Achieving Cyber Security Across Your Enterprise with ICS Shield and Risk Manager

Daniel Severino, Sam Wilson
October 2nd, 2018
Part of Honeywell Industrial Cyber Security Portfolio

Industrial Security Consulting:
- Industrial security program development
- Assessment services
- Architecture and design
- Implementation and systems integration
- Operational service and support
- Compliance audit & reporting

Integrated Security Technology:
- Whitelisting
- Antivirus
- Next-generation Firewall
- IDS/IPS
- Security Information & Event Management (SIEM)
- Threat Intelligence

Managed Security Services:
- Secure remote access
- Continuous monitoring and alerting
- Secure automated patch & signature updates
- Incident response & recovery/backup
- Security device co-management
- Hosting and management of ICS Managed Security Service Center

Cyber Security Software:
- Honeywell Industrial Cyber Security Risk Manager
- Secure Media Exchange (SMX)
- Advanced Threat Intelligence Exchange (ATIX)
- Industrial assessment software & tools
- ICS Shield platform for cyber security operations

Comprehensive, Proven and Trusted End to End Solutions
High-level Challenges of IT-OT Integration

ICS/SCADA Complexity
- Multiple sites
- Multiple vendors requiring access to assets
- Multiple protocols on ICS network
- Multiple businesses
- Mix of legacy and proprietary equipment

IT/OT Misalignment
- ICS security ownership is not clear
- OT/IT mindsets are very different
- Transition from plant-by-plant to plant-wide security practices

Skilled Resources Shortfall and Budget Limitation
- Cannot place experts at every site
- Manual processes don’t scale and only provide limited security
- Multiple security solutions partially utilized
Honeywell’s Industrial Cyber Security Risk Manager

Measure the Risks That Matter the Most

• First real-time cyber risk reporting platform designed for ICS & PCN industrial companies

• Measures, prioritizes and manages high priority ICS risk, to mitigate threats & improve compliance

• Speeds & simplifies PCN cyber data reporting, to save labor costs & improve ICS security posture
Risk Manager Evolves | Feature Highlights

Customer Prototype

2014

Honeywell Users Group 2014, 2015

Shipping Solution

2015

R140, R150
- Risk data collection & scoring
- Virtualization: Virtual RM
- Dynamic rules
- Expanded PCN visibility: C200/C300 Controller discovery

2016

Enterprise-Ready Feature Enhancements

2017

R160
- Enterprise-wide visibility: Enterprise Risk Manager
- Syslog Forwarding for SIEM support
- Power user analytics and ad-hoc reports (Analysis View)
- Single RM monitoring across multiple domains: AD Multiple Domain Support
- Customers pay less to get started: Subscription-based pricing structure

2018

R170
**Key R170 Features & Enhancements | Summary**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Risk Manager (ERM)</td>
<td>• Multi-site visibility of Risk Manager data, all in a single pane view</td>
</tr>
<tr>
<td>Syslog Forwarding</td>
<td>• Securely output Enterprise Risk Manager Syslog information to SIEM</td>
</tr>
<tr>
<td>Analysis View</td>
<td>• Enhanced reporting and analytic tools as part of Risk Manager dashboards</td>
</tr>
<tr>
<td>Multiple Domain &amp; Workgroup Support</td>
<td>• Single RM monitoring across multiple domains, and monitoring end nodes which are in a workgroup</td>
</tr>
<tr>
<td>New Risk Items and Dynamic Rule capabilities</td>
<td>• Expands monitored risk coverage</td>
</tr>
</tbody>
</table>

Risk Manager R170 helps industrial enterprise security teams easily automate and share consistent plant data -- OT & IT can work together to limit enterprise-wide cyber security risk.
R170 | ERM - Multi-Site Data in a Single Pane View

- Displays selected site’s Risk Manager Dashboard

<table>
<thead>
<tr>
<th>Site</th>
<th>Risk to Site</th>
<th>Endpoint Security</th>
<th>Network Security</th>
<th>Patches</th>
<th>Backup</th>
<th>System Health</th>
<th>Data Replication</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEMOSRV</td>
<td>100</td>
<td>80</td>
<td>90</td>
<td>100</td>
<td>95</td>
<td>Error</td>
<td>Critical</td>
</tr>
<tr>
<td>HTS-DEV-RM</td>
<td>70</td>
<td>10</td>
<td>0</td>
<td>67</td>
<td>70</td>
<td>Critical</td>
<td>Critical</td>
</tr>
<tr>
<td>L2DC-RMSITE</td>
<td>100</td>
<td>50</td>
<td>0</td>
<td>100</td>
<td>60</td>
<td>Critical</td>
<td>No Issues</td>
</tr>
<tr>
<td>PCTRMA-SITE</td>
<td>60</td>
<td>30</td>
<td>0</td>
<td>0</td>
<td>60</td>
<td>Critical</td>
<td>Critical</td>
</tr>
<tr>
<td>RMAUTO-SITE</td>
<td>70</td>
<td>35</td>
<td>0</td>
<td>62</td>
<td>70</td>
<td>Error</td>
<td>No Issues</td>
</tr>
</tbody>
</table>

- Displays selected site’s Risk Source page with chosen Risk Source details
- Displays selected site’s System Health Status page
ICS Shield
Honeywell ICS Shield

Top-down OT security management

- Automates top-down integrated approach for deployment and enforcement of plant-wide security policies
- Based on proven technology acquired through Nextnine acquisition – over 6000 installs
- Delivers unrivaled visibility, reliability and compliance for industrial plant operations
- Enables security of remote field assets from a single operations center

Key Features:
- Secure remote access
- Secure file transfer
- Automated patch and AV updates
- Asset discovery
- Performance/health monitoring
- Compliance reporting
Common OT Cyber Security Challenges

Varying coverage of security essentials

- Multiple access points
- No proper hardening
- No proper monitoring
- No proper governance
- Partial data on assets & events
- No proper planning & accountability

Remote employees, control system vendors, 3rd party vendors, contractors
ICS Shield™ Deployment

Distributed architecture and secure tunnel between site and SOC

- Install SC at the data center
- Install VSEs at each plant
- Establish a secure tunnel, outbound, using port 443, TLS encrypted
- One FW rule to manage all remote connections
Remote Access Flow:
Fast And Secure Access Of Experts To Assets

Supported remote access:
- RDP
- VNC
- Telnet
- SSH
- HTTP/HTTPS

Vendor-Based:
- Simatic
- RSLinx/Logix
- Centum
- ... and all TCP & UDP based protocols

1. 3rd party want to access an assets
2. User is authenticated
3. SC ask CS to open a tunnel
4. VSE polling the CS for requests
5. Following a certificate based handshake, TLS encrypted outbound tunnel is established
6. Plant can approve/deny access, and thereafter supervise, record and terminate the remote session
7. Following approval session is initiated with granular privilege
Demo – Risk Manager and ICS Shield Together
Risk Manager **excels at:**

- Being able to measure, monitor & manage risk
- Enterprise-wide dashboard visibility
- Out of the box recommendations for immediate action

“Risk Manager shows you what you need to do”

ICS Shield **strengths:**

- Asset **Discovery**
- **Connect** via Secure Remote Access
- **Protect** through multi-vendor monitoring and patching

“ICS Shield™ helps you do it!”
Get this Hot Deal at EMEA HUG:
SMX systems for €8,500 each and discounted SMX ATIX subscriptions (up to €24,000 total savings)

Visit the Promotions Center to learn more.

See details at www.hwwl.co/HUG18offers. These limited-time discounts and offerings are only available and valid for new inquiries and commitments made at 2018 EMEA HUG in Madrid, Spain, October 1–4. Orders must be placed within 90 days of receiving a proposal.
Thank you!
Backup Slides
Enterprise Risk Manager at Level 4 can forward data to a Level 4 SIEM

Syslog in R170 adds to Risk Manager existing capabilities:
- Forward to a SIEM in L3 or L3.5 or to a forwarding device to L4
- Calculations are available as SYSLOG output in either CSV or KVP

Using the Risk Manager Syslog Forwarding feature can eliminate the need for procuring, licensing, and configuring a third party syslog forwarding solution
Additional Features of IERM | Secure SYSLOG → Level 4

- Use same mechanism as ERM to securely forward SYSLOG messages to Level 4
  - Risk Manager can receive SYSLOG from multiple ICS devices
    - Set up devices to send SYSLOG to Risk Manager
    - Risk Manager configured to receive sent SYSLOGs
  - Risk Manager will forward the SYSLOG messages to Level 4 Enterprise Risk Manager
    - IERM will send all received SYSLOG messages to SIEM
R170 | Analysis Views

“Power User” Analytics to Understand and Act on Industrial Cyber Security Risks

- Drag-and-drop report creation helps simplify risk analytics: No configuration or programming required
- Location hierarchy view expedites search and analysis across sites
- Save and Save As report options help simplify report documentation
- Table and trend views of KPIs expedite analysis
- 8 standard reports included from integrated Risk Manager dashboard
Discover – The Starting Point For A Secure ICS

End-to-end visibility into the ICS

- Asset Discovery down to L2
- Configuration collection
- Change monitoring
- Classification & labeling
- Visualization
- Assets labeling
Connect – Expert To Asset, Fast And Secured

Improving Assets Reliability & Safety

AAA Remote Access Control

- Centralized authentication
- Granular privilege
- Accountability with full audit
- Real-time supervision and session termination
- Vault
- Files & Data transfer
Minimize manual effort and human mistakes

Improve security and compliance by standardizing on:

- Plant-wide policies
- System Patching
- Anti-virus
Case Study 1 – Discovery And Inventory

Multi-National Conglomerate

• Active & passive discovery
• Down to level 2
• 30 plants a year
• >200 plants in plan
• >1000 field assets/plant

SOLUTION BENEFITS

✓ Visibility of ICS network
✓ Inventory control
✓ Vulnerability snapshot
Case Study 2 – Secure Remote Access

Global Pulp & Paper Enterprise
• 150 plants
• 400-1000 field assets/plant
• 60 vendors
• 1500 routine users

SOLUTION BENEFITS
 ✓ 60 ➔ 1 remote access entry
 ✓ Reduced risk to ICS network
 ✓ Reduce TTR
Case Study 3 – Secure Remote Access

Global Chemical & Plastics Producer
- 130 plants
- 500-1200 field assets/plant
- ~80 vendors and 3rd party
- 25,000 users

SOLUTION BENEFITS
✓ ~80 ➔ 1 remote access entry point
✓ 30% operational savings
✓ Increased compliance
Case Study 4 – Security Essentials Coverage

Global Tier-1 Oil & Gas Enterprise
• 30 upstream & downstream plants
• More plants are pending
• Outsourcing Operations
• 2500 users
• Shielding 400-1600 field assets/plant

SOLUTION BENEFITS
✓ Drove annual cost savings
✓ Reduced risk to ICS network
✓ Increased compliance

Asset Inventory
• Semi-Automated Collection of PCD Assets and Asset Information

Process Control Domain (PCD) Access
• Standardised Remote Access on a Single Platform

Maturity Reporting
• Centralised, Automated Maturity & Compliance Reporting

Patch Management
• Automate QPL Synchronisation and Standardized, Automated Patching

Anti-Virus Management
• Automated Update of Approved AV Signature Files

Log Collection
• Leverages Group Standard SIEM for Global Awareness
ICS Shield™: Secure Tunnel and Communication Server

Maintain data integrity and reducing the attack surface

✓ TPM Trusted Platform Module - Mutual authentication between VSE and SC using standard public key/private key cryptography protocols
✓ Modified Purdue PERA compliant through VSP(proxies) and VSF(flippers)
✓ Application/Activity Granularity(2018)
✓ RDP and VNC Supervision and Recording of sessions
✓ Password Vault
✓ Transfer files & data from plant to SOC and from SOC to plants
✓ Tunnel overcomes unstable network conditions
✓ Can handle any type of remote connection over a single outbound port

Communication Server
Installed at the data center DMZ
Manage all communication between SC & VSE
Bridge remote access tunnel

Secure Tunnel Technology
Outbound only, port 443
To a specific IP address
Single FW rule
TLS 1.2- encrypted

PR.DS-2: Data-in-transit is protected
ICS Shield™ System Architecture

WMI / SNMP / OPC / SSH / HTTP / Telnet (CLI) / VNC
/ RDP / SFTP / FTP / RSLinx / RSLogix / SIMATIC
Any Proprietary TCP or UDP based protocols
Windows | Networking | Industrial
### Site Compliance Report

#### January 19, 2017

**Secure Plant Middle**

<table>
<thead>
<tr>
<th>Custodian</th>
<th>Exposure</th>
<th>IP</th>
<th>Type</th>
<th>AV Definitions</th>
<th>AV Installed</th>
<th>AV Service</th>
<th>Backup</th>
<th>Completeness</th>
<th>Logs</th>
<th>OS Patches</th>
<th>Supported OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smith</td>
<td>High</td>
<td>192.168.201.1</td>
<td>Network Dev</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>False</td>
</tr>
<tr>
<td>Smith</td>
<td>Medium</td>
<td>192.168.201.129</td>
<td>Connected</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>Smith</td>
<td>Medium</td>
<td>192.168.201.14</td>
<td>Connected</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>Smith</td>
<td>Medium</td>
<td>192.168.201.177</td>
<td>Connected</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>Smith</td>
<td>Medium</td>
<td>192.168.201.187</td>
<td>Connected</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>False</td>
</tr>
<tr>
<td>Smith</td>
<td>Low</td>
<td>192.168.201.14</td>
<td>Connected</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>Smith</td>
<td>High</td>
<td>192.168.201.127</td>
<td>Connected</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>Smith</td>
<td>Medium</td>
<td>192.168.201.228</td>
<td>Connected</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
</tr>
<tr>
<td>Smith</td>
<td>Medium</td>
<td>192.168.201.241</td>
<td>Connected</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
</tr>
<tr>
<td>Smith</td>
<td>Medium</td>
<td>192.168.201.251</td>
<td>Network Dev</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>Smith</td>
<td>Low</td>
<td>192.168.201.94</td>
<td>Connected</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>Alexey</td>
<td>High</td>
<td>192.168.22</td>
<td>Network Dev</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
</tr>
</tbody>
</table>
Active Asset Discovery and Inventory

LOGICAL WORKFLOW BASICS

The asset discovery high level workflow for detecting new devices is based on the following steps:

• VSEs will systematically scan designated DCS networks for existing and added assets
• Get all the required Properties from the Discovery Engine settings.
• With the given configuration and the IP range, execute network search for all the existing devices:
  ❖ **Windows machines:** WMI and run PowerShell commands on ports 135, 445, 3389
  ❖ **Linux Machines:** SSH on ports 22, 23
  ❖ **Networking equipment:** SNMP on port 161
• Each detected device will be classified according to its OS (based on ports scan)
• Once devices are added, the VSE will connect to them, using given credentials (read only), in order to collect inventory data points, such as: Asset tag, Manufacturer, Operating System information, CPU, Memory, and many others.
• The above collected information will be transmitted to the Security Center via port 443 outbound and will be assigned to the designated asset/device.
Configuration Data For Windows Devices

Configuration data is collected periodically

Automatically Collected via WMI
- IP addresses
- MAC addresses
- OS name and version
- Application software name and version
- OS patches name and date
- HW manufacturer and model
- AV agent name and version
- AV signatures file version and date
- AV service status
- Additional upon request

Added manually
- Custodian
- Criticality (C, E, N)
- Type (monitoring system, safety system, workstation, server…)
- Vendor
- Vendor software
- Function (metering, engineering station,..)
- Life-cycle (active, inactive …)
- Deviation (free text)
Configuration Data For Linux Devices

Configuration data is collected periodically

Automatically Collected via SSH
- IP addresses
- MAC addresses
- OS name and version
- Application software name and version
- OS patches name and date
- HW manufacturer and model
- AV agent name and version
- AV signatures file version and date
- AV service status
- Additional upon request

Added manually
- Custodian
- Criticality (C, E, N)
- Type (monitoring system, safety system, workstation, server…)
- Vendor
- Vendor software
- Function (metering, engineering station,..)
- Life-cycle (active, inactive …)
- Deviation (free text)
Configuration Data For Networking Devices

Automatically Collected via SNMP
- IP addresses
- MAC addresses
- Serial number
- Firmware revision
- HW manufacturer and model
- Device attributes
- Location
- Description
- Additional upon request

Added manually
- Custodian
- Criticality (C, E, N)
- Type (monitoring system, safety system, firewall, router…)
- Vendor
- Vendor software
- Life-cycle (active, inactive…)
- Deviation (free text)
### Supported Protocols

<table>
<thead>
<tr>
<th>OT protocols</th>
<th>IT Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC 60870-5-104</td>
<td>SMB/CIFS</td>
</tr>
<tr>
<td>DNP3</td>
<td>RPC/DCOM</td>
</tr>
<tr>
<td>ICCP TASE.2</td>
<td>LDAP</td>
</tr>
<tr>
<td>IEC 61850 (MMS, GOOSE, SV)</td>
<td>NetBIOS</td>
</tr>
<tr>
<td>IEEE C37.118 (Synchrophasor)</td>
<td>HTTP</td>
</tr>
<tr>
<td>Modbus/TCP</td>
<td>(T)FTP</td>
</tr>
<tr>
<td>EtherNet/IP</td>
<td>SSH</td>
</tr>
<tr>
<td>CSLib (ABB 800xA)</td>
<td>SSL</td>
</tr>
<tr>
<td>DMS (ABB AC 800 F)</td>
<td>SMTP</td>
</tr>
<tr>
<td>MMS (ABB AC 800 M)</td>
<td>IMAP</td>
</tr>
<tr>
<td>Step7 (Siemens)</td>
<td>POP3</td>
</tr>
<tr>
<td>OMS+ (Siemens)</td>
<td>VNC/RFB</td>
</tr>
<tr>
<td>OPC-DA</td>
<td>RDP</td>
</tr>
<tr>
<td>OPC-AE</td>
<td>Telnet</td>
</tr>
<tr>
<td>DeltaV (Emerson)</td>
<td>SNMP</td>
</tr>
<tr>
<td>Ovation (Emerson)</td>
<td>NTP</td>
</tr>
<tr>
<td>Vnet/IP (Yokogawa)</td>
<td>DNS</td>
</tr>
<tr>
<td>BACnet</td>
<td>Radius</td>
</tr>
<tr>
<td>PROFINET</td>
<td>Kerberos</td>
</tr>
<tr>
<td>Rockwell CIP extensions</td>
<td>MS-SQL</td>
</tr>
<tr>
<td>Experion (Honeywell)</td>
<td>SunRPC</td>
</tr>
<tr>
<td>OASyS (Telvent)</td>
<td>…and others…</td>
</tr>
</tbody>
</table>

---
Enjoy The Upside Of Connected Plants & Minimize Risk

Summary

• Assess your level of industrial cyber security maturity
• Manage cyber security as a program
• Solve the immediate challenges with clear ROI
• Ensure value for central IT as well as plant people
• Focus on the essentials
• Choose the right experienced partner
• Consider outsourcing planning, implementation and management
## Risk Source

Last updated less than a minute ago

<table>
<thead>
<tr>
<th>Source</th>
<th>Severity</th>
<th>Classification</th>
<th># of Devices</th>
<th>Risk Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Patches Missing (Non-Security)</td>
<td>High</td>
<td>Vulnerability</td>
<td>1 Device</td>
<td>Patches</td>
</tr>
<tr>
<td>Windows Patch Definitions Out of Date</td>
<td>High</td>
<td>Vulnerability</td>
<td>1 Device</td>
<td>Patches</td>
</tr>
<tr>
<td>Windows Patches Missing (Security)</td>
<td>Medium</td>
<td>Vulnerability</td>
<td>2 Devices</td>
<td>Patches</td>
</tr>
</tbody>
</table>

### Backup

![Backup Icon]
Windows Patches Missing (Non-Security) last updated less than a minute ago

<table>
<thead>
<tr>
<th>Severity</th>
<th>Classification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Vulnerability</td>
<td>A non-security patch is missing</td>
</tr>
</tbody>
</table>

Affected Devices

- Device: ICE-RM001S
  - Risk Score: 100
  - Risk Indicators: 13
  - Current Indicators: High
  - Severity: High
  - Details:
    - Missing Non-Security Patch Count: 6
    - 6 Missing Patches More Than 90 Days Old: KB2937495, KB29334051, KB2937892, KB29384439, KB29359877
    - 0 Missing Patches Less Than 90 Days Old:

Guidance

- Possible Causes
  - A non-security patch has not been applied

- Potential Impact
  - Available bug fixes or improvements are missing. This may impact reliability.

Recommended Actions

- Patch should be applied during the next patch cycle
Windows Patches Missing (Non-Security)

- Severity: High
- Classification: Vulnerability
- Description: A non-security patch is missing

Affected Devices

- ICE-RM001S
  - Device Risk Score: 100
  - Device Risk Indicators: 13
  - Current Indicators: High
  - Score: 94
  - Details: Missing Non-Security Patch Count: 6
    6 Missing Patches More Than 90 Days Old: KB929229, KB929229, KB929229, KB929229, KB929229, KB929229
    0 Missing Patches Less Than 90 Days Old:

Guidance

Possible Causes
- A non-security patch has not been applied

Potential Impact
- Available bug fixes or improvements are missing. This may impact reliability.

Recommended Actions
- Patch should be applied during the next patch cycle.

Activate Windows
Go to System in Control Panel to activate Windows.
### Network Risk from Connected Devices

<table>
<thead>
<tr>
<th>Severity</th>
<th>Classification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Threat</td>
<td>Indicates the risk to this device caused by other devices in the system.</td>
</tr>
</tbody>
</table>

### Affected Devices

<table>
<thead>
<tr>
<th>Device</th>
<th>Device Risk Score</th>
<th>Device Risk Indicators</th>
<th>Current Indicators Severity</th>
<th>Score</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICE-VO10C</td>
<td>100</td>
<td>8</td>
<td>High</td>
<td>100</td>
<td>10.10.30.252: NET-Rogue-Device-Detected-Wired</td>
</tr>
<tr>
<td>ICE-V015G</td>
<td>100</td>
<td>10</td>
<td>High</td>
<td>100</td>
<td>10.10.30.252: NET-Rogue-Device-Detected-Wired</td>
</tr>
<tr>
<td>ICE-AWL0101S</td>
<td>100</td>
<td>10</td>
<td>High</td>
<td>100</td>
<td>10.10.30.252: NET-Rogue-Device-Detected-Wired</td>
</tr>
<tr>
<td>ICE-V0004C</td>
<td>100</td>
<td>10</td>
<td>High</td>
<td>100</td>
<td>10.10.30.252: NET-Rogue-Device-Detected-Wired</td>
</tr>
<tr>
<td>ICE-RM001LS</td>
<td>100</td>
<td>13</td>
<td>High</td>
<td>100</td>
<td>10.10.30.252: NET-Rogue-Device-Detected-Wired</td>
</tr>
<tr>
<td>ICE-V0007C</td>
<td>100</td>
<td>10</td>
<td>High</td>
<td>100</td>
<td>10.10.30.252: NET-Rogue-Device-Detected-Wired</td>
</tr>
</tbody>
</table>

### Guidance

**Possible Causes**

- Risk from another device in the system is increasing the base risk of this device.
Demo – Risk Manager and ICS Shield™ Together
## All Devices

<table>
<thead>
<tr>
<th>Device Name</th>
<th>Device Address</th>
<th>Product Line</th>
<th>Model</th>
<th>Version</th>
<th>Active</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery Engine</td>
<td>127.0.0.1</td>
<td>NextNine, Asset Discovery V2</td>
<td>Engine</td>
<td>1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ePO Sync</td>
<td>10.8.123.233</td>
<td>NextNine, McAfee ePO Management</td>
<td>McAfee ePolicy Orchestrator</td>
<td>5.1.X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File Expander</td>
<td>127.0.0.3</td>
<td>NextNine, VSE Utilities</td>
<td>Windows</td>
<td>Big Dipper</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICS Jobs</td>
<td>127.0.0.2</td>
<td>NextNine, VSE Utilities</td>
<td>Windows</td>
<td>Big Ben</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NSDemoApp</td>
<td>10.8.123.230</td>
<td>NextNine, Windows Machine</td>
<td>Connected</td>
<td>1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NSDemoAVSim</td>
<td>10.8.123.232</td>
<td>NextNine, Windows Machine</td>
<td>Connected</td>
<td>1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NSDemoAVSite</td>
<td>10.8.123.233</td>
<td>NextNine, Windows Machine</td>
<td>Connected</td>
<td>1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NSDemoDB</td>
<td>10.8.123.229</td>
<td>NextNine, Windows Machine</td>
<td>Connected</td>
<td>1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NSDemoSrvVSE</td>
<td>10.8.123.228</td>
<td>NextNine, Windows Machine</td>
<td>Connected</td>
<td>1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NSDemoVOSEL3</td>
<td>10.8.123.231</td>
<td>NextNine, Windows Machine</td>
<td>Connected</td>
<td>1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NSDemoWSUSSim</td>
<td>10.8.123.234</td>
<td>NextNine, Windows Machine</td>
<td>Connected</td>
<td>1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Self-Monitoring</td>
<td>6.0.0.0</td>
<td>Remote Services, VSE Self-Monitoring</td>
<td>Windows</td>
<td>Big Dipper</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WSUS Sync</td>
<td>127.0.0.1</td>
<td>NextNine, WSUS</td>
<td>WSUS HTTP</td>
<td>Big Ben</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Total: 13**

**Active: 11**
<table>
<thead>
<tr>
<th>Status</th>
<th>Case</th>
<th>Severity</th>
<th>Description</th>
<th>System</th>
<th>Device</th>
<th>Detected Time (User)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Ack</td>
<td></td>
<td></td>
<td>[SEC][24H] EventCode 4732 - 2 time(s), EventCode 4733 - 2 time(s) indicates that LoC</td>
<td>ICS-Shield</td>
<td>D-SN03 <em>SUPP</em></td>
<td>15-JUN-2018 18:10:54</td>
</tr>
<tr>
<td>Not Ack</td>
<td></td>
<td></td>
<td>[SEC][24H] EventCode 4732 - 2 time(s), EventCode 4733 - 2 time(s) indicates that LoC</td>
<td>ICS-Shield</td>
<td>D-SN03 <em>SUPP</em></td>
<td>15-JUN-2018 17:10:53</td>
</tr>
<tr>
<td>Not Ack</td>
<td></td>
<td></td>
<td>[SEC][24H] EventCode 4732 - 2 time(s), EventCode 4733 - 2 time(s) indicates that LoC</td>
<td>ICS-Shield</td>
<td>D-SN03 <em>SUPP</em></td>
<td>15-JUN-2018 15:10:54</td>
</tr>
<tr>
<td>Not Ack</td>
<td></td>
<td></td>
<td>[SEC][AV][24H] McAfee antivirus is not installed</td>
<td>EPKS FTE1</td>
<td>D-ES11 <em>SUPP</em></td>
<td>15-JUN-2018 14:00:48</td>
</tr>
<tr>
<td>Not Ack</td>
<td></td>
<td></td>
<td>[SEC][AV][24H] McAfee antivirus is not installed</td>
<td>EPKS FTE1</td>
<td>D-ES11 <em>SUPP</em></td>
<td>15-JUN-2018 14:00:44</td>
</tr>
<tr>
<td>Not Ack</td>
<td></td>
<td></td>
<td>[SEC][AV][24H] McAfee antivirus is not installed</td>
<td>EPKS FTE1</td>
<td>D-ES21B <em>SUPP</em></td>
<td>15-JUN-2018 14:00:40</td>
</tr>
<tr>
<td>Not Ack</td>
<td></td>
<td></td>
<td>[AV][1W] installed version of Symantec not supported by Honeywell</td>
<td>EPKS FTE1</td>
<td>D-ES21B <em>SUPP</em></td>
<td>15-JUN-2018 14:00:37</td>
</tr>
<tr>
<td>Not Ack</td>
<td></td>
<td></td>
<td>[AV][1W] installed version of Symantec not supported by Honeywell</td>
<td>EPKS FTE1</td>
<td>D-ES11 <em>SUPP</em></td>
<td>15-JUN-2018 13:50:32</td>
</tr>
<tr>
<td>Not Ack</td>
<td></td>
<td></td>
<td>[SEC][24H] EventCode 4732 - 2 time(s), EventCode 4733 - 2 time(s) indicates that LoC</td>
<td>ICS-Shield</td>
<td>D-SN03 <em>SUPP</em></td>
<td>15-JUN-2018 13:10:52</td>
</tr>
<tr>
<td>Not Ack</td>
<td></td>
<td></td>
<td>[SEC][24H] USB Mass Storage devices are not restricted with current security policy</td>
<td>EPKS FTE1</td>
<td>D-ES11 <em>SUPP</em></td>
<td>15-JUN-2018 12:02:15</td>
</tr>
</tbody>
</table>