Detection of Connection Proxy, Detection Strategy DET0759

Archived: 2026-04-02 12:27:04 UTC

AN1891

Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g., extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g., monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)).
Monitor for known proxy protocols (e.g., SOCKS, Tor, peer-to-peer protocols) and tool usage (e.g., Squid, peer-to-peer software) on the network that are not part of normal operations. Also monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.

Log Sources
