Internet of Things

The Digital Oilfield: Security in SCADA and Process Control

Mahyar Khosravi
makhosra@cisco.com
“Critical infrastructures worldwide not ready to battle cyber attacks, claims new study”.
Ponemon-Unisys study July 2014

Oil companies remain complacent about computer dangers
July 10, 2014 at 2:38 pm by Jennifer A. Dlouhy

Two-thirds (67 percent) of IT security executives at utility, oil and gas, energy and manufacturing companies report that they have experienced at least one security breach in the past 12 months. Those incidents led to the loss of confidential information or the disruption of operations.
July 16, 2014 | By David Weldon

Energy companies now suffering more breaches than banks.

3 Bills to Protect Critical Infrastructure from Cyber Attack Passed by House

By: Homeland Security Today Staff
eBay steal personal records of 233 million users.

Montana Health Department breach may have affected more than 1 million people. The hack actually happened in July last year, but it wasn’t discovered until May this year,

P.F. Chang’s thousands of newly stolen credit and debit cards went up for sale online on June 9th.

Occidental
Actual results may differ from anticipated results..... labor unrest, weather, natural disasters, cyber attacks or insurgent activity;

The World's Critical Infrastructure Is at Risk

By Samuel Greengard

Energy Sector Leaders Still Not Taking Cyber Threats Seriously, Survey Finds
NATIONAL DEFENCE MAGAZINE

Although IT security executives are aware of the threats to industrial control systems (ICS) and supervisory control and data acquisition systems (SCADA), the IT professionals in the organizations said their companies are not fully committed to preventing attacks.
Security teams are “flying blind” without information about environments

Cost of security to operations to meet security & compliance is high

Security controls and solutions built up over time; difficult and costly to implement and maintain

Vendors require proprietary third party access to systems
Introducing Cisco Secure Ops Solution

Secure Ops

- Next generation Cyber Security, Risk and Compliance Management Solution for critical infrastructure
- Designed to support Implementation & Maintenance of Security Controls
- Forms a foundational technology platform; provides a “building block” approach to implementing desired security controls
- Allows central leadership to understand risks and make informed investment decisions

Supported and embraced by ICS Engineering Partners
Cisco Secure Ops Solution – 30,000 Foot View

- Flexible Commercial Models
  - Ability to transact globally
- Centralized or de-centralized architecture
- Sites are deployed on client premise
- World class, cross-trained engineers (ICS Engineering + Security + IT)

Commercial Model
- Either –
  - Monthly billing per site, per month basis, OR
  - CAPEX options available
- All start-up costs included in unit pricing
- Managed via SLO’s or SLA’s
- Flexible RACI model
Risk Control Framework for Industrial Automation Systems

Addresses the most significant attack vectors within Industrial Automation Systems by establishing required controls associated with best of breed security practices.

**Organize**
- Security Policy
- Process Inventory
- Asset Inventory & Management
- Assessments
- Change Management
- Education & Awareness
- Dashboards & Reporting

**Harden**
- Network Segmentation
- PCN Access & Control
- Anti-virus
- System Patches
- Encryption
- Virtualization

**Detect**
- Proactive Monitoring
- Security Monitoring
- Anomaly Detection
- Malware Detection
- Intrusion Detection
- Location Awareness

**Defend**
- Security Log Collection and Management
- KPI's and Analytics
- Threat Defense
- Backup and Restore
- Continuous Improvement

**Respond**
- Incident Response
- Disaster Recovery
- Backup and Restore
- Continuous Improvement

---

© 2013-2014 Cisco and/or its affiliates. All rights reserved.
Modular Secure Ops Offering and Operate Model

- **Modular Offering:**
  - Platform Services (required)
  - Plus… Building Blocks (as needed):
    - Secure Access
    - Asset Discovery & Inventory
    - Security Intelligence and Response
    - Secure Distribution
    - Compliance Monitoring & Reporting
  - Add-on Services

- **Flexible Operate Model:**
  - XaaS versus Assured Operate
  - Completely Cisco-managed versus Hybrid Customer-Cisco-Managed support model
## Sample Solution Capabilities

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High-availability infrastructure &amp; connectivity</strong></td>
<td>✓ Full redundancy maximizes operational availability</td>
</tr>
<tr>
<td><strong>Solution Infrastructure Scaling</strong></td>
<td>✓ Allows for significant growth in capabilities and additional services</td>
</tr>
<tr>
<td><strong>Secure PCN Access</strong></td>
<td>✓ Flexible and Secure, out-of-the-box web interface</td>
</tr>
<tr>
<td><strong>Passive Asset Discovery &amp; Query-based Asset Inventory</strong></td>
<td>✓ Automated, up-to-the minute updates for IP and Non-IP assets</td>
</tr>
<tr>
<td><strong>Information Repository</strong></td>
<td>✓ Central management provides central location for information, reporting and evidence collection (Maturity Reporting &amp; Risk Analysis)</td>
</tr>
<tr>
<td><strong>OS Security Patch Management</strong></td>
<td>✓ Automated distribution and tracking of Windows QPL availability and Automation Suppliers</td>
</tr>
<tr>
<td><strong>Anti-virus Management &amp; Updates</strong></td>
<td>✓ Automated signature update, Approved by Automation Suppliers</td>
</tr>
<tr>
<td><strong>Log Collection &amp; Management</strong></td>
<td>✓ Automated, daily collection</td>
</tr>
<tr>
<td><strong>Risk Management</strong></td>
<td>✓ Automatically generated risk profile of assets, based on criticality to operational process and real-time risk indicators from the network</td>
</tr>
<tr>
<td><strong>24x7x365, Globally supported solution</strong></td>
<td>✓ NOCs across the globe, “Follow the Sun” support model</td>
</tr>
<tr>
<td><strong>Proactive Performance &amp; Fault Monitoring</strong></td>
<td>✓ CPU, Memory, Disk Utilization, Fail Over State, Interface, Secure Ops Applications Up/Down</td>
</tr>
<tr>
<td><strong>Global Security Incident Response &amp; Monitoring Services</strong></td>
<td>✓ Product and Computer Security Incident Response</td>
</tr>
<tr>
<td><strong>Security Event Correlation and Incident Notifications</strong></td>
<td>✓ Alarm analysis &amp; classification, remediation &amp; recommendation</td>
</tr>
<tr>
<td><strong>Network Availability and Performance Monitoring, Reporting</strong></td>
<td>✓ Near real-time reporting capabilities</td>
</tr>
</tbody>
</table>

Secure Ops automates compliance and protects against risk while maximizing site productivity.
**Deployment Models (Centralized or De-Centralized)**

**Pattern 1**
**Local SecureSite w/ Center**
- Simple sites
- Greenfield

**Pattern 2**
**Distributed SecureSites (w/Satellites)**
- Geographically dispersed sites with PCN networks separated by L4/L5 networks

**Pattern 3**
**Virtual SecureSites (w/ Satellites)**
- Geographically dispersed sites with PCN "islands" separated by L4/L5 networks
- Fast, resilient networks to SecureSite Data Center within SecureCenter
- The SecureSite is a single, per-logical-site instance

**Pattern 4**
**SecureSite POD (w/ Satellites)**
- Physically separated island or sites that require local management only.
- Fast, rapid provisioning of sites
- The SecureSite POD is a single, per-logical-site instance
SecureSite Configuration (On-Premise)

High performance and secure networking, w/ unified computing, storage and virtualization

• Business Objectives:
  • Centralized monitoring, management and reporting of compliance data
  • Simplify and standardize solution across the business
  • Introduce agility and flexibility
  • Maintain security

• Technology Objectives:
  • Standardized, scalable repeatable solution
  • Maintain security while offering flexibility and improved manageability
  • High availability & Performance for business critical operations
Benefits

- Reduces risk to Industrial Control System Networks
- Reduces cost of delivering PCN Security
- Brings new services that improve productivity and reduce cost of production

~$700K of operational savings per site deployed (independent ROI study)

Security Maturity and Compliance improved significantly
Secure Ops Value Overview


Secure Ops is designed to evolve by the principle of Continuous Improvement. New releases of the Platform are improved based on lessons learned.

**Improved Service**
- Proactive tooling
- Shorter response times
- Reduced cost
- Reduced FTE allocation
- Out of the Box capabilities
- Single point of escalation

**Enhanced Security**
- Easier access to security enabling resources
- Up-to-date inventory of PCN/ICS assets and deployed software

**Better Information**
- Automated compliance information
- Standardized reporting
- Information is business ready
- Centralized reporting capabilities

**Increased Financial Value**
- Time saving for site resources
- License clean-up
- Improved functionality will increase use of remote access by automation vendors
Secure Ops Press Release

Cisco to Provide Secure Ops Solution to Shell

CHICAGO, IL, Oct 15, 2014 (Marketwired via COMTEX) -- IoT World Forum 2014 -- Cisco CSCO, +1.61% -- Today, at the Internet of Things World Forum in Chicago, Shell shared that it has deployed the Cisco Secure Ops Solution to increase security maturity level by improving its cyber security and risk management, while lowering costs of delivery and operations. Cisco's solution is designed to help companies combat new and evolving cyber security threats to the energy industry, specifically in the industrial control system (ICS) domain.
Thank you.