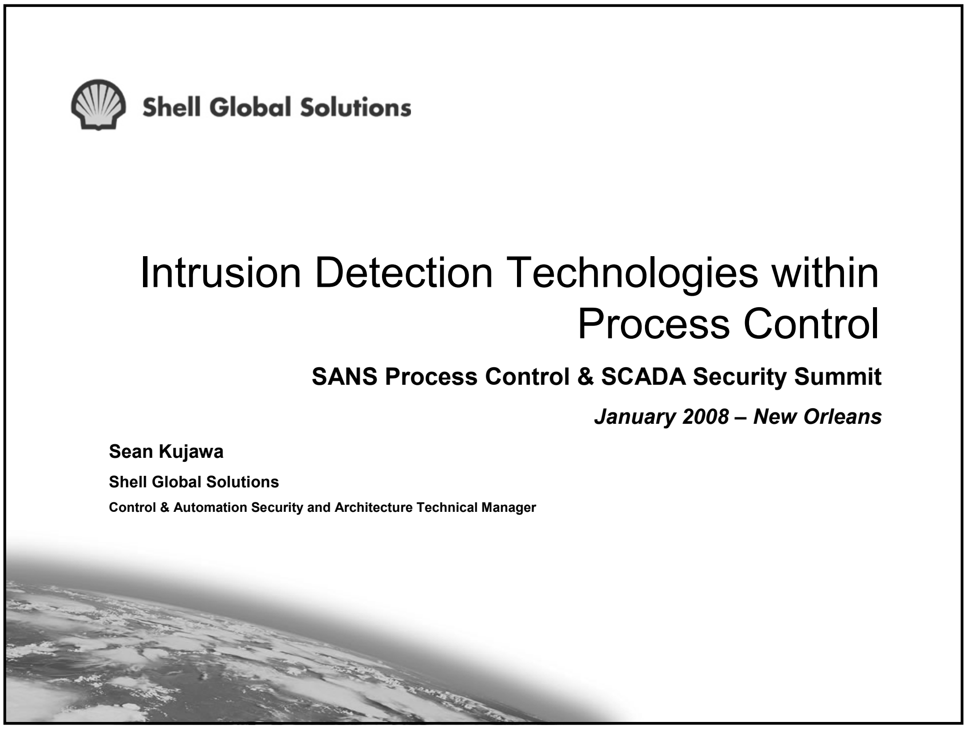


Shell Global Solutions

Intrusion Detection Technologies within Process Control

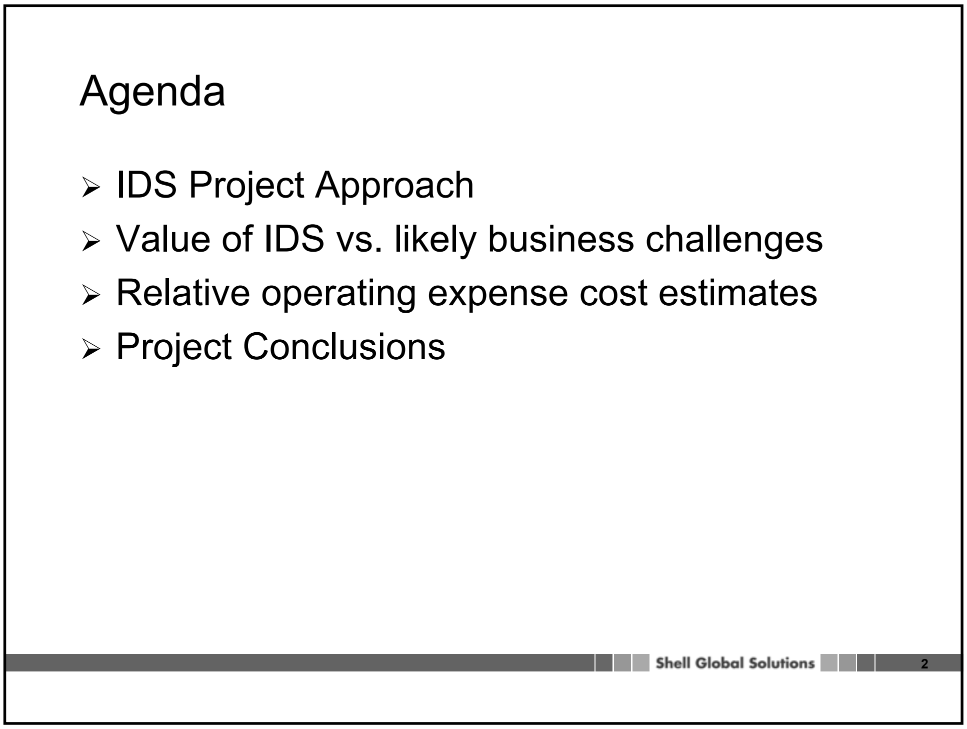
SANS Process Control & SCADA Security Summit

January 2008 – New Orleans

Sean Kujawa

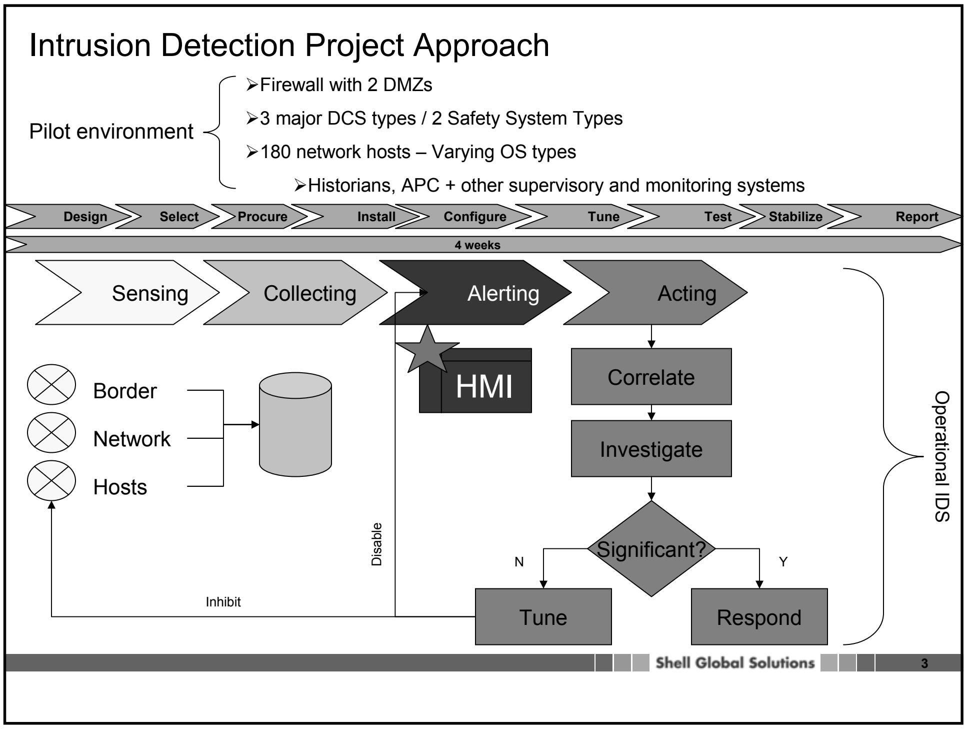
Shell Global Solutions

Control & Automation Security and Architecture Technical Manager



Agenda

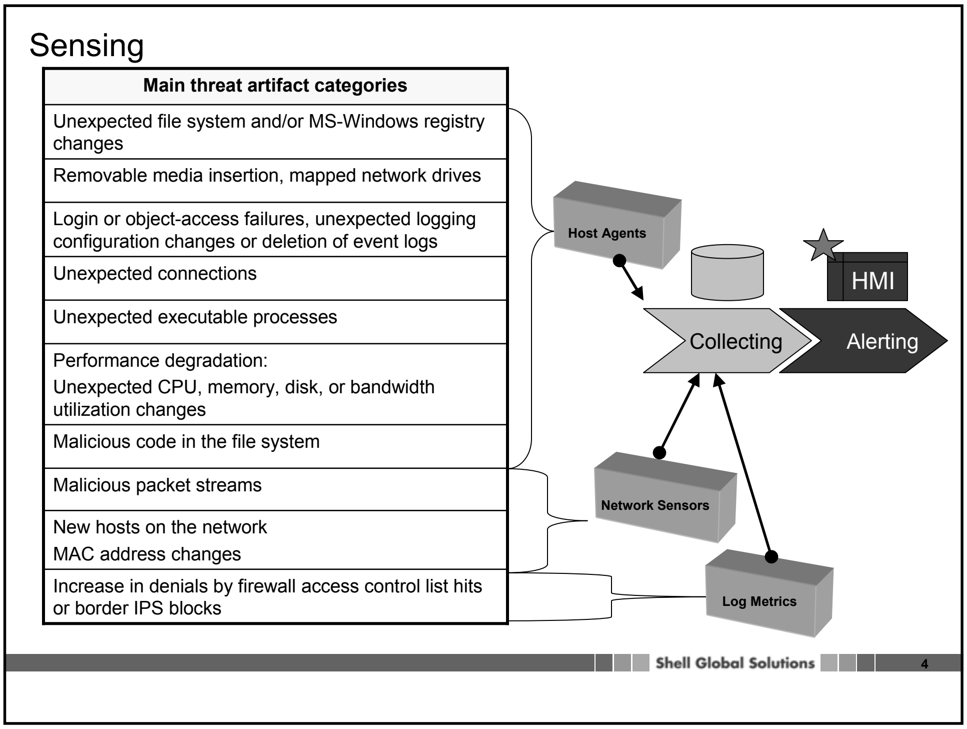
- IDS Project Approach
- Value of IDS vs. likely business challenges
- Relative operating expense cost estimates
- Project Conclusions



Intrusion Detection Project Approach

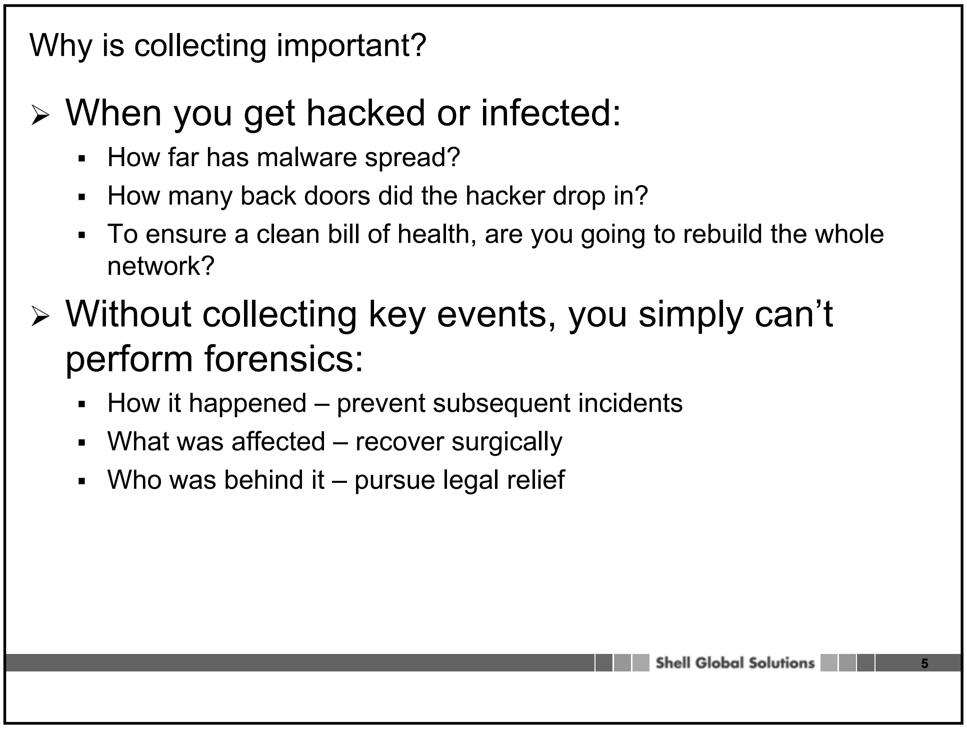
Pilot environment

- ➢Firewall with 2 DMZs
- ➢3 major DCS types / 2 Safety System Types
- ➢180 network hosts – Varying OS types
  - ➢Historians, APC + other supervisory and monitoring systems



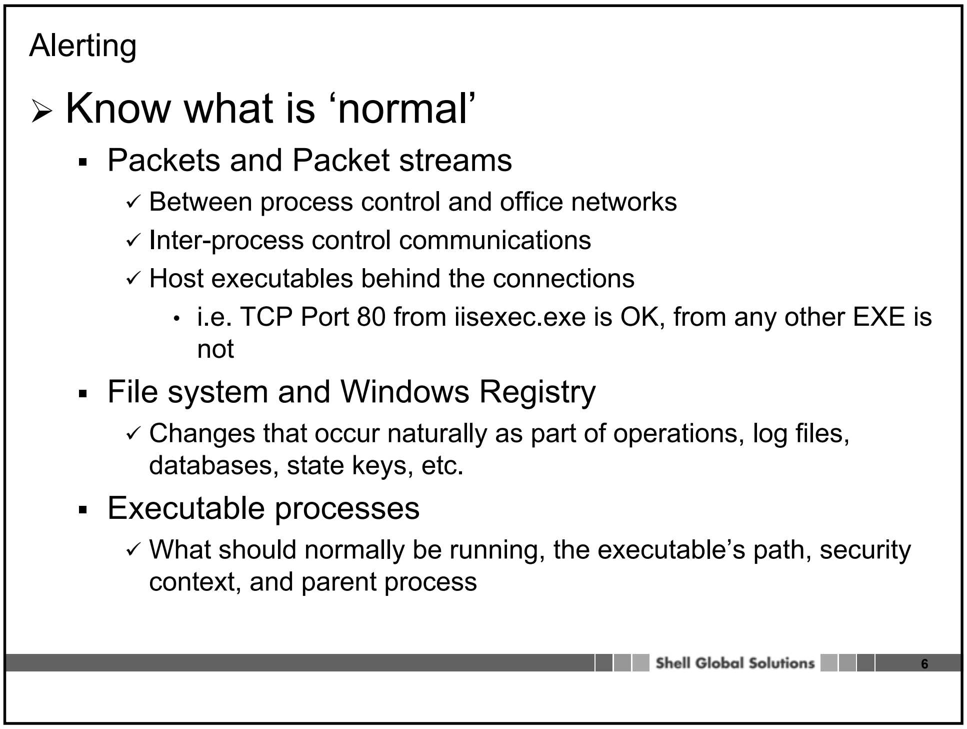
Sensing

Main threat artifact categories
Unexpected file system and/or MS-Windows registry changes
Removable media insertion, mapped network drives
Login or object-access failures, unexpected logging configuration changes or deletion of event logs
Unexpected connections
Unexpected executable processes
Performance degradation: Unexpected CPU, memory, disk, or bandwidth utilization changes
Malicious code in the file system
Malicious packet streams
New hosts on the network MAC address changes
Increase in denials by firewall access control list hits or border IPS blocks



Why is collecting important?

- When you get hacked or infected:
  - How far has malware spread?
  - How many back doors did the hacker drop in?
  - To ensure a clean bill of health, are you going to rebuild the whole network?
- Without collecting key events, you simply can’t perform forensics:
  - How it happened – prevent subsequent incidents
  - What was affected – recover surgically
  - Who was behind it – pursue legal relief



Alerting

- Know what is ‘normal’
  - Packets and Packet streams
    - ✓ Between process control and office networks
    - ✓ Inter-process control communications
    - ✓ Host executables behind the connections
      - i.e. TCP Port 80 from iisexec.exe is OK, from any other EXE is not
  - File system and Windows Registry
    - ✓ Changes that occur naturally as part of operations, log files, databases, state keys, etc.
  - Executable processes
    - ✓ What should normally be running, the executable’s path, security context, and parent process

Acting

- Requires a high level of asset intimacy
  - Regardless of how ‘smart’ the correlation engine/HMI is, the IDS operator must have a functional and robust knowledge of the assets
- IDS operator must have authority and capability to act
  - Decrease time-to-respond by eliminating ‘hand-offs’
- A well-tuned IDS system:
  - Can lead to a ‘comfort-zone’, when something does occur – you’re skeptical
- A poorly-tuned IDS system:
  - Enough ‘cry-wolfs’ over time desensitize the organization

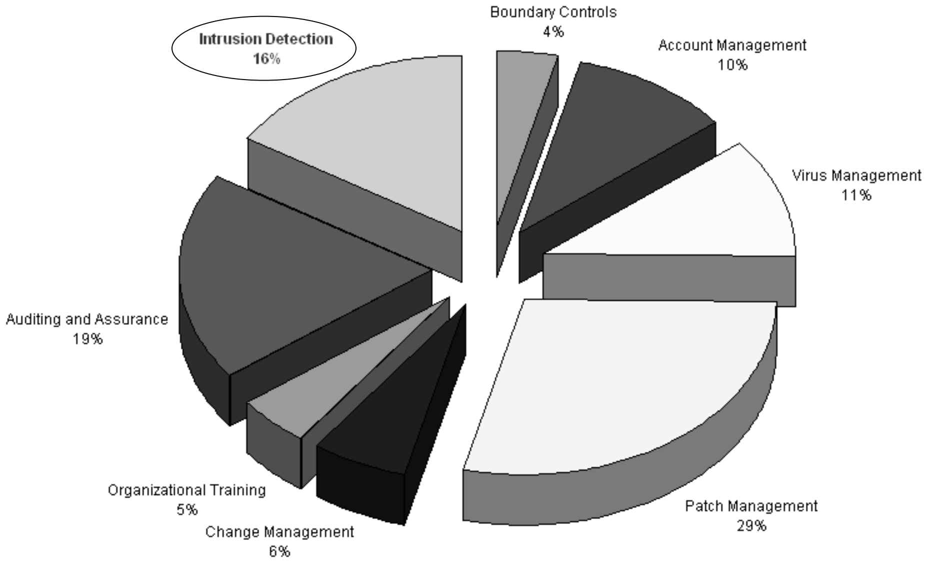
IDS Potential Value-adds / Likely Challenges

Potential value add
Reduction in event consequences - incident discovered and handled during the incipient stage.
Enables a more cost-effective implementation of existing security requirements and emerging accepted practices.
Increased visibility of process control behavior enables an improvement in system’s reliability.

Likely challenges
Difficult to justify investment against other risk mitigation opportunities – why purchase a home alarm system when you have yet to install locks on your doors?
Qualification by SCADA/DCS vendors – adds cost to the base-layer.
Organizational skills required don’t exist – How many staff have a mastery of control systems, IT, and security?

IDS estimated relative operating expense costs

*Normalized for a ‘typical’ PC environment – 150 hosts, locally managed



Conclusions

- IDS Technology is mature and capable
  - Though the supporting organization is likely not ready
- There are no technical reasons to not deploy
  - No unmanageable operational interferences
- There are many solutions to choose from today
  - And more will be offered as the market expands
- The Cost-to-Value ratio of IDS is currently a challenge
  - Managing viruses is more proactive / proven technique to mitigate risk
  - IDS is slightly more expensive than virus management / more reactive and theoretical in it’s ability to add equal value for the money