

Security Event Monitoring (SEM) Working Group

**Dale Peterson, SEM WG Chair
Digital Bond, Inc.**

Control Systems Are Being Monitored

- ◆ **Detecting Intrusions and Security Events**
- ◆ **Security Event Monitoring (SEM) Products**
- ◆ **Managed Security Services Providers (MSSP's)**

SEM Working Group Projects

- ◆ **Use data from monitored SCADA/DCS to quantify threat**
 - Risk = Threat x Vulnerability x Impact
- ◆ **Add SCADA/DCS intelligence to monitored solutions**
- ◆ **Working Group Meeting: Tomorrow at 2:00 – 4:30**
 - Salon B, Grande Ballroom

Adding SCADA Intelligence To SEM

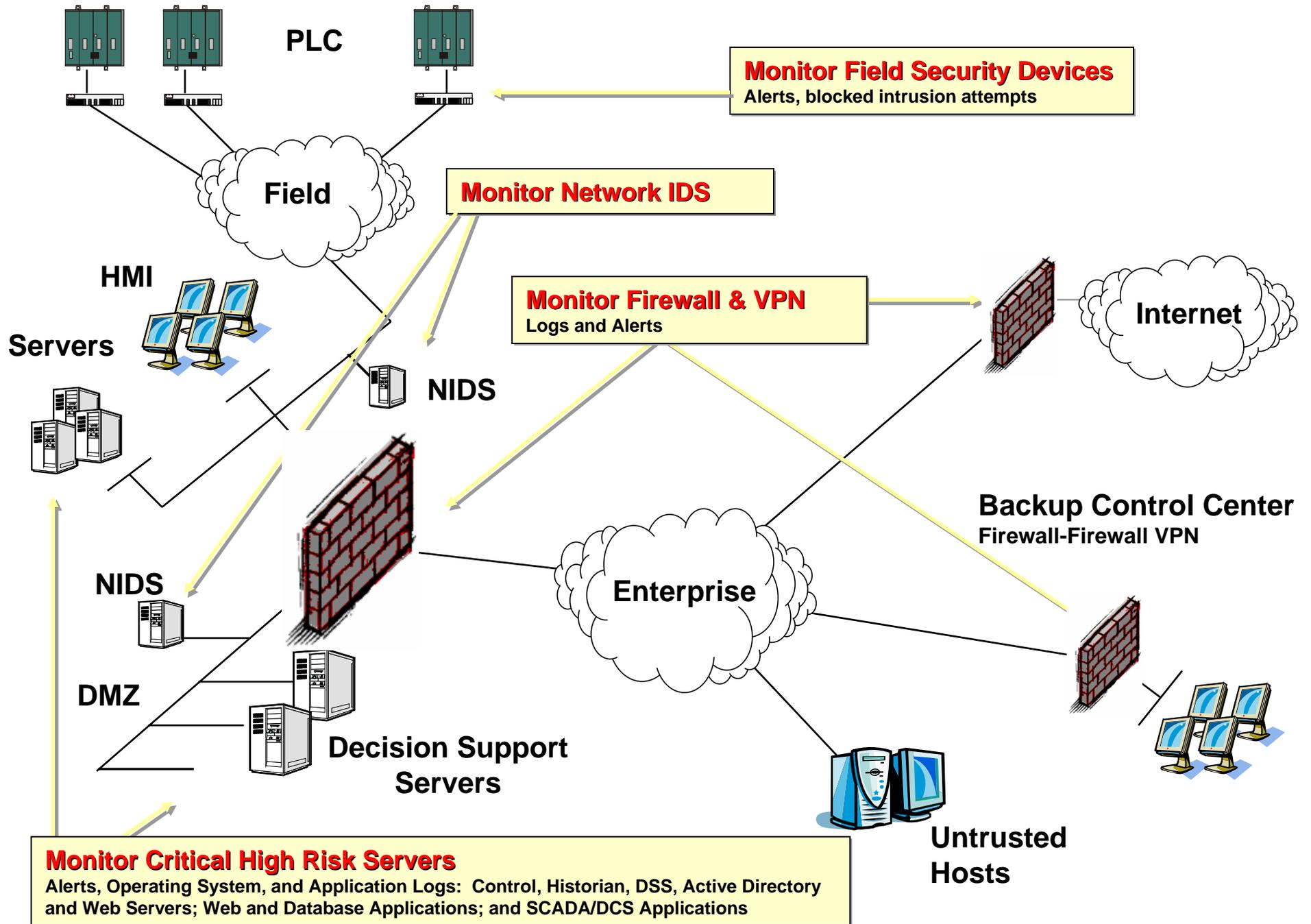
- ◆ **SEM not looking at SCADA/DCS application logs**
 - Many security events in these logs
 - Modify display, grant admin, server failover, ...
- ◆ **Proposed solution: Data Dictionary**
 - Identify and normalize security events
 - Create database tables with applicable patterns
- ◆ **Related Example: Project LOGI2C**

Quantifying The Threat

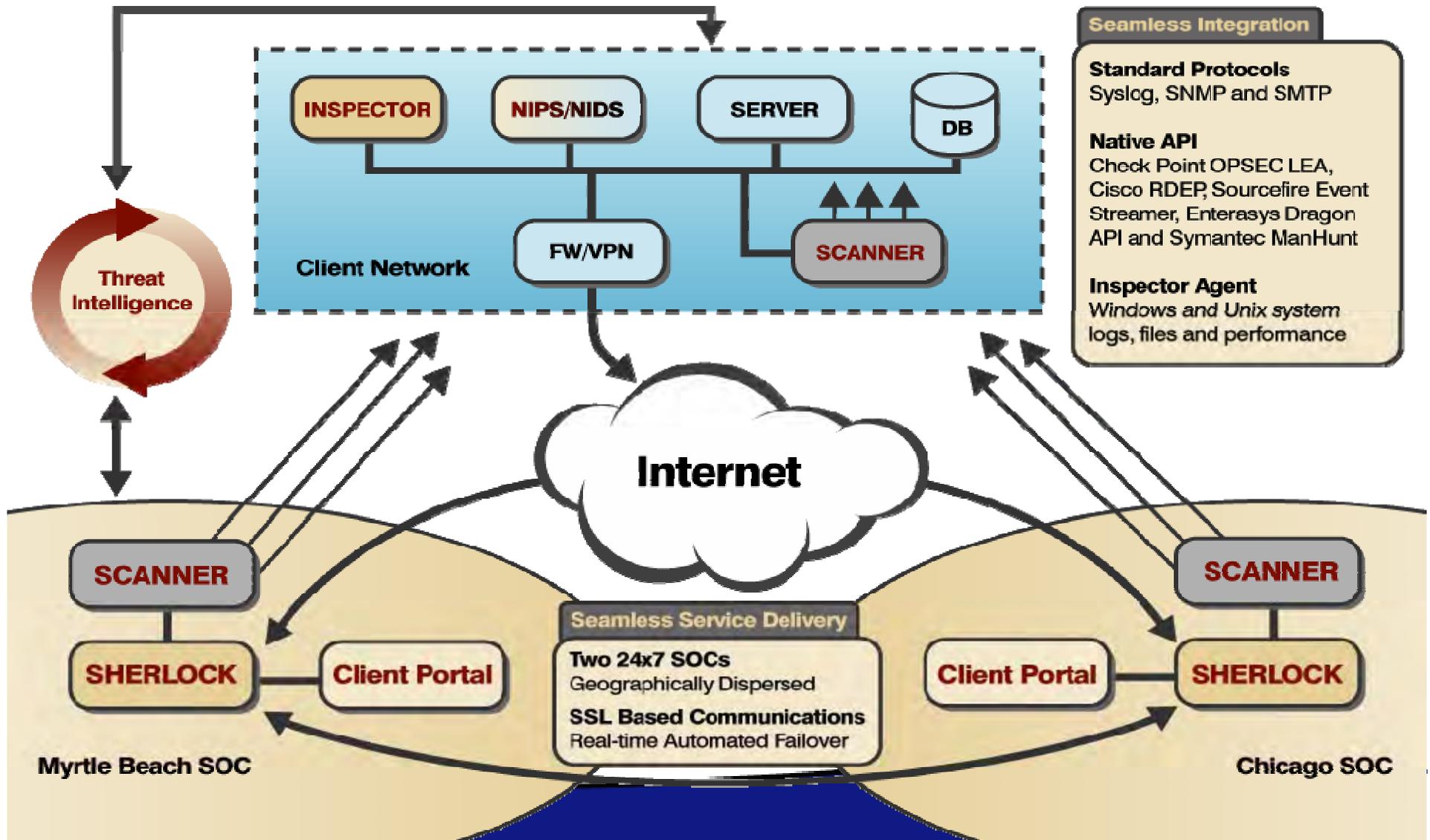
**Craig Baltes
LURHQ**

SCADA/DCS Network Monitoring

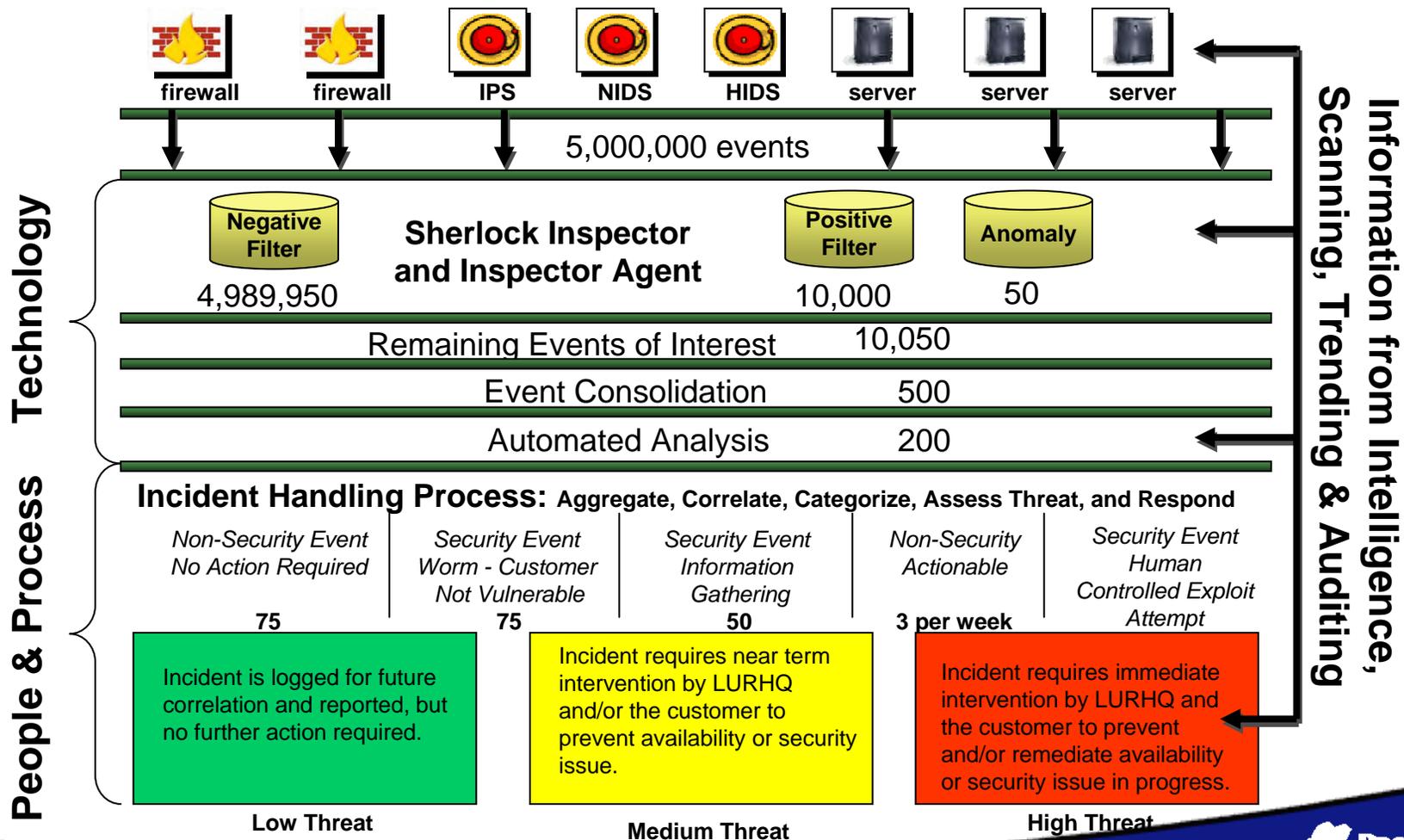
- ◆ What is being monitored?
- ◆ How does the Working Group insure only SCADA/DCS events are reported?
- ◆ What types of events are detected?



Sherlock Platform Architecture



Security Event Management



Threat Statistics

- ◆ **Number of control systems monitored**

- ◆ **Number of actionable events**

- An actionable event requires a MSSP call or email
- An actionable event causes an asset owner to investigate or initiate a response

- ◆ **Categorize the actionable events**

- Denial of Service
- Exploit
- Malware
- SCADA Application or Exploit
- Scan
- Suspicious User Activity
- Other

Threat Statistics Comments

- ◆ **Expectation is a low number of actionable events**
 - Activity on these networks is limited
 - Organizations monitoring are leading edge and more secure
- ◆ **Data is only provided in aggregate**
 - All asset owner and MSSP data is combined
- ◆ **MSSP's can be a big help**
 - Provide data on multiple control systems
 - Another level of anonymity
 - WG Request: ask your MSSP to participate

First set of data

- ◆ **April-May**
- ◆ **Monitoring 12 SCADA Networks**
- ◆ **8 Actionable Events**
 - 5 from Network Scans
 - 3 from Suspicious User Activity

Contact Information

Dale Peterson
Control System SEM Chair
Digital Bond, Inc.

954-384-7049
peterson@digitalbond.com

Craig Baltes
Senior Security Consultant
LURHQ

714-494-7455
cbaltes@lurhq.com