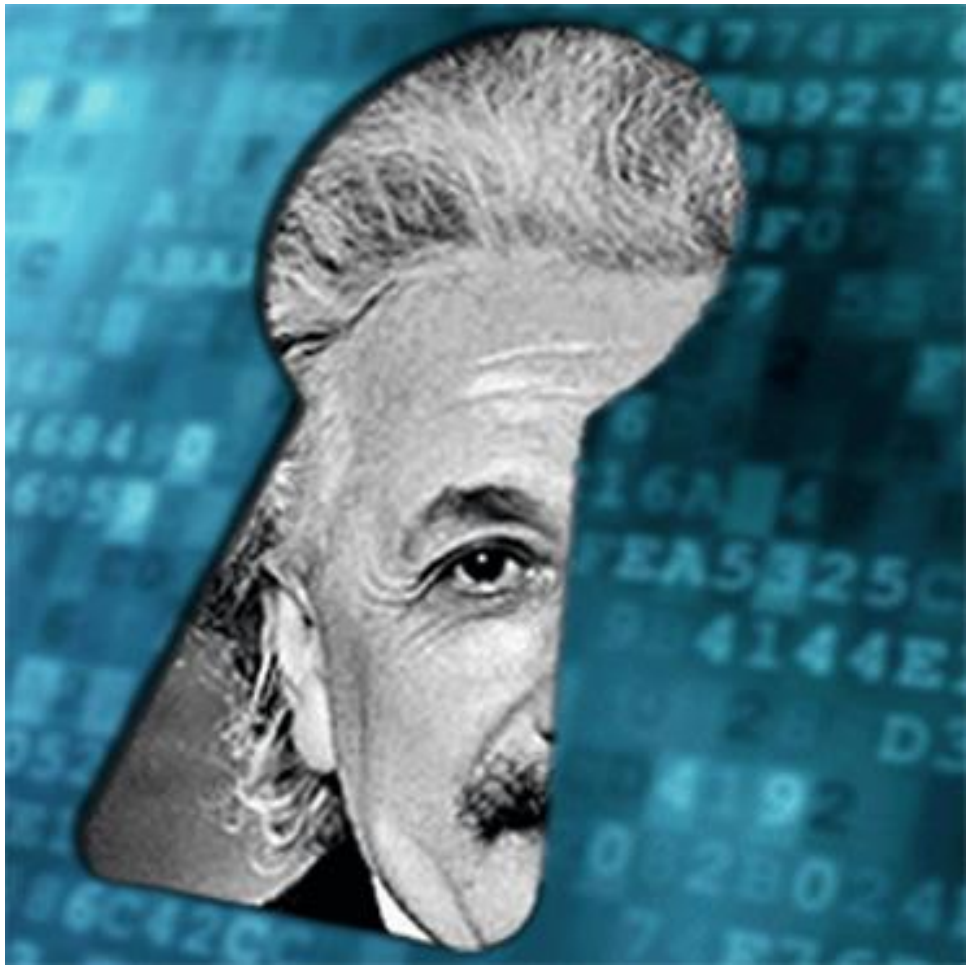
Unofficial: Not defined in the CIP standards or in audit worksheets.

Homeland Security “Einstein Program”

- IP addresses
- Domains
- E-mail headers
- Files
- Strings

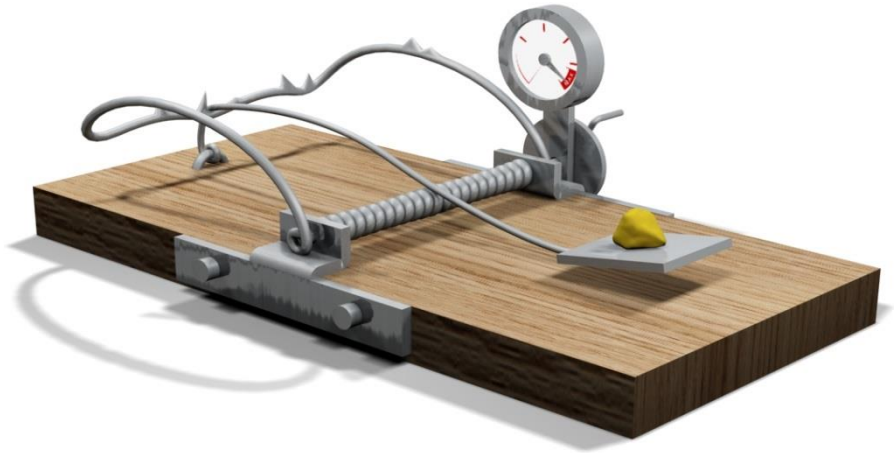
“1=1”

Common SQL Injection string fragment



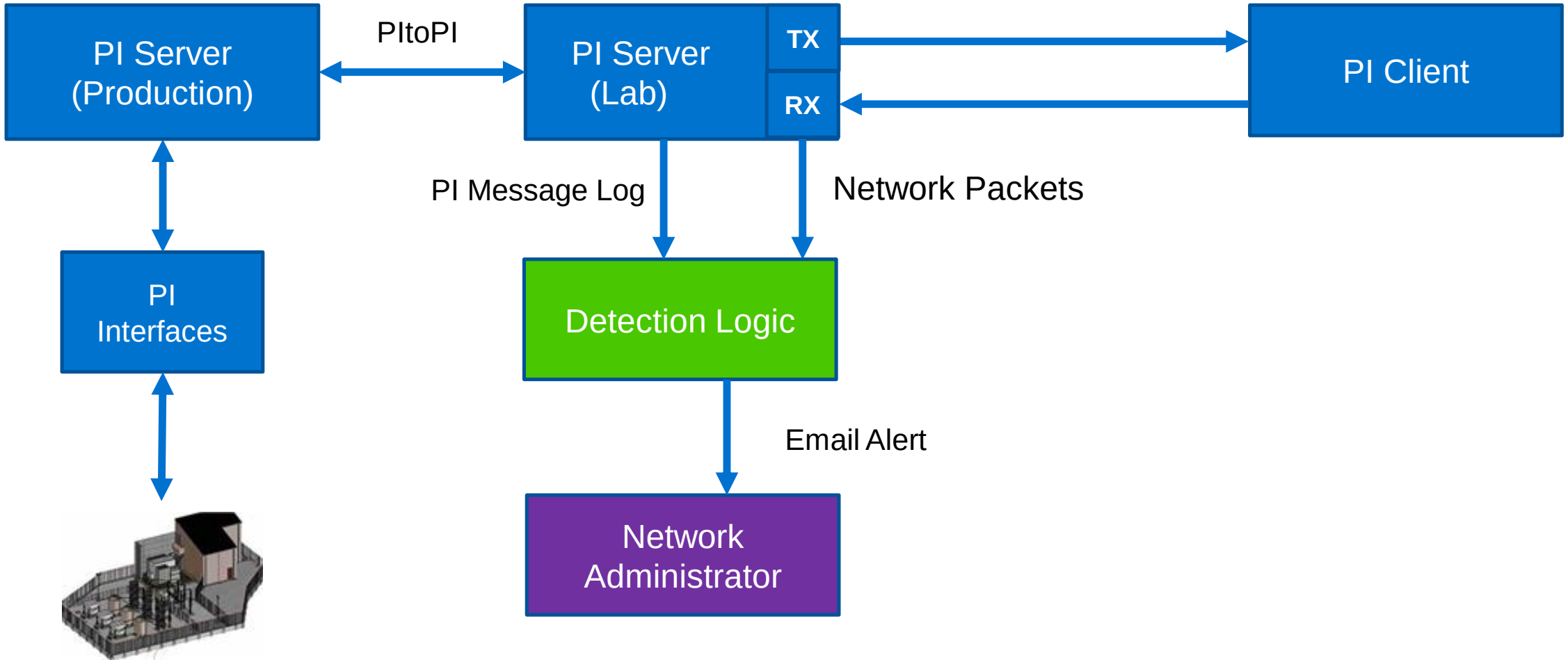
Einstein sensors for PI Server communication?

- IP addresses
  - Internal endpoints with private addresses
- Domains
  - Private DNS or alternative
- E-mail headers
  - Outbound notifications capable
- Files
  - Not a file transfer protocol
- Strings
  - Most communication is numeric

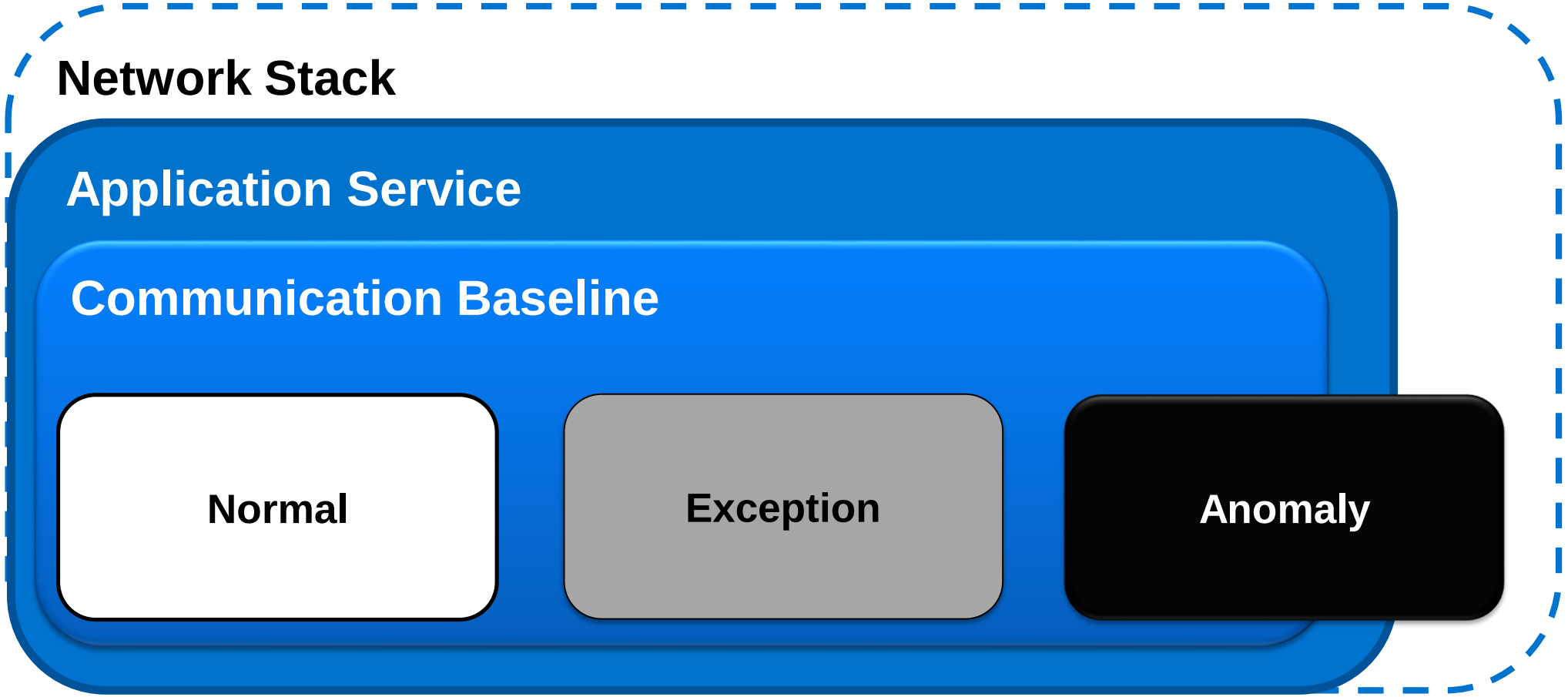


Research Project: Intrusion Detection for PI System

Test Bed



Approach: Baseline Normal Communication "Whitelisting"



Packet Detection “Whitelist”

- Test Case: Client Authentication

  - Timing
    - How long has it been between consecutive authentication attempts?

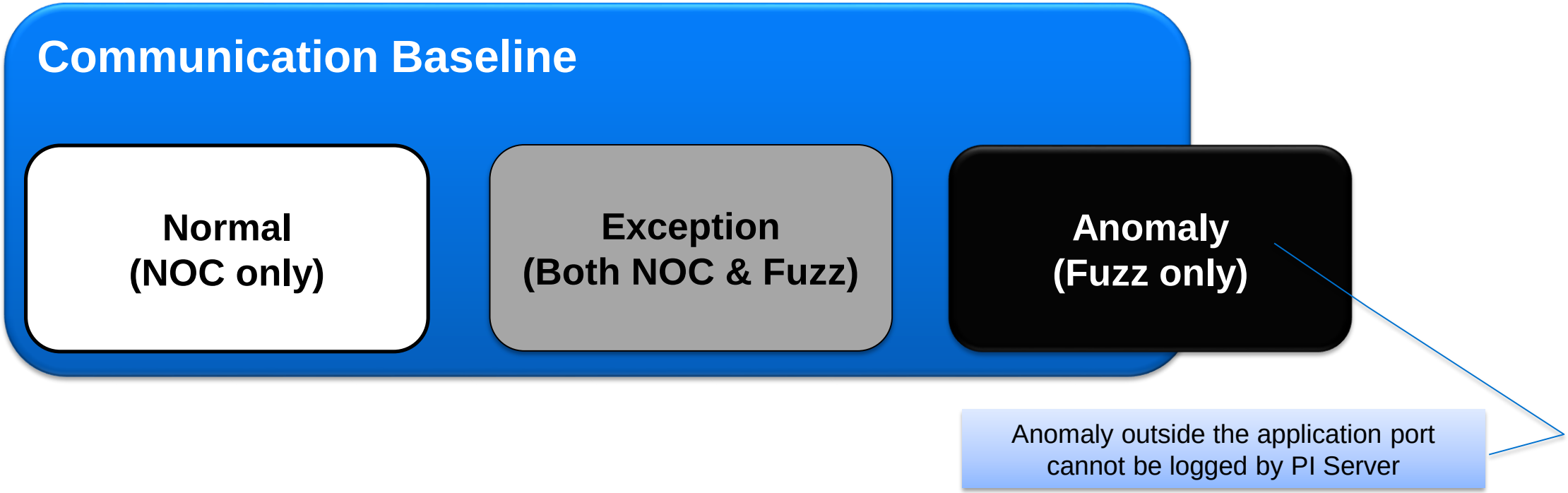
  - Ordering
    - Did the packets arrive in the correct sequence?

  - Consistency
    - Is packet payload consistent with protocol requirements?

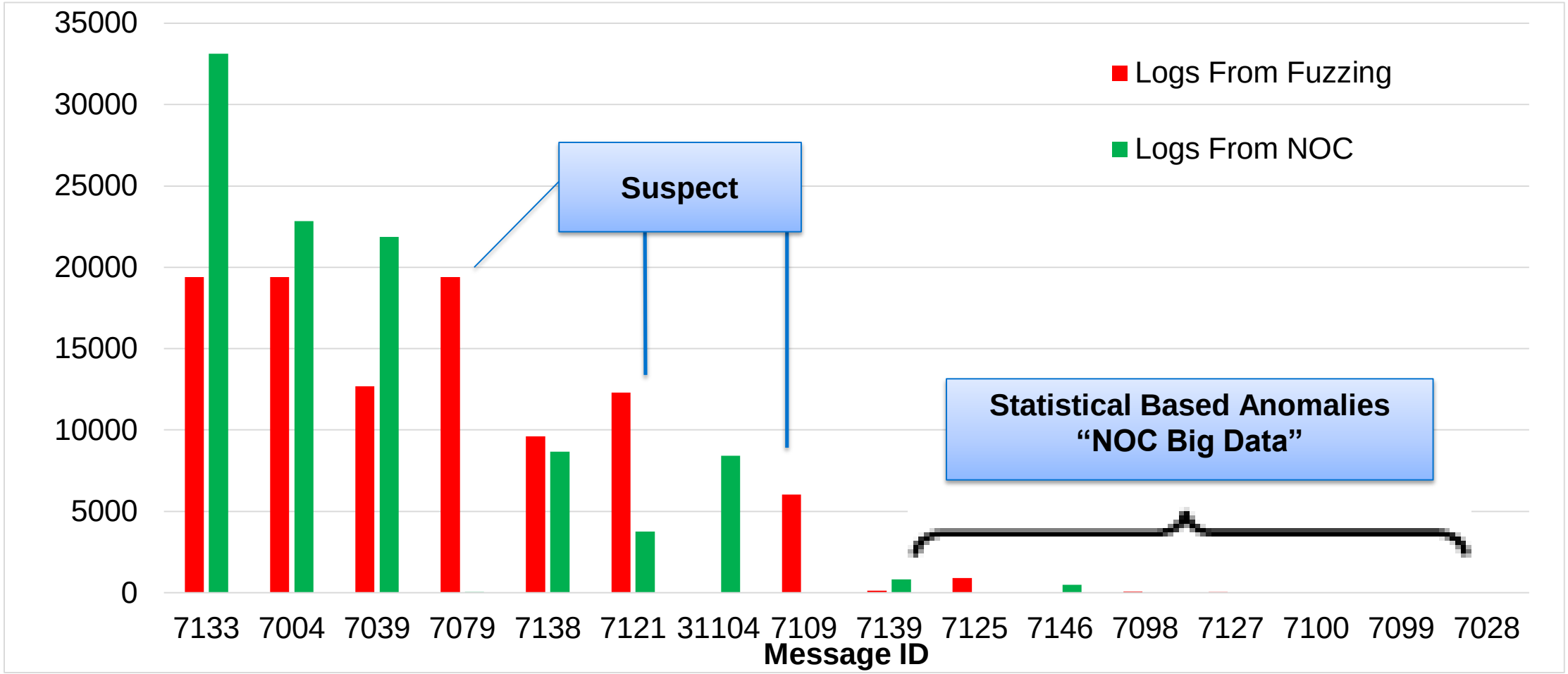
Test Methods: Generating Unusual Input

PI Message Log Baselines

- Normally ‘Good’
  - OSIsoft NOC Data Set
- Normally ‘Bad’
  - Fuzz Test Runs



Authentication Logs – Frequency Chart



Detection Capability with Both Sources

Class	Packet Inspection	PI Message Log
Timing	√	√
Sequence	√	
Consistency	√	√
Context*		√

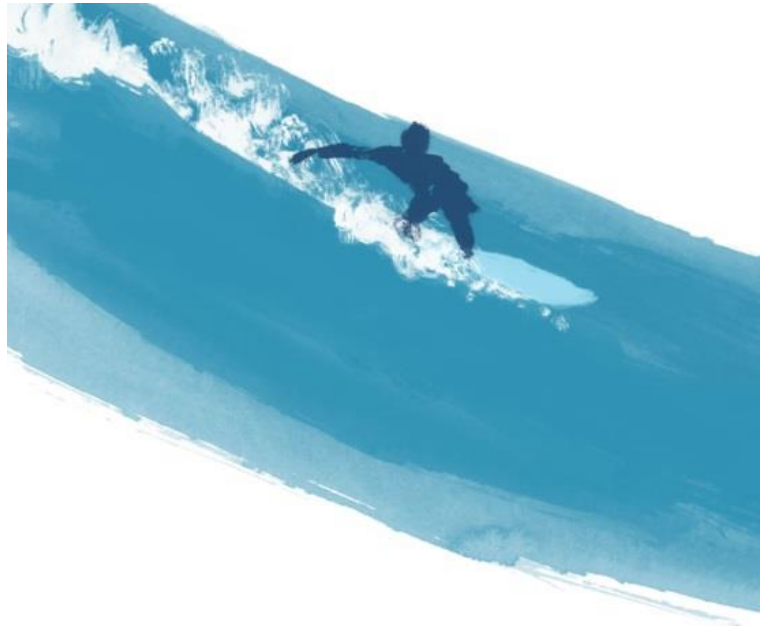
* Context such as user permissions is server side only (eg. whitelist read-only connections)

Summary

Electronic Security Perimeter

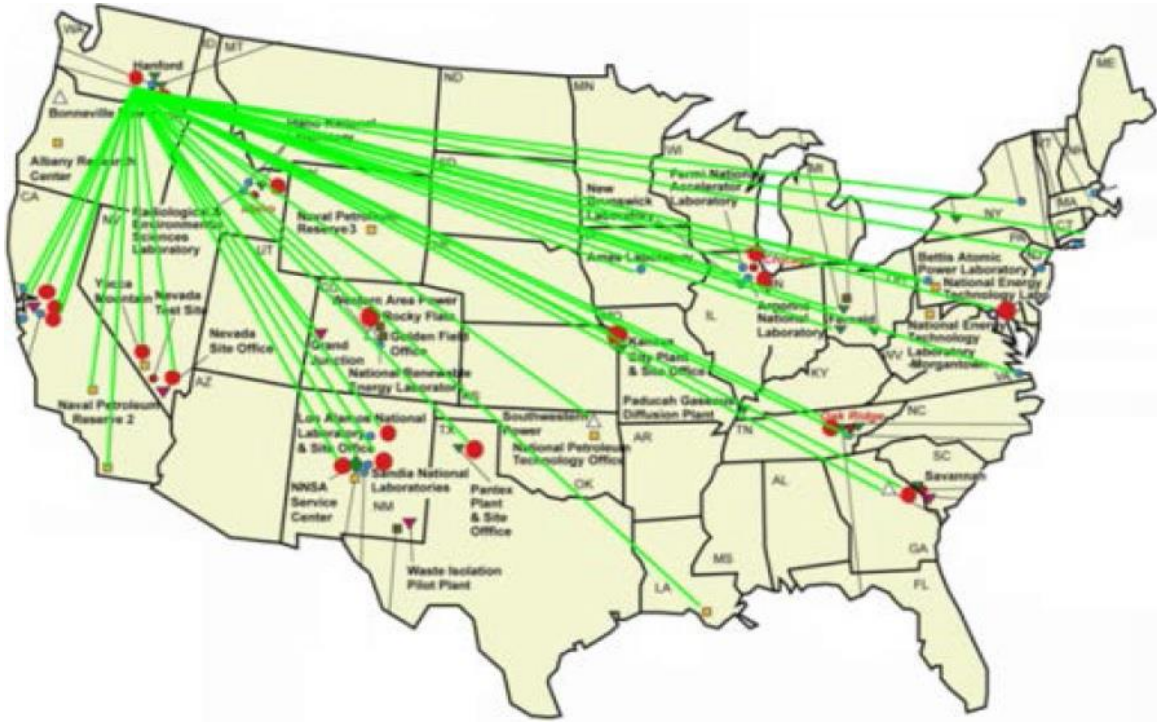
- Compliance
  - [CIP-005-5 R1.5] Access point firewall with commercial IDS module
  - Define “known or suspicious” malicious communication

- Security
  - Keep web servers and ‘surfers’ out of DMZ
  - Use PItoPI across ESP
  - Configure “Read Only” access where possible
    - [Consider absolute enforcement solutions]



Thoughts on Intrusion Detection for PI System

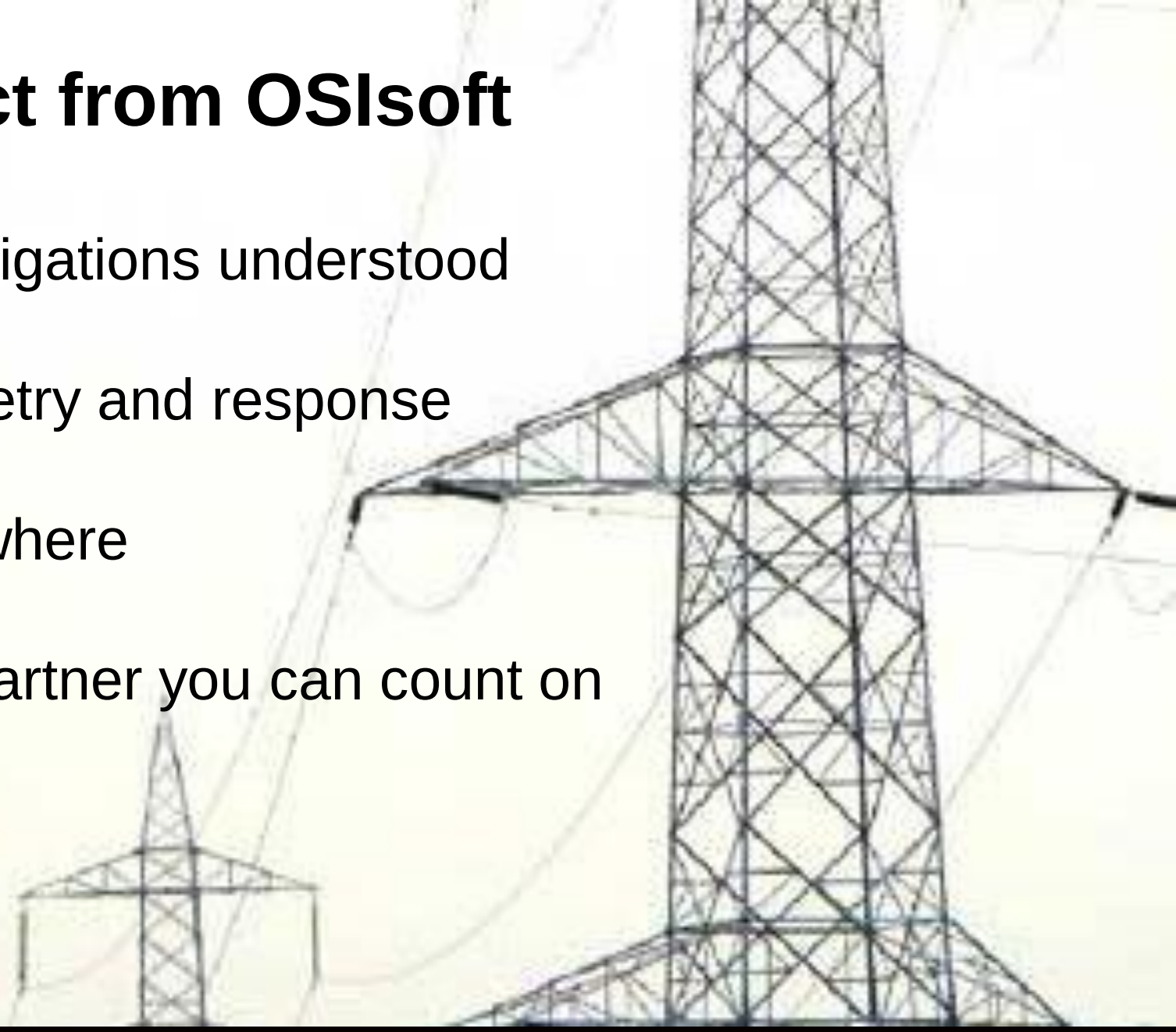
- Lower expectations
  - Intruders look like insiders
  - Deep packet inspection insufficient
- Higher expectations
  - Big Data approach
  - OSIsoft NOC monitoring



US DoE “CRISP” Monitor Map – National Labs and Industry Partners

What you can expect from OSIsoft

- Attendant threats and mitigations understood
- Increased logging, telemetry and response
- Transport security everywhere
- Data infrastructure and partner you can count on



References

KB00354 - Windows Security Requirements for PI Server
KB00833 - Seven best practices for securing your PI Server
KB00994 - Whitelisting with AppLocker
KB01062 - Anti-virus Software and the PI System
2820OSI8 - Which firewall ports should be opened for a PI Server?
Microsoft Security Patch Compatibility

Thank you

777 Davis St., San Leandro, CA 94577