SAND2007-1337C

New Era in Cyber Security Technology Development

LOGIIC™

Combining the Power of the Oil and Gas Industry, DHS, and the Vendor Community to Combat Cyber Security Threats

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

LOGIIC™

Presenters

- Ben Cook – Sandia National Labs
- Tom Aubuchon – Advanced Software Engineering
- Bryan Richardson – Sandia National Labs
- Leeanna Demers – ArcSight

http://www.logiic.org

NOTE: This is a condensed version of the presentations given at the DHS LOGIIC Cyber Security Project Presentation.

Topics

- **Tom Aubuchon**
  - **Government Industry Partnership: LOGIIC**
  - **LOGIIC Correlation Project (LOGIIC-1)**
  - **Overview**
  - **Project Model**
  - **PCS/PCN Lab Environment**
- Bryan Richardson
  - Attack Detection In Control Systems
  - Deploying Defense in Depth
  - Attack Scenarios
- Tom Aubuchon
  - Accomplishments
  - Successes
  - Example Correlation Results
  - Impact
- Leeanna Demers – LOGIIC 1 Correlation Demo

LOGIIC™ Defined

- **Linking the**
- **Oil and**
- **Gas**
- **Industry to**
- **Improve**
- **Cyber Security**

- **Forward looking** opportunity to reduce vulnerabilities of oil and gas process control environments.
- Create **a working model** to leverage the collective resources of the Oil & Gas Industry, government agencies, and national laboratories for future cyber-security projects

LOGIIC™ Correlation Project

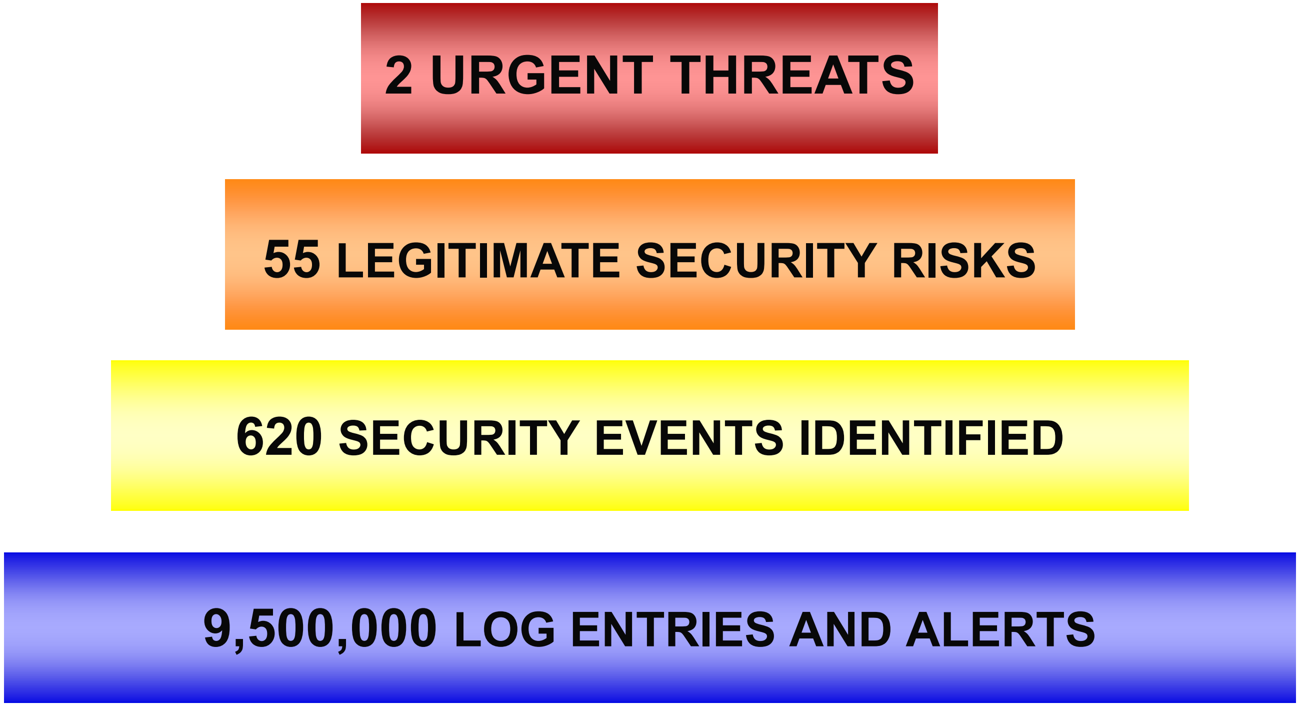
An Implementation of the Partnership Model

- LOGIIC-1: 12-month Technology Integration & Demonstration
- 1st Attempt to address an Oil & Gas Critical R&D need
- Jointly Supported By Industry Partners And The U.S. DHS
- Industry Contributes
  - Requirements and operational expertise
  - Project management
  - Product vendor channels
- DHS Science &Technology Contributes
  - National Security Perspective on threats
  - Access to long term security research
  - Independent researchers with technical security expertise
  - Testing facilities

LOGIIC Correlation Project

Addressing A Critical Need

- **PCN Monitoring: An Overwhelming Task**
- 1 Firewall; 1 Intrusion Detection device; 1 month



2 URGENT THREATS

55 LEGITIMATE SECURITY RISKS

620 SECURITY EVENTS IDENTIFIED

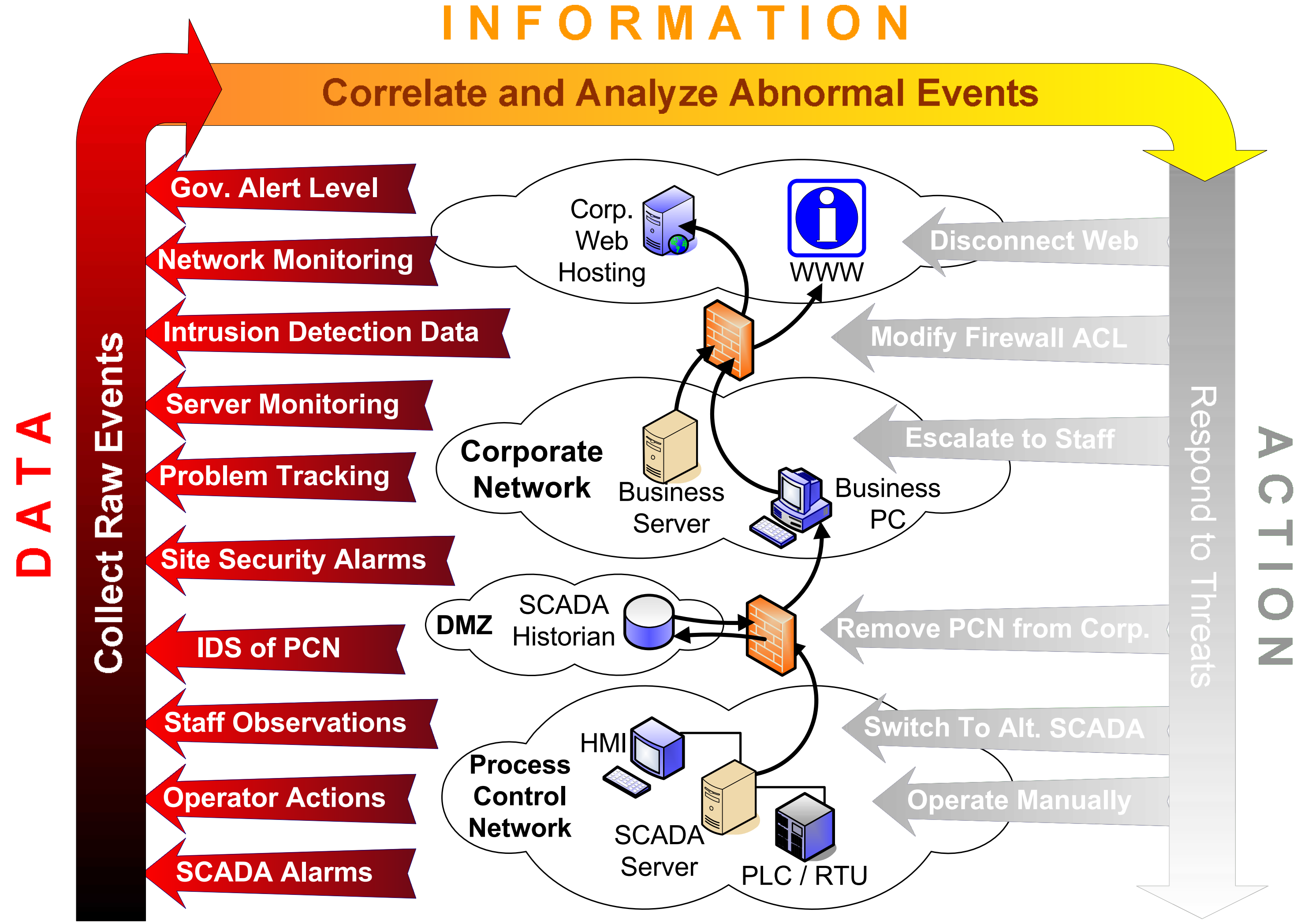
9,500,000 LOG ENTRIES AND ALERTS

LOGIIC Correlation Project

Overview

- Opportunity Statement
  - Reduce vulnerabilities of O&G PCS environments
    - by correlating and analyzing abnormal events
    - to identify and prevent cyber security threats
- Goals
  - Produce solution for use in industry operations
  - Defense in depth analysis of abnormal events
  - Ability to correlate abnormal events from
    - Business network
    - PCN interfaces
    - PCN directly
- What it is not

LOGIIC™ Correlation Project Model



INFORMATION

Correlate and Analyze Abnormal Events

DATA

Collect Raw Events

Gov. Alert Level

Network Monitoring

Intrusion Detection Data

Server Monitoring

Problem Tracking

Site Security Alarms

IDS of PCN

Staff Observations

Operator Actions

SCADA Alarms

Corp. Web Hosting

WWW

Corporate Network

Business Server

Business PC

DMZ

SCADA Historian

Process Control Network

HMI

SCADA Server

PLC / RTU

Disconnect Web

Modify Firewall ACL

Escalate to Staff

Remove PCN from Corp.

Switch To Alt. SCADA

Operate Manually

Respond to Threats

ACTION

LOGIIC™ Correlation Project

Challenges

- Technical
  - Identify what abnormal PCS/PCN events are
  - How to detect abnormal events within PCS/PCN
- Temporal
  - 12 Months to complete both “R” & “D”
- Organizational
  - Multiple Industry Partners
  - Multiple Gov interfaces (DHS; Lab; Researchers)
  - Disparate Vendor community

LOGIIC™ Correlation Project

Milestones

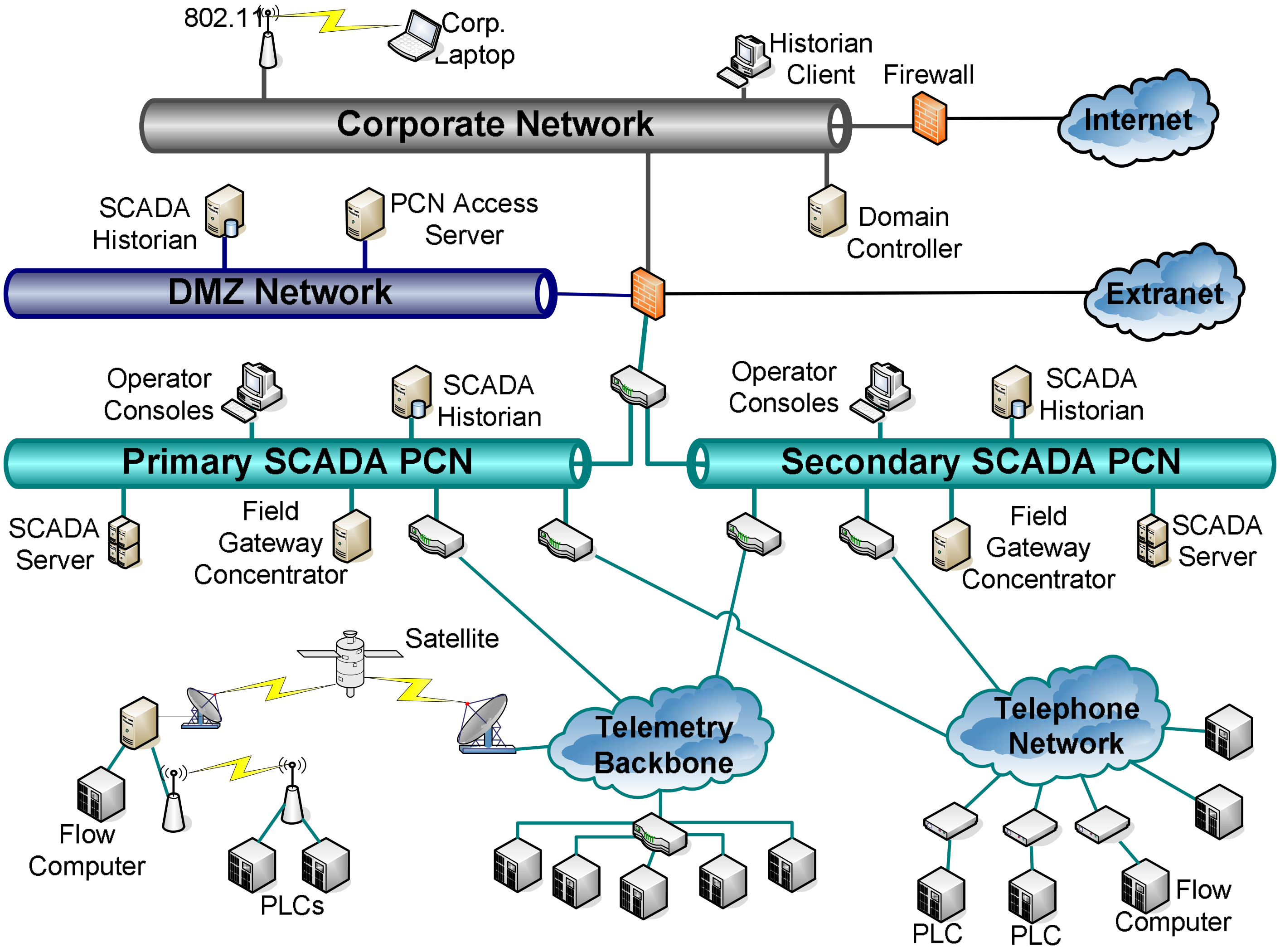
- Identify typical O&G PCS/PCN environments
- Create typical O&G PCS/PCNs within Lab Constraints
- Develop attack scenarios for PCS/PCN environments
- Select security sensors for use in PCS/PCN
- Integrate a best-in-class correlation engine
- Implement all components in test bed
- Simulate attacks from corp., public, partner, and PCS/PCN

LOGIIC Correlation Project Approach

- Divide and conquer: Three sub teams created
  - PCS Security Sub Team
    - Identify data sources available in PCS environment
    - Define security events that can be detected from the data
    - Define Attack Scenarios
  - IDS Sub Team
    - Identify security sensors
    - That can be deployed into the PCN environment
  - Correlation Sub Team
    - Identify correlation engine solutions that support:
      - Correlate data from various sources
      - Identify signatures
      - Identify anomalous events

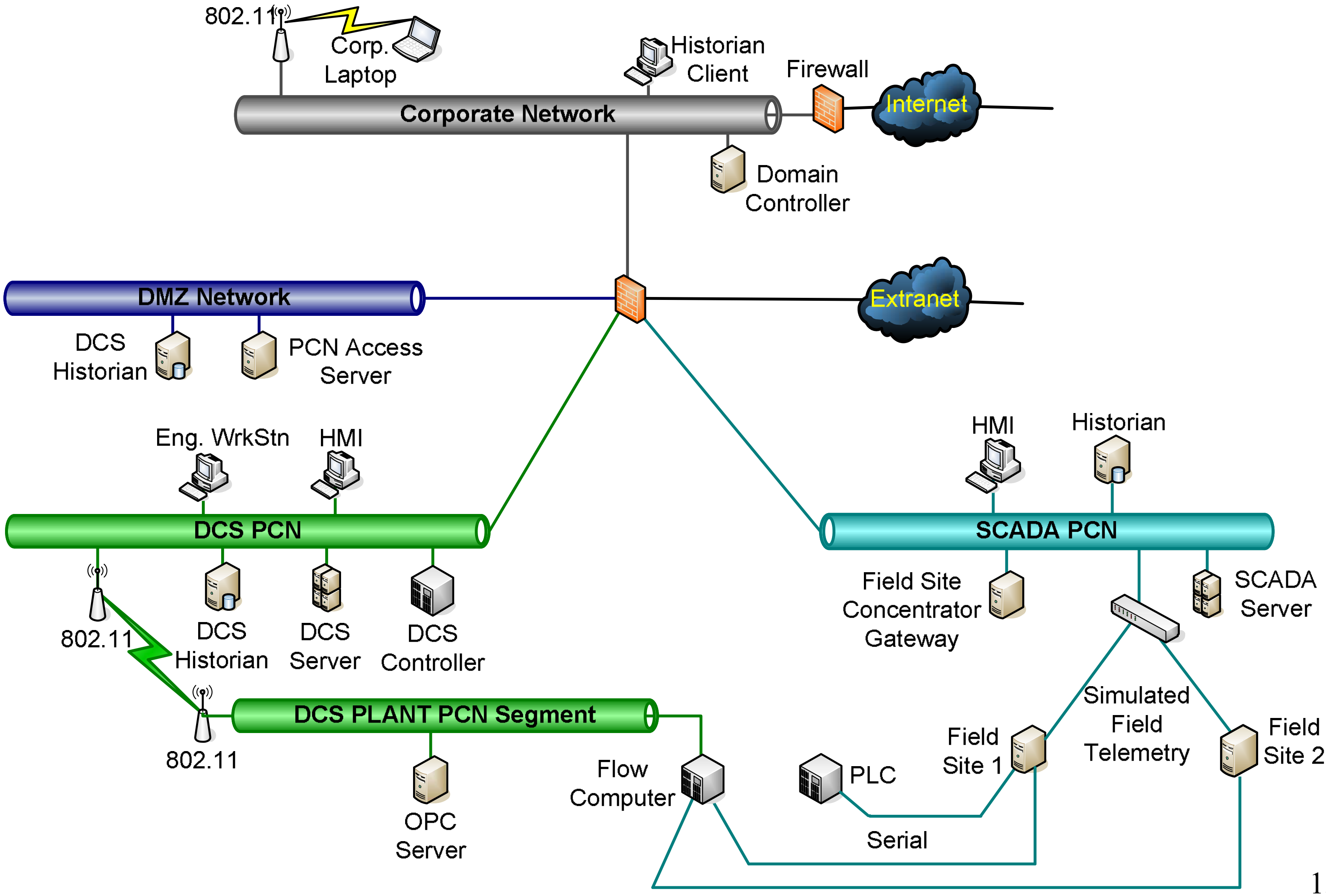
LOGIIC Correlation Project

No Such Thing as “Typical”



LOGIIC™ Correlation Project

Baseline O&G PCS/PCN Lab Environment



LOGIIC™ Correlation Project
Hypothetical Attack Scenario Creation

- Formulated in a collaborative effort
  - LOGIIC Team security SMEs
  - Oil and Gas Industry Participants.
- Realistic but Hypothetical
- Vulnerabilities explicitly added to Lab

Topics

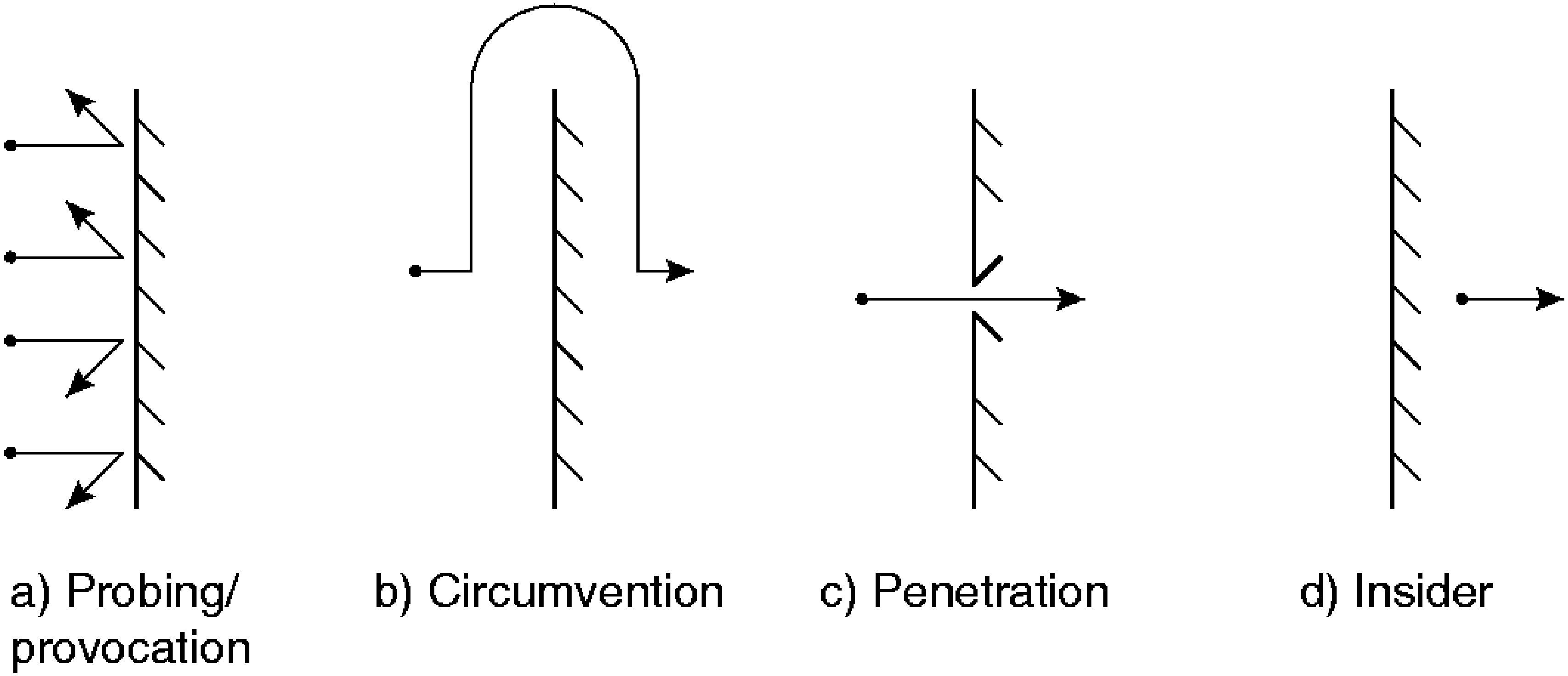
- Tom Aubuchon
  - Government Industry Partnership: LOGIIC
  - LOGIIC Correlation Project (LOGIIC-1)
  - Overview
  - Project Model
  - PCS/PCN Lab Environment
- **Bryan Richardson**
  - **Attack Detection In Control Systems**
  - **Deploying Defense in Depth**
  - **Attack Scenarios**
- Tom Aubuchon
  - Accomplishments
  - Successes
  - Example Correlation Results
  - Impact
- Leeanna Demers – LOGIIC 1 Correlation Demo

LOGIIC™ Correlation Project
Attack Detection in Control Systems

- Without detection, security response is blind
- Solutions exist for IT environments
- Prior to the LOGIIC Project, very little work on attack detection and correlation specifically tailored for control systems
- Technical challenge: Take existing solutions for IT and make them work in a realistic control system environment

LOGIIC Correlation Project

What Do We Want to Detect?

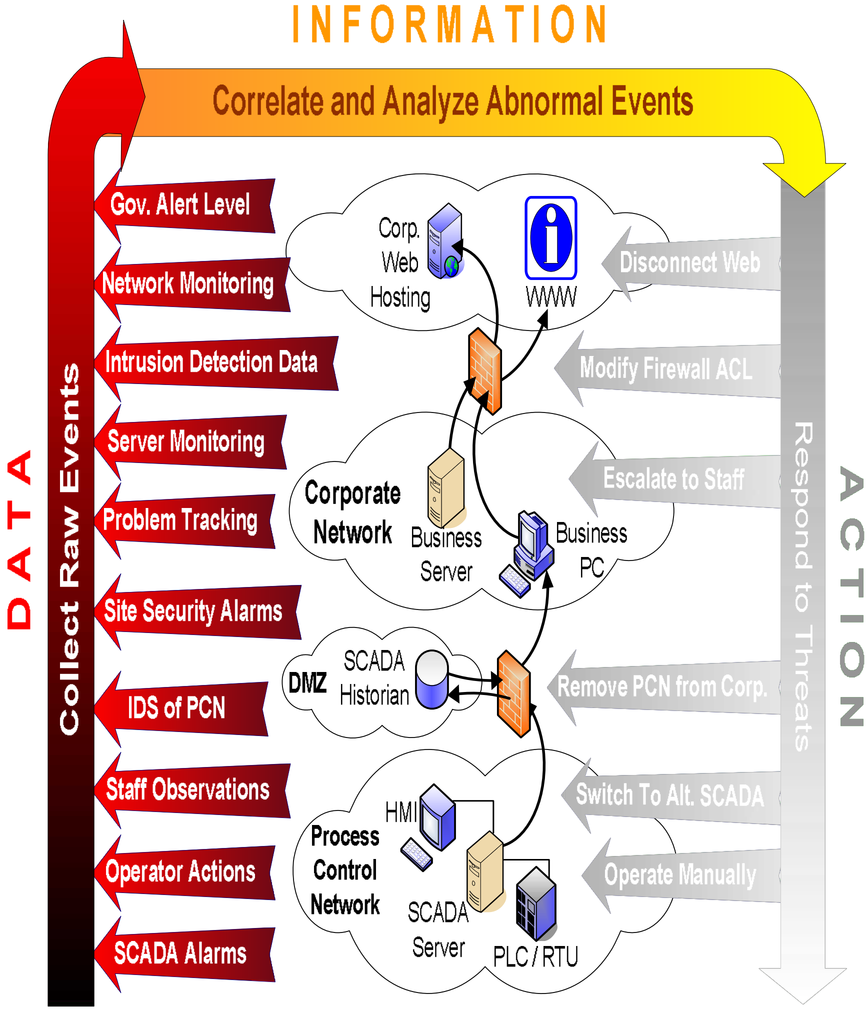


Lindqvist, U., *On The Fundamentals of Analysis and Detection of Computer Misuse*, Ph.D. Thesis, 1999

LOGIIC Correlation Project

Scoping Event Sources

- Standard IT Defenses
  - Network Segment Firewalls (in reporting mode, not blocking)
  - Host Firewalls (in reporting mode, not blocking)
  - Network Intrusion Detection Systems (IDS)
  - Network Devices (switches, routers, wireless devices)
- Control System Event Sources
  - Standard IT network IDS using signatures for a control system protocol (Modbus)
  - Alarms from SCADA and DCS systems
  - Alarms from a flow computer



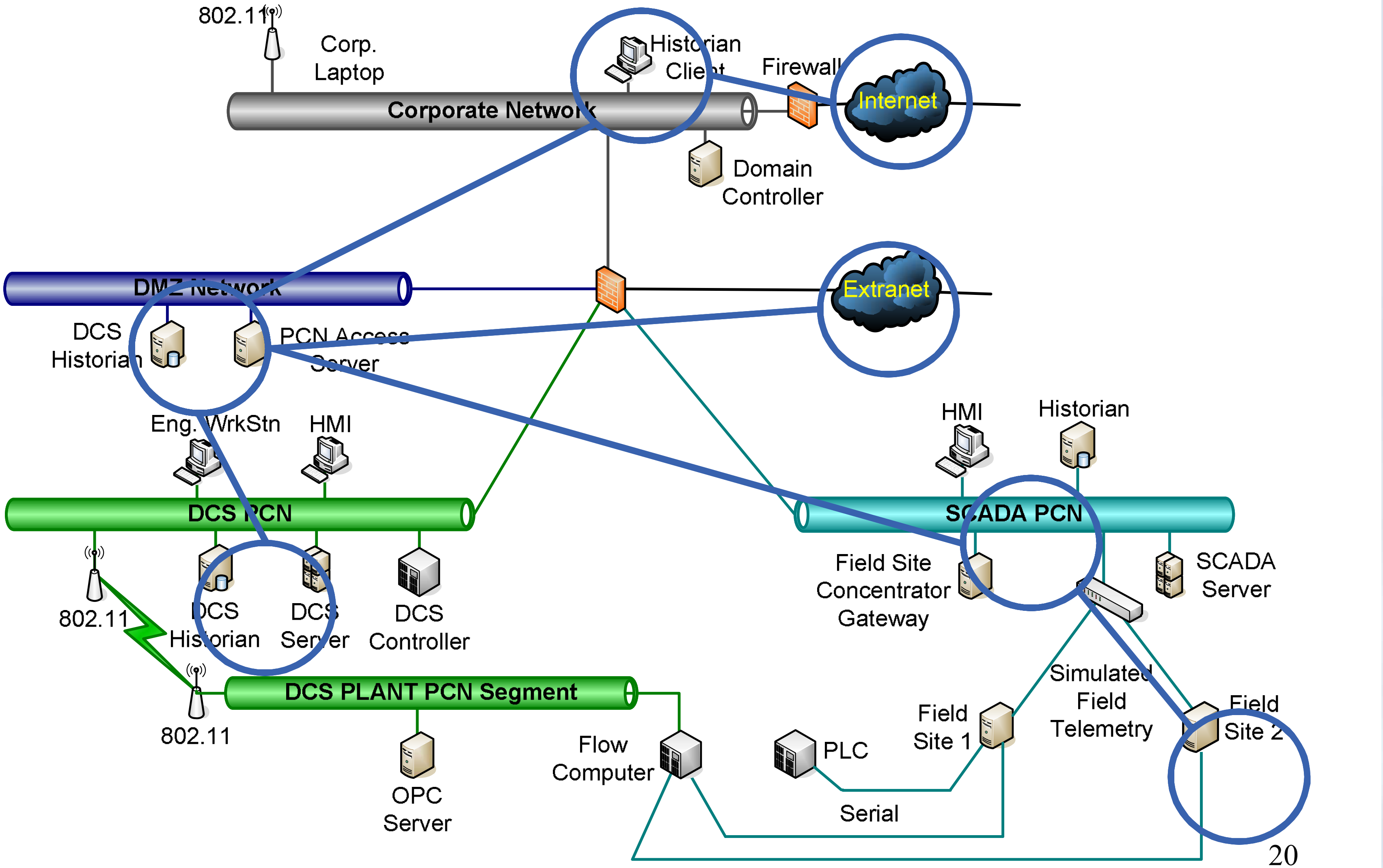
LOGIIC™ Correlation Project

Indicative PCS Disruption Events

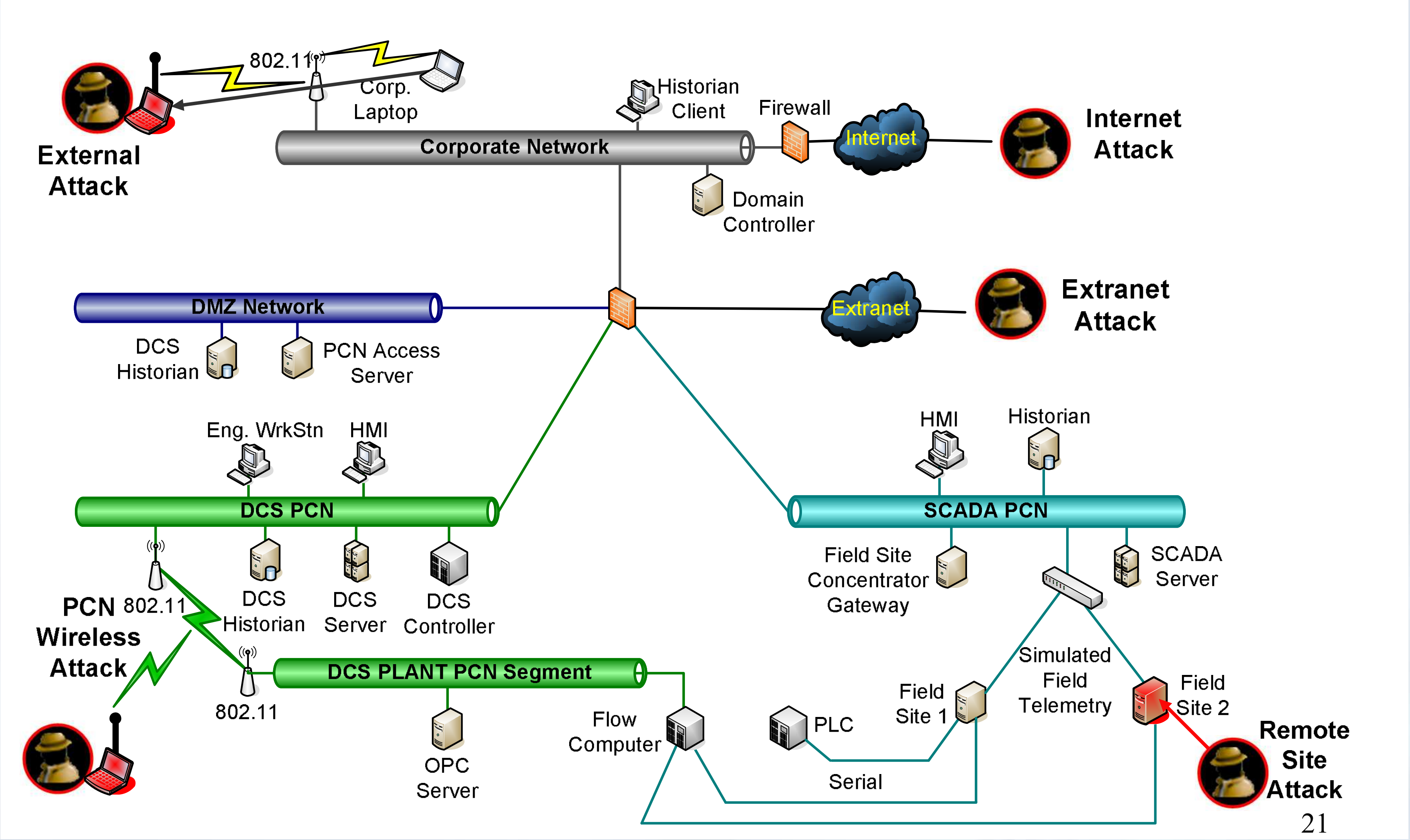
- Rogue Systems
  - All systems within PCS are assumed to be known
- Port Scans
  - This type of reconnaissance activity should not occur on PCS
- Modbus Exceptions
  - Modbus requests and responses should only originate from known masters and devices in PCS
- Configuration Changes
  - PCS networks are typically static networks
  - Ethernet configurations of devices in PCS should rarely change

LOGIIC™ Correlation Project

Vulnerability of Trust

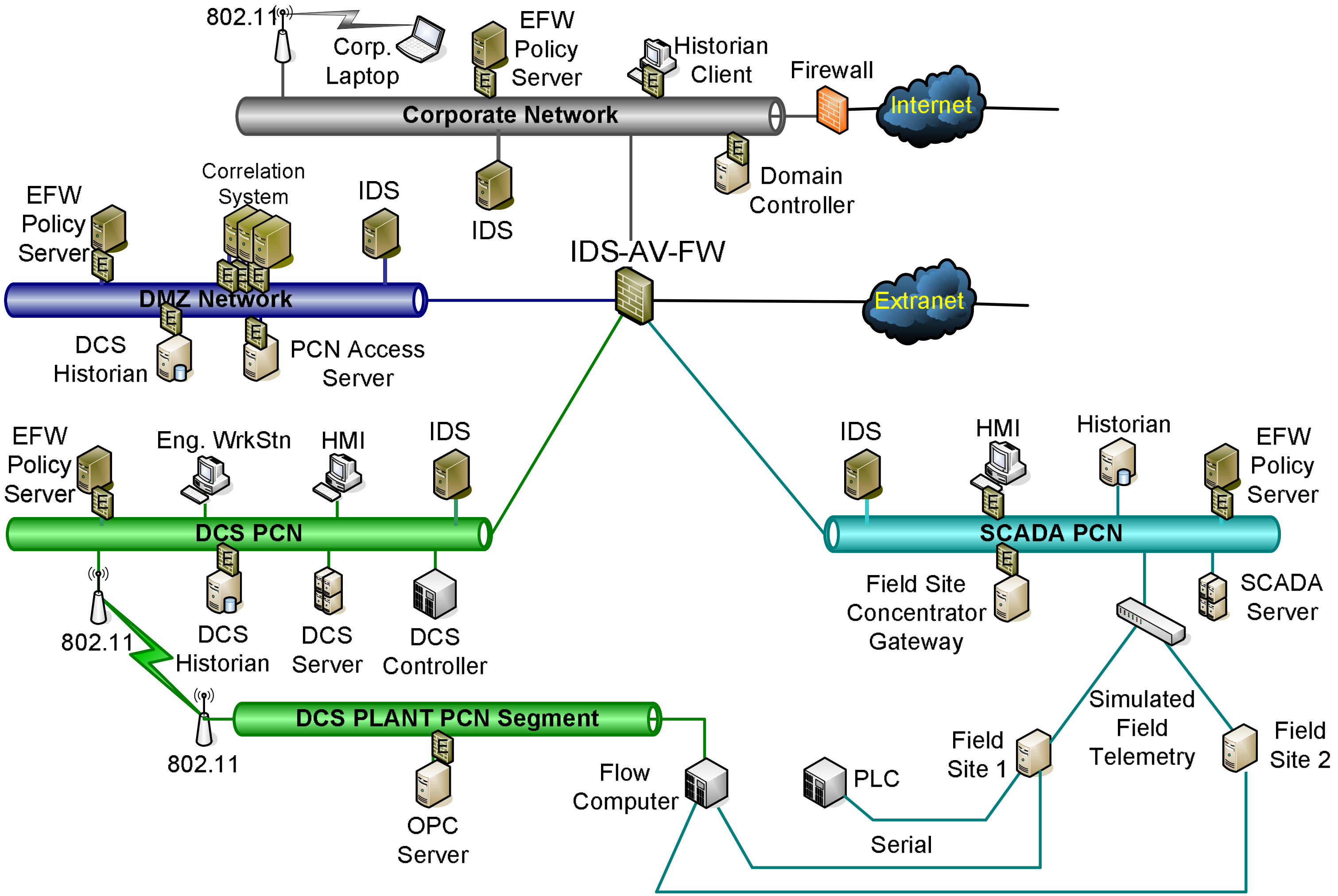


LOGIIC Correlation Project Potential Attack Vector Selection



LOGIIC™ Correlation Project

Deploying Defense In Depth

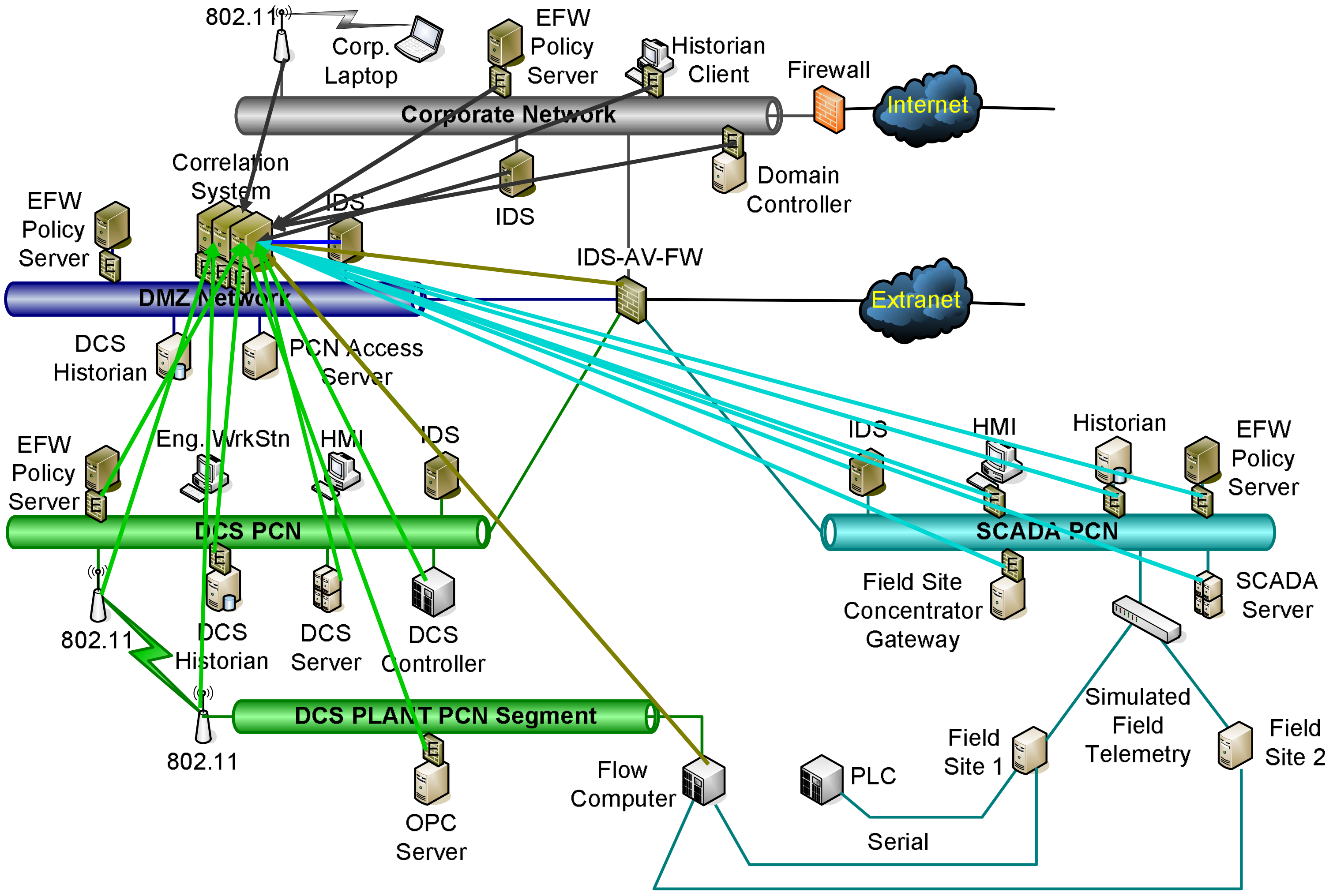


LOGIC™ Correlation Project

How does correlation work?

- Many event sources lead to information overload
  - Analysts need the big picture - Situational Awareness
- Event correlation
  - Discovers relationships between events
  - Infers the significance of those relationships
  - Builds a big picture of the network's health from many small data points
- A Correlation Engine Works by
  - Collecting all relevant event data
  - Normalizing the events
  - Categorizing events and prioritizing them
  - Filtering extraneous events
  - Aggregating similar events
- All of which lead to correlated events and situational awareness

LOGIIC Correlation Project
Defense in Depth Correlation Inputs

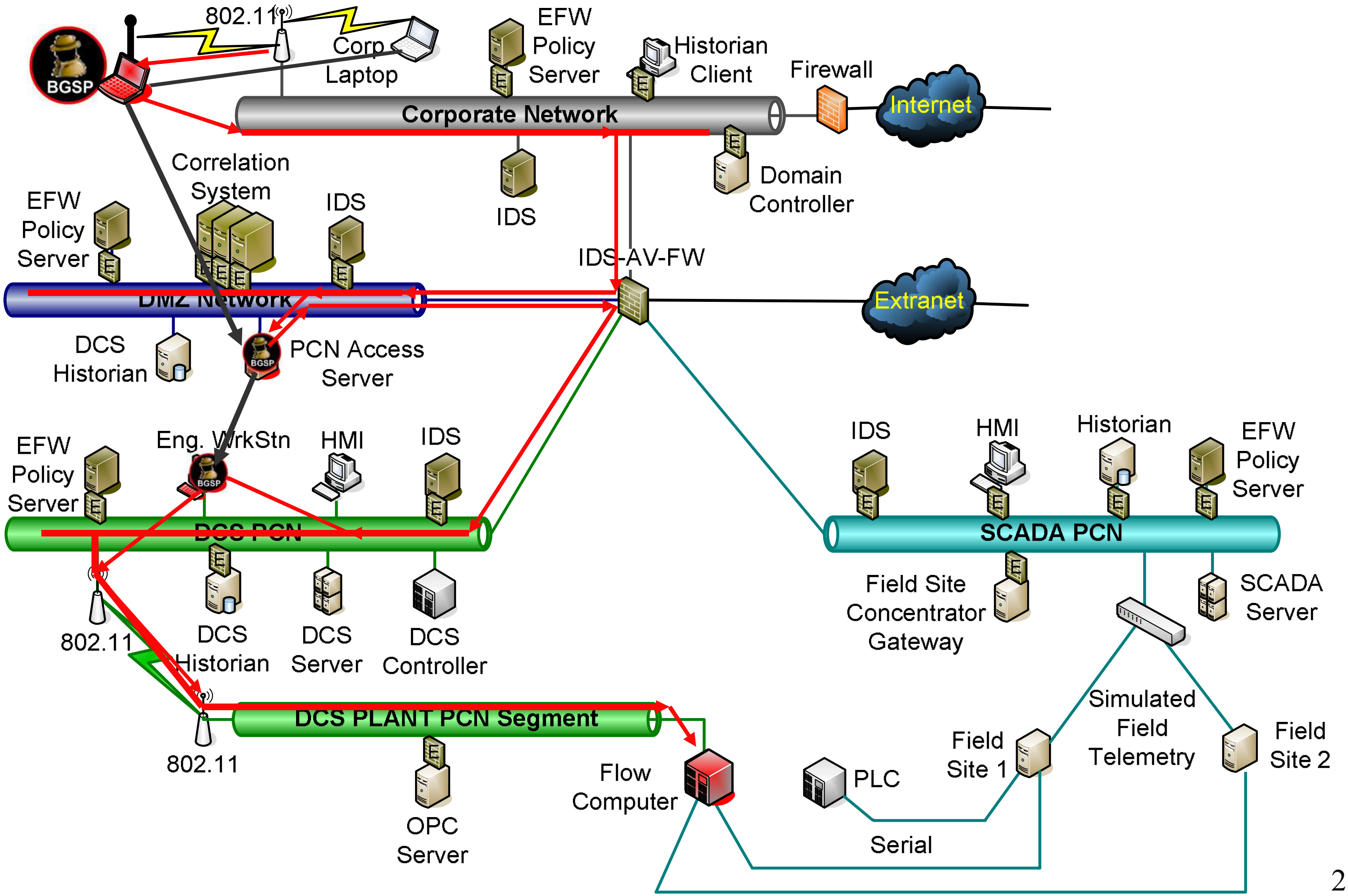


LOGIIC Correlation Project

Attack Scenarios

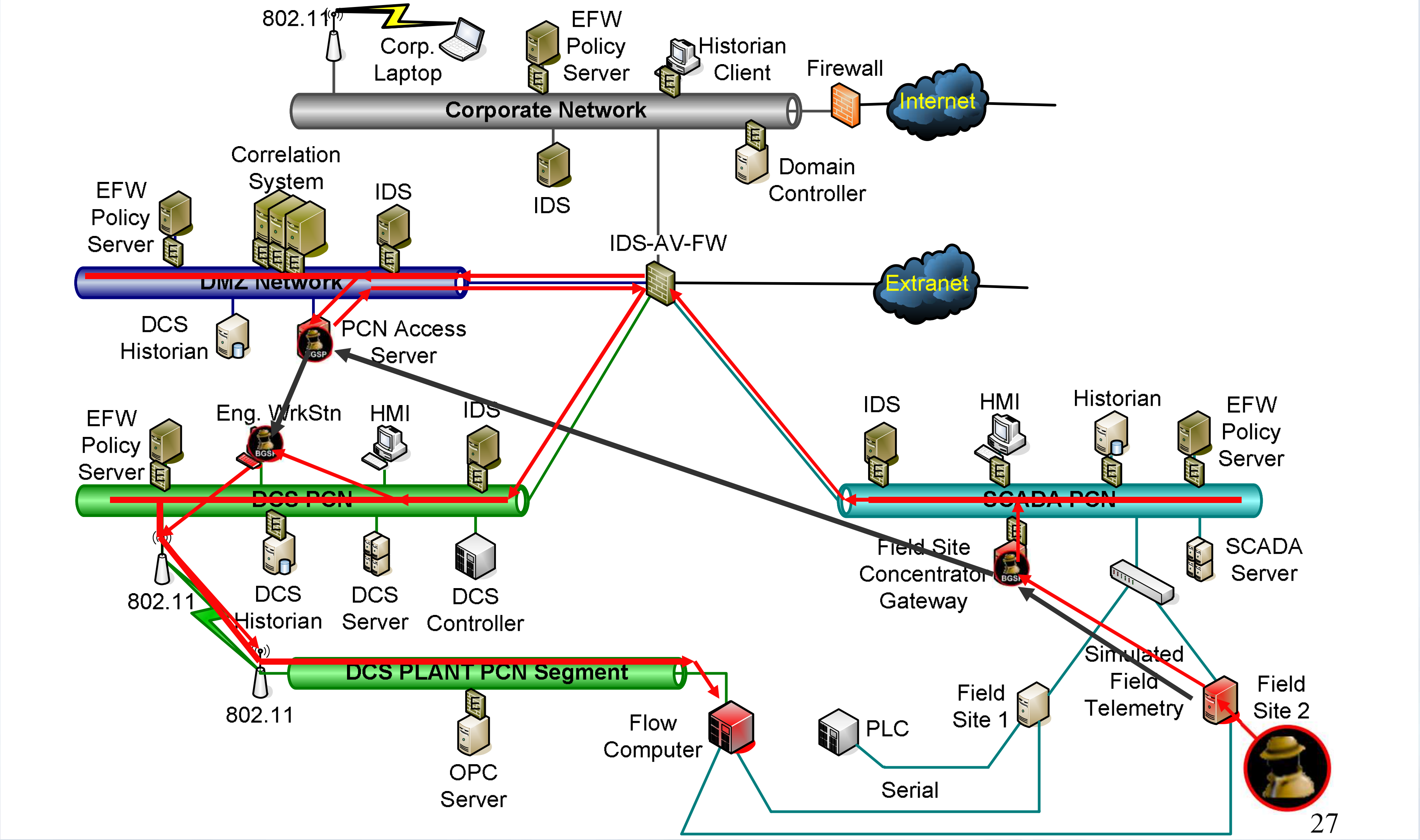
- External Attack Scenario
  - Trust between business and internet
  - Trust between DMZ and business
  - Trust between control network and DMZ
- Remote Site Attack Scenario
  - Trust between field equipment and control servers
  - Trust between control network and DMZ

LOGIIC™ Correlation Project
External Attacker Scenario



LOGIIC™ Correlation Project

Remote Site Attacker



Topics

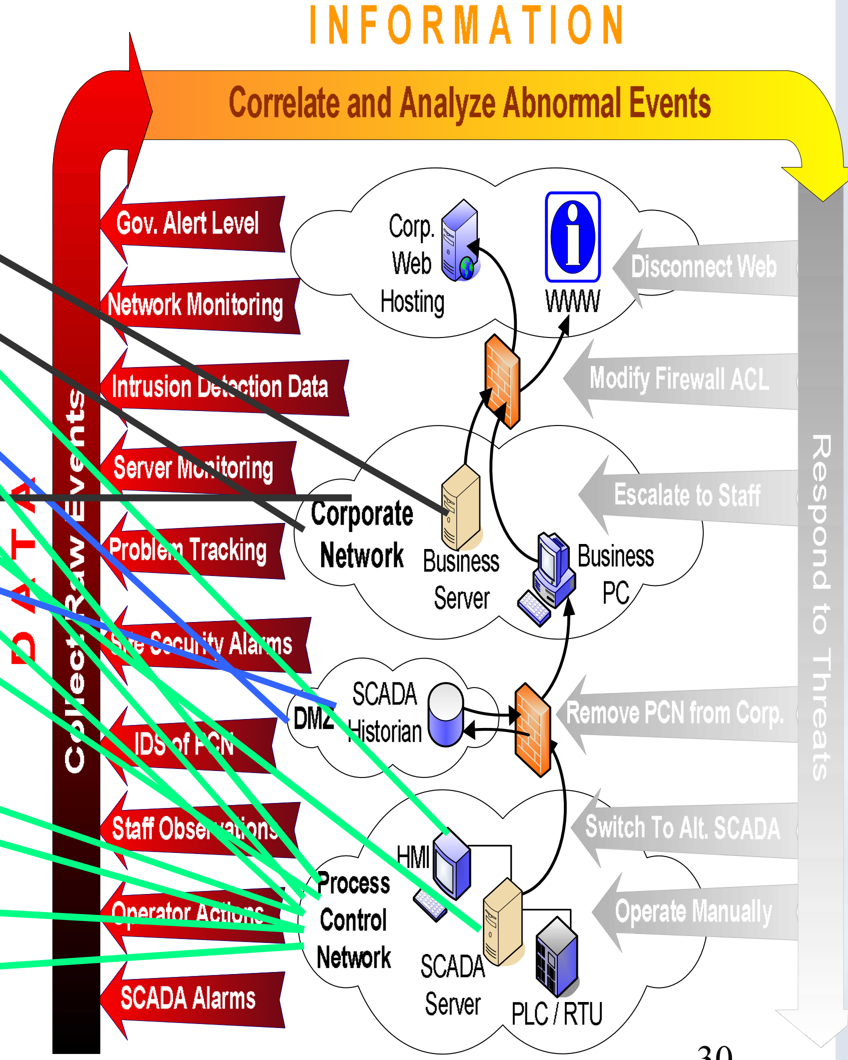
- Tom Aubuchon
  - Government Industry Partnership: LOGIIC
  - LOGIIC Correlation Project (LOGIIC-1)
  - Overview
  - Project Model
  - PCS/PCN Lab Environment
- Bryan Richardson
  - Attack Detection In Control Systems
  - Deploying Defense in Depth
  - Attack Scenarios
- **Tom Aubuchon**
  - **Accomplishments**
  - **Successes**
  - **Example Correlation Results**
  - **Impact**
- Leeanna Demers – LOGIIC 1 Correlation Demo

LOGIIC™ Correlation Project
12 Months of Accomplishments

- Implemented a pipeline SCADA system
- Implemented a refinery DCS
- Integrated two PCNs with business network
- Identified potential PCN risks, modeled attack scenarios
- Identified Security sensors for use in PCN
- Implemented EFWs & Policy Servers on PCN
- Integrated Correlation Engine with PCS environments
  - Developed 6 new connectors for collecting events
  - Identified and developed correlation rules
  - Implemented PCN policy rule enforcements
- Developed, tested, and implemented 4 attack scenarios

LOGIIC Correlation Project Successes

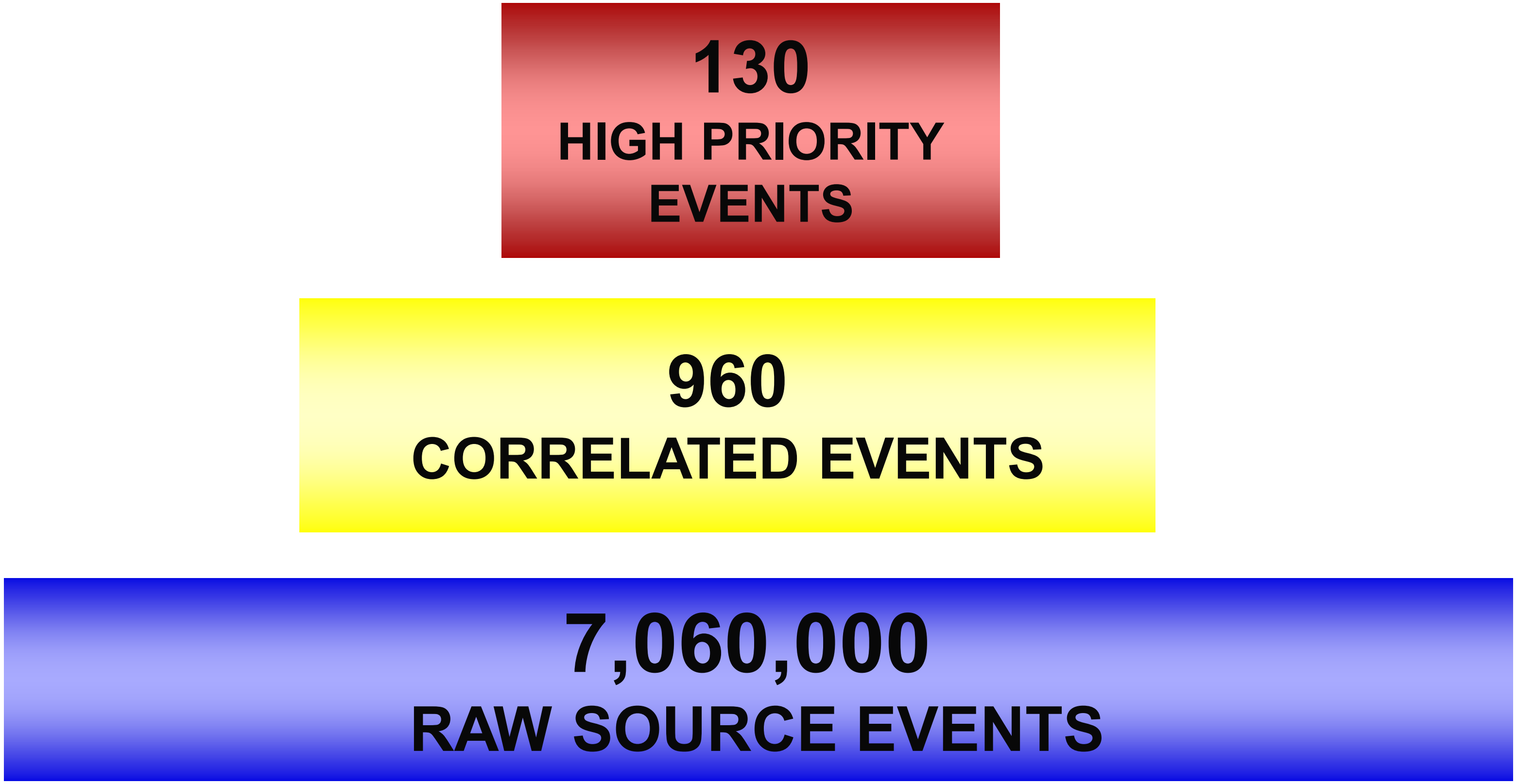
- Events For Correlation
  - Multiple subnets
  - Both IT and PCN devices
  - PCS applications
  - Modbus signatures
  - PCS Security Data Dictionary
  - All sources over time
- Rule Enforcement of common PCN policies
  - Nodes added on PCN
  - Reconnaissance on PCN
  - Modbus exceptions
  - Ethernet configuration changes to PCS devices



LOGIIC Correlation Project

Example Correlation Results

- **External Attack Results**



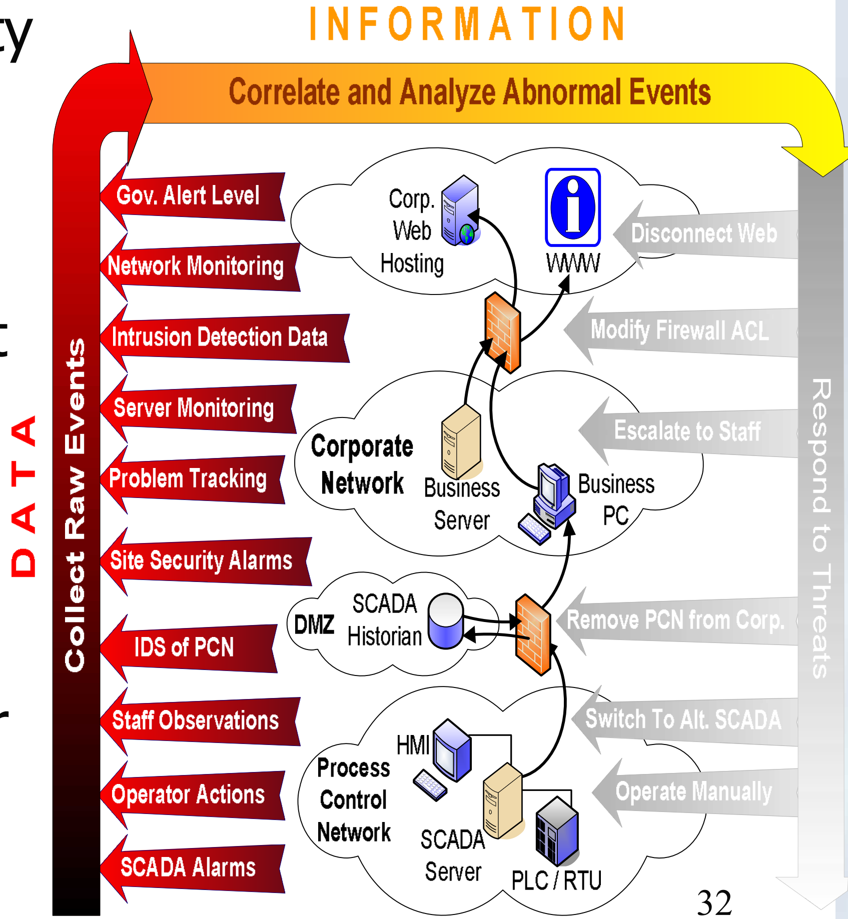
130
HIGH PRIORITY EVENTS

960
CORRELATED EVENTS

7,060,000
RAW SOURCE EVENTS

LOGIIC Correlation Project Results

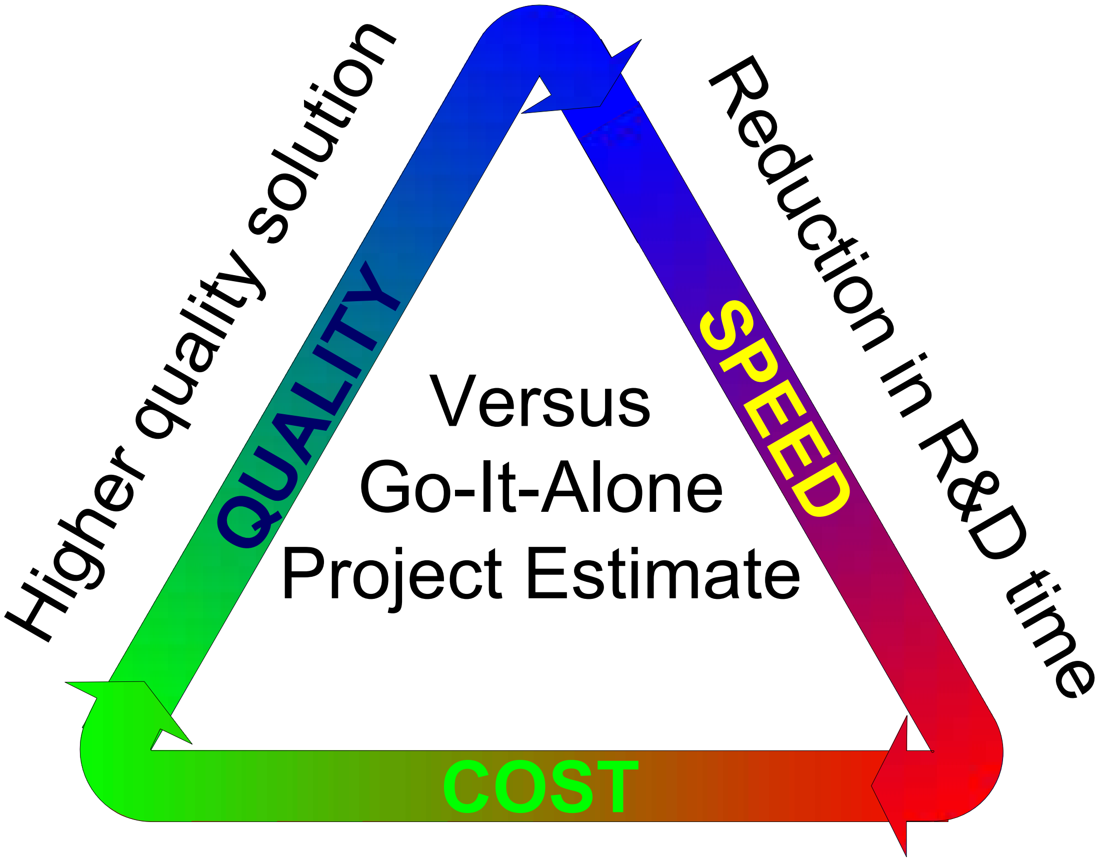
- Successfully developed, implemented and tested 4 attack scenarios
- Attack scenarios model new threats to PCS brought by standardization and interconnectivity
- Implemented PCS Security Data Dictionary
- Identified, correlated, and alerted the compromises to environment at & across all levels.
- Provided enhanced situational awareness
- Completed by deadline
- Built a defense in depth solution for industry deployment



LOGIIC Correlation Project Summary

- PCS detect events and report to the correlation engine
- Attacks can be observed from many different sources
- Attacks were detected with different methods
- Without attack detection, control systems may not be aware of attempted or successful attacks
- Integrated IT security solutions into the PCS world for the first time
- LOGIIC-1 was a completed successfully
- LOGIIC Team members showed strong dedication & talent

Synergy In Energy

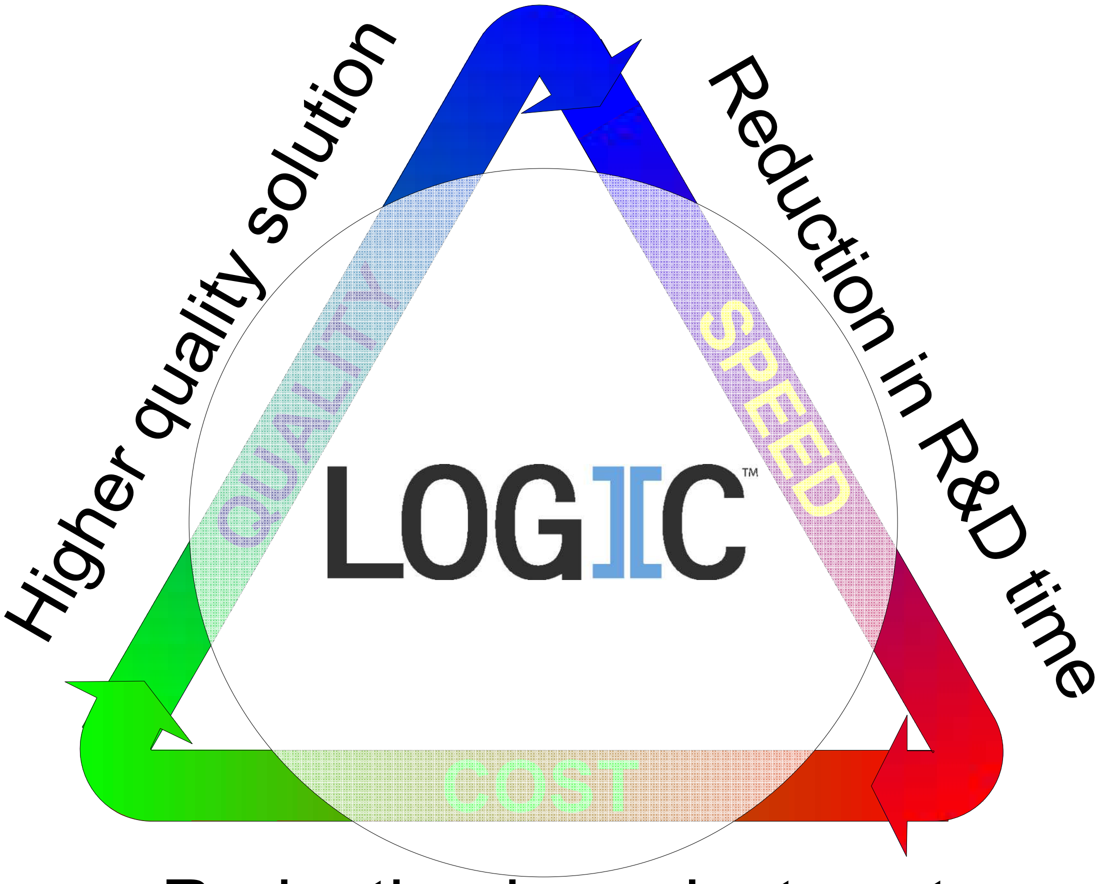


Versus
Go-It-Alone
Project Estimate

Reduction in project cost

Synergy In Energy

The whole is greater than the sum of its parts



Reduction in project cost

Topics

- Tom Aubuchon
  - Government Industry Partnership: LOGIIC
  - LOGIIC Correlation Project (LOGIIC-1)
  - Overview
  - Project Model
  - PCS/PCN Lab Environment
- Bryan Richardson
  - Attack Detection In Control Systems
  - Deploying Defense in Depth
  - Attack Scenarios
- Tom Aubuchon
  - Accomplishments
  - Successes
  - Example Correlation Results
  - Impact
- **Leeanna Demers – LOGIIC 1 Correlation Demo**

References

- *Linking Oil & Gas Industry to Improve Cyber Security* (LOGIIC) partnership with the Homeland Security Advanced Research Projects Agency, Department of Homeland Security (DHS): ”Project Framing Document for DHS LOGI2C Project”, paper developed by the project team, Jul. 2005.
- Lindqvist, U., On the Fundamentals of Analysis and Detection of Computer Misuse, Ph.D. Thesis, 1999.
- Paul, D.: “Partnership for Cyber Security” presented at DHS LOGIIC Cyber Security Project Presentation, Houston, Sept.11, 2006
- Jackson, R.: “LOGIIC Partnership: Continuous Opportunity for Growth” presented at DHS LOGIIC Cyber Security Project Presentation, Houston, Sept.11, 2006
- Susanto, I.:”Risk and Important of PCN Security” presented at DHS LOGIIC Cyber Security Project Presentation, Houston, Sept.11, 2006
- Aubuchon,T.:”LOGIIC Correlation Project” presented at DHS LOGIIC Cyber Security Project Presentation, Houston, Sept.11, 2006
- Parks,R.C.: ”Threats, Vulnerabilities, Attacks” presented at DHS LOGIIC Cyber Security Project Presentation, Houston, Sept.11, 2006
- Lindqvist, U.: “Technologies for Defense in Depth” presented at DHS LOGIIC Cyber Security Project Presentation, Houston, Sept.11, 2006
- Herzer, J.: “Correlation Technology and Result” presented at DHS LOGIIC Cyber Security Project Presentation, Houston, Sept.11, 2006