



NEX DEFENSE

**Cybersecurity
for
Control Systems**

COMPANY BACKGROUND



NEX DEFENSE



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



SOPHIA VERSION 2.1

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

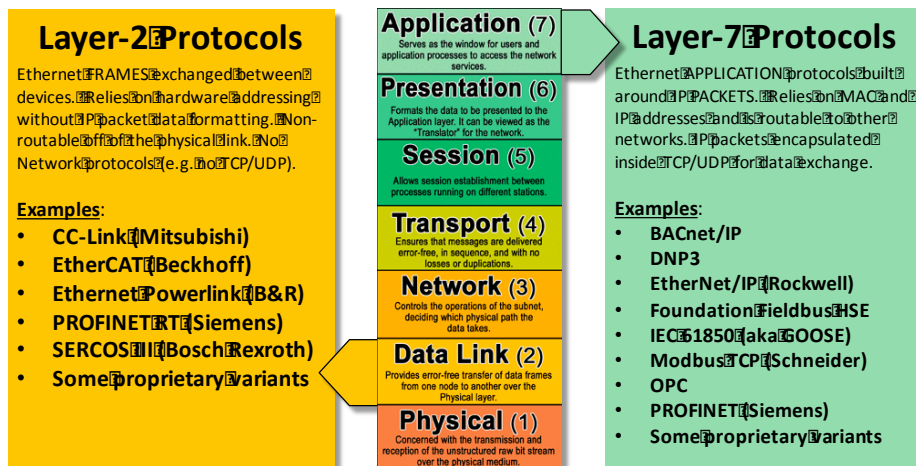


EXPANDED, REAL-TIME CONTROL PROTOCOL DEEP PACKET INSPECTION AND ANALYSIS

Deep Packet Inspection (DPI)

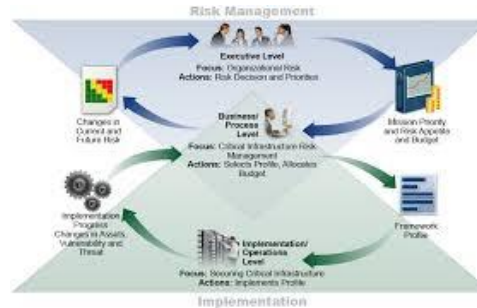
Overcoming Network Blind Spots

- 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

NIST CYBERSECURITY FRAMEWORK & SOPHIA



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

Function	Category	Compliance Fit
IDENTIFY (ID)	Asset Management (ID.AM)	 SOPHIA™
	Risk Assessment (ID.RA)	
	Risk Management Strategy (ID.RM)	
PROTECT (PR)	Access Control (PR.AC)	
	Data Security (PR.DS)	
	Information Protection Processes & Procedures (PR.IP)	
	Maintenance (PR.MA)	
	Protective Technology (PR.PT)	
DETECT (DE)	Anomalies and Events (DE.AE)	
	Security Continuous Monitoring (DE.CM)	
	Detection Processes (DE.DP)	
RESPOND (RS)	Response Planning (RS.RP)	
	Communications (RS.CO)	
	Analysis (RS.AN)	
	Mitigation (RS.MI)	
RECOVER (RC)	Communications (RC.CO)	



Preston Futrell
preston.futrell@nexdefense.com