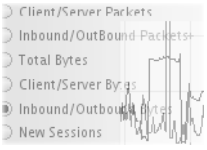
Network Situational Awareness and Correlation Products

Vincent Berk, Ph.D.
George Cybenko, Ph.D.
Process Query Systems LLC
Etna NH 03750
vberk@proquesys.com

ProQueSys LLC founded in 2005

1. ProQueSys NetSAW™

Semantic traffic analysis

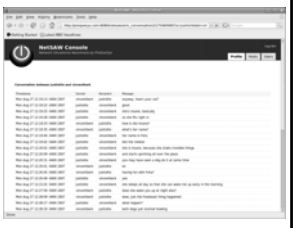


- Passive
- Real-time and forensic
- Packet inspection protocol specific
  - HTTP, IM, SNMP, proprietary SCADA protocols

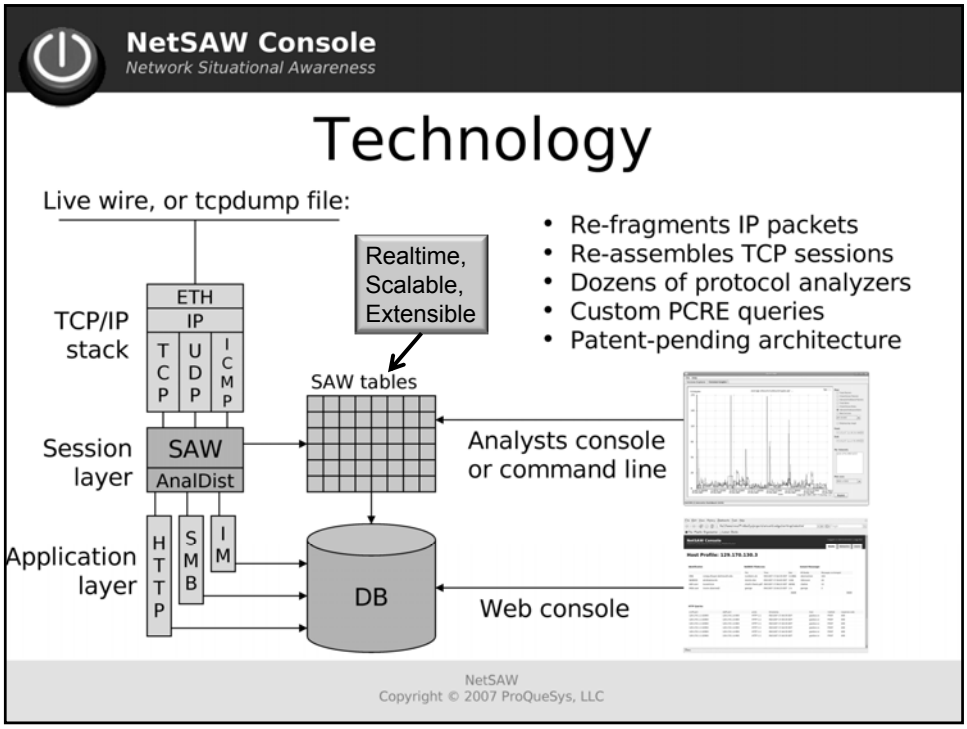
NetSAW™

Inspect the traffic

Inspect a host



Inspect a protocol

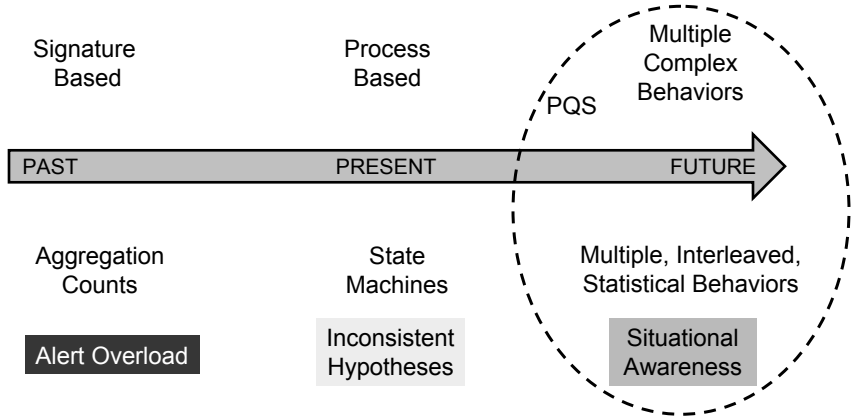


NetSAW™ Status

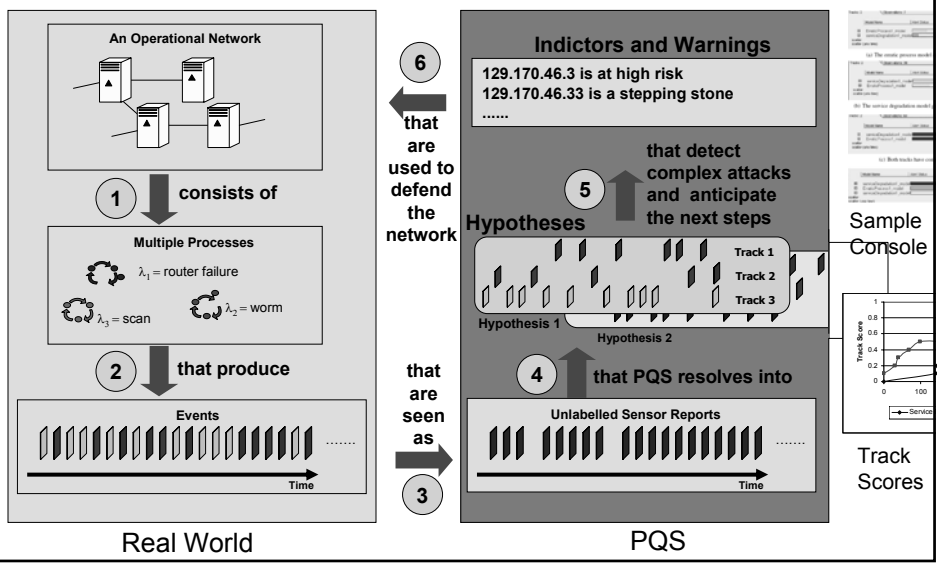
- In use by leading Defense contractor for:
  - enterprise network situational awareness
  - advanced diagnosis and response
- Commercial integration and distribution pending
- Seeking partners for SCADA monitoring and analysis – esp. vendors and asset owners

2. Behavior-based Correlation

- Process Query Systems (PQS)
  - see IEEE Computer, January 2007 article



PQS: Multiple Behavior Correlation



PQS Status

- Raytheon SCADA Cyber Attack Alert Tool (CAAT) and Critical Infrastructure Protection Protocol (CIPP)
  - TSWG/DHS
  - Industry Advisory Group (IAG) formed
  - Prototype in development
- DoD SBIR
  - AFRL Sensors Directorate
  - Autonomic distributed sensor systems
- Seeking development partners and users

For More Information

- www.proquesys.com
- www.pqsnet.net

- IEEE Computer January 2007 article

- vberk@proquesys.com
- gvc@proquesys.com