Threat Category: Unauthorized Access, Telnet Monitoring

Threat Description: The SNORT rule telnet_detect_1000017 is designed to detect connection attempts to the Telnet service over TCP port 23.

Indicators of Compromise (IoCs):

Destination Port: 23 (Telnet)

Protocol: TCP

Detection Mechanism:

Traffic Direction: -> (from any source to any destination)

Port Check: Destination TCP port 23

Possible Attribution & Use Cases:

Could be triggered by network scans looking for exposed Telnet services.

May indicate brute-force attempts or unauthorized access to network devices.

Recommended Actions:

Determine if the Telnet attempt was authorized. Correlate with user activity or device behavior.

Block Telnet (port 23) at the network perimeter and on internal segments unless absolutely necessary.

Migrate to SSH for secure remote access.

Author & Attribution:

Rule Author: Community

Rule Source:

SID: 1000017

Revision: 1