Detection of Standard Application Layer Protocol, Detection Strategy DET0799

Archived: 2026-04-02 12:45:00 UTC

AN1931

Monitor and analyze traffic flows that do not follow the expected protocol standards and traffic flows (e.g., extraneous packets that do not belong to established flows , or gratuitous or anomalous traffic patterns). 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 and analyze traffic patterns and packet inspection associated to protocol(s), leveraging SSL/TLS inspection for encrypted traffic, 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)).

Log Sources
