Appendix D

Cisco Cyber Vision vs. Cisco Secure Network Analytics (formerly Stealthwatch)

Cisco Secure Network Analytics and Cisco Cyber Vision are two Cisco security offerings to provide visibility on the network. This section explains their different strengths and recommended role in the industrial network.

Cisco Secure Network Analytics provides enterprise-wide network visibility and applies advanced security analytics to detect and respond to threats in real time. Using a combination of behavioral modeling, machine learning, and global threat intelligence, Secure Network Analytics can quickly, and with high confidence, detect threats such as command-and-control (C&C) attacks, ransomware, distributed-denial-of-service (DDoS) attacks, illicit crypto mining, unknown malware, and insider threats. With a single, agentless solution, you get comprehensive threat monitoring, even if it is encrypted. Secure Network Analytics focuses on Enterprise IT networks and requires the packets to have an IP address. It is recommended for network devices in Levels 3 to 5 in the Purdue model.

Cisco Cyber Vision is an ICS visibility solution specifically designed to ensure continuity, resilience, and safety of industrial operations. It monitors industrial assets and application flows to extend IT security to the OT domain through easy deployment within the industrial network. It focuses on industrial networks and protocols. Cisco Cyber Vision has the capability of detecting Layer 2 flows and is recommended for Levels 0 to 3 in the Purdue model.