Agenda

+ Connectivity
+ Cybersecurity
Know the Customer

**PROBLEM**

**SOLUTION**
Customer Value

**Peace of mind**
- Ready to Start
- Job security / Risk Management

**Simplicity**
- Trusted partners
- Value added support / tools

**System availability / reliability**
- Max. uptime / min. downtime
- System efficiency

**Reputation**
- Data security
- Brand recognition
- Safety / Compliance

**Profitability**
- Cost control

**Productivity**
- Maximum uptime
- Minimum downtime
- Asset utilization
- Value added support / tools

**Return on Investment**
- Cost Control
- Fuel management
- Reliability / durability

**Risk Management**
- Trusted partners
- Job security
- Safety / Compliance
- Theft prevention
Data Overload

Transform Data into Value
Connectivity Value

Identify Issues Before Failure
- Automated analysis
  - Data science
  - Human analysis
  - Deep domain experts

Operational Performance
- Asset Readiness/Status
- Operating Cost
- Efficiency
- Regulatory Requirements
  - Industry Specific
  - Emissions/Environmental Impact

Preventive Maintenance
- Understand the current condition of the equipment
- Schedule and Prepare
  - Optimize the work the plan
  - Ensure resource and material availability
  - Optimal time for the customer
- Spot and fix small problems before they become major problems
- Extend component Life

Respond Appropriately
- Quickly determine the problem
- Dispatch resources
Technology and Services create Value

TECHNOLOGY
- Data Collection Methods
- Data Transmission Options
- Data Storage

SERVICES
- Data Visibility/Usability
- Product Expertise
- Data Aggregation
- Security
- Analysis
- Recommendations
- Customized Information
- Support/Service
- Asset Management
- Risk Sharing
- Stability

VALUE ADDER
Real Time Information

- Visualize anywhere and anytime
  - Web Application
  - Mobile Application
- Operating status
- Availability
- Performance indicators
- Location
- Example: Customer monitors the fuel level at multiple locations to determine refill priority
Notifications

• Provided via Email or Text
• Alarms on the asset
• Location change
• Specific parameters
• Asset Availability
• Asset Operating Status
• Customizable by each user
• Example: Customer able to relocate their staff from generator room to other critical location
Reporting

- Asset Level
- Application Overview
- Industry Specific
- Insurance
- Regulatory
- Customizable

Example: Customer saved $20K by replacing emissions inspection with operating history report
Industrial Control Systems (ICS) Under Attack

Notable Breaches: Power Industry

- Davis-Besse nuclear power plant (Ohio – USA) - 2003
- Brown Ferry nuclear power plant (Alabama-USA) – 2006
- Stuxnet: Destruction of Iranian Nuclear Centrifuges (2011)
- Aurora Generator Destruction (2010)
- Ukraine power outage – 2015

➢ Attacks are increasing in number as well as sophistication
➢ Companies in the Energy and Transportation sector are now clearly targeted
## Cybersecurity Regulations/Standards

<table>
<thead>
<tr>
<th>Industry</th>
<th>Regulation/Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Industrial Control</td>
<td>ISA/IEC 62443 (formerly ISA-99)</td>
</tr>
<tr>
<td>Systems</td>
<td>IEC 62351 Part 1-8</td>
</tr>
<tr>
<td></td>
<td>ISO 27000/27001</td>
</tr>
<tr>
<td>Data Centers</td>
<td>NIST Frameworks (800-53, 800-82) and ISO 27000 series</td>
</tr>
<tr>
<td>Electric Power and Utilities</td>
<td>NERC-CIP (002 to 009)</td>
</tr>
<tr>
<td>Federal</td>
<td>Risk Management Framework (RMF), DIACAP, NIST Framework</td>
</tr>
<tr>
<td>Health Care</td>
<td>Health Insurance Portability and Accountability (HIPAA) - 1996</td>
</tr>
<tr>
<td></td>
<td>Health Information Technology Standard (HITECH) - 2009</td>
</tr>
<tr>
<td>Chemical</td>
<td>U.S. DHS CFATS</td>
</tr>
<tr>
<td>Marine</td>
<td>International Association of Classification Societies (IACS)</td>
</tr>
</tbody>
</table>

- Holistic Security Program that includes – Organization, Policies, and Technology
- Defense-in-Depth: Layers of Security Controls Across the System
- Network Segmentation

**Increasing number of security and data privacy regulations and standards**
Connected Asset Security Program

A collaborative business effort managing cybersecurity risks to Caterpillar’s ecosystem of connected solutions.

We provide cybersecurity governance and leadership to help Caterpillar’s businesses embed secure methods into the creation and support of connected products, digital services and connected production devices.
Managing the Cybersecurity Risk of Connected Assets

Our Connected Asset Journey… the CAPABILITIES

GOVERN
- Manage cybersecurity risks
- Inventory connected solutions
- Sustain business outcomes
- Provide cybersecurity guidance

PROTECT
- Protect connected asset (CA) data
- Embed secure methods in creating CAs
- Embed secure methods in supporting CAs

DETECT
- Collaborate with customers, partners and researchers
- Log and monitor security events

RESPOND
- Respond to cybersecurity incidents

EDUCATE
- Expand security awareness

Information Security Operating Framework

Measure, control and continually improve security

Equip and motivate our people to be our first and best line of defense

Contain, eradicate and quickly recover from information security incidents

Make it difficult to compromise confidential information

Identify anomalous behavior in our environment

Detect
Respone
Educate
Govern
Risk Tolerance
Threat Intelligence
Business Priorities
Integrating Security into Development Lifecycles

Governance
- Risk Profiling
- Data Governance Assessment
- Static Application Security Testing
- Dynamic Application Security Testing
- Attack and Penetration Testing

Requirements
- Minimum Security Requirements
- Threat Modeling

Design

Develop
- Vulnerability and Configuration Scanning
- End-user Security Guidance

Verification

Production

Security Threat and Architecture Review

Education and Lessons Learned
- Activity scaled based on risk
- Activity required for all products
**Defense-in-Depth - People, Policies and Technical Controls**

- **Physical** –
  - Physical Access Controls for Critical Areas

- **Network** –
  - Firewalls and Traffic Filtering
  - Intrusion detection and prevention

- **Computer Hardening** –
  - Patching and Anti-Virus
  - Remove unused applications/protocols/services
  - Close unnecessary logical and physical ports

- **Application** –
  - Authentication, Authorization, and Accounting

- **Device Hardening** –
  - Encryption

---

Note: “one-size-fits-all”
End to End Security Architecture

Product Link Device Security:
- Secure device software update
- Device hardening including disabling of unused ports and services

Remote Connection Security:
- Encrypted and authenticated connection
- Device initiated outbound connection only
- Device does not respond to general internet traffic

Web Application Security:
- HTTPS/SSL secured web application interface
- Login authentication and role-based access control
- Web application security scans

Customer Firewall: Customers may have to open their firewall to let the connection get across

Caterpillar IT Infrastructure Security:
- Intrusion detection and prevention solutions
- Network segmentation with multi-layer security protections
- Physical and Logical security for the data centers
- Incidence response and disaster recovery plans

Switchgear
EMCP
Engine
Engine and Generator Data
Product Link
Cellular, Satellite, or Ethernet
Customer Site Network
Servers and Databases
Web Application
Internet
Web Application
Users
System Considerations

+ **Products and Services**
  - Does it meet all the connection needs?
  - Transform Data into Value
  - Flexible
  - Expandable

+ **Support**
  - 24/7
  - Regional or World-Wide
  - Expertise level

+ **Commercial Plan/Cost**
  - Initial
  - Ongoing

+ **Company**
  - Expertise
  - Reliability
  - Security
  - History
  - Sustainability
THANK YOU

Eric Ditman
Sr. Digital Program Manager
Ditman_Eric_J@Cat.com
309-698-5275