Cybersecurity for Control Systems
COMPANY BACKGROUND
NEXDEFENSE SOPHIA™ SOLUTION

• **Passive** monitoring software
• Control system **Network Security Monitoring** solution
• **Automatic Discovery** of active devices on network
• **Visualization** of control system network activity
• Creates **Baseline** of expected communications
• **Monitoring & Alerting**
  – Alerting on unknown or suspicious activity
  – White/Blacklisting of communications
• **Notifications** for remediation process
Use Cases

- **Asset Discovery**
  - Active nodes and their connections automatically discovered
  - MAC address lookup
  - Geo-location of external nodes

- **Network Baselining**
  - Established and non-established connections
  - Create and validate a whitelist of good communications

- **Intrusion Detection**
  - Deep Packet Inspection of control and selective IT protocols
  - Access to the DPI engine to create/add custom signatures

- **Network Operations**
  - Plan or validate network segmentation
  - Identify misconfigured or unauthorized devices and connections
  - Spot network bottlenecks
  - FAT/SAT testing
**Product Enhancements**

**“NO BLIND SPOTS”**
- Detecting 60+ protocols via Deep Packet Inspection
- Every connected device visible (Layer-2 and higher)
- Now “seeing” devices/activities previously hidden

**USER-DEFINED CUSTOMIZATION**
- Tailor-fit 3D views and grouping to real-world systems
- Refined Tree-view (Device, Protocol and Connection)
  - Protocols on non-standard ports
  - VLAN tracking
  - IPv6 communications (largely ignored)

**EXPANDED DATA ANALYSIS, VIEWS & REPORTS**
- ICS Protocol Analysis for control commands
- Expanded event and alert database
- Enhanced filtering and data outputs

**DEVICE TRACABILITY**
- Tracking device connectivity by Network
- Accommodating Duplicate IPs on different Networks
EXPANDED, REAL-TIME CONTROL PROTOCOL
DEEP PACKET INSPECTION AND ANALYSIS

Overcoming Network Blind Spots

Deep Packet Inspection (DPI)

- Tracks and alerts on device activity at lowest communication levels
- Evaluates new devices, connections and data payloads for ICS protocols
- Detects 60+ network protocols
  - Industrial Control Protocols (ICS)
  - Standard Ethernet Suite (L2-L7)
- Distinguish ports & protocols based on packet payloads

**Layer-2 Protocols**
Ethernet FRAMES exchanged between devices. Relies on hardware addressing without IP packet data formatting. Non-routable off the physical link. No Network protocols (e.g. no TCP/UDP).

**Examples:**
- CC-Link (Mitsubishi)
- EtherCAT (Beckhoff)
- Ethernet Powerlink (B&R)
- PROFINET RT (Siemens)
- SERCOS III (Bosch Rexroth)
- Some proprietary variants

**Layer-7 Protocols**
Ethernet APPLICATION protocols built around IP PACKETS. Relies on MAC and IP addresses and is routable to other networks. IP packets encapsulated inside TCP/UDP for data exchange.

**Examples:**
- BACnet/IP
- DNP3
- EtherNet/IP (Rockwell)
- Foundation Fieldbus HSE
- IEC 61850 (aka GOOSE)
- Modbus TCP (Schneider)
- OPC
- PROFINET (Siemens)
- Some proprietary variants

**Application (7)**
Serves as the window for users and application processes to access the network.

**Presentation (6)**
Formats the data to be presented to the application layer. Relies on the "Translator" for network.

**Session (5)**
Allows session establishment between processes running on different devices.

**Transport (4)**
Serves as the end-to-end link in a network and adds no losses or duplications.

**Network (3)**
Defines the protocols of the network. decides which physical path the data takes.

**Data Link (2)**
Provides error-free transfer of data frames from one node to another over the physical layer.

**Physical (1)**
Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.
Assists sector asset owners and operators to fulfill CSF requirements for...

- Regular asset inventories
- Continuous network monitoring
- Issuance of alerts & alarms
- Change management comparisons
- Event tracking of abnormalities that may affect safety and reliability

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Compliance Fit</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDENTIFY (ID)</td>
<td>Asset Management (ID.AM)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risk Assessment (ID.RA)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risk Management Strategy (ID.RM)</td>
<td></td>
</tr>
<tr>
<td>PROTECT (PR)</td>
<td>Access Control (PR.AC)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data Security (PR.DS)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information Protection Processes &amp; Procedures (PR.IP)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Maintenance (PR.MA)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Protective Technology (PR.PT)</td>
<td></td>
</tr>
<tr>
<td>DETECT (DE)</td>
<td>Anomalies and Events (DE.AE)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security Continuous Monitoring (DE.CM)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Detection Processes (DE.DP)</td>
<td></td>
</tr>
<tr>
<td>RESPOND (RS)</td>
<td>Response Planning (RS.RP)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Communications (RS.CO)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Analysis (RS.AN)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mitigation (RS.MI)</td>
<td></td>
</tr>
<tr>
<td>RECOVER (RC)</td>
<td>Communications (RC.CO)</td>
<td></td>
</tr>
</tbody>
</table>
Preston Futrell
preston.futrell@nexdefense.com