Network Segmentation, Mitigation M0930 - ICS

Archived: 2026-04-05 15:13:19 UTC

ICS T0800 Activate Firmware Update Mode

Segment operational network and systems to restrict access to critical system functions to predetermined management systems. [3]

ICS T0830 Adversary-in-the-Middle

Network segmentation can be used to isolate infrastructure components that do not require broad network access. This may mitigate, or at least alleviate, the scope of AiTM activity.

ICS T0878 Alarm Suppression

Segment operational assets and their management devices based on their functional role within the process. Enabling more strict isolation to more critical control and operational information within the control environment. [4] [5] [3] [6]

ICS T0802 Automated Collection

Prevent unauthorized systems from accessing control servers or field devices containing industrial information, especially services used for common automation protocols (e.g., DNP3, OPC).

ICS T0805 Block Serial COM

Restrict unauthorized devices from accessing serial comm ports.

ICS T0806 Brute Force I/O

Segment operational assets and their management devices based on their functional role within the process. Enabling more strict isolation to more critical control and operational information within the control environment. [4] [5] [3] [6]

ICS T0858 Change Operating Mode

Segment operational network and systems to restrict access to critical system functions to predetermined management systems. [3]

ICS T0885 Commonly Used Port

Configure internal and external firewalls to block traffic using common ports that associate to network protocols that may be unnecessary for that particular network segment.

ICS T0868 Detect Operating Mode

Segment operational network and systems to restrict access to critical system functions to predetermined management systems. [3]

ICS T0816 Device Restart/Shutdown

Segment operational network and systems to restrict access to critical system functions to predetermined management systems. [3]

ICS T0819 Exploit Public-Facing Application

Segment externally facing servers and services from the rest of the network with a DMZ or on separate hosting infrastructure.

ICS T0866 Exploitation of Remote Services

Segment networks and systems appropriately to reduce access to critical system and services communications.

ICS T0822 External Remote Services

Deny direct remote access to internal systems through the use of network proxies, gateways, and firewalls. Consider a jump server or host into the DMZ for greater access control. Leverage this DMZ or corporate resources for vendor access. [5]

ICS T0883 Internet Accessible Device

Deny direct remote access to internal systems through the use of network proxies, gateways, and firewalls. Steps should be taken to periodically inventory internet accessible devices to determine if it differs from the expected.

ICS T0838 Modify Alarm Settings

Segment operational network and systems to restrict access to critical system functions to predetermined management systems. [3] [7]

ICS T0839 Module Firmware

Segment operational network and systems to restrict access to critical system functions to predetermined management systems. [3]

ICS T0842 Network Sniffing

Segment networks and systems appropriately to reduce access to critical system and services communications.

ICS T0861 Point & Tag Identification

Segment operational assets and their management devices based on their functional role within the process. Enabling more strict isolation to more critical control and operational information within the control environment. [4] [5] [3] [6]

ICS T0843 Program Download

Segment operational network and systems to restrict access to critical system functions to predetermined management systems. [3]

ICS T0845 Program Upload

Segment operational network and systems to restrict access to critical system functions to predetermined management systems. [3]

ICS T0886 Remote Services

Segment and control software movement between business and OT environments by way of one directional DMZs. Web access should be restricted from the OT environment. Engineering workstations, including transient cyber assets (TCAs) should have minimal connectivity to external networks, including Internet and email, further limit the extent to which these devices are dual-homed to multiple networks. [8]

ICS T0848 Rogue Master

Segment operational assets and their management devices based on their functional role within the process. Enabling more strict isolation to more critical control and operational information within the control environment. [4] [5] [3] [6]

ICS T0881 Service Stop

Segment operational network and systems to restrict access to critical system functions to predetermined management systems. [3]

ICS T0856 Spoof Reporting Message

Segment operational assets and their management devices based on their functional role within the process. Enabling more strict isolation to more critical control and operational information within the control environment. [4] [5] [3] [6]

ICS T0869 Standard Application Layer Protocol

Ensure proper network segmentation between higher level corporate resources and the control process environment.

ICS T0857 System Firmware

Segment operational network and systems to restrict access to critical system functions to predetermined management systems. [3]

ICS T0864 Transient Cyber Asset

Segment and control software movement between business and OT environments by way of one directional DMZs. Web access should be restricted from the OT environment. Engineering workstations, including transient

cyber assets (TCAs) should have minimal connectivity to external networks, including Internet and email, further limit the extent to which these devices are dual-homed to multiple networks. [8]

ICS T0855 Unauthorized Command Message

Segment operational assets and their management devices based on their functional role within the process. Enabling more strict isolation to more critical control and operational information within the control environment. [4] [5] [3] [6]
