Detection of Rogue Master, Detection Strategy DET0792

Archived: 2026-04-05 12:58:46 UTC

AN1924

Consult asset management systems which may help with the detection of computer systems or network devices that should not exist on a network.
Monitor for network traffic originating from unknown/unexpected devices or addresses. Local network traffic metadata could be used to identify unexpected connections, including unknown/unexpected source MAC addresses connecting to ports associated with operational protocols. Also, network management protocols such as DHCP and ARP may be helpful in identifying unexpected devices.
Monitor for new master devices communicating with outstations, which may be visible in alarms within the ICS environment.
Monitor for unexpected ICS protocol functions from new and existing devices. Monitoring known devices requires ICS function level insight to determine if an unauthorized device is issuing commands (e.g., a historian).
Monitor for new master devices communicating with outstation assets, which may be visible in asset application logs.

Log Sources
